ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Кафедра алгебры и геометрии

Т. В. Азовская, В. В. Севостьянова

ЗАДАЧИ ПО ТЕОРИИ ЧИСЕЛ

Утверждено редакционно-издательским советом университета в качестве учебного пособия

Самара
Издательство «Самарский университет»
2009

УДК 511.2
ББК 22.13
А 357

Рецензенты:
канд. физ.-мат. наук, доц. Н. А. Яковлева,
канд. физ.-мат. наук, доц. С. Ю. Попов

Азовская, Т. В.
А357 **Задачи по теории чисел**: учебное пособие / Т. В. Азовская, В. В. Севостьянова. — Самара: Издательство «Самарский университет», 2009. — 72 с.

Данное учебное пособие содержит материал теоретического курса и одновременно является задачником по теории чисел. В нем рассматриваются основные определения, понятия, теоремы и алгоритмы теории чисел, а также некоторые прикладные задачи. Расположение теоретического материала соответствует лекционному изложению курса. В конце каждого параграфа приводятся упражнения, иллюстрирующие теорию. В последней части пособия содержатся примерные варианты контрольной работы по курсу теории чисел.

Учебное пособие предназначено для студентов 1 и 2 курсов специальностей «Математика», «Компьютерная безопасность», «Математическое обеспечение и администрирование информационных систем».

УДК 511.2
ББК 22.13

Оглавление

Предисловие

В первом приближении элементарная теория чисел подразумевает изучение свойств чисел натурального ряда — одной из наиболее простых математических систем. Основные результаты, которые принято называть классическими, были полностью доказаны к XIX веку, но несмотря на это здесь осталось большое количество нерешенных и полурешенных задач высокого качества. Эти задачи, как правило, имеют простые математические формулировки, понятные и доступные уже школьнику. Их решения часто стимулируют создание новых математических теорий и определяют концепции развития науки на долгие годы. С одним из блестящих результатов такого сорта вы сможете познакомиться уже на начальном этапе изучения теории чисел. Без сомнения, речь идет о квадратичном законе взаимности, первое полное доказательство которого получил Ф. Гаусс. Другой блестящий пример — Великая теорема Ферма.

Пособие представляет собой комплекс теоретического курса и решения задач. Для понимания сути происходящего читателю достаточно знаний средней школы.

В целом при рассмотрении общих вопросов мы старались следовать классическому подходу. Расположение параграфов соответствует лекционному изложению материала. Доказательства большинства теорем, цитируемых в пособии, разбиты на отдельные задачи, решая которые можно самостоятельно получить то или иное утверждение. В конце каждого параграфа приведены упражнения, иллюстрирующие теорию. Задачи повышенной сложности отмечены звездочкой. Несколько слов о трудностях, с которыми может столкнуться студент. Дело в том, что в элементарной теории чисел не так много стандартных приемов, но много задач, которые требуют изобретательности и догадки. В пособии разобран ряд задач, демонстрирующих некоторые трюки. Осваивайте стандартные алгоритмы, анализируйте нестандартные приемы, разбирайте доказательства — только в этом залог вашего будущего успеха! Особое внимание — списку используемой литературы, он содержит лучшие, с нашей точки зрения, учебники по элементарной теории чисел. Большая часть упражнений заимствована из этих замечательных книг.

Мы старались не избегать изложения ряда прикладных аспектов элементарной теории чисел, что дало возможность разнообразить задачи и примеры. Содержание курса доказывает свою ценность в целом ряде приложений, связанных, например, с задачами криптографии. Подобные отклонения в области применения теории чисел будут интересны будущим специалистам по компьютерной безопасности.

В тех случаях, когда мы испытывали потребность дать единое толкование ряда фактов, мы обращались к понятиям группы, идеала, фактор кольца. Такие отступления оказываются весьма полезными при знакомстве с начальными понятиями абстрактной алгебры, поскольку первые примеры здесь связаны, как правило, с арифметикой кольца целых чисел.

При написании этого пособия нам существенно помогли советы наших коллег. Мы выражаем благодарность всем сотрудникам кафедры алгебры и геометрии за внимание к нашей работе. В частности, нам хотелось бы выразить признательность М. В. Игнатьеву за своевременные толковые замечания и Ю. Ю. Крутикову за апробацию нашего пособия.

1. Делимость чисел

Пусть a и b — целые числа, $b \neq 0$. Говорят, что b *делит* a, если найдется такое целое число c, что $a = b \cdot c$. Для записи делимости нацело используются стандартные обозначения $b|a$ (b делит a) и $a\vdots b$ (a делится на b).

Упражнение. Используя определение, докажите следующие свойства делимости:

a) если $a|b$ и $b|c$, то $a|c$;

b) если $a|b$ и $b|a$, то $a = \pm b$ (это свойство полезно при доказательстве равенства чисел с точностью до знака);

c) если $a|b$ и $a|c$, то $a|(b \pm c)$ и $a|(k \cdot b)$ при любом целом k.

Кольцо целых чисел $\mathbb{Z}$ — одно из колец, в котором имеется алгоритм деления с остатком.

Пусть $a, b \in \mathbb{Z}$, $b \neq 0$. *Разделить a с остатком на b* означает представить a в виде $a = bq + r$, где $0 \leqslant r < |b|$. В этой записи q называют *неполным частным*, а r — *остатком* от деления a на b.

Каждый школьник умеет делить с остатком и хорошо представляет себе правило выбора неполного частного.

Опираясь на "школьный" опыт, докажите следующую теорему существования и единственности деления с остатком:

Теорема. *Для любой пары целых чисел a и b, $b \neq 0$, a единственным образом представимо в виде $a = bq + r$, где $0 \leqslant r < |b|$.*

Примечание. Начните со случая $a > 0$, $b > 0$, а затем, используя доказанное, переберите все возможные варианты для a и b.

Задачи

1. Число n при делении на 16 дает в остатке 3. Какой остаток при делении на 12 даст число $3n$?

2. Какие остатки при делении на 24 могут иметь простое число и его квадрат?

3. Какие остатки при делении на p имеют квадраты и кубы целых чисел, если $p = 5$, $p = 7$?

   Используя результаты задачи, обоснуйте неразрешимость в целых числах уравнений

$$x^2 - 7yz = 10, \quad x^3 + 14y^2z = 19, \quad x^2 - 10yz^2 = 8.$$

Составьте алгебраические уравнения с целыми коэффициентами второй и третьей степени, не имеющие решений в целых числах.

Воспользуемся свойствами делимости и решим следующую задачу.

Задача. При каких натуральных n сократима дробь

$$\frac{8n+71}{5n+46}?$$

Решение. Пусть числитель $a = 8n + 71$ и знаменатель $b = 5n + 46$ кратны числу d, тогда d делит $5a - 8b = -13$. Отсюда получаем, что если дробь сократима, то только на $d = 13$. Теперь достаточно указать только те значения n, при которых b (или a) делится на 13.

Получаем, что 13 делит $5n + 46$ тогда и только тогда, когда 13 делит число $5n + 20$, а это в свою очередь равносильно тому, что 13 делит $n + 4$. Таким образом, дробь $\dfrac{8n+71}{5n+46}$ сократима тогда и только тогда, когда остаток от деления числа n на 13 равен 9. □

Замечание. Немного позже запись решения подобных задач мы станем воспроизводить, используя язык и свойства числовых сравнений.

Задачи

1. При каких целых значениях n следующая дробь есть целое число:

   a) $\dfrac{4n-7}{2n+3}$;

   b) $\dfrac{n^2-n+3}{n+1}$?

2. При каких натуральных n сократима дробь $\dfrac{n+7}{2n+3}$?

3. Известно, что $nm + st$ делится на $n + s$. Докажите, что число $nt + sm$ делится на $n + s$.

4. Докажите, что из n целых чисел всегда можно выбрать несколько таких чисел, что, поставив между ними знаки "+" и "—", можно получить число, делящееся на n.

5. Целые числа n и m таковы, что $m+3n$ кратно 13. Докажите, что число $11m + 7n$ делится на 13.

6. Целые числа n и m таковы, что $2m-n$ кратно 11. Докажите, что число $51m-8n$ делится на 11. Придумайте свою задачу такого типа.

7. Примените теорию делимости к доказательству равенства чисел:

$$(n, m) = (17n + 11m, 3n + 2m).$$

Составьте свою подобную задачу. Каким условиям удовлетворяют коэффициенты при n и m?

8. Докажите, что число, в десятичной записи которого участвуют пятнадцать единиц и некоторое число нулей, не может быть квадратом целого числа.

9. Каждый из людей, когда-либо живших на Земле, сделал определенное число рукопожатий. Докажите, что число людей, сделавших нечетное число рукопожатий, четно.

10. В ряд записаны числа $1, 2, \ldots, n$. Можно ли расставить между ними знаки "+" и "−" так, чтобы значение полученного выражения было равно нулю? Дайте ответ при $n = 17$.

11. На столе стоят 15 чашек, все вверх дном. За один ход разрешается перевернуть 4 чашки. Можно ли за несколько ходов добиться того, чтобы чашки стояли правильно?

12*. Натуральные числа m, n и k таковы, что m^n делится на n^m, а число n^k делится на k^n. Докажите, что число m^k делится на k^m.

13*. Докажите, что следующие числа не являются целыми:

a) $\dfrac{1}{2} + \dfrac{1}{3} + \ldots + \dfrac{1}{n}$;

b) $\dfrac{1}{3} + \dfrac{1}{5} + \ldots + \dfrac{1}{2n+1}$.

Указание. Обозначим

$$k = \max \nu_2(m),$$

где $\nu_2(m)$ — логарифмическая 2–норма (см. параграф 6 "Теоретико–числовые функции"). Покажите, что среди чисел от 1 до n имеется точно одно, кратное 2^k. Представив сумму $1 + \dfrac{1}{2} + \ldots + \dfrac{1}{n}$ в виде несократимой дроби, получите, что при четном числителе знаменатель окажется нечетным.

14. Докажите, что обыкновенная дробь $\frac{m}{n}$ представима в виде конечной десятичной дроби тогда и только тогда, когда n не делится на простые числа, отличные от 2 и 5.

15. Найдите наибольшее натуральное четырехзначное число, все цифры которого различны и которое делится на 2, 5, 9, 11.

16. Докажите, что если $a^3+b^3+c^3$ делится на 7 ($a, b, c \in \mathbb{Z}$), то abc делится на 7.

17. Доказать, что $6^{2k}+2^{k+4}$ делится на 17.

2. Алгоритм Евклида. Наибольший общий делитель и наименьшее общее кратное

Определение. Назовем *наибольшим общим делителем* чисел a и b (обозначается НОД(a,b) или (a,b)) такой их общий делитель, который делится на любой другой их общий делитель.

Наименьшим общим кратным чисел a и b (обозначается НОК(a,b) или $[a,b]$) назовем такое их общее кратное, на которое делится их любое общее кратное.

Для определенности будем считать наибольший общий делитель и наименьшее общее кратное неотрицательными числами.

Мы дали определение наибольшего общего делителя и наименьшего общего кратного на языке делимости. В школе эти понятия часто вводят как наибольший из возможных делителей и наименьшее из возможных кратных соответственно.

Упражнение. Докажите эквивалентность определений наибольшего общего делителя и наименьшего общего кратного на языке абсолютных величин и на языке делимости.

Задача. Примените теорию делимости к доказательству следующего равенства чисел: $(n,m)=(5n+3m, 13n+8m)$.

Решение. Введем обозначения:

$$d=(n,m); \quad D=(5n+3m, 13n+8m).$$

Очевидно, что d делит числа $5n+3m$ и $13n+8m$, отсюда заключаем, что d — их общий делитель и, следовательно, d делит D.

Обратно,

$$\begin{cases} 5n + 3m = Dt, \\ 13n + 8m = Ds \end{cases}$$

при некоторых $t, s \in \mathbb{Z}$. Выразив из этой системы n и m, получим

$$\begin{cases} n = D(8t - 3s), \\ m = D(5s - 13t), \end{cases}$$

откуда следует, что число D делит d. Из свойств делимости заключаем, что $D = \pm d$. $\square$

Одним из самых привлекательных свойств наибольшего общего делителя является простота его вычисления с помощью известного уже более 2300 лет метода, называемого алгоритмом Евклида. Суть метода заключается в последовательном выполнении деления с остатком. Делитель и остаток предыдущего шага становятся соответственно делимым и делителем следующего.

Пусть a, b — положительные целые числа. Предположим, что $a > b$, тогда

$$\begin{aligned} a &= bq_0 + r_0, \\ b &= r_0q_1 + r_1, \\ r_0 &= r_1q_2 + r_2, \\ &\dots\dots\dots\dots\dots \\ r_{n-2} &= r_{n-1}q_n + r_n, \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Делимость нацело в последней строке объясняется строгим убыванием и ограниченностью снизу нулем последовательности остатков $\{r_n\}$. Кроме того,

$$(a, b) = (b, r_1) = \ldots = (r_{n-1}, r_n) = r_n. \tag{1}$$

Таким образом, последний ненулевой остаток в алгоритме Евклида, примененного к числам a и b, и есть наибольший делитель этих чисел.

Упражнения

1. Умножив каждую строку в алгоритме Евклида на m, получите утверждение
$$(ma, mb) = m(a, b).$$

2. Пусть d — общий делитель чисел a и b. Докажите, что
$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

3. Пусть $d = (a, b)$. Докажите, что справедливо равенство

$$a = d \cdot a', \quad b = d \cdot b',$$

где $(a', b') = 1$.

С помощью алгоритма Евклида можно получить и нечто большее, чем наибольший общий делитель. Для этого выразим r_n из последней строки и будем "подниматься" вверх по строчкам алгоритма Евклида, заменяя на каждом шаге r_k на $r_{k-2} - r_{k-1}q_k$. В результате мы получим *линейное представление* наибольшего общего делителя (a, b), то есть представление наибольшего общего делителя в виде

$$(a, b) = au + bv$$

для некоторых целых u и v. Знание линейного представления наибольшего общего делителя будет нам полезно при решении ряда задач.

Упражнение. Докажите справедливость равенства (1).

Числа a и b, наибольший общий делитель которых равен $(a, b) = 1$, называют *взаимно простыми числами.*

Упражнения

1. Докажите, что числа a и b взаимно просты тогда и только тогда, когда единица представима в виде

$$1 = ax + by, \quad x, y \in \mathbb{Z}.$$

2. Докажите утверждение: если $(a, b) = 1$, то для любого c справедливо $(ac, b) = (c, b)$.

3. Докажите, что если $c|ab$ и $(a, c) = 1$, то $c|b$.

4. Докажите, что если $(a, b) = 1$, $a|c$ и $b|c$, то $ab|c$.

5. Используя свойства наибольшего общего делителя и упражнение 4, получите формулу, связывающую наибольший общий делитель и наименьшее общее кратное чисел a и b:

$$[a, b] = \frac{a \cdot b}{(a, b)}.$$

Задача. Найдите все целые решения *диофантова* уравнения

$$17x + 43y = 2.$$

Решение. Заметим, что наше уравнение определяет на плоскости прямую, и перейдем к ее параметрическому уравнению:

$$\begin{cases} x &= x_0 - 43t, \\ y &= y_0 + 17t \end{cases}$$

(здесь (x_0, y_0) — некоторая точка прямой с целыми коэффициентами).

Поскольку $(17, 43) = 1$, то найдутся целые u и v такие, что

$$17u + 43v = 1.$$

В качестве x_0 возьмем $2u$, тогда $y_0 = 2v$. Найдем u и v из алгоритма Евклида:

$$1 = 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17 = 2(43 - 17 \cdot 2) - 17 = 2 \cdot 43 - 17 \cdot 5.$$

Тогда $u = -5$, $v = 2$ и $x_0 = -10$, $y_0 = 4$. Если (x_1, y_1) — другая точка на прямой с целыми координатами, то

$$17(x_1 - x_0) = 43(y_0 - y_1).$$

Отсюда в силу взаимной простоты чисел 17 и 43 получаем, что 17 делит число $y_1 - y_0$ и 43 делит $x_1 - x_0$. Следовательно, точка (x_1, y_1) получается из параметрического уравнения прямой при некотором целом значении параметра t. Верно и обратное: любое целое значение t определяет точку на прямой с целыми координатами.

Получаем ответ: $x = -10 - 43t,\ y = 4 + 17t$, где t — любое целое число. □

Задачи

1. Какими могут быть числа a и b, если

   a) НОК$(a, b) = 2640$ и НОД$(a, b) = 15$;

   b) НОК(a, b) +НОД$(a, b) = 35$, НОД$(a, b) \neq 1$;

   c) НОК(a, b) ·НОД$(a, b) = 630$, НОД$(a, b) \neq 1$?

   Придумайте свои задачи подобного типа.

2. Найдите наибольший общий делитель следующих пар чисел $(1035, 1105)$, $(611, 676)$, $(8183, 1152)$.

3. Найдите линейное представление наибольшего общего делителя следующих пар чисел $(93, 39)$, $(76, 28)$, $(17, 101)$.

4. Используя линейное представление наибольшего общего делителя, решите в целых числах уравнения

   a) $37x - 28y = 11$;

   b) $59x + 14y = 2$;

   c) $63x - 8y = 5$;

   d) $16x - 28y = 13$.

5. Числа m и n — взаимно простые. Докажите, что следующие пары чисел взаимно простые:

   a) $m \cdot n$ и $m + n$;

   b) $m \cdot n$ и $m^2 + n^2$.

6. Числа m и n взаимно простые. Какие общие делители могут иметь числа

   a) $m + n$ и $m - n$;

   b) $m + n$ и $m^2 + n^2$?

7. Докажите, что если $(a, b) = 1$ и p — простое число, то $(a + b, a \cdot b \cdot p) = 1$ или $(a + b, a \cdot b \cdot p) = p$.

8. Докажите, что если числа a и b — взаимно простые, то наибольший общий делитель чисел $a \cdot c$ и b равен наибольшему общему делителю чисел b и c.

9. Докажите, что если $(a, b) = d$, то $(a + b \cdot c, a + b(c - 1)) = d$.

10. Установите, чему может быть равно наименьшее общее кратное трех последовательных натуральных чисел.

11. Пусть p — простое число. Докажите, что для $n = 1, 2, \ldots, p-1$ числа n и $p - n$ взаимно просты.

12*. Пусть r_n — n-значное число вида $111\ldots11$. Докажите, что

$$(r_n, r_m) = r_{(n,m)}.$$

13*. Докажите, что два различных *числа Ферма* $2^{2^n}+1$ и $2^{2^m}+1$ взаимно просты.

14. Верно ли, что если n делит $2^{n-1}-1$, то n — число простое?

15. Докажите, что если $n \geqslant 2$, то числа 2^n-1 и 2^n+1 взаимно просты.

16*. Найдите отношение $\dfrac{u}{v}$, если известно, что для всех натуральных k выполняется условие

$$(ku+2004, kv+2005) \neq 1.$$

3. Применение алгоритма Евклида

Пусть A — произвольное коммутативное кольцо.

Определение. Непустое подмножество I в A называется *идеалом*, если оно обладает двумя свойствами:

1. Из $x_1, x_2 \in I$ следует, что $x_1 - x_2 \in I$.

2. Из $x \in I$ следует, что $ax \in I$ для любого элемента $a \in A$.

Нетрудно убедиться, что произвольное конечное множество $a_1, a_2, \ldots, a_s$ элементов кольца A определяет идеал I, состоящий из элементов кольца, представимых в виде линейных комбинаций $\sum \lambda_i a_i$ с коэффициентами λ_i из A.

В этом случае говорят, что идеал порожден $\{a_i\}_{i=1}^s$ и пишут

$$I = (a_1, a_2, \ldots, a_s).$$

Идеал, порожденный одним элементом $I = (a)$, называется *главным*.

Алгоритм деления с остатком позволяет легко установить, что любой идеал в кольце целых чисел — главный идеал. В качестве образующей идеала I в кольце $\mathbb{Z}$ следует взять наименьшее неотрицательное число в I (проведите рассуждения полностью).

Задачи

1. Пусть $d =$НОД$(a_1, a_2, \ldots, a_s)$. Докажите, что

$$I = (a_1, a_2, \ldots, a_s) = (d).$$

2. Найдите необходимое и достаточное условие разрешимости в целых числах уравнения $ax+by=c$ и, шире, уравнения $a_1x_1+a_2x_2+\ldots+a_sx_s=b$.

3. Множество натуральных чисел разбито на два подмножества A и B так, что $A\cdot B$ (то есть множество всех произведений ab, где $a\in A$, $b\in B$) содержится в A и $A+B$ (то есть множество всех сумм вида $a+b$, где $a\in A$, $b\in B$). Докажите, что

   a) $A\cdot A$ содержится в A;

   b) A состоит из всех чисел, кратных некоторому числу d.

4*. Пусть $(a,b)=1$. Докажите, что любую сумму, начиная с $(a-1)(b-1)$, можно уплатить монетами достоинством a и b таньга, а сумму

$$(a-1)(b-1)-1$$

уже нельзя.

4. Простые и составные числа. Бесконечность множества простых чисел. Основная теорема арифметики

Одно из основных понятий в теории чисел — понятие простого числа. Напомним, что натуральное число p называется *простым*, если оно имеет ровно два натуральных делителя, а именно, 1 и p. Все другие натуральные числа называются *составными*. Единица по определению не является ни простым, ни составным числом.

Упражнение. Покажите, что наименьший простой делитель числа n не больше $\sqrt{n}$.

Теорема. *Простых чисел в натуральном ряду бесконечно много.*

Доказательство, которое мы приведем, принадлежит Евклиду. Оно проводится методом "от противного". Следует рассмотреть число

$$N=p_1p_2\ldots p_s+1,$$

где $p_1,p_2,\ldots,p_s$ — список всех простых чисел, и показать, что у него, с одной стороны, нет простых делителей, а с другой стороны, оно не может быть простым. $\square$

Поскольку единственное четное простое — это двойка, то теорему Евклида можно сформулировать иначе.

Теорема. *В арифметической прогрессии $n_k = 2k + 1$, где $n_0 = 1$, с разностью равной 2, существует бесконечно много простых.*

Обобщает теорему Евклида замечательный результат Дирихле.

Теорема (о простых числах в арифметических прогрессиях).
Любая арифметическая прогрессия $ak + b$, где a и b — целые числа,

$$\text{НОД}(a, b) = 1,\ a > 0,$$

число k — целое неотрицательное, содержит бесконечно много простых чисел.

Доказательство этой теоремы в общем случае проводится далеко не элементарными методами, однако некоторые частные случаи теоремы Дирихле можно достаточно легко получить.

Упражнение. Докажите, что существует бесконечно много простых вида $4k + 3$, k — целое неотрицательное.

Указание. Восстановите доказательство по следующему плану.

1. Нечетное простое при делении на 4 дает в остатке 1 или 3; если все простые $p_i \equiv 1 \pmod 4$, то

$$\prod_{i=1}^{k} p_i \equiv 1 \pmod 4.$$

2. Пусть $3, p_1, p_2, \ldots, p_s$ — все простые из прогрессии $4k+3$, $k = 0, 1, 2, \ldots$ Число $N = 4p_1p_2 \ldots p_s + 3$ не может быть простым и обязано делиться на простое из набора $p_1, p_2, \ldots, p_s$. $\square$

Задача. Опираясь на теорему Дирихле, покажите, что для каждого натурального m существует простое число, сумма цифр которого больше, чем m.

Решение. Рассмотрим арифметическую прогрессию

$$\underbrace{111\ldots11}_{m} + 10^{m+1} \cdot k,$$

где k — целое неотрицательное. Сумма цифр любого числа построенной прогрессии больше, чем m, следовательно, простые числа в данной прогрессии удовлетворяют нужному свойству. $\square$

Завершая обсуждение теоремы Евклида, обратим внимание читателей на замечательную книгу П. Рибенбойма [2]. В ней приводится более десятка различных доказательств бесконечности множества простых чисел.

Место следующей теоремы в элементарной теории чисел определено самим ее названием.

Основная теорема арифметики. *Каждое натуральное число $n > 1$ может быть однозначно записано в виде произведения степеней простых чисел:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

где p_i — различные простые делители числа n, $\alpha_i \in \mathbb{N}$.

Представление числа n в виде произведения *примарных* взаимно простых множителей называется *каноническим разложением* числа n.

Задачи

1. Докажите, что для того, чтобы нечетное натуральное число n было простым, необходимо и достаточно, чтобы представление n в виде $x^2 - z^2$ было единственным.

2. Докажите, что среди целых чисел, представимых многочленом положительной степени с целыми коэффициентами, имеется бесконечно много составных.

3. Пусть $M_n = 2^n - 1$ и $M_m = 2^m - 1$ — два числа Мерсенна, r — остаток от деления n на m. Покажите, что остаток от деления M_n на M_m равен числу M_r. Получите необходимое условие простоты чисел Мерсенна.

4. Докажите следующий критерий простоты натурального числа $n > 1$: натуральное число n является простым тогда и только тогда, когда для любой пары натуральных чисел a и b такой, что $n|(a \cdot b)$, следует, что $n|a$ или $n|b$.

5. Докажите теорему о бесконечности множества простых чисел, используя факт взаимной простоты чисел Ферма:

$$\left(2^{2^n} + 1, 2^{2^m} + 1\right) = 1, \text{ если } (n, m) = 1.$$

6*. Для натуральных n и k докажите, что если $2^n > (1+n)^k$, то среди чисел $1, 2, 2^2, \dots, 2^n$ существует по крайне мере $k+1$ простое число. Покажите, что отсюда следует бесконечность множества простых чисел.

7*. Докажите, что среди чисел $\{1, 2, \ldots, n\}$ не менее четверти свободны от квадратов. Получите из этого утверждения доказательство бесконечности множества простых чисел.

8. Опираясь на теорему Дирихле о простых числах в арифметических прогрессиях, докажите, что для всякого натурального числа n найдется простое число p такое, что каждое из чисел $p-1$ и $p+1$ имеет не более чем n различных делителей.

9*. Докажите, что в натуральном ряду существуют сколь угодно большие промежутки, не содержащие простых чисел.

Указание. Рассмотрите следующий ряд:

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1.$$

5. Непрерывные дроби

Рассмотрим рациональную дробь $\frac{a}{b} \in \mathbb{Q}$. Без ограничения общности будем считать, что $a > b$. Благодаря алгоритму Евклида рациональное $\frac{a}{b}$ может быть единственным образом записано в виде *конечной непрерывной дроби*:

$$\frac{a}{b} = \frac{bq_0 + r_0}{b} = q_0 + \frac{1}{\frac{b}{r_0}} = q_0 + \frac{1}{\frac{q_1 r_0 + r_1}{r_0}} =$$

$$= q_0 + \frac{1}{q_1 + \frac{1}{\frac{r_0}{r_1}}} = \ldots = q_0 + \frac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n}}} = [q_0; q_1, \ldots, q_n],$$

где q_k — неполные частные, а r_k — остатки из алгоритма Евклида.

Имеет место следующее

Утверждение. *Разложение в непрерывную дробь рационального числа конечно.*

Любая конечная непрерывная дробь является рациональным числом.

Следующую дробь будем называть *k-й подходящей дробью*:

$$\delta_k = \frac{P_k}{Q_k} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_k}}}.$$

Будем считать, что $P_{-1} = 1$, $Q_{-1} = 0$, $\delta_0 = q_0$, отсюда $P_0 = q_0$, $Q_0 = 1$, тогда

$$\delta_1 = \frac{q_0 q_1 + 1}{q_1}, \quad P_1 = q_0 q_1 + 1, \quad Q_1 = q_1.$$

Упражнение. Покажите, что

$$\begin{array}{ll} P_2 = q_0 q_1 q_2 + q_2 + q_0, & Q_2 = q_1 q_2 + 1, \\ P_3 = q_0 q_1 q_2 q_3 + q_0 q_1 + q_0 q_3 + q_2 q_3 + 1, & Q_3 = q_1 q_2 q_3 + q_1 + q_3; \end{array}$$

найдите P_4, Q_4.

Упражнение. Покажите индукцией по k, что числитель и знаменатель $(k+1)$-й подходящей дроби при $k \geqslant 2$ могут быть найдены с помощью рекуррентного соотношения:

$$\begin{aligned} P_{k+1} &= q_{k+1} P_k + P_{k-1}, \\ Q_{k+1} &= q_{k+1} Q_k + Q_{k-1}. \end{aligned}$$

О свойствах подходящих дробей можно прочитать, например, в [4].

При решении задач нам особенно полезно будет свойство, выражающее связь числителей и знаменателей двух соседних подходящих дробей, а именно:

$$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k-1}. \tag{2}$$

Упражнение. Докажите индукцией по k приведенное выше свойство.

Все подходящие дроби несократимы, а последняя подходящая дробь совпадает по значению с рациональным числом:

$$\frac{P_n}{Q_n} = \frac{a}{b}.$$

Поэтому, если наша дробь несократима, то есть $(a, b) = 1$, получаем

$$a Q_{n-1} - P_{n-1} b = (-1)^{n-1}.$$

При решении задач о нахождении целочисленных решений уравнений вида $ax + by = c$ удобно пользоваться соотношением (2).

Найдем решения в целых числах уравнения $ax + by = c$.

Предположим, что $(a, b) = 1$. Решение (x, y) нашего уравнения будем искать в виде

$$\begin{aligned} x &= x_0 + x_1, \\ y &= y_0 + y_1, \end{aligned}$$

где (x_0, y_0) — частное решение уравнения $ax + by = c$, а (x_1, y_1) — решение уравнения $ax_1 + by_1 = 0$.

Разложим в непрерывную дробь число $\dfrac{a}{b}$. Умножим равенство

$$aQ_{n-1} - P_{n-1}b = (-1)^{n-1}$$

на число $(-1)^{n-1}c$; получим

$$a\left((-1)^{n-1}cQ_{n-1}\right) + b\left((-1)^n cP_{n-1}\right) = c.$$

Таким образом, в качестве частного решения $ax + by = c$ возьмем

$$\begin{aligned} x_0 &= (-1)^{n-1}cQ_{n-1}, \\ y_0 &= (-1)^n cP_{n-1}. \end{aligned}$$

Решением уравнения $ax + by = 0$ является

$$\begin{aligned} x_1 &= bt, \\ y_1 &= -at; \end{aligned} \qquad t \in \mathbb{Z}.$$

Таким образом, множество целочисленных решений состоит из чисел вида

$$\begin{aligned} x &= (-1)^{n-1}cQ_{n-1} + bt, \\ y &= (-1)^n cP_{n-1} - at; \end{aligned} \qquad t \in \mathbb{Z}.$$

Пусть теперь $(a, b) = d > 1$. Тогда, если число d не делит c, уравнение $ax + by = c$ не имеет решений. Если же $d > 1$ является наибольшим общим делителем чисел a, b, c, следует решать уравнение

$$a_1x + b_1y = c_1,$$

где $a = da_1$, $b = db_1$ и $c = dc_1$.

Упражнения

1. Разложите в непрерывную дробь числа $\dfrac{107}{40}$, $\dfrac{125}{94}$, $\dfrac{78}{169}$, $\dfrac{115}{27}$.
2. Запишите в виде простой дроби $\dfrac{P}{Q}$ выражения

   a) $[1; 1, 2, 1, 2, 1, 2]$;

   b) $[0; 1, 2, 3, 4, 5]$;

   c) $[c; d, c, d, c]$.

3. Решите уравнения

   a) $[x; 2, 4, 6, 8] = \dfrac{1575}{457}$;

   b) $[2; 3, 4, x] = \dfrac{127}{55}$.

4. Найдите все целочисленные решения уравнений

   a) $3x - 14y = 1$;

   b) $41x - 103y = 1$;

   c) $75x + 37y = 4$;

   d) $571x + 359y = 10$.

Задачи

1. Докажите, что $P_{k-1}Q_{k+1} - P_{k+1}Q_{k-1} = (-1)^k q_{k+1}$.

2. Пользуясь предыдущей задачей, покажите, что последовательность подходящих дробей с четными индексами — возрастающая, а последовательность подходящих дробей с нечетными индексами — убывающая, то есть
$$\delta_0 < \delta_2 < \delta_4 < \ldots, \quad \delta_1 > \delta_3 > \delta_5 > \ldots$$

3. Пусть непрерывная дробь такова, что $q_0 = 0$ и при любом $1 \leqslant i \leqslant n$ выполняется $q_i = q$. Докажите, что при $k < n - 2$
$$P_k^2 + P_{k+1}^2 = p_{k-1}P_{k+1} + P_k P_{k+2}.$$

Будем рассматривать бесконечные дроби вида $[q_0; q_1, q_2, \ldots]$, где $q_k > 0$ — это целые числа. Такая дробь называется *периодической*, если существуют такие натуральные N и T, что
$$q_{k+T} = q_k$$
при $k \geqslant N$. В этом случае мы будем обозначать периодическую часть в символе дроби чертой сверху, то есть
$$[q_0; q_1, q_2, \ldots, q_{N-1}, \overline{q_N, q_{N+1}, \ldots, q_{N+T-1}}].$$

Задачи

1. Найдите значение дроби $[1;\overline{1}]$.

2. Найдите значения следующих дробей:

   a) $[4;\overline{4}]$;

   b) $[\overline{1;3}]$;

   c) $[1;\overline{2,1}]$.

3*. Докажите равенство: если $a \geqslant 2$ — натуральное число, то

$$\sqrt{a^2-1} = [a-1;\overline{1,2a-2}].$$

6. Теоретико–числовые функции

Для всех функций этого параграфа область определения — множество $\mathbb{Z}$ или $\mathbb{N}$.

Логарифмическая p-норма

Определение. Пусть натуральное число n таково, что $n = p^m s$, где p — простое, $(p,s) = 1$, тогда функция $\nu_p(n) = m$ называется *логарифмической p-нормой*, или *функцией порядка* или *p-адическим показателем.*

Приведем некоторые свойства функции порядка:

A. $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

B. $\nu_p(a+b) \geqslant \min\{\nu_p(a), \nu_p(b)\}$, если же $\nu_p(a) \neq \nu_p(b)$, то равенство точное.

C. $\nu_p(a) = 0$ тогда и только тогда, когда $(a,p) = 1$.

D. $\nu_p(p) = 1$.

E. Положим по определению $\nu_p(0) = \infty$.

Упражнение. Докажите свойства A—C функции порядка.

При вычислении логарифмической p-нормы от чисел вида $n!$ удобно использовать следующее утверждение.

Задача. Покажите, что показатель, с которым число p входит в разложение числа $n!$, равен

$$\nu_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots.$$

Здесь $[x]$ обозначает целую часть числа x.

Замечание. В действительности сумма, приведенная в задаче, содержит лишь конечное число ненулевых слагаемых, поскольку с некоторого момента целые части начнут обращаться в нуль.

Мультипликативные функции

Определение. Функция $f : \mathbb{N} \to \mathbb{C}$ называется *мультипликативной*, если она удовлетворяет условиям:

A. Существует такое натуральное число a_0, что $f(a_0) \neq 0$.

B. Для любых натуральных взаимно простых чисел a и b выполняется равенство $f(ab) = f(a)f(b)$.

Мультипликативную функцию достаточно задать на примарных числах, так как в силу мультипликативности она однозначно продолжается на все множество $\mathbb{N}$.

Задача. Докажите, что справедливы следующие свойства мультипликативных функций:

A. $f(1) = 1$.

B. Пусть f_1 и f_2 — мультипликативные функции, тогда $f_1 f_2$ — также мультипликативна.

Утверждение. *Пусть $f(n)$ — мультипликативная функция, каноническое разложение числа n:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

тогда

$$\sum_{d|n} f(d) = \prod_{p_i|n} \left(1 + f(p_i) + f(p_i^2) + \ldots + f(p_i^{\alpha_i})\right), \tag{3}$$

где суммирование ведется по всем делителям d числа n, а произведение — по всем простым p_i, делящим n.

Доказательство. Чтобы доказать это тождество, раскроем скобки в правой части равенства. Получим сумму слагаемых вида

$$f(p_1^{\beta_1}) f(p_2^{\beta_2}) \dots f(p_s^{\beta_s}) = f(p_1^{\beta_1} p_2^{\beta_2} \dots p_s^{\beta_s}),$$

$$0 \leqslant \beta_1 \leqslant \alpha_1, \quad 0 \leqslant \beta_2 \leqslant \alpha_2, \quad \dots, \quad 0 \leqslant \beta_s \leqslant \alpha_s,$$

причем ни одно слагаемое не будет пропущено и не повторится более одного раза, а это в точности то, что записано в левой части равенства. □

Упражнение. Докажите тождество

$$\sum_{d|n} d^t = \prod_{p_i|n} \left(1 + p_i^t + p_i^{2t} + \ldots + p_i^{\alpha_i t}\right),$$

если $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ — каноническое разложение числа n.

В качестве примеров мультипликативных функций рассмотрим следующие.

Сумма делителей числа n

Сумму делителей числа n обозначают

$$\sigma(n) = \sum_{d|n} d.$$

Число делителей числа n

Число делителей числа n обозначают

$$\tau(n) = \sum_{d|n} 1.$$

Упражнения

1. Найдите $\sigma(n)$ и $\tau(n)$, где $n = 14, 10, 63, 270, 300$.
2. Найдите значение $\sigma(p^\alpha)$, где p — простое число.

Задачи

1. Пусть $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Докажите формулы

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1),$$

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

2. Покажите, что $\sigma(n)$ и $\tau(n)$ — мультипликативные функции.

Функция Мебиуса

Определение. Функция Мебиуса $\mu(n)$ — мультипликативная функция, заданная на множестве $\mathbb{Z}_{>0}$ условием

$$\mu\left(p^{\alpha}\right) = \begin{cases} -1, & \text{для } \alpha = 1, \\ 0, & \text{для } \alpha > 1. \end{cases}$$

Утверждение 1. *Пусть $f(n)$ — мультипликативная функция. Тогда*

$$\sum_{d|n} \mu(d)\theta(d) = (1 - \theta(p_1)) \dots (1 - \theta(p_s)),$$

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

Доказательство. Поскольку $\mu(n)$ — мультипликативная функция, то $f_1(n) = \mu(n)f(n)$ также мультипликативна. Применим к ней (3): поскольку $f_1(p) = -f(p)$ и $f_1(p^s) = 0$ при $s > 1$, убеждаемся в справедливости нашего утверждения. □

Задачи

1. Докажите, что при $n > 1$ справедливо равенство

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{d|n} \left(1 - \frac{1}{p_i}\right). \tag{4}$$

2. Докажите, что сумма $\sum_{d|n} \mu(d)$ равна 1 при $n = 1$ и обращается в нуль при $n > 1$.

Утверждение 2. *Пусть целым положительным*

$$\delta = \delta_1, \delta_2, \dots, \delta_s$$

соответствуют любые вещественные или комплексные $n = n_1, n_2, \dots, n_s$. Обозначим через S' сумму значений n, соответствующих δ, равным единице, и через S_d — сумму значений n, отвечающих δ, кратным d. Тогда

$$S' = \sum_{d} \mu(d) S_d, \tag{5}$$

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

Доказательство. Из задачи 2 следует, что

$$S' = n_1 \sum_{d|\delta_1} \mu(d) + n_2 \sum_{d|\delta_2} \mu(d) + \ldots + n_s \sum_{d|\delta_s} \mu(d).$$

Собирая члены с одним значением d и вынося $\mu(d)$ за скобки, в скобках получим сумму тех и только тех n, у которых соответствующие им δ кратны d. Эта сумма в точности равна S_d. $\square$

Функция Эйлера

Определение. Функция Эйлера $\varphi(n)$ определена на множестве целых положительных чисел и принимает значение, равное количеству чисел ряда

$$0, 1, \ldots, n-1,$$

взаимно простых с n.

Упражнения

1. Вычислите по определению значение функции Эйлера $\varphi(n)$ для

$$n = 5, 8, 12.$$

2. Вычислите $\varphi(p)$, $\varphi(p^\alpha)$, $\varphi(p_1 p_2)$, где числа p, p_1, p_2 — простые.

3. Покажите, что если $\varphi(n) = n - 1$, то n — простое число.

Утверждение. *Пусть* $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — *каноническое разложение числа* n. *Тогда*

$$\varphi(n) = n \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right).$$

Доказательство. Применим формулу (5). При этом числа δ и n определим следующим образом: пусть x пробегает множество чисел $0, 1, \ldots, n-1$; каждому значению x поставим в соответствие число $\delta = (x, n)$, получим $S_0, \ldots, S_{n-1}$; возьмем все значения n_i равными 1.

Тогда S' равно числу значений $\delta = (x, n)$, равных 1, то есть $S' = \varphi(n)$. Число S_d равно числу значений $\delta = (x, n)$, кратных d. Заметим, что число d делит (x, n) только в случае, когда d — делитель n. Тогда S_d будет равна числу значений x, кратных d, то есть $S_d = \dfrac{n}{d}$. В результате в силу (4) получим

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d} = n \prod_{p_i|n} \left(1 - \frac{1}{p_i}\right),$$

что завершает доказательство утверждения. $\square$

Упражнение. Найдите $\varphi(362)$, $\varphi(2004)$.

Задача*. Докажите, что

$$\sum_{d|n} \varphi(d) = n.$$

Задачи

1. Найдите наименьшее натуральное число n, для которого $\tau(n) = 6$.
2. Докажите, что $\tau(n)$ нечетно тогда и только тогда, когда n — квадрат целого числа.
3. Докажите, что $\sigma(n)$ нечетно тогда и только тогда, когда n — квадрат или удвоенный квадрат целого числа.
4. Покажите, что r — простое тогда и только тогда, когда $\sigma(r) = r + 1$.
5. Решите уравнения
   a) $n^2 + \sigma^2(n) = 1845$;
   b) $n^2 + \sigma^2(n) = 2004$.

6*. Докажите следующее равенство:

$$\sigma(1) + \sigma(2) + \ldots + \sigma(n) = \left[\frac{n}{1}\right] + 2\left[\frac{n}{2}\right] + \ldots + n\left[\frac{n}{n}\right].$$

7. Покажите, что для функции Эйлера выполняются следующие свойства:
   a) $\varphi\left(p^n\right) = p^n - p^{n-1}$, где p — простое;
   b) $\varphi(n)$ четно, если $n > 2$;
   c)* $\varphi(m)\varphi(n) = \varphi\left((m,n)\right)\varphi\left([m,n]\right)$.
8. Некоторое натуральное число имеет 3 простых делителя, квадрат этого числа имеет 27 делителей. Сколько делителей имеет куб этого числа?
9. Что больше:
   a) $\sigma(mn)$ или $\sigma(m)\sigma(n)$;
   b) $\tau(mn)$ или $\tau(m)\tau(n)$?

10. Решите уравнения в целых положительных числах

    a) $\varphi(3^x) = 18$;

    b) $\varphi(x) = \dfrac{x}{2}$;

    c) $\varphi(3x) = \varphi(5x)$;

    d) $\varphi(x) = \dfrac{x}{5}$.

11. Докажите, что если $\varphi(n)$ — простое число, то $n = 3$, 4 или 6.

12. Покажите, что если m делит n, то $\varphi(m \cdot n) = m \cdot \varphi(n)$.

13. Покажите, что

$$\prod_{d|n} d = n^{\tau(n)/2},$$

    если n не является квадратом целого числа.

14. Используя свойства $\varphi(n)$, покажите, что простых чисел бесконечно много.

15*. Докажите *формулу обращения Мебиуса*: пусть

$$F(n) = \sum_{d|n} f(d),$$

    тогда

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

7. Теория сравнений

Мы уже использовали понятие модуля, рассматривая остатки от деления на 2, 4, 10, ... Интуитивно мы понимаем, что очень часто сравнение чисел только по величине остатка от деления на некоторое число m приводит нас к нужному результату.

Определение. Фиксируем целое число m, отличное от 0 и 1. Будем говорить, что два целых числа *a и b сравнимы по модулю m*, если выполняется одно из трех эквивалентных условий:

- a и b имеют одинаковые остатки при делении на m;

- m делит разность $a - b$;
- $a = b + mt$ для некоторого целого t.

Упражнение. Установите эквивалентность приведенных выше условий.

Для обозначения условия "a сравнимо с b по модулю m" используется следующая запись: $a \equiv b \pmod{m}$.

Исторически понятие сравнения было введено Гауссом, оно является ярким примером использования "правильного" обозначения. Поскольку для любой пары целых a и b выполняется или не выполняется условие

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

то сравнимость по модулю m определяет на $\mathbb{Z}$ бинарное отношение. Легко проверить, что данное отношение рефлексивно, симметрично и транзитивно и, следовательно, является отношением эквивалентности. Таким образом, все множество $\mathbb{Z}$ можно представить в виде объединения непересекающихся классов чисел, сравнимых по модулю m. Каждый класс сравнимых по модулю m чисел назовем *классом вычетов по модулю* m. Каждый класс вычетов однозначно определяется любым своим представителем.

Наименьший неотрицательный представитель класса вычетов — это остаток от деления на m чисел данного класса.

Введем следующие стандартные обозначения: классом элемента a (обозначается $\overline{a}$ или $[a]$) назовем множество $a + m\mathbb{Z}$.

Определение. Назовем любое множество представителей, взятых по одному из каждого класса вычетов по модулю m, *полной системой вычетов* по модулю m.

Если $b_1, \ldots, b_m$ — любая полная система вычетов, то

$$\mathbb{Z} = \bigcup_{i=1}^{m} \overline{b_i}.$$

Определение. Подмножество полной системы вычетов, состоящее из всех вычетов, взаимно простых с m, назовем *приведенной системой вычетов* по модулю m.

Упражнение. Покажите, что в приведенной системе вычетов по модулю m имеется $\varphi(m)$ представителей.

Свойства делимости на m, сохраняющиеся при арифметических операциях с целыми числами, удобно записывать на языке числовых сравнений.

Утверждение. *Справедливы следующие свойства числовых сравнений:*

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

B. *Если* $a \equiv b \pmod{m}$ *и* $b \equiv c \pmod{m}$, *то* $a \equiv c \pmod{m}$.

C. *Пусть* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$, *тогда* $a \pm c \equiv b \pm d \pmod{m}$.

D. *Если* $a \equiv b \pmod{m}$, *то* $a + k \equiv b + k \pmod{m}$ *для любого* $k \in \mathbb{Z}$.

E. *Пусть* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$, *тогда* $ac \equiv bd \pmod{m}$.

F. *Пусть* $a \equiv b \pmod{m}$, *тогда для любого целого* k *справедливо* $ak \equiv bk \pmod{m}$.

G. *Пусть* $a \equiv b \pmod{m}$, *тогда для любого* $n \in \mathbb{N}$ $a^n \equiv b^n \pmod{m}$.

H. *Пусть* $d = (k, m)$, *если* $ak \equiv bk \pmod{m}$, *тогда* $a \equiv b \pmod{\dfrac{m}{d}}$.

I. *Пусть* $P(x)$ — *многочлен с целыми коэффициентами степени* n *и* $a \equiv b \pmod{m}$, *тогда* $P(a) \equiv P(b) \pmod{m}$.

Упражнение. Докажите приведенные свойства.

Рассмотрим уравнение $f(x_1, x_2, \ldots, x_n) = 0$, где

$$f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n].$$

Если уравнение разрешимо в целых числах и $\alpha_1, \alpha_2, \ldots, \alpha_n$ — целое решение уравнения, тогда из условия

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$$

следует, что для *любого* m выполняется сравнение

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) \equiv 0 \pmod{m}.$$

Вопрос о разрешимости сравнения

$$f(x_1, x_2, \ldots, x_n) \equiv 0 \pmod{m} \tag{6}$$

может быть выяснен за конечное число шагов. Для этого в качестве значений переменных нужно перебрать некоторые полные системы вычетов по модулю m. Если удастся предъявить такой модуль, что сравнение (6) окажется

неразрешимым, тогда и уравнение не будет иметь решений в целых числах. Такую методику решения задач называют *методикой выбора модуля*.

В качестве примера приведем решение следующей задачи.

Задача. Даны две последовательности целых чисел:

$$\begin{aligned} &x_1 = x_2 = 10, && y_1 = y_2 = -10, \\ &x_{n+2} = (x_{n+1} + 1)\, x_n + 1, && y_{n+2} = (y_{n+1} + 1)\, y_n + 1. \end{aligned}$$

Возможно ли при каких-нибудь k и l совпадение x_k и y_l?

Решение. Покажем, что по модулю 101 последовательности постоянны и различны. Вычислим $x_3 = 111$, $x_4 = 1121$, $y_3 = 91$ и $y_4 = -919$. Нетрудно видеть, что при $i \leqslant 3$ выполняется

$$x_i \equiv x_{i+1} \pmod{101} \text{ и } y_i \equiv y_{i+1} \pmod{101}.$$

Докажем методом математической индукции, что последовательности $\{x_i\}$ и $\{y_i\}$ постоянны по модулю 101. Выполнение базы индукции очевидно. Пусть $x_{n+1} = (x_n + 1)\, x_{n-1} + 1 \equiv 10 \pmod{101}$, тогда

$$x_{n+2} = (x_{n+1} + 1)\, x_n + 1 \equiv (10 + 1)\, 10 + 1 \equiv 10 \pmod{101}.$$

Аналогично, $y_n \equiv -10 \pmod{101}$.

Таким образом, никакие два числа последовательностей $\{x_i\}$ и $\{y_i\}$ не совпадают по модулю 101, следовательно, никакие $\{x_l\}$ и $\{y_k\}$ не совпадают в $\mathbb{Z}$. $\square$

Упражнения

1. Верны ли следующие числовые сравнения:

   a) $39 \equiv 15 \pmod{14}$;

   b) $17 \equiv 21 \pmod{2}$;

   c) $-4 \equiv 35 \pmod{13}$;

   d) $-17 \equiv 29 \pmod{23}$?

2. Укажите наименьшее положительное число, с которым сравнимо число a по модулю m:

   a) $a = 73,\ m = 8$;

   b) $a = -59,\ m = 13$;

   c) $a = 112,\ m = 15$;

   d) $a = 75,\ m = 25$.

Как можно охарактеризовать наименьшее неотрицательное число, сравнимое с числом a по модулю m?

3. Укажите наименьшее по абсолютной величине число, с которым сравнимо число a по модулю m:

   a) $a = 17,\ m = 3$;

   b) $a = 28,\ m = 17$;

   c) $a = 67,\ m = 9$.

   Опишите способ получения этого числа.

4. Используя свойства числовых сравнений, найдите наименьшее положительное x, удовлетворяющее условию:

   a) $5x \equiv 35 \pmod{13}$;

   b) $7x \equiv 42 \pmod{15}$;

   c) $3x \equiv 5 \pmod{7}$;

   d) $9x \equiv 2 \pmod{20}$.

5. Найдите остаток от деления на m выражения $3x^9 + 5y^3 - 4z^5$:

   a) $m = 14,\ x \equiv 7 \pmod{14},\ y \equiv 9 \pmod{14},\ z \equiv -3 \pmod{14}$;

   b) $m = 31,\ x \equiv 2 \pmod{31},\ y \equiv -28 \pmod{31},\ z \equiv 25 \pmod{31}$.

   Сформулируйте свойства сравнений, использованные при решении этой задачи.

Задачи

1. Покажите, что по модулю 8 числа $-64, -14, 38, -1, 4, 11, 25, -3$ составляют полную систему вычетов, а числа $17, -11, -33, 19$ — приведенную систему вычетов.

2. Покажите, что числа $36, -11, -10, 9, -2, 11$ составляют полную систему вычетов по модулю 6. Выберите вычеты, составляющие приведенную систему вычетов по модулю 6.

3. Запишите полную систему вычетов по модулю 7, наименьших по абсолютной величине.

4. Для каких модулей числа a и $-a$ попадают в один и тот же класс вычетов?

5. Назовем натуральное простое число *абсолютно простым*, если при любой перестановке его цифр снова получается простое число. Докажите, что в записи абсолютно простого числа не может быть использовано более трех различных цифр.

6. Докажите, что если $(a, m) = 1$ и x пробегает полную систему вычетов по модулю m, то $ax + b$ тоже пробегает полную систему вычетов по модулю m.

7. Докажите, что остаток от деления любого числа на 3 или 9 совпадает с остатком от деления на 3 или 9 суммы цифр данного числа.

8. Получите признак делимости на 11.

9. Записав число в системе счисления с основанием 100, получите признак делимости на 101.

10. Записав число в системе счисления с основанием 1000, получите признаки делимости на 13, 7 и 37.

11. Докажите, что если $m|(a - b)$, то для любого $n > 1$ выполняется равенство
$$\frac{a^n - b^n}{a - b} - na^{n-1} \equiv 0 \pmod{m}.$$

12. Докажите, что
$$\left(\frac{a^n - 1}{a - 1}, a - 1\right) = (a - 1, n).$$

13*. Пусть p — нечетное простое число. Дано $p-1$ целых чисел, не делящихся на p. Докажите, что, заменив некоторые из этих чисел на противоположные, можно получить $p - 1$ чисел, сумма которых кратна p.

14. Докажите, что сумма квадратов пяти последовательных положительных целых чисел не является квадратом целого числа.

    Указание. Покажите, что сумма кратна 5 и не делится на 25.

15. Докажите, что если n — сумма квадратов целых чисел, то n при делении на 4 дает в остатке 0, 1 или 2.

Замечание. Полное описание чисел, являющихся суммами двух квадратов, нашел Ферма, а доказательство этого утверждения первым получил Эйлер.

16. Докажите, что сумма $2^2 + 4^4 + 6^6 + \ldots + 50^{50}$ не является квадратом целого числа.

17. Найдите $n \in \mathbb{N}$, для которых число $1! + 2! + \ldots + n!$ — квадрат целого числа.

18*. Докажите, что число $1^1 + 2^2 + 3^3 + \ldots + 2007^{2007}$ не может быть степенью целого числа.

19. Пусть p — простое, $8p^2 + 1$ — простое. Докажите, что $8p^2 - p + 2$ — также простое.

20. Докажите, что если n — сумма трех квадратов целых чисел, то n при делении на 8 не может давать в остатке 7.

    Замечание. Полное описание чисел, являющихся суммами трех квадратов, получил Гаусс. Лагранж доказал, что любое натуральное число есть сумма четырех квадратов целых чисел [2].

21. Ферма высказал гипотезу, что для всех целых натуральных чисел n число $2^{2^n} + 1$ является простым. Эйлер нашел пример, опровергающий эту гипотезу: число 641 делит $2^{32} + 1$. Подтвердите это, используя сравнения.

22. Найдите все арифметические прогрессии из пяти простых положительных чисел с разностью 6.

23. Найдите наибольшее число членов в конечной арифметической прогрессии, состоящей их простых чисел.

8. Теорема Эйлера. Малая теорема Ферма

Теорему, о которой мы будем говорить в этом разделе, называют "малой теоремой Ферма". Частный случай этой теоремы известен сотни лет, но Ферма, вероятно, был первым, кто доказал эту теорему в полной общности.

Малая теорема Ферма. *Пусть p — простое число, $(a, p) = 1$, тогда*

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

Следствие. *Для любого целого a выполняется*

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

Эйлер обобщил результат Ферма на случай составного m.

Теорема Эйлера. *Пусть $(a, m) = 1$, тогда*

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

Упражнение. Восстановите доказательство теоремы Эйлера, используя следующие свойства:

1. Умножение приведенной системы вычетов по модулю m на число a приводит к приведенной системе вычетов.
2. Произведения элементов двух любых приведенных систем вычетов по модулю m сравнимы по модулю m.
3. Сравнения можно делить на числа, взаимно простые с модулем m.

Задачи

1. Запишите и проверьте теорему Эйлера для следующих пар чисел:
   a) $a = 5$, $m = 24$;
   b) $a = 2$, $m = 39$;
   c) $a = 7$, $m = 6$.
2. Запишите и проверьте теорему Ферма для следующих пар чисел:
   a) $a = 3$, $m = 11$;
   b) $a = 2$, $m = 13$;
   c) $a = 2$, $m = 19$.
3. Сколько решений, то есть классов вычетов по модулю m, имеет сравнение $x^{p-1} \equiv 1 \pmod{p}$?
4. Найдите остатки от деления 7^{122} на 143, 8^{900} на 29.
5. Докажите *теорему Вильсона*: $(p-1)! \equiv -1 \pmod{p}$, где p — простое число.

6. Найдите простые числа p, для которых следующие числа простые:

   a) $p^2 - 6$ и $p^2 + 6$;

   b) $p^3 - 6$ и $p^3 + 6$;

   c) $2^p + 1$ и $2^p - 1$;

   d) $p^2 - 2$, $2p^2 - 1$ и $3p^2 + 4$.

   Придумайте свою задачу такого типа.

7. Покажите, что для нечетных n

$$n^n \equiv 1 \pmod 8.$$

8. Существует ли 99-значное число a такое, что число $\overline{aa}$ делится на a^2?

9. Докажите, что для любого натурального числа n, $(n, 10) = 1$, существует число вида $111\ldots1$, кратное n. Назовите минимальное число разрядов числа $111\ldots1$, кратного n.

10. Докажите, что если $a_1 + a_2 + \ldots + a_s \equiv 0 \pmod{30}$, то

$$a_1^5 + a_2^5 + \ldots + a_s^5 \equiv 0 \pmod{30}.$$

    Придумайте свою подобную задачу.

11. Докажите, что $(a + b)^p \equiv a^p + b^p \pmod p$, где p — простое, a — любое целое число.

12. Пусть a и b — взаимно простые числа. Докажите, что

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}.$$

9. Кольцо классов вычетов по модулю m

Множество классов вычетов по модулю m обозначают через

$$\mathbb{Z}/m\mathbb{Z} \text{ или } \mathbb{Z}_m.$$

Множество $\mathbb{Z}_m$ можно превратить в кольцо, определив сложение и умножение естественным образом. Если $\overline{a}, \overline{b} \in \mathbb{Z}_m$, то сумму двух классов вычетов $\overline{a} + \overline{b}$ мы определим как $\overline{a + b}$ и произведение $\overline{a} \cdot \overline{b}$ — как $\overline{a \cdot b}$.

Упражнение. Используя свойства числовых сравнений, покажите, что результаты определенных таким образом операций сложения и умножения классов вычетов по модулю m зависят лишь от классов вычетов, определяемых a и b.

Упражнение. Покажите, что $\mathbb{Z}_m$ с введенными операциями — кольцо.

Приведенные ниже таблицы в явном виде задают сложение и умножение в кольце $\mathbb{Z}_6$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Определение. Ненулевые элементы кольца называются *делителями нуля*, если их произведение равно нулю.

Упражнение. Покажите, что $\overline{a} \in \mathbb{Z}_m$ — делитель нуля, если $(a, m) > 1$.

Определение. Элемент $\overline{a}$ называется *обратимым в кольце* $\mathbb{Z}_m$, если для него существует $\overline{b} \in \mathbb{Z}_m$ такой, что $\overline{a} \cdot \overline{b} = \overline{1}$.

Упражнение. Покажите, что $\overline{a} \in \mathbb{Z}_m$ обратим тогда и только тогда, когда $(a, m) = 1$.

Упражнение. Покажите, что произведение обратимых элементов кольца обратимо.

Обратимые элементы кольца классов вычетов образуют группу по умножению, которая называется *мультипликативной группой кольца* и обозначается $\mathbb{Z}_m^*$.

Упражнение. Покажите, что мультипликативная группа кольца классов вычетов содержит $\varphi(m)$ элементов.

Пусть p — простое число. В этом случае кольцо $\mathbb{Z}_p$ не имеет делителей нуля, каждый ненулевой элемент $\mathbb{Z}_p$ обратим, следовательно, $\mathbb{Z}_p$ — *поле классов вычетов*.

Замечание. При решении арифметических задач иногда бывает удобнее работать с кольцом $\mathbb{Z}_m$, чем с понятием сравнения по модулю m. Так, решение сравнения

$$ax \equiv 1 \pmod{m}$$

эквивалентно нахождению обратного к $\overline{a}$ в кольце $\mathbb{Z}_m$; существование первообразного корня по модулю p (см. параграф "Первообразные корни") означает, что группа $\mathbb{Z}_p^*$ — циклическая, то есть состоит из степеней некоторого одного элемента.

Задача. Для кольца $\mathbb{Z}/24\mathbb{Z}$ выпишите делители нуля и обратимые элементы. Составьте таблицу умножения для $\mathbb{Z}_{24}^*$, по ней укажите пары взаимно обратимых элементов.

10. Вариации на тему малой теоремы Ферма

Приведет ли к успеху попытка обратить малую теорему Ферма? Китайские математики около 2000 тысяч лет назад ошибочно полагали, что если число $2^n - 2$ кратно n, то оно простое. Сейчас такие числа называют *псевдопростыми по базе* 2.

Определение. *Псевдопростыми по базе* a называют такие составные числа n, для которых $2^n - 2$ кратно n.

Числа, псевдопростые по любой базе, называются *абсолютно псевдопростыми* или *числами Кармайкла.*

Задачи

1. Доказать, что если число n не свободно от квадратов, то есть p^2 делит n для некоторого простого p, то n не является псевдопростым по базе $a = 1 + \dfrac{n}{p}$.

2*. Докажите, что для любого a существует бесконечно много псевдопростых по базе a чисел, являющихся составными. Такими являются, например, все числа из последовательности $\dfrac{a^{2p} - 1}{a^2 - 1}$, где p — простое, $n > 2$ и $\big(p, a^2 - 1\big) = 1$. Найдите наименьшее псевдопростое по базе 2.

3*. Покажите, что множество

$$\mathbb{F}_n = \big\{a \in (\mathbb{Z}/n\mathbb{Z})^* : \ a^{n-1} \equiv 1 \pmod{n}\big\}$$

является подгруппой в $(\mathbb{Z}/n\mathbb{Z})^*$.

4. Покажите, что если n не является псевдопростым по основанию хотя бы одного числа a, то

$$|\,\mathbb{F}_n| \leqslant \frac{\varphi(n)}{2}.$$

Ниже приведена теорема, играющая важную роль в некоторых алгоритмах распознавания простоты и построения больших простых чисел.

Теорема Люка. *Пусть $N > 1$ и нашлось целое число a со свойствами:*

1) $a^{N-1} \equiv 1 \pmod{N}$;

2) *a^m не сравнимо с 1 по модулю N для $m = 1, 2, \ldots, N-2$.*

Тогда число N является простым.

Замечание. Обратите внимание, что условие 1 в теореме Люка — малая теорема Ферма. Поскольку во многих классических учебниках по теории чисел эта теорема отсутствует, приведем здесь ее доказательство.

Доказательство. Заметим, что $\varphi(N) \leqslant N - 1$. Далее, поскольку

$$a^{N-1} \equiv 1 \pmod{N},$$

то $(a, N) = 1$. Кроме того, $\operatorname{ord} a$ делит число $\varphi(N)$. Из условия 2 следует, что $\operatorname{ord} a = N - 1$, следовательно, $\varphi(N) = N - 1$. Таким образом, N — число простое. $\square$

Задача. Покажите, что условие 2 теоремы Люка достаточно потребовать только для всех m, делящих $N - 1$.

11. Сравнения первой степени

Пусть $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ — многочлен с целыми коэффициентами. Будем рассматривать сравнение вида

$$f(x) \equiv 0 \pmod{m}. \tag{7}$$

Заметим, что если некоторый вычет b удовлетворяет сравнению (7), то все числа, сравнимые с b по модулю m, также удовлетворяют (7). Таким образом, под решением сравнения (7) понимается класс вычетов

$$x \equiv b \pmod{m}$$

такой, что

$$f(b) \equiv 0 \pmod{m}.$$

Рассмотрим важный частный случай:

$$ax \equiv b \pmod{m}. \tag{8}$$

Введем следующие обозначения:

$$d = (a, m); \quad a = da', \quad m = dm'.$$

Если d делит b, то обозначим $b = db'$. Будем различать три случая:

1. Если $(a, m) = 1$, то сравнение (8) имеет единственное решение (в смысле класса чисел по модулю m).

2. Если $(a, m) = d > 1$ и свободный член b не делится на d, то сравнение не имеет решений.

3. Если $(a, m) = d > 1$ и d делит b, то сравнение имеет d различных решений, которые находятся по формуле

   $$x_k \equiv \gamma + m'k \pmod{m},$$

   где $k = 0, 1, \ldots, d-1$; число γ удовлетворяет сравнению

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

   которое получается из исходного делением всех членов сравнения (8) на d.

Упражнение. Восстановите доказательства трех случаев по следующим кратким указаниям, расположенным в том же порядке, что и номера приведенных выше пунктов.

- Пусть $c_1, c_2, \ldots, c_m$ — некоторая полная система вычетов по модулю m. Тогда в полной системе вычетов $ac_1, ac_2, \ldots, ac_m$ найдется ровно один представитель, сравнимый с b по модулю m.

- Если число γ удовлетворяет сравнению (8), то $a\gamma \equiv b \pmod{d}$. Отсюда получаем, что $0 \equiv b \pmod{d}$, что противоречит условию.

- Заметим, что для числа γ справедливо

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

  тогда и только тогда, когда

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

  Сравнение $a'x \equiv b' \pmod{m'}$ имеет ровно одно решение $x \equiv \gamma \pmod{m'}$, то есть всякое решение сравнения (8) однозначно определено по модулю m'.

Покажем, что d вычетов $\gamma_k = \gamma + m'k$, где $k = 0, 1, \ldots, d-1$, удовлетворяют исходному сравнению и различны по модулю m.

Поскольку третий случай сводится к первому делением на d, то укажем методы решения сравнения (8) для взаимно простых a и m.

Применяются следующие способы решения:

1. Метод испытаний полной системы вычетов по модулю m.

2. Способ Эйлера, при котором решение находится по формуле

$$x \equiv a^{\varphi(m)-1} b \pmod{m},$$

где $\varphi(m)$ — функция Эйлера.

3. При помощи конечных непрерывных дробей по формуле

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

где P_{n-1} — числитель предпоследней подходящей дроби при разложении числа $\dfrac{m}{a}$ в непрерывную дробь.

4. При помощи преобразования правой части сравнения, а именно, замены вычета b другим вычетом того же класса, но кратным коэффициенту a. Проведя подобную замену и разделив обе части равенства на a, получаем x.

Задача. Решите сравнение

$$6x \equiv 39 \pmod{51}.$$

Решение. Проведем анализ: $(6, 51) = 3$, правая часть кратна 3, следовательно, имеем дело со случаем 3. Разделим обе части сравнения, включая модуль, на 3. Получим $2x \equiv 13 \pmod{17}$ или $2x \equiv -4 \pmod{17}$. Поскольку $(2, 17) = 1$, наше сравнение эквивалентно сравнению

$$x \equiv -2 \pmod{17}.$$

Отсюда по формуле 3 имеем $x_k \equiv -2 + 17k \pmod{51}$, где $k = 0, 1, 2$.

Ответом будут следующие три класса вычетов:

$$\begin{aligned} x_0 &\equiv -2 \pmod{51}, \\ x_1 &\equiv 15 \pmod{51}, \\ x_2 &\equiv 32 \pmod{51}. \ \square \end{aligned}$$

Задача. Решите сравнение

$$17x \equiv 2 \pmod{151}.$$

Решение. Проведем анализ: $(17, 151) = 1$, следовательно, сравнение имеет единственное решение. Будем решать сравнение с помощью непрерывных дробей. Запишем число $\dfrac{151}{17}$ в виде непрерывной дроби $\dfrac{151}{17} = [8; 1, 7, 2]$; здесь $n = 3$,

$$P_0 = 8, \quad P_1 = 8 \cdot 1 + 1 = 9, \quad P_3 = 9 \cdot 7 + 8 = 71.$$

Воспользуемся формулой

$$\begin{aligned} x &\equiv (-1)^3 \cdot 2 \cdot 71 \pmod{151}, \\ x &\equiv 9 \pmod{151}. \ \square \end{aligned}$$

Задача. Решите сравнение методом Эйлера:

$$93x \equiv 2 \pmod{17}.$$

Решение. Заметим, что $93 \equiv 8 \pmod{17}$, поэтому наше сравнение равносильно следующему:

$$8x \equiv 2 \pmod{17}.$$

По формуле Эйлера получаем

$$x \equiv 2 \cdot 8^{15} \equiv 2^{46} \pmod{17}.$$

Воспользуемся теоремой Эйлера: $2^{16} \equiv 1 \pmod{17}$, отсюда $x \equiv 2^{14} \pmod{17}$. Заметим, что $2^4 \equiv -1 \pmod{17}$, следовательно,

$$2^{12} \equiv -1 \pmod{17}.$$

Окончательно получаем $x \equiv -2^2 \equiv -4 \pmod{17}$.

Ответ: $x \equiv -4 \pmod{17}$. $\square$

Замечание. Если бы не был указан способ, которым следует решать задачу, то разумнее было бы поступать следующим образом. Заметим, что

$$2 \equiv 2 - 2 \cdot 17 \pmod{17},$$

поэтому сравнение $8x \equiv 2 \pmod{17}$ равносильно $8x \equiv -32 \pmod{17}$. Разделив на 8, получаем ответ

$$x \equiv -4 \pmod{17}.$$

12. Китайская теорема об остатках. Системы линейных сравнений

Согласно историческим данным, китайская теорема об остатках была известна еще в I веке до н. э.

Китайская теорема об остатках. *Пусть* $m_1, m_2, \ldots, m_s$ — *набор попарно взаимно простых чисел, а* $r_1, r_2, \ldots, r_s$ — *произвольные числа. Тогда система сравнений*

$$\begin{cases} x \equiv r_1 \pmod{m_1}, \\ x \equiv r_2 \pmod{m_2}, \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv r_s \pmod{m_s} \end{cases} \tag{9}$$

имеет единственное решение по модулю $M = m_1 m_2 \ldots m_s$.

Другими словами, набор остатков от деления на попарно взаимно простые числа позволяет восстановить число с точностью до слагаемого, кратного M.

В процессе доказательства теоремы строится вычет, удовлетворяющий системе сравнений.

Для этого обозначим

$$N_i = \frac{M}{m_i},$$

тогда $(N_i, m_i) = 1$ и найдутся целые d_i и l_i, для которых выполнено

$$1 = d_i N_i + l_i m_i.$$

Переходя к сравнениям, получаем, что для любого $i = 1, 2, \ldots, s$ справедливо

$$1 \equiv d_i N_i \pmod{m_i},$$

$$d_i N_i \equiv 0 \pmod{m_j}, \quad i \neq j.$$

Рассмотрим вычет

$$a = \sum_{k=1}^{s} r_k d_k N_k.$$

Приведем a по модулю m_i при любом i:

$$a = \sum_{k=1}^{s} r_k d_k N_k \equiv r_i \pmod{m_i}.$$

Очевидно, что $x \equiv a \pmod{M}$ — решение системы (9).

Упражнение. Покажите, что любые два вычета, удовлетворяющие системе (9), лежат в одном классе по модулю M.

Задача. Используя доказательство китайской теоремы об остатках, постройте решение системы

$$\begin{cases} x \equiv 3 \pmod 5, \\ x \equiv 1 \pmod 7, \\ x \equiv 0 \pmod 2. \end{cases}$$

Очевидно, что таким способом удастся решить далеко не всякую систему линейных сравнений.

В качестве универсального способа решения системы линейных сравнений можно указать один очень древний алгоритм. Он применялся еще в античности для решения проблем астрономии. Суть этого метода раскрывается в решении следующей задачи. Рассмотрим систему

$$\begin{cases} 3x \equiv 5 \pmod 7, \\ 4x \equiv 6 \pmod{10}, \\ x \equiv 1 \pmod 2. \end{cases}$$

Для первого сравнения имеем единственное решение

$$x \equiv 4 \pmod 7.$$

Вычеты этого класса следующие: $x = 4 + 7t$, $t \in \mathbb{Z}$. Найдем решение первого сравнения, которое одновременно удовлетворяет и второму:

$$4(4 + 7t) \equiv 6 \pmod{10}.$$

Разделив на 2, получим

$$4t \equiv 0 \pmod 5,$$

$$t \equiv 0 \pmod 5,$$

то есть $t = 5s$, $s \in \mathbb{Z}$. Итак, первым двум сравнениям удовлетворяют вычеты вида $x = 4 + 7 \cdot 5 \cdot s$. Подставим это выражение для x в третье сравнение:

$$4 + 35s \equiv 1 \pmod 2.$$

Откуда получаем, что $s \equiv 1 \pmod 2$ и $s = 1 + 2v$.

Окончательно $x = 4 + 35s = 39 + 70v$ или $x \equiv 39 \pmod{70}$. По модулю 140 система имеет два решения:

$$x \equiv 39 \pmod{140},\ x \equiv 109 \pmod{140}.\ \square$$

Замечание. Если на некотором шаге мы получаем сравнение, не имеющее решений, то это означает, что система несовместна.

При работе с большими модулями китайская теорема об остатках существенным образом помогает упростить вычисления.

Рассмотрим такую задачу.

Задача. Найдите остаток от деления 735^{286} на 2431.

Решение. Заметим, что применение теоремы Эйлера и приведение основания степени по модулю m нисколько не упрощает вычислений.

Разложим 2431 на множители. Перейдем от сравнения

$$x \equiv 735^{286} \pmod{2431}$$

к системе

$$\begin{cases} x \equiv 735^{286} \pmod{13}, \\ x \equiv 735^{286} \pmod{11}, \\ x \equiv 735^{286} \pmod{17}. \end{cases}$$

Здесь к каждому из сравнений можно уже применить малую теорему Ферма и уменьшить основание степени по соответствующему модулю

$$\begin{array}{ll} 735 \equiv -6 \pmod{13}, & 286 \equiv 10 \pmod{12}, \\ 735 \equiv -2 \pmod{11}, & 286 \equiv 6 \pmod{10}, \\ 735 \equiv 4 \pmod{17}, & 286 \equiv 14 \pmod{16}. \end{array}$$

Получаем эквивалентную систему

$$\begin{cases} x \equiv (-6)^{10} \pmod{13}, \\ x \equiv (-2)^{6} \pmod{11}, \\ x \equiv 4^{14} \pmod{17}. \end{cases}$$

Преобразуя правую часть этой системы, имеем:

$$6^{10} = (-3)^5 \equiv (-3)^3 \cdot (-4) \equiv 4 \pmod{13},$$

$$2^6 = 2^5 \cdot 2 \equiv -2 \pmod{11},$$

$$4^{14} = (2^2)^7 \equiv (-1)^7 \equiv -1 \pmod{17}.$$

Таким образом, получаем систему линейных сравнений

$$\begin{cases} x \equiv 4 \pmod{13}, \\ x \equiv -2 \pmod{11}, \\ x \equiv -1 \pmod{17}. \end{cases}$$

Решим ее описанным выше способом: $x = 4 + 13t$, $4 + 13t \equiv -2 \pmod{11}$, следовательно, $t \equiv -3 \pmod{11}$, откуда $x = 4 + 13(-3 + 11s)$. Далее

$$-35 + 13 \cdot 11 \cdot s \equiv -1 \pmod{17},$$

$$-4 \cdot (-6) \cdot s \equiv 34 \pmod{17},$$

$$7s \equiv 0 \pmod{17},$$

следовательно, $s = 17k$.

Окончательно

$$x = -35 + 11 \cdot 13 \cdot 17k = -35 + 2431k.$$

Остаток от деления — это наименьший неотрицательный вычет класса, то есть 2396. □

Опишем здесь еще одно интересное применение китайской теоремы об остатках. С долей юмора С.Коутинхо называет эту ипостась китайской теоремы "безопасной системой допуска живых к секретным сведениям".

Проблема здесь такова: имеется пароль или код, который можно считать большим натуральным числом N. Мы хотим распределить этот код между участниками так, чтобы каждый из них что–то знал об N. Для этого нам понадобится k больших попарно взаимно простых чисел m_i, удовлетворяющих условию $m_1 m_2 \dots m_k > N$. Каждому из участников сообщается свой фрагмент кода, состоящий из пары чисел: числа m_i и r_i — остатка от деления N на m_i. При наличии всех фрагментов код восстанавливается как наименьшее положительное решение системы

$$\begin{cases} x \equiv r_1 \pmod{m_1}, \\ x \equiv r_2 \pmod{m_2}, \\ \dots\dots\dots\dots\dots \\ x \equiv r_k \pmod{m_k}. \end{cases}$$

В отсутствии хотя бы одного участника мы знаем только арифметическую прогрессию

$$a + m_1 m_2 \dots m_{k-1} \cdot t,$$

членом которой является код. Чтобы восстановить пароль, следует провести порядка $\dfrac{N - a}{m_1 m_2 \dots m_{k-1}}$ испытаний.

Интересно и доступно об этом приложении китайской теоремы об остатках написано в [6].

Попробуйте решить следующую задачу.

Задача. Имеется три фрагмента пароля, модули фрагментов — последовательные числа Ферма: F_n, F_{n+1}, F_{n+2} (напомним, что $F_n = 2^{2^n} + 1$). Если двое втайне от третьего захотят вскрыть пароль, то сколько вариантов им придется перебрать?

Задачи

1. Решить системы сравнений:

$$\begin{cases} x \equiv 7 \pmod{12}, \\ x \equiv 4 \pmod{15}, \\ x \equiv -2 \pmod{21}; \end{cases} \quad \begin{cases} 7x \equiv 5 \pmod{11}, \\ 13x \equiv 12 \pmod{23}, \\ 15x \equiv 6 \pmod{21}; \end{cases} \quad \begin{cases} 4x \equiv 1 \pmod{9}, \\ 5x \equiv 3 \pmod{7}, \\ 4x \equiv 16 \pmod{12}. \end{cases}$$

2. При каких значениях a следующая система сравнений совместна:

$$\begin{cases} x \equiv 5 \pmod{18}, \\ x \equiv 8 \pmod{21}, \\ x \equiv a \pmod{35}? \end{cases}$$

3. Найти наименьшее натуральное число, которое при делении на n дает остаток $n-1$, а при делении на $n+1$ дает остаток n.

4. Упростив выражения с помощью китайской теоремы об остатках, решить следующие задачи:

   a) найти остатки от деления 129^{613} на 1001, 359^{204} на 646, 39^{50} на 2251;

   b) найти обратный к 347 по модулю 935.

5. Даша гадает на ромашке: "Любит — не любит, плюнет — поцелует, к сердцу прижмет — к черту пошлет". Глаша при гадании к этим шести вариантам добавляет еще свой: "Своей назовет". На ромашках с n и $2n$ лепестками у Даши хорошее предсказание, а у Глаши плохое. Чему равно n, если считать, что на ромашке не может быть более 100 лепестков?

6. Покажите, что система

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n} \end{cases}$$

   не может иметь более одного решения по модулю наименьшего общего кратного m и n.

7. Решите сравнение $x^2 + 42x + 21 \equiv 0 \pmod{105}$.

8. Пусть p и q — различные простые числа и $n = pq$. Предположим, что мы знаем решение уравнений $x^2 \equiv a \pmod{p}$ и $x^2 \equiv a \pmod{q}$. Покажите, как китайский алгоритм остатков можно использовать для решения сравнения $x^2 \equiv a \pmod{n}$.

13. Сравнения с одним неизвестным

Если $m = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ — каноническое разложение числа m, то сравнение (7) эквивалентно системе сравнений

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{k_1}}, \\ f(x) \equiv 0 \pmod{p_2^{k_2}}, \\ \dots\dots\dots\dots\dots\dots \\ f(x) \equiv 0 \pmod{p_s^{k_s}}. \end{cases} \tag{10}$$

Пусть для каждого из сравнений системы (10) найдено решение

$$x \equiv a_i \pmod{p_i^{k_i}},$$

тогда набор $(a_1, a_2, \dots, a_s)$ может быть единственным образом "поднят" до решения сравнения (7):

$$\begin{cases} x \equiv a_1 \pmod{p_1^{k_1}}, \\ x \equiv a_2 \pmod{p_2^{k_2}}, \\ \dots\dots\dots\dots\dots\dots \\ x \equiv a_s \pmod{p_s^{k_s}}. \end{cases}$$

Пусть N — число решений сравнения (7), а N_i — число решений сравнения

$$f(x) \equiv 0 \pmod{p_i^{k_i}},$$

тогда $N = N_1 N_2 \dots N_s$.

Поскольку каждое решение сравнения по примарному модулю

$$f(x) \equiv 0 \pmod{p^k} \tag{11}$$

является решением сравнения по простому модулю

$$f(x) \equiv 0 \pmod{p}, \tag{12}$$

то для некоторого класса решений можно описать процедуру "поднятия" решения сравнения (12) до решения сравнения (11).

Определение. Назовем решение $x \equiv a \pmod{p}$ сравнения (12) *неособым*, если $f'(a)$ не сравнимо с нулем по модулю p.

Сейчас мы покажем, что всякое неособое решение сравнения (12) единственным образом может быть "поднято" до решения сравнения (11). Достаточно описать переход от сравнения по модулю p^{k-1} к сравнению по модулю p^k.

Пусть $x \equiv a \pmod{p^{k-1}}$ — решение сравнения $f(x) \equiv 0 \pmod{p^{k-1}}$. Разложим $f(x)$ по степеням $x - a$:

$$f(x) = f(a) + b_1(x-a) + \ldots + b_n(x-a)^n \tag{13}$$

(здесь $b_1 = f'(a)$ не сравнимо с нулем по модулю p^{k-1}). Будем искать x в виде $x = a + tp^{k-1}$. После подстановки x в (13) получим

$$f(a) + tp^{k-1}f'(a) \equiv 0 \pmod{p^k},$$

откуда имеем

$$p^{k-1}f'(a)t \equiv -f(a) \pmod{p^k}, \quad p^{k-1} | f(a).$$

Разделим получившееся сравнение вместе с модулем на p^{k-1}:

$$f'(a)t \equiv -\frac{f(a)}{p^{k-1}} \pmod{p},$$

$(f'(a), p) = 1$, и найдем далее единственное $t \equiv s \pmod{p}$. Полученный класс чисел

$$x = a + tp^{k-1} \equiv a + sp^{k-1} \pmod{p^k}$$

определяет ровно один класс вычетов по модулю p^k, который является решением сравнения (11).

Поясним процедуру "поднятия" на примере.

Задача. Найдите все решения сравнения $x^3 \equiv 2 \pmod{125}$.

Решение.

Первый шаг. Решим сравнение $x^3 \equiv 2 \pmod{5}$ методом испытаний полной системы вычетов. Нетрудно получить ответ $x \equiv 3 \pmod{5}$.

Второй шаг. "Поднимем" решение сравнения $x^3 \equiv 2 \pmod{5}$ до решения $x^3 \equiv 2 \pmod{25}$.

Положим $x = 3+5t$. Тогда $f'(x) = 3x^2$, $f'(3) \equiv 2 \pmod{5}$, отсюда получим

$$f(3) + 2 \cdot 5t \equiv 0 \pmod{25},$$

$$2t \equiv \frac{-3^3+2}{5} \pmod 5,$$
$$t \equiv 0 \pmod 5,$$

следовательно, $x \equiv 3 \pmod{25}$.

Третий шаг. Теперь поднимем решение $x^3 \equiv 2 \pmod{25}$ до решения исходного сравнения. Аналогично

$$x = 3 + 25t,$$
$$2 \cdot 5^2 t \equiv -25 \pmod{125},$$
$$2t \equiv -1 \pmod 5,$$
$$t \equiv 2 \pmod 5.$$

В итоге получаем ответ: $x \equiv 53 \pmod{125}$. □

Определение. Назовем два сравнения по одному модулю *эквивалентными*, если множества решений этих сравнений совпадают.

Утверждение. *Сравнение* $f(x) \equiv 0 \pmod p$, $\deg f(x) \geqslant p$, *можно заменить эквивалентным степени, меньшей* p.

Доказательство. Разделим $f(x)$ на $x^p - x$ с остатком:

$$f(x) = (x^p - x)\, q(x) + r(x),$$

где $\deg r(x) < p$. Заметим, что в силу малой теоремы Ферма все классы вычетов по модулю p удовлетворяют сравнению

$$x\left(x^{p-1} - 1\right) \equiv 0 \pmod p.$$

Отсюда получаем, что сравнения $f(x) \equiv 0 \pmod p$ и $r(x) \equiv 0 \pmod p$ имеют одинаковые множества решений. □

Задача. Решите сравнение

$$f(x) \equiv 0 \pmod 5,$$

где $f(x) = 3x^7 + 2x^6 + x^5 - 3x^3 - x^2 - x - 1$.

Решение. Разделим многочлен $f(x)$ на многочлен $x^5 - x$ с остатком и перейдем к эквивалентному сравнению

$$f(x) = \left(3x^2 + 2x + 1\right)\left(x^5 - x\right) + x^2 - 1 \equiv 0 \pmod 5,$$

$x^2 - 1 \equiv 0 \pmod 5$, следовательно, $x \equiv \pm 1 \pmod 5$. □

Задача. Докажите, что среди чисел, представимых многочленом положительной степени с целыми коэффициентами, имеется бесконечно много составных.

Решение. Пусть $f(x) \in \mathbb{Z}[x]$ — многочлен степени $n \geqslant 1$ с целыми коэффициентами, a — целое число, не являющееся корнем $f(x)$ и $f(a) \neq 1$. Пусть $f(a) = m$. Многочлен $f(x)$ не может принимать значение m более n раз.

Рассмотрим значения многочлена $f(x)$ на последовательности $b_k = a + mk$, $k \in \mathbb{Z}$. По свойству I числовых сравнений из того, что $b_k \equiv a \pmod{m}$, следует

$$f(b_k) \equiv 0 \pmod{m}.$$

Получаем, что последовательность $f(b_k)$ состоит из чисел, кратных m. Так как каждое из чисел этой последовательности может появиться не более n раз, получаем, что среди $f(b_k)$ бесконечно много составных. □

Задача. Решите сравнения:

a) $7x^4 + 19x + 25 \equiv 0 \pmod{27}$,

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

14. Квадратичные вычеты. Символ Лежандра

Определение. Пусть $(a, m) = 1$. Число a называется *квадратичным вычетом по модулю m*, если разрешимо сравнение $x^2 \equiv a \pmod{m}$, иначе число a называют *квадратичным невычетом по модулю m*.

Докажите следующие

Утверждения.

1. *Если $m = p$ — простое число, $p > 2$ и a — квадратичный вычет по модулю p, то сравнение $x^2 \equiv a \pmod{p}$ имеет два решения.*

   Указание. Возведите в квадрат приведенную систему, состоящую из вычетов, наименьших по абсолютной величине.

2. *В приведенной системе вычетов по модулю p поровну квадратичных вычетов и невычетов.*

3. *Произведение двух вычетов есть вычет, произведение двух невычетов — вычет, а произведение вычета и невычета — невычет.*

4*. *Классы квадратичных вычетов образуют подгруппу индекса* 2 *в группе* $\mathbb{Z}_p^*$.

5. *Число* $p-1$ *является квадратичным вычетом тогда и только тогда, когда* $p = 4k+1$.

   Указание. Воспользоваться теоремой Вильсона и пунктом 3 предыдущего утверждения.

Определение. По определению, *символ Лежандра* $\left(\frac{a}{p}\right)$ равен 1, если a — квадратичный вычет, и равен -1, если a — невычет, $\left(\frac{a}{p}\right) = 0$, если p делит a.

Справедлива следующая формула, принадлежащая Эйлеру:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Упражнение. Пользуясь формулой Эйлера, получите следующие свойства символа Лежандра:

1. Если $a \equiv b \pmod{p}$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;
2. $\left(\frac{1}{p}\right) = 1$;
3. $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;
5. $\left(\frac{a^2}{p}\right) = 1$.

Вычисление символа Лежандра $\left(\frac{2}{p}\right)$ — особая задача. Ответ здесь таков:

6. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Имеет место следующий красивый результат, принадлежащий Гауссу.

Теорема (квадратичный закон взаимности). *Пусть p и q — нечетные простые, тогда*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Заметим, что символы Лежандра $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ различны только в одном случае, когда

$$p \equiv q \equiv 3 \pmod 4.$$

Упражнение. Покажите, что

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{когда } p \equiv \pm 1 \pmod 8; \\ -1, & \text{когда } p \equiv \pm 3 \pmod 8. \end{cases}$$

Задачи

1. Среди вычетов приведенной системы по модулю 19 укажите квадратичные вычеты.
2. Пользуясь критерием Эйлера, вычислите $\left(\frac{5}{73}\right)$, $\left(\frac{7}{31}\right)$.
3. Пусть $p \equiv 1 \pmod 4$. Докажите, что a и $-a$ одновременно являются или не являются квадратичными вычетами по модулю p.
4. Покажите, что число решений сравнения $x^2 \equiv a \pmod p$, где простое p не делит a, в точности равно $1 + \left(\frac{a}{p}\right)$.
5. Докажите, что
$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0,$$
где a пробегает полную систему вычетов по модулю p.

Разберем следующую задачу.

Задача. Используя квадратичный закон взаимности, вычислите символ Лежандра $\left(\frac{195}{101}\right)$.

Решение. Вычисления проведем, используя свойства символа Лежандра. Заметим, что $195 \equiv 94 \pmod{101}$. Значит,

$$\left(\frac{195}{101}\right) = \left(\frac{94}{101}\right) = \left(\frac{2}{101}\right) \cdot \left(\frac{47}{101}\right) = (-1) \cdot \left(\frac{101}{47}\right) = -\left(\frac{7}{47}\right) = \\ = \left(\frac{47}{7}\right) = \left(\frac{-2}{7}\right) = \left(\frac{-1}{7}\right) \cdot \left(\frac{2}{7}\right) = 1.$$

Промежуточные результаты таковы:

$$\left(\frac{2}{101}\right) = (-1)^{\frac{101^2-1}{8}} = -1; \quad \left(\frac{2}{7}\right) = 1;$$
$$\left(\frac{47}{101}\right) = (-1)^{\frac{47-1}{2} \cdot \frac{101-1}{2}} \left(\frac{101}{47}\right); \quad \left(\frac{-1}{7}\right) = -1. \ \square$$

Задачи

1. Используя свойства символа Лежандра, определите, сколько решений имеют сравнения:

   a) $x^2 \equiv 26 \pmod{71}$,

   b) $x^2 \equiv 48 \pmod{37}$,

   c) $x^2 \equiv 29 \pmod{73}$,

   d) $x^2 \equiv 32 \pmod{97}$,

   e) $x^2 \equiv 103 \pmod{89}$,

   f) $x^2 \equiv 54 \pmod{61}$.

2. Используя квадратичный закон взаимности, найдите $\left(\frac{3}{F_n}\right)$, где

   $$F_n = 2^{2^n} + 1 \text{ — простое число Ферма.}$$

3. Пусть $\left(\frac{a}{p}\right) = 1$. Найдите решения сравнения $x^2 \equiv a \pmod{p}$, где

   $$p \equiv 3 \pmod{4}.$$

   Указание. Покажите, что $a \equiv a^{(p+1)/2} \pmod{p}$, если $\left(\frac{a}{p}\right) = 1$.

4. Укажите способ отыскания решений сравнения $x^2 \equiv a \pmod{p}$, где

$$p \equiv 5 \pmod{8}.$$

Указание. Покажите, что $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$ и воспользуйтесь тем, что $\left(\frac{2}{p}\right) = 1$.

5. Докажите бесконечность множества простых чисел вида $1 + 4k$.

Решение. Пусть простых чисел вида $1 + 4k$ конечное число и пусть все они занесены в список $p_1, p_2, \ldots, p_s$. Составим число $1 + 4p_1^2 p_2^2 \ldots p_s^2$. Построенное число имеет простой делитель q, для которого

$$4p_1^2 p_2^2 \ldots p_s^2 \equiv -1 \pmod{q} \text{ и } \left(\frac{-1}{q}\right) = 1.$$

Следовательно, $q \equiv 1 \pmod{4}$ и q — число из указанного списка, чего быть не может. □

6. Докажите бесконечность множества простых чисел вида $1 + 6k$.

7. Найти арифметические прогрессии, в которых лежат простые p, для которых 3 — квадратичный вычет.

8. Пользуясь теоремой Вильсона, доказать, что решениями сравнения

$$x^2 + 1 \equiv 0 \pmod{p}, \text{ где } p = 4m + 1,$$

будут $x = \pm 1 \cdot 2 \cdot \ldots \cdot 2m \pmod{p}$.

15. Символ Якоби

Символ Якоби обобщает символ Лежандра на случай, когда знаменатель есть составное нечетное число.

Пусть m — любое нечетное положительное число, $m = p_1 p_2 \ldots p_s$ — каноническое разложение числа m на простые множители. (Здесь $p_1, p_2, \ldots p_s$ не обязательно различны.) Тогда определим *символ Якоби* $\left(\frac{a}{m}\right)$ как произведение символов Лежандра:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_s}\right).$$

Для символа Якоби верны свойства 1—6 символа Лежандра и квадратичный закон взаимности.

Замечание. Для символа Якоби условие $\left(\dfrac{a}{m}\right) = 1$ является необходимым, но не достаточным, чтобы сравнение

$$x^2 \equiv a \pmod{m} \tag{14}$$

имело решение.

Упражнение. Приведите пример не имеющего решений сравнения (14) такого, что символ Якоби $\left(\frac{a}{m}\right)$ не равен 1.

Упражнение. Используя квадратичный закон взаимности, проверьте формулу Эйлера

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

для $n = 221$ и $a = 2$.

Используя способы решения сравнений по примарному модулю, докажите следующее свойство.

Теорема. *Пусть p — нечетное простое, причем p не делит число a, тогда число N решений сравнения*

$$x^2 \equiv a \pmod{p^\beta}, \quad \beta \geqslant 1,$$

можно вычислить по формуле

$$N = 1 + \left(\frac{a}{p}\right). \tag{15}$$

Если $p = 2$, то сравнение (15) разрешимо и имеет 4 решения при $\beta \geqslant 3$ тогда и только тогда, когда

$$a \equiv 1 \pmod{8}.$$

16. Порядки (показатели) вычетов и их свойства

Пусть $(a, m) = 1$. Запишем теорему Эйлера:

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

Из сравнения следует, что существуют целые положительные числа k, удовлетворяющие условию

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

Определение. Наименьшее из таких чисел называют *показателем* или *порядком* вычета a по модулю m.

Стандартно, если m фиксировано, порядок и показатель обозначают соответственно $\operatorname{ord} a$ ($\operatorname{ord}_m a$) и $\delta(a)$ ($\delta_m(a)$). Легко получить следующие свойства:

A. Если $a \equiv b \pmod m$, то $\operatorname{ord} a = \operatorname{ord} b$.

B. Числа $a^0, a^1, a^2, \ldots, a^{k-1}$ различны по модулю m, где $k = \operatorname{ord} a$.

C. Порядок вычета a следует искать среди делителей числа $\varphi(m)$.

D. Если $a^n \equiv 1 \pmod n$, то $\operatorname{ord} a$ делит n.

E. Если $a^n \equiv a^s \pmod n$, то $n \equiv s \pmod k$, где $k = \operatorname{ord} a$.

F. Если $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, $a^n \equiv 1 \pmod m$ и a^{n/p_i} не сравнимо с 1 по модулю m, то $\operatorname{ord}_m a$ делится на $p_i^{\alpha_i}$.

Приведем здесь доказательства свойств C и F.

Доказательство свойства C.
Пусть $k = \operatorname{ord} a$. Разделим $\varphi(m)$ на k с остатком:

$$\varphi(m) = kq + r, \quad 0 \leqslant r \leqslant k;$$

$$1 \equiv a^{\varphi(m)} \equiv (a^k)^q \cdot a^r \equiv a^r \pmod m.$$

Используя определение порядка и то, что $r < k$, заключаем, что $r = 0$. $\square$

Доказательство свойства F.
Поскольку $k = \operatorname{ord} a$ — делитель числа n, то

$$k = p_1^{\beta_1} p_2^{\beta_2} \ldots p_s^{\beta_s},$$

где $0 \leqslant \beta_i \leqslant \alpha_i$. Получаем, что число $p_1^{\beta_1} p_2^{\beta_2} \ldots p_i^{\beta_i} \ldots p_s^{\beta_s}$ делит n и не делит $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i - 1} \ldots p_s^{\alpha_s}$. Следовательно, $p_i^{\beta_i}$ не делит $p_i^{\alpha_i - 1}$, откуда $\beta_i = \alpha_i$. $\square$

Упражнение. Докажите самостоятельно свойства A, B, D и E.

Задача 1. Докажите, что два числа Ферма $F_n = 2^{2^n} + 1$ и $F_m = 2^{2^m} + 1$, где $m \neq n$, взаимно просты.

Решение. Предположим, что $n > m$ и p — общий простой делитель чисел F_n и F_m. Тогда

$$2^{2^n} \equiv -1 \pmod p, \quad 2^{2^m} \equiv -1 \pmod p.$$

Получаем, что $\operatorname{ord}_p 2 \mid 2^{m+1}$, следовательно, $\operatorname{ord}_p 2 \mid 2^n$, но тогда

$$2^{2^n} \equiv 1 \pmod{p}. \square$$

Задача 2. Докажите, опираясь на свойства порядка, что

$$\text{если } (s, \operatorname{ord}_m a) = 1, \text{ то } \operatorname{ord}_m a^s = \operatorname{ord}_m a.$$

Задача 3*. Докажите, что если $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, $a^n \equiv 1 \pmod{m}$ и для любого $p_i \mid n$ числа a^{n/p_i} не сравнимы с 1 по модулю m, то $\operatorname{ord}_m a = n$.

Задача 4. Пусть $\operatorname{ord}_m a = k$ и $\operatorname{ord}_m b = s$, причем $(k, s) = 1$. Тогда $\operatorname{ord}_m(ab) = ks$.

Решение. Действительно, $(a \cdot b)^{ks} \equiv 1 \pmod{m}$, следовательно, $\operatorname{ord} a \cdot b$ делит $k \cdot s$.

Пусть теперь p — простой делитель $k \cdot s$. Тогда, если $p \mid k$, то $(p, s) = 1$. Рассмотрим

$$(ab)^{\frac{ks}{p}} \equiv (a^s)^{\frac{k}{p}} (b^s)^{\frac{k}{p}} \equiv (a^s)^{\frac{k}{p}}.$$

Заметим, что $a^{ks/p}$ не сравнимо с 1 по модулю m (см. задачу 2). Используя свойство F и задачу 3, получаем, что $\operatorname{ord}(a \cdot b)$ делится на $k \cdot s$. $\square$

Задача. Рассмотрим последовательность

$$c_n = a^n - b^n, \quad n \in \mathbb{N}.$$

Пусть простое p не делит $a \cdot b$. Найдите первый номер n, удовлетворяющий свойству

$$c_n \equiv 0 \pmod{p}.$$

17. Первообразные корни и индексы

Определение. Число a называется *первообразным корнем по модулю* m, если показатель (порядок) числа a по модулю m равен $\varphi(m)$.

Упражнение. Составьте таблицы показателей для приведенной системы вычетов по модулю m. Проведите вычисления для $m = 2, 4, 6, 7, 8, 9$. Для каких из перечисленных модулей существуют первообразные корни?

Теорема (Гаусса). *Первообразные корни существуют только для следующих модулей:*

$$2, 4, p^\alpha, 2p^\alpha,$$

где p — нечетное простое, α — целое положительное.

Доказать теорему Гаусса можно, реализовав следующий план:

A. Пусть $f(x)$ — многочлен степени n с целыми коэффициентами, среди которых не все кратны p. Тогда сравнение

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

имеет не более чем n решений. Воспользуйтесь этим предложением для доказательства следующего факта:
многочлен $x^d - 1$, где d — делитель числа $p-1$, имеет по модулю p ровно d корней.

Указание. Покажите, что справедливо сравнение

$$\prod_{a=1}^{p-1}(x-a) \equiv x^{p-1} - 1 \pmod{p}$$

и воспользуйтесь тем, что $x^{p-1} - 1$ делится на $x^d - 1$ без остатка.

B. Пусть $\psi(l)$ — количество вычетов в приведенной системе по модулю p, порядок которых равен l. Тогда

$$\sum_{l|d} \psi(l) = d$$

и, в частности,

$$\sum_{d|p-1} \psi(d) = p - 1.$$

Введем обозначения: $F(d) = \sum_{l|d} \psi(l) = d$, где d делит $p-1$. Будем рассматривать $F(n)$ как функцию на множестве целых положительных чисел, определенную условием

$$F(n) = \begin{cases} n, & \text{для } n|(p-1), \\ 0, & \text{для } n \nmid (p-1). \end{cases}$$

C. Применим к равенству

$$\sum_{d|(p-1)} \psi(d) = p - 1$$

формулу обращения Мебиуса:

$$\psi(p-1) = (p-1) \sum_{d|(p-1)} \frac{\mu(d)}{d} = \varphi(p-1) \geq 1.$$

Итак, *первообразный корень по модулю p существует, и число первообразных корней по модулю p равно $\varphi(p-1)$.*

D. Пусть g — некоторый первообразный корень по модулю p. Если порядок g по модулю p^2 *не равен*

$$\varphi(p^2) = (p-1) \cdot p,$$

то рассмотрим число $g \cdot (p+1)$. Заметим, что

$$(p+1)^p \equiv 1 \pmod{p^2}.$$

Чему равен показатель $p+1$ по модулю p^2?

Далее, пусть k — порядок g по модулю p^2, тогда

$$g^k \equiv 1 \pmod{p^2}$$

и, следовательно,

$$g^k \equiv 1 \pmod{p},$$

откуда следует, что $p-1$ делит k, то есть $k = (p-1) \cdot t$ и $\varphi(p^2)$ делится на k. Поскольку g — не первообразный корень по модулю p^2, то $k = p-1$.

Окончательно получаем, что $g \cdot (p+1)$ имеет порядок $\varphi(p^2)$.

E. Покажите, что любой первообразный корень g по модулю p^k будет первообразным корнем и по модулю p^{k+1}, где $k \geqslant 2$. Примените метод математической индукции, используя следующие указания.
Покажите, что справедливы сравнения

$$g^{(p-1)p^{k-2}} \equiv 1 \pmod{p^{k-1}},$$
$$g^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k},$$

откуда следует, что

$$g^{(p-1)p^{k-2}} = 1 + t \cdot p^{k-1}, \quad p \nmid t.$$

Далее

$$g^{(p-1)p^{k-1}} \equiv \left(1 + t \cdot p^{k-1}\right)^p \equiv 1 + t \cdot p^k \not\equiv 1 \pmod{p^{k+1}}.$$

Используя свойство порядка F, получите нужный результат.

F. Докажите, что первообразным корнем по модулю $2p^\alpha$ будет нечетный первообразный корень по модулю p^α.

G. Случаи $m = 2$ и $m = 4$ рассмотрите отдельно.

Как искать первообразные корни по модулю p? Запишем каноническое разложение числа $p-1 = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}$, где q_i — различные простые.

Нам нужно подобрать такой вычет a, чтобы $\operatorname{ord}_p a$ делился на $q_i^{\alpha_i}$ для любого $i = 1, 2, \dots, s$. Используя задачу 3, выпишем условие, определяющее первообразный корень по модулю p:

$$\begin{cases} a^{(p-1)/q_1} \not\equiv 1 \pmod p, \\ a^{(p-1)/q_2} \not\equiv 1 \pmod p, \\ \dots\dots\dots\dots\dots\dots \\ a^{(p-1)/q_s} \not\equiv 1 \pmod p. \end{cases}$$

Методом испытаний найдем нужное a.

Замечание. Поскольку $(p-1)$ — число четное, то одно из условий системы будет выглядеть следующим образом:

$$a^{(p-1)/2} \not\equiv 1 \pmod p$$

или, что то же самое,

$$\left(\frac{a}{p}\right) = -1.$$

Задача. Найдите наименьший первообразный корень по модулю 37.

Решение. Запишем систему, определяющую первообразный корень по модулю 37:

$$36 = 2^2 \cdot 3^2.$$

Заметим, что a — первообразный корень по модулю 37 тогда и только тогда, когда

$$\begin{cases} a^{18} \not\equiv 1 \pmod{37}, \\ a^{12} \not\equiv 1 \pmod{37}. \end{cases}$$

Начнем с $a = 2$. Первое сравнение выполняется:

$$2^{18} \equiv \left(\frac{2}{37}\right) = -1.$$

Проверим справедливость второго условия:

$$\begin{gathered} 2^5 \equiv 32 \equiv -5 \pmod{37}; \\ 2^{10} \equiv 25 \equiv -12 \pmod{37}; \\ 2^{12} \equiv -48 \not\equiv 1 \pmod{37}. \end{gathered}$$

Таким образом, 2 — наименьший первообразный корень по модулю 37. □

Пусть p — фиксированное простое число, g — некоторый первообразный корень по модулю p.

Степени первообразного корня

$$g^0, g^1, g^2, \ldots, g^{p-2}$$

образуют приведенную систему вычетов по модулю p. Для всякого целого a, взаимно простого с p, найдется число s такое, что $0 \leqslant s \leqslant p-2$ и

$$a = g^s \pmod{p}.$$

В этом случае показатель s называется *индексом числа a по основанию g* или *дискретным логарифмом по модулю p*. Для записи используют стандартное обозначение

$$s = \operatorname{ind}_g a.$$

Поскольку p — фиксированное число, то корректна и такая запись:

$$s = \operatorname{ind} a.$$

В качестве **упражнения** докажите следующие свойства индексов:

1. Если $a \equiv b \pmod{p}$, то $\operatorname{ind} a = \operatorname{ind} b$.
2. Если $g^s \equiv g^t \pmod{p}$, то $s \equiv t \pmod{p-1}$.
3. $\operatorname{ind}(a \cdot b) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{p-1}$.
4. $\operatorname{ind} a^k \equiv k \cdot \operatorname{ind} a \pmod{p-1}$.
5. $\operatorname{ind}(-1) = \dfrac{p-1}{2}$.

Свойства индексов позволяют сводить решения степенных сравнений к решению линейных сравнений. *Проиндексировать*, или *прологарифмировать*, сравнение

$$ax^n \equiv b \pmod{p}, \quad (a \cdot b, p) = 1,$$

означает перейти к эквивалентному линейному относительно $\operatorname{ind} x$ сравнению

$$\operatorname{ind} a + n \cdot \operatorname{ind} x \equiv \operatorname{ind} b \pmod{p-1}.$$

Задачи

1. Укажите число первообразных корней и найдите наименьший первообразный корень по модулю p, если $p = 23, 37, 97, 89$.

2. Докажите, что первообразный корень простого числа q вида $2p+1$ при простом p вида $4n+1$ есть 2, а при $p = 4n+3$ есть -2.

3. Докажите, что первообразный корень простого числа вида $4p+1$, где число p — простое, есть 2.

4. Докажите, что первообразный корень простого числа вида 2^n+1, где $n > 1$, есть 3.

5. Расположите на окружности числа от 1 до 29 так, чтобы для трех чисел a, b, c, идущих подряд, выполнялось

$$b^2 - ac \equiv 0 \pmod{29}.$$

   Сколькими способами это можно сделать?

6. Пусть p — нечетное простое. Покажите, что для четного первообразного корня a по модулю p число $a+p$ — первообразный корень по модулю $2p$.

7*. Укажите необходимое и достаточное условие разрешимости степенного сравнения

$$x^n \equiv a \pmod{p^\alpha},$$

   где $p \neq 2$.

8*. Докажите, что для любого m, такого, что m делит число $p-1$, в $\mathbb{Z}_p^*$ существует ровно $\varphi(m)$ чисел, порядок которых равен m.

9. Пусть $p_1, p_2, \ldots, p_s$ — нечетные простые числа. Докажите, что существует число a, являющееся одновременно первообразным корнем по каждому простому p_i.

10*. Обозначим через r_n остатки от деления n^n на p. Докажите, что последовательность r_n — периодическая. Найдите ее наименьший положительный период.

11. Известно, что a — первообразный корень по модулю p. Что можно сказать о значении $\left(\dfrac{a}{p}\right)$?

12. Докажите, что классы квадратичных вычетов по модулю p образуют подгруппу в мультипликативной группе поля. Что можно выбрать в качестве образующей этой группы?

13. Найдя наименьший первообразный корень по модулю 23, получите все квадратичные вычеты по модулю 23.

14. Пусть a — первообразный корень по модулю p^n. Покажите, что тогда a — первообразный корень по модулю p.

Приведем решение следующей задачи.
Задача. Решите сравнение

$$48x^7 \equiv 3 \pmod{61}.$$

Решение. Выпишем условия, определяющие первообразный корень по модулю 61:

$$\begin{cases} a^{30} \not\equiv 1 \pmod{61}, \\ a^{12} \not\equiv 1 \pmod{61}, \\ a^{20} \not\equiv 1 \pmod{61}. \end{cases}$$

Непосредственной подстановкой убеждаемся, что $a = 2$ — первообразный корень по модулю 61. Проиндексируем сравнение

$$\operatorname{ind} 48 + 7 \cdot \operatorname{ind} x \equiv \operatorname{ind} 3 \pmod{60}.$$

Составим фрагмент таблицы индексов:

$$\begin{array}{ll} 2^1 \equiv 2 \pmod{61}, & 2^2 \equiv 4 \pmod{61}, \\ 2^3 \equiv 8 \pmod{61}, & 2^4 \equiv 16 \pmod{61}, \\ 2^5 \equiv 32 \pmod{61}, & 2^6 \equiv 3 \pmod{61}, \\ 2^7 \equiv 6 \pmod{61}, & 2^8 \equiv 12 \pmod{61}, \\ 2^9 \equiv 24 \pmod{61}, & 2^{10} \equiv 48 \pmod{61}. \end{array}$$

$\operatorname{ind} a$	1	2	3	4	5	6	7	8	9	10
a	2	4	8	16	32	3	6	12	24	48

В итоге получим:

$$10 + 7 \cdot \operatorname{ind} x \equiv 8 \pmod{60};$$
$$7 \cdot \operatorname{ind} x \equiv -2 \pmod{60}.$$

Заметим, что $(7, 60) = 1$, следовательно, сравнение имеет единственное решение:

$$7 \cdot \operatorname{ind} x \equiv -2 - 3 \cdot 60 \equiv -182 \pmod{60};$$
$$\operatorname{ind} x \equiv -26 \pmod{60};$$
$$\operatorname{ind} x \equiv 34 \pmod{60}.$$

Окончательно находим x:

$$x \equiv 2^{34} \pmod{61};$$
$$x \equiv (2^{10})^3 \cdot 2^4 \equiv 48^3 \cdot 2^4 \equiv (-13)^3 \cdot 2^4 \equiv 45 \pmod{61}.$$

Решением исходного сравнения является

$$x \equiv 45 \pmod{61}. \square$$

Задача. Найдите наименьший первообразный корень по модулю p, а также составьте фрагмент таблицы индексов, необходимый для решения сравнения:

1. $51x^7 \equiv 14 \pmod{89}$,
2. $65x^5 \equiv 42 \pmod{89}$,
3. $6x^5 \equiv 30 \pmod{97}$,
4. $40x^8 \equiv 71 \pmod{97}$,
5. $4x^5 \equiv 5 \pmod{67}$,
6. $9x^8 \equiv 19 \pmod{67}$,
7. $59x^3 \equiv 51 \pmod{71}$,
8. $48x^7 \equiv 3 \pmod{61}$,
9. $24x^{11} \equiv 9 \pmod{61}$,
10. $18x^5 \equiv 4 \pmod{79}$,
11. $27x^{11} \equiv 54 \pmod{79}$,
12. $39x^5 \equiv 27 \pmod{37}$,
13. $25x^7 \equiv 29 \pmod{37}$.

Примерные варианты контрольной работы по курсу теории чисел

Вариант 1

1. Решите систему сравнений

$$\begin{cases} x \equiv 3 \pmod{13}, \\ x \equiv 0 \pmod{12}, \\ x \equiv 4 \pmod{5}. \end{cases}$$

2. Решите сравнения
   $6x \equiv 9 \pmod{15}$,
   $15x \equiv 7 \pmod{22}$.

3. Найдите наименьший первообразный корень по модулю 47.

4. Решите сравнение
   $7x^{11} \equiv 59 \pmod{71}$.

Вариант 2

1. Решите систему сравнений

$$\begin{cases} x \equiv 3 \pmod{9}, \\ x \equiv 1 \pmod{2}, \\ x \equiv 2 \pmod{5}. \end{cases}$$

2. Решите сравнения
   $18x \equiv 9 \pmod{36}$,
   $15x \equiv 18 \pmod{54}$.

3. Найдите наименьший первообразный корень по модулю 59.

4. Решите сравнение
   $12x^5 \equiv 43 \pmod{47}$.

Вариант 3

1. Решите систему сравнений

$$\begin{cases} x \equiv 2 \pmod{7}, \\ x \equiv 5 \pmod{6}, \\ x \equiv 1 \pmod{5}. \end{cases}$$

2. Решите сравнения
   $11x \equiv 37 \pmod{59}$,
   $6x \equiv 18 \pmod{27}$.

3. Найдите наименьший первообразный корень по модулю 79.

4. Решите сравнение
   $39x^{11} \equiv 27 \pmod{37}$.

Вариант 4

1. Решите систему сравнений

$$\begin{cases} x \equiv 1 \pmod{5}, \\ x \equiv 9 \pmod{11}, \\ x \equiv 2 \pmod{3}. \end{cases}$$

2. Решите сравнения
   $27x \equiv 9 \pmod{18}$,
   $37x \equiv 1 \pmod{18}$.

3. Найдите наименьший первообразный корень по модулю 37.

4. Решите сравнение
   $25x^{13} \equiv 28 \pmod{97}$.

Вариант 5

1. Решите систему сравнений

$$\begin{cases} x \equiv 6 \pmod{7}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 1 \pmod{3}. \end{cases}$$

2. Решите сравнения
   $12x \equiv 4 \pmod{16}$,
   $28x \equiv 7 \pmod{19}$.

3. Найдите наименьший первообразный корень по модулю 31.

4. Решите сравнение
   $9x^5 \equiv 2 \pmod{79}$.

Вариант 6

1. Решите систему сравнений

$$\begin{cases} x \equiv 2 \pmod 3, \\ x \equiv 1 \pmod 5, \\ x \equiv 4 \pmod{11}. \end{cases}$$

2. Решите сравнения
   $17x \equiv 24 \pmod{37}$,
   $14x \equiv 21 \pmod{35}$.

3. Найдите наименьший первообразный корень по модулю 29.

4. Решите сравнение
   $8x^7 \equiv 11 \pmod{53}$.

Вариант 7

1. Решите систему сравнений

$$\begin{cases} x \equiv 0 \pmod 3, \\ x \equiv 3 \pmod 5, \\ x \equiv 2 \pmod{11}. \end{cases}$$

2. Решите сравнения
   $39x \equiv 18 \pmod{42}$,
   $19x \equiv 7 \pmod{23}$.

3. Найдите наименьший первообразный корень по модулю 79.

4. Решите сравнение
   $31x^7 \equiv 52 \pmod{73}$.

Вариант 8

1. Решите систему сравнений

$$\begin{cases} x \equiv 2 \pmod{11}, \\ x \equiv 0 \pmod 2, \\ x \equiv 2 \pmod 5. \end{cases}$$

2. Решите сравнения
   $15x \equiv 37 \pmod{97}$,
   $4x \equiv 14 \pmod{26}$.

3. Найдите наименьший первообразный корень по модулю 83.

4. Решите сравнение
$12x^7 \equiv 35 \pmod{61}$.

Вариант 9

1. Решите систему сравнений

$$\begin{cases} x \equiv 1 \pmod{12}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 0 \pmod{7}. \end{cases}$$

2. Решите сравнения
$6x \equiv 33 \pmod{39}$,
$17x \equiv 61 \pmod{37}$.

3. Найдите наименьший первообразный корень по модулю 67.

4. Решите сравнение
$18x^{11} \equiv 72 \pmod{79}$.

Вариант 10

1. Решите систему сравнений

$$\begin{cases} x \equiv 1 \pmod{7}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 0 \pmod{9}. \end{cases}$$

2. Решите сравнения
$14x \equiv 28 \pmod{49}$,
$19x \equiv 3 \pmod{71}$.

3. Найдите наименьший первообразный корень по модулю 59.

4. Решите сравнение
$2x^{13} \equiv 27 \pmod{71}$.

Библиографический список

[1] Cohen H. A Course in Computational Algebraic Number Theory. New York: Springer-Verlag, 1996. 546 p.

[2] Ribenboim P. The New Book of Prime Number Records. New York: Springer-Verlag, 1996. 541 p.

[3] Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 415 с.

[4] Виноградов И. М. Основы теории чисел. М.: Изд-во «Лань», 2006. 176 с.

[5] Гашков С. Б., Чубариков В. Н. Арифметика. Алгоритмы. Сложность вычислений. М.: Изд-во «Дрофа», 2005. 319 с.

[6] Коутинхо С. Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. 328 с.

[7] Серпинский В. 250 задач по элементарной теории чисел. М.: Просвешение, 1968. 161 с.

Учебное издание

Азовская Татьяна Владимировна

Севостьянова Виктория Владимировна

Задачи по теории чисел

Учебное пособие

Редактор Н. А. Волынкина
Компьютерная верстка, макет В. В. Севостьянова

Подписано в печать 15.12.09. Формат 60×84/16.
Бумага офсетная. Печать офсетная. Усл.-печ. л. 4,2. Уч.-изд. л. 4,5.
Typeset by LaTeX. Тираж 150 экз. Заказ №
Издательство «Самарский университет»;
443011, Самара, ул. Академика Павлова, 1.
Тел. (846) 334—54—23.
Отпечатано на УОП СамГУ.