

XLIV Санкт-Петербургская ЛМШ  
*Группа С*



М.И. Магин  
Я.В. Нагибин  
С.И. Захаров

В данном файле находятся задачи и пунктирный конспект занятий группы *C* в XLV Санкт-Петербургской Летней Математической Школе, проходившей с 8 до 28 августа 2024г. в ДОЛ “Восход” близ города Луги. Занятия в этом лагере были посвящены, в основном, знакомству с элементарной арифметикой.



Составлением серий для группы *C* занимались А.С. Голованов и М.И. Магин, ликбезы читал М.И. Магин. Эта смена стала второй по счету для нашего городского кружка.

# Содержание

<b>1</b>	<b>Серии</b>	<b>4</b>
1.	Серия 1: про вычеты	4
2.	Серия 2: сначала стулья, всё остальное — потом.	4
3.	Серия 3: Соответствия.	5
4.	Серия 4: С приложениями знаний.	6
5.	Серия 5: Алгебра. В основном — алгебра.	7
6.	Серия 6: А с погодой повезло — дождь идёт четвёртый день.	8
6.	Серия 7. В постельных тонах.	8
8.	Серия 8: демонстрирующая неслыханный гуманизм.	9
9.	Серия 9: Улучшаем показатели	10
10.	Серия 10: с буквой $\sigma$	11
11.	Серия 11: с чем у нас плохо?	11
12.	Серия 12: Степени вхождения и кое-что новое.	12
<b>2</b>	<b>Вычеты</b>	<b>14</b>
2.1	Сравнения по модулю: напоминание	14
2.2	Полная и приведённая системы вычетов, их приложения.	16
2.3	Китайская теорема об остатках	18
2.4	Обратимые вычеты и теорема Вильсона	20
2.5	Линейное представление НОД	22
2.6	Линейные сравнения	23
2.7	Линейные диофантовы уравнения	24
<b>3</b>	<b>Мультипликативные функции</b>	<b>25</b>
3.1	Сумма делителей и количество делителей	25
3.2	Функция Эйлера	27
3.3	Показатель числа по модулю	28
3.4	Сумматоры мультипликативных функций	28
<b>4</b>	<b>Квадратичные вычеты</b>	<b>30</b>
4.1	Определения и базовые свойства	30
4.2	Критерий Эйлера	32

# 1 Серии

## Серия 1: про вычеты

1. Остап Бендер организовал раздачу слонов населению. Явилось двадцать человек. Остап построил их по кругу, дал одному первого слона, его соседу слева – второго, затем одного человека пропустил, следующему дал слона, пропустил двоих, следующему дал слона и т.д., пока не раздал всех 2024 имеющихся у него слонов. Скольким желающим не досталось ни одного слона?

2. При каких натуральных  $n$  значения выражения  $m^3 - 3m$  при натуральных  $m$  дают все возможные остатки от деления на  $n$ ?

3. Хан сказал Чаку натуральные числа  $n$  и  $d$ . Чак выписал все натуральные числа, а после этого подчеркнул все числа, дающие такой же остаток при делении на  $d$ , как и число  $2^{2^n} + 1$ . Нашлось такое натуральное число  $m \neq n$ , что число  $2^{2^m} + 1$  подчёркнуто. Докажите, что найдется такое натуральное число  $k$ , отличное от  $m$  и  $n$ , что число  $2^{2^k} + 1$  подчёркнуто.

4. На доске было написано натуральное число. Каждую минуту настойчивый мальчик Алёша увеличивает его на одно и то же натуральное  $d$ . Когда учительница заглянула в класс, на доске был написан точный квадрат. Докажите, что Алёша напишет ещё бесконечно много точных квадратов.

5. Можно ли, используя только три разных цифры, составить 56 четырехзначных чисел, дающих разные остатки при делении на 56?

6. У восьми натуральных чисел посчитали всевозможные попарные произведения. Докажите, что какие-то два из этих произведений дают одинаковые остатки при делении на 35.

7. Квадрат натурального числа даёт при делении на  $n$  остаток 8, а куб того же числа даёт при делении на  $n$  остаток 25. Чему может быть равно  $n$ ?

8. Одно и то же нечетное натуральное число разделили с остатком на каждое из чисел 2, 3, 4, ..., 1000000. Все полученные остатки оказались различными, при этом один из них равен нулю. Докажите, что нулевой остаток получился при делении на число, большее 500000.

## Серия 2: сначала стулья, всё остальное — потом.

1. Даны два различных натуральных числа  $a$  и  $b$ , меньшие 59. Для каждого натурального  $k < 59$  Петя вычислил остатки от деления чисел  $ak$  и  $bk$  на 59 и выписал в тетрадь сумму этих двух остатков. Сколько среди выписанных 58 сумм может быть тех, которые больше 59?

2. Дано простое число  $p$  и целое  $a$ , не кратное  $p$ . Рассмотрим ориентированный граф, вершины которого – ненулевые вычеты  $\bmod p$ , и из каждой вершины  $x$  стрелка ведёт в вершину  $ax$ .

а) Докажите, что полученный граф представляет собой объединение циклов без общих вершин.

б) Докажите, что во всех циклах поровну элементов.

в) Выведите из последнего утверждения малую теорему Ферма:  $a^{p-1} \equiv 1 \pmod{p}$ .

3. а) Докажите, что при простом  $p$  и  $0 < k < p$  число  $C_p^k$  делится на  $p$ .

б) Докажите, что при любых целых  $a, b$  и простом  $p$  число  $(a+b)^p - a^p - b^p$  делится на  $p$ .

в) Выведите из последнего утверждения малую теорему Ферма:  $a^p - a$  делится на  $p$  при целом  $a$  и простом  $p$ .

4. Номер телефона Иветты – 395322, а Соланж – 435903. Если разделить эти номера на трехзначный код города, где они живут, получатся одинаковые остатки, равные двузначному коду страны, где они живут. В какой стране живут девушки? Найдите хотя бы её код.

5. Найдите все точные квадраты, которые при делении на 11 дают в частном простое число, а в остатке 4.

6. Существует ли

а) 2023-значное число, 2023-я степень которого оканчивается самим этим числом?

б) 2024-значное число, 2024-я степень которого оканчивается самим этим числом?

(Напомним, что десятичная запись натурального числа не может начинаться с нуля.)

7. В последовательности  $a_1, a_2, \dots$  целых чисел есть бесконечно много положительных и бесконечно много отрицательных членов. Для каждого  $n$  числа  $a_1, a_2, \dots, a_n$  дают попарно различные остатки при делении на  $n$ . Сколько раз в последовательности встречается число 2024?

8. Дано 8 трехзначных чисел. Докажите, что из них можно выбрать два и записать их подряд таким образом, что получившееся шестизначное число будет делиться на 7.

### Серия 3: Соответствия.

Природа – некий храм, где от живых колонн  
Обрывки смутных фраз исходят временами.  
Как в чаще символов мы ходим в этом храме,  
И взглядом родственным глядит на смертных он.  
Подобно голосам на дальнем расстоянии,  
Когда их стройный хор един, как тень и свет,  
Перекликаются звук, запах, форма, цвет,  
Глубокий, темный смысл обретшие в слиянье.

Ш.Бодлер

1. а)  $p$  точек ( $p$  – простое) разбивают окружность на  $p$  равных дуг. Эти точки окрашиваются в  $n$  цветов. Сколько существует существенно различных раскрасок

(существенно различными мы считаем раскраски, не переходящие друг в друга при поворотах окружности)?

б) Выведите из результата п.а) малую теорему Ферма.

2. Докажите, что количество решений уравнения

$$x_1 + 2x_2 + \dots + nx_n = a$$

в натуральных числах равно количеству решений уравнения

$$y_1 + 2y_2 + \dots + ny_n = a - \frac{n(n+1)}{2}$$

в целых неотрицательных числах.

3. Докажите, что для каждого натурального  $a$  существует единственная пара натуральных чисел  $(x, y)$  такая, что

$$a = x + \frac{(x+y-1)(x+y-2)}{2}.$$

4. Пусть  $n$  – натуральное число. Докажите, что число упорядоченных пар натуральных чисел  $(u, v)$ , для которых  $[u, v] = n$ , равно числу натуральных делителей  $n^2$ .

5. Пусть  $x$  и  $y$  – натуральные числа, такие, что  $x+y$  – простое число и  $x^4+y^4$  делится на  $x+y$ . Найдите все такие числа  $x$  и  $y$ .

6. Все натуральные делители натурального числа  $d$  занумеровали в порядке возрастания:  $d_1 < d_2 < d_3 < \dots$ . Оказалось, что  $d_4 + d_6 + d_7 = d$ . Найдите число  $d$  (перечислите все возможности).

7. Некоторое число  $k$  равно произведению 100 различных простых чисел. Докажите, что у  $k$  найдутся 100 различных натуральных делителей, сумма которых взаимно проста с  $k$ .

8. Существует ли двузначное число, обладающее следующим свойством: если вставить между его цифрами произвольное ненулевое количество семерок, то полученное число будет делиться нацело на 13?

#### Серия 4: С приложениями знаний.

1. Дано простое число  $p$ . Числа от 1 до  $p-1$  выписаны в строку в некотором порядке. Под ними во второй строке выписаны те же числа в некотором (возможно, том же самом) порядке. В третьей строке выписаны числа, каждое из которых равно произведению двух чисел, стоящих над ним. Докажите, что в третьей строке есть два числа, дающие одинаковые остатки при делении на  $p$ .

2. Дано нечётное натуральное число  $n$ . На доске выписаны в порядке возрастания все остатки, которые могут давать степени 2 при делении на  $n$ . (Например, при  $n = 9$  на доске были бы написаны числа 1, 2, 4, 5, 7, 8.) Всегда ли по этим числам можно определить  $n$ ?

3. Натуральное число  $A$  таково, что при делении на  $A$  любое нечетное число и его куб дают один и тот же остаток. Найдите все такие числа.

4. Найдите все натуральные  $n$ , большие 1 и такие, что если  $ab + 1$  делится на  $n$  для каких-то натуральных чисел  $a$  и  $b$ , то и  $a + b$  тоже делится на  $n$ .

5. а) Докажите, что  $2^{3^{100}} + 1$  делится на  $3^{101}$ , и б) не делится на  $3^{102}$ .

6. В последовательности натуральных чисел каждый член – точный квадрат, и каждый член, начиная со второго, больше предыдущего на простое число или на квадрат простого числа. Какое наибольшее количество членов в ней может быть?

7. Докажите, что существует а) 4 последовательных натуральных числа, б) 100 последовательных натуральных чисел, каждое из которых делится на точный квадрат, больший 1.

8. Натуральный делитель натурального числа  $n$  будем называть *собственным*, если он отличен от 1 и  $n$ . В разложение натурального числа  $n$  на простые сомножители каждое простое число входит в нечётной степени. Докажите, что произведение двух самых больших собственных делителей  $n$  делится на произведение двух самых маленьких собственных делителей  $n$ .

### Серия 5: Алгебра. В основном – алгебра.

– Чем ты занимался, Лосяш, в этом средневековье?

– Алхимией. В основном – алхимией.

1. а)  $p$  точек ( $p$  – простое) разбивают окружность на  $p$  равных дуг. Сколько существует ориентированных звездчатых  $p$ -угольников (т.е. замкнутых  $p$ -звенных ломаных) с вершинами в этих  $p$  точках (мы считаем два  $p$ -угольника различными, если они отличаются направлением обхода вершин)?

б) Выведите из результата п.а) теорему Вильсона.

2. Натуральное  $n$  называется избыточным, если сумма всех его натуральных делителей, кроме него самого, больше  $n$ . Докажите, что если  $n$  – избыточное число, то для произвольного натурального числа  $k$  число  $kn$  тоже избыточно.

3. Найдите все совершенные  $n$  такие, что числа  $n - 1$  и  $n + 1$  – простые. (Совершенным числом называется натуральное число, равное сумме всех своих натуральных делителей, отличных от него самого.)

4. Натуральное число называется странным, если среди любых его трёх натуральных делителей можно выбрать два, один из которых делится на другой. Сколько странных чисел среди делителей числа  $30^{30}$ ?

5. Пусть  $e(k)$  – количество четных натуральных делителей натурального числа  $k$ , а  $o(k)$  – количество его нечетных натуральных делителей. Докажите, что  $e(1) + e(2) + \dots + e(n)$  отличается от  $o(1) + o(2) + \dots + o(n)$  не больше, чем на  $n$ .

6. Существует ли натуральное число, среди натуральных делителей которого точных квадратов ровно в 32 раза больше, чем точных четвёртых степеней?

7. У натурального числа  $n$  ровно 120 натуральных делителей (считая 1 и  $n$ ). Для каждого делителя  $d$  числа  $n$  нашли неполное частное и остаток от деления

$4n - 3$  на  $d$ . Пусть  $Q$  – сумма всех полученных неполных частных, а  $R$  – сумма всех полученных остатков. Чему может быть равно число  $Q - 4R$ ?

8. Назовем натуральное число *черным*, если оно равно 1 или является произведением четного количества простых чисел (необязательно различных). Все остальные натуральные числа назовем *белыми*. Существует ли натуральное число, у которого сумма всех белых делителей равна сумме всех черных? (1 и само число тоже считаются делителями.)

### Серия 6: А с погодой повезло — дождь идёт четвёртый день.

1. Докажите, что если  $a, b, c$  – натуральные числа такие, что  $3a + 1004b + 2006c = 0$ , то число  $N = 2ac - 3a^2$  делится на 2008.

2. Куб натурального числа записывается более чем тремя цифрами и не оканчивается нулем. Когда у него зачеркнули три последние цифры, получился также куб натурального числа. Чему мог быть равен исходный куб?

3. Натуральные числа  $a$  и  $b$  таковы, что натуральное число  $a - b$  делится на натуральное число  $2b - a$ . Докажите, что число  $2b - a$  является наибольшим общим делителем чисел  $a$  и  $b$ .

4. Дано число  $n = 2^{300} \cdot 3^{300}$ . Сколько существует делителей числа  $n^2$ , которые меньше  $n$ , но не являются делителями  $n$ ?

5. Для данного натурального  $n$  назовем *цепью делителей  $n$*  последовательность различных натуральных чисел, начинающуюся с 1, оканчивающуюся  $n$  и такую, что каждый ее член, начиная со второго, делится на предыдущий (например, при  $n = 20$  цепями делителей  $n$  являются последовательности 1, 5, 10, 20 и 1, 4, 20). Найдите количество цепей делителей числа 2310, состоящих из 6 чисел.

6. Докажите, что если числа  $ab, cd$  и  $ac + bd$  делятся на  $k$ , то  $ac$  и  $bd$  тоже делятся на  $k$  ( $a, b, c, d, k$  – натуральные числа).

7. Найдите все натуральные  $n$ , для которых  $\frac{4n-2}{2n+5}$  равно отношению квадратов двух натуральных чисел.

8. Даны натуральное  $n$  и простое  $p$ . Докажите, что если  $n!$  делится на  $p^p$ , то оно делится и на  $p^{p+1}$ .

### Серия 7. В постельных тонах.

1. Докажите, что  $\left(\frac{p-1}{2}\right)!^2 = \left(1 \cdot 2 \cdot 3 \times \dots \times \left(\frac{p-1}{2}\right)\right)^2 \equiv -1 \pmod{p}$  при простом  $p = 4k + 1$ .

2.  $p$  – простое число,  $p > 5$ . Докажите, что число, десятичная запись которого состоит из  $p - 1$  единицы, делится на  $p$ .

3. а) В группе  $C$  Санкт-Петербургской ЛМШ учится 16 человек. Сегодня каждый из них сдал постельное белье. 9 человек сдали пододеяльник, 14 человек сдали простыню и 11 человек сдали наволочку. При этом пододеяльник и простыню сдало 7 человек, простыню и наволочку — 9 человек, а наволочку и

пододеяльник — 8 человек. Сколько человек сдали полный комплект (из простыни, наволочки и пододеяльника)?

б) Всего в Санкт-Петербургской ЛМШ обучается 58 человек. На завтрак пришло 42 человека, на обед — 54, на полдник — 43, а на ужин — 51. На каждую пару приемов пищи сходило по 40 человек. На все, кроме завтрака ходили 32 человека, на все, кроме обеда — 25 человек, на все, кроме полдника — 30 человек, на все, кроме ужина — 12 человек, а на все четыре приема пищи сходил только один человек. Сколько людей в корпусе голодает?

в) Пусть  $A_1, A_2, \dots, A_n$  — конечные множества. Докажите, что тогда

$$\left| \bigcup_{i=1}^n A_i \right| = |A_1| + |A_2| + \dots + |A_n| - (|A_1 \cap A_2| + \dots + |A_{n-1} \cap A_n|) + (|A_1 \cap A_2 \cap A_3| + \dots + |A_{n-2} \cap A_{n-1} \cap A_n|) - \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_n|.$$

**Пояснение.** Во второй скобке все попарные пересечения. В третьей — все пересечения по три и т.д.

4. Докажите, что  $C_{p-1}^k \equiv \pm 1 \pmod{p}$  при  $0 \leq k \leq p-1$ .

5. Некоторое множество целых чисел, среди элементов которого есть как положительные, так и отрицательные, вместе с каждым своими элементами  $a$  и  $b$  содержит  $2a$  и  $a+b$ .

Доказать, что это множество содержит разность любых двух своих элементов.

6. Даны взаимно простые натуральные числа  $a$  и  $b$ . Найдите

а) наибольшее натуральное число, которое нельзя представить в виде  $ax+by$  с натуральными  $x$  и  $y$ ;

б) наибольшее натуральное число, которое нельзя представить в виде  $ax+by$  с целыми неотрицательными  $x$  и  $y$ .

7. В стране конечное число городов. Они связаны дорогами с односторонним движением. Известно, что для любых двух городов от одного можно добраться до другого. Доказать, что найдется город, из которого можно добраться до всех остальных.

8. На доске выписано несколько положительных вещественных чисел. Докажите, что среди них найдется такое, для которого среди выписанных нет ни втрое большего числа, ни вдвое меньшего.

## Серия 8: демонстрирующая неслыханный гуманизм.

Напомним, что через  $d(n)$  мы обозначаем количество натуральных делителей числа  $n$ .

1. Натуральное число  $n$  делится на 2 и на 9.

а)  $d(n) = 14$ . Докажите, что существует единственное такое  $n$ .

б)  $d(n) = 15$ . Докажите, что существует много таких  $n$ , и найдите их.

в)  $d(n) = 17$ . Докажите, что таких  $n$  не существует.

2. Докажите, что если число  $2^p - 1$  – простое, то число  $2^{p-1}(2^p - 1)$  – совершенное.

3. Число  $a$  не делится на 101. Докажите, что одно из чисел  $a^{50} - 1$  и  $a^{50} + 1$  делится на 101.

4.  $a$  – целое число,  $(a, 561) = 1$ . Докажите, что  $a^{560} \equiv 1 \pmod{561}$ .

5. Докажите, что для любых натуральных  $a$  и  $b$   $d(ab) \geq d(a) + d(b) - 1$ .

6. Докажите, что у любого шестизначного числа меньше 2000 делителей.

7. На доске написано несколько натуральных чисел, удовлетворяющих условию: ни одно из чисел не делится на другое. Петя каждую минуту дописывает на доску наименьшее из натуральных чисел, при выписывании которого условие не нарушается. Докажите, что когда-нибудь Петя выпишет простое число.

8. На доске в лаборатории написаны два числа. Каждый день старший научный сотрудник Петя стирает с доски оба числа и пишет вместо них их среднее арифметическое и среднее гармоническое. Утром первого дня на доске были написаны числа 1 и 2. Найдите произведение чисел, записанных на доске вечером 1999-го дня. (Средним арифметическим двух чисел  $a$  и  $b$  называется число  $\frac{a+b}{2}$ , а средним гармоническим – число  $\frac{2}{\frac{1}{a} + \frac{1}{b}}$ ).

## Серия 9: Улучшаем показатели

**Определение.** Для натурального  $n$  обозначим за  $\sigma(n)$  сумму всех натуральных делителей числа  $n$ .

1.  $N + 1$  делится на 24. Докажите, что  $\sigma(N)$  делится на 24.

2. а) Докажите, что числа  $2^m - 1$  и  $2^n - 1$  взаимно просты тогда и только тогда, когда взаимно просты  $m$  и  $n$ .

б) Найдите  $(2^m - 1, 2^n - 1)$  при всех натуральных  $m$  и  $n$ .

3. Найдите все такие пары  $(a, p)$ , где  $a$  – натуральное число, а  $p$  – простое, что сумма остатков от деления числа  $a$  на  $p$ ,  $2p$ ,  $3p$  и  $4p$  равна  $a + p$ .

4. На квадратной доске  $n \times n$  стоит  $n - 1$  фишка. Докажите, что, переставляя строки и столбцы, можно поместить все фишки ниже главной диагонали.

5. На доске выписаны числа  $1, 2, \dots, 1000000$ . На каждом этапе одновременно стираются все числа, имеющие среди нестертых чисел ровно один делитель (например, на первом этапе стирается только число 1). Какие числа будут стерты на последнем этапе?

6. Назовём натуральное число *хорошим*, если оно представимо в виде суммы трёх натуральных чисел  $a < b < c$  таких, что  $c$  делится на  $b$  и  $b$  делится на  $a$ . Найдите наибольшее нехорошее число.

7. Какое наибольшее количество чисел можно выбрать из всех натуральных чисел от 1 до  $2^n$  так, чтобы для любых двух различных выбранных чисел  $x$  и  $y$  наибольшая степень 2, на которую делится  $x - y$ , имела чётный показатель?

8. При каких натуральных  $n$  можно разложить  $n(n - 1)/2$  карточек, пронумерованных последовательно натуральными числами от 1 до  $n(n - 1)/2$ , в  $n$

стопок таким образом, чтобы в любых двух стопках было по одной карточке с последовательными номерами, или с номерами 1 и  $n(n-1)/2$ ?

### Серия 10: с буквой $\sigma$

1. Даны два целых положительных числа  $m$  и  $n$ . Выписываются все различные делители числа  $m$  — числа  $a, b, \dots, k$  — и все различные делители числа  $n$  — числа  $s, t, \dots, z$ . Оказалось, что  $a + b + \dots + k = s + t + \dots + z$  и  $\frac{1}{a} + \frac{1}{b} + \dots + \frac{1}{k} = \frac{1}{s} + \frac{1}{t} + \dots + \frac{1}{z}$ . Докажите, что  $m = n$ .

2. Докажите, что при любом натуральном  $n$  выполнено неравенство  $\sqrt{n} \leq \frac{\sigma(n)}{d(n)} < \frac{3}{4}n$ .

3. Докажите, что совершенное число (т.е. число, равное сумме всех своих натуральных делителей, за исключением его самого) не может быть точным квадратом.

4. Докажите, что нечётное совершенное число не может давать остаток 3 при делении на 4.

5. а)  $2^n - 2$  делится на  $n$ . Докажите, что  $2^{2^n-1} - 2$  делится на  $2^n - 1$ .

б) последовательность натуральных чисел  $\{a_k\}$  определена рекуррентно:  $a_1$  — простое,  $a_k = 2^{a_{k-1}} - 1$ . Докажите, что  $2^{a_k} - 2$  делится на  $a_k$  при всех натуральных  $k$ .

6. Дано простое число  $p$  и такие целые числа  $a, b, c, d, e$ , что числа  $a^2 - b, a^3 - c, c^5 - d, b^7 - e$  делятся на  $p$ . Докажите, что и число  $ae - d$  делится на  $p$ .

7. Правительство решило приватизировать гражданскую авиацию. Каждые два из  $n$  городов страны были соединены прямой авиалинией; все эти авиалинии предполагалось передать в частные руки. Народный хурал, заподозрив правительство в распродаже Родины, постановил, что для каждого трех городов хотя бы две из трех авиалиний, соединяющих эти города, должны быть проданы одной и той же компании. Какое наибольшее число компаний правительству удастся привлечь к участию в приватизации?

8. В некоторой компании более 10 человек, и у каждого количество знакомых делится на 10. Докажите, что есть хотя бы 11 человек с одинаковым количеством знакомых.

### Серия 11: с чем у нас плохо?

1. Остап Бендер организовал в городе Фуксе раздачу слонов населению. На раздачу явилось 28 членов профсоюза и 37 не членов, причем Остап раздавал слонов поровну всем членам профсоюза и поровну не членам. Оказалось, что существует лишь один способ такой раздачи (так, чтобы раздать всех слонов). Какое наибольшее число слонов могло быть у О.Бендера?

2. Докажите, что простых чисел вида  $4k + 3$  бесконечно много.

3. В лифте действуют две кнопки: одна, позволяющая подниматься на  $a$  этажей вверх, и другая, позволяющая спускаться на  $b$  этажей вниз. Мы говорим, что лифтом *можно пользоваться*, если с его помощью можно попасть с любого этажа на любой другой.

а) Докажите, что при  $(a, b) > 1$  пользоваться лифтом нельзя.

б) Докажите, что при  $(a, b) = 1$  существует такое  $N$  (зависящее от  $a$  и  $b$ ), что в доме высотой по крайней мере в  $N$  этажей пользоваться лифтом можно.

в) Пусть  $(a, b) = 1$ . Найдите наименьшее  $N$ , для которого имеет место утверждение пункта б).

4. Решите в целых числах уравнение  $x^n = y(y + 1)$ .

5. Пусть  $(a, b) = d$ ,  $(a', b') = d'$ . Докажите, что  $(aa', ab', ba', bb') = dd'$ .

6. Натуральные числа  $x$  и  $y$  таковы, что  $x^2 + y^2$  делится на  $xy$ . Докажите, что  $x = y$ .

7. Островное государство расположено на 100 островах, соединенных мостами, причем некоторые острова соединены мостом и с материком. Известно, что с каждого острова можно проехать на каждый (возможно, через другие острова). В целях повышения безопасности движения на всех мостах было введено одностороннее движение. Оказалось, что с каждого острова можно уехать только по одному мосту и что хотя бы с одного острова можно уехать на материк. Докажите, что с каждого острова можно доехать до материка, причем по единственному маршруту.

8. В некоторой стране есть столица и еще 100 городов. Некоторые города (в том числе столица) соединены дорогами с односторонним движением. Из каждого нестоличного города выходит 20 дорог, и в каждый такой город входит 21 дорога. Докажите, что в столицу нельзя проехать ни из одного города.

### Серия 12: Степени вхождения и кое-что новое.

1.  $a, b, c$  – натуральные числа такие, что  $a^3$  делится на  $b$ ,  $b^3$  делится на  $c$ , а  $c^3$  делится на  $a$ . Докажите, что  $(a + b + c)^{13}$  делится на  $abc$ .

2. Нечетное простое число  $p$  и натуральные числа  $a$  и  $b$  таковы, что  $a^2 + b^2$  и  $a(a + b)^2$  делятся на  $p^4$ . Докажите, что  $a(a + b)$  тоже делится на  $p^4$ .

3. Натуральные числа  $m, n, k$  таковы, что число  $m^n$  делится на  $n^m$ , а число  $n^k$  делится на  $k^n$ . Докажите, что число  $m^k$  делится на  $k^m$ .

4. Сумма четырех натуральных чисел  $a, b, c, d$  – простое число  $p$ . Докажите, что  $ab - cd$  не делится на  $p$ .

5.  $a, b$  и  $n$  – фиксированные натуральные числа. Известно, что при любом натуральном  $k$  ( $k \neq b$ ) число  $a - k^n$  делится без остатка на число  $b - k$ . Докажите, что  $a = b^n$ .

6. Докажите, что уравнение  $x^2 + x + 1 = py$  имеет решение в целых числах  $(x, y)$  для бесконечного числа простых  $p$ .

7. Докажите, что для каждого простого  $p$  существуют такие целые  $x$  и  $y$ , что  $x^2 + y^2 + 1$  делится на  $p$ .

8. Написанное на доске число  $n$  можно заменить на одно из чисел  $2n - 4$ ,  $3n - 8$  или  $8 - n$ . Можно ли за несколько таких операций из числа 41 получить число, большее 10000000, но меньшее 10000020?

## 2 Вычеты

### 2.1 Сравнения по модулю: напоминание

В этом параграфе (в прочем и в дальнейших — тоже)  $m$  обозначает ненулевое целое число.

**Определение 2.1.** Пусть  $a, b$  — целые числа. Будем говорить, что  $a$  *сравнимо с  $b$  по модулю  $m$*  и писать  $a \equiv b \pmod{m}$  (или  $a \equiv_m b$ ), если  $a$  и  $b$  дают одинаковые остатки от деления на  $m$ .

**Предложение 2.2** (Переформулировка определения).  $a \equiv b \pmod{m}$  тогда и только тогда, когда  $(a - b) : m$ .

*Доказательство.* В одну сторону утверждение совсем очевидно:

$$a = mq_1 + r, \quad b = mq_2 + r, \quad 0 \leq r < m \implies a - b = m(q_1 - q_2) : m$$

Теперь докажем утверждение в другую сторону. Действительно, пусть  $(a - b) : m$ , тогда

$$a - b = mk, \quad k \in \mathbb{Z} \iff a = mk + b.$$

Пусть  $b = mq + r, 0 \leq r < m$  — деление с остатком. Тогда

$$a = m(k + q) + r, \quad 0 \leq r < m,$$

то есть остаток от деления  $a$  на  $m$  тоже равен  $r$ , что и требовалось.  $\square$

**Теорема 2.3.** Отношение сравнимости по модулю  $m$  ( $a \sim b \iff a \equiv_m b$ ) — отношение эквивалентности.

*Доказательство.* Докажем по очереди все три нужных свойства:

- (1) *Рефлексивность:* Действительно,  $(a - a) = 0 : m \implies a \equiv_m a$ .
- (2) *Симметричность:* Действительно, Пусть  $a \equiv_m b$ , тогда  $(a - b) : m$ , из чего следует, что  $(b - a) : m$ , то есть  $b \equiv_m a$ .
- (3) *Транзитивность:* Нам нужно доказать, что

$$\begin{cases} a \equiv_m b \\ b \equiv_m c \end{cases} \implies a \equiv_m c.$$

Это следует из свойств делимости:  $a \equiv_m b$  и  $b \equiv_m c$ , то есть  $(a - b) : m$  и  $(b - c) : m$  Тогда и разность чисел  $(a - b)$  и  $(b - c)$  делится на  $m$ :

$$((a - b) - (b - c)) : m \iff (a - c) : m,$$

что и требовалось.

□

Таким образом, все числа разбиваются на классы эквивалентности по отношению сравнимости.

**Определение 2.4.** Класс эквивалентности элемента  $a$  по отношению сравнимости по модулю  $m$  называют *вычетом числа  $a$  по модулю  $m$* .

*Замечание 2.5.* Нетрудно заметить, что остаток от деления  $a$  на  $m$  — наименьший неотрицательный представитель класса эквивалентности.

**Теорема 2.6** (Арифметические свойства сравнений). Сравнения по модулю  $m$  обладают следующими арифметическими свойствами:

(1) Пусть  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , Тогда:

$$a + c \equiv b + d \pmod{m}, \quad a - c \equiv b - d \pmod{m}, \quad a \cdot c \equiv b \cdot d \pmod{m}.$$

(2) Пусть  $a \equiv b \pmod{m}$ . Тогда для любого натурального  $k$

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

(3) Пусть  $a \equiv b \pmod{m}$ . Тогда для любого целого  $k$

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

*Замечание 2.7.* Эти свойства показывают, что со сравнениями можно работать практически также, как с обычными равенствами чисел, например, из первого свойства следует, что можно переносить число в другую часть равенства с изменением знака:

$$a \equiv b \pmod{m} \implies a - b \equiv 0 \pmod{m}.$$

**Предложение 2.8.** Предположим, что  $ka \equiv kb \pmod{m}$  и  $(k, m) = 1$ . Тогда  $a \equiv b \pmod{m}$ . Иными словами, сравнение можно сокращать на сомножитель, взаимно простой с модулем.

*Доказательство.* В самом деле,

$$ka \equiv kb \pmod{m} \iff k(a - b) \equiv 0 \pmod{m},$$

а так как  $(k, m) = 1$ , это влечёт  $(a - b) \equiv 0 \pmod{m}$ , что и требовалось. □

**Предложение 2.9.** Если  $a \equiv b \pmod{m}$ , то  $(a, m) = (b, m)$ .

Действительно, так как  $a = qt + b$ , достаточно вспомнить алгоритм Евклида. Из этого также можно извлечь такое наблюдение

*У всех чисел с данным остатком от деления один и тот же НОД с  $m$ . В частности, либо они все не взаимно просты с  $m$ , либо они все взаимно просты с  $m$ .*

## 2.2 Полная и приведённая системы вычетов, их приложения.

Итак, мы вспомнили, что когда нам важно не само целое число  $n$ , а лишь его остаток по некоторому модулю  $m$ , то мы можем говорить о **вычете** числа  $n$  или **классе вычетов**, в котором лежит число  $n$ . Формально говоря, мы говорим о *классе эквивалентности* числа по отношению сравнимости по модулю  $m$ .

**Пример 2.10.** Например, числа  $\dots, -15, -7, 1, 9, \dots$  составляют один класс вычетов  $(\bmod 8)$ . А целиком этот класс можно описать как  $[1]_8 = \{8k + 1 \mid k \in \mathbb{Z}\}$ .

В этом параграфе мы познакомимся с двумя крайне важными понятиями, определяющимися ниже.

**Определение 2.11.** *Полная система вычетов  $\bmod m$*  — это набор чисел, дающих все всевозможные остатки от деления на  $m$  (которых, напомним,  $m$  штук).

**Пример 2.12.** Например, числа  $5, 10, -1, 12$  образуют полную систему вычетов  $(\bmod 4)$ . А набор  $0, 2, 2^2, 2^3, 2^4$  образует полную систему вычетов  $\bmod 5$ .

Ну и вообще, *любые  $m$  чисел, попарно не сравнимых друг с другом по модулю  $m$  образуют полную систему вычетов по модулю  $m$* , так как принадлежат разным классам вычетов и их количество равно количеству классов.

Еще, как мы видели, в вычислениях часто бывает полезным рассматривать маленькие по модулю представители классов вычетов (чтоб считать было проще). Так вот, набор целых чисел, удовлетворяющих неравенствам  $-\frac{m}{2} < x < \frac{m}{2}$  тоже всегда образует полную систему вычетов.

**Определение 2.13.** *Приведённая система вычетов  $\bmod m$*  — это набор чисел (вычетов), дающих **все** всевозможные остатки, взаимно простые с  $m$  (каждый по разу).

**Пример 2.14.** Приведём несколько примеров

- $1, 2$  — приведённая система вычетов  $\bmod 3$ .
- $1, 3$  — приведённая система вычетов  $\bmod 4$ .
- $1, 2, 3, 4$  — приведённая система вычетов  $\bmod 5$ .
- $1, 5$  — приведённая система вычетов  $\bmod 6$ .
- $1, 2, 3, 4, 5, 6$  — приведённая система вычетов  $\bmod 7$ .
- $1, 3, 5, 7$  — приведённая система вычетов  $\bmod 8$ .

Пользуясь наблюдением из конца предыдущего параграфа мы видим, что в приведённую систему вычетов мы выбираем те вычеты, в которых все представители взаимно просты с  $m$ .

**Теорема 2.15.** Если  $a_1, \dots, a_m$  — полная система вычетов  $\pmod{m}$  и  $(k, m) = 1$ , то  $ka_1, \dots, ka_m$  — тоже полная система вычетов  $\pmod{m}$ .

*Доказательство.* Предположим, противное:  $ka_i \equiv ka_j \pmod{m}$  для некоторых  $i, j$ . Так как  $(k, m) = 1$ , мы можем сократить это сравнение на  $k$  и получить, что  $a_i \equiv a_j \pmod{m}$ . Это противоречит тому, что  $\{a_1, \dots, a_m\}$  — полная система вычетов.  $\square$

*Замечание 2.16.* Полезно понимать, что смысл теоремы 2.15 в следующем: она утверждает, что если  $(k, m) = 1$ , то отображение домножения вычетов на  $k$  — биекция:

$$\varphi: \mathbb{Z}_m \rightarrow \mathbb{Z}_m, \quad \varphi(a) = k \cdot a.$$

При помощи этого достаточно простого утверждения мы докажем малую теорему Ферма. Это доказательство — лишь одна из иллюстраций важности трюка с домножением полной/приведённой системы вычетов на вычет.

**Теорема 2.17** (Малая теорема Ферма). Для целого  $a$  не кратного простому  $p$  выполнено сравнение  $a^{p-1} \equiv 1 \pmod{p}$ .

*Доказательство.* Рассмотрим самую очевидную полную систему вычетов по модулю  $p$ :  $0, 1, 2, \dots, p-1$ .

Так как  $(a, p) = 1$ , по теореме 2.15  $a \cdot 0, a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)$  — также полная система вычетов  $\pmod{p}$ .

Тогда если мы перемножим все из них кроме нуля, получится число, сравнимое с произведением всех ненулевых остатков  $\pmod{p}$ :

$$(a \cdot 1) \cdot (a \cdot 2) \cdot (a \cdot 3) \cdot \dots \cdot (a \cdot (p-1)) \equiv 1 \cdot 2 \cdot \dots \cdot (p-1) = (p-1)! \pmod{p}.$$

Значит, мы имеем сравнение  $a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$ . Сокращая его на  $(p-1)!$ , взаимно простое с модулем, мы получаем  $a^{p-1} \equiv_p 1$ , что и хотели.  $\square$

А что получится, если проделать такой же трюк, но для приведённых систем вычетов? Опять же, сначала давайте докажем вспомогательный результат.

**Теорема 2.18.** Пусть  $a_1, \dots, a_n$  — приведённая система вычетов  $\pmod{m}$ , а  $k$  взаимно просто с  $m$ . Тогда  $k \cdot a_1, k \cdot a_2, \dots, k \cdot a_n$  — тоже приведённая система вычетов  $\pmod{m}$ .

*Доказательство.* Действительно, все эти числа всё ещё взаимно просты с  $m$  и дают разные остатки  $\pmod{m}$ . Значит, так как их ровно  $n$  штук, они дают **все** разные остатки, взаимнопростые с  $m$  по разу.  $\square$

Теперь посмотрим на главное приложение этой простой теоремы.

**Определение 2.19.** Количество чисел от 1 до  $n$ , взаимно простых с  $n$  мы будем называть **функцией Эйлера** от числа  $n$  и обозначать  $\varphi(n)$ .

**Вопрос к детям.** Откуда и куда действует функция Эйлера?

**Пример 2.20.** Ясно, что  $\varphi(1) = 1$ ,  $\varphi(2) = 1$ ,  $\varphi(3) = 2$ ,  $\varphi(5) = 4$ ,  $\varphi(6) = 2$ ,  $\varphi(15) = 8$ . **Важные наблюдения:** Для простого  $p$  мы имеем  $\varphi(p) = p - 1$  и  $\varphi(p^k) = p^k - p^{k-1}$ .

Теперь мы можем существенно обобщить малую теорему Ферма.

**Теорема 2.21** (Теорема Эйлера). Если  $(a, n) = 1$ , то  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

*Доказательство.* Возьмём любую приведённую системы вычетов по модулю  $n$ , обозначим её за  $a_1, a_2, \dots, a_{\varphi(n)}$ . Тогда по теореме 2.18 набор  $a \cdot a_1, a \cdot a_2, \dots, a \cdot a_{\varphi(n)}$  снова будет приведённой системой вычетов. Тогда мы имеем

$$(a \cdot a_1) \cdot (a \cdot a_2) \cdot \dots \cdot (a \cdot a_{\varphi(n)}) \equiv a_1 \cdot a_2 \cdot \dots \cdot a_{\varphi(n)} \pmod{n} \implies a^{\varphi(n)} \equiv 1 \pmod{n}.$$

□

## 2.3 Китайская теорема об остатках

Начнём с нескольких мотивирующих примером. Часто в задачах возникает так, что нам нужно подобрать число, которые даёт нужные остатки по целому набору модулей.

**Пример 2.22.** Рассмотрим, например, систему сравнений

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{4} \end{cases}.$$

Подобрать такое число легко — например, подходит 10. Также нетрудно сообразить, что если  $a \equiv 10 \pmod{12}$ , то оно также подойдёт (так как из сравнения по модулю 12 следуют сравнения по модулям 3 и 4).

А вот для системы

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

подобрать ответ уже не так легко. Как в принципе решать такую задачу?

Стандартная идея такая: выписать вычеты, подходящие под первое условие (т.е. 3, 8, 13, 18, 23, ...), а потом вычеркнуть из них те, которые не подходят под второе. Но, в таком случае придётся перебрать от 1 до 45 9 таких чисел. Быстрее поступить иначе — выписать вычеты, подходящие под второе условие (их поменьше: 5 штук 1, 10, 19, 28, 47) и после найти среди них нужный класс  $x \equiv 28 \pmod{45}$ .

**Пример 2.23.** Посмотрим теперь еще на одну систему:

$$\begin{cases} x \equiv 2 \pmod{24} \\ x \equiv 1 \pmod{15}. \end{cases}$$

Тут мы действуя как в предыдущем примере к успеху не придём. Причина проста: из обоих сравнений следует сравнение по модулю 3 и мы получаем противоречие.

Сейчас мы сформулируем основной инструмент для работы с описанными выше ситуациями.

**Теорема 2.24** (Китайская теорема об остатках, Сунь-Цзы (3-5 век н.э.)). Пусть  $(m_1, m_2) = 1$ . Тогда любая система сравнений

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

имеет решение, причём это решение однозначно определено  $\pmod{m_1 m_2}$  (т.е. представляет один класс вычетов  $\pmod{m_1 m_2}$ ).

*Доказательство. Единственность.* Предположим противное, т.е., что у нас есть два решения

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \quad \text{и} \quad \begin{cases} y \equiv a_1 \pmod{m_1} \\ y \equiv a_2 \pmod{m_2} \end{cases}$$

Тогда  $x \equiv y \pmod{m_1, m_2}$ , откуда

$$\begin{cases} (x - y) : m_1 \\ (x - y) : m_2 \end{cases} \implies (x - y) : m_1 m_2 \iff x \equiv y \pmod{m_1 m_2}.$$

**Существование.**

Выпишем все остатки от 1 до  $m_1 m_2$  в табличку  $m_2 \times m_1$ .

1	2	3	...	$m_1$
$m_1 + 1$	$m_1 + 2$	$m_1 + 3$	...	$2m_1$
$2m_1 + 1$	$2m_1 + 2$	$2m_1 + 3$	...	$3m_1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(m_2 - 1)m_1 + 1$	$(m_2 - 1)m_1 + 2$	$(m_2 - 1)m_1 + 3$	...	$m_1 m_2$

Рассмотрим произвольный столбец, он состоит из чисел  $k, m_1 + k, 2m_1 + k, \dots, (m_2 - 1)m_1$ . Покажем, что это полная система вычетов  $\pmod{m_2}$ . Действительно, возьмём полную систему вычетов  $0, 1, \dots, m_2 - 1$ , домножим её на  $m_1$  (взаимно простое

с модулем), тогда по теореме 2.15 она останется полной. После этого сдвинем все числа в ней на  $k$ , так мы получим полную систему, записанную в  $k$ -м столбце.

Теперь заметим, что числа в первом столбце  $1 \pmod{m_1}$ , во втором  $2 \pmod{m_1}$  и так далее. Значит, все числа, сравнимые с  $a_1 \pmod{m_1}$ , заполняют какой-то один столбец, а так как (как мы показали выше), в нём написана полная система вычетов  $\pmod{m_2}$ , в нём найдётся число, сравнимое с  $a_2 \pmod{m_2}$ . □

### Комбинаторное доказательство существования.

Выпишем все числа от 1 до  $m_1 m_2$  и каждому из них сопоставим пару чисел: остаток от деления на  $m_1$  и остаток от деления на  $m_2$ , то есть рассмотрим отображение

$$a \pmod{m_1 m_2} \mapsto (a \pmod{m_1}, a \pmod{m_2}).$$

Например, для  $m_1 = 2, m_2 = 3$  мы получаем

$$1 \mapsto (1, 1), \quad 2 \mapsto (0, 2), \quad 3 \mapsto (1, 0), \quad 4 \mapsto (0, 1), \quad 5 \mapsto (1, 2), \quad 6 \mapsto (0, 0).$$

Заметим, что двум разным числам будут сопоставлены две разные пары остатков (иначе это противоречит уже доказанной выше единственности). Тогда всем  $m_1 m_2$  числам будут сопоставлено  $m_1 m_2$  разных пар остатков. Но, общее количество всевозможных пар как раз таково. Значит, каждая пара действительно была чему-то сопоставлена, а это ровно то, что требовалось доказать.

**Следствие 2.25.** Пусть  $m_1, \dots, m_k$  попарно взаимно просты. Тогда система

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

имеет решение, причём оно однозначно определено  $\pmod{m_1 m_2 \dots m_k}$ .

*Доказательство.* Индукция по  $k$ , база  $k = 2$  уже разобрана в теореме 2.24.

**Переход**  $k \mapsto k + 1$ . Делается стандартно. □

## 2.4 Обратимые вычеты и теорема Вильсона

**Определение 2.26.** Вычет  $a \pmod{m}$  мы будем называть *обратимым* (по модулю  $m$ ), если существует такой вычет  $b \pmod{m}$ , что  $a \cdot b \equiv 1 \pmod{m}$ . Мы часто будем обозначать его как  $1/a$ .

**Теорема 2.27.** Вычет  $a \in \mathbb{Z}_m$  обратим тогда и только тогда, когда  $(a, m) = 1$ .

*Доказательство.* Сначала докажем импликацию ( $\implies$ ). В самом деле, если существует такой вычет  $b \in \mathbb{Z}_m$ , что  $ab \equiv 1 \pmod{m}$ . Тогда  $ab = mq + 1$ , но

$$\begin{cases} (a, m) \mid m \\ (a, m) \mid ab \end{cases} \implies (a, m) \mid ab - mq = 1 \implies (a, m) = 1.$$

Теперь докажем обратную импликацию. Рассмотрим приведённую систему вычетов по модулю  $m$ , обозначим её  $x_1, \dots, x_{\varphi(m)}$ . Так как  $(a, m) = 1$ , по лемме 2.18  $a \cdot x_1, \dots, a \cdot x_{\varphi(m)}$  тоже приведённая система вычетов. Так как в ней обязательно есть единица, мы получили, что для некоторого  $i$  мы имеем  $a \cdot x_i \equiv 1 \pmod{m}$ , что и требовалось.  $\square$

*Замечание 2.28.* Так мы видим, например, что элементы приведённой системы вычетов — это в точности все обратимые элементы  $\pmod{m}$ . В частности,

$$\varphi(m) = \text{количество обратимых элементов } \mathbb{Z}_m.$$

И, совсем в частности, мы видим, что по модулю простого  $p$  обратимы **все ненулевые вычеты**.

**Пример 2.29.**  $\frac{1}{2} \equiv 3 \pmod{5}$ , так как  $6 \equiv 2 \cdot 3 \equiv 1 \pmod{5}$ .  $\frac{1}{3} \equiv 5 \pmod{7}$ , так как  $15 = 3 \cdot 5 \equiv 1 \pmod{7}$ . И так далее.

**Важное упражнение.** С дробями по модулю можно делать все стандартные операции: складывать, умножать, сокращать и т.п., то есть:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} \equiv \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} \pmod{m}, \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} \equiv \frac{a_1 a_2}{b_1 b_2} \pmod{m},$$

как только все эти выражения определены. Кроме того, если вдруг  $a$  делится на  $b$ , то  $\frac{a}{b} \equiv \frac{a}{n} \pmod{m}$  (вдумайтесь в эту запись).

**Комментарий.** Условие про взаимную простоту тут по существу. Например, число  $p(n) = \frac{n(n+1)}{2}$  вообще всегда целое, но воспринимать его как дробь по модулю 2 нельзя! Действительно, к примеру,  $1 \equiv 3 \pmod{2}$ , но  $p(1) \not\equiv p(3) \pmod{2}$ .

**Теорема 2.30** (Вильсон, 1770г.). Для простого  $p$  справедливо сравнение

$$(p-1)! \equiv -1 \pmod{p}.$$

*Доказательство.* Заметим, что так как  $p$  простое, все ненулевые вычеты обратимы, а значит, если  $a \not\equiv \frac{1}{a} \pmod{p}$ , то мы можем сократить их в произведении (т.е. в  $(p-1)!$ ). Осталось разобраться с такими вычетами  $a \in \mathbb{Z}_p$ , для которых  $a \equiv \frac{1}{a} \pmod{p}$ . Домножая это сравнение на  $a$ , мы получаем

$$a^2 \equiv 1 \pmod{p} \implies (a-1)(a+1) \equiv 0 \pmod{p},$$

откуда по лемме Евклида  $a \equiv \pm 1 \pmod{p}$ . Значит, сравнению  $a \equiv \frac{1}{a} \pmod{p}$  удовлетворяют только 1 и  $-1$ , откуда мы видим, что

$$(p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod{p}.$$

$\square$

## 2.5 Линейное представление НОД

Начнём с напомним алгоритм Евклида для нахождения наибольшего общего делителя.

$$\begin{array}{ll}
 a = bq_1 + r_1 & (a, b) = (b, r_1) \\
 b = r_1q_2 + r_2 & (b, r_1) = (r_1, r_2) \\
 r_1 = r_2q_3 + r_3 & (r_1, r_2) = (r_2, r_3) \\
 \dots & \dots \\
 r_{n-2} = r_{n-1}q_n + r_n & (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) \\
 r_{n-1} \div r_n & (r_{n-1}, r_n) = r_n
 \end{array}$$

Из правого столбца видно, что алгоритм Евклида вычисляет именно НОД. Ясно, что алгоритм Евклида заканчивается, так как  $r_1 > r_2 > r_3 > \dots$

Оказывается, если запустить “обратный ход” алгоритма Евклида, мы сможем выразить  $a$  и  $b$  через их НОД:

**Теорема 2.31** (Клод Гаспар Баше де Мезириак<sup>1</sup>, примерно 1624г.). Для натуральных  $a$  и  $b$  существуют такие  $x, y \in \mathbb{Z}$ , что  $ax + by = d$ , где  $d = (a, b)$ .

*Доказательство.* Запишем алгоритм Евклида

$$\begin{array}{ll}
 a = bq_1 + r_1 & (a, b) = (b, r_1) \\
 b = r_1q_2 + r_2 & (b, r_1) = (r_1, r_2) \\
 r_1 = r_2q_3 + r_3 & (r_1, r_2) = (r_2, r_3) \\
 \dots & \dots \\
 r_{n-2} = r_{n-1}q_n + r_n & (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) \\
 r_{n-1} \div r_n & (r_{n-1}, r_n) = r_n
 \end{array}$$

Внимательно посмотрев на первую строчку легко видеть, что  $r_1$  сразу выражается в виде  $ax + by$ :  $r_1 = a \cdot 1 - b \cdot q_1$ ,  $x = 1, y = -q_1$ .

Далее, из второй строчки  $r_2$  мы можем выразить через  $b$  и  $r_1$  и подставляя сюда выражение для  $r_1$  так мы выразим  $r_2$  через  $a$  и  $b$ .

Продолжая в том же духе, по индукции имеем нужное (доходя до  $r_n = d$ ).  $\square$

**Следствие 2.32.** Пусть  $a, b \in \mathbb{N}$ . Число  $c$  представимо в виде  $ax + by$  для некоторых целых  $x, y \in \mathbb{Z}$  тогда и только тогда, когда  $(a, b) \mid c$ .

---

<sup>1</sup>В англоязычных источниках называют леммой Безу, но Безу вообще говоря доказал это для многочленов. А для чисел это первым заметил Клод Гаспар Баше сильно раньше (правда, только для взаимно простых, но разница не велика).

**Пример 2.33.** Давайте сделаем это для 107 и 37:

$$107 = 37 \cdot 2 + 33 \quad 33 = 107 - 37 \cdot 2$$

$$37 = 33 \cdot 1 + 4 \quad 4 = 37 - 33 = 37 - (107 - 37 \cdot 2) = 37 \cdot 3 - 107$$

$$33 = 4 \cdot 8 + 1 \quad 1 = 33 - 4 \cdot 8 = (107 - 37 \cdot 2) - (37 \cdot 3 - 107) \cdot 8 = 107 \cdot 9 - 37 \cdot 26.$$

Итого, мы получили  $1 = 107 \cdot 9 - 37 \cdot 26$ .

Запись  $d = ax + by$  мы будем называть *линейным представлением наибольшего общего делителя чисел  $a$  и  $b$* .

### Нахождение обратного по модулю

В качестве первого приложения линейного представления НОД рассмотрим нахождение обратного по модулю. Мы обсуждали, что обратный вычит  $a$  по модулю  $m$  существует тогда и только тогда, когда  $(a, m) = 1$ . Соответственно, в этом в случае по теореме 2.31 существуют  $x, y \in \mathbb{Z}$  такие что

$$ax + my = 1 \implies ax \equiv 1 \pmod{m},$$

то есть в качестве обратного вычета к  $a$  по модулю  $m$  подходит  $x$  (который мы можем найти явно при помощи алгоритма Евклида).

## 2.6 Линейные сравнения

Под линейным сравнением мы будем понимать уравнение

$$ax \equiv b \pmod{m}, \tag{1}$$

где  $x$  — переменная,  $a, b \in \mathbb{Z}$ , а  $m$  — фиксированный модуль. Отметим отдельно, что под решением такого сравнения мы будем понимать не какое-то конкретное целое число, а вычит  $\pmod{m}$ .

**Пример 2.34.** Например, решением линейного сравнения  $5x \equiv 3 \pmod{7}$  является  $2 \pmod{7}$ .

На самом деле, такие сравнения мы уже научились решать в предыдущих двух параграфах. А именно, что бы мы делали, если бы мы решали над рациональными числами уравнение  $ax = b$ ? Наверное, мы бы сказали, что при  $a \neq 0$  сразу видим, что  $x = b/a$ , а при  $a = 0$  возможны два случая: если  $b = 0$ , то в качестве  $x$  годится что угодно, а если  $b \neq 0$ , то решений нет.

По модулю  $m$  ситуация устроена примерно также. Во-первых отметим, что необходимым условием разрешимости такого сравнения является  $b : (a, m)$ . Действительно, если решение существует (обозначим его за  $x_0$ ), то

$$ax_0 \equiv b \pmod{m} \implies b = ax_0 - qm : (a, m).$$

Отсюда мы получаем, что в случае  $b \not\equiv (a, m)$  сравнение 1 не имеет решений. Теперь заметим, что если  $(a, m) = 1$ , то по теореме 2.27 вычит  $a$  обратим, и тогда мы можем сказать, что

$$x \equiv \frac{b}{a} \pmod{m}, \text{ где } \frac{b}{a} = b \cdot \frac{1}{a} \pmod{m}.$$

Отметим также, что этот  $x$  мы можем **найти явно**, пользуясь линейным представлением НОД и наблюдением в конце предыдущего параграфа.

Теперь, предположим, что  $(a, m) \neq 1$ , но  $b \equiv (a, m)$ . В этом случае запишем

$$a = a_0(a, m), \quad m = m_0(a, m), \quad b = b_0(a, m),$$

перейдём к сравнению  $a_0 \equiv b_0 \pmod{m_0}$  (поделив на  $(a, m)$ ) и после, так как теперь  $(a_0, m_0) = \left(\frac{a}{(a, m)}, \frac{m}{(a, m)}\right) = \frac{1}{(a, m)}(a, m) = 1$  мы можем проделать то, что уже обсуждали выше.

Итак, рассуждениями выше мы доказали следующую теорему.

**Теорема 2.35.** Линейное сравнение  $ax \equiv b \pmod{m}$  разрешимо тогда и только тогда, когда  $(a, m) \mid b$ .

## 2.7 Линейные диофантовы уравнения

Напомним, что

**Определение 2.36.** Диофантовыми уравнениями называют уравнения в целых числах (т.е. те, в которых нас интересуют только *целочисленные* решения).

С такими задачами мы уже неоднократно сталкивались в сериях. В этом параграфе мы полностью научимся решать один из (простейших) классов таких уравнений. А именно, мы научимся решать *линейные диофантовы уравнения*

$$ax + by = c, \quad a, b, c \in \mathbb{Z}, \quad x, y \text{ — переменные.} \quad (2)$$

**Пример 2.37.** Например, уравнение  $3x + 6y = 17$  очевидно не имеет решений, так как левая часть делится на 3, а правая — нет.

Из примеры выше легко получить необходимое условие разрешимости уравнения (2). А именно, видно, что левая его часть делится, на  $(a, b)$ , откуда ясно, что должна делиться и правая (тут мы дословно повторяем рассуждение следствия 2.32). С другой стороны, если  $(a, b) \mid c$ , то для нахождения какого-нибудь одного решения  $(x_0, y_0)$  достаточно написать алгоритм Евклида и найти линейное представление  $(a, b)$ .

**Наблюдение.** Пусть  $(x_0, y_0)$  — какое-то решение уравнения (2). Заметим, что в таком случае  $(x_0 + b, y_0 - a)$  также является решением, так как

$$a(x_0 + b) + b(y_0 - a) = ax_0 + ab + by_0 - ab = ax_0 + by_0 = c.$$

Ну и вообще, ровно из тех же соображений решением будет всякая пара  $(x_0 + k \cdot b, y_0 - k \cdot a)$ , где  $k$  — произвольное целое.

Теперь наконец перейдём к общей теории.

**Теорема 2.38.** Предположим, что  $(a, b) = 1$ . Тогда для любого  $c \in \mathbb{Z}$  уравнение  $ax + by = c$  разрешимо, причём решений бесконечно много и все они имеют вид  $(x_0 + k \cdot b, y_0 - k \cdot a)$ , где  $(x_0, y_0)$  — какое-то фиксированное решение.

*Доказательство.* Нам осталось доказать, что все решения имеют такой вид. Предположим, что  $(x_1, y_1)$  — решение уравнения. Тогда

$$ax_0 + by_0 = ax_1 + by_1 \iff a(x_1 - x_0) = b(y_0 - y_1) \implies a(x_1 - x_0) : b,$$

откуда, так как  $(a, b) = 1$ , мы и имеем  $(x_1 - x_0) : b$ , то есть  $x_1 = x_0 + k \cdot b$  для некоторого  $k \in \mathbb{Z}$ . Теперь подставим это в тождество выше:

$$b(y_0 - y_1) = a \cdot kb \implies y_1 = y_0 - k \cdot a,$$

что и требовалось. □

Отметим, что в случае, когда  $c : (a, b)$ , но  $(a, b) \neq 1$  нужно лишь поделить на НОД и свести ситуацию к случаю теоремы 2.38.

## 3 Мультипликативные функции

**Определение 3.1.** Функция  $f: \mathbb{N} \rightarrow \mathbb{R}$  называется *мультипликативной*, если

$$\forall a, b \quad (a, b) = 1 \implies f(ab) = f(a)f(b)$$

В следующих нескольких параграфах мы изучим важнейшие примеры таких функций в арифметике, а также некоторые общие свойства мультипликативных арифметических функций. Начнём мы с уже давно знакомых нам примеров.

### 3.1 Сумма делителей и количество делителей

**Определение 3.2.** Для натурального  $n$  обозначим через  $d(n)$  количество его натуральных делителей (считая 1 и  $n$ ).

**Предложение 3.3.** Если  $n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$  — каноническое разложение числа  $n$ , то

$$d(n) = (k_1 + 1) \cdot (k_2 + 1) \cdot \dots \cdot (k_s + 1).$$

*Доказательство.* В самом деле, в каждый делитель  $n$  входят те же простые, что и в  $n$ , а для каждого  $p_i$  у нас ровно  $k_i + 1$  вариантов выбрать, в какой степени мы его берём (это числа  $0, 1, \dots, k_i$ ). □

Следующая лемма очевидно следует из основной теоремы арифметики.

**Лемма 3.4.** Пусть  $(a, b) = 1$ . Тогда любой делитель  $ab$  однозначно раскладывается в произведение двух множителей, первый из которых — делитель  $a$ , а второй — делитель  $b$ .

**Теорема 3.5.** Функция  $d(n)$  мультипликативна.

*Доказательство.* Выпишем все  $d(a)$  делителей числа  $a$ :  $x_1, \dots, x_{d(a)}$  и все  $d(b)$  делителей числа  $b$ :  $y_1, \dots, y_{d(b)}$ . Тогда по лемме 3.4 все делители  $ab$  выглядят как

$$\begin{array}{ccccccccc} x_1y_1 & x_1y_2 & x_1y_3 & \dots & x_1y_{d(b)} \\ x_2y_1 & x_2y_2 & x_2y_3 & \dots & x_2y_{d(b)} \\ x_3y_1 & x_3y_2 & x_3y_3 & \dots & x_3y_{d(b)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_{d(a)}y_1 & x_{d(a)}y_2 & x_{d(a)}y_3 & \dots & x_{d(a)}y_{d(b)} \end{array}$$

Заметим, что в этой таблице каждый делитель встречается ровно один раз, значит их ровно  $d(a) \cdot d(b)$  штук.  $\square$

**Следствие 3.6.** Отсюда еще раз можно получить формулу для количества делителей, пользуясь тем, что для простого  $p$  очевидно, что  $d(p^n) = n + 1$  и мультипликативностью.

**Определение 3.7.** Для натурального  $n$  обозначим через  $\sigma(n)$  сумму всех его натуральных делителей (считая 1 и  $n$ ).

**Теорема 3.8.** Функция  $\sigma$  мультипликативна.

*Доказательство.* Выпишем все  $d(a) = n$  делителей числа  $a$ :  $x_1, \dots, x_n$  и все  $d(b) = m$  делителей числа  $b$ :  $y_1, \dots, y_m$ . Тогда  $\sigma(a) = x_1 + \dots + x_n$ ,  $\sigma(b) = y_1 + \dots + y_m$ , откуда

$$\sigma(a)\sigma(b) = (x_1 + \dots + x_n)(y_1 + \dots + y_m) = x_1y_1 + x_1y_2 + \dots + x_ny_1 + \dots + x_ny_m.$$

Остаётся заметить, что по лемме 3.4 в сумме в правой части равенства выписаны в точности все делители  $ab$  (см. еще раз табличку в теореме 3.5).  $\square$

В качестве следствия получаем удобную формулу для  $\sigma(n)$ .

**Следствие 3.9.** Если  $n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$  — каноническое разложение числа  $n$ , то

$$\sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{k_1}) \cdot \dots \cdot (1 + p_s + p_s^2 + \dots + p_s^{k_s}) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_s^{k_s+1} - 1}{p_s - 1}.$$

*Доказательство.* Заметим, что для  $n = p^k$  тривиальным образом

$$\sigma(p^\ell) = 1 + p + p^2 + \dots + p^\ell.$$

Тогда для  $n = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$  мы получаем первую формулу просто по мультипликативности. Вторая же формула следует из следующей леммы.

**Лемма 3.10.** Для  $x \neq 1$  и  $k \in \mathbb{N}$  справедлива формула

$$1 + x + x^2 + \dots + x^k = \frac{x^{k+1} - 1}{x - 1}.$$

*Доказательство леммы.* Обозначим  $S = 1 + x + \dots + x^k$ , тогда

$$xS - S = x(1 + x + \dots + x^k) - (1 + x + \dots + x^k) = x^{k+1} - 1 = S(x - 1),$$

откуда имеем нужное. □

□

## 3.2 Функция Эйлера

**Теорема 3.11.** Функция Эйлера  $\varphi(n)$  мультипликативна.

*Доказательство.* По Китайской теореме об остатках (так как  $(m, n) = 1$ ) у нас есть **биекция** остатков по модулю  $mn$  и пар остатков  $(\text{mod } m, \text{mod } n)$ , которая посылает  $c \text{ mod } mn$  в пару  $(a, b)$  таких вычетов, что

$$\begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{n} \end{cases}.$$

Заметим, что тогда если  $(a, m) = 1$ , то и  $(c, m) = 1$  (так как они сравнимы) и аналогично для  $b$ . Значит, наша биекция даёт нам биекцию на приведённых системах вычетов, откуда

$$\varphi(mn) = \varphi(m)\varphi(n).$$

□

Пользуясь мультипликативностью, мы стандартным способом получаем формулу для функции Эйлера:

**Следствие 3.12.** а) Для  $n = p^k$  мы имеем  $\varphi(n) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$  (каждое  $p$ -е число делится на  $p$  и не взаимно просто с  $p$  соответственно).

б) Для  $n = p_1^{k_1} p_2^{k_2} \cdot \dots \cdot p_s^{k_s}$  мы имеем

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \dots \cdot (p_s^{k_s} - p_s^{k_s-1}).$$

Теперь вынесем в последней формуле из каждой скобки множитель  $p_j^{k_j}$ , получится

$$\varphi(n) = \underbrace{p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_s^{k_s}}_{=n} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_s}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

### 3.3 Показатель числа по модулю

Из теоремы Эйлера 2.21 мы знаем, что если  $(a, m) = 1$ , то

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

Но для некоторых  $a$  сравнение  $a^d \equiv 1 \pmod{m}$  может выполняться и при  $d < \varphi(m)$ . Например,  $(-1)^2 \equiv 1 \pmod{m}$  всегда.

**Определение 3.13.** Наименьшее натуральное число  $d$ , для которого  $a^d \equiv 1 \pmod{m}$  называют *показателем* числа  $a$  по модулю  $m$ . Обозначать такое  $d$  мы будем  $\text{ord}_m(a)$ .

**Лемма 3.14.** Пусть  $d$  — показатель числа  $a$  по модулю  $m$ . Тогда  $a^k \equiv 1 \pmod{m}$  тогда и только тогда, когда  $k$  делится на  $d$ . В частности,  $\varphi(m) : d$ .

*Доказательство.* Предположим, что  $a^k \equiv 1 \pmod{m}$ . Поделим  $k$  на  $d$  с остатком:  $k = qd + r$ ,  $0 \leq r < d$ . Тогда

$$a^k = a^{qd+r} = (a^d)^q a^r \equiv a^r \pmod{m}.$$

Так как  $d$  — наименьшее натуральное число с условием  $a^d \equiv_m 1$ , а  $r < d$ , отсюда  $r = 0$ . Значит,  $d \mid k$ , как мы и хотели.  $\square$

**Следствие 3.15.** Если  $(a, m) = 1$  и  $u, v$  удовлетворяют сравнению  $a^u \equiv a^v \pmod{m}$ , то  $u \equiv v \pmod{d}$ , где  $d$  — показатель числа  $a$  по модулю  $m$ .

*Доказательство.* Не умаляя общности,  $v > u$ . Так как  $(a, m) = 1$ , мы можем сократить сравнение на  $a^u$ :

$$a^u \equiv a^v \pmod{m} \implies a^{u-v} \equiv 1 \pmod{m},$$

откуда по лемме 3.14  $d \mid u - v \implies u \equiv v \pmod{m}$ .  $\square$

### 3.4 Сумматоры мультипликативных функций

**Определение 3.16.** Функции  $f: \mathbb{N} \rightarrow \mathbb{R}$  называют *арифметическими*.

Так как мы работаем только с такими, это слово мы будем иногда опускать.

**Определение 3.17.** Пусть  $f$  — арифметическая функция. Тогда её *сумматорной функцией* мы будем называть

$$F(n) = \sum_{d \mid n} f(d).$$

**Пример 3.18.** Например, для крайне интересной арифметической функции  $f(n) = 1$  мы имеем

$$F(n) = \sum_{d|n} 1 = d(n),$$

а для функции  $f(n) = n$  мы имеем

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

**Предложение 3.19.** Если  $f$  мультипликативна, то её сумматорная функция  $F$  также мультипликативна.

*Доказательство. Детское.* Пусть  $(a, b) = 1$ . Пусть  $x_1, \dots, x_n$  — делители  $a$ , а  $y_1, \dots, y_m$  — делители  $b$ ,  $(x_i, y_j) = 1$  для всех  $i, j$ . Тогда

$$\begin{aligned} F(a)F(b) &= (f(x_1) + f(x_2) + \dots + f(x_n))(f(y_1) + f(y_2) + \dots + f(y_m)) = \\ &= f(x_1)f(y_1) + f(x_1)f(y_2) + \dots + f(x_1)f(y_m) + \dots + f(x_n)f(y_1) + \dots + f(x_n)f(y_m) = f(x_1y_1) + f(x_1y_2) + \dots + f(x_ny_m) = F(ab). \end{aligned}$$

**То же самое, но взрослее.** Распишем  $F(ab)$  по определению

$$\begin{aligned} F(ab) &= \sum_{d|ab} f(d) = \sum_{d_1|a, d_2|b} f(d_1d_2) = \sum_{d_1|n} \sum_{d_2|n} f(d_1)f(d_2) = \sum_{d_1|n} f(d_1) \sum_{d_2|n} f(d_2) = \\ &= \left( \sum_{d_1|n} f(d_1) \right) \cdot \left( \sum_{d_2|n} f(d_2) \right) = F(a)F(b). \end{aligned}$$

□

**Следствие 3.20.** Функции  $d$  и  $\sigma$  мультипликативны.

Вычислим теперь сумматор функции Эйлера, пользуясь тем, что нам известна мультипликативность. Обозначим  $\Phi(n) = \sum_{d|n} \varphi(d)$ , тогда

$$\Phi(p^k) = \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^k) = 1 + p - 1 + p^2 - p + p^3 - p^2 + \dots + p^k - p^{k-1} = p^k.$$

Отсюда (в связи с мультипликативностью) сразу ясно, что  $\forall n \in \mathbb{N}$  мы имеем  $\Phi(n) = n$ . Таким образом, мы доказали достаточно красивое тождество

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

Это можно доказывать и немного иначе. Например, разобьем вычеты от 1 до  $n$  на непересекающиеся множества  $S_d$  следующим образом:

$$m \in S_d \iff 1 \leq m \leq n, \quad (m, n) = d.$$

Ясно, что в объединении эти множества покрывают всё множество  $\{1, \dots, n\}$ . Теперь заметим, что

$$m \in S_d \implies (m, n) = d \implies \left(\frac{m}{d}, \frac{n}{d}\right) = 1 \implies |S_d| = \varphi\left(\frac{n}{d}\right).$$

Таким образом, имеем

$$n = |\{1, \dots, n\}| = \sum_{d|n} |S_d| = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d).$$

Итак, только что мы двумя способами доказали следующую теорему:

**Теорема 3.21.**  $\sum_{d|n} \varphi(d) = n$ .

## 4 Квадратичные вычеты

### 4.1 Определения и базовые свойства

В этом параграфе  $p$  всегда обозначает нечётное простое число.

**Определение 4.1.** Ненулевой вычет  $a \pmod{m}$  называется *квадратичным вычетом* (по модулю  $p$ ), если существует такой вычет  $x$ , что  $x^2 \equiv a \pmod{p}$ .

Иными словами, квадратичные вычеты — это “точные квадраты по модулю  $p$ ”.

**Определение 4.2.** Ненулевой вычет  $a \pmod{m}$  называется *квадратичным невычетом* (по модулю  $p$ ), если для всех вычетов  $x$  мы имеем  $x^2 \not\equiv a \pmod{m}$ .

Сейчас нашей локальной целью будет доказательство такой теоремы.

**Теорема 4.3.** Любая приведённая система вычетов  $\pmod{p}$  содержит ровно  $\frac{p-1}{2}$  квадратичных вычетов и  $\frac{p-1}{2}$  невычетов.

Совершенно ясно, что каждый из квадратичных вычетов сравним с одним из чисел  $1^2, 2^2, \dots, (p-1)^2$ . Заметим, что

$$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p},$$

откуда следует, что можно ограничиться половиной этого списка:  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ .

В этом же списке все вычеты различны:

$$x^2 \equiv y^2 \pmod{p} \implies (x+y)(x-y) \vdots p \implies x+y \vdots p \text{ или } x-y \vdots p,$$

но так как  $0 < x, y < \frac{p}{2}$ , мы имеем  $0 < x+y < p$ , то есть  $x+y \not\vdots p$ , откуда  $x-y \vdots p \implies x \equiv y \pmod{p}$ .

При обсуждении квадратичных вычетов, для того чтоб сделать записи и вычисления сильно менее громоздкими, используют *символ Лежандра*.

**Определение 4.4.** Для ненулевого вычета  $a \pmod p$  символ Лежандра определяется как

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a \text{ — квадратичный вычет } \pmod p \\ -1, & a \text{ — квадратичный невычет } \pmod p \end{cases}.$$

Оказывается, что символ Лежандра крайне удобен, так как он перемножается при перемножении вычетов:

**Предложение 4.5.** Для произвольных ненулевых вычетов  $a, b \pmod p$  мы имеем

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right).$$

То есть, произведение двух квадратичных вычетов или двух квадратичных невычетов — квадратичный вычет, а произведение вычета и невычета — невычет.

*Доказательство предложения.* Утверждение для двух квадратичных вычетов очевидно:

$$a \equiv x^2 \pmod p, \quad b \equiv x^2 \pmod p \implies ab \equiv (xy)^2 \pmod p,$$

то есть  $ab$  — квадратичный вычет.

Теперь зафиксируем квадратичный вычет  $a$  и умножим его на все элементы приведенной системы вычетов  $\pmod p$  —  $\frac{p-1}{2}$ , квадратичных вычетов и столько же квадратичных невычетов. В результате этого умножения получится снова приведенная система вычетов, в которой тоже  $\frac{p-1}{2}$  квадратичных вычетов и столько же невычетов.

Как мы уже доказали, при умножении на  $a$  квадратичные вычеты перешли в квадратичные вычеты; значит, квадратичные невычеты перейдут в оставшиеся элементы приведенной системы, то есть в квадратичные невычеты. Так мы доказали, что произведение квадратичного вычета и квадратичного невычета — квадратичный невычет.

Эту часть доказательства можно провести иначе. Предположим, что произведение квадратичного вычета  $a$  и квадратичного невычета  $b$  — квадратичный вычет  $c$ . По определению квадратичного вычета  $a \equiv k^2 \pmod p$  и  $c \equiv \ell^2 \pmod p$ . У линейного сравнения  $kx \equiv \ell \pmod p$  имеется решение:  $k \cdot r \equiv \ell \pmod p$ . Возводя в квадрат, получаем

$$c \equiv \ell^2 \equiv k^2 r^2 \equiv ar^2 \pmod p \implies b \equiv r^2 \pmod p,$$

что противоречит тому, что  $b$  невычет.

Для разбора последнего случая зафиксируем квадратичный невычет  $a$  и умножим на него все элементы приведенной системы вычетов. Квадратичные вычеты, как мы доказали, перейдут в квадратичные невычеты.

Значит, квадратичные невычеты перейдут во все остальные элементы приведенной системы, то есть в квадратичные вычеты. что и требовалось доказать.  $\square$

*Замечание 4.6.* Часто символ Лежандра определяют для произвольного целого  $a$ , полагая  $\left(\frac{a}{p}\right) = 0$ , если  $a \div p$ . В таком случае арифметическая функция  $f(a) = \left(\frac{a}{p}\right)$  мультипликативна.

## 4.2 Критерий Эйлера

Теперь неплохо было бы научиться понимать, является ли число квадратичным вычетом или нет, то есть вычислять символ Лежандра.

Рассмотрим для начала целое  $a \not\div p$ , где  $p$  — нечётное простое. Тогда

$$a^{p-1} \equiv 1 \pmod{p} \implies \left(a^{\frac{p-1}{2}} - 1\right) \cdot \left(a^{\frac{p-1}{2}} + 1\right) \div p \implies a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Но как знак зависит от числа  $a$ ? Ответ на этот вопрос даёт следующая теорема.

**Теорема 4.7** (Критерий Эйлера, 1748г.). Для целого  $a \not\div p$ , где  $p$  — нечётное простое, справедливо

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

*Доказательство.* Если  $a$  — квадратичный вычет, то это немедленно следует из малой теоремы Ферма 2.17:

$$a \equiv x^2 \pmod{p} \implies a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Если же  $a$  — квадратичный невычет, то можно применить приём, аналогичный доказательству теоремы Вильсона. Рассмотрим ненулевой вычет  $x \pmod{p}$ , ему мы можем единственным способом сопоставить такой  $y \pmod{p}$ , что

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

Действительно, это решение соответствующего линейного сравнения (оно существует и единственно, так как  $(x, p) = 1$ ). Теперь заметим, что  $x \not\equiv y \pmod{p}$ , так как  $a$  — невычет. Значит, все ненулевые вычеты мы разбили на  $\frac{p-1}{2}$  пар  $(x, y)$  так, что произведение чисел в каждой паре сравнимо с  $a \pmod{p}$ . Давайте перемножим все такие произведения: с одной стороны получится  $a^{\frac{p-1}{2}}$  (так как пар  $\frac{p-1}{2}$ ), а с другой произведение всех ненулевых вычетов, но тогда по теореме Вильсона 2.30 мы имеем:

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

$\square$

*Замечание 4.8.* Из критерия Эйлера сразу же следует доказанная нами ранее (с некоторыми не слишком большими муками) мультипликативность символа Лежандра. В самом деле,

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