Лучшие классические учебники

И. М. ВИНОГРАДОВ

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

ЛАНЬ

Знание
Уверенность
Успех

ЛУЧШИЕ КЛАССИЧЕСКИЕ УЧЕБНИКИ

МАТЕМАТИКА

И. М. ВИНОГРАДОВ

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

УЧЕБНОЕ ПОСОБИЕ

Издание одиннадцатое,
стереотипное

САНКТ-ПЕТЕРБУРГ · МОСКВА · КРАСНОДАР
2006

ББК 22.13
В 49

Виноградов И. М.

В 49 Основы теории чисел: Учебное пособие. 11-е изд., стер. — СПб.: Издательство «Лань», 2006. — 176 с. — (Учебники для вузов. Специальная литература).

ISBN 5-8114-0535-9

В книге излагаются основы теории чисел в объеме университетского курса. Для студентов математических специальностей университетов и педвузов, аспирантов, научных работников в области математики.

ББК 22.13

Иван Матвеевич ВИНОГРАДОВ

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

УЧЕБНОЕ ПОСОБИЕ

Издание одиннадцатое,
стереотипное

Генеральный директор *А. Л. Кноп.* Директор издательства *О. В. Смирнова*
Художественный редактор *С. Л. Шапиро*

ЛР № 065466 от 21.10.97

Гигиенический сертификат 78.01.07.953.П.001665.03.02
от 18.03.2002 г., выдан ЦГСЭН в СПб

Издательство «ЛАНЬ»
lan@lpbl.spb.ru; www.lanpbl.spb.ru
192029, Санкт-Петербург, Общественный пер., 5.

Издательство: тел./факс: (812)567-29-35, 567-05-97, 567-92-72;
pbl@lpbl.spb.ru; print@lpbl.spb.ru

Книги издательства «Лань»
можно приобрести в оптовых книготорговых организациях:

ООО «ЛАНЬ-ТРЕЙД». 192029, Санкт-Петербург, ул. Крупской, 13,
тел./факс: (812)567-54-93, тел.: (812)567-85-78, (812)567-14-45,
567-85-82, 567-85-91; trade@lanpbl.spb.ru; www.lanpbl.spb.ru/price.htm

ООО «ЛАНЬ-ПРЕСС». 109263, Москва, 7-я ул. Текстильщиков, 6/19,
тел.: (095)178-65-85, 178-57-04; lanpress@ultimanet.ru

ООО «ЛАНЬ-ЮГ». 350072, Краснодар, ул. Жлобы, 1/1, тел.: (861)274-10-35;
lankrd98@mail.ru

Подписано в печать 20.10.05.
Бумага офсетная. Формат 84 x 108$^1/_{32}$.
Печать офсетная. Усл. п. л. 9,24. Тираж 2000 экз.

Заказ № 3086

Отпечатано с готовых диапозитивов
в ОАО «ПИК «Офсет»
660075, г. Красноярск, ул. Республики, д. 51

Обложка
С. ШАПИРО, А. ЛАПШИН

ОГЛАВЛЕНИЕ

ИЗ ПРЕДИСЛОВИЯ К ДЕВЯТОМУ ИЗДАНИЮ

Девятое издание является значительной переработкой предыдущего восьмого издания. В нем существенно перестроены и дополнены главы первая и вторая. Кроме того, из числа вопросов к главе шестой убраны некоторые, касающиеся характеров, взамен этого под названием «Характеры» добавлена новая, седьмая глава с вопросами и численные примеры к ней.

И. М. Виноградов

Глава I

ТЕОРИЯ ДЕЛИМОСТИ

§ 1. Основные понятия и теоремы

а. Теория чисел занимается изучением свойств целых чисел. Целыми мы будем называть не только числа натурального ряда 1, 2, 3, ... (положительные целые), но также нуль и отрицательные целые —1, —2, —3, ... Так что, расположив целые числа в возрастающем порядке, получим ряд, в котором разность между большим и меньшим соседними членами везде будет равна единице.

Как правило, при изложении теоретического материала мы будем обозначать буквами только целые числа. Случаи, когда буквы могут обозначать и не целые числа, если последнее не будет ясно само по себе, мы будем особо оговаривать.

Сумма $a+b$, разность $a-b$ и произведение ab двух целых a и b являются также целыми. Но частное $\frac{a}{b}$ от деления a на b (если b не равно нулю) может быть как целым, так и не целым.

b. В случае, когда частное $\frac{a}{b}$ от деления a на b — целое, обозначая его буквою q, имеем $a=bq$, т. е. *a представляется произведением b на целое.* Мы говорим тогда, что *a делится на b* или, что *b делит a.* При этом a называем *кратным* числа b, а b — *делителем* числа a. То обстоятельство, что b является делителем числа a, записывается так: $b \backslash a$.

Примеры. Имеем

$$21=7\cdot 3, \quad 0=9\cdot 0, \quad -85=17\,(-5).$$

Поэтому можем сказать 21 делится на 7, 0 делится на 9, —85 делится на 17, или: 7 делит 21, 9 делит 0, 17 делит —85.

Имеют место две следующие теоремы:

1. *Если a кратно m, m кратно b, то a кратно b*

Действительно, из $a=ma_1$, $m=bm_1$, следует $a=ba_1m_1$. Таким образом, a представляется произведением b на целое число a_1m_1 и тем самым делится на b.

2. *Если в равенстве вида $k+l+\ldots+n=p+q+\ldots+s$ относительно всех членов, кроме какого-либо одного, известно, что они кратны b, то и этот один член кратен b.*

Действительно, пусть таким одним членом будет k. Имеем

$$l=bl_1,\ \ldots,\ n=bn_1,\ p=bp_1,\ q=bq_1,\ \ldots,\ s=bs_1,$$

$$k=p+q+\ldots+s-l-\ldots-n=$$

$$=b(p_1+q_1+\ldots+s_1-l_1-\ldots-n_1).$$

Таким образом, k представляется произведением b на целое число $p_1+q_1+\ldots+s_1-l_1-\ldots-n_1$ и тем самым делится на b.

c. В заключение мы докажем еще одну теорему, которая нам будет весьма нужна в дальнейшем (теорема о делении с остатком).

Всякое целое a представляется единственным способом с помощью положительного целого b равенством вида

$$a=bq+r;\quad 0\leqslant r<b.$$

Действительно, одно представление числа a равенством такого вида получим, взяв bq равным наибольшему кратному числа b, не превосходящему a. Допустив же существование представления числа a еще одним равенством того же вида: $a=bq_1+r_1$; $0\leqslant r_1<b$, и вычитая почленно это последнее равенство из предыдущего, получим

$$0=b(q-q_1)+r-r_1. \qquad (1)$$

Отсюда убедимся (2, b), что разность $r-r_1$ кратна b. С другой стороны, легко видеть, что та же разность, как разность двух неотрицательных чисел, меньших b, сама будет численно меньше b, числом же, кратным b и численно меньшим b, является лишь число 0. Поэтому $r-r_1=0$, а отсюда и из равенства (1) будет следовать, что и $q-q_1=0$. Таким образом, второе представление числа a тождественно первому.

Число q называется *неполным частным*, а число r — *остатком* от деления a на b. Очевидно, что при $r=0$ понятия «неполное частное» и «частное» совпадают.

Примеры. Пусть $b=14$. Имеем

$$177=14\cdot 12+9, \qquad 0<9<14,$$
$$-64=14\cdot(-5)+6, \qquad 0<6<14,$$
$$154=14\cdot 11+0, \qquad 0=0<14.$$

§ 2. Общий наибольший делитель

a. В дальнейшем мы будем рассматривать лишь положительные делители чисел. Всякое целое, делящее одновременно целые $a, b, \ldots, l$, называется их *общим делителем*. Наибольший из общих делителей называется общим наибольшим делителем и обозначается символом $(a, b, \ldots, l)$. Если $(a, b, \ldots, l)=1$, то $a, b, \ldots, l$ называются *взаимно простыми*. Если каждое из чисел $a, b, \ldots, l$ взаимно просто с каждым другим из них, то $a, b, \ldots, l$ называются *попарно простыми*. Очевидно, числа попарно простые всегда и взаимно простые. В случае же двух чисел понятия «попарно простые» и «взаимно простые» совпадают.

Примеры. Числа 6, 10, 15, ввиду $(6, 10, 15)=1$,— взаимно простые. Числа 8, 13, 21, ввиду $(8, 13)=(8, 21)=(13, 21)=1$,— попарно простые.

b. Далее займемся общими делителями двух чисел.

1. *Если a кратно b, то совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b; в частности $(a, b)=b$.*

Действительно, всякий общий делитель чисел a и b является делителем и одного b. Обратно, раз a кратно b, то (1, b, § 1) всякий делитель числа b является также делителем числа a, т. е. является общим делителем чисел b и a. Таким образом, совокупность общих делителей чисел a и b совпадает с совокупностью делителей одного b. А так как наибольший делитель числа b есть само b, то $(a, b)=b$.

2. *Если*

$$a=bq+c,$$

то совокупность общих делителей чисел a и b совпадает с совокупностью общих делителей чисел b и c; в частности $(a, b)=(b, c)$.

Действительно, написанное равенство показывает, что всякий общий делитель чисел a и b делит также и c (2, b, § 1) и, следовательно, является общим делителем чисел b и c. Обратно, то же равенство показывает, что всякий общий делитель чисел b и c делит a и, следовательно, является общим делителем чисел a и b. Таким образом, общие делители чисел a и b суть те же, что и общие делители чисел b и c; в частности, должны совпадать и наибольшие из этих делителей, т. е. $(a, b) = (b, c)$.

c. Для разыскания общего наибольшего делителя, а также для вывода его важнейших свойств применяется *алгоритм Евклида*. Он состоит в нижеследующем. Пусть a и b — положительные целые и $a > b$. Согласно с, § 1 находим ряд равенств

$$\begin{array}{ll} a = bq_1 + r_2, & 0 < r_2 < b, \\ b = r_2 q_2 + r_3, & 0 < r_3 < r_2, \\ r_2 = r_3 q_3 + r_4, & 0 < r_4 < r_3, \\ \dots\dots\dots & \dots\dots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_n q_n, & \end{array} \qquad (1)$$

заканчивающийся, когда получается некоторое $r_{n+1} = 0$. Последнее неизбежно, так как ряд $b, r_2, r_3, \dots$ как ряд убывающих целых не может содержать более чем b положительных.

d. Рассматривая равенства (1), идя сверху вниз, убеждаемся (b), что общие делители чисел a и b одинаковы с общими делителями чисел b и r_2, далее одинаковы с общими делителями чисел r_2 и r_3, чисел r_3 и r_4, ..., чисел r_{n-1} и r_n, наконец (a), с делителями одного числа r_n, являющегося последним не равным нулю остатком алгоритма Евклида. Одновременно с этим имеем

$$(a, b) = (b, r_2) = (r_2, r_3) = \dots = (r_{n-1}, r_n) = r_n.$$

Мы приходим к следующим результатам.

1. *Совокупность общих делителей чисел a и b совпадает с совокупностью делителей их общего наибольшего делителя*

2. *Этот общий наибольший делитель равен последнему не равному нулю остатку алгоритма Евклида.*

Пример. Применим алгоритм Евклида к отысканию (525, 231). Находим (вспомогательные вычисления приведены слева)

$$\begin{array}{r|l} 525 & 231 \\ \hline 462 & 2 \\ \hline 63 & \\ \hline \end{array} \qquad \begin{array}{r|l} 231 & 63 \\ \hline 189 & 3 \\ \hline 42 & \\ \hline \end{array} \qquad \begin{array}{r|l} 63 & 42 \\ \hline 42 & 1 \\ \hline 21 & \\ \hline \end{array} \qquad \begin{array}{r|l} 42 & 21 \\ \hline 42 & 2 \\ \hline 0 & \\ \hline \end{array}$$

$$525 = 231 \cdot 2 + 63,$$
$$231 = 63 \cdot 3 + 42,$$
$$63 = 42 \cdot 1 + 21,$$
$$42 = 21 \cdot 2.$$

Здесь последний положительный остаток есть $r_4 = 21$. Значит, $(525, 231) = 21$.

е. 1. *Обозначая буквою m любое положительное целое, имеем* $(am, bm) = (a, b)\, m$.

2. *Обозначая буквою δ любой общий делитель чисел a и b, имеем* $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$; *в частности, имеем* $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$, *т. е. частные от деления двух чисел на их общий наибольший делитель суть числа взаимно простые.*

Действительно, умножив соотношения (1) почленно на m, получим новые соотношения, где вместо a, b, r_2, ..., r_n будут стоять am, bm, r_2m, ..., r_nm. Поэтому $(am, bm) = r_nm$ н, таким образом, верно утверждение 1.

Применяя утверждение 1, находим

$$(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta.$$

Отсюда следует утверждение 2.

f. 1. *Если* $(a, b) = 1$, *то* $(ac, b) = (c, b)$.

Действительно, (ac, b) делит ac и bc, значит, $(1, d)$ оно делит и (ac, bc) ввиду 1, е равное c. Но $(ac; b)$ делит и b, поэтому оно делит и (c, b). Обратно, (c, b) делит ac и b, поэтому оно делит и (ac, b). Таким образом, (ac, b) и (c, b) взаимно делят друг друга и, следовательно, равны между собою.

2. *Если* $(a, b)=1$ *и* ac *делится на* b, *то* c *делится на* b.

Действительно (**1**, **b**), при ac, делящемся на b, имеем $(ac, b)=b$ и из **1** получаем $b=(c, b)$. А этим (**1**, **b**) и доказывается делимость c на b.

3. *Если каждое* $a_1, a_2, \ldots, a_m$ *взаимно просто с каждым* $b_1, b_2, \ldots, b_n$, *то и произведение* $a_1a_2\ldots a_m$ *взаимно просто с произведением* $b_1b_2\ldots b_n$.

Действительно, согласно **1** находим

$$(a_1a_2a_3\ldots a_m, b_k)=(a_1a_2\ldots a_m, b_k)=$$
$$=(a_2\ldots a_m, b_k)=\ldots=(a_m, b_k)=1,$$

и далее, полагая ради краткости $a_1a_2a_3\ldots a_m=A$, точно таким же путем выводим

$$(b_1b_2b_3\ldots b_n, A)=(b_2b_3\ldots b_n, A)=$$
$$=(b_3\ldots b_n, A)=\ldots=(b_n, A)=1.$$

§ 3. Общее наименьшее кратное

a. Всякое целое, кратное всех данных чисел, называется их *общим кратным*. Наименьшее положительное общее кратное называется *общим наименьшим кратным*. Здесь мы будем рассматривать только общие кратные двух положительных чисел.

b. Пусть $(a, b)=d$, $a=da_1$, $b=db_1$ и, следовательно (**2**, **e**, § 2), $(a_1, b_1)=1$. Пусть M — какое-либо общее кратное чисел a и b. Так как M кратно a, то $M=ak$, где k — целое. Но M кратно и b. Поэтому

$$\frac{M}{b}=\frac{ak}{b}=\frac{a_1k}{b_1}$$

должно быть целым и, следовательно (**2**, **f**, § 2), k должно делиться на b_1. Поэтому $k=b_1t$, где t — целое, причем для M получается формула

$$M=\frac{ab}{d}t. \qquad (1)$$

Обратно, очевидно, что M, представляемое формулой (1) при любом целом t, будет общим кратным a и b, и, таким образом, формула (1) дает общий вид всех общих кратных чисел a и b.

Наименьшее положительное из этих общих кратных, т. е. общее наименьшее кратное, получаем при $t=1$. Оно будет

$$m=\frac{ab}{d}. \tag{2}$$

Теперь формулу (1) можно переписать так:

$$M=mt. \tag{3}$$

Формулы (3) и (2) приводят к теоремам.

1. *Совокупность общих кратных двух чисел совпадает с совокупностью кратных их общего наименьшего кратного.*

2. *Это общее наименьшее кратное двух чисел равно их произведению, деленному на их общий наибольший делитель.*

§ 4. Простые числа .

a. Число 1 имеет только один положительный делитель, именно 1. В этом отношении число 1 в ряде натуральных чисел стоит совершенно особо.

Всякое целое, большее 1, имеет не менее двух делителей, именно 1 и самого себя; если этими делителями исчерпываются все положительные делители целого числа, то оно называется *простым*. Целое, большее 1, имеющее кроме 1 и самого себя другие положительные делители, называется составным.

b. *Наименьший отличный от единицы делитель целого, большего единицы, есть число простое.*

Действительно, пусть q — наименьший отличный от 1 делитель целого a, большего 1. Если бы q было бы составным, то оно имело бы некоторый делитель q_1 с условием $1<q_1<q$, причем число a, делясь на q, должно (1, b, § 1) делиться на q_1. А это противоречило бы нашему предположению относительно числа q.

c. *Наименьший отличный от единицы делитель составного числа a (согласно* b *он будет простым) не превосходит* $\sqrt{a}$.

Действительно, пусть q — этот делитель, тогда $a=qa_1$, $a_1\geqslant q$, откуда, перемножая и сокращая на a_1, получим $a\geqslant q^2$, $q\leqslant\sqrt{a}$.

d. *Простых чисел бесконечно много.*

Справедливость этой теоремы следует из того, что каковы бы ни были различные простые $p_1, p_2, \ldots, p_k$, можно получить новое простое, среди них не находящееся. Таковым будет простой делитель суммы $p_1p_2\ldots p_k+1$, который деля всю сумму, не может совпадать ни с одним из простых $p_1, p_2, \ldots, p_k$ (2, b, § 1).

е. Для составления таблицы простых чисел, не превосходящих данного целого N, существует простой способ, называемый *решетом Эратосфена*. Он состоит в следующем.

Выписываем числа

$$1, 2, \ldots, N. \qquad (1)$$

Первое большее 1 число этого ряда есть 2. Оно делится только на 1 и на самого себя и, следовательно, оно простое.

Вычеркиваем из ряда (1) (как составные) все числа, кратные 2, кроме самого 2. Первое следующее за 2 невычеркнутое число есть 3. Оно не делится на 2 (иначе оно оказалось бы вычеркнутым). Следовательно, 3 делится только на 1 и на самого себя, а потому оно также будет простым.

Вычеркиваем из ряда (1) все числа, кратные 3, кроме самого 3. Первое следующее за 3 невычеркнутое число есть 5. Оно не делится ни на 2, ни на 3 (иначе оно оказалось бы вычеркнутым). Следовательно, 5 делится только на 1 и на самого себя, а потому оно также будет простым.

И т. д.

Когда указанным способом уже вычеркнуты все числа, кратные простых, меньших простого p, то все невычеркнутые, меньшие p^2, будут простые. Действительно, всякое составное a, меньшее p^2, нами уже вычеркнуто, как кратное его наименьшего простого делителя, который $\leqslant \sqrt{a} < p$. Отсюда следует:

1. *Приступая к вычеркиванию кратных простого p, это вычеркивание следует начинать с p^2.*

2. *Составление таблицы простых чисел, не превосходящих N, закончено, как только вычеркнуты все составные кратные простых, не превосходящих $\sqrt{N}$.*

§ 5. Единственность разложения на простые сомножители

a. *Всякое целое a или взаимно просто с данным простым p, или же делится на p.*

Действительно, (a, p), будучи делителем p, может быть равно или 1, или p. В первом случае a взаимно просто с p, во втором a делится на p.

b. *Если произведение нескольких сомножителей делится на данное простое p, то, по крайней мере, один из сомножителей делится на p.*

Действительно (a), каждый сомножитель или взаимно прост с p, или же делится на p. Если бы все сомножители были взаимно просты с p, то и их произведение (3, f, § 2) было бы взаимно просто с p. Поэтому хоть один сомножитель делится на p.

c. *Всякое целое, большее единицы, разлагается на произведение простых сомножителей и притом единственным способом (если отвлечься от порядка следования сомножителей).*

Действительно, пусть a—целое, большее 1; обозначая буквою p_1 его наименьший простой делитель, имеем $a = p_1 a_1$. Если $a_1 > 1$, то, обозначая буквою p_2 его наименьший простой делитель, имеем $a_1 = p_2 a_2$. Если $a_2 > 1$, то подобно этому находим $a_2 = p_3 a_3$ и т. д., пока не придем к какому-либо a_n, равному 1. Тогда получим $a_{n-1} = p_n$. Перемножив все найденные равенства и произведя сокращение, получим следующее разложение a на простые сомножители:

$$a = p_1 p_2 p_3 \cdots p_n.$$

Допустим, что для того же самого a существует и второе разложение на простые сомножители $a = q_1 q_2 q_3 \cdots q_s$. Тогда найдем

$$p_1 p_2 p_3 \cdots p_n = q_1 q_2 q_3 \cdots q_s.$$

Правая часть этого равенства делится на q_1. Следовательно (b), по крайней мере один из сомножителей левой части должен делиться на q_1. Пусть, например, p_1 делится на q_1 (порядок следования сомножителей в нашем распоряжении); тогда найдем $p_1 = q_1$ (p_1 кроме 1 делится только на p_1). Сократив обе части равенства на $p_1 = q_1$, получим $p_2 p_3 \cdots p_n = q_2 q_3 \cdots q_s$. Повторив прежние

рассуждения применительно к этому равенству, получим $p_3 \dots p_n = q_3 \dots q_s$ и т. д., пока, наконец, в одной части равенства, например, в левой не сократятся все сомножители. Но одновременно должны сократиться и все сомножители правой части, так как равенство $1 = q_{n+1} \dots q_s$ при $q_{n+1}, \dots, q_s$, превосходящих 1, невозможно. Таким образом, второе разложение на простые сомножители тождественно первому.

d. В разложении числа a на простые сомножители некоторые из них могут повторяться. Обозначая буквами $p_1, p_2, \dots, p_k$ различные из них и буквами $\alpha_1, \alpha_2, \dots, \alpha_k$ кратности их вхождения в a, получим так называемое *каноническое разложение* числа a на сомножители

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

Пример. Каноническое разложение числа 588 000 будет: $588\,000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$.

e. В заключение мы докажем несколько теорем, касающихся делителей числа, а также общего наибольшего делителя и общего наименьшего кратного нескольких чисел.

1. *Пусть $a = p_1^{\alpha_1} p_1^{\alpha_2} \dots p_k^{\alpha_k}$—каноническое разложение числа a. Тогда все делители числа суть все числа вида*

$$d = p_1^{\beta_1} p_1^{\beta_2} \dots p_k^{\beta_k}; \qquad (1)$$

$$0 \leqslant \beta_1 \leqslant \alpha_1, \ 0 \leqslant \beta_2 \leqslant \alpha_2, \ \dots, \ 0 \leqslant \beta_k \leqslant \alpha_k.$$

Действительно, пусть d делит a. Тогда (b, § 1) $a = dq$ и, следовательно, все простые делители числа d входят в каноническое разложение числа a с показателями, не меньшими тех, с которыми они входят в каноническое разложение числа d. Поэтому d имеет вид (1).

Обратно, всякое d вида (1) делит a.

Пример. Все делители числа $720 = 2^4 \cdot 3^2 \cdot 5$ получим, если в выражении $2^{\beta_1} 3^{\beta_2} 5^{\beta_3}$ заставим $\beta_1, \beta_2, \beta_3$ независимо друг от друга пробегать значения $\beta_1 = 0, 1, 3, 4$; $\beta_2 = 0, 1, 2$; $\beta_3 = 0, 1$. Поэтому указанные делители будут: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720.

2. *Общий наибольший делитель нескольких чисел является произведением степеней вида p^α, где p—общий простой делитель всех этих чисел, а α—наименьший из*

показателей, с которыми p входит в их канонические разложения.

3. *Совокупность общих делителей нескольких чисел совпадает с совокупностью делителей их общего наибольшего делителя.*

Действительно, пусть d — общий делитель чисел $a, \ldots, l$. Тогда имеют место равенства вида $a = da_1, \ldots, l = dl_1$, которые показывают, что: a) всякий простой делитель p числа d должен быть делителем и каждого из чисел $a, \ldots, l$, а также что: b) этот делитель p должен входить в каноническое разложение числа d с показателем, не превосходящим наименьшего из тех, с которыми он входит в канонические разложения чисел $a, \ldots, l$; обратно, каждое d, подчиненное условиям a) и b), очевидно, является общим делителем чисел $a, \ldots, l$.

Общим наибольшим делителем, т. е. наибольшим из общих делителей (a, § 2) является тот из последних, в каноническом разложении которого показатели степеней простых чисел точно равны наименьшим из тех, с какими эти простые числа входят в канонические разложения чисел $a, \ldots, l$.

А всякий общий делитель, как имеющий в своем каноническом разложении все показатели не превосходящими соответствующих показателей в каноническом разложении общего наибольшего делителя, будет делителем последнего.

Пример. Общий наибольший делитель чисел $6\,791\,400 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11$, $178\,500 = 2^2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 17$, $27\,720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$ равен $2^2 \cdot 3 \cdot 5 \cdot 7 = 420$.

4. *Общее наименьшее кратное нескольких чисел является произведением степеней вида p^{α}, где p — простой делитель по меньшей мере одного из этих чисел, а α — наибольший из показателей, с которыми p входит в их канонические разложения.*

5. *Общее наименьшее кратное нескольких попарно простых чисел равно их произведению.*

6. *Совокупность общих кратных нескольких чисел совпадает с совокупностью кратных их общего наименьшего кратного.*

Действительно, пусть M — общее кратное чисел $a, \ldots, l$. Тогда имеют место равенства вида $M = ad', \ldots, M = ll'$, которые показывают, что: a) всякий простой делитель p

каждого из чисел $a, \ldots, l$ должен быть делителем и числа M, а также что: b) этот делитель p должен входить в каноническое разложение числа M с показателем, не меньшим наибольшего из тех, с которыми он входит в канонические разложения чисел $a, \ldots, l$; обратно, каждое M, подчиненное условиям a) и b), очевидно, является общим кратным чисел $a, \ldots, l$.

Общим наименьшим кратным, т. е. наименьшим из общих кратных (a, § 3), является то из последних, в каноническом разложении которого показатели степеней простых чисел точно равны наибольшим из тех, с какими эти простые числа входят в канонические разложения чисел $a, \ldots, l$.

В случае, когда $a, \ldots, l$ — попарно простые и, следовательно, каждый множитель вида p^{α} канонического разложения общего наименьшего кратного входит в каноническое разложение одного и только одного из чисел $a, \ldots, l$, общее наименьшее кратное последних, очевидно, равно их произведению.

Всякое общее кратное, как имеющее в своем каноническом разложении все показатели не меньшими соответствующих показателей в каноническом разложении общего наименьшего кратного, будет кратным последнего.

Пример. Общее наименьшее кратное чисел $1800 = 2^3 \cdot 3^2 \cdot 5^2$, $3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7$, $8910 = 2 \cdot 3^4 \cdot 5 \cdot 11$ равно $2^3 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 = 1\,247\,400$.

§ 6. Непрерывные дроби и их связь с алгоритмом Евклида

a. Пусть α — любое вещественное число. Обозначим буквою q_1 наибольшее целое число, не превосходящее α. При нецелом α имеем $\alpha = q_1 + \frac{1}{\alpha_2}$; $\alpha_2 > 1$. Точно так же при нецелых $\alpha_2, \ldots, \alpha_{s-1}$ имеем

$$\alpha_2 = q_2 + \frac{1}{\alpha_3}; \qquad \alpha_3 > 1,$$

$$\ldots\ldots\ldots\ldots$$

$$\alpha_{s-1} = q_{s-1} + \frac{1}{\alpha_s}; \quad \alpha_s > 1,$$

ввиду чего получаем следующее *разложение α в непре-*

рывную дробь:

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{s-1} + \cfrac{1}{\alpha_s}}}} \qquad (1)$$

b. Если α — иррациональное, то и всякое α_1 — иррациональное (при рациональном α_s ввиду (1) рациональным оказалось бы и α) и указанный процесс может быть неограниченно продолжен.

Если же α — рациональное и, следовательно, может быть представлено рациональной несократимой дробью $\alpha = \frac{a}{b}$ с положительным знаменателем, то указанный процесс будет конечен и может быть выполнен с помощью алгоритма Евклида. Действительно, имеем:

$$a = bq_1 + r_2; \qquad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$b = r_2 q_2 + r_3; \qquad \frac{b}{r_2} = q_2 + \frac{1}{\frac{r_2}{r_3}}$$

. . . . . .

$$r_{n-2} = r_{n-1} q_{n-1} + r_n; \qquad \frac{r_{n-2}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_n q_n; \qquad \frac{r_{n-1}}{r_n} = q_n,$$

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}.$$

Числа $q_1, q_2, \ldots$, участвующие в разложении числа α в непрерывную дробь, называются *неполными частными* (в случае рационального α это будут, согласно b, неполные частные последовательных делений алгоритма Евклида), дроби же

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}, \quad \ldots$$

называются *подходящими дробями*.

c. Весьма простой *закон вычисления подходящих дробей* получим, заметив, что $\delta_s\,(s > 1)$ получается из δ_{s-1} заменой в буквенном выражении для δ_{s-1} числа q_{s-1} числом $q_{s-1} + \frac{1}{q_s}$. Действительно, полагая ради единообразия $P_0 = 1$, $Q_0 = 0$, мы можем последовательно представить подходящие дроби в следующем виде (здесь равенство $\frac{A}{B} = \frac{P_s}{Q_s}$ пишем, желая обозначить A символом P_s, а B — символом Q_s):

$$\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1},$$

$$\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2 q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_2 P_1 + P_0}{q_2 Q_1 + Q_0} = \frac{P_2}{Q_2},$$

$$\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right) P_1 + P_0}{\left(q_2 + \frac{1}{q_3}\right) Q_1 + Q_0} = \frac{q_3 P_2 + P_1}{q_3 Q_2 + Q_1} = \frac{P_3}{Q_3}$$

и т. д. и вообще при $s > 1$

$$\delta_s = \frac{q_s P_{s-1} + P_{s-2}}{q_s Q_{s-1} + Q_{s-2}} = \frac{P_s}{Q_s}. \tag{2}$$

Таким образом, числители и знаменатели подходящих дробей мы можем последовательно вычислять по формулам

$$\begin{aligned} P_s &= q_s P_{s-1} + P_{s-2}, \\ Q_s &= q_s Q_{s-1} + Q_{s-2}. \end{aligned} \tag{3}$$

Эти вычисления удобно делать по следующей схеме (два

последних столбца пишем лишь в случае, когда α — несократимая дробь с положительным знаменателем: $\alpha=\frac{a}{b}$):

q_s		q_1	q_2	...				...	q_{n-1}	q_n
P_s	1	q_1	P_2	...	P_{s-2}	P_{s-1}	P_s	...	P_{n-1}	a
Q_s	0	1	Q_2	...	Q_{s-2}	Q_{s-1}	Q_s	...	Q_{n-1}	b

Пример. Разложим в непрерывную дробь несократимую дробь $\frac{105}{38}$. Здесь имеем

$$105 = 2\cdot 38 + 29,\quad 38 = 1\cdot 29 + 9,\quad 29 = 3\cdot 9 + 2,\quad 9 = 4\cdot 2 + 1,\quad 2 = 2\cdot 1 + 0;$$

$$\frac{105}{38} = 2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{2}}}}.$$

Поэтому указанная выше схема дает:

q_s		2	1	3	4	2
P_s	1	2	3	11	47	105
Q_s	0	1	1	4	17	38

d.1. *При* $s>0$ *имеем* $P_sQ_{s-1}-Q_sP_{s-1}=(-1)^s$.

2. *При* $s>1$ *имеем* $\delta_s-\delta_{s-1}=\frac{(-1)^s}{Q_sQ_{s-1}}$.

Действительно, приняв обозначение $h_s = P_sQ_{s-1} - Q_sP_{s-1}$, мы при $s=1$ получим $h_1 = q_1 \cdot 0 - 1 \cdot 1 = -1$, а при $s > 1$ с помощью равенств (3) найдем $h_s = -h_{s-1}$. Отсюда получим $h_s = (-1)^s$. Пользуясь же этим равенством при $s > 1$, легко найдем

$$\delta_s - \delta_{s-1} = \frac{P_s}{Q_s} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_s}{Q_sQ_{s-1}} = \frac{(-1)^s}{Q_sQ_{s-1}}.$$

e. *Пусть* $1 < s$, *а если* α *— рациональная несократимая дробь* $\alpha = \frac{a}{b}$ *с положительным знаменателем, то пусть также* $s < n$. *Тогда* α *лежит между* δ_{s-1} *и* δ_s, *причем ближе к* δ_s, *нежели к* δ_{s-1}.

Действительно, заменив в равенстве (2) число q_s числом $q_s + \frac{1}{\alpha_{s+1}}$, получим

$$\alpha = \frac{\alpha_{s+1}P_s + P_{s-1}}{\alpha_{s+1}Q_s + Q_{s-1}},$$

$$\alpha\alpha_{s+1}Q_s + \alpha Q_{s-1} - \alpha_{s+1}P_s - P_{s-1} = 0,$$

$$\alpha_{s+1}Q_s\left(\alpha - \frac{P_s}{Q_s}\right) + Q_{s-1}\left(\alpha - \frac{P_{s-1}}{Q_{s-1}}\right) = 0,$$

откуда убеждаемся, что первая из разностей, стоящих в скобках, и по знаку противоположна второй и численно (ввиду $Q_s > Q_{s-1}$) меньше последней. А этим и доказываются наши утверждения.

Вопросы к главе I

1. Пусть a и b — целые, не равные одновременно нулю, и $d = ax_0 + by_0$ — наименьшее положительное число вида $ax + by$ (x и y — целые). Доказать, что $d = (a, b)$. Отсюда вывести теорему **1, d,** § 2 и теоремы **e,** § 2. Обобщить эти выводы, рассматривая числа вида $ax + by + \ldots + fu$.

2. Пусть p — простое число, a и b — натуральные числа, p делит ab. Методом математической индукции (индукцию вести по p) доказать, что p делит либо a, либо b. Отсюда вывести **b), c)** § 5.

3, a. Пусть (**c,** § 6) $1 < s$, а если $\alpha = \frac{a}{b}$ — несократимая дробь, то пусть также $s < n$ ($q_n = b$). Доказать, что α может приближаться несократимой дробью $\frac{c}{d}$ более точно, чем дробью δ_s, лишь в случае $d > Q_s$.

b. Пусть вещественное число α разложено в непрерывную дробь, N — целое положительное, k — число его десятичных знаков, n — наибольшее целое с условием $Q_n \leqslant N$. Доказать, что $n \leqslant 5k+1$. Для доказательства выражения для $Q_2, Q_3, Q_4, \ldots, Q_n$ следует сравнить с теми, которые они имели бы, если бы все q_s были равны 1, и сравнить далее с числами $1, \xi, \xi^2, \ldots, \xi^{n-1}$, где ξ — положительный корень уравнения $\xi^2 = \xi + 1$.

4. Пусть $\tau \geqslant 1$. Ряд расположенных в порядке возрастания рациональных несократимых дробей с положительными знаменателями, не превосходящими τ, называется *рядом Фарея, отвечающим* τ.

a. Доказать, что часть ряда Фарея, отвечающего τ, содержащая дроби α с условием $0 \leqslant \alpha \leqslant 1$, может быть получена следующим способом: пишем дроби $\frac{0}{1}, \frac{1}{1}$. Если $2 \leqslant \tau$, то между этими дробями вставим еще дробь $\frac{0+1}{1+1} = \frac{1}{2}$, затем в полученном ряде $\frac{0}{1}, \frac{1}{2}, \frac{1}{1}$ между каждыми двумя соседними дробями $\frac{a_1}{b_1}$ и $\frac{c_1}{d_1}$ с $b_1 + d_1 \leqslant \tau$ вставим дробь $\frac{a_1+c_1}{b_1+d_1}$ и т. д. до тех пор, пока это возможно. Предварительно доказать, что для любой пары соседних дробей $\frac{a}{b}$ и $\frac{c}{d}$ ряда, получаемого указанным способом, имеем $ad - bc = -1$.

b. Рассматривая ряд Фарея, доказать теорему: пусть $\tau \geqslant 1$, тогда всякое вещественное α можно представить в виде

$$\alpha = \frac{P}{Q} + \frac{\theta}{Q\tau}; \quad 0 < Q \leqslant \tau, \quad (P, Q) = 1, \quad |\theta| < 1.$$

c. Теорему вопроса b доказать, пользуясь 2, d, § 6.

5, a. Доказать бесконечность числа простых чисел вида $4m+3$.

b. Доказать бесконечность числа простых чисел вида $6m+5$.

6. Доказать бесконечность числа простых чисел, подсчитывая число чисел, не превосходящих N, в каноническое разложение которых не входят простые числа, отличные от $p_1, p_2, \ldots, p_k$.

7. Пусть K — целое положительное. Доказать, что в ряде натуральных чисел имеется бесчисленное множество последовательностей $M, M+1, \ldots, M+K-1$, не содержащих простых чисел.

8. Доказать, что среди чисел, представляемых многочленом $a_0x^n + a_1x^{n-1} + \ldots + a_n$, где $n > 0$, $a_0, a_1, \ldots, a_n$ — целые и $a_0 > 0$, имеется бесчисленное множество составных.

9, a. Доказать, что неопределенному уравнению

$$x^2 + y^2 = z^2, \quad x > 0, \; y > 0, \quad z > 0, \quad (x, y, z) = 1 \qquad (1)$$

удовлетворяют те и только те системы x, y, z, где одно из чисел x и y имеет вид $2uv$, другое — вид $u^2 - v^2$ наконец, z имеет вид $u^2 + v^2$, при этом $u > v > 0$, $(u, v) = 1$, uv — четное.

b. Пользуясь теоремой вопроса a, доказать неразрешимость в целых положительных x, y, z уравнения $x^4 + y^4 = z^2$.

10. Доказать теорему: если уравнение $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, где $n > 0$ и $a_1, \ldots, a_n$ — целые, имеет рациональный корень, то этот корень — целое число.

11, a. Пусть $S = \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$; $n > 1$. Доказать, что S — не целое.

b. Пусть $S = \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{2n+1}$; $n > 0$. Доказать, что S — не целое.

12. Пусть n — целое, $n > 0$. Доказать, что все коэффициенты разложения бинома Ньютона $(a+b)^n$ будут нечетными тогда и только тогда, когда n имеет вид $2^k - 1$.

Численные примеры к главе I

1, a. Применяя алгоритм Евклида, найти (6188, 4709).

b. Найти (81 719, 52 003, 33 649, 30 107).

2, a. Разложив в непрерывную дробь $\alpha = \frac{125}{92}$ и составив таблицу подходящих дробей (c, § 6), найти: α) δ_4, β) представление α в виде, указанном в вопросе **4, b**, считая $\tau = 20$.

b. Разложив в непрерывную дробь $\alpha - \frac{5391}{3976}$ и составив таблицу подходящих дробей, найти: α) δ_6, β) представление α в виде, указанном в вопросе **4, b**, считая $\tau = 1000$.

3. Составить ряд дробей Фарея (вопрос 4) от 0 до 1, исключая 1, со знаменателями, не превосходящими 8.

4. Составить таблицу простых чисел, меньших 100.

5, a. Найти каноническое разложение числа 82 798 848.

b. Найти каноническое разложение числа 81 057 226 635 000.

Глава II

ВАЖНЕЙШИЕ ФУНКЦИИ В ТЕОРИИ ЧИСЕЛ

§ 1. Функции $[x]$ и $\{x\}$

a. В первую очередь мы рассмотрим две следующие функции, определенные для всех вещественных значений x:

1. *Целую часть от* x, обозначаемую символом $[x]$, представляющую собою наибольшее целое число, не превосходящее x.

2. *Дробную часть от* x, обозначаемую символом $\{x\}$, представляющую собою разность $x-[x]$ между x и целой частью от x.

Примеры.

$$[7]=7, \quad [2{,}3]=2, \quad [-4{,}75]=-5,$$
$$\{7\}=0, \quad \{2{,}3\}=0{,}3, \quad \{-4{,}75\}=0{,}25.$$

b. *Показатель, с которым данное простое* p *входит в произведение* $n!$, *равен*

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots \qquad (1)$$

Действительно, число сомножителей произведения $n!$, кратных p, равно $\left[\frac{n}{p}\right]$, среди них число кратных p^2 равно $\left[\frac{n}{p^2}\right]$, среди последних число кратных p^3 равно $\left[\frac{n}{p^3}\right]$, и т. д. Сумма (1) и даст искомый показатель, так как каждый сомножитель произведения $n!$, кратный p^m, но не p^{m+1}, нами сосчитан точно m раз, как кратный p, p^2, p^3, ..., наконец, p^m.

Пример. Показатель, с которым число 3 входит в произведение 3671, равен

$$\left[\frac{367}{3}\right]+\left[\frac{367}{9}\right]+\left[\frac{367}{27}\right]+\left[\frac{367}{81}\right]+\left[\frac{367}{243}\right]=$$
$$=122+40+13+4+1=180.$$

§ 2. Мультипликативные функции

a. *Функция* $\theta(a)$ *называется мультипликативной, если она удовлетворяет двум следующим условиям:*

1. *Эта функция определена для всех целых положительных* a *и не равна нулю по меньшей мере при одном таком* a.

2. *Для любых положительных взаимно простых* a_1 *и* a_2 *имеем:*

$$\theta(a_1 a_2) = \theta(a_1)\,\theta(a_2).$$

Пример. Нетрудно видеть, что мультипликативной является функция a^s, где s — любое вещественное или комплексное число.

b. *Для всякой мультипликативной функции* $\theta(a)$ *имеем* $\theta(1) = 1$. Действительно, пусть $\theta(a_0)$ не равно нулю. Находим

$$\theta(a_0) = \theta(a_0 \cdot 1) = \theta(a_0)\,\theta(1), \qquad 1 = \theta(1).$$

c. Свойство 2, a мультипликативной функции $\theta(a)$ распространяется и на случай $k > 2$ попарно простых чисел $a_1, a_2, a_3, \ldots, a_k$. Действительно, имеем:

$$\theta(a_1 a_2 a_3 \ldots a_k) = \theta(a_1)\,\theta(a_2 a_3 \ldots a_k) =$$
$$= \theta(a_1)\,\theta(a_2)\,\theta(a_3 \ldots a_k) = \ldots = \theta(a_1)\,\theta(a_2)\,\theta(a_3)\ldots\theta(a_k).$$

В частности, находим

$$\theta(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_k^{\alpha_k}) = \theta(p_1^{\alpha_1})\,\theta(p_2^{\alpha_2})\,\theta(p_3^{\alpha_3})\ldots\theta(p_k^{\alpha_k}). \quad (1)$$

d. Обратно, *мы всегда построим некоторую мультипликативную функцию* $\theta(a)$, *если положив* $\theta(1) = 1$ *и назначив произвольно значения для* $\theta(p^\alpha)$, *отвечающих положительным степеням простых чисел, в общем случае определим эту функцию равенством* (1).

Действительно, если $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ представлено в виде произведения $a_1 a_2$ двух взаимно простых чисел a_1 и a_2, то справедливо тождество

$$\theta(a) = \theta(a_1)\,\theta(a_2),$$

левая часть которого является произведением чисел $\theta(p_s^{\alpha_s})$, отвечающих всем сомножителям вида $p_s^{\alpha_s}$ числа a, а правая часть является тем же произведением, но раз-

битым на два взаимно простых произведения, одно из которых $\theta(a_1)$ является произведением чисел $\theta(p_i^{\alpha_i s})$, отвечающих всем сомножителям вида $p_i^{\alpha_i s}$ числа a_1, другое же $\theta(a_2)$ является произведением чисел $\theta(p_i^{\alpha_i s})$, отвечающих всем сомножителям вида $p_i^{\alpha_i s}$ числа a_2.

Пример. Мультипликативную функцию можно построить, взяв $\theta(1)=1$ и $\theta(p^{\alpha})=2$, если $\alpha>0$. Тогда при $k>0$ будем иметь $\theta(p_1^{\alpha_1}\dots p_k^{\alpha_k})=2^k$. В частности, найдем:

$$\theta(1)=1,\quad \theta(2)=2,\quad \theta(3)=2,$$
$$\theta(4)=2,\quad \theta(5)=2,\quad \theta(6)=4.$$

e. *Произведение* $\theta(a)=\theta_1(a)\,\theta_2(a)$ *двух мультипликативных функций* $\theta_1(a)$ *и* $\theta_2(a)$ *также является мультипликативной функцией.*

Действительно, имеем $\theta(1)=\theta_1(1)\,\theta_2(1)=1$.

Кроме того, при $(a_1, a_2)=1$ находим

$$\theta(a_1a_2)=\theta_1(a_1a_2)\,\theta_2(a_1a_2)=\theta_1(a_1)\,\theta_1(a_2)\,\theta_2(a_1)\,\theta_2(a_2)=$$
$$=\theta_1(a_1)\,\theta_2(a_1)\,\theta_1(a_2)\,\theta_2(a_2)=\theta(a_1)\,\theta(a_2).$$

Доказанная теорема обобщается и на случай любого числа $k>2$ мультипликативных функций

$$\theta_1(a),\quad \theta_2(a),\quad \theta_3(a),\quad \dots,\quad \theta_k(a).$$

Действительно, пользуясь ею последовательно, убедимся в мультипликативности произведений:

$$\theta_1(a)\,\theta_2(a)\,\theta_3(a)=(\theta_1(a)\,\theta_2(a))\,\theta_3(a),$$
$$\theta_1(a)\,\theta_2(a)\,\theta_3(a)\,\theta_4(a)=(\theta_1(a)\,\theta_2(a)\,\theta_3(a))\,\theta_4(a),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\theta_1(a)\,\theta_2(a)\dots\theta_{k-1}(a)\,\theta_k(a)=(\theta_1(a)\,\theta_2(a)\dots\theta_{k-1}(a))\,\theta_k(a).$$

f. *Пусть* $\theta(a)$ *— мультипликативная функция и* $a=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ *— каноническое разложение числа* a. *Тогда, обозначая символом* $\sum_{d\mid a}$ *сумму, распространенную на все*

делители d числа a, будем иметь

$$\sum_{d \mid a} \theta(d) = (1+\theta(p_1)+\theta(p_1^2)+\ldots+\theta(p_1^{\alpha_1}))\ldots$$
$$\ldots\left(1+\theta(p_k)+\theta(p_k^2)+\ldots+\theta\left(p_k^{\alpha_k}\right)\right).$$

(*В случае $a=1$ правая часть считается равной* 1.)

Чтобы доказать это тождество, раскроем скобки в его правой части. Тогда получим сумму всех (без пропусков и повторений) слагаемых вида

$$\theta(p_1^{\beta_1})\theta(p_2^{\beta_2})\ldots\theta\left(p_k^{\beta_k}\right)=\theta\left(p_1^{\beta_1}p_2^{\beta_2}\ldots p_k^{\beta_k}\right);$$
$$0\leqslant\beta_1\leqslant\alpha_1,\ 0\leqslant\beta_2\leqslant\alpha_2,\ \ldots,\ 0\leqslant\beta_k\leqslant\alpha_k.$$

А это (**1**, **e**, $\S\,5$, гл. I) как раз и будет то, что стоит в левой части тождества.

§ 3. Число делителей и сумма делителей

a. 1. При $\theta(a)=1$ (пример **a**, § 2) тождество **f**, § 2 примет вид $\tau(a)=(\alpha_1+1)\ldots(\alpha_k+1)$, где $\tau(a)$ — число делителей числа a.

Пример. $\tau(720)=\tau(2^4\cdot3^2\cdot5)=(4+1)(2+1)(1+1)=30$.

2. $\tau(a)$ — *мультипликативная функция, для которой при* $\alpha>0$ *имеем* $\tau(p^\alpha)=\alpha+1$.

Это следует из найденной для $\tau(a)$ формулы и теоремы **d**, § 2.

b. 1. При $\theta(a)=a$ (пример **a**, § 2) тождество **d**, § 2 примет вид

$$S(a)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1},$$

где $S(a)$ — *сумма делителей числа* a.

Пример. $S(720)=S(2^4\cdot3^2\cdot5)=\frac{2^5-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1}=2418$.

2. $S(a)$ — *мультипликативная функция, для которой при* $\alpha>0$ *имеем* $S(p^\alpha)=\frac{p^{\alpha+1}-1}{p-1}$.

Это следует из найденной для $S(a)$ формулы и теоремы **d**, § 2.

§ 4. Функция Мёбиуса

а. *Функция Мёбиуса — мультипликативная функция, определенная равенствами:* $\mu(p) = -1$, $\mu(p^\alpha) = 0$, *если* $\alpha > 1$.

Из этого определения, в частности, следует, что:

α) Если в каноническом разложении $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ числа a по меньшей мере один из показателей $\alpha_1, \dots, \alpha_k$ превосходит 1 (если a делится на квадрат, отличный от 1), то имеем $\mu(a) = 0$.

β) В противном случае, т. е. в случае, если каноническое разложение числа a имеет вид $a = p_1 \dots p_k$, имеем $\mu(a) = (-1)^k$.

Примеры.

$$\mu(1) = 1, \quad \mu(5) = -1, \quad \mu(9) = 0,$$
$$\mu(2) = -1, \quad \mu(6) = 1, \quad \mu(10) = 1,$$
$$\mu(3) = -1, \quad \mu(7) = -1, \quad \mu(11) = -1,$$
$$\mu(4) = 0, \quad \mu(8) = 0, \quad \mu(12) = 0.$$

b. 1. *Пусть* $\theta(a)$ *— мультипликативная функция и* $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ *— каноническое разложение числа* a. *Тогда имеем:*

$$\sum_{a/b} \mu(d)\,\theta(d) = (1 - \theta(p_1)) \dots (1 - \theta(p_k))$$

(*в случае* $a = 1$ *правую часть считаем равной* 1).

Действительно, функция $\theta_1(a) = \mu(a)\,\theta(a)$, как произведение мультипликативных функций $\mu(a)$ и $\theta(a)$, сама является мультипликативной функцией. Применяя к ней тождество f, § 2 и имея в виду, что $\theta_1(p) = -\theta(p)$ и что $\theta_1(p^\alpha) = 0$, если $\alpha > 1$, мы и убедимся в справедливости нашего утверждения.

2. В частности, полагая $\theta(a) = 1$, из α) получим

$$\sum_{d \setminus a} \mu(d) = \begin{cases} 0, & \text{если } a > 1, \\ 1, & \text{если } a = 1. \end{cases}$$

3. Полагая же $\theta(a) = \frac{1}{a}$, получим

$$\sum_{d \setminus a} \frac{\mu(d)}{d} = \begin{cases} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right), & \text{если } a > 1, \\ 1, & \text{если } a = 1. \end{cases}$$

c. *Пусть целым положительным* $\delta = \delta_1, \ldots, \delta_n$ *отвечают любые вещественные, или комплексные* $f = f_1, \ldots, f_n$. *Тогда, обозначая символом* S' *сумму значений* f, *отвечающих значениям* δ, *равным* 1, *и символом* S_d *сумму значений* f, *отвечающих значениям* δ, *кратным* d, *будем иметь*

$$S' = \sum_d \mu(d) S_d,$$

где d *пробегает целые положительные числа, делящие хотя бы одно значение* δ.

Действительно **(2, b)**, имеем

$$S' = f_1 \sum_{d \setminus \delta_1} \mu(d) + \ldots + f_n \sum_{d \setminus \delta_n} \mu(d).$$

Собирая же вместе члены с одними и теми же значениями d и вынося при этом $\mu(d)$ за скобки, в скобках получим сумму тех и только тех значений f, которые отвечают значениям δ, кратным d, т. е. как раз и получим сумму S_d.

§ 5. Функция Эйлера

a. *Функция Эйлера* $\varphi(a)$ *определяется для всех целых положительных* a *и представляет собою число чисел ряда*

$$0, 1, \ldots, a-1, \tag{1}$$

взаимно простых с a.

Примеры.

$$\varphi(1) = 1, \quad \varphi(4) = 2,$$
$$\varphi(2) = 1, \quad \varphi(5) = 4,$$
$$\varphi(3) = 2, \quad \varphi(6) = 2.$$

b. 1. *Пусть*

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \tag{2}$$

— каноническое разложение числа a. *Тогда имеем*

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_k}\right), \tag{3}$$

или также

$$\varphi(a) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right)\ldots\left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right). \tag{4}$$

В частности, будем иметь

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}, \quad \varphi(p) = p-1. \tag{5}$$

Действительно, применим теорему c, § 4. При этом числа δ и числа f определим так: пусть x пробегает числа ряда (1); каждому значению x приведем в соответствие число $\delta = (x, a)$ и число $f = 1$.

Тогда S' обратится в число значений $\delta = (x, a)$, равных 1, т. е. в $\varphi(a)$. А S_d обратится в число значений $\delta = (x, a)$, кратных d. Но (x, a) может быть кратным d лишь при условии, что d — делитель числа a. При наличии же этого условия S_d обратится в число значений x, кратных d, т. е. в $\frac{a}{d}$. Поэтому

$$\varphi(a) = \sum_{d \setminus a} \mu(d) \frac{a}{d},$$

откуда (ввиду 3, b, § 4) следует формула (3), а из последней (ввиду 2)) следует формула (4).

Примеры.

$$\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16,$$

$$\varphi(81) = 81 - 27 = 54,$$

$$\varphi(5) = 5 - 1 = 4.$$

2. $\varphi(a)$ — *мультипликативная функция, для которой при* $\alpha > 0$ *имеем* $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Это следует из формулы (4) и теоремы d, § 2.

c. *Имеем*

$$\sum_{d \setminus a} \varphi(d) = a.$$

В справедливости этой формулы убедимся, применяя тождество f, § 2, которое при $\theta(a) = \varphi(a)$ дает

$$\sum_{d \setminus a} \varphi(a) = \left(1 + \varphi(p_1) + \ldots + \varphi\left(p_1^{\alpha_1}\right)\right)\ldots$$
$$\ldots\left(1 + \varphi(p_k) + \ldots + \varphi\left(p_k^{\alpha_k}\right)\right).$$

Ввиду (5) правая часть окажется равной

$$\left(1 + (p_1 - 1) + \ldots + \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\right)\ldots$$
$$\ldots\left(1 + (p_k - 1) + \ldots + \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)\right),$$

что после приведения в каждой большой скобке подобных членов обратится в

$$p_1^{\alpha_1}\dots p_k^{\alpha_k}=a.$$

Пример. Полагая $a=12$, находим

$$\varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(12)=$$
$$=1+1+2+2+2+4=12.$$

Вопросы к главе II

1, a. Пусть в интервале $Q\leqslant x\leqslant R$ функция $f(x)$ непрерывна и неотрицательна. Доказать, что сумма

$$\sum_{Q<x\leqslant R}[f(x)]$$

выражает число целых точек (точек с целыми координатами) плоской области: $Q<x\leqslant R$, $0<y\leqslant f(x)$.

b. Пусть P и Q — положительные нечетные взаимно простые. Доказать, что

$$\sum_{0<x<\frac{Q}{2}}\left[\frac{P}{Q}x\right]+\sum_{0<y<\frac{P}{2}}\left[\frac{Q}{P}y\right]=\frac{P-1}{2}\cdot\frac{Q-1}{2}.$$

c. Пусть $r>0$ и T — число целых точек области $x^2+y^2\leqslant r^2$. Доказать, что

$$T=1+4[r]+8\sum_{0<x\leqslant\frac{r}{\sqrt{2}}}[\sqrt{r^2-x^2}]-4\left[\frac{r}{\sqrt{2}}\right]^2.$$

d. Пусть $n>0$ и T — число целых точек области $x>0$, $y>0$, $xy\leqslant n$. Доказать, что

$$T=2\sum_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]-[\sqrt{n}]^2.$$

e. Рассмотрим многоугольник, вершины которого — целые точки и контур которого сам себя не пересекает и не касается. Пусть S — площадь многоугольника и $T=\sum\delta-1$, где суммирование распространяется на все целые точки, лежащие внутри многоугольника и на его контуре, причем $\delta=1$ для внутренних точек и $\delta=0{,}5$ для точек контура. Доказать, что $T=S$.

2. Пусть $n>0$, m — целое, $m>1$ и x пробегает целые положительные числа, не делящиеся на m-ю степень целого, превосходящего 1. Доказать, что

$$\sum_x\left[\sqrt[m]{\frac{n}{x}}\right]=[n].$$

3. Пусть положительные α и β таковы, что

$$[\alpha x];\quad x=1,\ 2,\ \ldots;\quad [\beta y],\quad y=1,\ 2,\ \ldots,$$

образуют, вместе взятые, все числа натурального ряда без повторений. Доказать, что это имеет место тогда и только тогда, когда α иррациональное, причем

$$\frac{1}{\alpha}+\frac{1}{\beta}=1.$$

4, a. Пусть $[\tau]\geqslant 1$, $t=[\tau]$ и $x_1,\ x_2,\ \ldots,\ x_t$ — числа $1, 2, \ldots, t$, расположенные в таком порядке, чтобы числа

$$0,\ \{\alpha x_1\},\ \{\alpha x_2\},\ \ldots,\ \{\alpha x_t\},\ 1$$

шли не убывая. Доказать теорему вопроса 4, b, гл. I, рассматривая разности соседних чисел последнего ряда.

b. Пусть $\tau_1, \tau_2, \ldots, \tau_k$ — вещественные числа, каждое из которых не меньше 1; $\alpha_1, \alpha_2, \ldots, \alpha_k$ — вещественные. Доказать, что существуют целые $\xi_1, \xi_2, \ldots, \xi_k$, не равные одновременно нулю, и целое η, удовлетворяющие условиям:

$$|\xi_1|\leqslant\tau_1,\quad |\xi_2|\leqslant\tau_2,\ \ldots,\ |\xi_k|\leqslant\tau_k\quad (\xi_1,\ \xi_2,\ \ldots,\ \xi_k,\ \eta)=1,$$

$$|\alpha_1\xi_1+\alpha_2\xi_2+\ldots+\alpha_k\xi_k-\eta|<\frac{1}{\tau_1\tau_2\ldots\tau_k}.$$

5. Пусть α — вещественное, c — целое, $c>0$. Доказать, что

$$\left[\frac{[\alpha]}{c}\right]=\left[\frac{\alpha}{c}\right].$$

6, a. Пусть $\alpha, \beta, \ldots, \lambda$ — вещественные. Доказать, что

$$[\alpha+\beta+\ldots+\lambda]\geqslant[\alpha]+[\beta]+\ldots+[\lambda].$$

b. Пусть $a, b, \ldots, l$ — целые положительные, $a+b+\ldots+l=n$. Применяя b, § 1, доказать, что

$$\frac{n!}{a!\,b!\ldots l!}$$

есть целое число.

7. Пусть h — целое, $h>0$, p — простое и

$$u_s=\frac{p^{s+1}-1}{p-1}.$$

Представляя h в виде $h=p_mu_m+p_{m-1}u_{m-1}+\ldots+p_1u_1+p_0$, где u_m — наибольшее u_s, не превосходящее h, p_mu_m — наибольшее кратное u_m, не превосходящее h, $p_{m-1}u_{m-1}$ — наибольшее кратное u_{m-1}, не превосходящее $h-p_mu_m$, $p_{m-2}u_{m-2}$ — наибольшее кратное u_{m-2}, не превосходящее $h-p_mu_m-p_{m-1}u_{m-1}$, и т. д., доказать, что числа a с условием, что в каноническое разложение $a!$ число p входит с показателем h, существуют тогда и только тогда, когда все $p_m, p_{m-1}, \ldots, p_1, p_0$ меньше p, причем в этом случае указанные a суть все числа вида

$$a=p_mp^{m+1}+p_{m-1}p^m+\ldots+p_1p^2+p_0p+p',$$

где p' имеет значения: $0, 1, \ldots, p-1$.

8, a. Пусть в интервале $Q \leqslant x \leqslant R$ функция $f(x)$ имеет вторую непрерывную производную. Полагая

$$\rho(x) = \frac{1}{2} - \{x\}, \quad \sigma(x) = \int_0^x \rho(z)\, dz,$$

доказать, что

$$\sum_{Q < x \leqslant R} f(x) = \int_Q^R f(x)\, dx + \rho(R) f(R) - \rho(Q) f(Q) -$$

$$- \sigma(R) f'(R) + \sigma(Q) f'(Q) + \int_Q^R \sigma(x) f''(x)\, dx.$$

b. Пусть условие вопроса a выполняется при сколь угодно больших R, причем $\int_Q^\infty |f''(x)|\, dx$ сходится. Доказать, что

$$\sum_{Q < x \leqslant R} f(x) = C + \int_Q^R f(x)\, dx + \rho(R) f(R) - \sigma(R) f'(R) - \int_R^\infty \sigma(x) f''(x) dx,$$

где C не зависит от R.

c. Если B принимает лишь положительные значения и отношение $\frac{|A|}{B}$ остается ограниченным сверху, то пишем $A = O(B)$, или $A \ll B$.

Пусть n—целое, $n > 1$. Доказать, что

$$\ln(n!) = n \ln n - n + O(\ln n).$$

9, a. Пусть $n \geqslant 2$, $\Theta(z, z_0) = \sum_{z_0 < p \leqslant z} \ln p$, где p пробегает простые числа Пусть, далее, $\Theta(z) = \Theta(z, 0)$ и при $x > 0$.

$$\psi(x) = \Theta(x) + \Theta(\sqrt{x}) + \Theta(\sqrt[3]{x}) + \ldots$$

Доказать, что

α) $\ln([n]!) = \psi(n) + \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) + \ldots$;

β) $\psi(n) < 2n$,

γ) $\Theta\left(n, \frac{n}{2}\right) + \Theta\left(\frac{n}{3}, \frac{n}{4}\right) + \Theta\left(\frac{n}{5}, \frac{n}{6}\right) + \ldots = n \ln 2 + O(\sqrt{n})$.

b. При $n > 2$ доказать, что

$$\sum_{p \leqslant n} \frac{\ln p}{p} = \ln n + O(1),$$

где p пробегает простые числа.

c. Пусть ε—произвольное положительное постоянное. Доказать, что в ряде натуральных чисел существует бесчисленное множество пар p_n, p_{n+1} простых чисел с условием $p_{n+1} < p_n(1+\varepsilon)$.

d. Пусть $n > 2$. Доказать, что

$$\sum_{p \leqslant n} \frac{1}{p} = C + \ln \ln n + O\left(\frac{1}{\ln n}\right),$$

где p пробегает простые числа и C не зависит от n.

e. Пусть $n > 2$. Доказать, что

$$\prod_{p \leqslant n} \left(1 - \frac{1}{p}\right) = \frac{C_0}{\ln \ln n}\left(1 + O\left(\frac{1}{\ln n}\right)\right),$$

где p пробегает простые числа и C_0 не зависит от n

f. Доказать существование постоянного $s_0 > 2$ с условием, что при любом целом $s > s_0$ для s-го простого числа p_s ряда 2, 3, 5, ... имеет место неравенство

$$p_s < 1{,}5 s \ln s.$$

g. Доказать, что

$$\frac{a}{\varphi(a)} = O(\ln \ln a).$$

10, a. Пусть $\theta(a)$ — функция мультипликативная. Доказать, что $\theta_1(a) = \sum_{d \setminus a} \theta(d)$ — также функция мультипликативная.

b. Пусть функция $\theta(a)$ определена для всех целых положительных a и функция $\psi(a) = \sum_{d \setminus a} \theta(a)$ — мультипликативная. Доказать, что функция $\theta(a)$ также мультипликативная.

11. Пусть при $m > 0$ $\tau_m(a)$ обозначает число решений неопределенного уравнения $x_1 x_2 \ldots x_m = a$ ($x_1, x_2, \ldots, x_m$ независимо друг от друга пробегают целые положительные числа); в частности, очевидно, $\tau_1(a) = 1$, $\tau_2(a) = \tau(a)$. Доказать, что

a. $\tau_m(a)$ — функция мультипликативная.

b. Пусть p — простое, $\alpha \geqslant 0$ и $m > 1$. Тогда

$$\tau_m(p^\alpha) = \frac{(\alpha+1)(\alpha+2)\ldots(\alpha+m-1)}{1 \cdot 2 \ldots (m-1)}.$$

c. Если ε — произвольное положительное постоянное, то

$$\lim_{a \to \infty} \frac{\tau_m(a)}{a^\varepsilon} = 0.$$

d. $\sum_{0 < a \leqslant n} \tau_m(a)$ выражает число решений неравенства $x_1 x_2 \ldots x_m \leqslant n$ в целых положительных $x_1, x_2, \ldots, x_m$.

12. Пусть $R(s)$ обозначает вещественную часть числа s.

При $R(s) > 1$ полагаем $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$. Пусть $m > 0$, m — целое.

Доказать, что

$$(\zeta(s))^m = \sum_{n=1}^{\infty} \frac{\tau_m(n)}{n^s}.$$

13, a. При $R(s) > 1$ доказать, что

$$\zeta(s) = \prod \frac{1}{1-\frac{1}{p^s}},$$

где p пробегает все простые числа.

b. Доказать бесконечность числа простых чисел, исходя из того, что гармонический ряд — расходящийся.

c. Доказать бесконечность числа простых чисел, исходя из того, что $\zeta(2) = \frac{\pi^2}{6}$ — число иррациональное.

14. Пусть $\Lambda(a) = \ln p$ для $a = p^l$, где p — простое и l — целое положительное; $\Lambda(a) = 0$ для других целых положительных a. При $R(s) > 1$ доказать, что

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

15. Пусть $R(s) > 1$. Доказать, что

$$\prod_p \left(1-\frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

где p пробегает простые числа.

16, a. Пусть $n \geqslant 1$. Применяя **c**, § 4, доказать, что

$$1 = \sum_{0<d\leqslant n} \mu(d) \left[\frac{n}{d}\right].$$

b. Пусть $M(z, z_0) = \sum_{z_0 < a \leqslant z} \mu(a)$; $M(x) = M(x, 0)$. Доказать, что

$$\alpha)\ M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + \ldots = 1, \quad n \geqslant 1,$$

$$\beta)\ M\left(n, \frac{n}{2}\right) + M\left(\frac{n}{3}, \frac{n}{4}\right) + M\left(\frac{n}{5}, \frac{n}{6}\right) + \ldots = -1, \quad n \geqslant 2.$$

c. Пусть $n \geqslant 1$. l — целое, $l > 1$, $T_{l,n}$ — число целых x с условием $0 < x \leqslant n$, не делящихся на l-ю степень целого, превосходящего 1. Применяя **c**, § 4, доказать, что

$$T_{l,n} = \sum_{d=1}^{\infty} \mu(d) \left[\frac{n}{d^l}\right].$$

17, a. Пусть a — целое, $a > 0$, и для целых $x_1, x_2, \ldots, x_n$ однозначно определена функция $f(x)$. Доказать, что

$$S' = \sum_{d \setminus a} \mu(d)\, S_d,$$

где S' обозначает сумму значений $f(x)$, распространенную на значения x, взаимно простые с a, и S_d — сумму значений $f(x)$, распространенную на значения x, кратные d.

b. Пусть $k > 1$ и заданы системы

$$x_1', x_2', \ldots, x_k'; \quad x_1'', x_2'', \ldots, x_k''; \quad \ldots; \quad x_1^{(m)}, x_2^{(m)}, \ldots, x_k^{(n)},$$

каждая из которых состоит из целых чисел, не равных одновременно нулю. Пусть далее для этих систем однозначно определена функция $f(x_1, x_2, \ldots, x_k)$. Доказать, что

$$S' = \sum \mu(d)\, S_d,$$

где S' обозначает сумму значений $f(x_1, x_2, \ldots, x_k)$, распространенную на системы взаимно простых чисел, и S_d обозначает сумму значений $f(x_1, x_2, \ldots, x_k)$, распространенную на системы чисел, одновременно кратных d. При этом d пробегает целые положительные числа.

c. Пусть a — целое, $a > 0$, и для делителей δ числа a однозначно определена функция $F(\delta)$. Полагая

$$G(\delta) = \sum_{d \setminus \delta} F(d),$$

доказать, что (закон обращения числовых функций)

$$F(a) = \sum_{d \setminus a} \mu(d)\, G\left(\frac{a}{d}\right).$$

d. Пусть целым положительным

$$\delta_1, \delta_2, \ldots, \delta_n$$

отвечают любые вещественные или комплексные, не равные нулю:

$$f_1, f_2, \ldots, f_n.$$

Доказать, что

$$P' = \prod P_d^{\mu(d)},$$

где P' обозначает произведение значений f, отвечающих значениям δ, равным 1, P_d обозначает произведение значений f, отвечающих значениям δ, кратным d, причем d пробегает все целые положительные числа, делящие хотя бы одно δ.

18. Пусть a — целое, $a > 1$, $\sigma_m(n) = 1^m + 2^m + \ldots + n^m$, $\psi_m(a)$ — сумма m-х степеней чисел ряда 1, 2, ..., a, взаимно простых с a; $p_1, p_2, \ldots, p_k$ — все простые делители числа a.

a. Применяя теорему вопроса 17, a, доказать, что

$$\psi_m(a) = \sum_{d \setminus a} \mu(d)\, d^m \sigma_m\left(\frac{a}{d}\right).$$

b. Доказать, что

$$\psi_1(a)=\frac{a}{2}\varphi(a).$$

c. Доказать, что

$$\psi_2(a)=\left(\frac{a^2}{3}+\frac{(-1)^k}{6}p_1p_2\dots p_k\right)\varphi(a).$$

19. Пусть $z>1$, a—целое, $a>0$, T_z—число чисел x с условиями $0<x\leqslant z$, $(x, a)=1$, ε—произвольное положительное постоянное.

a. Доказать, что

$$T_z=\sum_{d\backslash a}\mu(d)\left[\frac{z}{d}\right].$$

b. Доказать, что

$$T_z=\frac{z}{a}\varphi(a)+O(a^\varepsilon).$$

c. Пусть $z>1$, $\pi(z)$—число простых чисел, не превосходящих z, a—произведенне простых чисел, не превосходящих $\sqrt{z}$.

Доказать, что

$$\pi(z)=\pi(\sqrt{z})-1+\sum_{d\backslash a}\mu(d)\left[\frac{z}{d}\right].$$

20. Пусть $R(s)>1$, a—целое, $a>0$. Доказать, что

$$\sum{}'\frac{1}{n^s}=\zeta(s)\prod\left(1-\frac{1}{p^s}\right),$$

где в левой части n пробегает целые положнтельные числа, взаимно простые с a, а в правой части p пробегает все простые делнтели числа a

21, a. Вероятность P того, что k целых положительных чисел $x_1, x_2, \dots, x_k$ будут взаимно простымн, определим как предел при $N\to\infty$ вероятности P_N того, что будут взанмно простыми k чисел $x_1, x_2, \dots, x_k$, каждому из которых независнмо от остальных присвоено одно из значений $1, 2, \dots, N$, принимаемых за равновозможные. Прнменяя теорему вопроса 17, b, доказать, что $P=(\zeta(k))^{-1}$.

b. Определяя вероятность P несократимости дробн $\frac{x}{y}$ аналогично тому, как в вопросе a при $k=2$, доказать, что

$$P=\frac{6}{\pi^2}.$$

22, a. Пусть $r\geqslant 2$ и T—число целых точек (x, y) с взаимно простымн координатами, лежащих в областн $x^2+y^2\leqslant r^2$. Доказать, что

$$T=\frac{6}{\pi}r^2+O(r\ln r),$$

b. Пусть $r \geqslant 2$ и T — число целых точек (x, y, z) с взаимно простыми координатами, лежащих в области $x^2+y^2+z^2 \leqslant r^2$. Доказать, что

$$T = \frac{4\pi r^3}{3\zeta(3)} + O(r^2).$$

23, a. Теорему 2, b, § 4 доказать, считая делители числа a, не делящиеся на квадрат целого, превосходящего 1, и имеющие 1, 2, ... простых делителей.

b. Пусть a — целое, $a > 1$, d пробегает делители числа a, имеющие не более чем m простых делителей. Доказать, что при m четном $\sum \mu(d) \geqslant 0$, а при m нечетном $\sum \mu(d) \leqslant 0$.

c. При условиях теоремы c, § 4, считая все f неотрицательными и заставляя d пробегать лишь числа, имеющие не более чем m простых делителей, доказать, что

$$S' \leqslant \sum \mu(d) S_d, \quad S' \geqslant \sum \mu(d) S_d$$

в зависимости от того, будет ли m четным или нечетным.

d. Такие же, как в вопросе c, неравенства доказать при условиях вопроса **17, a**, считая все значения $f(x)$ неотрицательными, а также при условиях **17, b**, считая все значения $f(x_1, x_2, \ldots, x_k)$ неотрицательными.

24. Пусть ε — любое постоянное с условиями $0 < \varepsilon < \frac{1}{6}$, $N \geqslant 8$, $r = \ln N$, $0 < q \leqslant N^{1-\varepsilon}$, $0 \leqslant l < q$, $(q, l) = 1$, $\pi(N, q, l)$ — число простых чисел с условиями: $p \leqslant N$, $p = qt + l$, где t — целое. Доказать, что

$$\pi(N, q, l) = O(\Delta); \quad \Delta = \frac{Nr^{\varepsilon}}{r\varphi(q)}.$$

Для доказательства, полагая $h = r^{1-0.5\varepsilon}$, простые числа с указанными условиями следует рассматривать как частный случай всех чисел с этими условиями взаимно простых с a, где a — произведение всех простых, не превосходящих e^h и не делящих q. Следует применить теорему вопроса **23, d** (условия вопроса **17, a**) с указанным a и $m = 2[2 \ln r + 1]$.

25. Пусть k — четное; $k > 0$, каноническое разложение числа a имеет вид $a = p_1 p_2 \ldots p_k$ и d пробегает делители числа a с условием $0 < d < \sqrt{a}$. Доказать, что

$$\sum_d \mu(d) = 0.$$

26. Пусть k — целое, $k > 0$, d пробегает делители числа с условием $\varphi(d) = k$. Доказать, что

$$\sum_d \mu(d) = 0.$$

27. Пользуясь выражением для $\varphi(a)$, доказать бесконечность числа простых чисел.

28, a. Теорему c, § 5 доказать, установив, что число чисел ряда 1, 2, ..., a, имеющих с a одни и тот же общий наибольший делитель δ, равно $\varphi\left(\frac{a}{\delta}\right)$.

b. Вывести выражение для $\varphi(a)$:

α) пользуясь теоремой вопроса **10, b**;

β) пользуясь теоремой вопроса **17, c**.

29. Пусть $R(s) > 2$. Доказать, что

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}.$$

30. Пусть n — целое, $n \geqslant 2$. Доказать, что

$$\sum_{m=1}^{n} \varphi(m) = \frac{3}{\pi^2} n^2 + O(n \ln n).$$

Численные примеры к главе II

1, a. Найти показатель, с которым 5 входит в каноническое разложение 52581 (см. вопрос **5**).

b. Найти каноническое разложение числа 1251

2, a. Найти τ (5600) и S (5600).

b. Найти τ (116 424) и S (116 424).

3. Составить таблицу значений функции $\mu(a)$ для всех $a = 1, 2, \ldots, 100$

4. Найти: α) φ (5040), β) φ (1 294 700).

5. Составить таблицу значений функции $\varphi(a)$ для всех $a = 1, 2, \ldots, 50$, пользуясь только формулой (5), § 5 и мультипликативностью функции $\varphi(a)$.

Глава III

СРАВНЕНИЯ

§ 1. Основные понятия

а. Мы будем рассматривать целые числа в связи с остатками от деления их на данное целое положительное m, которое назовем *модулем*.

Каждому целому числу отвечает определенный остаток от деления его на m (с, § 1, гл. I); если двум целым a и b отвечает один и тот же остаток r, то они называются *равноостаточными* по модулю m или *сравнимыми* по модулю m.

b. Сравнимость чисел a и b по модулю m записывается так:

$$a \equiv b \pmod{m},$$

что читается: a сравнимо с b по модулю m.

c. *Сравнимость чисел a и b по модулю m равносильна:*

1. *Возможности представить a в виде $a = b + mt$, где t — целое.*

2. *Делимости $a - b$ на m.*

Действительно, из $a \equiv b \pmod{m}$ следует

$$a = mq + r, \quad b = mq_1 + r; \quad 0 \leqslant r < m,$$

откуда

$$a - b = m(q - q_1), \quad a = b + mt, \quad t = q - q_1.$$

Обратно, из $a = b + mt$, представляя b в виде

$$b = mq_1 + r, \quad 0 \leqslant r < m,$$

выводим

$$a = mq + r; \quad q = q_1 + t,$$

т. е.

$$a \equiv b \pmod{m}.$$

Поэтому верно утверждение 1.

Из 1 непосредственно следует утверждение 2.

§ 2. Свойства сравнений, подобные свойствам равенств

a. *Два числа, сравнимые с третьим, сравнимы между собою.*

Следует из a, § 1.

b. *Сравнения можно почленно складывать.*

Действительно, пусть

$$a_1 \equiv b_1 \pmod m, \quad a_2 \equiv b_2 \pmod m, \ \ldots, \ a_k \equiv b_k \pmod m. \quad (1)$$

Тогда (1, c, § 1)

$$a_1 = b_1 + mt_1, \quad a_2 = b_2 + mt_2, \ \ldots, \ a_k = b_k + mt_k, \quad (2)$$

откуда

$$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k + m\,(t_1 + t_2 + \ldots + t_k)$$

или (1, c, § 1)

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod m.$$

Слагаемое, стоящее в какой-либо части сравнения, можно переносить в другую часть, переменив знак на обратный.

Действительно, складывая сравнение $a + b \equiv c \pmod m$ с очевидным сравнением $-b \equiv -b \pmod m$, получим $a \equiv c - b \pmod m$.

К каждой части сравнения можно прибавить любое число, кратное модуля.

Действительно, складывая сравнение $a \equiv b \pmod m$ с очевидным сравнением $mk \equiv 0 \pmod m$, получим $a + mk \equiv b \pmod m$.

c. *Сравнения можно почленно перемножать.*

Действительно, рассмотрим снова сравнения (1) и вытекающие из них равенства (2). Перемножая почленно равенства (2), получим

$$a_1 a_2 \ldots a_k = b_1 b_2 \ldots b_k + mN,$$

где N — целое. Следовательно (1, c, § 1),

$$a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \pmod m.$$

Обе части сравнения можно возвести в одну и ту же степень.

Это следует из предыдущего утверждения.

Обе части сравнения можно умножить на одно и то же целое.

Действительно, перемножив сравнение $a \equiv b \pmod m$ с очевидным сравнением $k \equiv k \pmod m$, получим $ak \equiv bk \pmod m$.

d. Свойства **b** и **c** (сложение и умножение сравнений) обобщаются следующей теоремой.

Если в выражении многочлена с целыми коэффициентами $S = \sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ *заменим* $A_{\alpha_1, \ldots, \alpha_k}$, $x_1, \ldots, x_k$ *числами* $B_{\alpha_1, \ldots, \alpha_k}$, $y_1, \ldots, y_k$, *сравнимыми с прежними по модулю* m, *то новое выражение* S *будет сравнимо с прежним по модулю* m.

Действительно, из

$$A_{\alpha_1, \ldots, \alpha_k} \equiv B_{\alpha_1, \ldots, \alpha_k} \pmod m,$$

$$x_1 \equiv y_1 \pmod m, \quad \ldots, \quad x_k \equiv y_k \pmod m$$

находим (c)

$$x_1^{\alpha_1} \equiv y_1^{\alpha_1} \pmod m, \quad \ldots, \quad x_k^{\alpha_k} \equiv y_k^{\alpha_k} \pmod m,$$

$$A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv B_{\alpha_1, \ldots, \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k} \pmod m,$$

откуда, суммируя, получим

$$\sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv \sum B_{\alpha_1, \ldots, \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k} \pmod m.$$

Если

$$a \equiv b \pmod m, \quad a_1 \equiv b_1 \pmod m, \quad \ldots, \quad a_n \equiv b_n \pmod m,$$

$$x \equiv x_1 \pmod m,$$

то

$$ax^n + a_1 x^{n-1} + \ldots + a_n \equiv bx_1^n + b_1 x_1^{n-1} + \ldots + b_n \pmod m.$$

Это утверждение есть частный случай предыдущего.

e. *Обе части сравнения можно разделить на их общий делитель, если последний взаимно прост с модулем.*

Действительно, из $a \equiv b \pmod m$, $a = a_1 d$, $b = b_1 d$, $(d, m) = 1$ следует, что разность $a - b$, равная $(a_1 - b_1) d$, делится на m. Поэтому (2, f, § 2, гл. I) $a_1 - b_1$ делится на m, т. е. $a_1 \equiv b_1 \pmod m$.

§ 3. Дальнейшие свойства сравнений

a. *Обе части сравнения и модуль можно умножить на одно и то же целое.*

Действительно, из $a \equiv b \pmod{m}$ следует

$$a = b + mt, \quad ak = bk + mkt$$

и, следовательно, $ak \equiv bk \pmod{mk}$.

b. *Обе части сравнения и модуль можно разделить на любой их общий делитель.*

Действительно, пусть

$$a \equiv b \pmod{m}, \quad a = a_1 d, \quad b = b_1 d, \quad m = m_1 d.$$

Имеем

$$a = b + mt, \quad a_1 d = b_1 d + m_1 dt, \quad a_1 = b_1 + m_1 t$$

и, следовательно, $a_1 \equiv b_1 \pmod{m_1}$.

c. *Если сравнение $a \equiv b$ имеет место по нескольким модулям, то оно имеет место и по модулю, равному общему наименьшему кратному этих модулей.*

В самом деле, из $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$ следует, что разность $a - b$ делится на все модули $m_1, m_2, \ldots, m_k$. Поэтому (6, e, § 5, гл. I) она должна делиться и на общее наименьшее кратное m этих модулей, т. е. $a \equiv b \pmod{m}$.

d. *Если сравнение имеет место по модулю m, то оно имеет место и по модулю d, равному любому делителю числа m.*

В самом деле, из $a \equiv b \pmod{m}$ следует, что разность $a - b$ должна делиться на m; поэтому (1, b, § 1, гл. I) она должна делиться и на любой делитель d числа m, т. е. $a \equiv b \pmod{d}$.

e. *Если одна часть сравнения и модуль делятся на какое-либо число, то и другая часть сравнения должна делиться на то же число.*

Действительно, из $a \equiv b \pmod{m}$ следует $a - b + mt$; если a и m кратны d, то (2, b, § 1, гл. I) и b должно быть кратным d, что и утверждалось.

f. *Если $a \equiv b \pmod{m}$, то $(a, m) = (b, m)$.*

Действительно, ввиду 2, b, § 2, гл. I это равенство непосредственно следует из $a = b + mt$.

§ 4. Полная система вычетов

а. Числа равноостаточные, или, что то же самое, сравнимые по модулю m, образуют *класс* чисел по модулю m.

Из такого определения следует, что всем числам класса отвечает один и тот же остаток r, и мы получим все числа класса, если в форме $mq+r$ заставим q пробегать все целые числа.

Соответственно m различным значениям r имеем m классов чисел по модулю m.

b. Любое число класса называется *вычетом по модулю m* по отношению ко всем числам того же класса. Вычет, получаемый при $q=0$, равный самому остатку r, называется *наименьшим неотрицательным вычетом*.

Вычет ρ, самый малый по абсолютной величине, называется *абсолютно наименьшим вычетом*.

Очевидно, при $r < \frac{m}{2}$ имеем $\rho = r$, при $r > \frac{m}{2}$ имеем $\rho = r - m$; наконец, если m четное и $r = \frac{m}{2}$, то за ρ можно принять любое из двух чисел $\frac{m}{2}$ и $\frac{m}{2} - m = -\frac{m}{2}$.

Взяв от каждого класса по одному вычету, получим *полную систему вычетов по модулю m*. Чаще всего в качестве полной системы вычетов употребляют наименьшие неотрицательные вычеты $0, 1, \ldots, m-1$ или также абсолютно наименьшие вычеты; последние, как это следует из вышеизложенного, в случае нечетного m представляются рядом

$$-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2},$$

а в случае четного m каким-либо из двух рядов

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2},$$

$$-\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1$$

с. *Любые m чисел, попарно несравнимые по модулю m, образуют полную систему вычетов по этому модулю.*

Действительно, будучи несравнимы, эти числа тем самым принадлежат к различным классам, а так как их m, т. е. столько же, сколько и классов, то в каждый класс наверно попадет по одному числу.

d. *Если* $(a, m) = 1$ *и* x *пробегает полную систему вычетов по модулю* m, *то* $ax + b$, *где* b — *любое целое, тоже пробегает полную систему вычетов по модулю* m.

Действительно, чисел $ax + b$ будет столько же, сколько и чисел x, т. е. m. Согласно с остается, следовательно, только показать, что любые два числа $ax_1 + b$ и $ax_2 + b$, отвечающие несравнимым x_1 и x_2, будут сами несравнимы по модулю m.

Но допустив, что $ax_1 + b \equiv ax_2 + b \pmod m$, мы придем к сравнению $ax_1 = ax_2 \pmod m$, откуда, вследствие $(a, m) = 1$, получим $x_1 = x_2 \pmod m$, что противоречит предположению о несравнимости чисел x_1 и x_2.

§ 5. Приведенная система вычетов

a. Согласно f, § 3 числа одного и того же класса по модулю m имеют с модулем один и тот же общий наибольший делитель. Особенно важны классы, для которых этот делитель равен единице, т. е. классы, содержащие числа, взаимно простые с модулем.

Взяв от каждого такого класса по одному вычету, получим *приведенную систему вычетов по модулю* m. Приведенную систему вычетов, следовательно, можно составить из чисел полной системы, взаимно простых с модулем. Обыкновенно приведенную систему вычетов выделяют из системы наименьших неотрицательных вычетов: 0, 1, ..., $m-1$. Так как среди этих чисел число взаимно простых с m есть $\varphi(m)$, то число чисел приведенной системы, равно как и число классов, содержащих числа, взаимно простые с модулем, есть $\varphi(m)$.

Пример. Приведенная система вычетов по модулю 42 будет

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

b. *Любые* $\varphi(m)$ *чисел, попарно несравнимые по модулю* m *и взаимно простые с модулем, образуют приведенную систему вычетов по модулю* m.

Действительно, будучи несравнимыми и взаимно простыми с модулем, эти числа тем самым принадлежат к различным классам, содержащим числа, взаимно простые с модулем, а так как их $\varphi(m)$, т. е. столько же, сколько и классов указанного вида, то в каждый класс наверно попадет по одному числу.

c. *Если* $(a, m) = 1$ *и* x *пробегает приведенную систему вычетов по модулю* m, *то* ax *тоже пробегает приведенную систему вычетов по модулю* m.

Действительно, чисел ax будет столько же, сколько и чисел x, т. е. $\varphi(m)$. Согласно **b** остается, следовательно, только показать, что числа ax по модулю m несравнимы и взаимно просты с модулем. Но первое доказано в **d**, § 4 для чисел более общего вида $ax+b$, второе же следует из $(a, m) = 1$, $(x, m) = 1$.

§ 6. Теоремы Эйлера и Ферма

a. *При* $m > 1$ *и* $(a, m) = 1$ *имеем (теорема Эйлера):*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Действительно, если x пробегает приведенную систему вычетов

$$x = r_1, r_2, \ldots, r_c; \quad c = \varphi(m),$$

составленную из наименьших неотрицательных вычетов, то наименьшие неотрицательные вычеты $\rho_1, \rho_2, \ldots, \rho_c$ чисел ax будут пробегать ту же систему, но расположенную, вообще говоря, в ином порядке (c, § 5).

Перемножая почленно сравнения

$$ar_1 \equiv \rho_1 \pmod{m}, \quad ar_2 \equiv \rho_2 \pmod{m}, \quad \ldots, \quad ar_c \equiv \rho_c \pmod{m},$$

получим

$$a^c r_1 r_2 \ldots r_c \equiv \rho_1 \rho_2 \ldots \rho_c \pmod{m},$$

откуда, деля обе части на произведение $r_1 r_2 \ldots r_c = \rho_1 \rho_2 \ldots \rho_c$, получим

$$a^c \equiv 1 \pmod{m}.$$

b. *При* p *простом и* a, *не делящемся на* p, *имеем (теорема Ферма):*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Эта теорема является следствием теоремы **a** при $m = p$. Последней теореме можно придать более удобную форму. Именно, умножая обе части сравнения (1) на a, получим сравнение

$$a^p \equiv a \pmod{p},$$

справедливое уже при всех целых a, так как оно верно и при a, кратном p.

Вопросы к главе III

1, a. Представляя целое число в обычной десятичной системе исчисления, вывести признаки делимости на 3, 9, 11.

b. Представляя целое число в системе исчисления с основанием 100, вывести признак делимости на 101.

c. Представляя целое число в системе исчисления с основанием 1000, вывести признаки делимости на 37, 7, 11, 13.

2. Пусть $m > 1$, $(a, m) = 1$, b—целое, x пробегает полную, а ξ—приведенную систему вычетов по модулю m. Доказать, что

$$\alpha) \sum_x \left\{\frac{ax+b}{m}\right\} = \frac{1}{2}(m-1).$$

$$\beta) \sum_\xi \left\{\frac{a\xi}{m}\right\} = \frac{1}{2}\varphi(m).$$

3, a. Пусть $m > 0$, $(a, m) = 1$, $h \geqslant 0$, c—вещественное,

$$S = \sum_{x=0}^{m-1} \left\{\frac{ax+\psi(x)}{m}\right\},$$

где $\psi(x)$ для рассматриваемых значений x принимает значения с условием $c \leqslant \psi(x) \leqslant c+h$. Доказать, что

$$\left|S - \frac{i}{2}m\right| \leqslant h + \frac{1}{2}.$$

b. Пусть M—целое, $m > 0$, $(a, m) = 1$, A и B—вещественные,

$$A = \frac{a}{m} + \frac{\lambda}{m^2}; \quad S = \sum_{x=M}^{M+m-1} \{Ax+B\}.$$

Доказать, что

$$\left|S - \frac{1}{2}m\right| \leqslant |\lambda| + \frac{1}{2}.$$

c. Пусть M—целое, $m > 0$, $(a, m) = 1$,

$$S = \sum_{x=M}^{M+m-1} \{f(x)\},$$

где в интервале $M \leqslant x \leqslant M+m-1$ функция $f(x)$ имеет непрерывные производные $f'(x)$ и $f''(x)$, причем выполняются условия

$$f'(M) = \frac{a}{m} + \frac{\theta}{m^2}; \quad (a, m) = 1; \quad |\theta| < 1; \quad \frac{1}{A} \leqslant |f''(x)| \leqslant \frac{k}{A},$$

где

$$1 \leqslant m \leqslant \tau, \quad \tau = A^{\frac{1}{3}}, \quad A \geqslant 2, \quad k \geqslant 1.$$

Доказать, что

$$\left| S - \frac{1}{2} m \right| < \frac{k+3}{2}.$$

4. Пусть в разложении иррационального числа A в непрерывную дробь все неполные частные ограничены, M—целое, m—целое, $m > 0$, B—вещественное. Доказать, что

$$\sum_{x=M}^{M+m-1} \{Ax + B\} = \frac{1}{2} m + O(\ln m).$$

5, a. Пусть $A > 2$, $k \geqslant 1$ и в интервале $Q \leqslant x \leqslant R$ функция $f(x)$ имеет вторую непрерывную производную, удовлетворяющую условиям

$$\frac{1}{A} \leqslant |f''(x)| \leqslant \frac{k}{A}.$$

Доказать, что

$$\sum_{Q < x \leqslant R} \{f(x)\} = \frac{1}{2}(R-Q) + \theta\Delta; \quad |\theta| < 1,$$

$$\Delta = (2k^2(R-Q)\ln A + 8kA) A^{-\frac{1}{3}}.$$

b. Пусть $0 < \sigma \leqslant 1$, Q и R—целые. При условиях вопроса a доказать, что число $\psi(\sigma)$ дробей $\{f(x)\}$; $x = Q+1, \ldots, R$ с условием $0 \leqslant \{f(x)\} < \sigma$ выражается формулой

$$\Phi(\sigma) = \sigma(R-Q) + \theta' \cdot 2\Delta; \quad |\theta'| < 1.$$

6, a. Пусть T—число целых точек (x, y) области $x^2 + y^2 \leqslant r^2$ $(r \geqslant 2)$. Доказать, что

$$T = \pi r^2 + O\left(r^{\frac{2}{3}} \ln r\right).$$

b. Пусть n—целое, $n > 2$, E—постоянная Эйлера. Доказать, что

$$\tau(1)+\tau(2)+\ldots+\tau(n)=n(\ln n+2E-1)+O\left(n^{\frac{1}{3}}(\ln n)^2\right).$$

c. При $N \geqslant 2$ и целом положительном l доказать, что

$$\sum_{0<a\leqslant N}\frac{(\tau(a))^l}{a} \ll (\ln N)^{2^l}. \qquad (1)$$

Для доказательства воспользоваться очевидным неравенством: $\tau(uv) \leqslant \tau(u)\,\tau(v)$.

d. При $N \geqslant 2$ и целом положительном l доказать, что

$$\sum_{0<a\leqslant N}(\tau(a))^l \ll N(\ln N)^{2^l-1}. \qquad (2)$$

7. Систему n целых положительных чисел, каждое из которых представлено в системе исчисления с основанием 2, назовем правильной, если при всяком целом неотрицательном s число чисел, в представление которых входит 2^s, будет четным, и неправильной, если хотя бы при одном s это число будет нечетным.

Доказать, что неправильную систему путем уменьшения или полного изъятия некоторого одного ее члена можно сделать правильной, а правильная система от уменьшения или полного изъятия любого ее члена делается неправильной.

8, a. Доказать, что сумма

$$3^n x_n+3^{n-1}x_{n-1}+\ldots+3x_1+x_0,$$

где $x_n, x_{n-1}, \ldots, x_1, x_0$ независимо друг от друга пробегают значения —1, 0, 1, представляет все числа

$$-H, \ldots, -1, 0, 1, \ldots, H; \quad H=\frac{3^{n+1}-1}{3-1},$$

причем каждое число—единственным способом.

b. Пусть $m_1, m_2, \ldots, m_k$—положительные попарно простые. Пользуясь c, § 4, доказать, что полную систему вычетов по модулю $m_1m_2\ldots m_k$ получим, заставляя в сумме

$$x_1+m_1x_2+m_1m_2x_3+\ldots+m_1m_2\ldots m_{k-1}x_k$$

числа $x_1, x_2, \ldots, x_k$ пробегать полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$.

9. Пусть $m_1, m_2, \ldots, m_k$—попарно простые и

$$m_1m_2\ldots m_k=M_1m_1=M_2m_2=\ldots=M_km_k.$$

a. Применяя c, § 4, доказать, что полную систему вычетов по модулю $m_1m_2\ldots m_k$ получим, заставляя в сумме

$$M_1x_1+M_2x_2+\ldots+M_kx_k$$

числа $x_1, x_2, \ldots, x_k$ пробегать полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$.

b. Применяя b § 5, гл. II и b, § 5, доказать, что приведенную систему вычетов по модулю $m_1 m_2 \dots m_k$ получим, заставляя в сумме

$$M_1 x_1 + M_2 x_2 + \dots + M_k x_k$$

числа $x_1, x_2, \dots, x_k$ пробегать приведенные системы вычетов по модулям $m_1, m_2, \dots, m_k$.

c. Доказательство теоремы вопроса b провести независимо от теоремы b, § 5, гл. II и тогда уже вывести последнюю теорему, как следствие первой.

d. Найти элементарным путем выражение для $\varphi(p^\alpha)$ и, пользуясь мультипликативностью $\varphi(a)$, вывести известное выражение для $\varphi(a)$.

10. Пусть $m_1, m_2, \dots, m_k$ — попарно простые, превосходящие 1, $m = m_1 m_2 \dots m_k$,

a. Пусть $x_1, x_2, \dots, x_k, x$ пробегают полные, а $\xi_1, \xi_2, \dots, \xi_k, \xi$ — приведенные системы вычетов по модулям $m_1, m_2, \dots, m_k, m$. Доказать, что дроби

$$\left\{ \frac{x_1}{m_1} + \frac{x_2}{m_2} + \dots + \frac{x_k}{m_k} \right\}$$

совпадают с дробями $\left\{ \frac{x}{m} \right\}$, а дроби $\left\{ \frac{\xi_1}{m_1} + \frac{\xi_2}{m_2} + \dots + \frac{\xi_k}{m_k} \right\}$ совпадают с дробями $\left\{ \frac{\xi}{m} \right\}$.

b. Пусть задан многочлен $f(x, \dots, w)$ с целыми коэффициентами от r переменных $x, \dots, w$ $(r \geqslant 1)$:

$$f(x, \dots, w) = \sum_{\alpha, \dots, \delta} c_{\alpha, \dots, \delta} x^\alpha \dots w^\delta$$

и пусть

$$a = M_1 a_1 + \dots + M_k a_k,$$

$x_s, \dots, w_s$ пробегают полные, а $\xi_s, \dots, \omega_s$ — приведенные системы вычетов по модулю m_s; $x, \dots, w$ пробегают полные, а $\xi, \dots, \omega$ — приведенные системы вычетов по модулю m. Доказать, что дроби $\left\{ \frac{a_1 f(x_1, \dots, w_1)}{m_1} + \dots + \frac{a_k f(x_k, \dots, w_k)}{m_k} \right\}$ совпадают с дробями $\left\{ \frac{af(x, \dots, w)}{m} \right\}$, а дроби $\left\{ \frac{a_1 f(\xi_1, \dots, \omega_1)}{m_1} + \dots + \frac{a_k f(\xi_k, \dots, \omega_k)}{m_k} \right\}$ совпадают с дробями $\left\{ \frac{af(\xi, \dots, \omega)}{m} \right\}$ (обобщение теорем вопроса a).

11, a. Пусть m — целое, $m > 0$, a — целое, x пробегает полную систему вычетов по модулю m. Доказать, что

$$\sum e^{2\pi i \frac{ax}{m}} = \begin{cases} m, & \text{если } a \text{ кратно } m, \\ 0 & \text{в противном случае.} \end{cases}$$

b. Пусть α — вещественное, M — целое, P — целое $P>0$. Обозначая символом (α) численное значение разности между α и ближайшим к α целым числом (расстояние α до ближайшего целого), доказать, что

$$\left|\sum_{x=M}^{M+P-1} e^{2\pi i\alpha x}\right| \leqslant \min\left(P, \frac{1}{(\alpha)h}\right); \quad h \geqslant \begin{cases} 2 & \text{всегда,} \\ 3 & \text{при } (\alpha) \leqslant \frac{1}{6}. \end{cases}$$

c. Пусть m — целое, $m>1$ и функции $M(a)$ и $P(a)$ для значений $a=1, 2, \ldots, m-1$ принимают целые значения с условием $P(a)>0$. Доказать, что

$$\sum_{a=1}^{m-1}{}' \left|\sum_{x=M(a)}^{M(a)+P(a)-1}{}' e^{2\pi i\frac{a}{m}x}\right| < \delta;$$

$$\delta = \begin{cases} m\ln m, \\ m\ln m - \frac{m}{2} \text{ при } m \geqslant 12, \\ m\ln m - m \text{ при } m \geqslant 60. \end{cases}$$

12, a. Пусть m — целое, $m>0$, ξ пробегает приведенную систему вычетов по модулю m. Доказать, что

$$\mu(m) = \sum_{\xi} e^{2\pi i\frac{\xi}{m}}.$$

b. Пользуясь теоремой вопроса a, доказать первую из теорем c, § 4, гл. II (см. решение вопроса 28, a, гл. II).

c. Теорему вопроса a вывести, пользуясь теоремой вопроса 17, a, гл. II.

d. Пусть

$$f(x, \ldots, w) = \sum_{\alpha, \ldots, \delta} c_{\alpha, \ldots, \delta} x^{\alpha} \ldots w^{\delta}$$

— многочлен с целыми коэффициентами от r переменных $x, \ldots, w$ ($r \geqslant 1$), a — целое, m — целое, $m>0$, $x, \ldots, w$ пробегают полные, а $\xi, \ldots, \omega$ — приведенные системы вычетов по модулю m. Вводим обозначения

$$S_{a, m} = \sum_{x} \ldots \sum_{w} e^{2\pi i\frac{af(x, \ldots, w)}{m}}, \quad S'_{a, m} = \sum_{\xi} \ldots \sum_{\omega} e^{2\pi i\frac{af(\xi, \ldots, \omega)}{m}}.$$

Пусть далее $m = m_1 \ldots m_k$, где $m_1, \ldots, m_k$ — попарно простые, превосходящие 1, и пусть $m = M_s m_s$. Доказать, что

$$S_{a_1, m_1} \ldots S_{a_k, m_k} = S_{M_1 a_1 + \ldots + M_k a_k, m},$$

$$S'_{a_1, m_1} \ldots S'_{a_k, m_k} = S'_{M_1 a_1 + \ldots + M_k a_k, m}$$

e. При обозначениях вопроса d полагаем

$$A(m)=m^{-r}\sum_{a}S_{a,m},\quad A'(m)=m^{-r}\sum_{a}S'_{a,m},$$

где a пробегает приведенную систему вычетов по модулю m.
Доказать, что

$$A(m_1)\ldots A(m_k)=A(m),\quad A'(m_1)\ldots A'(m_k)=A'(m).$$

13, a. Доказать, что

$$\varphi(a)=\sum_{n=0}^{a-1}\prod_{p}\left(1-\frac{1}{p}\sum_{x=0}^{p-1}e^{2\pi i\frac{nx}{p}}\right),$$

где p пробегает простые делители числа a.
b. Из тождества вопроса a вывести извеетное выражение для $\varphi(a)$.
14. Доказать, что

$$\tau(a)=2\sum_{0<x<\sqrt{a}}\frac{1}{x}\sum_{k=0}^{x-1}e^{2\pi i\frac{ak}{x}}+\delta,$$

где $\delta=1$ или $\delta=0$, в зависимости от того, является ли a квадратом целого числа или нет.
15, a. Пусть p—простое и $h_1, h_2, \ldots, h_a$—целые. Доказать, что

$$(h_1+h_2+\ldots+h_a)^p\equiv h_1^p+h_2^p+\ldots+h_a^p\pmod p.$$

b. Из теоремы вопроса a вывести теорему Ферма.
c. Из теоремы Ферма вывести теорему Эйлера.

Численные примеры к главе III

1, a. Найти остаток от деления

$$(12371^{56}+34)^{28}\text{ на }111.$$

b. Делится ли на 1093^2 число $2^{1093}-2$?
2, a. Применяя признаки делимости вопроса 1, найти каноническое разложение числа 244943325.
b. Найти каноническое разложение числа 282321246671737.

Глава IV

СРАВНЕНИЯ С ОДНИМ НЕИЗВЕСТНЫМ

§ 1. Основные понятия

Нашей ближайшей задачей будет изучение сравнений такого общего вида:

$$f(x) \equiv 0 \pmod m; \quad f(x) = ax^n + a_1x^{n-1} + \ldots + a_n. \quad (1)$$

Если a не делится на m, то n называется *степенью сравнения*.

Решить сравнение — значит найти все значения x, ему удовлетворяющие. Два сравнения, которым удовлетворяют одни и те же значения x, называются равносильными.

Если сравнению (1) удовлетворяет какое-либо $x = x_1$, то (d, § 2, гл. III) тому же сравнению будут удовлетворять и все числа, сравнимые с x_1 по модулю m: $x \equiv x_1 \pmod m$. Весь этот класс чисел считается за *одно решение*. При таком соглашении *сравнение* (1) *будет иметь столько решений, сколько вычетов полной системы ему удовлетворяет*.

Пример. Сравнению

$$x^5 + x + 1 \equiv 0 \pmod 7$$

среди чисел 0, 1, 2, 3, 4, 5, 6 полной системы вычетов по модулю 7 удовлетворяют два числа: $x = 2$ и $x = 4$. Поэтому указанное сравнение имеет два решения:

$$x \equiv 2 \pmod 7, \quad x \equiv 4 \pmod 7.$$

§ 2. Сравнения первой степени

а. Сравнение первой степени перенесением свободного члена (с обратным знаком) в правую часть можно привести к виду

$$ax \equiv b \pmod m. \quad (1)$$

b. Приступая к исследованию вопроса о числе решений, мы сначала ограничим сравнение условием $(a, m) = 1$. Согласно § 1 наше сравнение имеет столько решений, сколько вычетов полной системы ему удовлетворяет. Но когда x пробегает полную систему вычетов по модулю m, то ax пробегает полную систему вычетов (d, § 4, гл. III). Следовательно, при одном и только одном значении x, взятом из полной системы, ax будет сравнимо с b. Итак, при $(a, m) = 1$ сравнение (1) имеет одно решение.

c. Пусть теперь $(a, m) = d > 1$. Тогда, чтобы сравнение (1) имело решения, необходимо (e, § 3, гл. III), чтобы b делилось на d, иначе сравнение (1) невозможно ни при каком целом x. Предполагая поэтому b кратным d, положим $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Тогда сравнение (1) будет равносильно такому (по сокращении на d): $a_1 x \equiv b_1 \pmod{m_1}$, в котором уже $(a_1, m_1) = 1$, и потому оно будет иметь одно решение по модулю m_1. Пусть x_1 — наименьший неотрицательный вычет этого решения по модулю m_1, тогда все числа x, образующие это решение, найдутся в виде

$$x \equiv x_1 \pmod{m_1}. \tag{2}$$

По модулю же m числа (2) образуют не одно решение, а больше, именно столько решений, сколько чисел (2) найдется в ряде $0, 1, 2, \ldots, m-1$ наименьших неотрицательных вычетов по модулю m. Но сюда попадут следующие числа (2):

$$x_1,\ x_1 + m_1,\ x_1 + 2m_1,\ \ldots,\ x_1 + (d-1)\, m_1,$$

т. е. всего d чисел (2); следовательно, сравнение (1) имеет d решений.

d. Собирая все доказанное, получаем теорему:

Пусть $(a, m) = d$. Сравнение $ax \equiv b \pmod{m}$ невозможно, если b не делится на d. При b, кратном d, сравнение имеет d решений.

e. Обращаясь к разысканию решений сравнения (1), мы укажем только способ, основанный на теории непрерывных дробей, причем достаточно ограничиться лишь случаем $(a, m) = 1$.

Разлагая в непрерывную дробь отношение $m:a$,

$$\frac{m}{a}=q_1+\cfrac{1}{q_2+\cfrac{1}{q_3+}}\cdots+\frac{1}{q_n}$$

и рассматривая две последние подходящие дроби:

$$\frac{P_{n-1}}{Q_{n-1}},\quad \frac{P_n}{Q_n}=\frac{m}{a},$$

согласно свойствам непрерывных дробей (d, § 6, гл. I) имеем

$$mQ_{n-1}-aP_{n-1}=(-1)^n,$$

$$aP_{n-1}\equiv(-1)^{n-1}\pmod m,$$

$$a\cdot(-1)^{n-1}P_{n-1}b\equiv b\pmod m.$$

Итак, наше сравнение имеет решение

$$x\equiv(-1)^{n-1}P_{n-1}b\pmod m,$$

для разыскания которого достаточно вычислить P_{n-1} согласно способу, указанному в с, § 6, гл. I.

Пример. Решим сравнение

$$111x=75\pmod{321}. \tag{3}$$

Здесь $(111, 321)=3$, причем 75 кратно 3. Поэтому сравнение имеет три решения.

Деля обе части сравнения и модуль на 3, получим сравнение

$$37x\equiv 25\pmod{107}, \tag{4}$$

которое нам следует сначала решить. Имеем

107	37				
74	2				
37	33				
33	1				
33	4				
32	8				
4	1				
4	4				

q		2	1	8	4
P_s	1	2	3	26	107

Значит, в данном случае $n=4$, $P_{n-1}=26$, $b=25$, и мы имеем решение сравнения (4) в виде

$$x \equiv -26 \cdot 25 \equiv 99 \pmod{107}.$$

Отсюда решения сравнения (3) представляются так:

$$x \equiv 99;\ 99+107;\ 99+2\cdot 107 \pmod{321},$$

т. е.

$$x \equiv 99;\ 206;\ 313 \pmod{321}.$$

§ 3. Система сравнений первой степени

a. Мы рассмотрим лишь простейшую систему сравнений

$$\begin{aligned} x &\equiv b_1 \pmod{m_1}, \\ x &\equiv b_2 \pmod{m_2}, \\ &\cdots\cdots\cdots \\ x &\equiv b_k \pmod{m_k} \end{aligned} \tag{1}$$

с одним неизвестным, но с разными и притом попарно простыми модулями.

b. Решить систему (1), т. е. найти все значения x, ей удовлетворяющие, можно, применяя следующую теорему:

Пусть числа M_s и M_s' определены из условий

$$m_1 m_2 \ldots m_k = M_s m_s, \quad M_s M_s' \equiv 1 \pmod{m_s}$$

и пусть

$$x_0 = M_1 M_1' b_1 + M_2 M_2' b_2 + \ldots + M_k M_k' b_k.$$

Тогда совокупность значений x, удовлетворяющих системе (1), *определяется сравнением*

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_k}. \tag{2}$$

Действительно, ввиду делимости на m_s всех M_j, отличных от M_s, при любом $s=1, 2, \ldots, k$ имеем

$$x_0 \equiv M_s M_s' b_s \equiv b_s \pmod{m_s},$$

и, следовательно, система (1) равносильна системе

$$x \equiv x_0 \pmod{m_1}, \quad x \equiv x_0 \pmod{m_2}, \quad \ldots, \quad x \equiv x_0 \pmod{m_k} \tag{3}$$

(т. е. системам (1) и (3) удовлетворяют одни и те же значения x). Системе же (3), ввиду теорем c и d § 3, гл. III, удовлетворяют те и только те значения x, которые удовлетворяют сравнению (2).

c. *Если $b_1, b_2, \ldots, b_k$ независимо друг от друга пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$, то x_0 пробегает полную систему вычетов по модулю $m_1 m_2 \ldots m_k$.*

Действительно, x_0 пробегает $m_1 m_2 \ldots m_k$ значений, ввиду d, § 3, гл. III, несравнимых по модулю $m_1 m_2 \ldots m_k$.

d. Пример. Решим систему

$$x \equiv b_1 \pmod 4, \quad x \equiv b_2 \pmod 5, \quad x \equiv b_3 \pmod 7.$$

Здесь $4 \cdot 5 \cdot 7 = 35 \cdot 4 = 28 \cdot 5 = 20 \cdot 7$, причем

$$35 \cdot 3 \equiv 1 \pmod 4, \quad 28 \cdot 2 \equiv 1 \pmod 5, \quad 20 \cdot 6 \equiv 1 \pmod 7.$$

Поэтому

$$x_0 = 35 \cdot 3b_1 + 28 \cdot 2b_2 + 20 \cdot 6b_3 = 105b_1 + 56b_2 + 120b_3$$

и, следовательно, совокупность значений x, удовлетворяющих системе, может быть представлена в виде

$$x \equiv 105b_1 + 56b_2 + 120b_3 \pmod{140}.$$

Так, например, совокупность значений x, удовлетворяющих системе

$$x \equiv 1 \pmod 4, \quad x \equiv 3 \pmod 5, \quad x \equiv 2 \pmod 7,$$

будет

$$x \equiv 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 \equiv 93 \pmod{140},$$

а совокупность значений x, удовлетворяющих системе

$$x \equiv 3 \pmod 4, \quad x \equiv 2 \pmod 5, \quad x \equiv 6 \pmod 7,$$

будет

$$x \equiv 105 \cdot 3 + 56 \cdot 2 + 120 \cdot 6 \equiv 27 \pmod{140}.$$

§ 4. Сравнения любой степени по простому модулю

a. Пусть p — простое. Докажем общие теоремы, относящиеся к сравнению вида

$$f(x) \equiv 0 \pmod p; \quad f(x) = ax^n + a_1 x^{n-1} + \ldots + a_n. \quad (1)$$

b. *Сравнение вида* (1) *равносильно сравнению степени не выше* $p - 1$.

Действительно, деля $f(x)$ на $x^p - x$, имеем

$$f(x) = (x^p - x)\,Q(x) + R(x),$$

где степень $R(x)$ не выше $p-1$. А так как $x^p - x \equiv 0 \pmod p$, то $f(x) \equiv R(x) \pmod p$, откуда и следует указанная теорема.

c. *Если сравнение* (1) *имеет более чем n решений, то все коэффициенты* $f(x)$ *кратны p.*

Действительно, пусть сравнение (1) имеет, по крайней мере, $n+1$ решение. Обозначая буквами $x_1, x_2, \ldots, x_n, x_{n+1}$ вычеты этих решений, мы можем $f(x)$ представить в виде

$$\begin{aligned} f(x) = {} & a(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1})(x-x_n) + \\ & + b(x-x_1)(x-x_2)\ldots(x-x_{n-2})(x-x_{n-1}) + \\ & + c(x-x_1)(x-x_2)\ldots(x-x_{n-2}) + \\ & + \ldots\ldots\ldots\ldots\ldots + \\ & + k(x-x_1)(x-x_2) + \\ & + l(x-x_1) + \\ & + m. \end{aligned} \tag{2}$$

Действительно, преобразовав раскрытием скобок произведения правой части в многочлены, мы b возьмем равным коэффициенту при x^{n-1} разности между $f(x)$ и первым многочленом, затем c возьмем равным коэффициенту при x^{n-2} разности между $f(x)$ и двумя первыми многочленами и т. д.

Полагая в (2) последовательно $x = x_1, x_2, \ldots, x_n, x_{n+1}$, убеждаемся в том, что все $m, l, k, \ldots, c, b, a$ кратны p. Значит, и все $a, a_1, \ldots, a_n$ кратны p (как суммы чисел, кратных p).

d. *При простом p справедливо сравнение (теорема Вильсона)*

$$1 \cdot 2 \ldots (p-1) + 1 \equiv 0 \pmod p. \tag{3}$$

Действительно, если $p = 2$, то теорема очевидна. Если же $p > 2$, то рассмотрим сравнение

$$(x-1)(x-2)\ldots(x-(p-1)) - (x^{p-1}-1) \equiv 0 \pmod p;$$

оно степени не выше $p-2$ и имеет $p-1$ решение, именно

решения с вычетами $1, 2, \ldots, p-1$. Следовательно, по теореме с все его коэффициенты кратны p; в частности, на p делится и свободный член, равный как раз левой части сравнения (3).

Пример. Имеем $1\cdot2\cdot3\cdot4\cdot5\cdot6+1=721=0 \pmod 7$.

§ 5. Сравнения любой степени по составному модулю

а. *Если* $m_1, m_2, \ldots, m_k$ *попарно простые, то сравнение*

$$f(x) \equiv 0 \pmod{m_1 m_2 \ldots m_k} \qquad (1)$$

равносильно системе

$$f(x) \equiv 0 \pmod{m_1},$$
$$f(x) \equiv 0 \pmod{m_2}, \ \ldots, \ f(x) \equiv 0 \pmod{m_k}.$$

При этом, обозначая через $T_1, T_2, \ldots, T_k$ *числа решений отдельных сравнений этой системы по соответственным модулям и через* T *— число решений сравнения* (1), *будем иметь*

$$T = T_1 T_2 \ldots T_k.$$

Действительно, первая часть теоремы следует из с и d, § 3, гл. III. Вторая часть следует из того, что каждое сравнение

$$f(x) \equiv 0 \pmod{m_s} \qquad (2)$$

выполняется тогда и только тогда, когда выполняется одно из T_s сравнений вида

$$x \equiv b_s \pmod{m_s},$$

где b_s пробегает вычеты решений сравнения (2), причем возможно всего $T_1 T_2 \ldots T_k$ различных комбинаций вида

$$x \equiv b_1 \pmod{m_1}, \ x \equiv b_2 \pmod{m_2}, \ \ldots, \ x \equiv b_k \pmod{m_k},$$

приводящих (с, § 3) к различным классам по модулю

$$m_1 m_2 \ldots m_k.$$

Пример. Сравнение

$$f(x) \equiv 0 \pmod{35}, \quad f(x) = x^4 + 2x^3 + 8x + 9 \qquad (3)$$

равносильно системе

$$f(x) \equiv 0 \pmod 5, \quad f(x) \equiv 0 \pmod 7.$$

Легко убедимся (§ 1), что первое сравнение этой системы имеет 2 решения: $x \equiv 1.\ 4 \pmod 5$, второе же сравнение имеет 3 решения: $x \equiv 3;\ 5;\ 6 \pmod 7$. Поэтому сравнение (3) имеет $2 \cdot 3 = 6$ решений. Чтобы найти эти 6 решений, надо решить 6 систем вида

$$x \equiv b_1 \pmod 5, \quad x \equiv b_2 \pmod 7, \tag{4}$$

которые получим, заставляя b_1 пробегать значения $b_1 = 1; 4$, а b_2 пробегать значения $b_2 = 3;\ 5;\ 6$. Но, ввиду

$$35 = 7 \cdot 5 = 5 \cdot 7, \quad 7 \cdot 3 \equiv 1 \pmod 5, \quad 5 \cdot 3 \equiv 1 \pmod 7,$$

совокупность значений x, удовлетворяющих системе (4), представится в виде (b, § 3)

$$x \equiv 21 b_1 + 15 b_2 \pmod{35}.$$

Поэтому решения сравнения (3) будут

$$x \equiv 31;\ 26;\ 6;\ 24;\ 19;\ 34 \pmod{35}.$$

b. Ввиду теоремы a исследование и решение сравнения

$$f(x) \equiv 0 \left(\mathrm{mod}\ p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}\right)$$

сводятся к исследованию и решению сравнений вида

$$f(x) \equiv 0 \pmod{p^\alpha}; \tag{5}$$

это же последнее сравнение сводится вообще, как мы сейчас выясним, к сравнению

$$f(x) \equiv 0 \pmod p. \tag{6}$$

Действительно, всякое x, удовлетворяющее сравнению (5), необходимо должно удовлетворять и сравнению (6). Пусть

$$x \equiv x_1 \pmod p$$

— какое-либо решение сравнения (6). Тогда $x = x_1 + pt_1$, где t_1 — целое. Вставляя это значение x в сравнение

$$f(x) \equiv 0 \pmod{p^2}$$

и разлагая левую часть по формуле Тейлора, найдем

(принимая во внимание, что $\frac{1}{k!}f^{(k)}(x_1)$ — целое, и отбрасывая члены, кратные p^2)

$$f(x_1)+pt_1f'(x_1)\equiv 0 \pmod{p^2},\quad \frac{f(x_1)}{p}+t_1f'(x_1)\equiv 0 \pmod{p}.$$

Ограничиваясь здесь случаем, когда $f'(x_1)$ не делится на p, имеем одно решение:

$$t_1\equiv t_1' \pmod{p};\quad t_1=t_1'+pt_2.$$

Выражение для x принимает вид

$$x=x_1+pt_1'+p^2t_2=x_2+p^2t_2;$$

вставляя его в сравнение

$$f(x)\equiv 0 \pmod{p^3},$$

получим

$$f(x_2)+p^2t_2f'(x_2)\equiv 0 \pmod{p^3},$$
$$\frac{f(x_2)}{p^2}+t_2f'(x_2)\equiv 0 \pmod{p}.$$

Здесь $f'(x_2)$ не делится на p, так как

$$x_2\equiv x_1 \pmod{p},$$
$$f'(x_2)\equiv f'(x_1) \pmod{p},$$

и потому последнее сравнение имеет одно решение:

$$t_2\equiv t_2' \pmod{p};$$
$$t_2\equiv t_2'+pt_3.$$

Выражение для x принимает вид

$$x=x_2+p^2t_2'+p^3t_3=x_3+p^3t_3;$$

и т. д. Таким путем по данному решению сравнения (6) постепенно найдем сравнимое с ним решение сравнения (5). Итак, *всякое решение* $x\equiv x_1 \pmod{p}$ *сравнения* (6) *при условии, что* $f'(x_1)$ *не делится на* p, *даст одно решение сравнения* (5):

$$x\equiv x_\alpha+p^\alpha t_\alpha;$$
$$x\equiv x_\alpha \pmod{p^\alpha}.$$

Пример. Решим сравнение

$$f(x)\equiv 0 \pmod{27};$$
$$f(x)=x^4+7x+4. \qquad (7)$$

Сравнение $f(x) \equiv 0 \pmod 3$ имеет одно решение $x \equiv 1 \pmod 3$; при этом $f'(1) \equiv 2 \pmod 3$ и, следовательно, не делится на 3.

Находим:

$$x = 1 + 3t_1,$$

$$f(1) + 3t_1 f'(1) \equiv 0 \pmod 9; \quad 3 + 3t_1 \cdot 2 \equiv 0 \pmod 9,$$

$$2t_1 + 1 \equiv 0 \pmod 3, \quad t_1 \equiv 1 \pmod 3, \quad t_1 = 1 + 3t_2,$$

$$x = 4 + 9t_2,$$

$$f(4) + 9t_2 f'(4) \equiv 0 \pmod{27}, \quad 18 + 9t_2 \cdot 2 \equiv 0 \pmod{27},$$

$$2t_2 + 2 \equiv 0 \pmod 3, \quad t_2 \equiv 2 \pmod 3, \quad t_2 = 2 + 3t_3,$$

$$x = 22 + 27t_3.$$

Таким образом сравнение (7) имеет одно решение

$$x \equiv 22 \pmod{27}.$$

Вопросы к главе IV

1, a. Пусть m—целое, $m > 0$, $f(x, \ldots, w)$—целая рациональная функция с целыми коэффициентами от r переменных $x, \ldots, w$ $(r \geqslant 1)$. Если сравнению

$$f(x, \ldots, w) \equiv 0 \pmod m \tag{1}$$

удовлетворяет система $x \equiv x_0, \ldots, w \equiv w_0$, то (обобщение определения § 1) систему классов чисел по модулю m:

$$x \equiv x_0 \pmod m, \quad \ldots, \quad w \equiv w_0 \pmod m$$

будем считать за одно решение сравнения (1).

Пусть T—число решений сравнения (1). Доказать, что

$$Tm = \sum_{a=0}^{m-1} \sum_{x=0}^{m-1} \cdots \sum_{w=0}^{m-1} e^{2\pi i \frac{af(x, \ldots, w)}{m}}.$$

b. При обозначениях вопроса a и вопроса 12, e, гл. III доказать, что

$$Tm = m^r \sum_{m_0 \setminus m} A(m_0).$$

c. Равенство вопроса a применить к доказательству теоремы о числе решений сравнения первой степени.

d. Пусть m—целое, $m > 0$; $a, \ldots, f, g$—целые, их число равно $r+1$ $(r > 0)$: $d = (a, \ldots, f, m)$; T—число решений сравнения

$$ax + \ldots + fw + g \equiv 0 \pmod m.$$

Пользуясь равенством вопроса **a**, доказать, что

$$r = \begin{cases} m^{r-1}d, & \text{если } g \text{ кратно } d, \\ 0 & \text{в противном случае.} \end{cases}$$

e. Теорему вопроса **d** доказать, исходя из теоремы о числе решений сравнения $ax \equiv b \pmod m$.

2, a. Пусть $m > 1$, $(a, m) = 1$. Доказать, что сравнение $ax \equiv b \pmod m$ имеет решение $x \equiv ba^{\varphi(m)-1} \pmod m$.

b. Пусть p—простое, $0 < a < p$. Доказать, что сравнение $ax \equiv b \pmod p$ имеет решение

$$x \equiv b(-1)^{a-1}\frac{(p-1)(p-2)\dots(p-a+1)}{1\cdot 2\dots a} \pmod p.$$

c, α) Указать возможно более простой способ решения сравнения вида

$$2^k x \equiv b \pmod m; \quad (2, m) = (2, b) = 1.$$

β) Указать возможно более простой способ решения сравнения

$$3^k x \equiv b \pmod m; \quad (3, m) = (3, b) = 1.$$

γ) Пусть $(a, m) = 1$, $1 < a < m$. Развивая способы, указанные в вопросах **α)** и **β)**, доказать, что разыскание решения сравнения $ax \equiv b \pmod m$ может быть приведено к разысканию решений сравнений вида $b + mt \equiv 0 \pmod p$, где p—простой делитель числа a.

3. Пусть m—целое, $m > 1$, $1 \leqslant \tau < m$, $(a, m) = 1$. Пользуясь теорией сравнений, доказать существование целых x и y с условиями

$$ax \equiv y \pmod m, \quad 0 < x \leqslant \tau, \quad 0 < |y| < \frac{m}{\tau}.$$

4, a. При $(a, m) = 1$ будем рассматривать символическую дробь $\frac{b}{a}$ по модулю m, обозначающую любой вычет решения сравнения $ax \equiv b \pmod m$. Доказать, что (сравнения берутся по модулю m):

α) При $a \equiv a_1$, $b \equiv b_1$ имеем $\frac{b}{a} \equiv \frac{b_1}{a_1}$.

β) Числитель b символической дроби $\frac{b}{a}$ можно заменить сравнимым b_0, кратным a. Тогда символическая дробь $\frac{b}{a}$ сравнима с целым числом, представляемым обычной дробью $\frac{b_0}{a}$.

γ) $\frac{b}{a} + \frac{d}{c} \equiv \frac{bc+ad}{ac}$.

δ) $\frac{b}{a} \cdot \frac{d}{c} \equiv \frac{bd}{ac}$.

b, α) Пусть p — простое, $p > 2$, a — целое, $0 < a < p-1$. Доказать, что

$$\binom{p-1}{a} \equiv (-1)^a \pmod{p}.$$

β) Пусть p — простое, $p > 2$. Доказать, что

$$\frac{2^{p-2}}{p} \equiv 1 - \frac{1}{2} + \frac{1}{3} - \ldots - \frac{1}{p-1} \pmod{p}.$$

5, a. Пусть d — делитель числа a, не делящийся на квадрат целого, превосходящего 1, и на простые, меньшие n, и $\varkappa$ — число различных простых делителей числа d. Доказать, что в ряде

$$1 \cdot 2 \ldots n, \quad 2 \cdot 3 \ldots (n+1), \quad \ldots, \quad a(a+1)\ldots(a+n-1) \qquad (1)$$

чисел, кратных d, будет $\frac{n^{\varkappa} a}{d}$.

b. Пусть $p_1, p_2, \ldots, p_k$ — различные простые делители числа a, причем ни один из них не меньше чем n. Доказать, что число чисел ряда (1), взаимно простых с a, будет

$$a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\ldots\left(1-\frac{n}{p_k}\right).$$

6. Пусть $m_{1,2,\ldots,k}$ — общее наименьшее кратное чисел $m_1, m_2, \ldots, m_k$

a. Пусть $d = (m_1, m_2)$. Доказать, что система

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}$$

разрешима тогда и только тогда, когда $b_2 - b_1$ кратно d, причем в случае разрешимости совокупность значений x, удовлетворяющих этой системе, определяется сравнением вида

$$x \equiv x_{1,2} \pmod{m_{1,2}}; \quad m_{1,2} = \frac{m_1 m_2}{d}.$$

b. Доказать, что в случае разрешимости системы

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad \ldots, \quad x \equiv b_k \pmod{m_k}$$

совокупность значений x, ей удовлетворяющих, определяется сравнением вида

$$x \equiv x_{1,2,\ldots,k} \pmod{m_{1,2,\ldots,k}}.$$

7. Пусть m — целое, $m > 1$, a и b — целые,

$$\left(\frac{a,b}{m}\right) = \sum_x e^{\frac{2\pi i}{m}\cdot\frac{ax+bx^2}{m}},$$

где x пробегает приведенную систему вычетов по модулю m, причем

$x' = \frac{1}{x} \pmod m$ (в смысле вопроса 4, а). Доказать следующие свойства символа $\left(\frac{a, b}{m}\right)$:

α) $\left(\frac{a, b}{m}\right)$ — вещественное.

β) $\left(\frac{a, b}{m}\right) = \left(\frac{b, a}{m}\right)$.

γ) При $(h, m) = 1$ имеем $\left(\frac{a, bh}{m}\right) = \left(\frac{ah, b}{m}\right)$.

δ) При $m_1, m_2, \ldots, m_k$ попарно простых, полагая $m_1 m_2 \ldots m_k = m$, $m = M_s m_s$, имеем

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right)\cdots\left(\frac{a_k, 1}{m_k}\right) = \left(\frac{M_1^2 a_1 + M_2^2 a_2 + \ldots + M_k^2 a_k, 1}{m}\right).$$

8. Пусть сравнение

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0 \pmod p$$

имеет n решений $x \equiv x_1, x_2, \ldots, x_n \pmod p$.

Доказать, что

$$\begin{aligned} a_1 &\equiv -a_0 S_1 \pmod p, \\ a_2 &\equiv a_0 S_2 \pmod p, \\ a_3 &\equiv -a_0 S_3 \pmod p, \\ &\ldots\ldots\ldots \\ a_n &\equiv (-1)^n a_0 S_n \pmod p, \end{aligned}$$

где S_1 есть сумма всех x_s, S_2 — сумма произведений по два, S_3 — сумма произведений по три и т. д.

9, а. Доказать теорему Вильсона, рассматривая пары x, x' чисел ряда 2, 3, ..., $p-2$, удовлетворяющие условию $xx' \equiv 1 \pmod p$.

b. Пусть P — целое, $P > 1$, $1 \cdot 2 \ldots (P-1) + 1 = 0 \pmod P$. Доказать, что P — простое.

10, а. Пусть $(a_0, m) = 1$. Указать сравнение n-й степени со старшим коэффициентом 1, равносильное сравнению

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0 \pmod m.$$

b. Доказать, что необходимое и достаточное условие того, что сравнение $f(x) = 0 \pmod p$; $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n$; $n \leqslant p$, имеет n решений, есть делимость на p всех коэффициентов остатка от деления $x^p - x$ на $f(x)$.

c. Пусть n — делитель $p-1$, $n > 1$, $(A, p) = 1$. Доказать, что необходимое и достаточное условие разрешимости сравнения $x^n \equiv A \pmod p$ есть $A^{\frac{p-1}{n}} \equiv 1 \pmod p$, причем в случае разрешимости указанное сравнение имеет n решений.

11. Пусть n — целое, $n > 0$ $(A, m) = 1$, и известно одно решение $x = x_0 \pmod m$ сравнения $x^n = A \pmod m$. Доказать, что все решения этого сравнения представятся произведением x_0 на вычеты решений сравнения $y^n \equiv 1 \pmod m$.

Численные примеры к главе IV

1, a. Решить сравнение $256x \equiv 179 \pmod{337}$.

b. Решить сравнение $1215x \equiv 560 \pmod{2755}$.

2, a. Сравнения примеров **1, a** и **1, b** решить по способу вопроса **2, c.**

b. Сравнение $1296x \equiv 1105 \pmod{2413}$ решить по способу вопроса **2, c.**

3. Найти все пары x, y, удовлетворяющие неопределенному уравнению $47x - 111y = 89$.

4, a. Указать общее решение для системы

$$x \equiv b_1 \pmod{13}, \quad x \equiv b_2 \pmod{17}.$$

Пользуясь этим общим решением, далее найти три числа, которые при делении на 13 и 17 давали бы соответственно остатки 1 и 12, 6 и 8, 11 и 4.

b. Указать общее решение для системы

$$x \equiv b_1 \pmod{25}, \quad x \equiv b_2 \pmod{27}, \quad x \equiv b_3 \pmod{59}.$$

5, a. Решить систему сравнений (вопрос **6, a**)

$$x \equiv 3 \pmod 8, \quad x \equiv 11 \pmod{20}, \quad x \equiv 1 \pmod{15}.$$

b. Решить систему сравнений

$$x \equiv 1 \pmod 3, \quad x \equiv 4 \pmod 5, \quad x \equiv 2 \pmod 7,$$
$$x \equiv 9 \pmod{11}, \quad x \equiv 3 \pmod{13}.$$

6. Решить систему сравнений

$$3x + 4y - 29 \equiv 0 \pmod{143}, \quad 2x - 9y + 84 \equiv 0 \pmod{143}.$$

7, a. Какому сравнению степени ниже 5 равносильно сравнение $3x^{14} + 4x^{13} + 3x^{12} + 2x^{11} + x^9 + 2x^8 + 4x^7 + x^6 + 3x^4 + x^3 + 4x^2 + 2x \equiv 0 \pmod 5$?

b. Какому сравнению степени ниже 7 равносильно сравнение $2x^{17} + 6x^{16} + x^{15} + 5x^{12} + 3x^{11} + 2x^{10} + x^9 + 5x^5 + 2x^7 + 3x^5 + 4x^3 + 6x^3 + 4x^2 + x + 4 \equiv 0 \pmod 7$?

8. Какому сравнению со старшим коэффициентом 1 равносильно сравнение (вопрос **10, a**)

$$70x^6 + 78x^5 + 25x^4 + 68x^3 + 52x^2 + 4x + 3 \equiv 0 \pmod{101}?$$

9, a. Решить сравнение

$$f(x) \equiv 0 \pmod{27}, \quad f(x) = 7x^4 + 19x + 25,$$

найдя сначала с помощью проб все решения сравнения

$$f(x) \equiv 0 \pmod 3.$$

b. Решить сравнение $9x^2 + 29x + 62 \equiv 0 \pmod{64}$.

10, a. Решить сравнение $x^3 + 2x + 2 \equiv 0 \pmod{125}$.

b. Решить сравнение $x^4 + 4x^3 + 2x^2 + 2x + 12 \equiv 0 \pmod{625}$.

11, a. Решить сравнение $6x^3 + 27x^2 + 17x + 20 \equiv \pmod{30}$.

b. Решить сравнение $31x^4 + 57x^3 + 96x + 191 \equiv 0 \pmod{225}$.

Глава V

СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ

§ 1. Общие теоремы

a. Из сравнений степени $n > 1$ в дальнейшем будут рассматриваться лишь простейшие, а именно — *двучленные сравнения*:

$$x^n \equiv a \pmod{m}; \quad (a, m) = 1. \tag{1}$$

Если сравнение (1) имеет решения, то a называется *вычетом степени n по модулю m*. В противном случае a называется *невычетом степени n по модулю m*. В частности, при $n = 2$ вычеты или невычеты называются *квадратичными*, при $n = 3$ — *кубическими*, при $n = 4$ — *биквадратичными*.

b. В этой главе мы подробно рассмотрим случай $n = 2$ и в первую очередь рассмотрим двучленные сравнения второй степени по простому нечетному модулю p:

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1. \tag{2}$$

c. *Если a — квадратичный вычет по модулю p, то сравнение (2) имеет два решения.*

Действительно, если a — квадратичный вычет, то сравнение (2) имеет, по крайней мере, одно решение $x \equiv x_1 \pmod{p}$. Но тогда, ввиду $(-x_1)^2 = x_1^2$, то же сравнение имеет и второе решение $x \equiv -x_1 \pmod{p}$. Это второе решение отлично от первого, так как из $x_1 \equiv -x_1 \pmod{p}$ мы имели бы $2x_1 \equiv 0 \pmod{p}$, что невозможно, ввиду $(2, p) = (x_1, p) = 1$.

Указанными двумя решениями и исчерпываются все решения сравнения (2), так как последнее, будучи сравнением второй степени, более двух решений иметь не может (с, § 4, гл. IV).

d. *Приведенная система вычетов по модулю p состоит из* $\frac{p-1}{2}$ *квадратичных вычетов, сравнимых с числами*

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2, \tag{3}$$

и $\frac{p-1}{2}$ *квадратичных невычетов.*

Действительно, среди вычетов приведенной системы по модулю p квадратичными вычетами являются те и и только те, которые сравнимы с квадратами чисел (приведенная система вычетов)

$$-\frac{p-1}{2},\ \ldots,\ -2,\ -1,\ 1,\ 2,\ \ldots,\ \frac{p-1}{2}; \tag{4}$$

т. е. с числами (3). При этом числа (3) по модулю p не сравнимы, так как из $k^2 \equiv l^2 \pmod p$, $0 < k < l \leqslant \frac{p-1}{2}$, следовало бы, что сравнению $x^2 \equiv l^2 \pmod p$, вопреки c, среди чисел (4) удовлетворяют четыре: $x = -l,\ -k,\ k,\ l$.

§ 2. Символ Лежандра

a. Введем в рассмотрение *символ Лежандра* $\left(\frac{a}{p}\right)$ (читается: символ a по p; a называется числителем, p — знаменателем символа). Этот символ определяется для всех a, не делящихся на p. Он задается равенством $\left(\frac{a}{p}\right) = 1$, если a — квадратичный вычет по модулю p, и равенством $\left(\frac{a}{p}\right) = -1$, если a — квадратичный невычет по модулю p.

b. Вычислить символ $\left(\frac{a}{p}\right)$ (и таким путем определить, является a квадратичным вычетом или же квадратичным невычетом по модулю p) позволяет следующая теорема (*критерий Эйлера*).

При a, не делящемся на p, имеем

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Действительно, по теореме Ферма

$$a^{p-1} \equiv 1 \pmod p,\quad \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Один и только один из сомножителей левой части последнего сравнения делится на p (оба сомножителя не могут одновременно делиться на p, в противном случае их разность 2 должна была бы делиться на p). Поэтому имеет место одно и только одно из сравнений

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{1}$$

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{2}$$

Но всякий квадратичный вычет a удовлетворяет при некотором x сравнению $a \equiv x^2 \pmod{p}$ и, следовательно, также получаемому из него почленным возведением в степень $\frac{p-1}{2}$ сравнению (1). При этом квадратичными вычетами и исчерпываются все решения сравнения (1), так как, будучи сравнением степени $\frac{p-1}{2}$, оно не может иметь более чем $\frac{p-1}{2}$ решений.

Поэтому квадратичные невычеты удовлетворяют сравнению (2).

Пример 1. Имеем

$$5^{14} \equiv 1 \pmod{29}.$$

Поэтому $\left(\frac{5}{29}\right) = 1$ и 5 — квадратичный вычет по модулю 29 (сравнение $x^2 \equiv 5 \pmod{29}$ имеет два решения).

Пример 2. Имеем

$$3^{14} \equiv -1 \pmod{29}.$$

Поэтому $\left(\frac{3}{29}\right) = -1$ и 3 — квадратичный невычет по модулю 29 (сравнение $x^2 \equiv 3 \pmod{29}$ не имеет решений).

Далее мы выведем важнейшие свойства символа $\left(\frac{a}{p}\right)$.

с. *Если* $a \equiv a_1 \pmod{p}$, *то* $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.

Это свойство следует из того, что числа одного и того же класса будут одновременно квадратичными вычетами или невычетами.

d. $\left(\frac{1}{p}\right)=1$.

Действительно, $1=1^2$ и, следовательно, 1 — квадратичный вычет.

e. $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Это свойство следует из b при $a=-1$.

Так как $\frac{p-1}{2}$ — четное, если p вида $4m+1$, и нечетное, если p вида $4m+3$, то отсюда следует, что -1 является квадратичным вычетом по модулю p, если p вида $4m+1$, и является квадратичным невычетом по модулю p, если p вида $4m+3$.

f. $\left(\frac{ab\ldots l}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{l}{p}\right)$.

Действительно, имеем

$$\left(\frac{ab\ldots l}{p}\right)\equiv(ab\ldots l)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\ldots l^{\frac{p-1}{2}}\equiv$$
$$\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{l}{p}\right)\pmod p,$$

откуда и вытекает наше утверждение. Отсюда следствие:

$$\left(\frac{ab^2}{p}\right)=\left(\frac{a}{p}\right),$$

т. е. в числителе символа можно отбросить любой квадратичный множитель.

g. Чтобы вывести дальнейшие свойства символа Лежандра, мы сначала докажем некоторую вспомогательную формулу. Полагая $p_1=\frac{p-1}{2}$, рассмотрим сравнения

$$\begin{aligned}
a\cdot 1&\equiv\varepsilon_1 r_1\pmod p,\\
a\cdot 2&\equiv\varepsilon_2 r_2\pmod p,\\
&\ldots\ldots\ldots\ldots\\
a\cdot p_1&\equiv\varepsilon_{p_1} r_{p_1}\pmod p,
\end{aligned}\tag{3}$$

где $\varepsilon_x r_x$ — абсолютно наименьший вычет ax, r_x — его модуль, так что $\varepsilon_x=\pm 1$.

Числа $a\cdot 1$, $-a\cdot 1$, $a\cdot 2$, $-a\ 2$, ... $a\cdot p_1$, $-a\ p_1$ образуют приведенную систему вычетов по модулю p (c, § 5, гл. III); их абсолютно наименьшие вычеты суть $\varepsilon_1 r_1$, $-\varepsilon_1 r_1$, $\varepsilon_2 r_2$, $-\varepsilon_2 r_2$, ..., $\varepsilon_{p_1} r_{p_1}$, $-\varepsilon_{p_1} r_{p_1}$. Положительные из последних, т. е. $r_1, r_2, \ldots, r_{p_1}$, должны совпадать с числами 1, 2, ..., p_1 (b, § 4, гл. III).

Перемножая теперь сравнения (3) и сокращая на

$$1\cdot 2 \ldots p_1 = r_1 r_2 \ldots r_{p_1},$$

получим $a^{\frac{p-1}{2}} = \varepsilon_1\varepsilon_2 \ldots \varepsilon_{p_1} \pmod p$, откуда (b) имеем

$$\left(\frac{a}{p}\right) = \varepsilon_1\varepsilon_2 \ldots \varepsilon_{p_1}. \tag{4}$$

Далее находим

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right],$$

что будет четным или нечетным, в зависимости от того, будет ли наименьший неотрицательный вычет числа ax меньше или больше $\frac{1}{2}p$, т. е. будет ли $\varepsilon_x = 1$ или $\varepsilon_x = -1$. Отсюда, очевидно,

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]},$$

и потому из (4) находим

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1}\left[\frac{2ax}{p}\right]}.$$

Предполагая a нечетным, преобразуем последнее равенство. Имеем ($a+p$ — четное)

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) =$$

$$= (-1)^{\sum_{x=1}^{p_1}\left[\frac{(a+p)x}{p}\right]} = (-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x},$$

откуда

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]+\frac{p^2-1}{8}} \tag{5}$$

Формула (5) и есть та, которую мы имели в виду доказать. Она позволит нам вывести еще два важнейших свойства символа Лежандра.

h. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

Следует из формулы (5) при $a=1$.

Но p можно представить в виде $p=8m+s$, где s—одно из чисел 1, 3, 5, 7. При этом $\frac{(8m+s)^2-1}{8}=8m^2+2ms+\frac{s^2-1}{8}$, что будет четным при $s=1$ и при $s=7$ и будет нечетным при $s=3$ и $s=5$. Поэтому 2 будет квадратичным вычетом по модулю p, если p вида $8m+1$ или вида $8m+7$, и будет квадратичным невычетом по модулю p, если p вида $8m+3$ или вида $8m+5$.

i. *Если p и q—простые нечетные, то* (*закон взаимности квадратичных вычетов*)

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

Так как $\frac{p-1}{2}\cdot\frac{q-1}{2}$ будет нечетным лишь в случае, когда оба числа p и q будут вида $4m+3$, и четным, если хоть одно из этих чисел будет вида $4m+1$, то указанное свойство можно формулировать так:

Если оба числа p и q вида $4m+3$, то

$$\left(\frac{q}{p}\right)=-\left(\frac{p}{q}\right);$$

если же хоть одно из них вида $4m+1$, то

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right).$$

Для доказательства заметим, что ввиду h формула (5) принимает вид

$$\left(\frac{a}{p}\right)=(-1)^{\sum_{x=1}^{p_1}\left[\frac{ax}{p}\right]} \tag{6}$$

Полагая теперь $\frac{q-1}{2}=q_1$, рассмотрим p_1q_1 пар чисел, получаемых, когда в выражениях qx, py числа x и y независимо друг от друга пробегают системы значений

$$x=1,\ 2,\ \ldots,\ p_1,\quad y=1,\ 2,\ \ldots,\ q_1.$$

Никогда не может быть $qx=py$, потому что из этого равенства следовало бы, что py кратно q, что ввиду $(p,\ q)=(y,\ q)=1$ (так как $0<y<q$) невозможно. Поэтому мы можем положить $p_1q_1=S_1+S_2$, где S_1—число пар с $qx<py$ и S_2—число пар с $py<qx$.

Очевидно, S_1 есть также число пар с $x<\frac{p}{q}y$ (этому не противоречит неравенство $x\leqslant p_1$, так как из $\frac{p}{q}y<\frac{p}{2}$ следует $\left[\frac{p}{q}y\right]\leqslant\left[\frac{p}{2}\right]=p_1$). Поэтому

$$S_1=\sum_{y=1}^{q_1}\left[\frac{p}{q}y\right].$$

Аналогичным путем убедимся, что

$$S_2=\sum_{x=1}^{p_1}\left[\frac{q}{p}x\right].$$

Но тогда равенство (6) дает нам

$$\left(\frac{p}{q}\right)=(-1)^{S_1},\quad \left(\frac{q}{p}\right)=(-1)^{S_2},$$

поэтому

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{S_1+S_2}=(-1)^{p_1q_1},$$

откуда и следует отмеченное свойство.

§ 3. Символ Якоби

a. Полезным обобщением символа Лежандра является *символ Якоби*. Пусть P — нечетное, большее единицы, и $P = p_1 p_2 \dots p_r$ — разложение его на простые сомножители (среди них могут быть и равные). Пусть, далее, $(a, P) = 1$. Тогда символ Якобн $\left(\frac{a}{P}\right)$ определяется равенством

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right).$$

Известные свойства символа Лежандра дают возможность установить аналогичные свойства и для символа Якоби.

b. *Если* $a \equiv a_1 \pmod P$, *то* $\left(\frac{a}{P}\right) = \left(\frac{a_1}{P}\right)$.

Действительно,

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_r}\right) = \left(\frac{a_1}{p_1}\right)\left(\frac{a_1}{p_2}\right)\dots\left(\frac{a_1}{p_r}\right) = \left(\frac{a_1}{P}\right),$$

потому что a, будучи сравнимо с a_1 по модулю P, будет сравнимо с a_1 и по модулям p_1, p_2, ..., p_r, которые являются делителями P.

c. $\left(\frac{1}{P}\right) = 1$.

В самом деле,

$$\left(\frac{1}{P}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_2}\right)\dots\left(\frac{1}{p_r}\right) = 1.$$

d. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$.

Чтобы убедиться в этом, заметим, что

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\dots\left(\frac{-1}{p_r}\right) = (-1)^{\frac{p_1-1}{2}+\frac{p_2-1}{2}+\dots+\frac{p_r-1}{2}}; \tag{1}$$

но

$$\frac{P-1}{2} = \frac{p_1 p_2 \dots p_r - 1}{2} =$$

$$= \frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_2-1}{2}\right)\dots\left(1+2\frac{p_r-1}{2}\right)-1}{2} =$$

$$= \frac{p_1-1}{2} + \frac{p_2-1}{2} + \dots + \frac{p_r-1}{2} + 2N,$$

ввиду чего из формулы (1) выводим

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}.$$

e. $\left(\frac{ab\ldots l}{P}\right)=\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)\ldots\left(\frac{l}{P}\right)$.

Действительно,

$$\left(\frac{ab\ldots l}{P}\right)=\left(\frac{ab\ldots l}{p_1}\right)\ldots\left(\frac{ab\ldots l}{p_r}\right)=$$
$$=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\ldots\left(\frac{l}{p_1}\right)\ldots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\ldots\left(\frac{l}{p_r}\right);$$

собирая символы с одинаковыми числителями, мы и получим утверждаемое свойство. Отсюда следствие:

$$\left(\frac{ab^2}{P}\right)=\left(\frac{a}{P}\right).$$

f. $\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}$

Действительно,

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\ldots\left(\frac{2}{p_r}\right)=(-1)^{\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_r^2-1}{8}}; \tag{2}$$

но

$$\frac{P^2-1}{8}=\frac{p_1^2p_2^2\ldots p_r^2-1}{8}=$$
$$=\frac{\left(1+8\frac{p_1^2-1}{8}\right)\left(1+8\frac{p_2^2-1}{8}\right)\ldots\left(1+8\frac{p_r^2-1}{8}\right)-1}{8}=$$
$$=\frac{p_1^2-1}{8}+\frac{p_2^2-1}{8}+\ldots+\frac{p_r^2-1}{8}+2N,$$

ввиду чего из формулы (2) выводим

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

g. *Если P и Q — положительные нечетные взаимно простые, то*

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Действительно, пусть $Q = q_1 q_2 \dots q_s$ есть разложение Q на простые сомножители (среди них опять-таки могут быть равные). Имеем

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\dots\left(\frac{Q}{p_r}\right) = \prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{q_\beta}{p_\alpha}\right) =$$

$$= (-1)^{\sum_{\alpha=1}^{r}\sum_{\beta=1}^{s}\frac{p_\alpha-1}{2}\cdot\frac{q_\beta-1}{2}} \prod_{\alpha=1}^{r}\prod_{\beta=1}^{s}\left(\frac{p_\alpha}{q_\beta}\right) =$$

$$= (-1)^{\left(\sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2}\right)\left(\sum_{\beta=1}^{s}\frac{q_\beta-1}{2}\right)}\left(\frac{P}{Q}\right).$$

Но, подобно тому, как в **d**, находим

$$\frac{P-1}{2} = \sum_{\alpha=1}^{r}\frac{p_\alpha-1}{2} + 2N, \quad \frac{Q-1}{2} = \sum_{\beta=1}^{s}\frac{q_\beta-1}{2} + 2N_1,$$

ввиду чего последняя формула дает

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

h. Рассматривая символ Лежандра как частный случай символа Якоби и пользуясь свойствами последнего, можно вычислить символ Лежандра быстрее, чем с помощью теоремы **b**, § 2.

Пример. Узнаем, сколько решений имеет сравнение

$$x^2 \equiv 219 \pmod{383}.$$

Имеем (применяя последовательно свойства **g**, **b**, следствие **e**, **g**, **b**, **e**, **f**, **g**, **b**, **d**):

$$\left(\frac{219}{383}\right) = -\left(\frac{383}{219}\right) = -\left(\frac{164}{219}\right) = -\left(\frac{41}{219}\right) =$$

$$= -\left(\frac{219}{41}\right) = -\left(\frac{14}{41}\right) = -\left(\frac{2}{41}\right)\left(\frac{7}{41}\right) =$$

$$= -\left(\frac{7}{41}\right) = -\left(\frac{41}{7}\right) = -\left(\frac{-1}{7}\right) = 1;$$

следовательно, рассмотренное сравнение имеет два решения.

§ 4. Случай составного модуля

a. Двучленные сравнения второй степени по составному модулю исследуются и решаются согласно общим указаниям § 5, гл. IV.

b. Сначала рассмотрим сравнение

$$x^2 \equiv a \pmod{p^\alpha}; \quad a > 0, \quad (a, p) = 1, \tag{1}$$

где p — простое нечетное.

Полагая $f(x) = x^2 - a$, будем иметь $f'(x) = 2x$, и если $x \equiv x_1 \pmod{p}$ есть решение сравнения

$$x^2 \equiv a \pmod{p}, \tag{2}$$

то ввиду $(a, p) = 1$ также $(x_1, p) = 1$, а так как p — нечетное, то $(2x_1, p) = 1$, т. е. $f'(x_1)$ не делится на p. Поэтому к разысканию решений сравнения (1) можно применить рассуждения b, § 5, гл. IV, причем каждое решение сравнения (2) даст одно решение сравнения (1). Из сказанного выводим, что

Сравнение (1) *имеет два решения или же ни одного, в зависимости от того, будет ли число a квадратичным вычетом или же невычетом по модулю p.*

c. Далее рассмотрим сравнение

$$x^2 \equiv a \pmod{2^\alpha}; \quad \alpha > 0, \quad (a, 2) = 1. \tag{3}$$

Здесь $f'(x_1) = 2x_1$ делится на 2, и потому рассуждения b, § 5, гл. IV неприменимы; они должны быть видоизменены следующим образом:

d. Если сравнение (3) разрешимо, то ввиду $(a, 2) = 1$ имеем $(x, 2) = 1$; следовательно (h, § 2), $x^2 - 1$ делится на 8. Поэтому, приводя сравнение (3) к виду

$$(x^2 - 1) + 1 \equiv a \pmod{2^\alpha},$$

убеждаемся, что для разрешимости этого сравнения необходимо

$$a \equiv 1 \pmod 4 \quad \text{при} \quad \alpha = 2; \quad a = 1 \pmod 8 \quad \text{при} \quad \alpha \geqslant 3. \tag{4}$$

e. В случаях, когда условия (4) не нарушены, рассмотрим вопрос о разыскании решений и их числе.

Для случаев $\alpha \leqslant 3$ ввиду d сравнению удовлетворяют все нечетные числа. Поэтому сравнение $x^\alpha \equiv a \pmod 2$

имеет одно решение: $x \equiv 1 \pmod 2$, сравнение $x^2 \equiv a \pmod 4$ имеет два решения: $x \equiv 1; 3 \pmod 4$, сравнение $x^2 \equiv a \pmod 8$ имеет четыре решения: $x \equiv 1; 3; 5; 7 \pmod 8$.

Для рассмотрения случаев $\alpha = 4, 5, \ldots$ все нечетные числа полезно объединить в две арифметические прогрессии:

$$x = \pm (1 + 4t_3) \tag{5}$$

$(1 + 4t_3 \equiv 1 \pmod 4); \quad -1 - 4t_3 \equiv -1 \equiv 3 \pmod 4)$.

Посмотрим, какие из чисел (5) удовлетворяют сравнению $x^2 \equiv a \pmod{16}$. Находим

$$(1 + 4t_3)^2 \equiv a \pmod{16}, \quad t_3 \equiv \frac{a-1}{8} \pmod 2,$$

$$t_3 = t_3' + 2t_4,$$

$$x = \pm (1 + 4t_3' + 8t_4) = \pm (x_4 + 8t_4).$$

Посмотрим, какие из последних чисел удовлетворяют сравнению $x^2 \equiv a \pmod{32}$. Находим

$(x_4 + 8t_4)^2 \equiv a \pmod{32}$, $t_4 = t_4' + 2t_5$, $x = \pm (x_5 + 16t_5)$,

и т. д. Таким путем убедимся, что при любом $\alpha > 3$ значения x, удовлетворяющие сравнению (3), представятся в виде

$$x = \pm (x_\alpha + 2^{\alpha-1} t_\alpha).$$

Эти значения x образуют четыре различных решения сравнения (3)

$$x \equiv x_\alpha; \; x_\alpha + 2^{\alpha-1}; \; -x_\alpha; \; -x_\alpha - 2^{\alpha-1} \pmod{2^\alpha}$$

(по модулю 4 два первых сравнимы с 1, а два последних сравнимы с -1).

Пример. Сравнение

$$x^2 \equiv 57 \pmod{64} \tag{6}$$

ввиду $57 \equiv 1 \pmod 8$ имеет четыре решения. Представляя x в виде $x = \pm (1 + 4t_3)$, находим

$$(1 + 4t_3)^2 \equiv 57 \pmod{16}, \quad 8t_3 \equiv 56 \pmod{16},$$
$$t_3 \equiv 1 \pmod 2, \quad t_3 = 1 + 2t_4, \quad x = \pm (5 + 8t_4),$$
$$(5 + 8t_4)^2 \equiv 57 \pmod{32}, \quad 5 \cdot 16 t_4 \equiv 32 \pmod{32},$$
$$t_4 \equiv 0 \pmod 2, \quad t_4 = 2t_5, \quad x = \pm (5 + 16 t_5),$$
$$(5 + 16t_5)^2 \equiv 57 \pmod{64}, \quad 5 \cdot 32 t_5 \equiv 32 \pmod{64},$$
$$t_5 \equiv 1 \pmod 2, \quad t_5 = 1 + 2t_6, \quad x = \pm (21 + 32t_6).$$

Поэтому решения сравнения (6) будут:

$$x \equiv \pm 21; \quad \pm 53 \pmod{64}.$$

f. Из **c**, **d** и **e** следует:
Для сравнения

$$x^2 \equiv a \pmod{2^\alpha}; \quad (a, 2) = 1$$

необходимыми условиями разрешимости будут: $a \equiv 1 \pmod 4$ *при* $\alpha = 2$, $a \equiv 1 \pmod 8$ *при* $\alpha \geqslant 3$. *Если эти условия не нарушены, число решений будет:* 1 *при* $\alpha = 1$; 2 *при* $\alpha = 2$; 4 *при* $\alpha \geqslant 3$.

g. Из **b**, **f** и из **a**, § 5, гл. IV следует:
Для сравнения общего вида

$$x^2 \equiv a \pmod m; \quad m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}; \quad (a, m) = 1$$

необходимыми условиями разрешимости будут:

$$a \equiv 1 \pmod 4 \quad \text{при} \quad \alpha = 2, \quad a \equiv 1 \pmod 8 \text{ при } \alpha \geqslant 3,$$

$$\left(\frac{a}{p_1}\right) = 1, \quad \left(\frac{a}{p_2}\right) = 1, \quad \dots, \quad \left(\frac{a}{p_k}\right) = 1.$$

Если ни одно из этих условий не нарушено, число решений будет: 2^k *при* $\alpha = 0$ *и при* $\alpha = 1$; 2^{k+1} *при* $\alpha = 2$; 2^{k+2} *при* $\alpha \geqslant 3$.

Вопросы к главе V

Буквою p здесь всегда обозначаем простое нечетное число.

1. Доказать, что разыскание решений сравнения вида

$$ax^2 + bx + c \equiv 0 \pmod m, \quad (2a, m) = 1$$

сводится к разысканию решений сравнения вида $x^2 \equiv q \pmod m$.

2, a. Пользуясь **b**, § 2, найти решения сравнения (в случае его возможности)

$$x^2 \equiv a \pmod p; \quad p = 4m + 3.$$

b. Пользуясь **b** и **h**, § 2, указать способ разыскания решений сравнений вида

$$x^2 \equiv a \pmod p; \quad p = 8m + 5.$$

c. Указать возможно более простой способ разыскания решений сравнений вида

$$x^2 \equiv a \pmod p; \quad p = 8m + 1$$

в случае, когда известен некоторый квадратичный невычет N по модулю p.

d. Пользуясь теоремой Вильсона, доказать, что решения сравнения

$$x^2+1 \equiv 0 \pmod{p}; \quad p=4m+1$$

будут

$$x \equiv \pm 1\cdot 2 \ldots 2m \pmod{p}.$$

3, a. Доказать, что сравнение

$$x^2+1 \equiv 0 \pmod{p} \tag{1}$$

разрешимо тогда и только тогда, когда p имеет вид $4m+1$; сравнение

$$x^2+2 \equiv 0 \pmod{p} \tag{2}$$

разрешимо тогда и только тогда, когда p имеет вид $8m+1$ или $8m+3$, сравнение

$$x^2+3 \equiv 0 \pmod{p} \tag{3}$$

разрешимо тогда и только тогда, когда p имеет вид $6m+1$.

b. Доказать бесконечность числа простых чисел вида $4m+1$.

c. Доказать бесконечность числа простых чисел вида $6m+1$.

4. Пусть, разбивая числа $1, 2, \ldots, p-1$ на две совокупности, вторая из которых содержит не менее одного числа, имеем: произведение двух чисел одной совокупности сравнимо по модулю p с числом первой совокупности, а произведение двух чисел различных совокупностей сравнимо по модулю p с числом второй совокупности. Доказать, что это будет тогда и только тогда, когда первая совокупность состоит из квадратичных вычетов, а вторая — из квадратичных невычетов по модулю p.

5, a. Вывести теорию сравнений вида

$$x^2 \equiv a \pmod{p^\alpha}; \quad (a, p)=1,$$

представляя a и x в системе исчисления с основанием p.

b. Вывести теорию сравнений вида

$$x^2 \equiv a \pmod{2^\alpha}; \quad (a, 2)=1,$$

представляя a и x в системе исчисления с основанием 2.

6. Доказать, что решения сравнения

$$x^2 \equiv a \pmod{p^\alpha}; \quad (a, p)=1$$

будут $x \equiv \pm PQ' \pmod{p^\alpha}$, где

$$P=\frac{(z+\sqrt{a})^\alpha+(z-\sqrt{a})^\alpha}{2},$$

$$Q=\frac{(z+\sqrt{a})^\alpha-(z-\sqrt{a})^\alpha}{2\sqrt{a}},$$

$$z^2 \equiv a \pmod{p}, \quad QQ' \equiv 1 \pmod{p^\alpha}.$$

7. Указать способ решения сравнения $x^2 \equiv 1 \pmod{m}$, основанный на том обстоятельстве, что указанное сравнение равносильно такому: $(x-1)(x+1) \equiv 0 \pmod{m}$.

8. Пусть $\left(\frac{a}{p}\right)=0$ при $(a, p)=p$.

a. При $(k, p)=1$ доказать, что

$$\sum_{x=0}^{p-1}\left(\frac{x(x+k)}{p}\right)=-1.$$

b. Пусть каждое из чисел ε и η имеет одно из значений ± 1, T — число пар x, $x+1$, где $x=1, 2, \ldots, p-2$, с условием $\left(\frac{x}{p}\right)=\varepsilon$, $\left(\frac{x+1}{p}\right)=\eta$. Доказать, что

$$T=\frac{1}{4}\left(p-2-\varepsilon\left(\frac{-1}{p}\right)-\eta-\varepsilon\eta\right).$$

c. Пусть $(k, p)=1$,

$$S=\sum_{x}\sum_{y}\left(\frac{xy+k}{p}\right),$$

где x и y пробегают возрастающие последовательности, составленные соответственно из X и Y вычетов полной системы по модулю p. Доказать, что

$$|S|<\sqrt{XYp}.$$

Для доказательства следует воспользоваться неравенством

$$S^2\leqslant X\sum_{x}\left|\sum_{y}\left(\frac{xy+k}{p}\right)\right|^2.$$

d. Пусть Q — целое, $1<Q<p$,

$$S=\sum_{x=0}^{p-1}S_x^2;\quad S_x=\sum_{z=0}^{Q-1}\left(\frac{x+z}{p}\right).$$

α) Доказать, что $S=(p-Q)\,Q$.

β) Пусть λ — постоянное; $0<\lambda<1$. Доказать, что число T чисел ряда $x=0, 1, \ldots, p-1$, для которых не выполняется условие $S_x\leqslant Q^{0{,}5+0{,}5\lambda}$, удовлетворяет условию $T\leqslant pQ^{-\lambda}$.

γ) Пусть M — целое, $Q=[\sqrt{p}]$, $0<M$, $M+2Q\leqslant p$. Доказать, что в ряде

$$M, M+1, \ldots, M+2Q-1$$

имеется квадратичный невычет по модулю p.

9, a. Доказать, что число представлений целого $m>1$ в виде

$$m=x^2+y^2,\quad (x, y)=1,\quad x>0,\quad y>0 \tag{1}$$

равно числу решений сравнения

$$z^2+1\equiv 0 \pmod m. \tag{2}$$

Для доказательства, положив $\tau = \sqrt{m}$, воспользоваться представлением $\alpha = \frac{z}{m}$ согласно теореме вопроса 4, b, гл. I, и рассмотреть сравнение, получаемое почленным умножением (2) на Q^2.

b. Пусть a — одно из чисел 2 и 3. Доказать, что число представлений простого p с условием $p > a$ в виде

$$p = x^2 + ay^2, \quad x > 0, \quad y > 0 \tag{3}$$

равно половине числа решений сравнения

$$z^2 + a \equiv 0 \pmod{p}. \tag{4}$$

c. Пусть p имеет вид $4m+1$, $(k, p) = 1$,

$$S(k) = \sum_{x=0}^{p-1} \left(\frac{x(x^2+k)}{p} \right).$$

Доказать, что

α) $S(k)$ — четное число.

β) $S(kt^2) = \left(\frac{t}{p}\right) S(k)$.

γ) При $\left(\frac{r}{p}\right) = 1$, $\left(\frac{n}{p}\right) = -1$ имеем

$$p = \left(\frac{1}{2} S(r)\right)^2 + \left(\frac{1}{2} S(n)\right)^2.$$

10. Пусть D — целое положительное, не являющееся квадратом целого числа. Доказать, что:

a. Если при данном целом k уравнению

$$x^2 - Dy^2 = k$$

удовлетворяют две пары целых $x = x_1$, $y = y_1$ и $x = x_2$, $y = y_2$, то уравнению

$$X^2 - DY^2 = k^2$$

удовлетворяют целые X, Y, определяемые равенством (знак $\pm$ выбирается произвольно)

$$X + Y\sqrt{D} = (x_1 + y_1\sqrt{D})(x_2 \pm y_2\sqrt{D}),$$

b. Уравнение (уравнение Пелля)

$$x^2 - Dy^2 = 1 \tag{1}$$

разрешимо в целых положительных x, y.

c. Если x_0, y_0 — пара положительных x, y с наименьшим x (или, что равносильно, с наименьшим $x + y\sqrt{D}$), удовлетворяющая уравнению (1), то все пары положительных x, y, удовлетворяющие этому уравнению, определяются равенством

$$x + y\sqrt{D} = (x_0 + y_0\sqrt{D})^r; \quad r = 1, 2, \ldots \tag{2}$$

11. Пусть $m > 2$, $(a, m) = 1$,

$$S_{a,m} = \sum_{x=0}^{m-1} e^{2\pi i \cdot \frac{ax^2}{m}}.$$

а. Доказать, что

$$|S_{a,m}| = \sqrt{m}, \quad \text{если} \quad m \equiv 1 \pmod 2,$$
$$|S_{a,m}| = 0, \quad \text{если} \quad m \equiv 2 \pmod 4,$$
$$|S_{a,m}| = \sqrt{2m}, \quad \text{если} \quad m \equiv 0 \pmod 4.$$

b. Пусть $(A, p) = 1$, M и Q — целые, $0 < M < M + Q \leqslant p$.

α) При любом целом a доказать, что

$$\left| \sum_{x=0}^{p-1} e^{2\pi i \frac{Ax^2+ax}{p}} \right| = \sqrt{p}.$$

β) При $p > 60$, пользуясь теоремой вопроса α), доказать, что

$$\left| \sum_{x=M}^{M+Q-1} e^{2\pi i \frac{Ax^2}{p}} \right| < \sqrt{p} \ln p.$$

γ) Пусть M_0 и Q_0 — целые, $0 < M_0 < M_0 + Q_0 \leqslant p$ и T обозначает число чисел Ax^2; $x = M, M+1, \ldots, M+Q-1$, сравнимых по модулю p с числами ряда $M_0, M_0+1, \ldots, M_0+Q-1$. Доказать, что при $p > 60$ имеем

$$T = \frac{Q_0 Q}{p} + \theta \sqrt{p} \, (\ln p)^2, \quad |\theta| < 1.$$

δ) Пусть $(a, p) = 1$. Доказать, что

$$S_{a,p} = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{ax}{p}}.$$

ε) Из теоремы вопроса **11**, а следует, что $|S_{a,p}| = \sqrt{p}$. То же самое доказать, используя представление $S_{a,p}$ равенством вопроса δ).

η) Пусть $(a, p) = 1$. Доказать, что при некотором θ с условием $|\theta| = 1$, не зависящем от a, имеем

$$\left(\frac{a}{p}\right) = \frac{S_{a,p}}{\theta \sqrt{p}}.$$

ϰ) Пользуясь теоремой вопроса δ), доказать, что

$$\left| \sum_{x=M}^{M+Q-1} \left(\frac{x}{p}\right) \right| < \sqrt{p} \ln p.$$

λ) Пусть R — число квадратичных вычетов, а N — число квадратичных невычетов в ряде $M, M+1, \ldots, M+Q-1$. Доказать, что

$$R = \frac{1}{2} Q + \frac{\theta}{2} \sqrt{p} \ln p, \quad N = \frac{1}{2} Q - \frac{\theta}{2} \sqrt{p} \ln p, \quad |\theta| < 1.$$

μ) Вывести формулы вопроса λ), рассматривая сумму

$$\sum_{a=0}^{p-1}\sum_{\alpha=1}^{p-1}\sum_{x=M}^{M+Q-1}\sum_{y=M}^{M+Q-1}\left(\frac{\alpha}{p}\right)e^{2\pi i\frac{a(x-\alpha y)}{p}}.$$

ν) Пользуясь теоремой вопроса δ), при $p>60$, $Q=[6\sqrt{p}]$ доказать, что в ряде $M, M+1, \ldots, M+Q-1$ имеется квадратичный невычет по модулю p.

Численные примеры к главе V

1, a. Среди вычетов приведенной системы по модулю 23 указать квадратичные вычеты.

b. Среди вычетов приведеиной системы по модулю 37 указать квадратичные невычеты.

2, a. Применяя b, § 2 указать число решений сравнений

α) $x^2\equiv 3 \pmod{31}$; β) $x^2\equiv 2 \pmod{31}$.

b. Указать число решений сравнений:

α) $x^2\equiv 5 \pmod{73}$; β) $x^2\equiv 3 \pmod{73}$.

3, a. Вычисляя символ Якоби, указать число решений сравнений

α) $x^2\equiv 226 \pmod{563}$; β) $x^2\equiv 429 \pmod{563}$.

b. Указать число решений сравнений:

α) $x^2\equiv 3766 \pmod{5987}$; β) $x^2\equiv 3149 \pmod{5987}$.

4, a. Применяя способы вопросов 2, a; 2, b; 2, c, решить сравнения

α) $x^2\equiv 5 \pmod{19}$; β) $x^2\equiv 5 \pmod{29}$; γ) $x^2\equiv 2 \pmod{97}$.

b. Решить сравнения:

α) $x^2\equiv 2 \pmod{311}$; β) $x^2\equiv 3 \pmod{277}$; γ) $x^2\equiv 11 \pmod{353}$.

5, a. Решить сравнение $x^2\equiv 59 \pmod{125}$ способами α) b, § 4; β) вопроса 5, a; γ) вопроса 6.

b. Решить сравнение $x^2\equiv 91 \pmod{243}$.

6, a. Решить сравнение $x^2\equiv 41 \pmod{64}$ способами:

α) d, § 4, β) вопроса 5, b.

b. Решить сравнение $x^2\equiv 145 \pmod{256}$.

Глава VI

ПЕРВООБРАЗНЫЕ КОРНИ И ИНДЕКСЫ

§ 1. Общие теоремы

a. При $(a, m) = 1$ существуют положительные γ с условием $a^\gamma \equiv 1 \pmod m$, например (теорема Эйлера) $\gamma = \varphi(m)$. Наименьшее из них называется: *показатель, которому a принадлежит по модулю m.*

b. *Если a по модулю m принадлежит показателю* δ, *то числа* $1 = a^0, a^1, \ldots, a^{\delta-1}$ *по модулю m несравнимы.*

Действительно, из $a^l \equiv a^k \pmod m$, $0 \leqq k < l < \delta$ следовало бы $a^{l-k} \equiv 1 \pmod m$; $0 < l-k < \delta$, что противоречит определению δ.

c. *Если a по модулю m принадлежит показателю* δ, *то* $a^\gamma \equiv a^{\gamma'} \pmod m$ *тогда и только тогда, когда* $\gamma \equiv \gamma' \pmod \delta$; *в частности (при* $\gamma' = 0$*),* $a^\gamma \equiv 1 \pmod m$ *тогда и только тогда, когда* γ *делится на* δ.

Действительно, пусть r и r_1 — наименьшие неотрицательные вычеты чисел γ и γ' по модулю δ; тогда при некоторых q и q_1 имеем $\gamma = \delta q + r$, $\gamma' = \delta q_1 + r_1$. Отсюда и из $a^\delta \equiv 1 \pmod m$ следует

$$a^\gamma = (a^\delta)^q a^r = a^r \pmod m,$$
$$a^{\gamma'} = (a^\delta)^{q_1} a^{r_1} = a^{r_1} \pmod m.$$

Поэтому $a^\gamma \equiv a^{\gamma'} \pmod m$ тогда и только тогда, когда $a^r \equiv a^{r_1} \pmod m$, т. е. (**b**), когда $r = r_1$.

d. Пусть a по модулю m принадлежит показателю δ. Тогда из **c** ($\gamma' = 0$) и из $a^{\varphi(m)} \equiv 1 \pmod m$ следует, что $\varphi(m)$ делится на δ. Таким образом, *показатели, которым числа принадлежат по модулю m, суть делители* $\varphi(m)$. Наибольший из этих делителей есть само $\varphi(m)$. Числа, принадлежащие показателю $\varphi(m)$ (если такие существуют), называются *первообразными корнями по модулю m.*

§ 2. Первообразные корни по модулям p^α и $2p^\alpha$

a. Пусть p — простое нечетное и $\alpha \geqslant 1$. Докажем существование первообразных корней по модулям p^α и $2p^\alpha$.

b. *Если x по модулю m принадлежит показателю ab, то x^a принадлежит показателю b.*

Действительно, пусть x^a принадлежит показателю δ. Тогда $(x^a)^\delta \equiv 1 \pmod m$, откуда $x^{a\delta} \equiv 1 \pmod m$; следовательно (c, § 1), $a\delta$ делится на ab, т. е. δ делится на b. С другой стороны, $x^{ab} \equiv 1 \pmod m$, откуда $(x^a)^b = 1 \pmod m$; следовательно (c, § 1), b делится на δ. Поэтому $\delta = b$.

c. *Если x по модулю m принадлежит показателю a, а y — показателю b, причем $(a, b) = 1$, то xy принадлежит показателю ab.*

Действительно, пусть xy принадлежит показателю δ. Тогда $(xy)^\delta \equiv 1 \pmod m$. Отсюда $x^{b\delta}y^{b\delta} = 1 \pmod m$ и (c, § 1) $x^{b\delta} \equiv 1 \pmod m$. Поэтому (c, § 1) $b\delta$ делится на a, и ввиду $(b, a) = 1$ δ делится на a. Так же находим, что δ делится на b. Делясь же на a и на b, ввиду $(a, b) = 1$ δ делится и на ab. С другой стороны, из $(xy)^{ab} \equiv 1 \pmod m$ следует (c, § 1), что ab делится на δ. Поэтому $\delta = ab$.

d. *Существуют первообразные корни по модулю p.*

Действительно, пусть

$$\delta_1, \delta_2, \ldots, \delta_r \qquad (1)$$

— все различные показатели, которым по модулю p принадлежат числа 1, 2, ..., $(p-1)$. Пусть τ — общее наименьшее кратное этих показателей и

$$\tau = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$$

— его каноническое разложение. Каждый множитель $q_s^{\alpha_s}$ этого разложения делит по меньшей мере одно число δ_j ряда (1), которое, следовательно, может быть представлено в виде: $\delta_j = aq_s^{\alpha_s}$. Пусть ξ_j — одно из чисел ряда 1, 2, ..., $p-1$, принадлежащих показателю δ_j. Согласно b число $\eta_j = \xi_j^a$ принадлежит показателю $q_s^{\alpha_s}$, согласно c произведение $g = \eta_1\eta_2 \ldots \eta_k$ принадлежит показателю $q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k} = \tau$. Поэтому (d, § 1) τ — делитель $p-1$.

Но поскольку числа (1) делят τ, все $1, 2, \ldots, p-1$ являются решениями (с, § 1) сравнения $x^\tau \equiv 1 \pmod p$; поэтому, согласно с, § 4, гл. IV, будем иметь $p-1 \leqslant \tau$. Следовательно, $\tau = p-1$ и g — первообразный корень.

e. *Пусть g — первообразный корень по модулю p. Можно указать t с условием, что u, определяемое равенством $(g+pt)^{p-1} = 1 + pu$, не делится на p. Соответствующее $g+pt$ будет первообразным корнем по модулю p^α при любом $\alpha > 1$.*

Действительно, имеем

$$\begin{aligned} g^{p-1} &= 1 + pT_0, \\ (g+pt)^{p-1} &= 1 + p(T_0 - g^{p-2}t + pT) = 1 + pu, \end{aligned} \tag{2}$$

где, одновременно с t, u пробегает полную систему вычетов по модулю p. Поэтому можно указать t с условием, что u не делится на p. При таком t из (2) выводим

$$\begin{aligned} (g+pt)^{p(p-1)} &= (1+pu)^p = 1 + p^2 u_2, \\ (g+pt)^{p^2(p-1)} &= 1 + p^3 u_3, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ (g+pt)^{p^{\alpha-1}(p-1)} &= 1 + p^\alpha u_\alpha, \end{aligned} \tag{3}$$

где все $u_2, u_3, \ldots, u_\alpha$ также не делятся на p. Пусть $g+pt$ принадлежит показателю δ по модулю p^α. Тогда имеем $(g+pt)^\delta \equiv 1 \pmod{p^\alpha}$, откуда, в частности, находим $g^\delta \equiv 1 \pmod p$. Поэтому (с, § 1) δ делится на $p-1$ и, будучи (**d**, § 1) делителем числа $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, должно иметь вид $\delta = p^{r-1}(p-1)$, где r — одно из чисел $1, \ldots, \alpha$. А так как равенства (2) и (3) показывают, что сравнение

$$(g+pt)^{p^{r-1}(p-1)} \equiv 1 \pmod{p^\alpha}$$

верно при $r = \alpha$ и неверно при $r < \alpha$, то (**d**, § 1) $\delta = p^{\alpha-1}(p-1) = \varphi(p^\alpha)$ и $g+pt$ — первообразный корень по модулю p^α.

f. *Пусть $\alpha \geqslant 1$ и g — первообразный корень по модулю p^α. Нечетное g_0 из чисел g и $g+p^\alpha$ будет первообразным корнем по модулю $2p^\alpha$.*

Действительно, $\varphi(p^\alpha)$ и $\varphi(2p^\alpha)$ равны между собою (имеем $\varphi(2p^\alpha) = \varphi(2)\varphi(p^\alpha) = \varphi(p^\alpha)$); их общее значение обозначим буквою c. Далее легко убедимся, что сравнения $g_0^r \equiv 1 \pmod{p^\alpha}$ и $g_0^r \equiv 1 \pmod{2p^\alpha}$ могут выпол-

няться лишь одновременно ($g_0^r - 1$ делится на 2). А так как g_0 — первообразный корень по модулю p^α и первое сравнение верно при $r = c$ и неверно при $r < c$, то тем самым и второе сравнение верно при $r = c$ и неверно при $r < c$ и g_0 — первообразный корень по модулю $2p^\alpha$.

§ 3. Разыскание первообразных корней по модулям p^α и $2p^\alpha$

Первообразные корни по модулям p^α и $2p^\alpha$, где p — простое нечетное и $\alpha \geqslant 1$, можно разыскивать, пользуясь следующей общей теоремой:

Пусть $c = \varphi(m)$ и $q_1, q_2, \ldots, q_k$ — различные простые делители числа c. Для того чтобы число g, взаимно простое с m, было первообразным корнем по модулю m, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^{\frac{c}{q_1}} \equiv 1 \pmod m, \quad g^{\frac{c}{q_2}} \equiv 1 \pmod m, \quad \ldots, \quad g^{\frac{c}{q_k}} \equiv 1 \pmod m. \tag{1}$$

Действительно, если g — первообразный корень, то тем самым оно принадлежит показателю c и, следовательно, ни одному из сравнений (1) удовлетворять не может.

Обратно, допустим, что g не удовлетворяет ни одному из сравнений (1). Если бы показатель δ, которому принадлежит g, оказался меньше c, то, обозначая буквою q один из простых делителей $\frac{c}{\delta}$, мы имели бы $\frac{c}{\delta} = qu$, $\frac{c}{q} = \delta u$, $g^{\frac{c}{q}} \equiv 1 \pmod p$, что противоречит нашему допущению. Значит, $\delta = c$ и g — первообразный корень.

Пример 1. Пусть $m = 41$. Имеем $\varphi(41) = 40 = 2^3 \cdot 5$, $\frac{40}{5} = 8$, $\frac{40}{2} = 20$. Следовательно, для того чтобы число g, не делящееся на 41, было первообразным корнем по модулю 41, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^8 \equiv 1 \pmod{41}, \quad g^{20} \equiv 1 \pmod{41}. \tag{2}$$

Но, испытывая числа 2, 3, 4, ..., находим (по модулю 41)

$$2^8 = 10, \quad 3^8 = 1, \quad 4^8 = 18, \quad 5^8 = 18, \quad 6^8 \equiv 10,$$
$$2^{20} \equiv 1, \qquad 4^{20} = 1, \quad 5^{20} \equiv 1, \quad 6^{20} = 40.$$

Отсюда видим, что числа 2, 3, 4, 5—не первообразные корни, так как каждое из них удовлетворяет, по крайней мере, одному из сравнений (2). Число 6—первообразный корень, так как оно не удовлетворяет ни одному из сравнений (2).

Пример 2. Пусть $m = 1681 = 41^2$. Первообразный корень и здесь можно было бы найти, пользуясь общей теоремой. Но мы найдем его проще, применяя теорему e, § 2. Зная уже (пример 1), что первообразный корень по модулю 41 есть 6, находим

$$6^{40} = 1 + 41\,(3 + 41l),$$
$$(6 + 41t)^{40} = 1 + 41\,(3 + 41l - 6^{39}t + 41T) = 1 + 41u.$$

Чтобы u не делилось на 41, достаточно взять $t = 0$. Поэтому в качестве первообразного корня по модулю 1681 можно взять число $6 + 41 \cdot 0 = 6$.

Пример 3. Пусть $m = 3362 = 2 \cdot 1681$. Первообразный корень и здесь можно было бы найти, пользуясь общей теоремой. Но мы найдем его проще, применяя теорему f, § 2. Зная уже (пример 2), что первообразный корень по модулю 1681 есть 6, в качестве первообразного корня по модулю 3362 можно взять нечетное из чисел 6, $6 + 1681$, т. е. число 1687.

§ 4. Индексы по модулям p^α и $2p^\alpha$

a. Пусть p—простое нечетное, $\alpha \geqslant 1$; m—одно из чисел p^α и $2p^\alpha$; $c = \varphi(m)$, g—первообразный корень по модулю m.

b. *Если γ пробегает наименьшие неотрицательные вычеты $\gamma = 0, 1, \ldots, c-1$ по модулю c, то g^γ пробегает приведенную систему вычетов по модулю m.*

Действительно, g^γ пробегает c чисел, взаимно простых с m, и ввиду b, § 1, не сравнимых по модулю m.

c. Для чисел a, взаимно простых с m, введем понятие об индексе, представляющее аналогию понятию о ло-

гарифме; при этом первообразный корень играет роль, аналогичную роли основания логарифмов.

Если

$$a \equiv g^\gamma \pmod m$$

(считаем $\gamma \geqslant 0$), то γ называется *индексом числа* a *по модулю* m *при основании* g и обозначается символом $\gamma = \operatorname{ind} a$ (точнее, $\gamma = \operatorname{ind}_g a$).

Ввиду b всякое a, взаимно простое с m, имеет некоторый единственный индекс γ' среди чисел ряда

$$\gamma = 0,\ 1,\ \ldots,\ c-1.$$

Зная γ', мы можем указать и все индексы числа a; согласно c, § 1 это будут все неотрицательные числа класса

$$\gamma \equiv \gamma' \pmod c.$$

Непосредственно из данного здесь определения индекса следует, что числа с данным индексом γ образуют класс чисел по модулю m.

d. *Имеем*

$$\operatorname{ind} ab\ldots l \equiv \operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l \pmod c$$

и, в частности,

$$\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod c.$$

Действительно,

$$a \equiv g^{\operatorname{ind} a} \pmod m,\ b \equiv g^{\operatorname{ind} b} \pmod m,\ \ldots,\ l \equiv g^{\operatorname{ind} l} \pmod m,$$

откуда, перемножая, находим

$$ab\ldots l \equiv g^{\operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l} \pmod m.$$

Следовательно, $\operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l$ — один из индексов произведения $ab\ldots l$.

e. Ввиду практической пользы индексов для каждого простого модуля p (разумеется, не слишком большого) составлены *таблицы индексов*. Это две таблицы; одна — для нахождения индекса по числу, другая — для нахождения числа по индексу. Таблицы содержат наименьшие

неотрицательные вычеты чисел (приведенная система) и их наименьших индексов (полная система) соответственно по модулям p и $c=\varphi(p)=p-1$.

Пример. Построим указаиные таблицы для модуля $p=41$. Выше было показано (пример 1, § 3), что первообразным корнем по модулю 41 будет $g=6$; его мы примем за основание индексов. Находим (сравнения берутся по модулю 41):

$$\begin{array}{lllll}
6^0\equiv 1 & 6^8\equiv 10 & 6^{16}\equiv 18 & 6^{24}\equiv 16 & 6^{32}\equiv 37\\
6^1\equiv 6 & 6^9\equiv 19 & 6^{17}\equiv 26 & 6^{25}\equiv 14 & 6^{33}\equiv 17\\
6^2\equiv 36 & 6^{10}\equiv 32 & 6^{18}\equiv 33 & 6^{26}\equiv 2 & 6^{34}\equiv 20\\
6^3\equiv 11 & 6^{11}\equiv 28 & 6^{19}\equiv 34 & 6^{27}\equiv 12 & 6^{35}\equiv 38\\
6^4\equiv 25 & 6^{12}\equiv 4 & 6^{20}\equiv 40 & 6^{28}\equiv 31 & 6^{36}\equiv 23\\
6^5\equiv 27 & 6^{13}\equiv 24 & 6^{21}\equiv 35 & 6^{29}\equiv 22 & 6^{37}\equiv 15\\
6^6\equiv 39 & 6^{14}\equiv 21 & 6^{22}\equiv 5 & 6^{30}\equiv 9 & 6^{38}\equiv 8\\
6^7\equiv 29 & 6^{15}\equiv 33 & 6^{23}\equiv 30 & 6^{31}\equiv 13 & 6^{39}\equiv 7
\end{array}$$

поэтому указанные таблицы будут

$$p=41,\quad p-1=2^3\cdot 5,\quad g=6$$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

Здесь номер строки указывает число десятков, номер столбца — число единиц числа (индекса). В графе, общей указанным строке и столбцу, помещается соответствующий индекс (число).

Например, ind 25 найдем в графе первой таблицы, общей строке с номером 2 и столбцу с номером 5, т. е. $\operatorname{ind} 25=4$. Число, индекс которого 33, найдем в графе второй таблицы, общей строке с номером 3 и столбцу с номером 3, т. е. $33=\operatorname{ind} 17$.

§ 5. Следствия предыдущей теории

a. Пусть p—простое нечетное; $\alpha \geqslant 1$, m—одно из чисел p^{α}, $2p^{\alpha}$, наконец, $c = \varphi(m)$.

b. *Пусть* $(n, c) = d$; *тогда:*

1. *Сравнение*

$$x^n = a \pmod{m}; \quad (a, m) = 1 \tag{1}$$

разрешимо (и тем самым a *есть вычет степени* n *по модулю* m*) тогда и только тогда, когда* $\operatorname{ind} a$ *кратен* d.

В случае разрешимости сравнение имеет d *решений.*

2. *В приведенной системе вычетов по модулю* m *число вычетов степени* n *есть* $\frac{c}{d}$.

Действительно, сравнение (1) равносильно такому:

$$n \operatorname{ind} x = \operatorname{ind} a \pmod{c}, \tag{2}$$

которое разрешимо тогда и только тогда, когда $\operatorname{ind} a$ кратен d (**d**, § 2, гл. IV).

В случае разрешимости сравнения (2) найдем d несравнимых по модулю c значений для $\operatorname{ind} x$; им отвечает d несравнимых по модулю m значений для x.

Таким образом, верно утверждение **1**.

Среди чисел $0, 1, \ldots, c-1$, являющихся наименьшими индексами вычетов приведенной системы по модулю m, имеется $\frac{c}{d}$ кратных d. Поэтому верно утверждение **2**.

Пример 1. Для сравнения

$$x^3 = 23 \pmod{41} \tag{3}$$

имеем $(8, 40) = 8$, причем $\operatorname{ind} 23 = 36$ не делится на 8. Поэтому сравнение (3) неразрешимо.

Пример 2. Для сравнения

$$x^{12} = 37 \pmod{41} \tag{4}$$

имеем $(12, 40) = 4$, причем $\operatorname{ind} 37 = 32$ делится на 4. Поэтому сравнение (4) разрешимо, причем это сравнение имеет 4 решения. Указанные решения найдем следующим образом.

Сравнение (4) равносильно таким:

$$12 \operatorname{ind} x \equiv 32 \pmod{40}, \quad \operatorname{ind} x \equiv 6 \pmod{10}.$$

Отсюда для $\operatorname{ind} x$ найдем 4 несравнимых по модулю 40 значения:

$$\operatorname{ind} x = 6,\ 16,\ 26,\ 36,$$

соответственно чему найдем 4 решения сравнения (4)

$$x \equiv 39;\ 18;\ 2;\ 23 \pmod{41}.$$

Пример 3. Числа

$$1,\ 4,\ 10,\ 16,\ 18,\ 23,\ 25,\ 31,\ 37,\ 40, \qquad (5)$$

индексы которых кратны 4, суть все биквадратичные вычеты (или также все вычеты любой степени $n = 4, 12, 28, \ldots$, где $(n, 40) = 4$), имеющиеся среди наименьших положительных вычетов по модулю 41. Число чисел ряда (5) есть $10 = \frac{40}{4}$.

c. С утверждением **b, 1** тесно связано следующее.

Число a есть вычет степени n по модулю m тогда и только тогда, когда

$$a^{\frac{c}{d}} \equiv 1 \pmod{m}. \qquad (6)$$

Действительно, условие $\operatorname{ind} a \equiv 0 \pmod{d}$ равносильно такому: $\frac{c}{d} \operatorname{ind} a \equiv 0 \pmod{c}$. Последнее же равносильно условию (6).

Пример. В теореме § 3 невозможность сравнения $g^{\frac{c}{q}} \equiv 1 \pmod{m}$ равносильна условию, что g — невычет степени q по модулю m. В частности, невозможность сравнения $g^{\frac{c}{2}} \equiv 1 \pmod{m}$ равносильна условию, что g — квадратичный невычет по модулю m (ср. **b**, § 2, гл. V).

d.1. *Показатель δ, которому a принадлежит по модулю m, определяется равенством* $(\operatorname{ind} a, c) = \frac{c}{\delta}$; *в частности, принадлежность a к числу первообразных корней по модулю m определяется равенством* $(\operatorname{ind} a, c) = 1$.

2. *В приведенной системе вычетов по модулю m число чисел, принадлежащих показателю δ, есть $\varphi(\delta)$; в частности, число первообразных корней есть $\varphi(c)$.*

Действительно, δ есть наименьший делитель c с условием $a^\delta \equiv 1 \pmod m$. Это условие равносильно

$$\delta \operatorname{ind} a \equiv 0 \pmod c,$$

или

$$\operatorname{ind} a \equiv 0 \left(\operatorname{mod} \frac{c}{\delta}\right).$$

Значит, δ — наименьший делитель c, при котором $\frac{c}{\delta}$ делит $\operatorname{ind} a$, отсюда $\frac{c}{\delta}$ — наибольший делитель c, делящий $\operatorname{ind} a$, т. е. $\frac{c}{\delta} = (\operatorname{ind} a, c)$. Поэтому верно утверждение **1**.

Среди чисел $0, 1, \ldots, c-1$, являющихся наименьшими индексами вычетов приведенной системы по модулю m, кратными $\frac{c}{\delta}$ являются числа вида $\frac{c}{\delta} y$, где $y = 0, 1, \ldots, \delta - 1$. Условие $\left(\frac{c}{\delta} y, c\right) = \frac{c}{\delta}$ равносильно условию $(y, \delta) = 1$; последнему удовлетворяет $\varphi(\delta)$ значений y. Поэтому верно утверждение **2**.

Пример 1. В приведенной системе вычетов по модулю 41 числами, принадлежащими показателю 10, являются числа a с условием $(\operatorname{ind} a, 40) = \frac{40}{10} = 4$. т. е. числа

4, 23, 25, 31.

Число этих чисел есть $4 = \varphi(10)$.

Пример 2. В приведенной системе вычетов по модулю 41 первообразными корнями являются числа a с условием $(\operatorname{ind} a, 40) = 1$, т. е. числа

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35.

Число этих первообразных корней есть $16 = \varphi(40)$.

§ 6. Индексы по модулю 2^α

a. Для модуля 2 предыдущая теория заменяется несколько более сложной.

b. Пусть $\alpha = 1$. Тогда $2^\alpha = 2$. Имеем $\varphi(2) = 1$. Первообразным корнем по модулю 2 будет, например, $1 \equiv -1 \pmod 2$. Число $1^0 = (-1)^0 = 1$ образует приведенную систему вычетов по модулю 2.

c. Пусть $\alpha = 2$. Тогда $2^\alpha = 4$. Имеем $\varphi(4) = 2$. Первообразным корнем по модулю 4 будет, например, $3 = -1 \pmod 4$. Числа $(-1)^0 = 1$, $(-1)^1 \equiv 3 \pmod 4$ образуют приведенную систему вычетов по модулю 4.

d. Пусть $\alpha \geqslant 3$. Тогда $2^\alpha \geqslant 8$. Имеем $\varphi(2^\alpha) = 2^{\alpha-1}$. Нетрудно видеть, что первообразных корней в этом случае нет; более точно: показатель, которому принадлежит по модулю 2^α нечетное число x, не превосходит $2^{\alpha-2} = \frac{1}{2}\varphi(2^\alpha)$. Действительно, имеем

$$x^2 = 1 + 8t_1,$$
$$x^4 = 1 + 16t_2,$$
$$\ldots\ldots$$
$$x^{2^{\alpha-2}} = 1 + 2^\alpha t_{\alpha-2} \equiv 1 \pmod{2^\alpha}.$$

При этом числа, принадлежащие показателю $2^{\alpha-2}$, существуют. Таким числом будет, например, 5. Действительно,

$$5 = 1 + 4,$$
$$5^2 = 1 + 8 + 16,$$
$$5^4 = 1 + 16 + 32u_2,$$
$$\ldots\ldots\ldots$$
$$5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + 2^\alpha u_{\alpha-3},$$

откуда видим, что ни одна из степеней $5^1, 5^2, 5^4, \ldots, 5^{2^{\alpha-3}}$ не сравнима с 1 по модулю 2^α.

Нетрудно видеть, что числа двух следующих строк:

$$5^0, \quad 5^1, \quad \ldots, \quad 5^{2^{\alpha-3}-1}$$
$$-5^0, \quad -5^1, \quad \ldots, \quad -5^{2^{\alpha-3}-1},$$

образуют приведенную систему вычетов по модулю 2^α. Действительно, число этих чисел будет $2 \cdot 2^{\alpha-2} = \varphi(2^\alpha)$; числа каждой отдельно взятой строки между собой по модулю 2^α несравнимы (**b**, § 1); наконец, числа верхней строки несравнимы с числами нижней, так как первые по модулю 4 сравнимы с 1, а вторые с -1.

e. Для удобства дальнейших исследований мы выразим результаты **b**, **c**, **d** в более единообразной форме, которая будет пригодна и в случае $\alpha = 0$.

Пусть

$$c=1,\quad c_0=1,\qquad \text{если}\quad \alpha=0,\quad \text{или}\quad \alpha=1;$$
$$c=2,\quad c_0=2^{\alpha-2},\quad \text{если}\quad \alpha\geqslant 2$$

(*таким образом всегда* $cc_0=\varphi(2^\alpha)$), *и пусть* γ *и* γ_0 *независимо друг от друга пробегают наименьшие неотрицательные вычеты*

$$\gamma=0,\ \ldots,\ c-1;\quad \gamma_0=0,\ \ldots,\ c_0-1$$

по модулям c *и* c_0. *Тогда* $(-1)^\gamma 5^{\gamma_0}$ *пробегает приведенную систему вычетов по модулю* 2^α.

f. *Сравнение*

$$(-1)^\gamma 5^{\gamma_0}\equiv(-1)^{\gamma'}5^{\gamma_0'}\pmod{2^\alpha} \tag{1}$$

имеет место тогда и только тогда, когда

$$\gamma\equiv\gamma'\pmod c,\quad \gamma_0\equiv\gamma_0'\pmod{c_0}.$$

Действительно, при $\alpha=0$ теорема очевидна. Поэтому предположим, что $\alpha>0$. Пусть наименьшие неотрицательные вычеты по модулям c и c_0 для чисел γ и γ_0 будут r и r_0, а для чисел γ' и γ_0' будут r' и r_0'. Ввиду c, § 1 (-1 принадлежит показателю c, а 5 принадлежит показателю c_0), сравнение (1) имеет место тогда и только тогда, когда $(-1)^r 5^{r_0}\equiv(-1)^{r'}5^{r_0'}\pmod{2^\alpha}$, т. е. (ввиду e) когда $r=r'$, $r_0=r_0'$.

g. Если

$$a\equiv(-1)^\gamma 5^{\gamma_0}\pmod{2^\alpha},$$

то система γ, γ_0 называется *системой индексов числа* a *по модулю* 2^α.

Ввиду e всякое a, взаимно простое с 2^α (т. е. нечетное), имеет единственную систему индексов γ', γ_0' среди $cc_0=\varphi(2^\alpha)$ пар значений γ, γ_0, указанных в e.

Зная систему γ', γ_0', мы можем указать и все системы индексов числа a; согласно f это будут все пары γ, γ_0, составленные из неотрицательных чисел классов

$$\gamma\equiv\gamma'\pmod c,\quad \gamma_0\equiv\gamma_0'\pmod{c_0}.$$

Непосредственно из данного здесь определения системы индексов следует, что числа с данной системой индексов γ, γ_0 образуют класс чисел по модулю 2^α.

h. *Индексы произведения сравнимы по модулям c и c_0 с суммами индексов сомножителей.*

Действительно, пусть $\gamma(a)$, $\gamma_0(a)$; ...; $\gamma(l)$, $\gamma_0(l)$ — системы индексов чисел a, ..., l. Имеем

$$a \dots l = (-1)^{\gamma(a)+\dots+\gamma(l)} 5^{\gamma_0(a)+\dots+\gamma_0(l)}.$$

Следовательно, $\gamma(a)+\dots+\gamma(l)$, $\gamma_0(a)+\dots+\gamma_0(l)$ — индексы произведения $a \dots l$.

§ 7. Индексы по любому составному модулю

a. Пусть $m = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение числа m. Пусть далее c и c_0 имеют значения, указанные в e, § 6; $c_s = \varphi(p_s^{\alpha_s})$; g_s — наименьший первообразный корень по модулю $p_s^{\alpha_s}$.

b. Если

$$\begin{aligned} &a \equiv (-1)^\gamma 5^{\gamma_0} \pmod{2^\alpha}, \\ &a \equiv g_1^{\gamma_1} \pmod{p_1^{\alpha_1}}, \ \dots, \ a \equiv g_k^{\gamma_k} \pmod{p_k^{\alpha_k}}, \end{aligned} \tag{1}$$

то система γ, γ_0, γ_1, ..., γ_k называется *системой индексов числа a по модулю m.*

Из такого определения следует, что γ, γ_0 — система индексов числа a по модулю 2^α, а γ_1, ..., γ_k — индексы числа a по модулям $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$. Поэтому (g, § 6; c, § 4) всякое a, взаимно простое с m (тем самым оно взаимно простое и со всеми 2^α, $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$), имеет единственную систему индексов γ, γ_0', γ_1', ..., γ_k' среди $cc_0c_1 \dots c_k = \varphi(m)$ систем γ, γ_0, γ_1, ..., γ_k, которые получим, заставляя γ, γ_0, γ_1, ..., γ_k независимо друг от друга пробегать наименьшие неотрицательные вычеты по модулям c, c_0, c_1, ..., c_k, а все системы индексов числа a суть все системы γ, γ_0, γ_1, ..., γ_k, составленные из неотрицательных чисел классов

$$\gamma \equiv \gamma_1' \pmod{c}, \quad \gamma_0 \equiv \gamma_0' \pmod{c_0},$$
$$\gamma_1 \equiv \gamma_1' \pmod{c_1}, \ \dots, \ \gamma_k \equiv \gamma_k' \pmod{c_k}.$$

Числа a с данной системой индексов γ, γ_0, γ_1, ..., γ_k могут быть найдены путем решения системы (1), а сле-

довательно (b, § 3, гл. IV), образуют класс чисел по модулю m.

c. Так как индексы γ, γ_0, γ_1, ..., γ_k числа a по модулю m являются индексами его соответственно по модулям 2^α, $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$, то верна теорема:

Индексы произведения сравнимы по модулям c, c_0, c_1, ..., c_k *с суммами индексов сомножителей.*

d. Пусть $\tau = \varphi(2^\alpha)$ при $\alpha \leqslant 2$ и $\tau = \frac{1}{2}\varphi(2^\alpha)$ при $\alpha > 2$ и пусть h — общее наименьшее кратное чисел τ, c_1, ..., c_k. При всяком a, взаимно простом с m, сравнение $a^h \equiv 1$ верно по всем модулям 2^α, $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$, значит, это сравнение верно и по модулю m. Поэтому a не может быть первообразным корнем по модулю m в тех случаях, когда $h < \varphi(m)$. Но последнее имеет место при $\alpha > 2$, при $k > 1$, а также при $\alpha = 2$, $k = 1$. Поэтому для $m > 1$ первообразные корни могут существовать лишь в случаях $m = 2, 4$, $p_1^{\alpha_1}$, $2p_1^{\alpha_1}$. Но как раз для этих случаев существование первообразных корней было доказано выше (§§ 6, 2). Поэтому

Все случаи, когда существуют первообразные корни по модулю m, *превосходящему* 1, *суть*

$$m = 2,\ 4,\ p^\alpha,\ 2p^\alpha.$$

e. Таблицу индексов можно составить и для любого целого положительного m, выписывая соответственно каждому числу приведенной системы вычетов по модулю m отвечающие этому числу значения индексов γ, γ_0, γ_1, ..., γ_k (полные системы вычетов по модулям c, c_0, c_1, ..., c_k).

Пример 1. Построим таблицу индексов по модулю 8. Здесь имеем $c = 2$, $c_0 = 2^{3-2} = 2$ и для каждого числа N приведенной системы вычетов по модулю 8 будем иметь $N \equiv (-1)^\gamma 5^{\gamma_0} \pmod 8$, где γ равно одному из чисел 0, 1 (полная система вычетов по модулю c) и γ_0 равно одному из чисел 0, 1 (полная система вычетов по модулю c_0). Находим

$$\begin{aligned} (-1)^0 &= 1, & (-1)^1 &= -1, \\ 5^0 &= 1 & 5^1 &= 5, \\ -5^0 &\equiv 7 \pmod 8, & -5^1 &\equiv 3 \pmod 8. \end{aligned}$$

Поэтому таблица индексов по модулю 8 будет

N	1	3	5	7
γ	0	1	0	1
γ_0	0	1	1	0

Пример 2. Построим таблицу индексов по модулю 40. Здесь имеем $40 = 8 \cdot 5$, причем для каждого числа N приведенной системы вычетов по модулю 40 мы значения индексов γ и γ_0 найдем в таблице индексов по модулю 8 примера 1, а значения индекса γ_1 найдем в таблице индексов по модулю 5, т. е. в таблице

N	1	2	3	4
γ_1	0	1	3	2

В результате получим следующую таблицу индексов по модулю 40:

N	1	3	7	9	11	13	17	19
γ	0	1	1	0	1	0	0	1
γ_0	0	1	0	0	1	1	0	1
γ_1	0	3	1	2	0	3	1	2
N	21	23	27	29	31	33	37	39
γ	0	1	1	0	1	0	0	1
γ_0	1	0	1	1	0	0	1	0
γ_1	0	3	1	2	0	3	1	2

Пример 3. Построим таблицу индексов по модулю 9 и таблицу индексов по модулю 18. Здесь имеем $\varphi(9) = 6 = 2 \cdot 3$. Число 5 будет первообразным корнем по мо-

дулю 9, так как оно не удовлетворяет ни одному из сравнений $5^{\frac{6}{2}} \equiv 1 \pmod 9$, $5^{\frac{6}{3}} \equiv 1 \pmod 9$. При этом имеем (сравнения берутся по модулю 9):

$$5^0 \equiv 1, \quad 5^1 \equiv 5, \quad 5^2 \equiv 7, \quad 5^3 \equiv 8, \quad 5^4 \equiv 4, \quad 5^5 \equiv 2.$$

Следовательно, таблица индексов по модулю 9 будет

N	1	2	4	5	7	8
γ_1	0	5	4	1	2	3

А таблица индексов по модулю 18 будет

N	1	5	7	11	13	17
γ	0	0	0	0	0	0
γ_1	0	1	2	5	4	3

Пример 4. Построим таблицу индексов по модулю 21. Здесь имеем $21 = 3 \cdot 7$, и для каждого числа N приведенной системы вычетов по модулю 21 мы значение индекса γ_1 найдем в таблице индексов по модулю 3, т. е. в таблице

N	1	2
γ_1	0	1

а значение индекса γ_2 найдем в таблице индексов по модулю 7, т. е. в таблице

N	1	2	3	4	5	6
γ_2	0	2	1	4	5	3

В результате получим следующую таблицу индексов по модулю 21:

N	1	2	4	5	8	10	11	13	16	17	19	20
γ_1	0	1	0	1	1	0	1	0	0	1	0	1
γ_2	0	2	4	5	0	1	4	3	2	1	5	3

Вопросы к главе VI

Буквою p здесь всегда обозначаем простое нечетное число.

1, a. Пусть a—целое, $a > 1$. Доказать, что простые нечетные делители числа $a^p - 1$ делят $a-1$ или имеют вид $2px+1$.

b. Пусть a—целое, $a > 1$. Доказать, что простые нечетные делители числа $a^p + 1$ делят $a+1$ или имеют вид $2px+1$.

c. Доказать бесконечность числа простых чисел вида $2px+1$.

d. Пусть n—целое, $n > 0$. Доказать, что простые делители числа $2^{2^n}+1$ имеют вид $2^{n+1}x+1$.

2. Пусть a—целое, $a > 1$, n—целое, $n > 0$. Доказать, что $\varphi(a^n-1)$ кратно n.

3, a. Пусть n—целое, $n > 1$. Из чисел 1, 2, ..., n при нечетном n образуем перестановки

$$1, 3, 5, \ldots, n-2, n, n-1, n-3, \ldots, 4, 2;$$

$$1, 5, 9, \ldots, 7, 3$$

и т. д., а при четном n образуем перестановки

$$1, 3, 5, \ldots, n-1, n, n-2, \ldots, 4, 2;$$

$$1, 5, 9, \ldots, 7, 3$$

и т. д. Доказать, что k-я операция дает исходный ряд тогда и только тогда, когда $2^k \equiv \pm 1 \pmod{2n-1}$.

b. Пусть n—целое, $n > 1$, m—целое, $m > 1$. Будем считать числа 1, 2, ..., n в прямом порядке от 1 до n, далее в обратном порядке от n до 2, затем опять в прямом порядке от 1 до n, далее опять в обратном порядке от n до 2 и т. д. При таком счете выписываем числа 1-е, $(m+1)$-е, $(2m+1)$-е и т. д., пока не получим n чисел. С этим новым рядом n чисел повторим ту же операцию и т. д. Доказать, что k-я операция дает исходный ряд тогда и только тогда, когда

$$m^k \equiv \pm 1 \pmod{2n-1}.$$

4. При $m=p$ теорему 2, d, § 5 доказать, рассматривая сравнение $x^\delta \equiv 1 \pmod p$ (вопрос 10, c, гл. IV) и применяя c, § 4, гл. II.

5, a. Доказать, что первообразный корень простого числа вида 2^n+1, $n > 1$, есть 3.

b. Доказать, что первообразный корень простого числа вида $2p+1$ при p вида $4n+1$ есть 2, а при p вида $4n+3$ есть -2.

c. Доказать, что первообразный корень простого числа вида $4p+1$ есть 2.

d. Доказать, что первообразный корень простого числа вида

$$2^n p+1 \quad \text{при} \quad n > 1 \quad \text{и} \quad p > \frac{3^{2^{n-1}}}{2^n} \quad \text{есть 3.}$$

6, a. α) Пусть n—целое, $n \geqslant 0$, $S = 1^n + 2^n + \ldots + (p-1)^n$.

Доказать, что

$$S \equiv -1 \pmod p, \quad \text{если } n \text{ кратно } p-1,$$
$$S \equiv 0 \pmod p \quad \text{в противном случае.}$$

β) При обозначениях вопросов 9, c, гл. V доказать, что

$$S(t) \equiv -\left(\frac{\frac{p-1}{2}}{\frac{p-1}{4}}\right) \pmod p.$$

b. Теорему Вильсона доказать, применяя b, § 4.

7. Пусть g и g_1 — первообразные корни по модулю p, $\alpha \operatorname{ind}_g g_1 \equiv 1 \pmod{p-1}$. При $(a, p) = 1$ доказать, что:

$$\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a \pmod{p-1}.$$

8. Пусть $m > 1$, $(a, m) = 1$.

α) Пусть

$$S = \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \xi(x)\, \eta(y)\, e^{2\pi i \frac{axy}{m}};$$

$$\sum_{x=0}^{m-1} |\xi(x)|^2 = X, \quad \sum_{y=0}^{m-1} |\eta(y)|^2 = Y.$$

Доказать, что $|S| \leqslant \sqrt{XYm}$.

β) Пусть $\sum_s'$ обозначает суммирование, распространенное на числа s ряда $0, 1, \ldots, m-1$, взаимно простые с m. Пусть n — целое, превосходящее 1, и

$$S = \sum_x' e^{2\pi i \frac{ax^n}{m}}.$$

Доказать, что $|S| \leqslant K\sqrt{m}$, где K — число решений сравнения $x^n \equiv 1 \pmod m$.

γ) Пусть $m = 2^\alpha p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — каноническое разложение числа m. Доказать, что указанное в вопросе β) число K решений сравнения $x^n \equiv 1 \pmod m$ не превосходит $2n^{\omega+1}$ и что в случае постоянного n имеем $K = O(m^\varepsilon)$, где ε — произвольное положительное постоянное.

9, a. Пусть $(a, p) = (b, p) = 1$, n — целое, отличное от 1. $|n| = n_1$, $0 < n_1 < p$,

$$S = \sum_{x=1}^{p-1} e^{2\pi i \frac{ax^n + bx}{p}}.$$

Доказать, что

$$|S| < \frac{3}{2} n_1^{\frac{1}{4}} p^{\frac{3}{4}}.$$

b. Пусть $(a, p)=1$, n—целое, $|n|=n_1$, $0 < n_1 < p$, M и Q—целые, $0 < M < M+Q < p$. При $p > 60$ доказать, что

$$\left| \sum_{x=M}^{M+Q-1} e^{\frac{2\pi i a x^n}{p}} \right| < \frac{3}{2} n_1^{\frac{1}{4}} p^{\frac{3}{4}} \ln p.$$

c. Пусть $(a, p)=1$, M_0 и Q_0—целые, $0 < M_0 < M_0+Q_0 \leqslant p$, M и Q—целые, $0 < M < M+Q \leqslant p$, n—целое, $|n|=n_1$, $0 < n_1 < p$, T обозначает число чисел ряда ax^n, $x = M_0, M_0+1, \ldots, M_0+Q_0-1$, сравнимых по модулю p с числами ряда $M, M+1, \ldots, M+Q-1$. Доказать, что при $p > 60$ будем иметь

$$T = \frac{Q_0 Q}{p} + \vartheta \frac{3}{2} n_1^{\frac{1}{4}} p^{\frac{3}{4}} (\ln p)^2; \quad |\vartheta| < 1.$$

Численные примеры к главе VI

1, a. Найти (путем возможно более простых вычислений) показатель, которому принадлежит 7 по модулю 43.

b. Найти показатель, которому принадлежит 5 по модулю 108.

2, a. Найти первообразные корни по модулям 17, 289, 578.

b. Найти первообразные корни по модулям 23, 529, 1058

c. Найти наименьший первообразный корень по модулю 242.

3, a. Составить таблицы индексов по модулю 17.

b. Составить таблицы индексов по модулю 23.

4, a. Найти первообразный корень по модулю 71, применяя указание примера c, § 5.

b. Найти первообразный корень по модулю 191.

5, a. Пользуясь таблицей индексов, указать число решений сравнений:

$\alpha)$ $x^{60} \equiv 79 \pmod{97}$, $\beta)$ $x^{55} \equiv 17 \pmod{97}$, $\gamma)$ $x^{15} \equiv 46 \pmod{97}$.

b. Указать число решений сравнений

$\alpha)$ $3x^{12} \equiv 31 \pmod{41}$, $\beta)$ $7x^7 \equiv 11 \pmod{41}$, $\gamma)$ $5x^{30} \equiv 37 \pmod{41}$.

6, a. Пользуясь таблицей индексов, решить сравнения

$\alpha)$ $x^2 \equiv 59 \pmod{67}$, $\beta)$ $x^{35} \equiv 17 \pmod{67}$, $\gamma)$ $x^{30} \equiv 14 \pmod{67}$.

b. Решить сравнения

$\alpha)$ $23x^5 \equiv 15 \pmod{73}$, $\beta)$ $37x^6 \equiv 69 \pmod{73}$,

$\gamma)$ $44x^{21} \equiv 53 \pmod{73}$.

7, a. Пользуясь теоремой c, § 5, определить число решений сравнений

$\alpha)$ $x^3 \equiv 2 \pmod{37}$, $\beta)$ $x^{16} \equiv 10 \pmod{37}$.

b. Определить число решений сравнений

$\alpha)$ $x^5 \equiv 3 \pmod{71}$, $\beta)$ $x^{21} \equiv 5 \pmod{71}$.

8, a. Пользуясь таблицей индексов, среди вычетов приведенной системы по модулю 19 указать: α) квадратичные нычеты, β) кубические вычеты.

b. Среди вычетов приведенной системы по модулю 37 указать: α) вычеты степени 15, β) вычеты степени 8.

9, a. Среди вычетов приведенной системы по модулю 43 указать: α) числа, принадлежащие показателю 6, β) первообразные корни.

b. Среди вычетов приведенной системы по модулю 61 указать: α) числа, принадлежащие показателю 10, β) первообразные корни.

10. Составить таблицы индексов по модулям:

α) 2. β) 4. γ) 10. δ) 12. ε) 15. ζ) 16. η) 25.

Глава VII

ХАРАКТЕРЫ

§ 1. Определения

а. *Пусть* m — *целое положительное и* c, c_0, c_1, ..., c_k *имеют значения, указанные в* а, § 7, гл. VI, *а* R, R_0, R_1, ..., R_k *обозначают какие-либо корни уравнений*

$$R^c = 1,\ R^{c_0} = 1,\ R^{c_1} = 1,\ \ldots,\ R^{c_k} = 1\ *).$$

При $(a, m) = 1$ *полагаем*

$$\chi(a) = R^{\gamma} R_0^{\gamma_0} R_1^{\gamma_1} \ldots R_k^{\gamma_k}, \qquad (1)$$

где γ, γ_0, γ_1, ..., γ_k — система индексов числа a.

А при $(a, m) > 1$ *полагаем* $\chi(a) = 0$.

Определенная таким образом для всякого целого a *функция* $\chi(a)$ *называется характером по модулю* m.

b. *Если* $R = R_0 = R_1 = \ldots = R_k = 1$, *то* $\chi(a)$ *называется главным характером по модулю* m; *он имеет значение* 1 *при* $(a, m) = 1$ *и значение* 0 *при* $(a, m) > 1$.

с. *Два характера по модулю* m *считаются различными, если по меньшей мере при одном значении* a *их значения не совпадают.*

§ 2. Важнейшие свойства характеров

а. В первую очередь отметим три следующих свойства характеров:

α) $\chi(1) = 1$.

β) $\chi(a_1 a_2) = \chi(a_1)\,\chi(a_2)$.

γ) *Из* $a_1 = a_2 \pmod m$ *следует* $\chi(a_1) = \chi(a_2)$.

---

*) Корни уравнения $R^\sigma = 1$ суть числа $e^{\frac{2\pi i s}{\sigma}}$; $s = 0, 1, \ldots, \sigma - 1$.

Действительно, свойство α) найдем из (1), § 1, положив $a=1$. При $(a_1a_2,\ m)=1$ равенство β) следует из (1), § 1 и теоремы с, § 7, гл. VI, а при $(a_1a_2,\ m)>1$ оно обращается в тождество $0=0$. Наконец, свойство γ) является следствием определения системы индексов, данного в § 7, гл. VI.

b. *Число различных характеров по модулю m равно $\varphi(m)$.*

Действительно, указанным в **a**, § 1 способом получим $cc_0c_1\ldots c_k$ характеров. При этом при $\varphi(m)>1$ у каких-либо двух из них, пусть у $\chi'(a)$ и $\chi''(a)$, будут различны значения R' и R'' по меньшей мере одного из корней $R,\ R_0,\ R_1,\ \ldots,\ R_k$. Для числа a, у которого все индексы равны нулю, кроме лишь одного, отвечающего этим R' и R'', равного 1, будем иметь $\chi'(a)=R'$, $\chi''(a)=R''$. Поэтому характеры $\chi'(a)$ и $\chi''(a)$ различны и наше утверждение верно.

c. *Имеем*

$$\sum_{a=0}^{m-1}\chi(a)=\begin{cases}\varphi(m) & \text{для главного характера,}\\ 0 & \text{для других характеров.}\end{cases}$$

Действительно, применяя формулу (1), § 1, находим

$$\sum_{a=0}^{m-1}\chi(a)=\sum_{\gamma}R^{\gamma}\sum_{\gamma_0}R_0^{\gamma_0}\sum_{\gamma_1}R_1^{\gamma_1}\ldots\sum_{\gamma_k}R_k^{\gamma_k},$$

где $\gamma,\ \gamma_0,\ \gamma_1,\ \ldots,\ \gamma_k$ пробегают наименьшие неотрицательные вычеты по модулям $c,\ c_0,\ c_1,\ \ldots,\ c_k$.

Если $\chi(a)$ — главный характер, то правая часть равна $cc_0c_1\ldots c_k=\varphi(m)$. Если же $\chi(a)$ — не главный характер, то по меньшей мере один из корней $R,\ R_0,\ R_1,\ \ldots,\ R_k$ не равен 1 и соответствующая ему сумма правой части равна нулю. А вместе с нею равна нулю и вся правая часть.

d. *Распространяя суммирование на все $\varphi(m)$ различных характеров, имеем*

$$\sum_{\chi}\chi(a)=\begin{cases}\varphi(m) & \text{при } a\equiv 1 \pmod m.\\ 0 & \text{в противном случае.}\end{cases}$$

Действительно, теорема верна при $(a,\ m)>1$, так как в этом случае имеем $\chi(a)=0$. Теорема верна и при $a\equiv 1 \pmod m$, т. е. в случае $\gamma=\gamma_0=\gamma_1=\ldots=\gamma_k=0$;

это следует из α), **a**, § 2 и **b**, § 2. Остается рассмотреть лишь случай $(a, m)=1$, но при условии, что a не сравнимо с 1 по модулю m, т. е. при условии, что среди чисел γ, γ_0, γ_1, ..., γ_k имеется по меньшей мере одно γ', не равное нулю. Но из (1), § 1 следует равенство

$$\sum_{\chi} \chi(a) = \sum_{R} R^{\gamma} \sum_{R_0} R_0^{\gamma_0} \sum_{R_1} R_1^{\gamma} \ldots \sum_{R_k} R_k^{\gamma_k},$$

которое и доказывает теорему, так как среди сомножителей его правой части имеется сумма, отвечающая указанному γ', равная нулю.

e. Характеры по модулю m обладают следующими свойствами:

α) *Если* $\chi_0(a)$ *и* $\chi(a)$ *— характеры,* $\chi_0(a)\chi(a)$ *— также характер.*

β) *Если* $\chi_0(a)$ *— характер и* $\chi(a)$ *пробегает все характеры, то* $\chi_0(a)\chi(a)$ *также пробегает все характеры.*

γ) *При* $(l, m)=1$ *имеем*

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \begin{cases} \varphi(m) & \text{в случае } a \equiv l \pmod m, \\ 0 & \text{в противном случае.} \end{cases}$$

Действительно, пусть R', R_0', R_1', ..., R_k' и R, R_0, R_1, ..., R_k — значения корней, входящих в определение характеров $\chi_0(a)$ и $\chi(a)$. Тогда $\chi_0(a)\chi(a)$ — характер, у которого соответствующими значениями корней являются $R'R$, $R_0'R_0$, $R_1'R_1$, ..., $R_k'R_k$. При этом, если каждое R, R_0, R_1, ..., R_k пробегает все свои значения, то и каждое $R'R$, $R_0'R_0$, $R_1'R_1$, ..., $R_k'R_k$ в некотором порядке пробегает те же самые значения. Свойства α) и β) установлены.

Далее, найдя l' из условия $ll' \equiv 1 \pmod m$, выводим

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \sum_{\chi} \frac{\chi(a)\chi(l')}{\chi(l)\chi(l')} = \sum_{\chi} \chi(al') = \begin{cases} \varphi(m) & \text{в случае } a \equiv l \pmod m, \\ 0 & \text{в противном случае.} \end{cases}$$

Свойство γ) также установлено.

f. *Характером по модулю m является всякая функция $\psi(a)$, определенная для всех целых a и удовлетворяющая условиям:*

$\alpha)$ $\psi(a)=0$, *если* $(a, m)>1$,

$\beta)$ $\psi(a)$ *не равна тождественно нулю*,

$\gamma)$ $\psi(a_1a_2)=\psi(a_1)\psi(a_2)$,

$\delta)$ $\psi(a_1)=\psi(a_2)$, *если* $a_1\equiv a_2 \pmod m$.

Действительно, согласно $\beta)$ существует такое a_0, для которого $\psi(a_0)$ не равно нулю. Из $a_0=a_0\cdot 1$ согласно $\gamma)$ находим $\psi(a_0)=\psi(a_0)\cdot\psi(1)$. Отсюда, разделив почленно на $\psi(a_0)$, получим $\psi(1)=1$.

Пусть a — любое число с условием $(a, m)=1$. Определив a' сравнением $aa'\equiv 1 \pmod m$, согласно $\gamma)$ имеем $\psi(a)\psi(a')=1$. Отсюда следует, что $\psi(a)$ не равно нулю.

Заставляя a пробегать приведенную систему вычетов по модулю m, а χ пробегать все $\varphi(m)$ различных характеров, рассмотрим сумму

$$H=\sum_a\sum_\chi \frac{\chi(a)}{\psi(a)}=\sum_a U_a;\qquad U_a=\sum_\chi \frac{\chi(a)}{\psi(a)}.$$

Замечая (**d**), что $U_a=\varphi(m)$ при $a\equiv 1 \pmod m$ и $U_a=0$ в противном случае, получим $H=\varphi(m)$, откуда, представляя H в виде

$$H=\sum_\chi V_\chi;\qquad V_\chi=\sum_a \frac{\chi(a)}{\psi(a)},$$

убедимся в существовании по меньшей мере одного $\chi=\chi_0$ с V_χ, не равным нулю. При этом при каждом a_1 с условием $(a_1, m)=1$ будем иметь

$$V_{\chi_0}=\sum\frac{\chi_0(a)}{\psi(a)}=\sum\frac{\chi_0(a_1a)}{\psi(a_1a)}=\frac{\chi_0(a_1)}{\psi(a_1)}V_{\chi_0};$$

$$1=\frac{\chi_0(a_1)}{\psi_0(a_1)},\quad \chi_0(a_1)=\psi(a_1);$$

отсюда и из α) следует, что функция $\psi(a_1)$ для каждого a_1 совпадает с характером $\chi_0(a_1)$.

Пример 1. Построим все $\varphi(5)=4$ характеров по модулю 5 (для каждого характера выписываем значения, отвечающие числам полной системы вычетов по модулю 5). Здесь корнями уравнения $\rho^4=1$ будут

$$\rho_0=e^{2\pi i\frac{0}{4}}=1,\quad \rho_1=e^{2\pi i\frac{1}{4}}=i,$$

$$\rho_2=e^{2\pi i\frac{2}{4}}=-1,\quad \rho_3=e^{2\pi i\frac{3}{4}}=-i.$$

А таблица индексов по модулю 5 (с основанием 2) будет

N	1	2	3	4
γ_1	0	1	3	2

Поэтому таблица значений характеров, отвечающих корням ρ_0, ρ_1, ρ_2, ρ_3, будет

N	0	1	2	3	4
χ_0	0	1	1	1	1
χ_1	0	1	i	$-i$	-1
χ_2	0	1	-1	-1	1
χ_3	0	1	$-i$	$-i$	-1

Пример 2. Укажем все $\varphi(21)=2\cdot 6=12$ характеров по модулю 21. Здесь корень R_{c_1} уравнения $R_{c_1}^2=1$ имеет 2 значения: $R_{c_1}=e^{2\pi i\frac{s}{2}}$; $s=0$, 1, а корень R_{c_2} уравнения $R_{c_2}^6=1$ имеет 6 значений: $R_{c_2}=e^{2\pi i\frac{s}{6}}$: $s=0, \ldots, 5$. При

этом характер, отвечающий какой-либо из 12 пар значений R_{c_1} и R_{c_2}, будет (пример 4, е, § 7, гл. VI):

N	0	1	2	3	4	5	6	7	8	9
χ	0	1 R_{c_2}	R_{c_1} $R_{c_2}^2$	0	1 $R_{c_2}^4$	R_{c_1} $R_{c_2}^5$	0	0	R_{c_1} 1	0

N	10	11	12	13	14	15	16	17	18	19	20
χ	1 R_{c_2}	R_{c_1} $R_{c_2}^4$	0	1 $R_{c_2}^2$	0	0	1 $R_{c_2}^3$	R_{c_1} R_{c_2}	0	1 $R_{c_2}^5$	R_{c_1} $R_{c_2}^3$

Здесь значение характера, отвечающее какому-либо числу N, взаимно простому с 21, получаются перемножением степеней чисел R_{c_1} и R_{c_2}, помещенных ниже этого числа N.

Вопросы к главе VII

1. Пусть $\chi(a)$ — неглавный характер по модулю p, отвечающий корню $R=e^{2\pi i\frac{s}{p-1}}$ уравнения $R^{p-1}=1$ (следовательно, при a, кратном p, как $\chi(a)$, так и $\overline{\chi(a)}=(\chi(a))^{-1}$ считаются равными нулю).

α) При $(k, p)=1$ доказать, что

$$\sum_{x=1}^{p-1}\overline{\chi(x)}\,\chi(x+k)=-1.$$

β) Пусть Q — целое, $1<Q<p$,

$$S=\sum_{x=0}^{p-1}\left|\sum_{z=0}^{Q-1}\chi(x+z)\right|^2.$$

Доказать, что $S=(p-Q)\,Q$.

2. Пусть $\chi(a)$ — характер по модулю p,

$$U_{a,p}=\sum_{x=1}^{p-1}\chi(x)\,e^{2\pi i\frac{ax}{p}}.$$

α) При $(a, p)=1$ доказать, что $|U_{a,p}|=\sqrt{p}$ для неглавного характера и $U_{a,p}=-1$ для главного характера.

β) Пусть $\chi(a)$ — неглавный характер по модулю p и $(a, p)=1$.

Доказать, что

$$(\chi(a))^{-1}=\frac{U_{a,p}}{U_{1,p}}.$$

γ) Пусть p имеет вид $p=4m+1$ (следовательно, $p-1=4m$), $R=e^{2\pi i\frac{m}{p-1}}=e^{2\pi i\frac{1}{4}}$,

$$S=\sum_{x=1}^{p-1}\chi(x^2+x).$$

Доказать (ср. вопросы 9, а и 9, с, гл. V), что $p=A^2+B^2$, где A и B — целые, определяемые равенством $S=A+Bi$.

δ) Пусть n — делитель числа $p-1$, $1<n<p-1$, $\nu=\frac{1}{n}$, $(a, p)=1$, наконец, x_s пробегает числа приведенной системы вычетов по модулю p с условием $\operatorname{ind} x_s\equiv s \pmod n$. Доказать, что

$$\sum_{x_s}e^{2\pi i\frac{ax_s}{p}}=-\nu+\theta_s(1-\nu)\sqrt{p};\quad |\theta_s|=1.$$

3. Пусть n — целое, $n>2$, $(a, m)=1$,

$$S_{a,m}=\sum_x e^{2\pi i\frac{ax^n}{m}},\quad S'_{a,m}=\sum_\xi e^{2\pi i\frac{a\xi^n}{m}},$$

где x пробегает полную, а ξ пробегает приведенную системы вычетов по модулю m (ср. вопрос 12, а, гл. III).

α) Пусть $\delta=(n, p-1)$. Доказать, что

$$|S_{a,p}|\leqslant(\delta-1)\sqrt{p}.$$

β) Пусть s — целое, $1<s\leqslant n$, $(n, p)=1$. Доказать, что

$$S_{a,p^s}=p^{s-1},\quad S'_{a,p^s}=0.$$

γ) Пусть n — целое, $s>n$. Доказать, что

$$S_{a,p^s}=p^{n-1}S_{a,p^{s-n}},\quad S'_{a,p^s}=0.$$

δ) Доказать, что

$$|S_{a,m}|<Cm^{1-\frac{1}{n}},$$

где C зависит только от n.

4. Пусть M и Q — целые, $0<M<M+Q\leqslant p$, $p>60$, $\chi(a)$ — неглавный характер по модулю p.

α) Доказать, что

$$\left|\sum_{x=M}^{M+Q-1}\chi(x)\right|<\sqrt{p}\,(\ln p-1).$$

β) Пусть n — делитель числа $p-1$, $1 < n < p-1$, $\nu = \frac{1}{n}$, $p > 36n^2$, наконец, x_s пробегает числа приведенной системы вычетов по модулю p с условием $\operatorname{ind} x_s \equiv s \pmod n$. Доказать, что число чисел x_s, заключенных среди чисел $M, \ldots, M+Q-1$, выражается формулой

$$T = \frac{Q}{n} + \theta\sqrt{p}\,(\ln p - 1).$$

γ) При условиях вопроса β) показать, что при $Q = [8n\sqrt{p}]$ среди чисел $M, \ldots, M+Q-1$ находится по меньшей мере одно число x_s.

δ) Пусть k — число простых делителей числа $p-1$ и H — число первообразных корней по модулю p, заключенных среди чисел $M, \ldots, M+Q-1$. Доказать, что

$$H = \frac{\varphi(p-1)}{p-1} Q + \theta 2^k \sqrt{p} \ln p; \quad |\theta| < 1.$$

ε) Пусть M_1 и Q_1 — целые, $0 < M_1 < M_1 + Q_1 \leqslant p-1$, J — число чисел ряда $\operatorname{ind} M, \ldots, \operatorname{ind}(M+Q-1)$, заключенных среди чисел ряда $M_1, \ldots, M_1+Q_1-1$. Доказать, что

$$J = \frac{QQ_1}{p-1} + \theta\sqrt{p}\,(\ln p)^2; \quad |\theta| < 1.$$

η) Доказать существование постоянного p_0 с условием: если $p > p_0$, n — делитель $p-1$, $1 < n < p-1$, то наименьший из положительных невычетов степени n по модулю p будет

$$< h; \quad h = p^{\frac{1}{c}} (\ln p)^2, \quad c = 2e^{1-\frac{1}{n}}.$$

5. Пусть $m > 1$, $(a, m) = 1$, n — целое, $n > 0$, K — число решений сравнения $x^n \equiv 1 \pmod m$

$$S = \sum_{x=1}^{m-1} \chi(x)\, e^{2\pi i \frac{ax^n}{m}}.$$

В случае, когда $\chi(x)$ — неглавный характер по модулю m, доказать, что

$$S < K\sqrt{m}.$$

6. Пусть g пробегает первообразные корни по модулю p, заключенные в приведенной системе вычетов, $(a, p) = 1$, k — число различных простых делителей числа $p-1$ и $S = \sum_g{}' e^{2\pi i \frac{ag}{p}}$.

α) Доказать, что

$$|S| \leqslant \frac{9}{8} \frac{\varphi(p-1)}{p-1} 2^k \sqrt{p}.$$

β) Пусть M и Q — целые, $0 < M < M+Q \leqslant p$. Доказать, что число T первообразных корней, находящихся в ряде $M, \ldots, M+Q-1$, выражается формулой

$$T = \frac{\varphi(p-1)}{p-1}\left(Q + \theta \frac{9}{8} 2^k \sqrt{p}\right), \qquad |\theta| < 1.$$

Численные примеры к главе VII

1. Указать все характеры по модулям:
α) 2. β) 4. γ) 8. δ) 9. ε) 10. η) 40.

РЕШЕНИЯ ВОПРОСОВ

Решения к главе I

1. Остаток от деления $ax+by$ на d, имея вид $ax'+by'$ и будучи меньше d, непременно равен нулю. Поэтому d — делитель всех чисел вида $ax+by$ и, в частности, общий делитель чисел $a\cdot 1+b\cdot 0=a$ и $a\cdot 0+b\cdot 1=b$. С другой стороны, выражение для d показывает, что всякий общий делитель чисел a и b делит d. Поэтому $d=(a, b)$ и верна теорема 1, d, § 2. Теоремы e, § 2 выводятся так. наименьшее положительное число вида $amx+bmy$ есть amx_0+bmy_0; наименьшее положительное число вида $\frac{a}{\delta}x+\frac{b}{\delta}y$ есть $\frac{a}{\delta}x_0+\frac{b}{\delta}y_0$. Обобщение этих результатов тривиально.

2. При $p=2$ утверждение очевидно. Пусть $p>2$ и утверждение справедливо для всех простых чисел, меньших p. Докажем его для p. Если a не делится на p, b не делится на p, то по с. § 1 $a=a_2p+a_1$, $0<a_1<p$, $b=b_2p+b_1$, $0<b_1<p$. Следовательно, по 2, § 1 a_1b_1 делится на p, т. е.

$$a_1b_1=pm, \quad m \text{ — натуральное число.}$$

Каждый простой делитель чисел a_1, b_1 меньше p, поэтому по индукционному предположению он делит m. Производя сокращения, приходим к равенству

$$1=pm_1,$$

которое противоречиво, а это и доказывает наше утверждение.

3, a. Действительно, всегда будем иметь

$$\left|\frac{c}{d}-\delta_{s+1}\right|<|\delta_s-\delta_{s+1}|,$$

откуда найдем

$$\frac{1}{dQ_{s+1}}<\frac{1}{Q_sQ_{s+1}}, \quad d>Q_s.$$

b. При $n\leqslant 6$ теорема очевидна, поэтому предполагаем $n>6$. Имеем

$$\xi=\frac{1+\sqrt{5}}{2}=1{,}618\ldots; \quad \log_{10}\xi=0,\ 2,\ \ldots;$$

$$Q_2\geqslant 1 \quad =g_1=1,$$

$$Q_3\geqslant Q_2+1 \quad \geqslant g_2=2>\xi,$$

$$Q_4\geqslant Q_3+Q_2 \quad \geqslant g_3=g_2+g_1>\xi+1=\xi^2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Q_n\geqslant Q_{n-1}+Q_{n-2}\geqslant g_{n-1}=g_{n-2}+g_{n-3}>\xi^{n-3}+\xi^{n-4}=\xi^{n-2}.$$

Отсюда

$$N > \xi^{n-2}, \quad n < \frac{\log_{10} N}{\log_{10} \xi} + 2 < 5k + 2; \quad n \leqslant 5k + 1.$$

4, a. Для дробей $\frac{0}{1}$ и $\frac{1}{1}$ имеем $0 \cdot 1 - 1 \cdot 1 = -1$. Вставляя между дробями $\frac{A}{B}$ и $\frac{C}{D}$ с условием $AD - BC = -1$ дробь $\frac{A+C}{B+D}$, имеем $A(B+D) - B(A+C) = (A+C)D - (B+D)C = -1$. Поэтому верно утверждение, отмеченное в конце вопроса. Существование дроби $\frac{k}{l}$ с условиями $\frac{a}{b} < \frac{k}{l} < \frac{c}{d}$, $l \leqslant \tau$ невозможно. В противном случае мы имели бы

$$\frac{k}{l} - \frac{a}{b} \geqslant \frac{1}{lb}; \quad \frac{c}{d} - \frac{k}{l} \geqslant \frac{1}{ld}; \quad \frac{c}{d} - \frac{a}{b} \geqslant \frac{b+d}{lbd} > \frac{1}{bd}.$$

b. Очевидно, достаточно рассматривать случай $0 \leqslant \alpha < 1$. Пусть $\frac{a}{b} \leqslant \alpha < \frac{c}{d}$, где $\frac{a}{b}$ и $\frac{c}{d}$ — соседние дроби ряда Фарея, отвечающего τ. Возможны два случая:

$$\frac{a}{b} \leqslant \alpha < \frac{a+c}{b+d}; \quad \frac{a+c}{b+d} \leqslant \alpha < \frac{c}{d}.$$

Поэтому верно одно из двух неравенств

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b(b+d)}; \quad \left|\alpha - \frac{c}{d}\right| \leqslant \frac{1}{d(b+d)},$$

откуда ввиду $b + d > \tau$ указанная теорема следует непосредственно.

c. В случае, когда α — несократимая дробь $\alpha = \frac{a}{b}$ с условием $b \leqslant \tau$, за $\frac{P}{Q}$ можно принять саму дробь $\frac{a}{b}$. В противном случае за $\frac{P}{Q}$ можно принять подходящую дробь $\frac{P_s}{Q_s}$ с условием $Q_s \leqslant \tau < Q_{s+1}$.

5, a. Нечетные простые числа при делении на 4 дают остаток 1 или же 3. Произведение чисел вида $4m+1$ имеет вид $4m+1$. Поэтому число $4p_1 \ldots p_k - 1$, где $p_1, \ldots, p_k$ — простые вида $4m+3$, наверно имеет простой делитель q вида $4m+3$. При этом q не совпадает ни с одним из чисел $p_1, \ldots, p_k$.

b. Простые числа, превосходящие 3, имеют вид $6m+1$ или же $6m+5$. Число $6p_1 \ldots p_k - 1$, где $p_1, \ldots, p_k$ — простые вида $6m+5$, наверно имеет простой делитель q вида $6m+5$. При этом q не совпадает ни с одним из чисел $p_1, \ldots, p_k$.

6. Пусть $p_1, \ldots, p_k$ — какие-либо k простых чисел и N — целое с условиями $2 < N$, $(3 \ln N)^k < N$. Число чисел a ряда $1, 2, \ldots, N$, каноническое разложение которых имеет вид $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, ввиду

$\alpha_s \leqslant \frac{\ln N}{\ln 2}$, не больше чем

$$\left(\frac{\ln N}{\ln 2}+1\right)^k < (3\ln N)^k < N.$$

Поэтому в ряде 1, 2, ..., N найдутся числа, в каноническое разложение которых входят простые, отличные от $p_1, \ldots, p_k$.

7. Например, такие последовательности получим при

$$M = 2\cdot 3 \ldots (K+1)\,t+2; \quad t = 1, 2, \ldots$$

8. Взяв целое x_0 с условием, что при $x \geqslant x_0$, $f(x) > 1$ и $f'(x) > 0$, положим $f(x_0) = X$. Составными (кратными X) будут все числа $f(x_0 + Xt)$; $t = 1, 2, \ldots$

9, a. При наличии (1) одно из чисел x, y, пусть именно x, будет четным; из

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2}\,\frac{z-y}{2},$$

где, очевидно, $\left(\frac{z+y}{2}, \frac{z-y}{2}\right) = 1$, убеждаемся в существовании положительных целых u и v с условиями

$$\frac{x}{2} = uv, \quad \frac{z+y}{2} = u^2, \quad \frac{z-y}{2} = v^2.$$

Отсюда следует необходимость условий, указанных в вопросе.

Достаточность этих условий очевидна.

b. Условимся здесь обозначать буквами лишь целые положительные числа. Допустив существование систем x, y, z с условиями $x^4 + y^4 = z^2$, $x > 0$, $y > 0$, $z > 0$, $(x, y, z) = 1$, выберем из них систему с наименьшим z. Предполагая x четным, найдем $x^2 = 2uv$, $y^2 = u^2 - v^2$, $u > v \geqslant 1$, $(u, v) = 1$, где v — четное (при четном u было бы $y^2 = 4N+1$, $u^2 = 4N_1$, $v^2 = 4N_2 + 1$, $4N+1 = 4N_1 - 4N_2 - 1$, что невозможно). Отсюда $u = z_1^2$, $v = 2w^2$, $y^2 + 4w^4 = z_1^4$, $2w^2 = 2u_1v_1$, $u_1 = x_1^2$, $v_1 = y_1^2$, $x_1^4 + y_1^4 = z_1^2$, что ввиду $z_1 < z$ невозможно.

Из неразрешимости уравнения $x^4 + y^4 = z^2$ как частный случай, очевидно, следует и неразрешимость уравнения $x^n + y^n = t^n$ в целых положительных x, y, t.

10. Полагая $x = \frac{k}{l}$; $(k, l) = 1$, находим

$$k^n + a_1k^{n-1}l + \ldots + a_nl^n = 0.$$

Поэтому k^n кратно l и, следовательно, $l = 1$.

11, a. Пусть k — наибольшее целое с условием $2^k \leqslant n$ и P — произведение всех нечетных чисел, не превосходящих n. Число $2^{k-1}PS$ представится суммою, все слагаемые которой, кроме $2^{k-1}P\frac{1}{2^k}$, суть целые числа.

b. Пусть k — наибольшее целое с условием $3^k \leqslant 2n+1$ и P — произведение всех взаимно простых с 6 чисел, не превосходящих

$2n+1$. Число $3^{k-1}PS$ представится суммою, все слагаемые которой, кроме $3^{k-1}P\frac{1}{3^k}$, суть целые числа.

12. При $n \leqslant 8$ теорема проверяется непосредственно. Поэтому достаточно, считая при $n > 8$ теорему верной для биномов $a+b$, $(a+b)^2$, ..., $(a+b)^{n-1}$, доказать справедливость теоремы и для бинома $(a+b)^n$. Но коэффициенты разложения этого бинома за исключением крайних, равных 1, суть числа

$$\frac{n}{1}, \quad \frac{n(n-1)}{1\cdot 2}, \quad \ldots, \quad \frac{n(n-1)\ldots 2}{1\cdot 2\ldots(n-1)}.$$

Для нечетности же всех этих чисел необходимо и достаточно, чтобы нечетными были крайние из них, как раз равные n, и чтобы также нечетными были числа, получаемые вычеркиванием нечетных сомножителей из числителей и знаменателей оставшихся чисел. Но, полагая $n=2n_1+1$, эти числа можно представить членами ряда

$$\frac{n_1}{1}, \quad \frac{n_1(n_1-1)}{1\cdot 2}, \quad \ldots, \quad \frac{n_1(n_1-1)\ldots 2}{1\cdot 2\ldots(n_1-1)}.$$

Последние же ввиду $n_1 < n$ будут все нечетными тогда и только тогда, когда n_1 имеет вид 2^k-1, т. е. когда n имеет вид $2(2^k-1)+1 = 2^{k+1}-1$.

Решения к главе II

1, a. На ординате точки кривой $y=f(x)$ с абсциссою x лежит $[f(x)]$ целых точек указанной области.

b. Указанное равенство следует из $T_1+T_2=T$, где T_1, T_2, T обозначают числа целых точек областей

$$0 < x < \frac{Q}{2}, \quad 0 < y < \frac{P}{Q}x;$$

$$0 < y < \frac{P}{2}, \quad 0 < x \leqslant \frac{Q}{P}y;$$

$$0 < x < \frac{Q}{2}, \quad 0 < y < \frac{P}{2}.$$

c. Указанное равенство следует из

$$T = 1 + 4(T_1+T_2+T_3-T_4),$$

где T_1, T_2, T_3, T_4 обозначают числа целых точек областей

$$x=0, \qquad 0 < y \leqslant r;$$

$$0 < x \leqslant \frac{r}{\sqrt{2}}, \quad 0 < y \leqslant \sqrt{r^2-x^2};$$

$$0 < y \leqslant \frac{r}{\sqrt{2}}, \quad 0 < x \leqslant \sqrt{r^2-y^2};$$

$$0 < x \leqslant \frac{r}{\sqrt{2}}, \quad 0 < y \leqslant \frac{r}{\sqrt{2}}.$$

d. Указаяное равенство следует из $T = I_1 + I_2 - I_3$, где T_1, T_2, T_3 обозначают числа целых точек областей

$$0 < x \leqslant \sqrt{n}, \quad 0 < y \leqslant \frac{n}{x};$$

$$0 < y \leqslant \sqrt{n}, \quad 0 < x \leqslant \frac{n}{y};$$

$$0 < x \leqslant \sqrt{n}, \quad 0 < y \leqslant \sqrt{n}.$$

e. В случае треугольника, не имеющего других целых точек, кроме вершин, теорема тривиальна. К этому же случаю сводится и случай каждого выпуклого многоугольника. А случай невыпуклого многоугольника путем соединения прямолинейным отрезком некоторой пары его вершин можно свести к случаю многоугольника более простого вида.

2. Число целых положительных чисел, не превосходящих n, равно $[n]$. Каждое из них единственным способом представляется в виде xk^m, где k—целое положительное; при этом данному x отвечает $\left[\sqrt[m]{\frac{n}{x}}\right]$ чисел такого вида.

3. Докажем необходимость указанных условий. Число значений x с условием $[\alpha x] \leqslant N$ можно представить в виде $\frac{N}{\alpha} + \lambda$; $0 \leqslant \lambda < \frac{1}{\alpha}$, а число значений y с условием $[\beta y] \leqslant N$ можно представить в виде $\frac{N}{\beta} + \lambda_1$; $0 \leqslant \lambda_1 < \frac{1}{\beta}$. Из $\frac{N}{\alpha} + \lambda + \frac{N}{\beta} + \lambda_1 = N$, деля на N и переходя к пределу, при $N \to \infty$ получим $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Последнее равенство при рациональном $\alpha = \frac{a}{b}$ $(a > b > 0)$ дало бы $[\alpha b] = [\beta(a-b)]$. Поэтому α и β не могут быть рациональными.

Пусть указанные условия выполнены. Пусть c—натуральное число. Пусть $x_0 = \frac{c}{\alpha} + \xi$ и $y_0 = \frac{c}{\beta} + \eta$—наименьшие целые числа с условием $x_0 > \frac{c}{\alpha}$, $y_0 > \frac{c}{\beta}$. Очевидно, $[\alpha x]$ не равно c при x, не равном x_0, и $[\beta y]$ не равно c при y, не равном y_0; при этом $0 < \xi < 1$, $0 < \eta < 1$, $\alpha\xi$ и $\beta\eta$—иррациональные. Ввиду $x_0 + y_0 = c + \xi + \eta$ имеем $\xi + \eta = 1$, $\frac{\alpha\xi}{\alpha} + \frac{\beta\eta}{\beta} = 1$. Поэтому одно и только одно из чисел $[\alpha x_0]$ и $[\beta y_0]$ равно c.

4,а. Упомянутые разности при $\{\alpha x_t\} > 0$ равны

$$\{\alpha x_1\}, \{\alpha(x_2 - x_1)\}, \ldots, \{\alpha(x_t - x_{t-1})\}, \{-\alpha x_t\}.$$

Они неотрицательные, их сумма равна 1, их число равно $t+1$. Поэтому по меньшей мере одна из этих разностей не превосходит $\frac{1}{t+1} < \frac{1}{\tau}$. Но она имеет вид $\{\alpha x'\} = \alpha x' - y'$, где x'—целое число

с условием $0 < |x'| \leqslant \tau$ и $y' = [\alpha x']$. Поэтому, обозначая буквой h то из чисел 1 и -1, при котором $hx' > 0$, будем иметь $|\alpha hx' - hy'| < \frac{1}{\tau}$. Отсюда, обозначая буквами Q и P частные от деления hx' и hy' на (hx', hy'), получим

$$|\alpha Q - P| < \frac{1}{\tau}; \quad 0 < Q \leqslant \tau,$$

откуда и следует упомянутая в вопросе теорема.

b. Полагая $t_1 = [\tau_1]$, $t_2 = [\tau_2]$, ..., $t_k = [\tau_k]$ и заставляя $x_1, x_2, \ldots, x_k$ пробегать значения

$$x_1 = 0, 1, \ldots; t_1; \quad x_2 = 0, 1, \ldots, t_2; \ldots; x_k = 0, 1, \ldots, t_k,$$

рассмотрим ряд, образованный расположенными в неубывающем порядке числами $\{\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_k x_k\}$ и числом 1. Составляя разности, образованные соседними такими числами, получим $(t_1+1) \times (t_2+1) \ldots (t_k+1)$ разностей. По меньшей мере одна из них не превосходит

$$\frac{1}{(t_1+1)(t_2+1)\ldots(t_k+1)} < \frac{1}{\tau_1\tau_2\ldots\tau_k}.$$

Но она имеет вид $\{\alpha_1 x_1' + \alpha_2 x_2' + \ldots + \alpha_k x_k'\}$, где $x_1', x_2', \ldots, x_k'$ — целые числа с условиями $|x_1'| \leqslant \tau_1$, $|x_2'| \leqslant \tau_2$, ..., $|x_k'| \leqslant \tau_k$, не равные нулю одновременно. Полагая $[\alpha_1 x_1' + \alpha_2 x_2' + \ldots + \alpha_k x_k'] = y'$ и обозначая символами $\xi_1, \xi_2, \ldots, \xi_k, \eta$ частные от деления $x_1', x_2', \ldots, x_k', y'$ на $(x_1', x_2' \ldots, x_k', y')$, получим

$$|\alpha_1\xi_1 + \alpha_2\xi_2 + \ldots + \alpha_k\xi_k - \eta| < \frac{1}{\tau_1\tau_2\ldots\tau_k},$$

что и доказывает указанную в вопросе теорему.

5. Имеем $\alpha = cq + r + \{\alpha\}$; $0 \leqslant r < c$,

$$\left[\frac{|\alpha|}{c}\right] = \left[q + \frac{r}{c}\right] = q, \quad \left[\frac{\alpha}{c}\right] = \left[q + \frac{r + \{\alpha\}}{c}\right] = q.$$

6,a. Имеем $[\alpha+\beta+\ldots+\lambda] = [\alpha]+[\beta]+\ldots+[\lambda]+[\{\alpha\}+\{\beta\}+\ldots+\{\lambda\}]$

b. Простое p входит в $n!$, $a!$, ..., $l!$ с показателями

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots, \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \ldots, \ldots, \left[\frac{l}{p}\right] + \left[\frac{l}{p^2}\right] + \ldots$$

При этом

$$\left[\frac{n}{p^s}\right] \geqslant \left[\frac{a}{p^s}\right] + \ldots + \left[\frac{l}{p^s}\right].$$

7. Допуская, что число a с указанными свойствами существует, представим его в виде

$$a = q_k p^{k+1} + q_{k-1} p^k + \ldots + q_1 p^2 + q_0 p + q';$$

$0 < q_k < p$, $0 \leqslant q_{k-1} < p$, $\ldots$, $0 \leqslant q_1 < p$, $0 \leqslant q_0 < p$, $0 \leqslant q' < p$.

Согласно b, § 1 должно быть

$$h = q_k u_k + q_{k-1} u_{k-1} + \ldots + q_1 u_1 + q_0 u_0.$$

Далее при любом $s = 1, 2, \ldots, m$ имеем

$$q_{s-1} u_{s-1} + q_{s-2} u_{s-2} + \ldots + q_1 u_1 + q_0 u_0 < u_s.$$

Поэтому последнее выражение для h должно полностью совпасть с указанным в вопросе.

8,a. Пусть x_1 — целое, $Q \leqslant \alpha < \beta \leqslant R$, $x_1 < \alpha < \beta < x_1 + 1$; интегрированием по частям находим

$$-\int_\alpha^\beta f(x)\,dx = \int_\alpha^\beta \rho'(x) f(x)\,dx =$$

$$= \rho(\beta) f(\beta) - \rho(\alpha) f(\alpha) - \sigma(\beta) f'(\beta) + \sigma(\alpha) f'(\alpha) + \int_\alpha^\beta \sigma(x) f''(x)\,dx.$$

В частности, при $Q \leqslant x_1$, $x_1 + 1 \leqslant R$, переходя к пределу, имеем

$$-\int_{x_1}^{x_1+1} f(x)\,dx = -\frac{1}{2} f(x_1 + 1) - \frac{1}{2} f(x_1) + \int_{x_1}^{x_1+1} \sigma(x) f''(x)\,dx.$$

Указанная формула теперь получается без всякого труда.

b. Переписав формулу вопроса **a** в виде

$$\sum_{Q < x \leqslant R} f(x) = \int_Q^R f(x)\,dx + \rho(R) f(R) - \rho(Q) f(Q) -$$

$$- \sigma(R) f'(R) + \sigma(Q) f'(Q) + \int_Q^\infty \sigma(x) f''(x)\,dx - \int_R^\infty \sigma(x) f''(x)\,dx,$$

убеждаемся в справедливости указанной формулы.

c. Применяя результат вопроса b, находим

$$\ln 1 + \ln 2 + \ldots + \ln n = C + n \ln n - n + \frac{1}{2} \ln n + \int_n^\infty \frac{\sigma(x)}{x^2}\,dx - n \ln n - n + O(\ln n).$$

9,a, α) Имеем (b, § 1)

$$\ln([n]!) = \sum_{p \leqslant n} \left(\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots \right) \ln p. \qquad (1)$$

Здесь правая часть представляет сумму значений функции $\ln p$, распространенную на целые точки (p, s, u) с простыми p области

$p>0$, $s>0$, $0<u\leqslant\frac{n}{p^s}$. Часть этой суммы, отвечающая данным s и u, равна $\Theta\left(\sqrt[s]{\frac{n}{u}}\right)$; часть, отвечающая данному u, равна $\psi\left(\frac{n}{u}\right)$.

β) Применяя при $n\geqslant 2$ результат вопроса α), имеем

$$\ln([n]!)-2\ln\left(\left[\frac{n}{2}\right]!\right)=$$
$$=\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\ldots\geqslant\psi(n)-\psi\left(\frac{n}{2}\right).$$

Полагая $\left[\frac{n}{2}\right]=m$, отсюда находим ($[n]=2m$, или $[n]=2m+1$)

$$\psi(n)-\psi\left(\frac{n}{2}\right)\leqslant\ln\frac{(2m+1)!}{(m!)^2}\leqslant\ln\left(2^m\frac{3\cdot5\ldots(2m+1)}{1\cdot2\ldots m}\right)\leqslant\ln(2^m3^m)<n,$$

$$\psi(n)=\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{2}\right)-\psi\left(\frac{n}{4}\right)+$$
$$+\psi\left(\frac{n}{4}\right)-\psi\left(\frac{n}{8}\right)+\ldots<n+\frac{n}{2}+\frac{n}{4}+\ldots=2n.$$

γ) Имеем (решение вопроса β) и результат вопроса 8,c)

$$\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\ldots=\ln\frac{[n]!}{\left(\left[\frac{n}{2}\right]!\right)^2}=$$
$$=[n]\ln[n]-[n]-2\left[\frac{n}{2}\right]\ln\left[\frac{n}{2}\right]+2\left[\frac{n}{2}\right]+O(\ln n)=$$
$$=n\ln 2+O(\ln n).$$

Далее, при $s\geqslant 2$ находим (вопрос β))

$$\Theta\left(\sqrt[s]{n}\right)-\Theta\left(\sqrt[s]{\frac{n}{2}}\right)+\Theta\left(\sqrt[s]{\frac{n}{3}}\right)-$$
$$-\Theta\left(\sqrt[s]{\frac{n}{4}}\right)+\ldots\begin{cases}<2\sqrt[s]{n} & \text{всегда,}\\ =0 & \text{при } s>\tau,\ \tau=\left[\frac{\ln n}{\ln 2}\right].\end{cases}$$

Поэтому

$$0\leqslant\psi(n)-\psi\left(\frac{n}{2}\right)+\psi\left(\frac{n}{3}\right)-\psi\left(\frac{n}{4}\right)+\ldots$$
$$\ldots-\left(\Theta(n)-\Theta\left(\frac{n}{2}\right)+\Theta\left(\frac{n}{3}\right)-\Theta\left(\frac{n}{4}\right)+\ldots\right)<$$
$$<2\sqrt{n}+2\sqrt[3]{n}+2\sqrt[4]{n}+\ldots+2\sqrt[\tau]{n}<2\left(\sqrt{n}+\tau\sqrt[3]{n}\right)=O\left(\sqrt{n}\right).$$

b. Следует из равенства (1), неравенства вопроса а, β) и равенства вопроса 8,с.

c. Равенство вопроса b при достаточно больших m дает

$$\sum_{m<p\leqslant m^2}\frac{\ln p}{p}=\ln m+O(1)\geqslant\frac{\ln m}{2},\qquad \sum_{m<p\leqslant m^2}\frac{4}{p}>1.$$

Если для всех пар p_n, p_{n+1} с услонием $m<p_n<p_{n+1}\leqslant m^2$ имело бы место неравенство $p_{n+1}>p_n(1+\varepsilon)$, то было бы

$$\sum_{r=0}^{\infty}\frac{4}{m(1+\varepsilon)^r}>1,$$

что при достаточно больших m невозможно.

d. Очевидно, достаточно рассматривать лишь случай, когда n — целое.

Полагая $\gamma(r)=\frac{\ln r}{r}$ при r простом и $\gamma(r)=0$ при $r=1$, или при r составном, имеем (вопрос b)

$$\gamma(1)+\gamma(2)+\ldots+\gamma(r)=\ln r+\alpha(r);\quad |\alpha(r)|<C_1,$$

где C_1 — постоянное. Отсюда при $r>1$

$$\gamma(r)=\ln r-\ln(r-1)+\alpha(r)-\alpha(r-1),$$

$$\sum_{0<p\leqslant n}\frac{1}{p}=T_1+T_2;\quad T_1=\sum_{1<r\leqslant n}\frac{\ln r-\ln(r-1)}{\ln r},$$

$$T_2=\sum_{1<r\leqslant n}\frac{\alpha(r)-\alpha(r-1)}{\ln r}.$$

Имеем (8, b)

$$T_1=\sum_{1<r\leqslant n}\frac{1}{r\ln r}+\sum_{1<r\leqslant n}\left(\frac{1}{2r^2\ln r}+\frac{1}{3r^3\ln r}+\ldots\right)=$$

$$=C_2+\ln\ln n+O\left(\frac{1}{\ln n}\right),$$

где C_2 — постоянное. Далее находим

$$T_2=\alpha(2)\left(\frac{1}{\ln 2}-\frac{1}{\ln 3}\right)+\ldots+\alpha(n-1)\left(\frac{1}{\ln(n-1)}-\frac{1}{\ln n}\right)+\frac{\alpha(n)}{\ln n},$$

откуда следует, что

$$T_2=C_3+O\left(\frac{1}{\ln n}\right),$$

где C_3 — сумма абсолютно сходящегося ряда

$$\alpha(2)\left(\frac{1}{\ln 2}-\frac{1}{\ln 3}\right)+\alpha(3)\left(\frac{1}{\ln 3}-\frac{1}{\ln 4}\right)+\ldots$$

e. Имеем

$$\ln \prod_{p \leqslant n} \left(1-\frac{1}{p}\right) = -\sum_{p \leqslant n} \frac{1}{p} - \sum_{p \leqslant n} \left(\frac{1}{2p^2}+\frac{1}{3p^3}+\dots\right) =$$

$$= C' - \ln \ln n + O\left(\frac{1}{\ln n}\right),$$

где C' — постоянное. Отсюда, полагая $C' = \ln C_0$, мы и получим указанное равенство.

f. Полагая $n = [1{,}5s \ln s]$ и обозначая символом $\pi(n)$ число простых чисел, не превосходящих n, из равенства вопроса 9, a, γ) выводим (C — положительное постоянное число)

$$\pi(n) > \frac{n \ln 2 - C\sqrt{n}}{\ln n},$$

что больше s, если s_0 выбрано достаточно большим. Отсюда следует, что p_s при $s \geqslant s_0$ находится среди простых чисел, не превосходящих n.

g. Пусть $q_1, q_2, \dots, q_s$ — различные простые делители числа a. Находим: $2 \cdot 3 \cdot 4 \dots (s+1) \leqslant a$ откуда (вопрос 8, c)

$$(s+1)\ln(s+1) + O(s+1) \leqslant \ln a, \quad s = O(\ln a).$$

Поэтому (вопросы e и f)

$$\frac{a}{\varphi(a)} = \frac{1}{\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\dots\left(1-\frac{1}{q_s}\right)} \leqslant$$

$$\leqslant \frac{1}{\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\dots\left(1-\frac{1}{p_s}\right)} = O(\ln p_s) = O(\ln \ln a).$$

10, a. Следует из d, § 2.

b. Ввиду $\theta(1) = \psi(1) = 1$ условие 1, a, § 2 для функции $\theta(a)$ выполнено. Пусть $a = a_1 a_2$ — одно из разложений a на два взаимно простых сомножителя. Имеем

$$\sum_{d_1 \backslash a_1} \sum_{d_2 \backslash a_2} \theta(d_1 d_2) = \psi(a) = \psi(a_1)\psi(a_2) = \sum_{d_1 \backslash a_1} \sum_{d_2 \backslash a_2} \theta(d_1)\theta(d_2). \qquad (1)$$

Если условие 2, a, § 2 выполнено для всех произведений, меньших a, то при $d_1 d_2 < a$ имеем $\theta(d_1 d_2) = \theta(d_1)\theta(d_2)$, и равенство (1) дает $\theta(a_1 a_2) = \theta(a_1)\theta(a_2)$, т. е. условие 2, a, § 2 выполняется и для всех произведений $a_1 a_2$, равных a. Но условие 2, a, § 2 выполняется для единственного произведения $1 \cdot 1$, равного 1. Следовательно, оно выполняется и для всех произведений.

11, a. Пусть $m > 1$; для каждого данного x_m делящего a, неопределенное уравнение $x_1 \dots x_{m-1} x_m = a$ имеет $\tau_{m-1}\left(\frac{a}{x_m}\right)$ решений. Поэтому

$$\tau_m(a) = \sum_{x_m \backslash a} \tau_{m-1}\left(\frac{a}{x_m}\right),$$

но когда x_m пробегает все делители числа a, то $d=\frac{a}{x_m}$ в обратном порядке пробегает те же делители. Следовательно,

$$\tau_m(a)=\sum_{d\mid a}\tau_{m-1}(d).$$

Поэтому (вопрос 10, а) если теорема верна для функции $\tau_{m-1}(a)$, то она верна и для функции $\tau_m(a)$. Но теорема верна для функции $\tau_1(a)=1$. Значит, она верна всегда.

b. Если теорема верна для функции $\tau_m(p^\alpha)$, то имеем

$$\tau_{m+1}(p^\alpha)=\sum_{s=0}^{\alpha}\tau_m(p^s)=\sum_{s=0}^{\alpha}\frac{(s+1)(s+2)\dots(s+m-1)}{1\cdot 2\dots(m-1)}=$$

$$=\frac{(\alpha+1)(\alpha+2)\dots(\alpha+m)}{1\cdot 2\dots m}.$$

Следовательно, теорема верна и для функции $\tau_{m+1}(p^\alpha)$. Но теорема верна для функции $\tau_2(p^\alpha)$ $\left(\text{очевидно равной } \frac{\alpha+1}{1}\right)$. Поэтому она верна всегда.

c. Пусть $\varepsilon=m\varepsilon_2$, $\varepsilon_2=2\eta$, $a=p_1^{\alpha_1}\dots p_k^{\alpha_k}$ — каноническое разложение числа a, причем $p_1, \dots, p_k$ расположены в возрастающем порядке. Для функции $\tau_2(a)=\tau(a)$ имеем

$$\frac{\tau(a)}{a^\eta}\leqslant\frac{\alpha_1+1}{2^{\alpha_1\eta}}\frac{\alpha_2+1}{3^{\alpha_2\eta}}\dots\frac{\alpha_k+1}{(k+1)^{\alpha_k\eta}}.$$

Предполагая для простоты рассуждений, что $\varepsilon<1$, убеждаемся, что каждый из сомножителей произведения, стоящего справа, меньше $\frac{1}{\eta}$; сомножители $\frac{\alpha_{r-1}+1}{r^{\alpha_{r-1}\eta}}$ с условием $r>2^{\frac{1}{\eta}}$ меньше 1. Поэтому, полагая $C=\left(\frac{1}{\eta}\right)^{2^{\frac{1}{\eta}}}$, находим

$$\frac{\tau(a)}{a^\eta}<C,\quad \lim_{a\to\infty}\frac{\tau(a)}{a^{\varepsilon_2}}\leqslant\lim_{a\to\infty}\frac{C}{a^\eta}=0.$$

При $m>2$, очевидно, имеем $\tau_m(a)\leqslant(\tau(a))^m$. Поэтому

$$\lim_{a\to\infty}\frac{\tau_m(a)}{a^\varepsilon}\leqslant\lim\left(\frac{\tau(a)}{a^{\varepsilon_2}}\right)^m=0.$$

d. Системы значений $x_1, \dots, x_m$, удовлетворяющие указанному неравенству, разобьем на $[n]$ совокупностей с номерами $1, 2, \dots, [n]$. К совокупности с номером a отнесем системы с условием $x_1\dots x_m=a$; число этих систем есть $\tau_m(a)$.

12. При $R(s) > 1$ ряд, выражающий $\zeta(s)$, абсолютно сходится. Поэтому

$$(\zeta(s))^m = \sum_{n_1=1}^{\infty} \cdots \sum_{n_m=1}^{\infty} \frac{1}{(n_1 \ldots n_m)^s},$$

причем при данном положительном n число систем $n_1, \ldots, n_m$ с условием $n_1 \ldots n_m = n$ равно $\tau_m(n)$.

13, a. При $R(s) > 1$ произведение $P = \prod_p \frac{1}{1-\frac{1}{p^s}}$ абсолютно сходится. Ввиду $\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots$ при $N > 2$ имеем

$$\prod_{p \leqslant N} \frac{1}{1-\frac{1}{p^s}} = \sum_{0 < n \leqslant N} \frac{1}{n^s} + \sum' \frac{1}{n^s},$$

где во второй сумме правой части n пробегает лишь числа, превосходящие N. В пределе при $N \to \infty$ левая часть обратится в P, первая сумма правой части — в $\zeta(s)$, вторая — в нуль.

b. Пусть $N > 2$. Допустив, что простых чисел, отличных от $p_1, \ldots, p_k$, нет, находим (ср. решение вопроса a)

$$\prod_{j=1}^{k} \frac{1}{1-\frac{1}{p_j}} \geqslant \sum_{0 < n \leqslant N} \frac{1}{n}.$$

Это неравенство ввиду расходимости гармонического ряда $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ при достаточно больших N невозможно.

c. Допустив, что простых чисел, отличных от $p_1, \ldots, p_k$, нет, находим (вопрос a)

$$\prod_{j=1}^{k} \frac{1}{1-\frac{1}{p_j^2}} = \zeta(2).$$

Это равенство ввиду иррациональности $\zeta(2) = \frac{\pi^2}{6}$ невозможно.

14. При $R(s) > 1$ бесконечное произведение для $\zeta(s)$ вопроса **13**, a абсолютно сходится. Поэтому

$$\ln \zeta(s) = \sum_p \left(\frac{1}{p^s} + \frac{1}{2p^{2s}} + \frac{1}{3p^{3s}} + \ldots \right),$$

где p пробегает все простые числа. Дифференцируя, имеем

$$\frac{\zeta'(s)}{\zeta(s)}=\sum_{p}\left(-\frac{\ln p}{p^s}-\frac{\ln p}{p^{2s}}-\frac{\ln p}{p^{3s}}-\dots\right)=-\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}.$$

15. Пусть $N>2$. Применяя теорему b, § 4, имеем

$$\prod_{p\leqslant N}\left(1-\frac{1}{p^s}\right)=\sum_{0<n\leqslant N}\frac{\mu(n)}{n^s}+\sum{}'\frac{\mu(n)}{n^s},$$

где во второй сумме правой части n пробегает лишь числа, большие N. В пределе при $N\to\infty$ мы и получим указанное тождество.

16, a. Применим c, § 4 к случаю

$$\delta=1,\ 2,\ \dots,\ [n],\quad f=1,\ 1,\ \dots,\ 1.$$

Тогда, очевидно, $S'=1$. Далее S_d обращается в число значений δ, кратных d, т. е. в $\left[\frac{n}{d}\right]$.

b, α) Правая часть равенства вопроса a выражает сумму значений функции $\mu(d)$, распространенную на целые точки (d, u) области $d>0$, $0<u\leqslant\frac{n}{a}$. Часть этой суммы, отвечающая данному u, равна $M\left(\frac{n}{u}\right)$.

β) Указанное равенство получается почленным вычитанием равенств

$$M(n)+M\left(\frac{n}{2}\right)+M\left(\frac{n}{3}\right)+M\left(\frac{n}{4}\right)+\dots=1,$$

$$2M\left(\frac{n}{2}\right)+\qquad 2M\left(\frac{n}{4}\right)+\dots=2.$$

c. Пусть $n_1=[n]$; $\delta_1, \delta_2, \dots, \delta_{n_1}$ определяются условием: δ_s есть наибольшее целое, l я степень которого делит s, $f_s=1$. Тогда $S'=T_{l,n}$, S_d равно числу чисел, не превосходящих n, кратных d^l, т. е. $S_d=\left[\frac{n}{d^l}\right]$. Отсюда получается указанное выражение для $T_{l,n}$. В частности, ввиду $\zeta(2)=\frac{\pi^2}{6}$ для числа $T_{2,n}$ чисел, не превосходящих n и не делящихся на квадрат целого, превосходящего 1, имеем

$$T_{2,n}=\frac{6}{\pi^2}n+O(\sqrt{n}).$$

17, a. Указанное равенство получим из c, § 4, если положим

$$\delta_s=(x_s, a),\quad f_s=f(x_s).$$

b. Указанное равенство получим из c, § 4, если положим

$$\delta_s=(x_1^{(s)}, \dots, x_k^{(s)}),\quad f_s=f(x_1^{(s)}, \dots, x_k^{(s)}).$$

c. Применяя с, § 4 к случаю

$$\delta=\delta_1,\ \delta_2,\ \ldots,\ \delta_\tau,$$

$$f=F\left(\frac{a}{\delta_1}\right),\ F\left(\frac{a}{\delta_2}\right),\ \ldots,\ F\left(\frac{a}{\delta_\tau}\right),$$

где в первой строке выписаны все делители числа a, имеем

$$S'=F(a),\quad S_d=\sum_{D\backslash\frac{a}{d}}F\left(\frac{a}{dD}\right)=G\left(\frac{a}{d}\right).$$

d. Указанное равенство следует из

$$\sum_{P'=f_1^{d/\delta_1}}\mu(d)\sum_{f_2^{d/\delta_2}}\mu(d)\ldots\sum_{f_n^{d/\delta_n}}\mu(d).$$

18, a. Применим теорему вопроса 17, a, заставляя x пробегать числа $1, 2, \ldots, a$ и беря $f(x)=x^m$. Тогда

$$S'=\psi_m(a),\quad S_d=d^m+2^md^m+\ldots+\left(\frac{a}{d}\right)^m d^m=d^m\sigma_m\left(\frac{a}{d}\right).$$

b. Имеем

$$\psi_1(a)=\sum_{d\backslash a}\mu(d)\left(\frac{a^2}{2d}+\frac{a}{2}\right)=\frac{a}{2}\varphi(a).$$

Тот же результат можно получить проще. Напишем числа ряда $1, \ldots, a$, взаимно простые с a, сначала в возрастающем, затем в убывающем порядке. Сумма членов обоих рядов, равноотстоящих от начала, равна a, число членов каждого ряда равно $\varphi(a)$.

c. Имеем

$$\psi_2(a)=\sum_{d\backslash a}\mu(d)\left(\frac{a^3}{3d}+\frac{a^2}{2}+\frac{a}{6}d\right)=\frac{a^2}{3}\varphi(a)+\frac{a}{6}(1-p_1)\ldots(1-p_k).$$

19, a. Применим теорему вопроса 17, a, заставляя x пробегать числа $1, 2, \ldots, [z]$ и беря $f(x)=1$. Тогда $S'=T_z$, S_d равно числу чисел, не превосходящих z, кратных d, т. е. $S_d=\left[\frac{z}{d}\right]$.

b. Имеем

$$T_z=\sum_{d\backslash a}\mu(d)\frac{z}{d}+O(\tau(a))=\frac{z}{a}\varphi(a)+O(a^\varepsilon).$$

c. Следует из равенства вопроса a.

20. Применим теорему вопроса 17, a, заставляя x пробегать числа $1, 2, \ldots, N$, где $N>a$, и беря $f(x)=\frac{1}{x^s}$. Тогда найдем

$$\sum_{x\leqslant N}{}'\frac{1}{x^s}=\sum_{d\backslash a}\mu(d)\sum_{0<x\leqslant\frac{N}{d}}\frac{1}{d^sx^s}=\sum_{d\backslash a}\frac{\mu(d)}{d^s}\sum_{0<x\leqslant\frac{N}{d}}\frac{1}{x^s}.$$

В пределе при $N\longrightarrow\infty$ получим указанное тождество.

21, a. Применим теорему вопроса 17, b, рассматривая указанные в определении вероятности P_N системы значений $x_1, x_2, \ldots, x_k$ и беря $f(x_1, x_2, \ldots, x_k)=1$. Тогда $P_N=\frac{S'}{N^k}$, $S_d=\left[\frac{N}{d}\right]^k$, и мы получим

$$P_N=\frac{\sum_{d=1}^{N}\mu(d)\left[\frac{N}{d}\right]^k}{N^k}=\sum_{d=1}^{N}\frac{\mu(d)}{d^k}+O\left(\sum_{d=1}^{N}\frac{1}{Nd^{k-1}}\right).$$

Поэтому

$$P_N=(\zeta(k))^{-1}+O(\Delta);\quad \Delta=\frac{1}{N}\ \text{при}\ k>2,\quad \Delta=\frac{\ln N}{N}\ \text{при}\ k=2.$$

b. Имеем $\zeta(2)=\frac{\pi^2}{6}$.

22. a. Элементарные рассуждения показывают, что число целых точек (u, v) области $u^2+v^2\leqslant\rho^2$; $\rho>0$, не считая точки (0, 0), равно $\pi\rho^2+O(\rho)$. Применим теорему вопроса 17, b, рассматривая координаты x, y целых точек области $x^2+y^2\leqslant r^2$, отличных от точки (0, 0), и полагая $f(x, y)=1$. Тогда $T=S'+1$, S_d равно числу целых точек области $u^2+v^2\leqslant\left(\frac{r}{d}\right)^2$, не считая точки (0, 0). Поэтому

$$S_d=\pi\frac{r^2}{d^2}+O\left(\frac{r}{d}\right),$$

$$T=\sum_{d=1}^{[r]}\mu(d)\,\pi\frac{r^2}{d^2}+O\left(\sum_{d=1}^{[r]}\frac{r}{d}\right)=\frac{6}{\pi}r^2+O(r\ln r).$$

b. Рассуждая аналогично предыдущему, получим

$$T=\sum_{d=1}^{[r]}\mu(d)\,\frac{4}{3}\pi\frac{r^3}{d^3}+O\left(\sum_{d=1}^{[r]}\frac{r^2}{d^2}\right)=\frac{4\pi r^3}{3\zeta(3)}+O(r^2).$$

23, a. Число делителей d числа $a=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$, не делящихся на квадрат целого, превосходящего 1, и имеющих $\varkappa$ простых делителей, равно $\binom{k}{\varkappa}$; при этом $\mu(d)=(-1)^{\varkappa}$. Поэтому

$$\sum_{d\mid a}\mu(d)=\sum_{\varkappa=0}^{k}\binom{k}{\varkappa}(-1)^{\varkappa}=(1-1)^{\varkappa}=0.$$

b. Пусть a имеет тот же вид, что и в вопросе a. Достаточно рассматривать случай $m<k$. Для указанной суммы имеем два выражения

$$\sum\mu(d)=\binom{k}{0}-\binom{k}{1}+\ldots+(-1)^m\binom{k}{m}=$$

$$=(-1)^m\left(\binom{k}{m+1}-\binom{k}{m+2}+\ldots\right).$$

Если m четное, то при $m \leqslant \frac{k}{2}$ первое выражение > 0, а при $m > \frac{k}{2}$ второе выражение $\geqslant 0$. Если m нечетное, то при $m \leqslant \frac{k}{2}$ первое выражение < 0, а при $m > \frac{k}{2}$ второе выражение $\leqslant 0$.

c. Доказательство почти такое же, как в c, § 4, но с учетом результата вопроса b

d. Доказательство почти такое же, как в вопросах 17,a и b.

24. Пусть d пробегает делители числа a, $\Omega(d)$ — число простых делителей числа d, $\Omega(a) = s$. Согласно сделанному в вопросе указанию, имеем (считаем N достаточно большим)

$$\pi(N, q, l) \leqslant \sum_{\Omega(d) \leqslant m} \mu(d) \left(\frac{N}{qd} + \theta_d \right) = T + T_0 - T_1; \quad |\theta_d| \leqslant 1,$$

$$|T| \leqslant \sum_{\Omega(d) \leqslant m} 1, \quad T_0 = \frac{N}{q} \sum_{d} \frac{\mu(d)}{d}, \quad |T_1| = \sum_{\Omega(d) > m} \frac{N}{qd}.$$

Далее находим

$$|T| \leqslant \sum_{n=0}^{m} \binom{s}{n} \leqslant s^m \leqslant e^{hm} < e^{s^{r-1}-\varepsilon} \frac{qr}{N} \frac{N}{q^r} = O(\Delta),$$

$$T_0 = \frac{N}{q} \frac{\prod_{p \leqslant e^h} \left(1 - \frac{1}{p}\right)}{\prod_{p \setminus q} \left(1 - \frac{1}{q}\right)} = O(\Delta)$$

Наконец, обозначая буквами C_1 и C_2 некоторые постоянные, имеем

$$|T_1| \leqslant \frac{N}{q} \sum_{n=m+1}^{s} \sum_{\Omega(d)=n} \frac{1}{d} \leqslant \frac{N}{q} \sum_{n=m+1}^{s} \frac{\left(\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p_s}\right)^n}{n!} \leqslant$$

$$\leqslant \frac{N}{q} \sum_{n=m+1}^{s} \left(\frac{C_1 + \ln r}{4 \ln r} e \right)^n \leqslant \frac{N}{q} \sum_{n=m+1}^{s} \left(\frac{3}{4} \right)^n <$$

$$< C_2 \frac{N}{q} r^{-4 \ln \frac{4}{3}} = O(\Delta).$$

25. Всякому делителю d_1 числа a с условием $d_1 < \sqrt{a}$ отвечает делитель d_2 с условиями $d_2 > \sqrt{a}$, $d_1 d_2 = a$. При этом $\mu(d_1) = \mu(d_2)$. Поэтому

$$2 \sum_{d_1} \mu(d_1) = \sum_{d_1} \mu(d_1) + \sum_{d_2} \mu(d_2) = \sum_{d \setminus a} \mu(d) = 0.$$

26. Числа d, не делящиеся на квадрат целого, превосходящего 1, и удовлетворяющие условию $\varphi(d)=k$, рассмотрим попарно так, чтобы в каждую пару входило некоторое нечетное d_1 и четное $2d_1$. Будем иметь $\mu(d_1)+\mu(2d_1)=0$.

27. Пусть $p_1, \ldots, p_k$ — различные простые числа. Полагая $a=p_1 \ldots p_k$, имеем

$$\varphi(a)=(p_1-1)\ldots(p_k-1).$$

Между тем, при отсутствии простых чисел, отличных от $p_1, \ldots, p_k$, мы имели бы $\varphi(a)=1$.

28, a. Указанные числа найдутся среди чисел $s\delta$; $s=1, 2, \ldots, \frac{a}{\delta}$. Но $(s\delta, a)=\delta$ тогда и только тогда, когда $\left(s, \frac{a}{\delta}\right)=1$ (см. § 2, гл. I). Поэтому верно утверждение, отмеченное в вопросе, и мы имеем

$$a=\sum_{\delta \setminus a}\varphi\left(\frac{a}{\delta}\right)=\sum_{d \setminus a}\varphi(d).$$

b, α) Пусть $a=p_1^{\alpha_1}\ldots p_k^{\alpha_k}$ — каноническое разложение числа a. Ввиду а функция $\varphi(a)$ мультипликативная, причем

$$p_s^{\alpha}s=\sum_{d \setminus p_s^{\alpha}s}\varphi(d), \quad p_s^{\alpha}s^{-1}=\sum_{d \setminus p_s^{\alpha}s^{-1}}\varphi(d),$$

$$p_s^{\alpha}s-p_s^{\alpha}s^{-1}=\varphi\left(p_s^{\alpha}s\right).$$

β) Для целого $m>0$ имеем

$$m=\sum_{d \setminus m}\varphi(d).$$

Поэтому

$$\varphi(a)=\sum_{d \setminus a}\mu(d)\frac{a}{d}.$$

29. Имеем (p пробегает все простые числа)

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\prod_p\left(1+\frac{\varphi(p)}{p^s}+\frac{\varphi(p^2)}{p^{2s}}+\ldots\right)=\prod_p\frac{1-\frac{1}{p^s}}{1-\frac{1}{p^{s-1}}}=\frac{\zeta(s-1)}{\zeta(s)}.$$

30. Имеем

$$\varphi(1)+\varphi(2)+\ldots+\varphi(n)=$$

$$=\sum_{d \setminus 1}\frac{\mu(d)}{d}+2\sum_{d \setminus 2}\frac{\mu(d)}{d}+\ldots+n\sum_{d \setminus n}\frac{\mu(d)}{d}=\sum_{d=1}^{n}\mu(d)\left(1+2+\ldots+\left[\frac{n}{d}\right]\right)=$$

$$=\sum_{d=1}^{n}\mu(d)\frac{n^2}{2d^2}+O(n\ln n)=\frac{n^2}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}+O(n\ln n)=\frac{3}{\pi^2}n^2+O(n\ln n).$$

Решения к главе III

1, a. Из

$$P = a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_1,$$

замечая, что $10 \equiv 1 \pmod 9$, имеем

$$P \equiv a_n + a_{n-1} + \ldots + a_1 \pmod 9.$$

Следовательно, P кратно 3 тогда и только тогда, когда сумма цифр, его изображающих, кратна 3; оно кратно 9 тогда и только тогда, когда указанная сумма кратна 9.

Замечая, что $10 \equiv -1 \pmod{11}$, имеем

$$P \equiv (a_1 + a_3 + \ldots) - (a_2 + a_4 + \ldots) \pmod{11}.$$

Следовательно, P кратно 11 тогда и только тогда, когда разность между суммою цифр, стоящих на нечетных (считая справа) местах, и суммою цифр, стоящих на четных местах, кратна 11.

b. Из

$$P = b_n 100^{n-1} + b_{n-1} 100^{n-2} + \ldots + b_1$$

ввиду $100 \equiv -1 \pmod{101}$ имеем

$$P \equiv (b_1 + b_3 + \ldots) - (b_2 + b_4 + \ldots) \pmod{101}.$$

Поэтому P кратно 101 тогда и только тогда, когда $(b_1 + b_3 + \ldots) - (b_2 + b_4 + \ldots)$ кратно 101.

c. Из

$$P = c_n 1000^{n-1} + c_{n-1} 1000^{n-2} + \ldots + c_1$$

ввиду $1000 \equiv 1 \pmod{37}$ имеем

$$P \equiv c_n + c_{n-1} + \ldots + c_1 \pmod{37}.$$

Поэтому P кратно 37 тогда и только тогда, когда $c_n + c_{n-1} + \ldots + c_1$ кратно 37.

Ввиду $1000 \equiv -1 \pmod{7 \cdot 11 \cdot 13}$ имеем

$$P \equiv (c_1 + c_3 + \ldots) - (c_2 + c_4 + \ldots) \pmod{7 \cdot 11 \cdot 13}.$$

Поэтому P кратно одному из чисел 7, 11, 13 тогда и только тогда, когда $(c_1 + c_3 + \ldots) - (c_2 + c_4 + \ldots)$ кратно этому же числу.

2, α) Когда x пробегает полную систему вычетов по модулю m, то $ax + b$ также пробегает полную систему; наименьший неотрицательный вычет r числа $ax + b$ пробегает значения $0, 1, \ldots, m-1$. Поэтому

$$\sum_x \left\{\frac{ax+b}{m}\right\} = \sum_{r=0}^{m-1} \frac{r}{m} = \frac{1}{2}(m-1).$$

β) Применяя результат вопроса 18, b, гл. II, находим

$$\sum_\xi \left\{\frac{a\xi}{m}\right\} = \frac{\psi_1(m)}{m} = \frac{1}{2}\varphi(m).$$

3, a. Пусть r — наименьший неотрицательный вычет числа $ax+[c]$ по модулю m. Имеем

$$S=\sum_{r=0}^{m-1}\left\{\frac{r+\Phi(r)}{m}\right\},$$

где $\varepsilon\leqslant\Phi(r)\leqslant\varepsilon+h$; $\varepsilon=\{c\}$. При $m\leqslant 2h+1$ теорема очевидна. Поэтому рассмотрим лишь случай $m>2h+1$. Полагая

$$\left\{\frac{r+\Phi(r)}{m}\right\}-\frac{r}{m}=\delta(r),$$

имеем $-1+\frac{\varepsilon}{m}\leqslant\delta(r)\leqslant\frac{h+\varepsilon}{m}$ при $r=m-[h+\varepsilon], \ldots, m-1$; $\frac{\varepsilon}{m}\leqslant$ $\leqslant\delta(r)\leqslant\frac{h+\varepsilon}{m}$ в остальных случаях. Поэтому

$$-[h+\varepsilon]+\varepsilon\leqslant S-\frac{m-1}{2}\leqslant h+\varepsilon,\quad \left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

b. Имеем

$$S=\sum_{z=0}^{m-1}\left\{\frac{az+\psi(z)}{m}\right\};\quad \psi(z)=m(AM+B)+\frac{\lambda}{m}z.$$

Применим теорему вопроса a, полагая $h=[\lambda]$. Тогда и получим указанный результат.

c. Находим

$$\sum_{z=0}^{m-1}\left\{f(M)+\frac{az}{\ldots}+\frac{\theta z}{\ldots^2}+\frac{f''(M+z_0)}{2}z^2\right\};\quad 0<z_0<m-1.$$

Применим теорему вопроса a, полагая $h=1+\frac{k}{z}$. Тогда получим указанный результат.

4. Разложим A в непрерывную дробь. Пусть $Q_n=Q'$ — наибольший из знаменателей подходящих дробей, не превосходящий m, имеем (вопрос 4, b, гл. I)

$$A=\frac{P'}{Q'}+\frac{\theta'}{Q'm},\quad (P', Q')=1,\quad |\theta'|<1.$$

При этом из $m<Q_{n+1}\leqslant(q_{n+1}+1)Q_n\leqslant CQ_n$, где C — постоянное, которого не превосходят все q_s+1, для наибольшего целого H' с условием $H'Q'\leqslant m$ следует $H'<C$. Применяя теорему вопроса 3, b, находим

$$\left|\sum_{x=M}^{M+H'Q'-1}\{Ax+B\}-\frac{1}{2}H'Q'\right|\leqslant\frac{3}{2}C.$$

Пусть $m_1 = m - H'Q'$. Если $m_1 > 0$, то выбирая в зависимости от m_1 числа Q'' и H'' таким же способом, как раньше в зависимости от m были выбраны числа Q' и H', найдем

$$\left| \sum_{x=M_1}^{M_1+H''Q''-1} \{Ax+B\} - \frac{1}{2} H''Q'' \right| \leqslant \frac{3}{2} C,$$

где применяем обозначение $M_s = M_{s-1} + H^{(s)}Q^{(s)}$. Пусть $m_2 = m_1 - H''Q'$ Если $m_2 > 0$, то подобно предыдущему найдем

$$\left| \sum_{x=M_2}^{M_2+H'''Q'''-1} \{Ax+B\} - \frac{1}{2} H'''Q''' \right| < \frac{3}{2} C$$

и т. д., пока не придем к некоторому $m_k = 0$. Тогда получим $(H'Q' + H''Q'' + \ldots + H^{(k)}Q^{(k)} = m)$

$$\left| \sum_{x=M}^{M+m-1} \{Ax+B\} - \frac{1}{2} m \right| < \frac{3}{2} Ck.$$

Числа Q', Q'', ..., $Q^{(k)}$ удовлетворяют условиям

$$m \geqslant Q' > m_1 \geqslant Q'' > m_2 \geqslant \ldots > m_{k-1} \geqslant Q^{(k)} \geqslant 1.$$

Поэтому (вопрос 3, b гл. I) $k = O(\ln m)$ и, следовательно, формула, указанная в вопросе, верна.

5, a. Сумму, стоящую слева, обозначим буквою S. Пусть $\tau = A^{\frac{1}{3}}$. При $\tau \leqslant 40$ теорема очевидна. Поэтому предполагаем $\tau > 40$. Взяв $M_1 = [Q+1]$, найдем числа a_1, m_1, θ_1 с условиями

$$f'(M_1) = \frac{a_1}{m_1} + \frac{\theta_1}{m_1\tau}; \quad 0 < m_1 \leqslant \tau; \quad (a_1, m_1) = 1, \quad |\theta_1| < 1.$$

Взяв $M_2 = M_1 + m_1$, аналогичным путем найдем числа a_2, m_2, θ_2; взяв $M_3 = M_2 + m_2$, найдем числа a_3, m_3, θ_3, и т. д., пока не придем к $M_{s+1} = M_s + m_s$ с условием $0 \leqslant [R] - M_{s+1} < [\tau]$. Применяя теорему вопроса 3, c, найдем

$$\left| S - \frac{1}{2}\left(m_1 + m_2 + \ldots + m_s + [R] + 1 - M_{s+1}\right) \right| < s\frac{k+3}{2} + \frac{1}{2}([R] + 1 - M_{s+1}),$$

$$\left| S - \frac{1}{2}(R-Q) \right| < s\frac{k+3}{2} + \frac{\tau+1}{2}.$$

Длина интервала, для которого $\frac{a}{m} - \frac{1}{m\tau} \leqslant f'(x) \leqslant \frac{a}{m} + \frac{1}{m\tau}$, не превосходит $\frac{2A}{m\tau}$. Следовательно, с одной и той же дробью $\frac{a}{m}$ связано $\leqslant \frac{2A}{m^2\tau} + 1$ чисел m_1, m_2, ..., m_s. Пусть a_1 и a_2 — наименьшее и наибольшее значения a, отвечающие данному m.

Имеем

$$\frac{a_2-a_1}{m}-\frac{2}{m\tau}\leqslant\frac{k(R-Q)}{A};\quad a_2-a_1+1\leqslant\frac{k(R-Q)m}{A}+1{,}05.$$

Следовательно, с данным m связано

$$<\left(\frac{2A}{m^2\tau}+1\right)\left(\frac{k(R-Q)m}{A}+1{,}05\right)=$$

$$=\frac{k(R-Q)}{\tau}\left(\frac{2}{m}+\frac{m}{\tau^2}\right)+\left(\frac{2A}{m^2\tau}+1\right)1{,}05$$

чисел $m_1, m_2, \ldots, m_s$. Суммируя последнее выражение по всем $m=1, 2, \ldots, [\tau]$, получим

$$s<\frac{k(R-Q)}{\tau}\left(2\ln\tau+2+\frac{\tau^2+\tau}{2\tau^2}\right)+\frac{10A}{3\tau}1{,}05<\frac{k(R-Q)}{\tau}\ln A+\frac{7}{2}\frac{A}{\tau},$$

$$\left|S-\frac{1}{2}(R-Q)\right|<2\frac{k^2(R-Q)}{\tau}\ln A+8k\frac{A}{\tau}.$$

b. Имеем

$$\left|\sum_{Q<x\leqslant R}\{f(x)+1-\sigma\}-\frac{1}{2}(R-Q)\right|<\Delta,$$

$$\left|\sum_{Q<x\leqslant R}\{f(x)\}-\frac{1}{2}(R-Q)\right|<\Delta,$$

откуда, полагая $\delta(x)=\{f(x)+1-\sigma\}-\{f(x)\}$, находим

$$\left|\sum_{Q<x\leqslant R}\delta(x)\right|<2\Delta.$$

Но при $\{f(x)\}<\sigma$ имеем $\delta(x)=1-\sigma$, а при $\{f(x)\}\geqslant\sigma$ имеем $\delta(x)=-\sigma$. Поэтому $|(1-\sigma)\psi(\sigma)-\sigma(R-Q-\psi(\sigma))|<2\Delta$, откуда и получим указанную формулу.

6, а. Применим формулу вопроса 1, с, гл. II. Полагая $f(x)=-\sqrt{r^2-x^2}$, в интервале $0\leqslant x\leqslant\frac{r}{\sqrt{2}}$ имеем

$$f'(x)=-\frac{x}{\sqrt{r^2-x^2}},\quad f''(x)=\frac{-r^2}{(r^2-x^2)^{3/2}},\quad \frac{1}{r}\leqslant|f''(x)|\leqslant\frac{\sqrt{8}}{r}.$$

Поэтому (вопрос 8, а, гл. II, вопрос 5, а)

$$T=4r+8\int_0^{\frac{r}{\sqrt{2}}}\sqrt{r^2-x^2}\,dx+8\rho\left(\frac{r}{\sqrt{2}}\right)\frac{r}{\sqrt{2}}-8\rho(0)\cdot r-4\frac{r}{\sqrt{2}}-4\frac{r^2}{2}+$$

$$+8\frac{r}{\sqrt{2}}\left\{\frac{1}{\sqrt{2}}\right\}+O(r^{\frac{2}{3}}\ln r)=\pi r^2+O(r^{\frac{2}{3}}\ln r).$$

b. Имеем (вопросы 11, d и 1, d, гл. II)

$$\tau(1)+\tau(2)+\ldots+\tau(n)=2\sum_{0<x\leqslant\sqrt{n}}\left[\frac{n}{x}\right]-\left[\sqrt{n}\right]^2.$$

Достаточно рассмотреть лишь случай $n>64$. Интервал $X<x\leqslant\sqrt{n}$, где $X=2n^{\frac{1}{3}}$, разобьем на $O(\ln n)$ интервалов вида $M<x\leqslant M'$, где $M'\leqslant 2M$. Полагая $f(x)=\frac{n}{x}$, в интервале $M<x\leqslant M'$ имеем

$$f'(x)=-\frac{n}{x^2},\quad f''(x)=\frac{2n}{x^3};\quad \frac{n}{4M^3}\leqslant f''(x)\leqslant\frac{8n}{4M^3}.$$

Поэтому (вопрос 5, a)

$$\sum_{M<x\leqslant M'}\left\{\frac{n}{x}\right\}=\frac{1}{2}(M'-M)+O(n^{\frac{1}{3}}\ln n),$$

$$\sum_{0<x\leqslant\sqrt{n}}\left\{\frac{n}{x}\right\}=\frac{1}{2}\sqrt{n}+O(n^{\frac{1}{3}}(\ln n)^2).$$

Далее (вопрос 8, b, гл. II)

$$\sum_{0<x\leqslant\sqrt{n}}\frac{n}{x}=En+\frac{1}{2}n\ln n+\rho(\sqrt{n})\sqrt{n}+O(1).$$

Поэтому

$$\tau(1)+\tau(2)+\ldots+\tau(n)=2En+n\ln n+2\rho(\sqrt{n})\sqrt{n}-\sqrt{n}-n+$$

$$+2\sqrt{n}\{\sqrt{n}\}+O(n^{\frac{1}{3}}(\ln n)^2)=n(\ln n+2E-1)+O(n^{\frac{1}{3}}(\ln n)^2).$$

c. Напишем ряды дробей

$$1.\ \frac{1}{2},\ \frac{1}{3},\ \frac{1}{4},\ \frac{1}{5},\ \frac{1}{6},\ \ldots,$$

$$\frac{1}{2},\quad\frac{1}{4}\quad\frac{1}{6},\ \ldots,$$

$$\frac{1}{3},\quad\frac{1}{6},\ \ldots,$$

с знаменателями, не превосходящими N. Дробь $\frac{1}{a}$ с условием $0<a\leqslant N$ встретится в $\tau(a)$ рядах. Поэтому сумма всех членов, содержащихся во всех рядах, равна

$$\sum_{0<a\leqslant N}\frac{\tau(a)}{a}.$$

С другой стороны, сумма членов s-го ряда $\leqslant\frac{1}{s}\ln N$. Поэтому та же

сумма всех членов, содержащихся во всех рядах, будет

$$\ll \ln N \sum_{0<s\leqslant N} \frac{1}{s} \ln N \ll (\ln N)^2.$$

Следовательно, неравенство (1) верно при $l=1$.

Далее, допустив справедливость неравенства (1) при каком-либо l, докажем, что оно останется верным и после замены l на $l+1$. Напишем новые ряды дробей

$$\frac{(\tau(1))^l}{1}, \frac{(\tau(2))^l}{2}, \frac{(\tau(3))^l}{3}, \frac{(\tau(4))^l}{4}, \frac{(\tau(5))^l}{5}, \frac{(\tau(6))^l}{6}, \ldots,$$
$$\frac{(\tau(2))^l}{2}, \frac{(\tau(4))^l}{4}, \frac{(\tau(6))^l}{6}, \ldots$$
$$\frac{(\tau(3))^l}{3}, \frac{(\tau(6))^l}{6}, \ldots$$

со знаменателями, не превосходящими N. Здесь сумма всех членов, содержащихся во всех рядах, равна

$$\sum_{0<a\leqslant N} \frac{(\tau(a))^{l+1}}{a}.$$

С другой стороны, сумма членов s-го ряда

$$\ll \frac{(\tau(s))^l}{s}\left(\frac{(\tau(1))^l}{1}+\ldots+\frac{(\tau([Ns^{-1}]))^l}{[Ns^{-1}]}\right) \ll \frac{(\tau(s))^l}{s}(\ln N)^{2^l}.$$

Поэтому та же самая сумма, содержащаяся во всех рядах, будет

$$\ll (\ln N)^{2^l} \sum_{0<s\leqslant N} \frac{(\tau(s))^l}{s} \ll (\ln N)^{2^l+1}.$$

И мы убедимся, что неравенство (1) останется верным и после замены l на $l+1$.

d. В случае $l=1$ неравенство (2) является следствием неравенства вопроса b. Далее, допустив справедливость неравенства (2) для какого-либо l, докажем, что оно останется верным и после замены l на $l+1$. Напишем ряды

$$(\tau(1))^l, (\tau(2))^l, (\tau(3))^l, (\tau(4))^l, (\tau(5))^l, (\tau(6))^l, \ldots$$
$$(\tau(2))^l, (\tau(4))^l, (\tau(6))^l, \ldots$$
$$(\tau(3))^l, (\tau(6))^l, \ldots$$

включающие только значения $\tau(a)$ с условием $a\leqslant N$. Здесь сумма всех членов, содержащихся во всех рядах, равна

$$\sum_{0<a\leqslant N} (\tau(a))^{l+1}.$$

С другой стороны, сумма членов s-го ряда будет

$$\ll (\tau(s))^l((\tau(1))^l+\ldots+(\tau([Ns^{-1}]))^l) \ll (\tau(s))^l \frac{N^l}{s^l}(\ln N)^{2^l-1}.$$

Поэтому (теорема вопроса c) сумма всех членов, содержащихся во всех рядах, будет

$$\ll N(\ln N)^{2^l-1} \sum_{0<s\leqslant N} \frac{(\tau(s))^l}{s} \ll N(\ln N)^{2^{l+1}-1}.$$

И мы убедимся, что неравенство (2) останется верным и после замены l на $l+1$.

7. Пусть система неправильная и s — наибольшее число с условием, что 2^s входит в нечетное число чисел системы. Одно из последних чисел мы заменим меньшим, содержащим лишь степени 2^s, входящие в нечетное число чисел оставшейся системы.

Пусть система — правильная. Число, меньшее одного из чисел T этой системы, отличается от T, по крайней мере, одним знаком в системе исчисления с основанием 2.

8, a. Добавив к каждому из чисел, представляемых указанным способом, число $H=3^n+3^{n-1}+\ldots+3+1$, получим числа, которые можно получить, заставляя в той же сумме $x_n, x_{n-1}, \ldots, x_1, x_0$ пробегать значения 0, 1, 2, т. е. получим все числа $0, 1, \ldots, 2H$.

b. Указанным способом получим $m_1m_2\ldots m_k$ чисел, не сравнимых между собою по модулю $m_1m_2\ldots m_k$, так как из

$$x_1+m_1x_2+m_1m_2x_3+\ldots+m_1m_2\ldots m_{k-1}x_k \equiv$$
$$\equiv x_1'+m_1x_2'+m_1m_2x_3'+\ldots+m_1m_2\ldots m_{k-1}x_k' \pmod{m_1m_2\ldots m_k}$$

последовательно находим

$$x_1 \equiv x_1' \pmod{m_1}, \quad x_1=x_1'; \quad m_1x_2 \equiv m_1x_2' \pmod{m_1m_2}, \quad x_2=x_2';$$

$$m_1m_2x_2 \equiv m_1m_2x_3' \pmod{m_1m_2m_3}, \quad x_3=x_3';$$

и т. д.

9, a. Указанным способом получим $m_1m_2\ldots m_k$ чисел, не сравнимых по модулю $m_1m_2\ldots m_k$, так как из

$$M_1x_1+M_2x_2+\ldots+M_kx_k \equiv$$
$$\equiv M_1x_1'+M_2x_2'+\ldots+M_kx_k' \pmod{m_1m_2\ldots m_k}$$

следовало бы (всякое M_j, отличное от M_s, кратно m_s)

$$M_sx_s \equiv M_sx_s' \pmod{m_s}, \quad x_s \equiv x_s' \pmod{m_s}, \quad x_s=x_s'.$$

b. Указаиным способом получим $\varphi(m_1)\ \varphi(m_2)\ldots\varphi(m_k)=$
$$=\varphi(m_1m_2\ldots m_k)$$

чисел ввиду теоремы вопроса a, не сравнимых по модулю $m_1m_2\ldots m_k$, и ввиду $(M_1x_1+M_2x_2+\ldots+M_kx_k,\ m_s)=(M_sx_s,\ m_s)=1$, взаимно простых с $m_1m_2\ldots m_k$.

c. Согласно теореме вопроса a число $M_1x_1+M_2x_2+\ldots+M_kx_k$, где $x_1, x_2, \ldots, x_k$ пробегают полные системы вычетов по модулям $m_1, m_2, \ldots, m_k$, пробегает полную систему вычетов по модулю $m_1m_2\ldots m_k$. Это число взаимно просто с $m_1m_2\ldots m_k$ тогда и только тогда, когда $(x_1,\ m_1)=(x_2,\ m_2)=\ldots=(x_k,\ m_k)=1$. Поэтому $\varphi(m_1m_2\ldots m_k)=$
$=\varphi(m_1)\varphi(m_2)\ldots\varphi(m_k)$.

d. Чтобы получить все числа ряда 1, 2, ..., p^α, взаимно простые с p^α, следует вычеркнуть числа этого ряда, кратные p, т. е. числа

$p, 2p, \ldots, p^{\alpha-1}p$. Поэтому $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Отсюда и из мультиплнкативности $\varphi(a)$ известное выражение для $\varphi(a)$ следует непосредственно.

10, a Первое утверждение следует из

$$\left\{\frac{x_1}{m_1} + \ldots + \frac{x_k}{m_k}\right\} = \left\{\frac{M_1x_1 + \ldots + M_kx_k}{m}\right\};$$

второе утверждение следует из

$$\left\{\frac{\xi_1}{m_1} + \ldots + \frac{\xi_k}{m_k}\right\} = \left\{\frac{M_1\xi_1 + \ldots + M_k\xi_k}{m}\right\}.$$

b. Дроби $\left\{\frac{a_1 f(x_1, \ldots, w_1)}{m_1} + \ldots + \frac{a_k f(x_k, \ldots, w_k)}{m_k}\right\}$ совпадают с дробями

$$\left\{\frac{a_1 f(M_1x_1 + \ldots + M_kx_k, \ldots, M_1w_1 + \ldots + M_kw_k)}{m_1} + \ldots \right.$$
$$\left. \ldots + \frac{a_k f(M_1x_1 + \ldots + M_kx_k, \ldots, M_1w_1 + \ldots + M_kw_k)}{m_k}\right\},$$

т. е. с дробями $\left\{\frac{af(x, \ldots, w)}{m}\right\}$. Второе утверждение доказывается аналогичным способом.

11, a. Прн a, кратном m, имеем

$$\sum_x e^{2\pi i \frac{ax}{m}} = \sum_x 1 = m.$$

При a, не делящемся на m, имеем

$$\sum_x e^{2\pi i \frac{ax}{m}} = \frac{e^{2\pi i \frac{a}{m}} - 1}{e^{2\pi i \frac{ax}{m}} - 1} = 0.$$

b. При нецелом α левая часть равиа

$$\left|\frac{e^{2\pi i\alpha(M+P)} - e^{2\pi i\alpha M}}{e^{2\pi i\alpha} - 1}\right| \leqslant \frac{1}{\sin\pi(\alpha)} \leqslant \frac{1}{(\alpha)h}.$$

c. Согласно теореме вопроса b левая часть не превосходит T_m, где

$$T_m = \sum_{a=1}^{m-1} \frac{1}{h\left(\frac{a}{m}\right)}.$$

Но при нечетном m

$$T_m < m \sum_{0 < a < \frac{m}{2}} \ln\frac{2a+1}{2a-1} = m \ln m,$$

а при четном m

$$T_m < \frac{m}{2} \sum_{0 < a \leqslant \frac{m}{2}} \ln \frac{2a+1}{2a-1} + \frac{m}{2} \sum_{0 < a < \frac{m}{2}} \ln \frac{2a+1}{2a-1} < m \ln m.$$

При $m \geqslant 6$ ввиду $\frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ границу $m \ln m$ можно уменьшить на

$$2 \frac{m}{6} \sum_{0 < a \leqslant \frac{m}{6}} \ln \frac{2a+1}{2a-1} = \frac{m}{3} \ln \left(2 \left[\frac{m}{6}\right] + 1\right).$$

Последнее выражение $> \frac{m}{2}$ при $m \geqslant 12$ и $> m$ при $m \geqslant 60$.

12, a. Пусть $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ — каноническое разложение числа m. Полагая $p_1^{\alpha_1} = m_1, \ldots, p_k^{\alpha_k} = m_k$, при обозначениях вопроса 10, а имеем

$$\sum_{\xi_1} e^{2\pi i \frac{\xi_1}{m_1}} \cdot \ldots \cdot \sum_{\xi_k} e^{2\pi i \frac{\xi_k}{m_k}} = \sum_{\xi} e^{2\pi i \frac{\xi}{m}}.$$

Но при $\alpha_s = 1$ находим

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - 1 = -1.$$

При $\alpha_s > 1$, полагая $m_s = p_s m_s'$, находим

$$\sum_{\xi_s} e^{2\pi i \frac{\xi_s}{m_s}} = \sum_{x_s} e^{2\pi i \frac{x_s}{m_s}} - \sum_{u=0}^{m_s'-1} e^{2\pi i \frac{u}{m_s'}} = 0.$$

b. Пусть m — целое, $m > 1$. Имеем $\sum_{x=0}^{m-1} e^{2\pi i \frac{x}{m}} = 0$. Сумма слагаемых левой части этого равенства с условием $(x, m) = d$ согласно теореме вопроса а равна $\mu\left(\frac{m}{d}\right)$.

c. Находим

$$\sum_{\xi} e^{2\pi i \frac{\xi}{m}} = \sum_{d \setminus m} \mu(d) S_d,$$

где, полагая $m = m_0 a$, имеем

$$S_d = \sum_{u=0}^{m_0-1} e^{2\pi i \frac{u}{m_0}}.$$

Последнее равно 0 при $d < m$ и равно 1 при $d = m$. Отсюда и получаем теорему вопроса a.

d. Равенства следуют из вопроса **10, b.**

e. Имеем

$$A(m_1) \dots A(m_k) = m^{n-r} \sum_{a_1} \dots \sum_{a_k} S_{a_1, m_1} \dots S_{a_k, m_k},$$

где $a_1, \dots, a_k$ пробегают приведенные системы вычетов по модулям $m_1, \dots, m_k$. Отсюда (вопрос d) первое равенство вопроса следует непосредственно.

Аналогичным путем докажем и второе равенство.

13, a. Имеем

$$\sum_{x=0}^{p-1} e^{2\pi i \frac{nx}{p}} = \begin{cases} p, & \text{если } n \text{ кратно } p, \\ 0 & \text{в противном случае.} \end{cases}$$

b. Раскрывая произведение, отвечающее данному n, имеем

$$\sum_{d \setminus a} \frac{\mu(d)}{d} \sum_{x=0}^{d-1} e^{2\pi i \frac{nx}{d}}.$$

Отсюда, суммируя по всем $n = 0, 1, \dots, a-1$, и получим известное выражение для $\varphi(a)$.

14. Часть выражения, стоящего справа, отвечающая x, делящему a, равна 1, часть, отвечающая x, не делящему a, равна 0. Поэтому указанное выражение равно удвоенному числу делителей числа a, меньших $\sqrt{a}$, сложенному с δ, т. е. равно $\tau(a)$.

15, a. Имеем

$$(h_1 + h_2)^p = h_1^p + \binom{p}{1} h_1^{p-1} h_2 + \dots + \binom{p}{p-1} h_1 h_2^{p-1} + h_2^p \equiv h_1^p + h_2^p \pmod p;$$

$$(h_1 + h_2 + h_3)^p \equiv (h_1 + h_2)^p + h_3^p \equiv h_1^p + h_2^p + h_3^p \pmod p,$$

и т. д.

b. Полагая $h_1 = h_2 = \dots = h_a = 1$, из теоремы вопроса a получим теорему Ферма.

c. Пусть $(a, p) = 1$. При некоторых целых $N_1, N_2, \dots, N_\alpha$ имеем

$$a^{p-1} = 1 + N_1 p, \quad a^{p(p-1)} = (1 + N_1 p)^p = 1 + N_2 p^2,$$

$$a^{p^2(p-1)} = 1 + N_3 p^3, \quad \dots, \quad a^{p^{\alpha-2}(p-1)} = 1 + N_\alpha p^\alpha,$$

$$a^{\varphi(p^\alpha)} \equiv 1 \pmod{p^\alpha}.$$

Пусть $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — каноническое разложение числа m. Имеем

$$a^{\varphi(p^\alpha)} \equiv 1 \left(\mathrm{mod}\ p_1^{\alpha_1}\right), \quad \dots, \quad a^{\varphi(p^\alpha)} \equiv 1 \left(\mathrm{mod}\ p_k^{\alpha_k}\right),$$

$$a^{\varphi(m)} \equiv 1 \left(\mathrm{mod}\ p_1^{\alpha_1}\right), \quad \dots, \quad a^{\varphi(m)} \equiv 1 \left(\mathrm{mod}\ p_k^{\alpha_k}\right),$$

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Решения к главе IV

1, a. Теорема непосредственно следует из теоремы вопроса 11, a, гл. III.

b. Пусть d—делитель числа m, $m=m_0d$, H_d обозначает сумму слагаемых с условием $(a, m)=d$ в выражении для Tm вопроса a. Находим

$$H_d=\sum_{a_0}\sum_{x=0}^{m-1}\cdots\sum_{w=0}^{m-1}\varepsilon^{\frac{a_0f(x,\ \ldots,\ w)}{m_0}},$$

где a_0 пробегает приведенную систему вычетов по модулю m_0. Отсюда выводим

$$H_d=d^r\sum_{a_0}\sum_{x_0=0}^{m_0-1}\cdots\sum_{w_0=0}^{m_0-1}e^{\frac{a_0f(x_0,\ \ldots,\ w_0)}{m_0}}=m^rA(m_0).$$

c. Пусть $m>0$, $(a, m)=d$, $a=a_0d$, $m=m_0d$, T—число решений сравнения $ax\equiv b \pmod m$. Имеем

$$T_m=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}e^{\frac{2\pi i\,\alpha(ax-b)}{m}}=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}e^{2\pi i\frac{\alpha a_0}{m_0}x-2\pi i\frac{b\alpha}{m}}=$$

$$=m\sum_{\alpha_1=0}^{d-1}e^{-2\pi i\frac{b\alpha_1}{d}}=\begin{cases}md, & \text{если } b \text{ кратно } d,\\ 0 & \text{в противном случае.}\end{cases}$$

d. Полагая $(a, m)=d_1$, $(b, d_1)=d_2$, $\ldots$, $(f, d_{r-1})=d_r$, $m=d_1m_1$, $d_1=d_2m_2$, $\ldots$, $d_{r-1}=d_rm_r$, находим $d=d_r$,

$$T_m=\sum_{\alpha=0}^{m-1}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{2\pi i\frac{\alpha(ax+by+\ldots+fw+g)}{m}}=$$

$$=m\sum_{\alpha_1=0}^{d_1-1}\sum_{y=0}^{m-1}\cdots\sum_{w=0}^{m-1}e^{\frac{\alpha_1(by+\ldots+fw+g)}{d_1}}$$

. . . . . .

$$=m^{r-1}\sum_{\alpha_{r-1}=0}^{d_{r-1}-1}\sum_{w=0}^{m-1}e^{\frac{\alpha_{r-1}(fw+g)}{d_{r-1}}}=m^r\sum_{\alpha_r=0}^{d_r-1}e^{2\pi i\frac{\alpha_rg}{d_r}}.$$

e. Применим метод индукции. Пусть при обозначениях вопроса d теорема верна для r переменных. Рассмотрим сравнение

$$lv+ax+\ldots+fw+g\equiv 0 \pmod m. \qquad (2)$$

Пусть $(l, m)=d_0$. Условием возможности сравнения (2) будет $ax+\ldots+fw+g\equiv 0 \pmod{d_0}$. Последнее сравнение возможно лишь в случае, когда g кратно d', где $d'=(a, \ldots, f\ d_0)=(l, a, \ldots, f, m)$, причем тогда оно имеет $a_0^{r-1}a'$ решений. Следовательно,

сравнение (2) возможно лишь в случае, когда g кратно d', и тогда оно имеет $d_0^{r-1}d'\left(\frac{m}{d_0}\right)^r d_0 = m^r d'$ решений. Таким образом, теорема верна и для $r+1$ переменных. Но теорема верна для одного переменного. Значит, она верна всегда.

2, a. Имеем $a^{\varphi(m)} \equiv 1 \pmod m$, $a \cdot a^{\varphi(m)-1} \equiv b \pmod m$.

b. Имеем

$$1\cdot 2\ldots(a-1)\,ab\,(-1)^{a-1}\frac{(p-1)\ldots(p-a+1)}{1\cdot 2\ldots a} \equiv$$

$$\equiv b\cdot 1\cdot 2\ldots(a-1) \pmod p,$$

откуда, деля почленно на $1\cdot 2\ldots(a-1)$, и получим указанную теорему.

c, α) Выбирая надлежащим образом знак, имеем $b \pm m \equiv 0 \pmod 4$. Пусть 2^δ—наибольшаи степень 2, делящая $b \pm m$. При $\delta \geqslant k$ имеем

$$x \equiv \frac{b \pm m}{2^k} \pmod m.$$

Если же $\delta < k$, то имеем

$$2^{k-\delta}x \equiv \frac{b \pm m}{2^\delta} \pmod m.$$

С этим сравнением повторяем аналогичную операцию, и т. д.

β) Выбрав надлежащим образом знак, имеем $b \pm m \equiv 0 \pmod 3$. Пусть 3^δ—наибольшая степень 3, делящая $b \pm m$. При $\delta \geqslant k$ имеем

$$x \equiv \frac{b \pm m}{3^k} \pmod m.$$

Если же $\delta < k$, то имеем

$$3^{k-\delta}x \equiv \frac{b \pm m}{3^\delta} \pmod m.$$

С этим сравнением повторяем аналогичную операцию, и т. д.

γ) Пусть p—простой делитель числа a. Найдем t из условия $b+mt \equiv 0 \pmod p$. Пусть p^δ—наибольшаи степень p, делящая $(a, b+mt)$, и пусть $a = a_1 p^\delta$. Имеем

$$a_1 x \equiv \frac{b \pm m}{p^\delta} \pmod m.$$

Если $a_1 > 1$, то с этим новым сравнением повторяем аналогичную операцию, и т. д.

Указанный способ удобен в случае небольших простых сомножителей числа a.

3. Полагая $t = [\tau]$, пишем сравнении

$$a\cdot 0 \equiv 0 \pmod m,$$
$$a\cdot 1 \equiv y_1 \pmod m,$$
$$\ldots\ldots\ldots$$
$$a\cdot t \equiv y_t \pmod m,$$
$$a\cdot 0 \equiv m \pmod m.$$

Расположив эти сравнения в порядке возрастания правых частей (ср. вопрос 4, а, гл. II) и вычитая почленно каждое сравнение (кроме последнего) из следующего за ним, получим $t+1$ сравнений вида $az \equiv u \pmod m$; $0 < |z| \leqslant \tau$. При этом, по крайней мере, в одном сравнении будет $0 < u < \frac{m}{\tau}$. Действительно, u имеет $t+1 > \tau$ значений, эти значения положительные, и их сумма равна m.

4, а, α) Следует из определения символической дроби.

β) Здесь можно положить $b_0 = b + mt$, где t определяется из условия $b + mt \equiv 0 \pmod a$; тогда сравнению $ax \equiv b$ удовлетворяет целое число, представляемое обычной дробью $\frac{b_0}{a}$.

γ) Имеем (b_0 кратно a, d_0 кратно c)

$$\frac{b}{a} + \frac{d}{c} = \frac{b_0}{a} + \frac{d_0}{c} = \frac{b_0 c + a d_0}{ac} = \frac{bc + ad}{ac}.$$

δ) Имеем

$$\frac{b}{a} \cdot \frac{d}{c} = \frac{b_0}{a} \cdot \frac{d_0}{c} = \frac{b_0 d_0}{ac} = \frac{bd}{ac}.$$

b, α) Имеем (сравнения берутся по модулю p)

$$\binom{p-1}{a} \equiv \frac{(p-1)(p-2)\dots(p-a)}{1 \cdot 2 \dots a} \equiv \frac{(-1)^a 1 \cdot 2 \dots a}{1 \cdot 2 \dots a} \equiv (-1)^a.$$

Вопрос 2, b теперь проще решать так:

$$\frac{b}{a} \equiv \frac{b(-1)^{a-1}(p-1)\dots(p-(a-1))}{1 \cdot 2 \dots (a-1)\, a} \pmod p.$$

β) Имеем

$$\frac{2^p - 2}{p} \equiv 1 + \frac{p-1}{1 \cdot 2} + \frac{(p-1)(p-2)}{1 \cdot 2 \cdot 3} + \dots + \frac{(p-1)(p-2)\dots(p-(p-2))}{1 \cdot 2 \dots (p-1)} \pmod p.$$

5, а. Числа s, $s+1$, ..., $s+n-1$ попарно не могут иметь общего делителя с d. Произведения $s(s+1)\dots(s+n-1)$ могут быть объединены в n^x совокупностей по числу способов, сколькими число d может быть разбито на n попарно простых сомножителей с учетом порядка последних (вопрос 11, b, гл II). Пусть $d = u_1 u_2 \dots u_n$ — одно из таких разбиений. Число произведений с условием $s \equiv 0 \pmod{u_1}$,

$$s+1 \equiv 0 \pmod{u_2}, \ \dots, \ s+n-1 \equiv 0 \pmod{u_n}$$

равно $\frac{a}{d}$. Поэтому искомое число равно $n^x \frac{a}{d}$.

b. Указанное число равно

$$\sum_{d \setminus a} \mu(d) S_d; \quad S_d = \frac{n^x a}{d},$$

где $\varkappa$ — число различных простых делителей числа d. При этом

$$\sum_{a \setminus a} \mu(a) \frac{n^{\varkappa} a}{d} = a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\dots\left(1-\frac{n}{p_k}\right).$$

6. a. Все значения x, удовлетворяющие первому сравнению, даются равенством $x = b_1 + m_1 t$, где t — целое. Чтобы выбрать из них те, которые удовлетворяют также и второму сравнению, надо ограничиться лишь теми значениями t, которые удовлетворяют сравнению

$$m_1 t \equiv b_2 - b_1 \pmod{m_2}.$$

Но это сравнение разрешимо тогда и только тогда, когда $b_2 - b_1$ кратно d. При этом в случае разрешимости совокупность значений t, ему удовлетворяющих, определяется равенством вида $t = t_0 + \frac{m_2}{d} t'$, где t' — целое, вместе с тем совокупность значений x, удовлетворяющих рассматриваемой в вопросе системе, определится равенством

$$x = b_1 + m_1\left(t_0 + \frac{m_2}{d} t'\right) = x_{1,2} + m_{1,2} t', \quad x_{1,2} = b_1 + m_1 t_0.$$

b. В случае разрешимости системы

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}$$

совокупность значений x, ей удовлетворяющих, представится сравнением вида $x = x_{1,2} \pmod{m_{1,2}}$. В случае разрешимости системы

$$x \equiv x_{1,2} \pmod{m_{1,2}}, \quad x \equiv b_3 \pmod{m_3}$$

совокупность значений x, ей удовлетворяющих, представится сравнением вида $x \equiv x_{1,2,3} \pmod{m_{1,2,3}}$. В случае разрешимости системы

$$x \equiv x_{1,2,3} \pmod{m_{1,2,3}}, \quad x = b_4 \pmod{m_4}$$

совокупность значений x, ей удовлетворяющих, представится сравнением вида $x \equiv x_{1,2,3,4} \pmod{m_{1,2,3,4}}$ и т. д.

7. α) От замены x на $-x$ (вследствие чего x' заменится на $-x'$) величина суммы $\left(\frac{a, b}{m}\right)$ не изменится.

β) Когда x пробегает приведенную систему вычетов по модулю m, то и x' пробегает приведенную систему вычетов по модулю m.

γ) Полагая $x \equiv hz \pmod{m}$, получим

$$\left(\frac{a, bh}{m}\right) = \sum_z e^{2\pi i \frac{ahz + bz'}{m}} = \left(\frac{ah, b}{m}\right).$$

δ) Имеем

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right) = \sum_x \sum_y e^{2\pi i \frac{a_1 m_2 x + a_2 m_1 y + m_2 x' + m_1 y'}{m_1 m_2}}.$$

Полагая $m_2 x' + m_1 y' = z'$, имеем

$$(a_1 m_2 x + a_2 m_1 y)(m_2 x' + m_1 y') \equiv a_1 m_2^2 + a_2 m_1^2 \pmod{m_1 m_2},$$

$$\left(\frac{a_1, 1}{m_1}\right)\left(\frac{a_2, 1}{m_2}\right) = \left(\frac{m_2^2 a_1 + m_1^2 a_2, 1}{m_1 m_2}\right),$$

что и доказывает указанное свойство в случае двух сомножителей. Обобщение на случай более чем двух сомножителей тривиально.

8. Сравнение

$$a_0x^n+a_1x^{n-1}+\ldots+a_n-a_0(x-x_1)(x-x_2)\ldots(x-x_n)\equiv 0 \pmod p$$

имеет n решений. Оно степени ниже n. Следовательно, все его коэффициенты кратны p, а это и выражается сравнениями, указанными в вопросе.

9, a. При $p>3$ соответственно x, взятому из ряда $2, 3, \ldots, p-2$, найдем отличное от него число x' того же ряда с условием $xx'\equiv 1 \pmod p$; действительно, из $x=x'$ следовало бы $(x-1)(x+1)\equiv 0 \pmod p$; $x\equiv 1$ или $x\equiv p-1$. Поэтому

$$2\cdot 3\ldots(p-2)\equiv 1 \pmod p; \quad 1\cdot 2\ldots(p-1)\equiv -1 \pmod p.$$

b. Пусть $P>2$. Допустив, что P имеет делитель u с условием $1<u<P$, мы имели бы $1\cdot 2\ldots(P-1)+1\equiv 1 \pmod u$.

10, a. Находим h с условием $a_0h\equiv 1 \pmod m$. Данное сравнение равносильно такому:

$$x^n+a_1hx^{n-1}+\ldots+a_nh\equiv 0 \pmod m.$$

b. Пусть $Q(x)$ — частное и $R(x)$ — остаток от деления x^p-x на $f(x)$. Все коэффициенты $Q(x)$ и $R(x)$ — целые, $Q(x)$ — степени $p-n$, $R(x)$ — степени ниже n,

$$x^p-x=f(x)\,Q(x)+R(x).$$

Пусть сравнение $f(x)\equiv 0 \pmod p$ имеет n решений. Те же решения будут решениями и сравнения $R(x)\equiv 0 \pmod p$; поэтому все коэффициенты $R(x)$ кратны p.

Обратно, пусть все коэффициенты $R(x)$ кратны p. Тогда $f(x)\,Q(x)$ кратно p при тех же значениях x, что и x^p-x; поэтому сумма чисел решений сравнений

$$f(x)\equiv 0 \pmod p, \quad Q(x)\equiv 0 \pmod p$$

не меньше чем p. Пусть первое имеет α, а второе β решений. Из

$$\alpha\leqslant n, \quad \beta\leqslant p-n, \quad p\leqslant\alpha+\beta$$

выводим $\alpha=n$, $\beta=p-n$.

c. Возвышая данное сравнение почленно в степень $\frac{p-1}{n}$, убеждаемся в необходимости указанного условия. Пусть это условие выполнено; из $x^p-x=x\left(x^{p-1}-A^{\frac{p-1}{n}}+A^{\frac{p-1}{n}}-1\right)$ следует, что остаток от деления x^p-x на x^n-A есть $\left(A^{\frac{p-1}{n}}-1\right)x$, где $A^{\frac{p-1}{n}}-1$ кратно p.

11. Из $x_0^n\equiv A \pmod m$, $y^n\equiv 1 \pmod m$ следует $(x_0y)^n\equiv A \pmod m$; при этом произведения x_0y, отвечающие несравнимым (по модулю m) y, несравнимы. Из $x_0^n\equiv A \pmod m$, $x^n\equiv A \pmod m$ следует $x^n\equiv x_0^n \pmod m$, причем, определяя y условием $x\equiv yx_0 \pmod m$, имеем

$$y^n\equiv 1 \pmod m.$$

Решения к главе V

1. Указанное сравнение равносильно такому: $(2ax+b)^2 \equiv b^2 - 4ac \pmod m$. Соответственно каждому решению $z \equiv z_0 \pmod m$ сравнения $z^2 \equiv b^2 - 4ac \pmod m$ из $2ax+b \equiv z_0 \pmod m$ найдем одно решение указанного сравнения.

2, a. При $\left(\frac{a}{p}\right)=1$ имеем $a^{2m+1} \equiv 1 \pmod p$, $(a^{m+1})^2 \equiv a \pmod p$, $x \equiv \pm a^{m+1} \pmod p$.

b. При $\left(\frac{a}{p}\right)=1$ имеем $a^{4m+2} \equiv 1 \pmod p$, $a^{2m+1} \equiv \pm 1 \pmod p$, $a^{2m+2} \equiv \pm a \pmod p$. Ввиду $\left(\frac{2}{p}\right)=-1$ имеем также $2^{4m+2} \equiv -1 \pmod p$. Поэтому при некотором s, имеющем одно из значений 0; 1, получим

$$a^{2m+2}2^{(4m+2)s} \equiv a \pmod p, \quad x \equiv \pm a^{m+1}2^{(2m+1)s} \pmod p.$$

c. Пусть $p=2^k h+1$, где $k \geqslant 3$ и h — нечетное, $\left(\frac{a}{p}\right)=1$. Имеем

$$a^{2^{k-1}h} \equiv 1 \pmod p, \quad a^{2^{k-2}h} \equiv \pm 1 \pmod p, \quad N^{2^{k-1}h} \equiv -1 \pmod p.$$

Поэтому при некотором целом неотрицательном s_2 получим

$$a^{2^{k-2}h}N^{s_2 2^{k-1}} \equiv 1 \pmod p, \quad a^{2^{k-2}h}N^{s_2 2^{k-1}} \equiv \pm 1 \pmod p;$$

отсюда при некотором целом неотрицательном s_3 получим

$$a^{2^{k-3}h}N^{s_3 2^{k-2}} \equiv 1 \pmod p, \quad a^{2^{k-3}h}N^{s_3 2^{k-3}} \equiv \pm 1 \pmod p,$$

и т. д.; наконец, получим

$$a^h N^{s_k} \equiv 1 \pmod p, \quad x \equiv \pm a^{\frac{h+1}{2}} N^{s_k} \pmod p.$$

d. Имеем

$$1 \cdot 2 \ldots 2m\,(p-2m) \ldots (p-2)(p-1)+1 \equiv 0 \pmod p,$$
$$(1 \cdot 2 \ldots 2m)^2+1 \equiv 0 \pmod p.$$

3, a. Условия разрешимости сравнений (1) и (2) выводятся тривиально (e и h § 2). Сравнение (3) разрешимо тогда и только тогда, когда $\left(\frac{-3}{p}\right)=1$. Но $\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$, причем

$$\left(\frac{p}{3}\right) = \begin{cases} 1, & \text{если } p \text{ имеет вид } 6m+1, \\ -1, & \text{если } p \text{ имеет вид } 6m+5. \end{cases}$$

b. Каковы бы ни были различные простые $p_1, p_2, \ldots, p_k$ вида $4m+1$, наименьший простой делитель p числа $(2p_1p_2 \ldots p_k)^2+1$ будет отличен от $p_1, p_2, \ldots, p_k$ и ввиду $(2p_1p_2 \ldots p_k)^2+1 \equiv 0 \pmod p$ имеет вид $4m+1$.

c. Каковы бы ни были различные простые $p_1, p_2, \ldots, p_k$ вида $6m+1$, наименьший простой делитель p числа $(2p_1p_2 \ldots p_k)^2+3$ будет отличен от $p_1, p_2, \ldots, p_k$ и ввиду $(2p_1p_2 \ldots p_k)^2+3 \equiv 0 \pmod p$ имеет вид $6m+1$.

4. Среди чисел первой совокупности будут числа, сравнимые с $1\cdot1,\ 2\cdot2,\ \ldots,\ \frac{p-1}{2}\cdot\frac{p-1}{2}$, т. е. все квадратичные вычеты; число, входящее по условию во вторую совокупность, будет квадратичный невычет. Но во вторую совокупность войдут все произведения этого невычета на все вычеты, т. е. войдут все квадратичные невычеты.

5, а. Пусть в системе исчисления с основанием p

$$a = a_{\alpha-1}p^{\alpha-1} + \ldots + a_1 p + a_0$$

и искомое решение (наименьший неотрицательный вычет)

$$x = x_{\alpha-1}p^{\alpha-1} + \ldots + x_1 p + x_0. \qquad (1)$$

Составим таблицу:

$a_{\alpha-1}$	...	a_4	a_3	a_2	a_1	a_0
$2x_0x_{\alpha-1}$	...	$2x_0x_4$	$2x_0x_3$	$2x_0x_2$	$2x_0x_1$	x_0^2
$2x_1x_{\alpha-2}$	...	$2x_1x_3$	$2x_1x_2$	x_1^2		
$2x_2x_{\alpha-3}$	...	x_2^2				
...						

где в столбце под a_s стоят числа, сумма которых образует коэффициент при p^s в разложении квадрата правой части (1) по степеням p. Находим x_0 из условия

$$x_0^2 \equiv a_0 \pmod p.$$

Полагая $\frac{x_0^2 - a_0}{p} = p_1$, находим x_1 из условия

$$p_1 + 2x_0x_1 \equiv a_1 \pmod p.$$

Полагая $\frac{p_1 + 2x_0x_1 - a_1}{p} = p_2$, находим x_2 из условия

$$p_2 + 2x_0x_2 + x_1^2 \equiv a_2 \pmod p,$$

и т. д. При данном x_0 ввиду $(x_0,\ p) = 1$ числа $x_1,\ x_2,\ \ldots,\ x_{\alpha-1}$ определятся однозначно.

б. Здесь

$$a = a_{\alpha-1}2^{\alpha-1} + \ldots + a_3 2^3 + a_2 2^2 + a_1 2 + a_0,$$
$$x = x_{\alpha-1}2^{\alpha-1} + \ldots + x_3 2^3 + x_2 2^2 + x_1 2 + x_0.$$

и мы будем иметь следующую таблицу:

$a_{\alpha-1}$	...	a_4	a_3	a_2	a_1	a_0
$x_0x_{\alpha-2}$	...	x_0x_3	x_0x_2	x_0x_1		x_0^2
$x_1x_{\alpha-3}$	...	x_1x_2		x_1^2		
$x_2x_{\alpha-4}$	...	x_2^2				

Рассмотрим лишь случай $\alpha \geqslant 3$. Ввиду $(a, 2)=1$ необходимо $a_0=1$. Поэтому $x_0=1$. Далее необходимо $a_1=0$, и ввиду $x_0x_1+x_1^2=x_1+x_1^2 \equiv 0 \pmod 2$ необходимо $a_2=0$. Для x_1 возможны два значения: 0 и 1. Числа $x_2, x_3, \ldots, x_{\left[\frac{\alpha}{2}\right]}$ определятся однозначно, а для $x_{\left[\frac{\alpha}{2}\right]+1}$ возможны два значения: 0 и 1. Поэтому при $\alpha \geqslant 3$ необходимо $a \equiv 1 \pmod 8$, и тогда указанное сравнение имеет 4 решения.

6. Очевидно, P и Q — целые, причем Q по модулю p сравнимо с числом, которое получим, заменяя a на z^2, для чего достаточно $\sqrt{a}$ заменить на z. Поэтому $Q \equiv 2^{\alpha-1}z^{\alpha-1} \pmod p$; следовательно, $(Q, p)=1$ и Q' действительно можно определить из сравнения $QQ' \equiv 1 \pmod{p^\alpha}$. Имеем

$$P^2-aQ^2=(z+\sqrt{a})^\alpha (z-\sqrt{a})^\alpha=(z^2-a)^\alpha \equiv 0 \pmod{p^\alpha},$$

откуда

$$(PQ')^2 \equiv a\,(QQ')^2 \equiv a \pmod{p^\alpha}.$$

7. Пусть $m=2^\alpha p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — каноническое разложение числа m. Тогда m представляется в виде $m=2^\alpha ab$, где $(a, b)=1$, 2^k способами.

Пусть $\alpha=0$. Из $(x-1)(x+1) \equiv 0 \pmod m$ следует, что при некоторых a и b

$$x \equiv 1 \pmod a; \quad x \equiv -1 \pmod b.$$

Решая эту систему, получим $x \equiv x_0 \pmod m$. Поэтому указанное сравнение имеет 2^k решений.

Пусть $\alpha=1$. При некоторых a и b

$$x \equiv 1 \pmod{2a}; \quad x \equiv -1 \pmod{2b}.$$

Решая эту систему, получим $x \equiv x_0 \pmod m$. Поэтому указанное сравнение имеет 2^k решений.

Пусть $\alpha=2$. При некоторых a и b

$$x \equiv 1 \pmod{2a}; \quad x \equiv -1 \pmod{2b}.$$

Решая эту систему, получим $x=x_0 \left(\mathrm{mod}\ \frac{m}{2}\right)$. Поэтому указанное сравнение имеет 2^{k+1} решений.

Пусть $\alpha \geqslant 3$. При некоторых a и b должна выполняться одна из систем

$$x \equiv 1 \pmod{2a}; \qquad x \equiv -1 \pmod{2^{\alpha-1}b};$$
$$x \equiv 1 \pmod{2^{\alpha-1}a}; \quad x \equiv -1 \pmod{2b}.$$

Решая одну из этих систем, получим $x \equiv x_0 \left(\mathrm{mod}\ \frac{m}{2}\right)$. Поэтому указанное сравнение имеет 2^{k+2} решений.

8, a. Определяя x' сравнением $xx' \equiv 1 \pmod{p}$, имеем

$$\sum_{x=1}^{p-1}\left(\frac{x(x+k)}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{xx'(xx'+kx')}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{1+kx'}{p}\right).$$

Очевидно, $1+kx'$ пробегает все вычеты полной системы, кроме 1. Отсюда и следует указанная теорема.

b. Указанное равенство следует из

$$\tau = \frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)\right)\left(1+\eta\left(\frac{x+1}{p}\right)\right) =$$
$$= \frac{1}{4}\sum_{x=1}^{p-2}\left(1+\varepsilon\left(\frac{x}{p}\right)+\eta\left(\frac{x+1}{p}\right)+\varepsilon\eta\left(\frac{x(x+1)}{p}\right)\right).$$

c. Пусть δ обозначает число значений y, равных нулю (следовательно, $\delta = 0$ или $\delta = 1$). Имеем

$$S^2 \leqslant X\sum_{y_1}\sum_{y} S_{y_1, y}; \qquad S_{y_1, y} = \sum_{x=0}^{p-1}\left(\frac{(xy+k)(xy_1+k)}{p}\right).$$

При этом находим:

$$S_{y_1, y} = \begin{cases} p, & \text{если } y_1 = y = 0; \\ 0, & \text{если только одно из чисел } y_1 \text{ и } y \text{ равно нулю;} \end{cases}$$

$$S_{y_1, y} = \begin{cases} p-1 = p-\left(\frac{y_1 y}{p}\right), & \text{если } y_1 = y > 0; \\ -\left(\frac{y_1 y}{p}\right) & \text{в остальных случаях.} \end{cases}$$

Поэтому

$$S^2 \leqslant X\left(p\delta + p(Y-\delta) - \left(\sum_{y>0}\left(\frac{y}{p}\right)\right)^2\right) \leqslant XYp.$$

d, α) Имеем

$$S = \sum_{x=0}^{p-1}\sum_{z_1=0}^{Q-1}\sum_{z=0}^{Q-1}\left(\frac{(x+z_1)(x+z)}{p}\right).$$

При $z_1 = z$ суммированне по x дает $p-1$. При z_1, не равном z, суммирование по x (вопрос a) дает -1. Поэтому $S = pQ - Q^2$.

β) Согласно теореме вопроса α) имеем

$$T\,(Q^{0,5+0,5\lambda})^2 < pQ \quad T < pQ^{-\lambda}.$$

γ) При $p \leqslant 5$ теорема тривиальна. При $p > 5$ применим теорему вопроса α). Допустив, что в указанном в вопросе ряде квадратичных невычетов нет, убедимся, что $S_x = Q$ при $x = M,\ M+1,\ \ldots,\ M+Q$. Поэтому ($Q^2+2Q$ и Q^2+2Q+1 не равны p как составные) найдем

$$(Q+1)\,Q^2 \leqslant (p-Q)\,Q, \quad Q^2+2Q < p,\ (Q+1)^2 < p,$$

что невозможно.

9, a. Если m представляется в виде (1), то решение

$$z \equiv z_0 \pmod m \tag{5}$$

сравнения $x \equiv zy \pmod m$ является также и решением сравнении (2). Мы будем говорить, что указанное представление связано с решением (5) сравнения (2).

С каждым решением (5) сравнения (2) связано не менее одного представления (1). Действительно, взяв $\tau = \sqrt{m}$, имеем

$$\frac{z_0}{m} = \frac{P}{Q} + \frac{\theta}{Q\sqrt{m}}, \quad (P,\ Q) = 1;\ 0 < Q \leqslant \sqrt{m},\ |\theta| < 1.$$

Поэтому $z_0 Q = mP + r$, где $|r| < \sqrt{m}$. Далее, из (2) следует, что $|r|^2 + Q^2 \equiv 0 \pmod m$. Отсюда и из $0 < |r|^2 + Q^2 < 2m$ находим

$$m = |r|^2 + Q^2. \tag{6}$$

При этом $(|r|,\ Q) = 1$ ввиду

$$1 = \frac{r^2+Q^2}{m} = \frac{(z_0Q - mP)\,z_0Q - rmP + Q^2}{m} \equiv -rP \pmod Q.$$

Если $|r| = r$, то ввиду $r = z_0 Q \pmod m$ представление (6) связано с решением (5). Если $|r| = -r$, то ввиду $z_0^2 Q \equiv z_0 r \pmod m$, $Q \equiv z_0\,|r| \pmod m$, представление $m = Q^2 + |r|^2$ связано с решением (5). С каждым решением (5) связано не более одного представления (1). Действительно, если два представления $m = x^2 + y^2$ и $m = x_1^2 + y_1^2$ числа m в виде (1) связаны с одним и тем же решением (5), то из $x = z_0 y \pmod m$, $x_1 \equiv z_0 y_1 \pmod m$ следует $xy_1 = x_1 y \pmod m$. Поэтому $xy_1 = x_1 y$, откуда ввиду $(x,\ y) = (x_1,\ y_1) = 1$ следует $x = x_1$, $y = y_1$.

b. Если p представляется в виде (3), то решение

$$z \equiv z_0 \pmod p \tag{7}$$

сравнения $x \equiv zy \pmod p$ является также и решением сравнения (4). Мы будем говорить, что указанное представленне связано с решеннем (7) сравнения (4).

Зная решение (7) сравнения (4), найдем не менее одного представления (3). Действительно, взяв $\tau = \sqrt{p}$, имеем

$$\frac{z_0}{p} = \frac{P}{Q} + \frac{\theta}{Q\sqrt{p}}; \quad (P,\ Q) = 1, \quad 0 < Q \leqslant \sqrt{p},\ |\theta| < 1.$$

Поэтому $z_0 Q \equiv r \pmod p$, где $|r| < \sqrt{p}$. Далее из (4) следует, что $|r|^2 + aQ^2 \equiv 0 \pmod p$. Отсюда и из $0 < |r|^2 + aQ^2 < (1+a)p$ следует, что при $a=2$ должно быть или $|r|^2 + 2Q^2 = p$, или $|r|^2 + 2Q^2 = 2p$. В последнем случае $|r|$ — четное, $|r| = 2r_1$, $p = Q^2 + 2r_1^2$. При $a=3$ должно быть или $|r|^2 + 3Q^2 = p$, или $|r|^2 + 3Q^2 = 2p$, или $|r|^2 + 3Q^2 = 3p$. Второй случай невозможен: по модулю 4 левая часть сравнима с 0, а правая — с 2. В третьем случае $|r|$ кратно 3, $|r| = 3r_1$, $p = Q^2 + 3r_1^2$.

Допустив, что два представления $p = x_1^2 + ay_1^2$ и $p = x_2^2 + ay_2^2$ числа p в виде (3) связаны с одним и тем же решением сравнения (4), найдем $x = x_1$, $y = y_1$. Допустив, что эти представления связаны с различными решениями сравнения (4), найдем $x \equiv zy \pmod p$, $x_1 \equiv -zy_1 \pmod p$, откуда $xy_1 + x_1 y \equiv 0 \pmod p$, что ввиду $0 < (xy_1 + x_1 y)^2 \leqslant (x^2 + y^2)(x_1^2 + y_1^2) < p^2$ невозможно.

с, α) Слагаемые суммы $S(k)$ с $x = x_1$ и $x = -x_1$ равны.

β) Имеем

$$S(kt^2) = \sum_{x=0}^{p-1} \left(\frac{xt\,(x^2t^2 + kt^2)}{p} \right) = \left(\frac{t}{p} \right) S(k).$$

γ) Полагая $p - 1 = 2p_1$, имеем

$$p_1 (S(r))^2 + p_1 (S(n))^2 = \sum_{t=1}^{p_1} (S(rt^2))^2 + \sum_{t=1}^{p_1} (S(nt^2))^2 =$$

$$= \sum_{k=0}^{p-1} (S(k))^2 = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \sum_{k=0}^{p-1} \left(\frac{xy\,(x^2+k)\,(y^2+k)}{p} \right).$$

При y, не равном x или $p-x$, результат суммирования по k будет $-\left(\frac{xy}{p}\right)$; при $y = x$ или $y = p - x$ он будет $(p-1)\left(\frac{xy}{p}\right)$. Поэтому

$$p_1 (S(r))^2 + p_1 (S(n))^2 = 4pp_1, \quad p = \left(\frac{1}{2} S(r) \right)^2 + \left(\frac{1}{2} S(n) \right)^2.$$

10, а. Имеем

$$X^2 - DY^2 =$$

$$= (x_1 + y_1 \sqrt{D})(x_2 \pm y_2 \sqrt{D})(x_1 - y_1 \sqrt{D})(x_2 \mp y_2 \sqrt{D}) = k^2.$$

в. Взяв любое τ_1 с условием $\tau_1 > 1$, найдем целые x_1, y_1 с условиями $|y_1 \sqrt{D} - x_1| < \frac{1}{\tau_1}$, $0 < y \leqslant \tau_1$, откуда, умножая почленно на $y_1 \sqrt{D} + x_1 < 2y_1 \sqrt{D} + 1$, получим $|x_1^2 - Dy_1^2| < 2\sqrt{D} + 1$. Взяв $\tau_2 > \tau_1$ с условием $|y_1 \sqrt{D} - x_1| > \frac{1}{\tau_2}$, найдем новые целые x_2, y_2 с условием $|x_2^2 - Dy_2^2| < 2\sqrt{D} + 1$ и т. д.

Очевидно, в интервале $-2\sqrt{D}-1 < k < 2\sqrt{D}+1$ существует такое целое, не равное нулю k, что среди пар x_1, y_1; x_2, y_2; ... найдется бесчисленное множество пар x, y с условием $x^2-Dy^2=k$: среди же последних наверно найдутся две пары ξ_1, η_1 и ξ_2, η_2 с условием $\xi_1 \equiv \xi_2 \pmod{|k|}$, $\eta_1 \equiv \eta_2 \pmod{|k|}$. Определяя целые ξ_0, η_0 равенством $\xi_0+\eta_0\sqrt{D}=(\xi_1+\eta_1\sqrt{D})(\xi_2-\eta_2\sqrt{D})$, имеем (вопрос а)

$$\xi_0^2-D\eta_0^2=|k|^2; \quad \xi_0 \equiv \xi_1^2-D\eta_1^2 \equiv 0 \pmod{|k|};$$

$$\eta_0 \equiv -\xi_1\eta_1+\xi_1\eta_1=0 \pmod{|k|}.$$

Поэтому $\xi_0=\xi|k|$, $\eta_0=\eta|k|$, где ξ и η — целые и $\xi^2-D\eta^2=1$.

с. Числа x, y, определяемые равенством (2), удовлетворяют (вопрос а) уравнению (1).

Допустив существование пары целых положительных x, y, удовлетворяющих уравнению (1), но отличной от пар, определяемых равенством (2), мы при некотором $r=1, 2, \ldots$ будем иметь

$$(x_0+y_0\sqrt{D})^r < x+y\sqrt{D} < (x_0+y_0\sqrt{D})^{r+1}.$$

Отсюда, деля почленно на $(x_0+y_0\sqrt{D})^r$, получим

$$1 < X+Y\sqrt{D} < x_0+y_0\sqrt{D}, \tag{3}$$

где (вопрос а) X и Y — целые, определяемые равенством

$$X+Y\sqrt{D}=\frac{x+y\sqrt{D}}{(x_0+y_0\sqrt{D})^r}=(x+y\sqrt{D})(x_0-y_0\sqrt{D})^r$$

и удовлетворяющие уравнению

$$X^2-DY^2=1. \tag{4}$$

Но из (4) следуют неравенства $0 < X-Y\sqrt{D} < 1$, которые в соединении с первым неравенством (3) показывают, что X и Y — положительные. Поэтому второе неравенство (3) противоречит определению чисел x_0 и y_0.

11, а. Имеем

$$|S_{a,m}|^2=\sum_{t=0}^{m-1}\sum_{x=0}^{m-1} e^{\frac{2\pi i a(t^2+2tx)}{m}}.$$

При данном t суммирование по x дает $me^{\frac{2\pi i at^2}{m}}$ или 0, в зависимости от того, делится $2t$ на m или нет. При нечетном m имеем

$$|S_{a,m}|^2=me^{\frac{2\pi i a\cdot 0^2}{m}}=m.$$

При четном $m=2m_1$ имеем

$$|S_{a,m}|^2=m\left|e^{\frac{2\pi i a\cdot 0^2}{m}}+e^{\frac{2\pi i a\cdot m_1^2}{m}}\right|.$$

Здесь правая часть равна 0 при нечетном m_1 и равна $2m$ при четном m_1.

b, α) При любом целом b имеем

$$|S_{a,b}| = \left| \sum_{x=0}^{p-1} e^{2\pi i \frac{Ax^2+2Abx}{p}} \right|,$$

откуда, выбрав b из условия $2Ab \equiv a \pmod p$, мы и получим указанный результат.

β) Имеем

$$\sum_{x=M}^{M+Q-1} e^{2\pi i \frac{Ax^2}{p}} = \sum_{x=0}^{p-1} e^{2\pi i \frac{Ax^2}{p}} \sum_{z=M}^{M+Q-1} \frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i \frac{a(x-z)}{p}}.$$

Часть правой части, отвечающая $a=0$, численно равна $\frac{Q}{\sqrt{p}} < \sqrt{p}$. А оставшаяся часть численно не превосходит

$$\frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} \left| \sum_{z=M}^{M+Q-1} e^{2\pi i \frac{-az}{p}} \right| < \sqrt{p}\,(\ln p - 1).$$

γ) Имеем

$$T = \sum_{x=M_0}^{M_0+Q_0-1} \sum_{z=M}^{M+Q-1} \frac{1}{p} \sum_{a=0}^{p-1} e^{2\pi i \frac{a(Ax^2-z)}{p}}$$

Часть правой части, отвечающая $a=0$, равна $\frac{Q_0 Q}{p}$. А оставшаяся часть численно меньше чем

$$\frac{1}{\sqrt{p}} \ln p \sum_{a=1}^{p-1} \left| \sum_{z=M}^{M+Q-1} e^{2\pi i \frac{-az}{p}} \right| < \sqrt{p}\,(\ln p)^2.$$

δ) Пусть r пробегает квадратичные вычеты, а n пробегает квадратичные невычеты по модулю p, заключенные в ряде $1, \ldots, p-1$. Справедливость теоремы следует из равенств

$$S_{a,p} = 1 + 2\sum_r e^{2\pi i \frac{ar}{p}}, \quad 1 + \sum_r e^{2\pi i \frac{ar}{p}} + \sum_n e^{2\pi i \frac{an}{p}}.$$

ε) Имеем

$$|S_{a,p}|^2 = S_{a,p}\,\overline{S}_{a,p} = \sum_{t=1}^{p-1} \sum_{x=1}^{p-1} \left(\frac{t}{p}\right) e^{2\pi i \frac{ax(t-1)}{p}}.$$

При $t=1$ суммирование по x дает $p-1$, при $t>1$ оно дает $-\left(\frac{t}{p}\right)$. Поэтому

$$|S_{a,p}|^2 = p - 1 - \sum_{t=2}^{p-1} \left(\frac{t}{p}\right) = p, \quad |S_{a,p}| = \sqrt{p}.$$

Или (второе решение): имеем

$$|S_{a,p}|^2 = S_{a,p}\overline{S}_{a,p} = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x+t}{p}\right)\left(\frac{x}{p}\right)e^{2\pi i\frac{at}{p}}.$$

При $t=0$ суммирование по x дает $p-1$. При $t>0$ оно дает $-e^{2\pi i\frac{at}{p}}$ (вопрос 8). Поэтому

$$|S_{a,p}|^2 = p-1-\sum_{t=1}^{p-1}e^{2\pi i\frac{at}{p}} = p, \quad |S_{a,p}| = \sqrt{p}.$$

η) Следует из легко выводимого равенства

$$S_{a,p} = \left(\frac{a}{p}\right)S_{1,p}.$$

ϰ) Имеем

$$\sum_{x=M}^{M+Q-1}\left(\frac{x}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{z=M}^{M+Q-1}\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(x-z)}{p}}.$$

Часть правой части, отвечающая $a-0$, равна 0. Оставшаяся часть численно меньше, чем (вопрос η) и вопрос 11, с, гл. III)

$$\frac{1}{\sqrt{p}}\sum_{a=1}^{p-1}\left|\sum_{z=M}^{M+Q-1}e^{2\pi i\frac{-az}{p}}\right| < \sqrt{p}\ln p.$$

λ) Следует из неравенства вопроса ϰ) и равенства $R+N=Q$.

μ) Часть суммы с $\left(\frac{a}{p}\right)=1$ равна $p(R^2+N^2)$, а часть суммы с $\left(\frac{a}{p}\right)=-1$ равна $-2pRN$. Поэтому вся сумма равна $p(R-N)^2$.

Часть суммы с $a=0$ равна 0, а оставшаяся часть численно меньше, чем

$$\sum_{a=1}^{p-1}\left|\sum_{x=M}^{M+Q-1}e^{2\pi i\frac{ax}{p}}\right|\left|\sum_{\alpha=1}^{p-1}\left|\sum_{y=M}^{M+Q-1}e^{2\pi i\frac{-a\alpha y}{p}}\right| < p^2(\ln p)^2.$$

Следовательно,

$$p(R-N)^2 < p^2(\ln p)^2, \quad |R-N| < \sqrt{p}\ln p.$$

ν) Теорема будет доказана, если покажем, что при $Y=[3\sqrt{p}]$ сумма

$$T = \sum_{x=1}^{p-1}\left(\frac{x}{p}\right)\sum_{y=0}^{Y-1}\sum_{y_1=0}^{Y-1}\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(x-M-y-y_1)}{p}}$$

будет меньше, чем Y^2. Но часть суммы T, отвечающая $a=0$, равна нулю, а оставшаяся часть численно меньше, чем

$$\frac{2}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\min\left(Y^2, \frac{1}{4\left(\frac{a}{p}\right)^2}\right) <$$

$$< \frac{2}{\sqrt{p}}\left(\int_0^{\frac{p}{2Y}} Y^2\,da + Y^2 + \int_{\frac{p}{2Y}}^{\infty}\frac{p^2}{4a^2}\,da\right) = Y^2\left(\frac{2\sqrt{p}}{Y}+\frac{2}{\sqrt{p}}\right) < Y^2.$$

Решения к главе VI

1, a. Если q — простое нечетное и $a^p \equiv 1 \pmod q$, то a по модулю q принадлежит одному из показателей $\delta = 1; p$. При $\delta = 1$ имеем $a \equiv 1 \pmod q$, при $\delta = p$ имеем $q - 1 = 2px$; x — целое.

b. Если q — простое нечетное и $a^p + 1 \equiv 0 \pmod q$, то $a^{2p} \equiv 1 \pmod q$. Поэтому a по модулю q принадлежит одному из показателей $\delta = 1, 2, p, 2p$. Случаи $\delta = 1; p$ невозможны. При $\delta = 2$ имеем $a^2 = 1 \pmod q$, $a + 1 \equiv 0 \pmod q$. При $\delta = 2p$ имеем $q - 1 = 2px$; x — целое.

c. Простыми вида $2px + 1$ будут, например, простые делители числа $2^p - 1$. Пусть $p_1, p_2, \ldots, p_k$ — какие-либо k простых чисел вида $2px + 1$; число $(p_1 p_2 \ldots p_k)^p - 1$ имеет простой делитель вида $2px + 1$, отличный от $p_1, p_2, \ldots, p_k$.

d. Если q — простое и $2^{2^n} + 1 \equiv 0 \pmod q$, то $2^{2^{n+1}} \equiv 1 \pmod q$. Поэтому 2 по модулю q принадлежит показателю 2^{n+1} и, следовательно, $q - 1 = 2^{n+1}x$; x — целое.

2. Очевидно, a по модулю $a^n - 1$ принадлежит показателю n. Поэтому n — делитель $\varphi(a^n - 1)$.

3, a. Пусть после k-й операции снова получается исходный ряд. Очевидно, k-я операция равносильна следующей в ряде

$$1, 2, \ldots, n-1, n, n-1, \ldots, 2, 1, 2, \ldots$$
$$\ldots, n-1, n, n, n-1, \ldots, 2, 1, 2, \ldots$$

берутся числа, стоящие на $1, 1+2^k, 1+2\cdot 2^k, \ldots$ местах. Поэтому на $1+2^k$ месте в исходном ряде должно стоять число 2. Следовательно, указанное в вопросе условие необходимо. Достаточность этого условия очевидна.

b. Решение аналогично решению вопроса a.

4. Решение сравнения $x^\delta \equiv 1 \pmod p$ принадлежит показателю вида $\frac{\delta}{\delta'}$, где δ' — делитель δ. При этом δ' кратно d тогда и только тогда, когда $x^{\frac{\delta}{d}} \equiv 1 \pmod p$. Выписав все $\tau(\delta)$ значений δ' и взяв $f = 1$, получим $S' = \sum_{d \mid \delta} \mu(d) S_d$, где S' — искомое число и $S_d = \frac{\delta}{d}$.

5, a. Здесь (§ 3; пример с. § 5) должно быть $\left(\frac{g}{2^n+1}\right)=-1$. Это требование выполняется при $g=3$.

b. Здесь не должно быть $\left(\frac{g}{2p+1}\right)=1$, $g^2\equiv 1 \pmod{2p+1}$. Это требование выполняется при указанных значениях g.

c. Здесь не должно быть $\left(\frac{g}{4p+1}\right)=1$, $g^2\equiv 1 \pmod{4p+1}$. Это требование выполняется при $g=2$.

d. Здесь не должно быть $\left(\frac{g}{2^n p+1}\right)=1$, $g^{2^{n-1}}\equiv 1 \pmod{2^n p+1}$. Это требование выполняется при $g=3$.

6, a, α) При n, кратном $p-1$, теорема очевидна. Пусть n не делится на $p-1$. Числа $1, 2, \ldots, p-1$, если отвлечься от порядка их следования, по модулю p сравнимы с числами $g, 2g, \ldots, (p-1)g$, где g — первообразный корень по модулю p. Поэтому

$$S_n \equiv g^n S_n \pmod{p}, \quad S_n = 0 \pmod{p}.$$

β) Имеем

$$\sum_{x=1}^{p-1}\left(\frac{x(x^2+1)}{p}\right) \equiv \sum_{x=1}^{p-1} x^{\frac{p-1}{2}} (x^2+1)^{\frac{p-1}{2}} \pmod{p},$$

откуда (вопрос α)) и получается указанный результат.

b. При $p>2$ имеем

$$1\cdot 2 \ldots (p-1) \equiv g^{1+2+\ldots+p-1} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

7. Имеем $g_1^{\operatorname{ind}_{g_1} a} \equiv a \pmod{p}$, $\operatorname{ind}_{g_1} a \operatorname{ind}_g g_1 \equiv \operatorname{ind}_g a \pmod{p-1}$, $\operatorname{ind}_{g_1} a \equiv \alpha \operatorname{ind}_g a \pmod{p-1}$.

8, α) Имеем

$$|S|^2 \leqslant X \sum_{x=0}^{m-1} \sum_{y_1=0}^{m-1} \sum_{y=0}^{m-1} \eta(y_1)\overline{\eta(y)}\, e^{2\pi i \frac{ax(y_1-y)}{m}}.$$

При данных y_1 и y суммирование по x дает $Xm|\eta(y)|^2$ или нуль, в зависимости от того, будет ли y_1-y или нет. Поэтому

$$|S|^2 \leqslant XYm, \quad |S| \leqslant \sqrt{XYm}.$$

β) Имеем

$$S = \frac{1}{\varphi(m)} \sum_x{}' \sum_y{}' e^{2\pi i \frac{ax^n y^n}{m}} = \frac{1}{\varphi(m)} \sum_u \sum_v \xi(u)\eta(v) e^{2\pi i \frac{auv}{m}},$$

где $\xi(u)$ — число решений сравнения $x^n \equiv u \pmod{m}$, $\eta(v)$ — число решений сравнения $y^n \equiv v \pmod{m}$. Здесь $\xi(u)$ не превосходит K (вопрос 11, гл. IV), а сумма всех значений $\xi(u)$ равна $\varphi(m)$. Поэтому

$$\sum_u |\xi(u)|^2 \leqslant K\varphi(m).$$

Аналогично находим

$$\sum_v |\eta(v)|^2 \leqslant K\varphi(m).$$

Следовательно (вопрос α)),

$$|S| \leqslant \frac{1}{\varphi(m)} \sqrt{K\varphi(m) K\varphi(m)\, m} = K\sqrt{m}.$$

γ) Сравнение $x^n \equiv 1 \pmod m$ равносильно системе

$$x^n \equiv 1 \pmod{2^\alpha}, \quad x^n \equiv 1 \pmod{p_1^{\alpha_1}}, \quad \ldots, \quad x^n \equiv 1 \pmod{p_k^{\alpha_k}}.$$

Пусть $\gamma(x)$ и $\gamma_0(x)$ — индексы числа x по модулю 2^α (g, § 6), сравнение $x^n \equiv 1 \pmod{2^\alpha}$ равносильно системе $n\gamma(x) \equiv 0 \pmod c$, $n\gamma_0(x) \equiv 0 \pmod{c_0}$. Первое сравнение этой системы имеет не более 2 решений, второе — не более n решений. Поэтому сравнение $x^n \equiv 1 \pmod{2^\alpha}$ имеет не более $2n$ решений. Согласно b, § 5 каждое из сравнений $x^n \equiv 1 \pmod{p_1^{\alpha_1}}$, ..., $x^n \equiv 1 \pmod{p_k^{\alpha_k}}$ имеет не более n решений. Следовательно, $K < 2n^{k+1}$. Отсюда при постоянном n будем иметь (вопрос 11, c, гл. II)

$$K \leqslant 2\,(\tau(m))^{\frac{\ln n}{\ln 2}} = O(m^\varepsilon).$$

9, a. Имеем

$$S = \frac{1}{p-1} \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} e^{2\pi i \frac{ax^n y^n + bxy}{p}},$$

$$|S|^2 \leqslant \frac{1}{p-1} \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} \psi(u, v) S_{u,v}; \quad S_{u,v} = \sum_{x=1}^{p-1} e^{2\pi i \frac{ax^n u + bxv}{p}},$$

где $\psi(u, v)$ — число решений системы

$$y_1^n - y^n \equiv u \pmod p, \quad y_1 - y \equiv v \pmod p,$$

когда y_1 и y независимо друг от друга пробегают значения 1, ..., $p-1$. Поэтому

$$|S|^2 \leqslant \frac{UV}{(p-1)^2}; \quad U = \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} (\psi(u, v))^2, \quad V = \sum_{u=0}^{p-1} \sum_{v=0}^{p-1} |S_{u,v}|^2.$$

Нетрудно видеть, что $\psi(0, 0) = p-1$, $\psi(u, 0) = 0$ при $u > 0$ и $\psi(u, v) \leqslant 2n_1$ при $v > 0$. Поэтому

$$U < (p-1)^2 + 2p(p-1)n_1 < 3p(p-1)n_1.$$

Кроме того, находим $V < p^2(p-1)$. Следовательно,

$$|S|^4 < 3p^3 n_1, \quad |S| < \frac{3}{2} n_1^{\frac{1}{4}} p^{\frac{3}{4}}.$$

b. Имеем

$$\sum_{x=M}^{M+Q-1} e^{2\pi i \frac{ax^n}{p}} = \sum_{x=1}^{p-1} e^{2\pi i \frac{ax^n}{p}} \sum_{z=M}^{M+Q-1} \frac{1}{p} \sum_{b=0}^{p-1} e^{2\pi i \frac{b(x-z)}{p}}.$$

Часть правой части, отвечающая $b=0$, численно $< n\sqrt{p}$ (вопр. 8). А оставшаяся часть численно не превосходит

$$\frac{3}{2} n_1^{\frac{1}{4}} p^{\frac{3}{4}-1} \sum_{b=1}^{p-1} \left| \sum_{z=M}^{M+Q-1} e^{2\pi i \frac{-bz}{p}} \right| < \frac{3}{2} n_1 p^{\frac{3}{4}} \ln p.$$

c. Имеем

$$T = \sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i \frac{ax^n}{p}} \sum_{z=M}^{M+Q-1} \frac{1}{p} \sum_{b=0}^{p-1} e^{2\pi i \frac{b(x^n-z)}{p}}.$$

Часть правой частн, отвечающая $b=0$, равна $\frac{Q_0 Q}{p}$. А оставшаяся часть численно меньше

$$\frac{3}{2} n_1 p^{\frac{3}{4}} \ln p \sum_{b=1}^{p-1} \left| \sum_{z=M}^{M+Q-1} e^{2\pi i \frac{-bz}{p}} \right| < \frac{3}{2} n_1 p^{\frac{3}{4}} (\ln p)^2.$$

Решения к главе VII

1, α) Определив прн $(x, p)=1$ число x' сравнением $xx' \equiv 1 \pmod p$, находим

$$\sum_{x=1}^{p-1} \overline{\chi(x)}\, \chi(x+k) = \sum_{x=1}^{p-1} \chi(1+kx') = -1.$$

β) Имеем

$$S = \sum_{x=0}^{p-1} \sum_{z_1=0}^{Q-1} \sum_{z=0}^{Q-1} \overline{\chi(x+z_1)}\, \chi(x+z).$$

Прн $z_1=z$ суммнрованне по x дает $p-1$. Прн z_1, не равном z, суммнрованне по x (вопрос а) дает -1. Поэтому

$$S = Q(p-1) - Q(Q-1) = (p-Q)Q.$$

2, α) Имеем

$$|U_{a,p}|^2 = \sum_{t=1}^{p-1} \sum_{x=1}^{p-1} \chi(xt)\, \overline{\chi(x)}\, e^{2\pi i \frac{a(tx-x)}{p}} =$$

$$= \sum_{t=1}^{p-1} \sum_{x=1}^{p-1} \chi(t)\, e^{2\pi i \frac{a(t-1)x}{p}} = p-1-\sum_{t=2}^{p-1} \chi(t) = p.$$

β) При $(a, p)=p$ теорема тривиальна. При $(a, p)=1$ имеем

$$U_{a,p}=(\chi(a))^{-1}\sum_{x=1}^{p-1}\chi(ax)e^{2\pi i\frac{ax}{p}}=(\chi(a))^{-1}U_{1,p}.$$

γ) Очевидно, A и B—целые, причем $|S|^2=A^2+B^2$. Находим вопрос β))

$$S=\frac{1}{\varepsilon\sqrt{p}\,\overline{\varepsilon\sqrt{p}}}\sum_{z_1=1}^{p-1}\sum_{z=1}^{p-1}\sum_{x=0}^{p-1}e^{-2\pi i\frac{\operatorname{ind}z_1+\operatorname{ind}z}{4}}e^{2\pi i\frac{z_1x+z(x+1)}{p}};\ |\varepsilon|=1.$$

При z_1+z, не равном нулю, суммирование по x дает нуль. Поэтому

$$S=\varepsilon'\sum_{z=1}^{p-1}\left(\frac{z}{p}\right)e^{2\pi i\frac{z}{p}}=\varepsilon''\sqrt{p},\quad|\varepsilon'|=|\varepsilon''|=1,\quad S^2=p.$$

δ) Имеем

$$\sum_{x,s}e^{2\pi i\frac{axs}{n}}=\nu\sum_{x=1}^{p-1}\sum_{z=0}^{n-1}e^{2\pi i\frac{z(\operatorname{ind}x-s)}{n}}e^{2\pi i\frac{ax}{p}}.$$

Часть правой части, отвечающая $z=0$, равна $-\nu$. А оставшаяся часть численно меньше $(1-\nu)\sqrt{p}$ (вопрос α)).

3, α) При $(z, p)=1$ сравнение $x^n\equiv z\pmod p$ возможно лишь в случае, когда $\operatorname{ind}z$ делится на δ, причем тогда это сравнение имеет δ решений. Следовательно,

$$S_{a,p}=1+\delta\sum_{z_0}e^{2\pi i\frac{az_0}{p}},$$

где z_0 пробегает числа приведенной системы вычетов по модулю p с условием $\operatorname{ind}z_0\equiv 0\pmod\delta$. Поэтому

$$S_{a,p}-1\mid\delta\left(-\frac{1}{\delta}+\theta_s\left(1-\frac{1}{\delta}\right)\sqrt{p}\right)=\theta'(\delta-1)\sqrt{p}.$$

β) Полагая

$$x=u+p^{s-1}v;\quad u=0,\ \ldots,\ p^{s-1}-1;\quad v=0,\ \ldots,\ p-1,$$

имеем

$$e^{2\pi i\frac{axn}{p^s}}=e^{2\pi ia\,(u^np^{-s}+nu^{n-1}p^{-1}v)}$$

При $(u, p)=1$ суммирование по v дает нуль. Поэтому $(x=pz)$

$$S_{a,p^s}=\sum_{z=0}^{p^{s-1}-1}e^{2\pi iap^{-s}+n_2n}=p^{s-1}S_{a,p}.$$

γ) Полагая

$$(n, p^s)=p^\sigma,\quad x=u+p^{s-\sigma-1}v.\quad u=0,\ \ldots,\ p^{s-\sigma-1}-1,$$
$$v=0,\ \ldots,\ p^{\sigma+1}-1,$$

находим

$$e^{\frac{2\pi i}{p^s}\frac{a\lambda^n}{}} = e^{2\pi i a\,(u^n p^{-s} + nu^{n-1}p^{-s-1}v)}.$$

При $(u, p)=1$ суммирование по v дает нуль. Поэтому $(x=pz)$

$$S_{a,\,p^s} = \sum_{z=0}^{p^{s-1}-1} e^{2\pi i \frac{az^n}{p^{s-n}}} = p^{s-1}S_{a,\,p^{s-n}}.$$

б) Пусть $p_1^{\alpha_1}\dots p_k^{\alpha_k}$ — каноническое разложение числа m. Полагая

$$T_{a,\,m} = m^{-1+\nu}S_{a,\,m},\quad \nu=\frac{1}{n},\quad m = M_1p_1^{\alpha_1} = \dots = M_kp_k^{\alpha_k}$$

и определяя $a_1, \dots, a_k$ из условия $a \equiv M_1a_1 + \dots + M_ka_k \pmod m$, имеем (вопросы 12, d и 9, a, гл. III)

$$T_{a,\,m} = T_{a_1,\,p_1^{\alpha_1}}\dots T_{a_k,\,p_k^{\alpha_k}}.$$

Но при $s=1$ имеем

$$|T_{a,\,p}| < p^{-1+\nu}n\sqrt{p} < np^{-\frac{1}{6}}.$$

При $1 < s \leqslant n$, $(n, p)=p$ имеем

$$|T_{a,\,p^s}| \leqslant p^{-s+s\nu}p^s \leqslant n.$$

При $1 < s \leqslant n$, $(n, p)=1$ имеем

$$|T_{a,\,p^s}| = p^{-s+s\nu}p^{s-1} \leqslant 1;$$

наконец, случай $s>n$, ввиду $|T_{a,\,p^s}| = p^{-s+s\nu}p^{n-1}|S_{a,\,p^{s-n}}| = |T_{a,\,p^{s-n}}|$ сводится к случаю $0 < s \leqslant n$. Следовательно, при некотором C, зависящем только от n, будем иметь

$$|T_{a,\,m}| < C,\quad |S_{a,\,m}| < Cm^{1-\nu}.$$

4, α) Имеем

$$\sum_{x=M}^{M+Q-1}\chi(x) - \sum_{x=1}^{p-1}\chi(x)\sum_{z=M}^{M+Q-1}\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(x-z)}{p}}.$$

Часть правой части, отвечающая $a=0$, равна нулю. А оставшаяся часть численно не превосходит $\sqrt{p}\,(\ln p - 1)$.

β) Имеем

$$T = \sum_{x=M}^{M+Q-1}\frac{1}{n}\sum_{a=0}^{n-1}e^{\frac{2\pi i}{n}a(\operatorname{ind} x - s)}.$$

Часть правой части, отвечающая $a=0$, равна $\frac{Q}{n}$. А оставшаяся часть численно меньше $\sqrt{p}\ln p$.

γ) Теорема будет доказана, если при $Y=[4n\sqrt{p}]$ будет показано, что сумма

$$T=\sum_{x=1}^{p-1}\chi(x)\sum_{y=0}^{Y-1}\sum_{y_1=0}^{Y-1}\frac{1}{\bar{r}}\sum_{a=0}^{p-1}e^{2\pi i\frac{a(x-M-y-y_1)}{p}}$$

будет меньше, чем νY^2. Но часть суммы T, отвечающая $a=0$, равна нулю. А оставшаяся часть численно меньше, чем

$$\frac{2}{\sqrt{p}}\sum_{a=1}^{\frac{p-1}{2}}\min\left(Y^2,\frac{1}{4\left(\frac{a}{p}\right)^2}\right)\leqslant\frac{2}{\sqrt{p}}\left(\int_0^{\frac{p}{2Y}}Y^2\,da+Y^2+\int_{\frac{p}{2Y}}^{\infty}\frac{p^2}{4a^2}\,da\right)=$$

$$=Y^2\left(\frac{2\sqrt{p}}{Y}+\frac{2}{\sqrt{p}}\right),\quad |T|<Y^2\left(\frac{2\sqrt{p}}{Y}+\frac{3}{\sqrt{p}}\right)<\nu Y^2.$$

δ) Взяв $f(x)=1$ и заставляя x пробегать значения $x=\operatorname{ind}M,\ \ldots,\ \operatorname{ind}(M+Q-1)$, получим (вопрос 17, а, гл. II)

$$S'=\sum_{d\backslash p-1}\mu(d)\,S_d,$$

здесь S' — число значений x с условием $(x,\ p-1)=1$, поэтому $S'=H$. Далее, S_d — число значений x, кратных d. Поэтому

$$H=\sum_{d\backslash p-1}\mu(d)\left(\frac{Q}{d}+\theta_d\sqrt{p}\right);\quad |\theta_d|<1,\ |\theta_1|=0.$$

ε) Имеем

$$J=\sum_{x=M}^{M+Q-1}\sum_{z=M_1}^{M_1+Q_1-1}\frac{1}{p-1}\sum_{a=0}^{p-2}e^{2\pi i\frac{a(x-z)}{p-1}}.$$

Часть правой части, отвечающая $a=0$, равна $\frac{QQ_1}{p-1}$. А оставшаяся часть численно меньше

$$\sqrt{p}\ln p\,\frac{1}{p-1}\sum_{a=1}^{p-2}\left|\sum_{z=M_1}^{M_1+Q_1-1}e^{2\pi i\frac{-az}{p-1}}\right|<\sqrt{p}\,(\ln p)^2.$$

η) Допустим, что невычетов, не превосходящих h, нет. Число невычетов степени n средн чисел

$$1,\ \ldots,\ Q;\quad Q-[\sqrt{p}\,(\ln p)^2]$$

можно оценить двумя способами: исходя из формулы вопроса β) и исходя из того, что невычетами могут быть лишь числа, делящиеся на простые, большие h. Получим

$$1-\frac{1}{n}<\ln\frac{\frac{1}{c}\ln p+2\ln\ln p}{\frac{1}{c}\ln p+2\ln\ln p}+O\left(\frac{1}{\ln p}\right),$$

$$0<\ln\frac{1+4\frac{\ln\ln p}{\ln p}}{1+2c\frac{\ln\ln p}{\ln p}}+O\left(\frac{1}{\ln p}\right).$$

Невозможность последнего неравенства при всех достаточно больших p и доказывает теорему.

5. Имеем

$$S=\frac{1}{\varphi(m)}\sum_{u}\sum_{v}\chi(u)\,\chi(v)\,e^{2\pi i\frac{au^nv^n}{m}},$$

где u и v пробегают приведенные системы вычетов по модулю m. Отсюда

$$S=\frac{1}{\varphi(m)}\sum_{x=0}^{m-1}\sum_{y=0}^{m-1}\nu(x)\,\rho(y)\,e^{2\pi i\frac{axy}{m}};$$

$$\nu(x)=\sum_{u^n\equiv x\pmod m}\chi(u),\quad \rho(y)=\sum_{u^n\equiv y\pmod m}\chi(v),$$

где имеем (вопрос 8, α), гл. VI и вопрос 11, гл. IV)

$$\sum_{x=0}^{m-1}|\nu(x)|^2\leqslant K\varphi(m),\quad \sum_{y=0}^{m-1}|\rho(y)|^2\leqslant K\varphi(m).$$

Поэтому

$$|S|\leqslant\frac{1}{\varphi(m)}\sqrt{K\varphi(m)\,K\varphi(m)\,m}=K\sqrt{m}.$$

6, α) Пусть $p-1=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ — каноническое разложение числа $p-1$; $p_1=2$. Пусть $s_1, s_1', s_2, s_2', \dots, s_k, s_k'$ пробегают значения, подчиненные условиям:

$s_1=0,\ s_1'=1$, если $\alpha_1=1$,

$s_1\equiv 0\pmod 2,\quad 0\leqslant s_1\leqslant 2^{\alpha_1}$

$s_1'\equiv 1\pmod 2,\quad 0<s_1'<2^{\alpha_1}$ } если $\alpha_1>1$,

. . . . . .

$s_r\equiv 0,\ \dots,\ \frac{p_r-1}{2},\quad 0\leqslant s_r\leqslant p_r^{\alpha_r}$

$s_r'\equiv 1,\ \dots,\ \frac{p_r-1}{2},\quad 0<s_r'\leqslant p_r^{\alpha_r}$ } если $r>1$.

Пусть $M_r=(p-1)\,p_r^{-\alpha_r}r$ и z и z' пробегают значения

$$z=M_1s_1+M_2s_2+\ldots+M_ks_k,$$
$$z'=M_1s_1'+M_2s_2'+\ldots+M_ks_k'.$$

Легко видеть, что z пробегает

$$u=(p-1)\,2^{-k}\left(1+\frac{1}{p_2}\right)\ldots\left(1+\frac{1}{p_k}\right)$$

значений, а z' пробегает

$$v=(p-1)\,2^{-k}\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right)$$

значений, причем

$$uv=(p-1)^2\,2^{-2k}\left(1-\frac{1}{p_2^2}\right)\ldots\left(1-\frac{1}{p_k^2}\right)>\frac{4}{5}\,(p-1)^2\,2^{-2k}.$$

Теперь рассмотрим сумму

$$W=\sum_t S_t,\quad S_t=\sum_z\sum_{z'}e^{2\pi i\,\frac{ag^{tz}\,g^{tz'}}{p}},$$

где g—какой-либо первообразный корень по модулю p и t пробегает приведенную систему вычетов по модулю p. Очевидно, имеем

$$W=uvS.$$

С другой стороны, находим

$$S_t=\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\xi(x)\,\eta(y)\,e^{2\pi i\,\frac{axy}{p}},$$

где $\xi(x)$—число решений сравнения $g^{tz}\equiv x\pmod p$, а $\eta(y)$—число решений сравнения $g^{tz'}\equiv y\pmod p$. Очевидно, $X=u$, $Y=v$ (вопрос 8, α), гл. VI). Поэтому

$$|S_t|<\sqrt{uvp},\quad |S|<\frac{\varphi(p-1)}{\sqrt{uv}}\sqrt{p}<\frac{9}{8}\,\frac{\varphi(p-1)}{p-1}\,2^k\sqrt{p}.$$

β) Имеем

$$T=\sum_g\sum_{z=M}^{M+Q-1}\frac{1}{p}\sum_{a=0}^{p-1}e^{2\pi i\,\frac{a(g-z)}{p}}.$$

Часть правой части этого равенства, отвечающая $a=0$, равна $\frac{\varphi(p-1)\,Q}{p}$. Оставшая часть численно не превосходит

$$\frac{9}{8}\,\frac{\varphi(p-1)}{p-1}\,2^k\sqrt{p}\,\frac{1}{p}\sum_{a=1}^{p-1}\left|\sum_{z=M}^{M+Q-1}e^{2\pi i\,\frac{-az}{p}}\right|<\frac{9}{8}\,\frac{\varphi(p-1)}{p-1}\,2^k\sqrt{p}\ln p.$$

Поэтому

$$T=\frac{\varphi(p-1)}{p-1}\left(Q+\theta\,\frac{9}{8}\,2^k\sqrt{p}\ln p\right).$$

ОТВЕТЫ К ЧИСЛЕННЫМ ПРИМЕРАМ

Ответы к главе I

1, a. 17. b. 23.

2, a. α) $\delta_4 = \frac{15}{11}$; β) $\alpha = \frac{19}{14} + \frac{\theta}{14 \cdot 20}$.

b. α) $\delta_6 = \frac{80}{59}$; β) $\alpha = \frac{1002}{739} + \frac{\theta}{739 \cdot 1000}$.

3. Всего получим 22 дроби.

5, a. $2^8 \cdot 3^5 \cdot 11^3$. b. $2^3 \cdot 3^3 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 17 \cdot 23 \cdot 37$.

Ответы к главе II

1, a. 1312.

b. $2^{119} \cdot 3^{59} \cdot 5^{31} \cdot 7^{19} \cdot 11^{12} \cdot 13^9 \cdot 17^7 \cdot 19^6 \cdot 23^5 \cdot 29^4 \cdot 31^4 \cdot 37^3 \cdot 41^3 \cdot 43^2 \cdot 47^2 \times$
$\times 53^2 \cdot 59^2 \cdot 61^2 \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113$.

2, a. $\tau(5600) = 36$; $S(5600) = 15\,624$.

b. $\tau(116\,424) = 96$; $S(116\,424) = 410\,400$.

3. Сумма всех значений равна 1.

4. α) 1152; β) 466 400.

5. Сумма всех значений равна 774.

Ответы к главе III

1, a. 70. b. Делится.

2, a. $3^3 \cdot 5^2 \cdot 11^2 \cdot 2999$. b. $7 \cdot 13 \cdot 37 \cdot 73 \cdot 101\ 137 \cdot 17 \cdot 19 \cdot 257$.

Ответы к главе IV

1, a. $x \equiv 81 \pmod{337}$. b. $x = 200, 751; 1302; 1853;$ **2404 (mod 2755).**

2, b. $x \equiv 1630 \pmod{2413}$.

3. $x = 94 + 111t$; $y = 39 + 47t$, где t — любое число.

4, a. $x \equiv 170b_1 + 52\,b_2 \pmod{221}$;
$x \equiv 131 \pmod{221}$; $x \equiv 110 \pmod{221}$; $x \equiv 89 \pmod{221}$.

b. $x \equiv 11\,151b_1 + 11\,800b_2 + 16\,875b_3 \pmod{39\,825}$.

5, a. $x = 91 \pmod{120}$. b. $x = 8479 \pmod{15\,015}$.

6. $x \equiv 100 \pmod{143}$; $y \equiv 111 \pmod{143}$.

7, a. $3x^4 + 2x^3 + 3x^2 + 2x = 0 \pmod 5$.

b. $5x^6 + x^5 + 5x^4 + 3x^2 + 3x + 4 = 0 \pmod 7$.

8. $x^6 + 4x^5 + 22x^4 + 76x^3 + 70x^2 + 52x + 39 = 0 \pmod{101}$.

9, a. $x = 16 \pmod{27}$. b. $x = 22; 53 \pmod{64}$.

10, a. $x \equiv 113 \pmod{125}$.

b. $x = 43, 123, 168, 248, 293, 373, 418, 498, 543, 623 \pmod{625}$.

11, a. $x = 2, 5, 11, 17, 20, 26 \pmod{30}$.

b. $x \equiv 76, 22, 176, 122 \pmod{225}$.

Ответы к главе V

1, a. 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
b. 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35,
2, a. α) 0; β) 2. b. α) 0; β) 2.
3, a. α) 0; β) 2. b. α) 0; β) 2.
4, a. α) $x \equiv \pm 9 \pmod{19}$; β) $x \equiv \pm 11 \pmod{29}$;
γ) $x \equiv \pm 14 \pmod{97}$.
b. α) $x \equiv \pm 66 \pmod{311}$, β) $x \equiv \pm 130 \pmod{277}$;
γ) $x \equiv \pm 94 \pmod{353}$.
5, a. $x \equiv \pm 72 \pmod{125}$. b. $x \equiv \pm 127 \pmod{243}$.
6, a. $x \equiv 13,\ 19,\ 45,\ 51 \pmod{64}$. b. $x \equiv 41, 87, 169, 215 \pmod{256}$.

Ответы к главе VI

1, a. 6. b. 18.
2, a. 3, 3, 3. b. 5, 5, 5 c. 7.
5, a. α) 0; β) 1; γ) 3. b. α) 0, β) 1; γ) 10.
6, a. α) $x \equiv 40;\ 27 \pmod{67}$; β) $x \equiv 33 \pmod{67}$;
γ) $x \equiv 8,\ 36,\ 28,\ 59,\ 31,\ 39 \pmod{67}$.
b. α) $x \equiv 17 \pmod{73}$, β) $x \equiv 50,\ 12,\ 35,\ 23,\ 61,\ 38 \pmod{73}$,
γ) $x \equiv 3,\ 24,\ 46 \pmod{73}$.
7, a. α) 0; β) 4. b. α) 0; β) 7.
8, a. α) 1, 4, 5, 6, 7, 9, 11, 16, 17; β) 1, 7, 8, 11, 12, 18.
b. α) 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36;
β) 1, 7, 9, 10, 12, 16, 26, 33, 34.
9, a. α) 7, 37; β) 3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34.
b. α) 3, 27, 41, 52;
β) 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59.

10, α)

N	1
γ	0

β)

N	1	3
γ	0	1

γ)

N	1	3	7	9
γ	0	0	0	0
γ_0	0	1	3	2

δ)

N	1	5	7	11
γ	0	0	1	1
γ_1	0	1	0	1

ε)

N	1	2	4	7	8	11	13	14
γ_1	0	1	0	0	1	1	0	1
γ_2	0	1	2	1	3	0	3	2

η)

N	1	3	5	7	9	11	13	15
γ	0	1	0	1	0	1	0	1
γ_0	0	3	1	2	2	1	3	0

ϰ)

N	1	2	3	4	6	7	8	9	11	12	13	14	16	17	18	19	21	22	23	24
γ_1	0	1	7	2	8	5	3	14	16	9	19	6	4	13	15	18	12	17	11	10

Ответы к главе VII

1, α)

N	0	1
χ	0	1

β)

N	0	1	2	3
χ	0	1	0	R_c

; $c=2$.

γ)

N	0	1	2	3	4	5	6	7
χ	0	1 1	0	R_c R_{c_0}	0	R_c R_{c_0}	0	R_c 1

; $c=2$, $c_0=2$.

δ)

N	0	1	2	3	4	5	6	7	8	9
χ	0	1 1 1	0	R_c R_{c_0} $R^3_{c_1}$	0	0	0	R_c 1 R_{c_1}	0	1 1 $R^2_{c_1}$

10	11	12	13	14	15	16	17	18	19
0	R_c R_{c_0} 1	0	R_c R_{c_0} $R^3_{c_1}$	0	0	0	1 1 R_{c_1}	0	R_c R_{c_0} $R^2_{c_1}$

ε)

N	20	21	22	23	24	25	26	27	28	29
χ	0	R_c R_{c_0} 1	0	R_c 1 $R^3_{c_1}$	0	0	0	R_c R_{c_0} R_{c_1}	0	R_c R_{c_0} $R^2_{c_1}$

30	31	32	33	34	35	36	37	38	39
0	R_c 1 1	0	1 1 $R^3_{c_1}$	0	0	0	R_c R_{c_0} R_{c_1}	0	R_c 1 $R^2_{c_1}$

$c=2$, $c_0=2$, $c_1=4$.

ТАБЛИЦЫ ИНДЕКСОВ

$p=3,\quad p-1=2,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

$p=5,\quad p-1=2^2,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

$p=7,\quad p-1=2\cdot 3,\quad g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

$p=11,\quad p-1=2\cdot 5,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

$p=13,\quad p-1=2^2\cdot 3,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	4	2	9	5	11	3	8
1	10	7	6							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	3	6	12	11	9	5
1	10	7								

$p=17,\quad p-1=2^4,\quad g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	14	1	12	5	15	11	10	2
1	3	7	13	4	9	6	8			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	10	13	5	15	11	16	14
1	8	7	4	12	2	6				

$p=19,\quad p-1=2\cdot 3^2,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	13	7	14	9	18
1	17	15	11	3	6	12	5	10		

$p=23,\quad p-1=2\cdot 11,\quad g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

$p=29,\quad p-1=2^2\cdot 7,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

$p=31,\quad p-1=2\cdot3\cdot5,\quad g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

$p=37,\quad p-1=2^2\cdot3^2,\quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

$p=41,\quad p-1=2^3\cdot5,\quad g=6$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

$p=43,\quad p-1=2\cdot3\cdot7,\quad g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

$p=47, \quad p-1=2\cdot 23, \quad g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	6	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

$p=53, \quad p-1=2^2\cdot 13, \quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

$p=59, \quad p-1=2\cdot 29, \quad g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

$p=61$, $p-1=2^2\cdot 3\cdot 5$, $g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	0	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

$p=67$, $p-1=2\cdot 3\cdot 11$, $g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

$p=71$, $p-1=2\cdot 5\cdot 7$, $g=7$

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

$p = 73$, $p - 1 = 2^3 \cdot 3^2$, $g = 5$

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

$p = 79$, $p - 1 = 2 \cdot 3 \cdot 13$, $g = 3$

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

$p = 83$, $p - 1 = 2 \cdot 41$, $g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

$p=89, \quad p-1=2^3\cdot 11, \quad g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

$p=97, \quad p-1=2^5\cdot 3, \quad g=5$

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

ТАБЛИЦА ПРОСТЫХ ЧИСЕЛ < 4070 И ИХ НАИМЕНЬШИХ ПЕРВООБРАЗНЫХ КОРНЕЙ

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

Продолжение

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	3	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3851	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	7	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	2	3881	13
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2647	3	2927	5	3299	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	5	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

Иван Матвеевич ВИНОГРАДОВ (1891–1983) — профессор, академик АН СССР по Отделению физико-математических наук (математика), почетный член Лондонского Королевского общества, Национальной академии деи Линчен в Риме, член-корреспондент Парижской академии наук и других научных обществ мира.

Работал в Пермском университете, в Ленинградском государственном университете и Ленинградском политехническом институте, был директором Математического института АН СССР им. В. А. Стеклова и возглавлял в нем отдел теории чисел.

Работы И. М. Виноградова посвящены аналитической теории чисел, им решены проблемы, которые считались недоступными математике начала XX в. И. М. Виноградов — создатель одного из самых сильных методов аналитической теории чисел — метода тригонометрических сумм.

За выдающиеся работы в области математики награжден Ленинской премией (1972), Государственной премией СССР (1941, 1983), золотой медалью им. М. В. Ломоносова (1971), дважды Герой социалистического труда (1945, 1976).

ISBN 5-8114-0535-9