16.12.2024

Малая Теорема Ферма. Группы, кольца, поля. Решение задач на теорию чисел.

Филиппов Михаил Витальевич

m.filippov@g.nsu.ru

89232283872

Императивное программирование, 2024-2025

Новосибирский государственный университет

*НАСТОЯЩАЯ НАУКА

Давайте познакомимся

Филиппов Михаил Витальевич

- Окончил магистратуру ФФ НГУ
- Окончил аспирантуру ИТ СО РАН
- Являюсь м.н.с. ИТ СО РАН
- 7+ лет опыт в программировании C/C++

План лекции

Теория сравнений (продолжение)

35 минут

Группы, кольца, поля

35 минут

Решение практических задач

20 минут

План лекции

Теория сравнений (продолжение)

35 минут

Группы, кольца, поля

35 минут

Решение практических задач

20 минут

Мультипликативные функции

Определение. Функция θ : **R** → **R** (или, более общо, θ : **C** → **C**) называется мультипликативной если:

1) Функция θ определена всюду на **N** и существует $a \in \mathbf{N}$ такой, что $\theta(a) \neq 0$.

2) Для любых взаимно простых натуральных чисел a_1 и a_2 выполняется $\theta(a_1 \cdot a_2) = \theta(a_1) \cdot \theta(a_2)$.

Пример 1. $\theta(a) = a^s$, где s – любое (хоть действительное, хоть комплексное) число.

Перечислим, кое-где доказывая, некоторые свойства ультипликативных функций. Пусть всюду ниже $\theta(a)$ – произвольная мультипликативная функция.

Свойство 1. $\theta(1) = 1$.

Доказательство. Пусть a – то самое натуральное число, для которого $\theta(a) \neq 0$. Тогда $\theta(a \cdot 1) = \theta(a) \cdot \theta(1) = \theta(a)$. ♦

Свойство 2. $\theta\left(p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}\right) = \theta\left(p_1^{a_1}\right)\theta\left(p_2^{a_2}\right) \dots \theta\left(p_n^{a_n}\right)$, где $p_1, p_2, \dots, p_n$ –различные простые числа.

Доказательство очевидно. ♦

Мультипликативные функции

Свойство 3. Обратно, мы всегда построим некоторую мультипликативную функцию θ(*a*), если зададим θ(1) = 1 и произвольно определим θ(*p*α) для всех простых *p* и всех натуральных α , а для остальных натуральных чисел доопределим функцию θ(*a*) используя равенство**.**

$$\theta\left(p_1^{a_1}\, p_2^{a_2} \ldots p_n^{a_n}\right) = \theta\left(p_1^{a_1}\right)\theta\left(p_2^{a_2}\right) \ldots \theta\left(p_n^{a_n}\right)$$

Доказательство сразу следует из основной теоремы арифметики.♦

Пример 2. Пусть θ(1) = 1 и θ(p^{α}) = 2 для всех *p* и α . Тогда, для произвольного числа, $\theta\left(p_1^{a_1}\, p_2^{a_2} \ldots p_n^{a_n}\right) = 2^n$.

Свойство 4. Произведение нескольких мультипликативных функций является мультипликативной функцией.

Доказательство. Сначала докажем для двух сомножителей: Пусть θ_1 и θ_2 **–** мультипликативные функции $\theta = \theta_1 \cdot \theta_2$, тогда (проверяем аксиомы определения)

1) $\theta(1) = \theta_1(1) \cdot \theta_2(1) = 1$ и, кроме того, существует такое *a* (это *a* = 1), что θ(*a*) ≠ 0.

2) Пусть (*a*, *b*) = 1 – взаимно просты. Тогда $\theta(a \cdot b) = \theta_1(a \cdot b) \cdot \theta_2(a \cdot b) =$

$= \theta_1(a)\, \theta_1(b)\, \theta_2(a)\, \theta_2(b) = \theta_1(a)\, \theta_2(a) \cdot \theta_1(b)\, \theta_2(b) = \theta(a)\, \theta(b)$.

Доказательство для большего числа сомножителей проводится стандартным индуктивным рассуждением. ♦

Мультипликативные функции

Введем удобное обозначение. Всюду далее, символом $\sum_{d|n}$ будем обозначать сумму чего-либо, в которой суммирование проведено по всем делителям *d* числа *n*.

Лемма 1. Пусть $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ – каноническое разложение числа $a \in \mathbf{N}$, θ – любая мультипликативная функция. Тогда:

$$\sum_{d \mid a} \theta(d)$$
$$= \left(1 + \theta(p_1) + \theta(p_1^2) + \cdots + \theta\left(p_1^{a_1}\right)\right) \times \left(1 + \theta(p_2) + \theta(p_2^2) + \cdots + \theta\left(p_2^{a_2}\right)\right) \times \cdots$$
$$\times \left(1 + \theta(p_n) + \theta(p_n^2) + \cdots + \theta\left(p_n^{a_n}\right)\right)$$

Если $a = 1$, то считаем правую часть равной 1.

Доказательство. Раскроем скобки в правой части. Получим сумму всех (без пропусков и повторений) слагаемых вида

$$\theta\left(p_1^{\beta_1}\right)\theta\left(p_2^{\beta_2}\right)\dots\theta\left(p_n^{\beta_n}\right),$$

где $0 \le \beta_k \le \alpha_k$, для всех $k \le n$. Так как различные простые числа заведомо взаимно просты, то

$\theta\left(p_1^{\beta_1}\right)\theta\left(p_2^{\beta_2}\right)\dots\theta\left(p_n^{\beta_n}\right) = \theta\left(p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}\right)$ а это как раз то, что стоит в доказываемом равенстве слева. ♦

Мультипликативные функции

Лемма 2. Пусть θ(*a*) – любая мультипликативная функция. Тогда $\chi(a) = \sum_{d \mid a} \theta(d)$ – также мультипликативная функция.

Доказательство. Проверим для χ(*a*) аксиомы определения мультипликативной функции.

1). $\chi\,(1) = \sum_{d \mid 1} \theta(d) = \ \theta(1) = 1$

2). Пусть (*a*, *b*) = 1; $a = p_1^{a_1}\, p_2^{a_2} \ldots p_n^{a_n}, b = q_1^{\beta_1}\, q_2^{\beta_2} \ldots q_n^{\beta_n}$, и все *p* и *q* различны. Тогда, по предыдущей лемме, имеем: (благо, делители у чисел *a* и *b* различны)

$$\chi\,(1) = \sum_{d \mid ab} \theta(d)$$

$$= \prod_i \left(1 + \theta(p_i) + \theta\left(p_i^2\right) + \cdots + \theta\left(p_i^{a_i}\right)\right) \times \prod_j \left(1 + \theta\left(q_j\right) + \theta\left(q_j^2\right) + \cdots + \theta\left(q_j^{\beta_j}\right)\right)$$

$$= \chi\,(a)\chi\,(b)$$

Примеры мультипликативных функций

Пример 3. Число делителей данного числа.

Пусть θ(a) = $a^0 \equiv 1$ – тождественная единица (заведомо мультипликативная функция). Тогда, если $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, то тождество леммы 1 принимает вид:

$\tau(a) = \sum_{d \mid a} \theta(d) = (1 + a_1)(1 + a_2) \dots (1 + a_n) = \sum_{d \mid a} 1$ – это не что иное, как количество делителей числа a. По лемме 2, количество делителей т(a) числа a есть мультипликативная функция.

Численный пример. т(720) = т($2^4 \cdot 3^2 \cdot 5$) = (4 + 1)(2 + 1)(1 + 1) = 30.

Пример 4. Сумма делителей данного числа.

Пусть θ(a) = $a^1 \equiv a$ – тождественная мультипликативная функция. Тогда, если $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, то тождество леммы 1 пункта вид:

$$S(a) = \sum_{d \mid a} d = \sum_{d \mid a} \theta(d) = \left(1 + p_1 + p_1^2 + \dots + p_1^{a_1}\right)\left(1 + p_2 + p_2^2 + \dots p_2^{a_2}\right) \dots \left(1 + p_n + p_n^2 + \dots + p_n^{a_n}\right)$$

$$= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_n^{a_n+1} - 1}{p_n - 1}$$

– сумма всех делителей числа a. По лемме 2, сумма всех делителей - мультипликативная функция.

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

Примеры мультипликативных функций

Пример 5. Функция Мебиуса.

Функция Мебиуса μ (a) – это мультипликативная функция, определяемая следующим образом: если p – простое число, то μ(p) = −1; μ (p^α) = 0, при α > 1; на остальных натуральных числах функция доопределяется по мультипликативности.

Таким образом, если число a делится на квадрат натурального числа, отличный от единицы, то μ (a) = 0; если же a = $p_1p_2\cdots p_k$, то μ(a) = $(-1)^k$, где k – число различных простых делителей a . Понятно, что μ (1) = (–1)^0 = 1, как и должно быть.

Лемма 3. Пусть θ(a) – произвольная мультипликативная функция, а $a = p_1^{a_1}\, p_2^{a_2} \ldots p_n^{a_n}$. Тогда:

$$\sum_{d \mid a} \mu(d)\theta(d) = \big(1-\theta(p_1)\big)\big(1-\theta(p_2)\big)\ldots\big(1-\theta(p_n)\big),$$

(при a = 1 считаем правую часть равной 1).

Доказательство. Рассмотрим функцию $\theta_1(x) = \mu(x)\cdot\theta(x)$. Эта функция мультипликативна, как произведение мультипликативных функций. Для $\theta_1(x)$ имеем (p – простое): $\theta_1(p) = -\theta(x)$; $\theta_1(p^\alpha) = 0$, при α > 1.

Следовательно, для $\theta_1(x)$ тождество леммы 1 выглядит так:

$$\sum_{d \mid a} \theta_1(d) = \prod_{k=1}^{n}(1-\theta(p_k))$$

♦

Примеры мультипликативных функций

Следствие 1. Пусть $\theta(d) = d^{-1} = \frac{1}{d}$ (это, конечно, мультипликативная функция), $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, a > 1 . Тогда:

$$\sum_{d \mid a} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right).$$

Физический смысл этой правой части раскрывает пример следующей функции.

Пример 6. Функция Эйлера.

Функция Эйлера, пожалуй, самая знаменитая и “дары приносящая” функция из всех функций, рассматриваемых в этом пункте. Функция Эйлера ϕ(a) есть количество чисел из ряда 0, 1, 2, ... , a-1, взаимно простых с a.

Лемма 4. Пусть $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$. Тогда:

1) $\phi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right)$ (формула Эйлера);

2) $\phi(a) = \left(p_1^{a_1} - p_1^{a_1 - 1}\right)\left(p_2^{a_2} - p_2^{a_2 - 1}\right) \dots \left(p_n^{a_n} - p_n^{a_n - 1}\right)$, в частности, $\phi\,(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$, $\phi\,(p) = p - 1$.

Примеры мультипликативных функций

Доказательство. Пусть x пробегает числа 0, 1, 2, ... , a-1. Положим $\delta_x = (x, a)$ – наибольший общий делитель. Тогда ϕ(a) есть число значений δ_x, равных 1. Придумаем такую функцию $\chi(\delta_x)$, чтобы она была единицей, когда δ_x единица, и была нулем в остальных случаях. Вот подходящая кандидатура:

$$\chi(\delta_x) = \sum_{d|\delta_x} \mu(d) = \begin{cases} 0, \text{если } \delta_x > 1 \\ 1, \text{если } \delta_x = 1 \end{cases}$$

Последнее легко понять, если вспомнить лемму 1 из этого пункта и в ее формулировке взять θ(d) ≡ 1. Далее, сделав над собой некоторое усилие, можно усмотреть, что:

$$\varphi(a) = \sum_{0 \le x < a} \chi(\delta_x) = \sum_{0 \le x < a} \sum_{d|\delta_x} \mu(d)$$

Зафиксируем некоторое d_0 такое, что d_0 делит a, d_0 делит x, x < a. Значит в сумме справа в скобках слагаемых $\mu(d_0)$ ровно a/d_0 штук и ϕ(a) есть просто сумма $\sum_{d_0|a} \frac{a}{d_0}$. После этого, равенство

$$a \sum_{d \mid a} \frac{\mu(d)}{d} = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right)$$

получается применением следствия из леммы 3. Поскольку справа сумма в скобках берется по всем делителям d числа $\delta_x = (x, a)$, то d делит x и d делит a. Значит в первой сумме справа в суммировании участвуют только те x, которые кратны d . Таких x среди чисел 0, 1, 2, ... , a-1 ровно a/d штук. Получается, что:

$$\varphi(a) = \sum_{d \mid a} \frac{a}{d} \mu(d) = a \sum_{d \mid a} \frac{\mu(d)}{d} = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right).$$

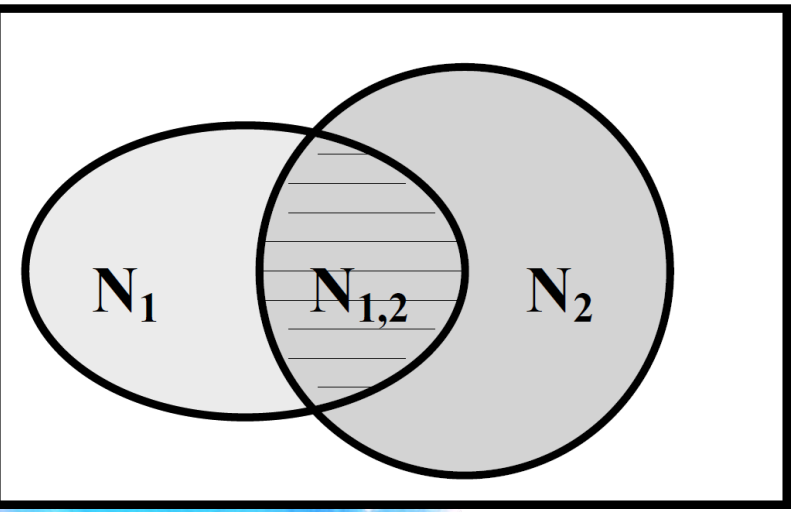
Примеры мультипликативных функций

Формула

$$\phi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)$$

для вычисления функции Эйлера имеет ясный “физический смысл”.

Правило включений и исключений. Пусть задано множество A и выделено k его подмножеств. Количество элементов множества A, которые не входят ни в одно из выделенных подмножеств, подсчитывается так: надо из общего числа элементов A вычесть количества элементов всех k подмножеств, прибавить количества элементов всех их попарных пересечений, вычесть количества элементов всех тройных пересечений, прибавить количества элементов всех пересечений по четыре и т.д. вплоть до пересечения всех k подмножеств. **Пример** подсчета функции Эйлера для чисел вида $a = p_1^{a_1}\, p_2^{a_2}$.



Прямоугольник изображает множество всех целых чисел от 0 до a; овал N_1 – множество чисел, кратных p_1; кружок N_2 – числа, кратные p_2; пересечение $N_{1,2}$ – множество чисел, делящихся одновременно на p_1 и p_2, т.е. на p_1p_2; числа вне овала и кружочка взаимно просты с a. Для подсчета числа чисел, взаимно простых с a, нужно из a вычесть количество чисел в N_1 и количество чисел в N_2 (их, соответственно, a/p_1 и a/p_2 штук), при этом общая часть $N_{1,2}$ (там $a/(p_1p_2$ штук чисел) вычтется дважды, значит ее надо один раз прибавить (вот оно, “включение - исключение”!). В результате получим:

$$\phi(a) = a - \frac{a}{p_1} - \frac{a}{p_2} + \frac{a}{p_1p_2} = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)$$

Примеры мультипликативных функций

Следствие 2. Функция Эйлера мультипликативна.

Доказательство. Имеем:

$$\phi(a) = a \sum_{d \mid a} \frac{\mu(d)}{d}$$

– произведение двух мультипликативных функций, первая из которых мультипликативна по лемме 2. Значит, ϕ(a) – мультипликативна. ♦

Следствие 3. $\sum_{d \mid a} \varphi(d) = a$.

Доказательство. Пусть $a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$. Тогда, по лемме 1 имеем:

$$\sum_{d \mid a} \varphi(d) = \prod_{k=1}^{n} \left(1 + \varphi(p_k) + \varphi\left(p_k^2\right) + \cdots + \varphi\left(p_k^{a_k}\right)\right)$$

♦

Численные примеры.

$$\phi(5) = 5 - 1 = 4$$

$$\phi(30) = \phi(2 \cdot 3 \cdot 5) = (2 - 1)(3 - 1)(5 - 1) = 8$$

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

$$\sum_{d \mid 30} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$$

Вступление про Эйлера

Леонард Эйлер (1707 – 1783 – ...) – самый плодовитый математик восемнадцатого столетия, если только не всех времен.

- Опубликовано более двухсот томов его научных трудов. Слепой Эйлер, пользуясь своей феноменальной памятью, диктовал свои работы, общее число которых достигло 886.
- Как ученый, Эйлер сформировался в швейцарском городе Базеле, университет которого долгое время был средоточием европейской науки того времени.
- Его работы посвящены анализу, алгебре, дискретной математике (теории графов), вариационному исчислению, функциям комплексного переменного, астрономии, гидравлике, теоретической механике, кораблестроению, артиллерии, теории музыки и т.д., и т.п.
- Эйлер находил сумму ряда:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots$$

- “Изучение работ Эйлера остается наилучшей школой в различных областях математики, и ничто другое не может это заменить”.
- Он был дважды женат и имел тринадцать детей.

Теорема Эйлера

Теорема (Эйлер). Пусть m > 1 , (a, m) = 1 , ϕ (m) – функция Эйлера. Тогда:

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

Доказательство: Пусть x пробегает приведенную систему вычетов по mod m:

$$x = r_1, r_2, \dots r_c;$$

где c = ϕ (m) − их число, $r_1, r_2, \dots r_c$ − наименьшие неотрицательные вычеты по mod m. Следовательно, наименьшие неотрицательные вычеты, соответствующие числам ax суть соответственно:

$$\rho_1, \rho_2, \dots, \rho_c$$

– тоже пробегают приведенную систему вычетов, но в другом порядке. Значит:

$$a \cdot r_1 \equiv \rho_{j_1}(mod\ m)$$
$$a \cdot r_2 \equiv \rho_{j_2}(mod\ m)$$
$$\vdots$$
$$a \cdot r_c \equiv \rho_{j_c}(mod\ m)$$

Перемножим эти c штук сравнений. Получится:

$$a^c r_1 r_2 \dots r_c \equiv \rho_1 \rho_2 \dots \rho_c (mod\ m).$$

Так как $r_1 r_2 \dots r_c = \rho_1 \rho_2 \dots \rho_c \neq 0$ и взаимно просто с модулем m, то, поделив последнее сравнение на $r_1 r_2 \dots r_c$, получим $a^{\varphi(m)} \equiv 1(mod\ m)$. ♦

Теорема Ферма

Теорема (Ферма). Пусть *p* – простое число, *p* не делит *a* . Тогда: $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

Доказательство 1. Положим в условии теоремы Эйлера *m* = *p*, тогда ϕ (*m*) = *p* − 1. Получаем $a^{p-1} \equiv 1(mod\ p)$.♦

Доказательство 2. Так как *p* − простое число, то все биномиальные коэффициенты:

$$C_p^k = \frac{p(p-1)(p-2)\ldots(p-k+1)}{1 \cdot 2 \cdot 3 \cdot \ldots \cdot k}$$

(кроме C_p^0 и C_p^p) делятся на *p* , ибо числитель выписанного выражения содержит *p*, а знаменатель не содержит этого множителя. Если вспомнить бином Ньютона, то становится понятно, что разность

$$(A+B)^p - A^p - B^p = C_p^1 A^{p-1} B^1 + C_p^2 A^{p-2} B^2 + \cdots C_p^{p-1} A^1 B^{p-1}$$

где *A* и *B* – какие угодно целые числа, всегда делится на *p*. Последовательным применением этого незатейливого наблюдения получаем, что

$(A+B+C)^p - A^p - B^p - C^p = \{[(A+B)+C]^p - (A+B)^p - C^p\} + (A+B)^p - A^p - B^p$ всегда делится на *p*; $(A+B+C+D)^p - A^p - B^p - C^p - D^p$ всегда делится на *p* ; и вообще, $(A+B+C+\cdots+K)^p - A^p - B^p - C^p - \cdots - K^p$ всегда делится на *p*. Положим теперь в последнем выражении *A* = *B* = *C* =...= *K* = 1 и возьмем количество этих чисел равным *a*. Получится, что , $a^p - a$ делится на *p* , а это и есть теорема Ферма в более общей формулировке.

Следствия

Следствие 4. Без всяких ограничений на $a \in \mathbf{Z}$, $a^p \equiv a(mod\ p)$.

Доказательство. Умножим обе части сравнения $a^{p-1} \equiv 1(mod\ p)$ на a. Ясно, что получится сравнение, справедливое и при a, кратном p. ♦

Следствие 5. $(A+B)^p \equiv A^p - B^p(mod\ p)$.

Пример 7. Девятая степень однозначного числа оканчивается на 7. Найти это число.

Решение. $a^9 \equiv 7(\mathrm{mod}10)$ – это дано. Кроме того, очевидно, что (7, 10)=1 и (a, 10)=1. По теореме Эйлера, $a^{\phi(10)} \equiv 1\ (\mathrm{mod}\ 10)$. Следовательно, $a^4 \equiv 1(\mathrm{mod}10)$ и, после возведения в квадрат, $a8 \equiv 1(\mathrm{mod}10)$. Поделим почленно $a^9 \equiv 7(\mathrm{mod}10)$ на $a^8 \equiv 1(\mathrm{mod}10)$ и получим $a \equiv 7(\mathrm{mod}10)$. Это означает, что $a = 7$.

Пример 8. Доказать, что $1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv -1(\mathrm{mod}\ 7)$.

Доказательство. Числа 1, 2, 3, 4, 5, 6 взаимно просты с 7. По теореме Ферма имеем:

$$1^6 \equiv 1(mod\ 7)$$
$$2^6 \equiv 1(mod\ 7)$$
$$\vdots$$
$$3^6 \equiv 1(mod\ 7)$$

Возведем эти сравнения в куб и сложим:

$1^{18} + 2^{18} + 3^{18} + 4^{18} + 5^{18} + 6^{18} \equiv 6(\mathrm{mod}\ 7) \equiv -1(\mathrm{mod}\ 7)$.

Примеры

Пример 9. Найти остаток от деления 7^{402} на 101.

Решение. Число 101 – простое, (7, 101)=1, следовательно, по теореме Ферма:
$7^{100} \equiv 1(\mathrm{mod}101)$. Возведем это сравнение в четвертую степень: $7^{400} \equiv 1(\mathrm{mod}101)$, домножим его на очевидное сравнение $7^2 \equiv 49(\mathrm{mod}101)$, получим: $7^{402} \equiv 49(\mathrm{mod}101)$. Значит, остаток от деления 7^{402} на 101 равен 49.

Пример 10. Найти две последние цифры числа 243^{402}.

Решение. Две последние цифры этого числа суть остаток от деления его на 100.
Имеем: 243=200+43; 200 + 43 ≡ 43(mod100) и, возведя последнее очевидное сравнение в 402-ую степень, раскроем его левую часть по биному Ньютона. Все слагаемые, кроме последнего, содержат степень числа 200, т.е. делятся на 100, поэтому $243^{402} \equiv 43^{402}$ (mod100). Далее, 43 и 100 взаимно просты, значит, по теореме Эйлера, $43^{\phi(100)} \equiv 1(\mathrm{mod}100)$. Считаем: $\phi(100) = \phi(2^2 \cdot 5^2) = (10 - 5)(10 - 2) = 40$.
Имеем сравнение: $43^{40} \equiv 1(\mathrm{mod}100)$, которое немедленно возведем в десятую степень и умножим почленно на очевидное сравнение, проверенное на калькуляторе: $43^2 \equiv 49(\mathrm{mod}100)$. Получим: $43^{402} \equiv 49(\mathrm{mod}100)$, следовательно, две последние цифры числа 243^{402} будут 4 и 9 .

Пример 11. Доказать, что $(73^{12} - 1)$ делится на 105.

Решение. Имеем: 105 = 3·5·7, (73, 3) = (73, 5) = (73, 7) = 1. По теореме Ферма:

$$73^2 \equiv 1(mod\ 7)$$
$$73^4 \equiv 1(mod\ 7)$$
$$73^6 \equiv 1(mod\ 7)$$

Перемножая, получаем: $73^{12} \equiv 1(\mathrm{mod}\ 3),(\mathrm{mod}\ 5),(\mathrm{mod}\ 7)$, откуда, по свойствам сравнений, изложенным в п
16, немедленно следует: $73^{12} - 1 \equiv 0(\mathrm{mod}105)$, ибо 105 − наименьшее общее кратное чисел 3, 5 и 7.

Сравнения второй степени

Двучленные сравнения второй степени:

$x^2 \equiv a(mod\ p)$, где *a* и *p* взаимно просты, а *p* − нечетное простое число. Обратите внимание, что условие взаимной простоты (*a, p*)=1 исключает из нашего рассмотрения случай *a* = 0.

Нас будет интересовать вопрос, при каких *a* простейшее двучленное сравнение второй степени имеет решение, а при каких – не имеет. Ясно, что сравнение $x^2 \equiv a(\mathrm{mod}\ 2)$ имеет решение при любых *a*, т.к. вместо *a* достаточно подставлять только 0 или 1, а числа 0 и 1 являются квадратами. Именно поэтому случай *p* = 2 не представляет особого интереса и выводится из дальнейшего рассмотрения вышенаписанной странноватой фразой. Что касается сравнения $x^2 \equiv 0(\mathrm{mod}\ p)$, то оно, очевидно, всегда имеет решение *x* = 0. Итак, интерес представляет только ситуация с нечетным простым модулем и *a* ≠ 0, поэтому далее мы будем трудиться только в рамках оговоренных ограничений.

Определение. Если сравнение $x^2 \equiv a(mod\ p)$ имеет решения, то число *a* называется квадратичным вычетом по модулю *p*. В противном случае, число *a* называется квадратичным невычетом по модулю *p*.

Итак, если *a* – квадрат некоторого числа по модулю *p* , то *a* −“квадратичный вычет”, если же никакое число в квадрате не сравнимо с *a* по модулю *p* , то *a* − “квадратичный невычет”. Смиримся с этим.

Сравнения второй степени

Пример 12. Число 2 является квадратом по модулю 7, т.к. 42 ≡ 16 ≡ 2(mod7). Значит, 2 − квадратичный вычет. (Сравнение $x^2 \equiv 2(\mathrm{mod}7)$ имеет еще и другое решение: $3^2 \equiv 9 \equiv 2(\mathrm{mod}\ 7)$.) Напротив, число 3 является квадратичным невычетом по модулю 7 , т.к. сравнение $x^2 \equiv 3(\mathrm{mod}7)$ решений не имеет, в чем нетрудно убедиться последовательным перебором полной системы вычетов: $x = 0, 1, 2, 3, 4, 5, 6$.

Простое наблюдение: Если *a* − квадратичный вычет по модулю *p*, то сравнение $x^2 \equiv a(mod\ p)$ имеет в точности два решения. Действительно, если *a* – квадратичный вычет по модулю *p*, то у сравнения $x^2 \equiv a(mod\ p)$ есть хотя бы одно решение $x \equiv x_1(\mathrm{mod}\ p)$. Тогда $x_2 = -x_1$ − тоже решение, ведь $(-x_1)^2 = x_1^2$. Эти два решения не сравнимы по модулю $p > 2$, так как из $x_1 \equiv x_1(\mathrm{mod}\ p)$ следует $2x_1 \equiv 0(\mathrm{mod}\ p)$, т.е. (поскольку $p \neq 2$) $x_1 \equiv 0(\mathrm{mod}\ p)$, что невозможно, ибо $a \neq 0$. Поскольку сравнение $x^2 \equiv a(mod\ p)$ есть сравнение второй степени по простому модулю, то больше двух решений оно иметь не может.

Еще одно простое наблюдение: Приведенная (т.е. без нуля) система вычетов $-\frac{p-1}{2}, \dots, -2, -1, 1, 2, \dots, \frac{p-1}{2}$ по модулю *p* состоит из $\frac{p-1}{2}$ квадратичных вычетов, сравнимых с числами $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$, и $\frac{p-1}{2}$ квадратичных невычетов, т.е. вычетов и невычетов поровну.

Определение. Пусть *a* не кратно *p*. Тогда символ Лежандра определяется как:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, \text{если а} - \text{квадратичный вычет по модулю р.} \\ -1, \text{если а} - \text{квадратичный невычет по модулю р.} \end{cases}$$

Сравнения второй степени

Теорема. (Критерий Эйлера) Пусть *a* не кратно *p*. Тогда:

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

Доказательство. По теореме Ферма, $a^{p-1} \equiv 1(\mathrm{mod}\ p)$, т.е.

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(\mathrm{mod}\ p)$$

В левой части последнего сравнения в точности один сомножитель делится на *p*, ведь оба сомножителя на *p* делиться не могут, иначе их разность, равная двум, делилась бы на $p > 2$. Следовательно, имеет место одно и только одно из сравнений:

$$a^{\frac{p-1}{2}} \equiv 1(mod\ p)$$

$$a^{\frac{p-1}{2}} \equiv -1(mod\ p)$$

Но всякий квадратичный вычет *a* удовлетворяет при некотором *x* сравнению $a \equiv x^2(mod\ p)$ и, следовательно, удовлетворяет также получаемому из него почленным возведением в степень $\frac{p-1}{2}$ сравнению $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1(mod\ p)$ (опять теорема Ферма). При этом, квадратичными вычетами и исчерпываются все решения сравнения $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$, т.к., будучи сравнением степени $\frac{p-1}{2}$, оно не может иметь более $\frac{p-1}{2}$ решений. Это означает, что квадратичные невычеты удовлетворяют сравнению $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$. ♦

Свойства символа Лежандра

Пример 13. Крошка-сын к отцу пришел, и спросила кроха: “Будет ли число 5 квадратом по модулю 7?”. Гигант-отец тут же сообразил:

$$5^{\frac{7-1}{2}} = 5^3 = 125 = 18 \cdot 7 - 1 \equiv -1(mod\ 7),$$

т.е. сравнение $x^2 \equiv 5(mod\ 7)$ решений не имеет и 5 − квадратичный невычет по модулю 7. Кроха-сын, расстроенный, пошел на улицу делиться с друзьями полученной информацией.

Перечислим далее, кое-где доказывая или комментируя, простейшие свойства символа Лежандра.

Свойство 5. Если $a \equiv b(mod\ p)$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Это свойство следует из того, что числа одного и того же класса по модулю *p* будут все одновременно квадратичными вычетами либо квадратичными невычетами. ♦

Свойство 6. $\left(\frac{1}{p}\right) = 1$.

Доказательство очевидно, ведь единица является квадратом. ♦

Свойства символа Лежандра

Свойство 7. $\left(\frac{-1}{p}\right)(-1)^{\frac{p-1}{2}}$.

Доказательство этого свойства следует из критерия Эйлера при *a* = −1. Так как $\frac{p-1}{2}$ – четное, если *p* вида 4*n* +1 , и нечетное, если *p* вида 4*n* +3, то число −1 является квадратичным вычетом по модулю *p* тогда и только тогда, когда *p* вида 4*n* +1. ♦

Свойство 8. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Действительно, $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (mod\ p)$. ♦

Свойство 8, очевидно, распространяется на любое конечное число сомножителей в числителе символа Лежандра, взаимно простых с *p*. Кроме того, из него следует

Свойство 9. $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$, т.е. в числителе символа Лежандра можно отбросить любой квадратный множитель.

Действительно:

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

Историческое отступление про Гаусса

Карл Фридрих Гаусс (1777 – 1855) – величественная фигура математики рубежа восемнадцатого – девятнадцатого столетий.

Он родился в немецком городке Брауншвейге, был сыном поденщика.

Математические способности Гаусса проявились очень рано, а, согласно его дневникам, в 17 лет Карл Фридрих уже начал делать выдающиеся математические открытия. Дебютом Гаусса явилось доказательство возможности построения правильного семнадцатиугольника циркулем и линейкой.

В 1795 – 1798 годах юный гений учился в Геттингенском университете, в 1799 году он получил степень доктора, а с 1807 года до самой смерти он спокойно работал в качестве директора астрономической обсерватории и профессора математики Геттингенского университета.

Гаусс составил огромные таблицы простых чисел и самостоятельно, путем внимательного их разглядывания, он открыл квадратичный закон взаимности: если *p* и *q* – два нечетных простых числа, то

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

Столь выдающийся результат Гаусса был назван современниками “золотая теорема” (“theorema aurum”).

Пусть *p* – нечетное простое число, $S = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ − множество всех положительных чисел из приведенной системы вычетов по модулю *p* . Рассмотрим

сравнение $a \cdot s \equiv \varepsilon_s r_s (mod\ p)$, где *a* − числитель исследуемого символа Лежандра, $s \in S$, $\varepsilon_s r_s$ − абсолютно наименьший вычет числа *as* по модулю *p* (т.е. вычет, абсолютная величина которого наименьшая), r_s − абсолютная величина этого вычета, а ε_s, стало быть, его знак. Таким образом, $\varepsilon_s \in S$, а $\varepsilon_s = \pm 1$.

Свойства символа Лежандра

Лемма 5 (Гаусс). $\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_s$.

Доказательство. Рассмотрим сравнения

$$\begin{cases} a \cdot 1 = \varepsilon_1 r_1 (mod\ p) \\ a \cdot 2 = \varepsilon_2 r_2 (mod\ p) \\ \vdots \\ a \cdot \dfrac{p-1}{2} = \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}} (mod\ p) \end{cases}$$

Множество чисел

$$\{\pm as | s \in S\} = \left\{a \cdot 1, -a \cdot 1, a \cdot 2, -a \cdot 2, \dots, a \cdot \frac{p-1}{2}, -a \cdot \frac{p-1}{2}\right\}$$

является приведенной системой вычетов по модулю p. Их абсолютно наименьшие вычеты соответственно суть

$$\{\pm as | s \in S\} = \left\{\varepsilon_1 r_1, -\varepsilon_1 r_1, \varepsilon_2 r_2, -\varepsilon_2 r_2, \dots, \varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}, -\varepsilon_{\frac{p-1}{2}} r_{\frac{p-1}{2}}\right\},$$

положительные же из них, т.е. $r_1, r_2, \dots, r_{\frac{p-1}{2}}$, совпадают с числами $1,2,\dots,\frac{p-1}{2}$, т.е. образуют множество S. Перемножим теперь почленно сравнения $(*)$ и сократим произведение на

$$1 \cdot 2 \cdot \dots \cdot \frac{p-1}{2} = r_1 \cdot r_2 \cdot \dots \cdot r_{\frac{p-1}{2}} = \prod_{s \in S} s$$

Получим: $a^{\frac{p-1}{2}} = \varepsilon_1 \varepsilon_2 \varepsilon_{\frac{p-1}{2}} (mod\ p)$. Согласно критерию Эйлера из предыдущего пункта, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (mod\ p)$, т.е. $\left(\frac{a}{p}\right) = \prod_{s \in S} \varepsilon_s$, что и требовалось. ♦

Свойства символа Лежандра

Лемма 6. При нечетном *a*,

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}+\sum_{s\in S}\left[\frac{as}{p}\right]},$$

где $\left[\frac{as}{p}\right]$ − целая часть числа $\frac{as}{p}$.

Доказательство. Имеем:

$$\left[\frac{2as}{p}\right] = \left[2\cdot\left[\frac{as}{p}\right] + 2\left\{\frac{as}{p}\right\}\right] = 2\cdot\left[\frac{as}{p}\right] + \left[2\left\{\frac{as}{p}\right\}\right],$$

что будет четным или нечетным, в зависимости от того, будет ли наименьший неотрицательный вычет числа *as* меньше или больше числа $\frac{p}{2}$, т.е. будет ли ε_s = 1 или ε_s = −1.

Отсюда, очевидно, $\varepsilon_s = (-1)^{\left[\frac{2as}{p}\right]}$,

поэтому, в силу леммы Гаусса, $\left(\frac{a}{p}\right) = (-1)^{\sum_{s\in S}\left[\frac{2as}{p}\right]}$.

Преобразуем это равенство (помним, что *a* + *p* – четное, а квадратичный множитель из числителя символа Лежандра можно отбрасывать):

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+b}{2}}{p}\right) = \left(\frac{\frac{a+b}{2}}{p}\right) = (-1)^{\sum_{s\in S}\left[\frac{(a+p)s}{p}\right]} = (-1)^{\sum_{s\in S}\left[\frac{as}{p}\right]+\sum_{s\in S} s}$$

Поскольку $\left(\frac{2a}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{a}{p}\right)$, а $\sum_{s\in S} s = 1+2+\cdots+\frac{p-1}{2} = \frac{p^2-1}{8}$, то лемма 6 доказана. ♦

Свойства символа Лежандра

Лемма 7. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Доказательство. Непосредственно следует из леммы 2 при $a = 1$. ♦

Ни у кого не должно возникать недоумения по поводу возможности деления числа $p^2 - 1 = (p - 1)(p + 1)$ на 8 нацело, т.к. из двух последовательных четных чисел одно обязательно делится на 4. Кроме того, простое число p можно представить в виде $p = 8n + k$, где k – одно из чисел 1, 3, 5, 7. Так как число

$$\frac{(8n+k)^2 - 1}{8} = 8n^2 + 2nk + \frac{k^2 - 1}{8}$$

будет четным при $k = 1$ и $k = 7$, то 2 будет квадратичным вычетом по модулю p, если p вида $8n+1$ или $8n+7$. Если же p вида $8n+3$ или $8n+5$, то 2 будет квадратичным невычетом.

Теорема (Закон взаимности квадратичных вычетов). Если p и q – нечетные простые числа, то

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

Другими словами, если хоть одно из чисел p или q вида $4n + 1$, то p квадрат по модулю q тогда и только тогда, когда q квадрат по модулю p. Если же оба числа p и q вида $4n+3$, то p квадрат по модулю q тогда и только тогда, когда q не является квадратом по модулю p.

Свойства символа Лежандра

Доказательство. Поскольку $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, то формула из леммы 6 принимает вид:

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{s=1}^{\frac{p-1}{2}}\left[\frac{as}{p}\right]}$$

Рассмотрим два множества: $S = \left\{1, 2, \dots, \frac{p-1}{2}\right\}$ и $K = \left\{1, 2, \dots, \frac{q-1}{2}\right\}$.

Образуем $\frac{p-1}{2} \cdot \frac{q-1}{2}$ штук пар чисел (*qx*, *py*), где *x* пробегает ***S***, а *y* пробегает ***K***. Первая и вторая компонента одной пары никогда не совпадают, ибо из *py* = *qx* следует, что *py* кратно *q*. Но ведь это невозможно, так как (*p*,*q*) = 1 и, поскольку 0 < *y* < *q*, то (*y*,*q*) = 1. Положим, поэтому, $\frac{p-1}{2} \cdot \frac{q-1}{2} = V_1 + V_2$, где V_1 – число пар, в которых первая компонента меньше второй (*qx* < *py*), V_2 – число пар, в которых вторая компонента меньше первой (*qx* > *py*).

Очевидно, что V_1 есть число пар, в которых $x < \frac{p}{q}y$. (Вообще-то, $x \le \frac{p-1}{2}$, но $\frac{p}{q}y < \frac{1}{2}$ т.к. $\frac{y}{q} < \frac{1}{2}$, следовательно $\left[\frac{p}{q}y\right] \le \left[\frac{p}{2}\right] = \frac{p-1}{2}$, и неравенство $x < \frac{p}{q}y$ не противоречит неравенству $x \le \frac{p-1}{2}$.)

Поэтому, $V_1 = \sum_{y \epsilon K}\left[\frac{p}{q}y\right]$. Аналогично, $V_2 = \sum_{x \epsilon S}\left[\frac{p}{q}x\right]$. Тогда равенство из леммы 7, отмеченное в начале этого доказательства, дает: $\left(\frac{p}{q}\right) = (-1)^{V_1}$, $\left(\frac{q}{p}\right) = (-1)^{V_2}$.

Это означает, что $\left(\frac{p}{q}\right) = (-1)^{V_1+V_2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, а это, собственно, и требовалось. ♦

План лекции

Теория сравнений (продолжение)	**Группы, кольца, поля**	Решение практических задач
35 минут	35 минут	20 минут

Основные алгебраические структуры

Определение 2.1. Множество G с бинарной операцией ◦ называется группой, если выполняются следующие свойства (аксиомы группы):

1. (ассоциативность) для любых a, b, c ∈ G (a ◦ b) ◦ c = a ◦ (b ◦ c);

2. (существование нейтрального элемента) существует элемент e ∈ G такой, что для любого a ∈ G a ◦ e = e ◦ a = a (такой элемент называется нейтральным или единичным);

3. (существование обратного элемента) для любого a ∈ G существует элемент b ∈ G такой, что a ◦ b = b ◦ a = e (такой элемент называется обратным к a и обозначается a^{-1}).

Определение 2.2. Если G - группа, и для любых a, b ∈ G выполняется равенство a ◦ b = b ◦ a, то группа G называется коммутативной или абелевой.

Примеры.

(Z, +) - группа целых чисел по сложению; здесь e = 0, a^{-1} = -a.

(R, *) - группа отличных от 0 действительных чисел по умножению; здесь e = 1,

a^{-1} - 1/a.

S_n - группа подтановок (симметрическая группа степени n) - группа биективных преобразований множества из n элементов с операцией композиции.

Замечание 2.1. Единица в группе всегда определена однозначно. Если e_1 и e_2 -единицы, то $e_1 = e_1e_2 = e_2$. Обратный элемент тоже определён однозначно. Если x и y - обратные к a, то x = x(ay) = (xa)y = y.

Основные алгебраические структуры

Определение 2.3. Кольцо - это множество R с операциями сложения (+) и умножения (-), обладающее следующими свойствами:

1. (R, +) - абелева группа (называемая аддитивной группой кольца);
2. (ассоциативность умножения) для любых a, b, c ∈ R $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
3. (дистрибутивность) для любых a, b, c ∈ R $a \cdot (b + c) = ab + a \cdot c$ и $(b + c) \cdot a = b \cdot a + c \cdot a$.

Определение 2.4. Если в кольце R существует элемент 1, называемый единицей, такой что для любого a ∈ R

$a \cdot 1 = 1 \cdot a = a$,

то R называется кольцом с единицей; Если для любых a, b ∈ R

$a \cdot b = b \cdot a$,

то R называется коммутативным кольцом. Все кольца, которые у нас появятся, будут коммутативными, но свойства, связаные с коммутативностью, всё-таки будут оговариваться.

Примеры. Z - кольцо целых чисел;

- 2Z - кольцо целых чётных чисел (кольцо без единицы);
- R[x] - кольцо многочленов от переменной x с коэффициентами из кольца R.
- $R[[x]] = \{a_0 + a_1x + \ldots + a_nx^n + \ldots\}$ - кольцо формальных степенных рядов с переменной x с коэффициентами из кольца R.
- Множество всех функций $f : R \to R$.

Основные алгебраические структуры

Определение 2.5. Элемент a^{-1} кольца с единицей называется обратным к элементу a, если

$aa^{-1} = a^{-1}a = 1$.

(В коммутативном кольце достаточно требовать, чтобы $aa^{-1} = 1$.)

Элементы, для которых существуют обратные, называются обратимыми.

Определение 2.6. Полем называется коммутативное кольцо с единицей, в котором каждый ненулевой элемент обратим.

Замечание 2.2. Кольцо, состоящее из одного нуля, не считается полем. Таким образом, в поле всегда есть по крайней мере два различных элемента: 0 и 1.

Примеры. Q - поле рациональных чисел;

R - поле действительных чисел;

C - поле комплексных чисел;

F(x) - поле рациональных функций от переменной x над полем F.

Кольцо Z_m

Теорема 2.1. Множество классов вычетов по модулю m с операциями (3.1) является коммутативным кольцом с единицей.

Определение 2.7. Это кольцо называется кольцом классов вычетов по модулю m и обозначается Z_m

Доказательство. Нулевым элементом этого кольца является класс $\bar{0}$: для любого $\bar{a}$

$$\bar{a} + \bar{0} = \overline{a + 0} = \bar{a}, \qquad \overline{0 + a} = \bar{0} + \bar{a} = \bar{a}.$$

Единицей - класс вычетов $\bar{1}$:

$$\bar{a} \cdot \bar{1} = \overline{a \cdot 1} = \bar{a}, \bar{1} \cdot \bar{a} = \overline{1 \cdot a} = \bar{a}.$$

Ассоциативность умножения классов вычетов следует из ассоциативности умножения целых чисел:

$$\bar{a}(\bar{b}\bar{c}) = \bar{a}\overline{bc} = \overline{a(bc)} = \overline{(ab)c} = (\overline{ab})\bar{c} = (\bar{a}\bar{b})\bar{c}.$$

Доказательство дистрибутивности и коммутативности проводится аналогично.

Лемма 2.1. Множество всех обратимых элементов кольца образует мультипликативную группу.

Доказательство. Если a и b обратимы, то в качестве обратного к ab выступает элемент $(ab)^{-1} = b^{-1}a^{-1}$.

$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$.

Остальные аксиомы группы выполняются по очевидным причинам.

Кольцо Z_m

Определение 2.8. Множество всех обратимых элементов кольца R называется группой обратимых элементов (или группой единиц) и обозначается R*.

Эта группа всегда непустая, так как содержит по крайней мере единицу кольца. Для нас важным объектом будет группа Z_m - группа обратимых элементов кольца Z_m. Как показывает следующий результат, она представляет собой приведённую систему вычетов по модулю m с операцией умножения.

Теорема 2.2. $Z_m^* = \{\bar{x} \in Z_m : (x, m) = 1\}$.

Доказательство. Если (x, m) = 1, то (Лекция 17) найдутся такие u и v, что xu + mv = 1. Значит, xu = 1 (mod m), и класс x обратим. Если же (x, m) = d > 1, то равенство xu + mv = 1 невозможно, и класс x необратим.

Следствие 2.1. Кольцо Zm является полем тогда и только тогда, когда m – простое число.

Кольцо Z_p

Теорема 2.3 (Деление многочленов с остатком). Пусть P(x) и Q(x) - многочлены с коэффициентами из некоторого поля F, и deg Q(x) > 0. Тогда существуют многочлены T(x) и R(x) такие, что

P(x) = Q(x)T(x) + R(x), и deg R(x) < deg Q(x).

При этом многочлены T(x) и R(x) определяются однозначно.

Доказательство. Доказательство проведём индукцией по степени многочлена P(x). Пусть deg P(x) = n, deg Q(x) = n, $P(x) = a_n x^n + \ldots$, $Q(x) = b_m x^m + \ldots$

Если n < m, то достаточно положить T(x) = 0, R(x) = P(x). Предположим, что утверждение теоремы доказано для всех многочленов P(x), степень которых меньше n. Поскольку степень многочлена $P_1(x) = P(x) - Q(x)a_n b_m^{-1} x^{n-m}$ меньше n, к нему можно применить предположение индукции и получить представление

$P_1(x) = Q(x)T_1(x) + R_1(x)$, где deg $R_1(x)$ < m. Значит, $P(x) - Q(x)a_n b_m^{-1} x^{n-m} = Q(x)T_1(x) + R_1(x)$ и $P(x) = Q(x)T(x) + R(x)$, где R(x) = $R_1(x)$ и T(x) = $T_1(x) + a_n b_m^{-1} x^{n-m}$.

Для доказательства единственности предположим, что возможно два представления:

$P(x) = Q(x)T_1(x) + R_1(x) = Q(x)T_2(x) + R_2(x)$.

Остатки $R_1(x)$ и $R_2(x)$ должны быть различными, т.к. в противном случае будут совпадать и многочлены $T_1(x)$ и $T_2(x)$. Вычитая из одного представления другое, получаем, что

$Q(x)(T_1(x) - T_2(x)) = R_2(x) - R_1(x)$.

Но такое равенство невозможно, т.к. в правой части стоит многочлен, степень которого меньше m, а в левой части - многочлен, степень которого по крайней мере m.

Кольцо Z_p

Теорема 2.4 (Безу). Остаток от деления многочлена P(x) на x - a равен P(a).

Доказательство. По теореме 2.3 остаток от деления многочлена P(x) на (x-a) - это некоторая константа, то есть P(x) = (x - a)T(x) + c. Подставляя в это равенство x = a, находим, что значение этой константы равно P(a).

Следствие 2.2. Если a - корень многочлена P(x), то P(x) делится на x – a без остатка.

Теорема 2.5. Многочлен степени n над произвольным полем имеет не более n корней.

Доказательство. Если a_1, …, a_k - корни многочлена P(x), то, согласно следствию 2.2, многочлен P(x) имеет вид $P(x) = (x - a_1)\dots (x - a_k)T(x)$. Значит, $n = k + \deg T(x)$ и $k < n$.

Теорема 2.6 (Вильсон). Пусть p - простое число. Тогда $(p-1)! = -1 \pmod p$.

Доказательство. Корнями многочлена $x^{p-1} - 1 \in Z_p[x]$ являются все ненулевые числа поля Zp, то есть числа 1, 2, …, p - 1. Значит, над полем Z_p этот многочлен раскладывается на линейные множители

$x^{p-1} - 1 = (x - 1)(x - 2)\dots (x - p + 1)$.

Сравнивая коэффициенты при x^0 в обеих частях этого равенства, получаем сравнение $-1 = (-1)^{p-1}(p - 1)! \pmod p$, равносильное нужному.

Кольцо Z_p

Определение 2.9. Элементы a, b кольца R называют делителями нуля, если a · b = 0, но при этом a ≠ 0 и b ≠ 0.

Пример: 2,3 ∈ Z_6 – это делители нуля, поскольку в кольце Z_6 выполняется равенство 2 · 3 = 0.

Замечание 2.3. В поле нет делителей нуля.

Существование чисел Кармайкла показывает, что выполнение условия $a^n - 1 \equiv 1 \pmod n$ недостаточно для выяснения простоты n. Чтобы усилить это свойство заметим, что для простого n кроме сравнения $a^{n-1} \equiv 1 \pmod n$ выполняется сравнение $a^{\frac{n-1}{2}} \equiv \pm 1 (mod\, n)$. Далее, если $a^{\frac{n-1}{2}} \equiv 1 (mod\, n)$ и $\frac{n-1}{2}$ чётно, то $a^{\frac{n-1}{4}} \equiv \pm 1 (mod\, n)$ и т. д. В общем случае, верно, следующее утверждение.

Лемма 2.2. Пусть p > 2 - простое число, $p - 1 = 2^s \cdot d$, где d нечётно. Тогда для любого a ∈ $\boldsymbol{Z_p^*}$ выполняется одно из условий

- $a^d = 1 \pmod p$;
- существует r в пределах 0 < r < s - 1 такое, что $a^{2^r d} = -1\ (mod\, p)$.

Доказательство. Применяя последовательно формулу разности квадратов, приходим к разложению

$$a^{p-1} - 1 = (a^d - 1)(a^d + 1)(a^{2d} + 1)(a^{2^2 d} + 1) \ldots (a^{2^{k-1} d} + 1) = 0 (\mathrm{mod}\ \mathrm{p}).$$

В полученном произведении хотя бы одна из скобок должна быть нулём по модулю p.

Кольцо Z_p

Определение 2.10. Пусть n - нечётное составное число и $n - 1 = 2^s \cdot d$, где d нечётно, и $a \in Z_n^*$. Рассмотрим числа $x_r = a^{2^r d} \bmod n$. Число n называется сильно псевдопростым числом по основанию a, если либо $x_0 = 1$, либо найдется индекс r, $0 < r < s$, такой, что $x_r = -1$.

Пример. Посмотрим, как выглядят числа x, для конкретных значений n.

Например, если n = 89, то $n - 1 = 2^3 \cdot 11$. Выбирая основания a = 3,5, 11, 2, получим следующие значения:

a	a^{11}	a^{22}	a^{44}	a^{88}
3	37	34	-1	1
5	55	-1	1	1
11	-1	1	1	1
2	1	1	1	1

Если n = 25, то $n - 1 = 2^3 \cdot 3$. При a = 2,7 получим значения

a	a^3	a^6	a^{12}	a^{24}
2	8	14	21	16
7	18	-1	1	1

Таким образом число 25 - сильно псевдопростое по основанию 7, но не сильно псевдопростое по основанию 2.

Пример. Число n = 561 является числом Кармайкла, а значит, псевдопростым по основанию 2. Однако оно не является сильно псевдопростым по основанию 2.

Действительно, $n - 1 = 35 \cdot 24$, и $2^{35 \cdot 2^3} \equiv 1 \ (mod\ 561)$, а $2^{35 \cdot 2^2} = 67 \ (mod\ 561)$.

Кольцо Z_p

Алгоритм 2.1. Тест Миллера - Равина (тест сильной псевдопросты)

Вход: натуральное нечётное n.

Выход: один из двух ответов «n - составное» или «вероятно, n - простое».

1. Выбираем $b \in_r \{2, \ldots, n - 1\}$ и проверяем, что выполнено ли хотя бы одно из условий леммы 2.2. Если нет, то ответ «n - составное»

2. Если хотя бы одно из условий леммы 2.2, то ответ неопределён, тест можно повторить снова. После нескольких повторений выдаём ответ «вероятно, n - простое».

Теорема 2.7. Если тест сильной псевдопростоты выдает ответ «n – составное число», то n - составное число.

Доказательство. Утверждение теоремы следует из леммы 2.2.

Проведём анализ времени работы алгоритма четвертого вероятностного теста. Число b^t вычисляется за время $O(L^3(n))$, поскольку в алгоритме быстрого возведения в степень выполняется $O(L(d))$ умножений, $d < n$, и, так как длины умножаемых по модулю n чисел не превосходят $L(n)$, каждое умножение выполняется за время $O(L^2(n))$. После этого при вычислении последовательности x_r, $r = 1, 2, \ldots, s$ производится s возведений в квадрат, где также $s < L(n)$ и каждое возведение в квадрат выполняется за время $O(L^2(n))$. Таким образом, тест выполняется за время $O(L^3(n))$.

Кольцо Z_p

Определение 2.11. Для данного числа n через G_n множество оснований b, для которых число n оказывается сильно псевдопростым:

$$Gn = \{b \in Z_n^* : n \text{ сильно псевдопростое по основанию } b\}.$$

Следующий результат показывает, что множество Gn всегда достаточно мало.

Теорема 2.8 (Рабин). Пусть n > 9 - составное. Тогда $|G_n| < \varphi(n)/4$.

На практике для заданного числа n тест можно применить 100 раз, используя 100 случайно и независимо выбранных оснований b_i, $1 < b_i < n$. Если n составное, то по теореме Рабина тест определит это с вероятностью $> 1 - 4^{-100}$, и каждая проверка будет выполняться за полиномиальное время.

Замечание. Существует детерминированная версия вероятностного алгоритма 2.1, предложенная Миллером. Если $n \neq p^k$ ($k > 1$), то проверку достаточно сделать для простых b в пределах $2 < b < 70\ln^2 n$. Обоснование этого алгоритма опирается на расширенную гипотезу Римана. Константа 70 в последствии была заменена числом 2.

Изоморфизмы

Если какие-то математические объекты устроены одинаково, то говорят, что они изоморфны. В каждом случае фразе «устроены одинаково» нужно придать строгий математический смысл. Приведём определения изоморфизма наших основных алгебраических объектов - групп, колец и полей.

Определение 2.12. Две группы $(G_1, \circ)$ и $(G_2, *)$ называются изоморфными, если существует взаимно однозначное отображение $\varphi: G_1 \to G_2$ такое, что для любых $g, h \in G_1$ справедливо равенство $\varphi(g \circ h) = \varphi(g) * \varphi(h)$. Изоморфизм групп записывается в виде $G_1 \cong G_2$.

Про равенство φ(до h) = φ(g) * φ(h) говорят, что ф сохраняет операцию.

Примеры. Изоморфизм групп $(Z, +) \cong (2Z, +)$ задаётся отображением $\varphi: x \to 2x$.

Задача. (a) Пусть φ: G1 → G2 - изоморфизм групп. Докажите, что обратное отображение также является изоморфизмом.

(b) Докажите, что изоморфизм групп является отношением эквивалентности.

Все группы из одного класса можно рассматривать как различные конкретные реализации одной и той же абстрактной группы.

Изоморфизмы

Определение 2.13. Два кольца $(R_1, +, \cdot)$ и $(R_2, \oplus, \odot)$ называются изоморфными, если существует взаимно однозначное отображение $\varphi: R_1 \to R_2$ такое, что для любых $a, b \in R_1$ справедливы равенства

$\varphi(a + b) = \varphi(a) \oplus \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \odot \varphi(b)$.

Изоморфизм колец записывается также как и для групп: $R_1 \cong R_2$.

Прямым (или декартовым) произведением множеств M_1 и M_2 называется множество $M_1 \times M_2 = \{(x_1, x_2): x_1 \in M_1, x_2 \in M_2\}$, состоящее из всех упорядоченных пар элементов из M_1 и M_2.

Определение 2.14. Прямое произведение групп $(G_1, \bullet)$ и $(G_2, \circ)$ – это множество $G = G1 \times G2$ с операцией

$(x_1, x_2) * (y_1, y_2) := (x_1 \bullet y_1, x_2 \circ y_2)$.

Нетрудно проверить, что прямое произведение групп — это тоже группа. Ассоциативность операции в G следует из ассоциативности операций в G_1 и G_2. Роль нейтрального элемента играет пара (e_1, e_2), где e_1, e_2 - нейтральные элементы групп G_1 и G_2 соответственно. Обратным элементом к (x_1, x_2) будет $(x_1^{-1}, x_2^{-1},)$, где x_1^{-1}- обратный к x_1 в группе G_1, а x_2^{-1}, - обратный к x_2 в группе G_2.

Аналогично определяется прямое произведение колец.

Изоморфизмы

Следствие 2.3. Пусть $m_1, \dots, m_n$ целые попарно взаимно простые числа $m = m_1, \dots, m_n$. Тогда $Z_m^* \cong Z_{m_1}^* \times \cdots \times Z_{m_n}^*$ и

Доказательство. Поскольку кольца Z_m и $Z_{m_1} \times \cdots \times Z_{m_n}$, изоморфны, то изоморфны и группы обратимых элементов этих колец, то есть $Z_m^* \cong \left(Z_{m_1} \times \cdots \times Z_{m_n}\right)^*$. Остаётся заметить, что $\left(Z_{m_1} \times \cdots \times Z_{m_n}\right)^* = Z_{m_1}^* \times \cdots \times Z_{m_n}^*$. Это верно, поскольку элемент кольца Z_m обратим тогда и только тогда, когда он обратим по каждому из модулей $m_1, \dots, m_n$.

Следствие 2.4. Пусть $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ - каноническое разложение числа n на множители. Тогда значение функции Эйлера на этом числе можно найти по формуле

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right).$$

Изоморфизмы

Доказательство. Согласно следствию 2.3, $Z_n^* \cong Z_{p_1^{\alpha_1}}^* \times \cdots \times Z_{p_s^{\alpha_s}}^*$ Поэтому

$$\varphi(n) = \varphi\left(p_1^{\alpha_1}\right) \ldots \varphi\left(p_s^{\alpha_s}\right)$$

На степенях простых чисел значение функции Эйлера находится по определению. Если p - простое число, и a ≥ 1, то на отрезке от 1 до p^a есть p чисел, не взаимно простых с p. Поэтому $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$. Подставляя в равенство $\varphi(n)$ равенство $\varphi(p^{\alpha_i}) = p_i^{a_i}\left(1 - \frac{1}{p_i}\right)$,олучаем утверждение следствия.

Равенство означает, что функция Эйлера принадлежит классу мультипликативных функций.

Определение 2.16. Функция f : N → C называется мультипликативной, если она удовлетворяет двум условиям:

f(1) = 1 и f(m · n) = f(m) · f(n) при (m, n) = 1.

Криптосистема RSA

Криптосистема RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) - криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших простых чисел. В общем случае криптографическая система с открытым ключом (public-key cryptosystem или asymmetric cryptosystem) предполагает, что каждый участник имеет открытый ключ e (public key), и закрытый или секретный ключ d (private key). Эти ключи образуют «согласованную пару»: они позволяют построить пару взаимно обратных отображений Enc_e (encryption) - функция шифрования и Dec_d (decryption) – функция дешифровки. Функция Enc_e отображает множество всех допустимых сообщений M (m=message) в множество шифротекстов (c=ciphertext), которое может как совпадать с M так и отличаться от него. Функции должны удовлетворять условиям

1. для любого $m \in M$ выполнено равенство $Dec_d(Enc_e(m)) = m$;

2. для любого $c \in C$ выполнено равенство $Enc_e(Dec_d(c)) = c$.

Пара функций (Enc_e, Dec_d) должна обладать следующим свойством: знание функции Enc_e не даёт возможности по случайнлму шифротексту $c \in C$ найти сообщение $m \in M$ такое, что $Enc_e(m) = c$. Другими словами, знание секретного ключа s не позволяет найти соответствующий секретный ключ d.

Криптосистема RSA

В криптосистеме RSA алгоритм создания открытого и секретного ключей устроен следующим образом:

Алгоритм 2.2. Создание открытого и секретного ключей RSA

Вход: размер ключа.

Выход: Модуль n, открытая экспонента e и секретная экспонента d.

1. Выбираются два различных случайных простых числа p и q заданного размера (например, 1024 бита каждое).

2. Вычисляется их произведение $n = p \cdot q$ (модуль).

3. Вычисляется значение функции Эйлера от числа n: $\varphi(n) = (p - 1) \cdot (q - 1)$.

4. Выбирается целое число e в пределах $1 < e < \varphi(n)$, взаимно простое с $\varphi(n)$.

5. Находится число d, мультипликативно обратное к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее сравнению $de = 1 \pmod{\varphi(n)}$.

6. Пара (e, n) публикуется в качестве открытого ключа RSA.

7. Число d играет роль секретного ключа RSA и хранится в секрете.

Криптосистема RSA

Число e называется открытой экспонентой (public exponent). Обычно в качестве e берут простые числа, содержащие небольшое количество единичных бит в двоичной записи, например, простые числа Ферма (17, 257 или 65537). В этом случае время, необходимое для шифрования с использованием быстрого возведения в степень, будет меньше. Слишком малые значения e, например 3, потенциально могут ослабить безопасность схемы RSA. Число d называется секретной экспонентой (private key exponent). Обычно оно вычисляется при помощи расширенного алгоритма Евклида.

Сообщениями в криптосистеме RSA являются числа $m \in M = Z_n$. Шифротексты – числа из того же кольца ($C = M = Z_n$). Функции шифрования и дешифровки имеют вид:

$Enc_e(m) = m^e \bmod n$,

$Dec_d(c) = c^d \bmod n$.

Шифрование. Предположим, Боб хочет послать Алисе сообщение m. Тогда он должен взять открытый ключ Алисы (e, n) и вычислить шифротекст $c = Enc_e(m) = m^e \bmod n$.

Дешифровка. Алиса, получив шифротекст Боба c восстанавливает сообщение по формуле $m = Dec_d(c) = c^d \bmod n$.

Криптосистема RSA

Теорема 2.10. Функции Enc_e и Dec_d взаимно обратны: для любого $x \in Z_n$

$Dec_d(Enc_e(x)) = x$, $Enc_e(Dec_d(x)) = x$.

Доказательство. По определению

$Dec_d(Enc_e(x)) = Enc_e(Dec_d(x)) = x^{ed} \bmod n$.

Значит, для доказательства теоремы необходимо проверить, что для любого $x \in Z_n$ выполняется сравнение $x^{ed} = x \pmod n$. По определению d это сравнение можно переписать в виде

$$x^{t\varphi(n)+1} = x\ (mod\ n),$$

где t - некоторое целое число. Если (x, n) = 1, то справедливость этого сравнения следует из теоремы Эйлера. Сравнение очевидно, если $x = 0 \pmod n$. Поэтому остаётся рассмотреть случаи, когда (x, п) ≠ 1, п. Такая ситуация возможна, если x делится на одно из чисел p, q и не делится на другое. Без ограничения общности будем считать, что (x, n) = p. Сравнение $x^{t\varphi(n)+1} = x\ (mod\ n)$ равносильно системе из двух сравнений

$$x^{t\varphi(n)+1} = x\ (mod\ p), x^{t\varphi(n)+1} = x\ (mod\ q).$$

Первое из них очевидно, поскольку обе части делятся на p. Второе следует из малой теоремы Ферма:

$$x^{t\varphi(n)+1} = x^{t(p-1)(q-1)+1} = x(x^{q-1})^{t(p-1)} = x\ (mod\ q).$$

Криптосистема RSA

Цифровая подпись RSA. Предположим, что Алисе нужно отправить Бобу сообщение m, подтверждённое электронной цифровой подписью s = Sign(m) (signature). В качестве подписи Алиса может использовать число $s = Sign(m) = Dec_d(m)$ - сообщение m, зашифрованное секретным ключом Алисы. Алиса передаёт Бобу пару (m, s), а Боб проверяет правильность подписи, сравнивая m и $Enc_e(s)$.

Правильность подписи может проверить каждый, кто имеет доступ к паре (m, s). Если передаваемые числа дополнительно зашифровать открытым ключом Боба, то проверить правильность подписи сможет уже только Боб. Вместо подписи $Sign(m) = Dec_d(m)$ можно использовать подпись $Sign(m) = Dec_d(H(m))$, где H(m) – некоторая хеш-функция.

Подгруппы и смежные классы

Определение 2.17. Подгруппой группы G называется всякое подмножество $H \subset G$, удовлетворяющее следующим условиям:

1. если $a, b \in H$, то $ab \in H$;

2. если $a \in H$, то $a^{-1} \in H$;

3. $e \in H$.

Очевидно, что любая подгруппа сама является группой относительно той же операции.

Пример. $(2Z, +)$ - подгруппа чётных чисел в группе $(Z, +)$.

Определение 2.18. Группы, состоящие из конечного числа элементов, называют конечными. Число элементов конечной группы G называется порядком группы и обозначается $|G|$.

В дальнейшем нем понадобится следующее простое, но очень полезное утверждение.

Подгруппы и смежные классы

Теорема 2.11 (Лагранж). Порядок подгруппы конечной группы делит порядок группы.

Доказательство. Пусть $H \subset G$ и $g \in G$. Обозначим через gH множество, определяемое равенством $gH = \{gh : h \in H\}$ - (левый) смежный класс группы G по подгруппе H. Проверим, что любые два смежных класса либо совпадают, либо не пересекаются. Действительно, если $g \in g_1H \cap g_2H$, то для некоторых $h_1, h_2 \in H$ выполняется равенство $g = g_1h_1 = g_2h_2$. Значит, $g_1 = g_2h$, где $h = h_2h_1^{-1} \in H$, и, следовательно, $g_1H = g_2hH = g_2H$. Таким образом, множество G является объединением всех смежных классов группы G по подгруппе H. Учитывая, что число элементов любого смежного класса равно $|H]$, получим $|G| = n \cdot |H]$.

Определение 2.19. Число $[G : H] = |G|/|H]$ называется индексом подгруппы H в группе G. Другими словами $[G : H]$ – это число смежных классов в группе G по подгруппе H.

Циклические группы

В любой группе могут быть определены степени элемента:

$$g^k = \begin{cases} gg \dots g\ (k \text{ штук}), \text{если } k > 0; \\ e, \text{если } k = 0; \\ g^{-1}g^{-1} \dots g^{-1}\ (k \text{ штук}), \text{если } k < 0. \end{cases}$$

Из этого определения сразу следует, что для любых целых k, l выполняется равенство

$g^k g^l = g^{k+1}$. Кроме того, $(g^k)^{-1} = g^{-k}$, и по определению $e = g^0$. Таким образом, степени элемента $g \in G$ образуют подгруппу в G.

Определение 2.19. Подгруппа, порождённая элементом $g \in G$ называется, циклической подгруппой и обозначается $\langle g \rangle$.

Возможны два случая: либо все степени g различны, либо нет. В первом случае группа $\langle g \rangle$ бесконечна. Во втором случае, если $g^l = g^k$, то $g^{k-l} = e$, и для некоторого натурального m будет выполняться равенство $g^m = e$.

Определение 2.20. Группа G называется циклической, если существует такой элемент $g \in G$, что $G = \langle g \rangle$. Всякий такой элемент называется порождающим (образующим) элементом группы G.

Если требуется указать порядок циклической группы, то используются обозначения $G = \langle g \rangle_n$, (если $|G| = n < \infty$) и $G = \langle g \rangle_\infty$ (если $|G| <= \infty$).

Примеры. (Z, +) - циклическая группа, порождаемая элементом 1

Циклические группы

Теорема 2.12. Пусть G = $\langle g \rangle_n$. Элемент g^k (0 < k < n - 1) будет образующим элементом группы G тогда и только тогда, когда (k, n) = 1. Число образующих элементов группы G равно φ(n).

Доказательство. Если d = (k,n) > 1, то $\left(g^k\right)^{\frac{n}{d}} = \left(g^{\frac{k}{d}}\right)^n = e$, и поэтому элемент g^k не является образующим. Если же (k, n) = 1, то для некоторых u и v выполняется равенство uk + nv = 1. Следовательно $\left(g^k\right)^u = g^{1-nv} = g$. Значит, степени g^k порождают всю группу G.

Число образующих элементов группы G равно количеству чисел к от 0 до n – 1 взаимно простых с n, и поэтому равно φ(n).

Следствия теоремы Лагранжа

Следствие 2.5. Порядок любого элемента конечной группы делит порядок группы.

Доказательство. Порядок элемента равен порядку порождаемой им циклической подгруппы, и по теореме Лагранжа делит порядок группы.

Замечание. Теорема Эйлера, которую мы доказали используя свойства сравнений, является частным случаем этого утверждения. Ранее функцию Эйлера φ(m) мы определяли как количество чисел от 1 до m, взаимно простых с m. По-другому функцию φ(m) можно определить как порядок группы Z_m^*: φ(m) = $|Z_m^*|$. Поэтому, если a лежит в Z_m^*, то порядок элемента a должен делить порядок этой группы, то есть $a^{\varphi(m)} \equiv 1 \, (mod \, m)$.

Ранее мы отмечали, что для чисел Кармайкла тест «Ферма» крайне неэффективен. Проверим, что для всех остальных чисел он работает достаточно хорошо. Ключом к доказательству будет служить теорема Лагранжа.

Следствия теоремы Лагранжа

Теорема 2.13. Пусть n - нечетное составное число. Тогда

1. n псевдопростое по основанию a в том и только том случае, когда (a, n) = 1 и порядок элемента a в Z_n^* делит число n - 1;

2. если n псевдопростое по основаниям a, b$\in Z_m^*$, то n псевдопростое по основаниям ab и ab^{-1}.

3. множество $|H_n| = \{a \in Z_n : a^{n-1} \equiv 1 \pmod n\}$ образует подгруппу мультипликативной группы

4. если n не является псевдопростым хотя бы по одному основанию a $\in Z_n^*$,

$$|H_n| \le \frac{Z_n^*}{2} = \frac{\varphi(n)}{2} < \frac{n-1}{2}$$

Эта теорема означает, что если n не является числом Кармайкла, то тест «Ферма» даёт ответ «не удалось определить» с вероятностью меньшей 1/2.

Первообразные корни и индексы

Определение 2.19. Пусть m > 2, a ∈ Z и (a, m) = 1. Наименьшее натуральное d с условием $a^d \equiv 1 \pmod m$ - показатель a. a - первообразный корень по модулю m, если показатель a равен φ(m). Два первообразных корня a и b считаются различными, если $a \neq b \pmod m$.

Существование первообразного корня равносильно цикличности группы Z_m^*

Примеры. Первообразные корни по модулю 5 – это 2 и 3, по модулю 9 – 2 и 5, по модулю 10 – это 3 и 7.

Теорема 2.14 (критерий первообразного корня). Для того, чтобы число g было первообразным корнем по модулю m необходимо и достаточно, чтобы для любого простого числа p, делящего φ(m) выполнялось условие

$$g^{\frac{\varphi(m)}{p}} \neq 1 (mod\ p)$$

Доказательство. В одну сторону утверждение теоремы очевидно, поскольку по определению первообразный корень по модулю m в степенях, меньших чем φ(m) отличен от единицы.

Если $\varphi(m) = q_1^{\alpha_1} \dots q_s^{\alpha_s}$ – каноническое разложение числа ф(m) на множители, и g - не первообразный корень, то порядок элемента g в группе Z_m^* является числом вида $q_1^{\beta_1} \dots q_s^{\beta_s}$, где $0 \leq \beta_i \leq \alpha_i$ при i = 1,…,s, и хотя бы для одного номера i_0 выполняется строгое неравенство $\beta_{i_0} < \alpha_{i_0}$. Но тогда $g^{\frac{\varphi(m)}{p_{i_0}}} = 1$.

Первообразные корни и индексы

Теорема 2.15. Группа Z_m^* является циклической тогда и только тогда, когда m - одно из чисел вида m = 2, 4, p^a, $2p^a$, где p > 2 - простое число.

Существование первообразного корня по модулю простого числа p равносильно цикличности группы Z_p^* = Zp \{0} - мультипликативной группы поля Z_p.

Частичное доказательство этой теоремы будет разобрано на семинарах.

Определение 2.20. Пусть m > 2, (a, m) = 1 и (b, m) = 1. Число s называется индексом (дискретным логарифмом) b по основанию a, если $a^s = b \pmod m$.

Для индексов (дискретных логарифмов) используется обозначение $s = \mathrm{ind}_a b = \log_a b$. Если в качестве основания взять число a, не являющееся первообразным корнем по модулю m, то индексы будут существовать не для всех чисел b, взаимно простых с m. Если же g - первообразный корень, то для любого $b \in Z_m^*$ существует $s = \mathrm{ind}_a b$.

Лемма 2.3 (свойства индексов). Пусть m ≥ 2 и g - первообразный корень по модулю m. Тогда

1° если (b,m) = 1 и $b = c \pmod m$, то $\mathrm{ind}_g b = \mathrm{ind}_g c$;

2° если (a, m) = (b, m) = 1, то $\mathrm{ind}_g(ab) = \mathrm{ind}_g a + \mathrm{ind}_g b \pmod{\varphi(m)}$;

3° если (a, m) = (b, m) = 1, to $\mathrm{ind}_g(ab^{-1}) = \mathrm{ind}_g a - \mathrm{ind}_g b \pmod{\varphi(m)}$;

4° Если g' - ещё один первообразный корень по модулю m, то $\mathrm{ind}_{g'} a = \mathrm{ind}_{g'} g \mathrm{ind}_g a$.

Односторонние функции

Определение 2.21. Односторонняя функция - математическая функция, которая легко вычисляется для любого входного значения, но трудно найти аргумент по заданному значению функции.

В этом определении слова «легко» и «трудно» понимаются с точки зрения теории сложности вычислений. Разница между сложностью прямого и обратного преобразований определяет криптографическую эффективность односторонней функции.

Односторонние функции можно понимать как трудно обратимые или необратимые. Существование односторонних функций до сих пор не доказано. Их существование докажет, что классы сложности P и NP не равны, попутно разрешив ряд вопросов теоретической информатики. Современная асимметричная криптография основывается на предположении, что односторонние функции всё-таки существуют.

Одним из претендентов в односторонние функции является отображение $x \rightarrow g^x \bmod p$, где p - простое, и g - первообразный корень по модулю p. Вычисление обратной функции $DLP(p, g, g^x) = x \bmod (p - 1)$ называется задачей дискретного логарифмирования (discrete logarithm problem). В общем случае не известно алгоритмов, позволяющих эффективно решать эту задачу. Вычислительная сложность задачи дискретного логарифмирования лежит в основе стойкости криптосистем Диффи - Хеллмана и Эль-Гамаля.

Протокол Диффи - Хеллмана

Алгоритм 2.5. Создание общего секретного ключа

Вход: простое число p, первообразный корень д по модулю p.

Выход: общий секретный ключ К.

1. Алиса выбирает a $\in_R$ {1, 2, ..., p - 2), вычисляет A = g^a mod p и отправляет A Бобу.

2. Веб выбирает b $\in_R$ {1, 2, …, p - 2), вычисляет B = g^b mod p и отправляет B Алисе.

3. Алиса вычисляет общий секретный ключ K$\in Z_p^*$ по формуле K =B^a = g^{ab}

4. Боб вычисляет общий секретный ключ K $\in Z_p^*$ по формуле K = A^b = g^{ab}

Задача нахождения g^{ab} mod p по известным значениям (p, g, g^a, g^b) называется вычислительной задачей Диффи - Хеллмана2 (computational Diffie – Hellman problem), которая заключается в вычисления фуркции DH(p, g, да, gb) = gab mod p.

Стойкость протокола Диффи - Хеллмана обеспечивается (предполагаемой) сложностью решения этой задачи.

Криптосистема Эль-Гамаля

При создании общего секретного ключа криптосистема Эль-Гамаля работает так же как и протокол Диффи - Хеллмана.

Алгоритм 2.6. Создание ключа для шифрования Эль-Гамаля

1. Каждый участник A выбирает большое простое p, первообразный корень g по модулю p.

2. Затем A выбирает $x \in_R \{1, 2, \ldots, p - 2)$, вычисляет $h = g^x \bmod p$.

3. Открытый ключ участника A – это тройка (p, g, h), его секретный ключ x.

С помощью следующего алгоритма участник B, используя открытый ключ A x зашифровывает сообщение m. Затем A его расшифровывает.

Алгоритм 2.7. Шифрование Эль-Гамаля

1. Участник B получает открытый ключ (p, g, h) участника A. Выбирает $y \in_R \{1, 2, , p - 2\}$, вычисляет $c_1 = g^y \bmod p$ и $s = h^y \bmod p$.

2. По сообщению $m \in Z_p$ находится и $c_2 = ms \bmod p$.

3. Участнику A посылается шифротекст $c = Enc(m) = (c_1, c_2)$.

4. Участникк A восстанавливает сообщение по формуле $m = Dec_x(c_1,c_2) = c_2c_1^{-x} \bmod p$.

План лекции

Теория сравнений (продолжение)	Группы, кольца, поля	Решение практических задач
35 минут	35 минут	20 минут

Задача 1

Написать программу на С, которая вычисляет приближенное значение рационального числа с помощью его разложения в цепную дробь.

Решение:

Метод цепных дробей позволяет представить дробь в виде:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

Реконструкция приближения

Мы можем восстановить дробь, используя:

$$P_k = a_k P_{k-1} + P_{k-2}$$
$$Q_k = a_k Q_{k-1} + Q_{k-2}$$

Где:

- P_k, Q_k — числитель и знаменатель приближенной дроби.
- $P_{-1} = 0, P_0 = 1, Q_{-1} = 1, Q_0 = 0$

Решение

```c
#include <stdio.h>
// Функция разложения числа в цепную дробь
void continued_fraction(int numerator, int denominator, int terms[], int *size)
{
    int i = 0;
    while (denominator != 0)
    {
        terms[i++] = numerator / denominator;
        int temp = numerator % denominator;
        numerator = denominator;
        denominator = temp;
    }
    *size = i;
}
```

Шаг	Числитель (N)	Знаменатель (D)	частное	Остаток
1	22	7	3	1
2	7	1	7	0

$$\frac{22}{7} = 3 + \frac{1}{7}$$

Решение

```c
// Функция восстановления приближения дроби из цепной дроби
void fraction_approximation(int terms[], int size, int *num, int *den) {
    int P_prev = 0, P_curr = 1; // Начальные значения P
    int Q_prev = 1, Q_curr = 0; // Начальные значения Q
    for (int i = 0; i < size; i++) {
        int P_next = terms[i] * P_curr + P_prev;
        int Q_next = terms[i] * Q_curr + Q_prev;
        P_prev = P_curr;
        P_curr = P_next;
        Q_prev = Q_curr;
        Q_curr = Q_next;
    }
    *num = P_curr;
    *den = Q_curr;
}
```

Шаг	частное	P	Q
0	3	3 x 1 + 0 = 3	3 x 0 + 1 = 1
1	7	7 x 3 + 1 = 22	7 x 1 + 0 = 7

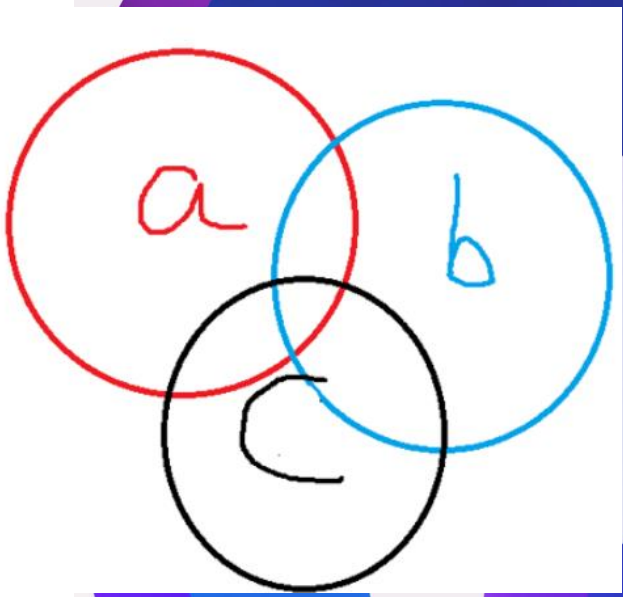
$$\frac{22}{7} = 3 + \frac{1}{7}$$

Решение

```c
int main(void) {
    int numerator, denominator;
    // Ввод числителя и знаменателя
    printf("Введите числитель и знаменатель: ");
    scanf("%d %d", &numerator, &denominator);
    int terms[100], size;
    // Разложение в цепную дробь
    continued_fraction(numerator, denominator, terms, &size);
    // Вывод цепной дроби
    printf("Цепная дробь: ");
    for (int i = 0; i < size; i++) {
        printf("%d ", terms[i]);
    }
    printf("\n");
    int approx_num, approx_den; // Восстановление приближения
    fraction_approximation(terms, size, &approx_num, &approx_den);
    printf("Приближенная дробь: %d/%d\n", approx_num, approx_den);
    printf("Приближение в виде десятичного числа: %.6f\n", (double)approx_num / approx_den);
    return 0;
}
```

Задача 2

Уродливое число — это положительное целое число, которое делится на a, b, или c.
Даны четыре целых числа n, a, b, и c, верните уродливое число .n^{th}



Пример 1:
Вход: n = 3, a = 2, b = 3, c = 5
Выход: 4
Пояснение: Некрасивые числа — 2, 3, 4, 5, 6, 8, 9, 10... Третье — 4.
Пример 2:
Ввод: n = 4, a = 2, b = 3, c = 4
Вывод: 6
Пояснение: Некрасивые числа — 2, 3, 4, 6, 8, 9, 10, 12... Четвертое — 6.
Пример 3:
Ввод: n = 5, a = 2, b = 11, c = 13
Вывод: 10
Пояснение: Некрасивые числа — 2, 4, 6, 8, 10, 11, 12, 13... Пятое число — 10.
Ограничения:
$1 <= n, a, b, c <= 10^9$
$1 <= a * b * c <= 10^{18}$
Гарантируется, что результат будет в пределах нормы .$[1, 2 * 10^9]$

Решение

```
int nthUglyNumber(int k, int A, int B, int C)
{
    int lo = 1, hi = 2 * (int)1e9;
    long a = long(A), b = long(B), c = long(C);
    long ab = a * b / __gcd(a, b);
    long bc = b * c / __gcd(b, c);
    long ac = a * c / __gcd(a, c);
    long abc = a * bc / __gcd(a, bc);
    while (lo < hi)
    {
        int mid = lo + (hi - lo) / 2;
        int cnt = mid / a + mid / b + mid / c - mid / ab - mid / bc - mid / ac + mid / abc;
        if (cnt < k)
            lo = mid + 1;
        else
            // the condition: F(N) >= k
            hi = mid;
    }
    return lo;
}
```

Задача 2 и 6 из пака - обсуждение

Решение

```
int nthUglyNumber(int k, int A, int B, int C)
{
    int lo = 1, hi = 2 * (int)1e9;
    long a = long(A), b = long(B), c = long(C);
    long ab = a * b / __gcd(a, b);
    long bc = b * c / __gcd(b, c);
    long ac = a * c / __gcd(a, c);
    long abc = a * bc / __gcd(a, bc);
    while (lo < hi)
    {
        int mid = lo + (hi - lo) / 2;
        int cnt = mid / a + mid / b + mid / c - mid / ab - mid / bc - mid / ac + mid / abc;
        if (cnt < k)
            lo = mid + 1;
        else
            // the condition: F(N) >= k
            hi = mid;
    }
    return lo;
}
```