Лекция
Элементы дискретной математики

- Лектор: профессор Яковлев В.А.

Модульная арифметика

$a:n = \begin{cases} c, \\ res\ (a) \end{cases}$ $a=cn+res(a)$

r=a(modn)

Переместительный закон (коммутативный)
(a+b)(modn)=(b+a)(modn)

Сочетальный закон (ассоциативный)
(a+(b+c))(modn)=((a+b)+c)(modn)

Распределительный закон

a(b+c)(modn)=ab(modn)+ac(modn)

(a+b)(modn)=[a(modn)+b(modn)](modn)
ab(modn)=[a(modn)b(modn)](modn)

Разложение на множители

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$$

p_i - различные простые числа

a_i - положительные целые числа

Пример:

$$n = 90 = 2 \cdot 3^2 \cdot 5$$

Число p называется простым, если оно не имеет делителей кроме тривиальных (1,-1, p, -p).

Наибольший общий делитель

- **Наибольшим общим делителем (НОД) двух чисел v и u называется наибольшее целое число, которое делит оба числа.**
- Нахождение НОД:
- Прямой метод - разложение чисел на множители.
  u=210 = 2•3•5•7, v=135=3•3•3•5. НОД(210,135)=15
- Алгоритм Евклида.

$u=a_1v+b_1$ — 210=1*135+75

$v=a_2b_1+b_2$ — 135=1*75+60

...

$b_{k-3}=a_{k-1}b_{k-2}+b_{k-1}$ — 75=1*60+**15**

$b_{k-2}=a_kb_{k-1}+b_k$ — 60=14*15+0

Если $b_k=1$, то НОД(u,v)=1,
если $b_k=0$, то НОД(u,v)= b_{k-1}

Числа u и v называются взаимопростыми, если НОД(u,v)=1

Теоремы Эйлера и Ферма

- **Функция Эйлера ϕ*(x)***. Определяет число натуральных чисел меньших *x* и взаимно простых с *x*. **ϕ*(1)=1***.
- **ϕ*(6)=2***. **ϕ*(xy)= ϕ(x)• ϕ(y)***. **ϕ*(p)=p-1,*** если p простое.
- **Теорема Эйлера:**
- *Если a и m взаимно простые числа,то*
- $a^{\varphi(m)}=1(modm)$ *a=5, m=6*

  $5^2(mod6)=25(mod6)=1$
- **Теорема Ферма:**
- *Если p простое число и p не делит a, то*
- $a^{p-1}=1(modp)$ *a=2, p=7*

  $2^6(mod7)=64(mod7)=1$

Обращение элемента по модулю n

Обратный элемент **x** к числу **a** - это такое целое число, которое удовлетворяет сравнению

$$xa \equiv 1 (mod n).$$

Обозначение обратного элемента - a^{-1}.

Обратный элемент существует только тогда, когда НОД (a,n)=1.

Пример. n=7,a=5. $a^{-1}=3$. 5•3=15, 15(mod7)=1.

Нахождение обратного элемента:

Известно представление НОД в виде

$$НОД(a,n)=z_1a+z_2n,$$

где z1,z2 –целые не обязательно положительные числа.

Так как НОД(a,n)=1, то

$1= (z_1a+z_2n) mod n=z_1a(mod n)$. Следовательно,

$a^{-1} =z_1 (mod n)$

Пример нахождения обратного элемента

n=17, a=13, a^{-1}=?

1. **и**спользуя алгоритм Евклида, находим НОД(17,13),

17=1*13+4

13=3*4+1, НОД=1

2. Найдем числа z_1 и z_2, удовлетворяющие условию:

1= (z1*13+z2*17)mod17=z1*13(mod17).

1=13-3*4

4=17-1*13

1=13-3*4=13-3*(17-1*13)=4*13-3*17

z1=4, z2=-3

3. a^{-1}= **z1=4**

4. Проверка 4*13(mod17)=52(mod17)=1

Пример 2

1. **и**используя алгоритм Евклида, находим НОД(97,77),

97=1*77+20
77=3*20+17
20=1*17+3
17=5*3+2
3=2*1+1, НОД=1

1=3-2*1 → 3-(17-5*3)*1=6*3-17*1=
2=17-5*3 =6*(20-1*17)-17*1=6*20-7*17=
3=20-1*17
17=77-3*20 =6*20-7*(77-3*20)=27*20-7*77=
20=97-1*77 =27*(97-77)-7*77=27*97-34*77

Получили представление
1=(z1*97+z2*77)mod97=z2*77(mod97)

a^{-1}= **z2=-34(mod97)= 63**

Проверка 63*77(mod97)=4851(mod97)=1

Возведение в степень

$y=a^x(\mathrm{mod} n)$

Прямой способ: $a\cdot a\cdot\ldots a\cdot a(\mathrm{mod} n)$

1. Быстрый способ возведения: **Пример:** $3^{37}(\mathrm{mod}7)$

Представим показатель степени в двоичном виде

$x=2^{k-1}x_{k-1}+2^kx_k+\ldots+2^2x_2+2^1x_1+2^0x_0$

$37=32+4+1=100101$

Найдем k степеней основания *a* путем последовательного возведения в квадрат a. $3^1=3(\mathrm{mod}7)$, $3^2=2(\mathrm{mod}7)$, $3^4=4(\mathrm{mod}7)$, $3^8=2(\mathrm{mod}7)$, $3^{16}=4(\mathrm{mod}7)$, $3^{32}=2(\mathrm{mod}7)$.

Перемножим между собой только те степени, которым соответствуют ненулевые коэффициенты в двоичном представлении числа x.

$3^1=3(\mathrm{mod}7)$, $3^4=4(\mathrm{mod}7)$, $3^{32}=2(\mathrm{mod}7)$.

$y=2\cdot4\cdot3(\mathrm{mod}7)=3$.

Возведение в степень

2. Быстрый способ возведения Д.Кнута.

- **представим показатель степени в двоичном виде;**
- **каждую единице заменим парой букв КУ (квадрат+умножение);**
- **каждый ноль заменим буквой К (квадрат);**
- **в образовавшейся последовательности вычеркнем первую пару КУ;**
- **над основанием а проводим вычисления, согласно полученной последовательности.**

Пример: $3^{37}(\mathrm{mod}7)$

37 = 100101 = КУККККУККУ= КККУККУ

$3\rightarrow 3^2(\mathrm{mod}7)=2\rightarrow 2^2(\mathrm{mod}7)=4\rightarrow 4^2(\mathrm{mod}7)=2\rightarrow 2\cdot 3(\mathrm{mod}7)=6\rightarrow 6^2(\mathrm{mod}7)=1\rightarrow 1^2(\mathrm{mod}7)=1\rightarrow 1\cdot 3(\mathrm{mod}7)=3$

Сложность вычислений для операции возведения в степень: $N\cong O(2\log x)$.

Вычисление дискретного логарифма

$\log_a y = x \pmod n$ $\qquad$ $y = a^x \pmod n$

Сложность вычислений для операции дискретного логарифмирования: $N \cong O((n)^{1/2})$.

Нахождение дискретного логарифма методом «встречи посредине»

Строим базу данных размера $O((n)^{1/2})$ вида $a^z \pmod n$ для случайных чисел $z \in [1,n]$ и сортируем ее.

- **Для случайных чисел b, таких что НОД(b,n-1)=1 вычисляем $y^b \pmod n$ и сравниваем с числами базы данных.**
- **С большой вероятностью после нескольких попыток получаем**

$$a^z \pmod n = y^b \pmod n$$

4. **Возводим обе части в степень b^{-1}, получим $a^{z \cdot b-1} \pmod n = y \pmod n$. Откуда следует**

$$zb^{-1} = x.$$

Этот метод имеет сложость $N_t \cong O((n)^{1/2} \log n)$, $N_v \cong O((n)^{1/2})$

Проверка чисел на простоту

Тест Ферма (вероятностный тест).

В его основе лежит теорема Ферма, т. е. если n- простое число и b взаимопростое с n, то $b^{n-1}=1(\mathrm{mod} n)$.

Для проверки нечетного числа n на простоту необходимо:

1. **Прогенерировать k' чисел b_i , i=1,2,…,k', $b_i<n$.**
2. **Проверить, что НОД(n, b_i)=1. Невзаимопростые с n числа отбросить. Остается k взаимопростых с n чисел. (для выполнения проверки используется алгоритм Евклида).**
3. **Проверить выполнение сравнения $b^{n-1}=1(\mathrm{mod} n)$ для i= 1,2,…. Если оно не выполняется хотя бы один раз, то n составное. Если выполняется для всех i, то n возможно простое**

Вероятность ошибки P(n-составное) $=1/2^k$

Тест не выполняется для так называемых псевдопростых чисел.

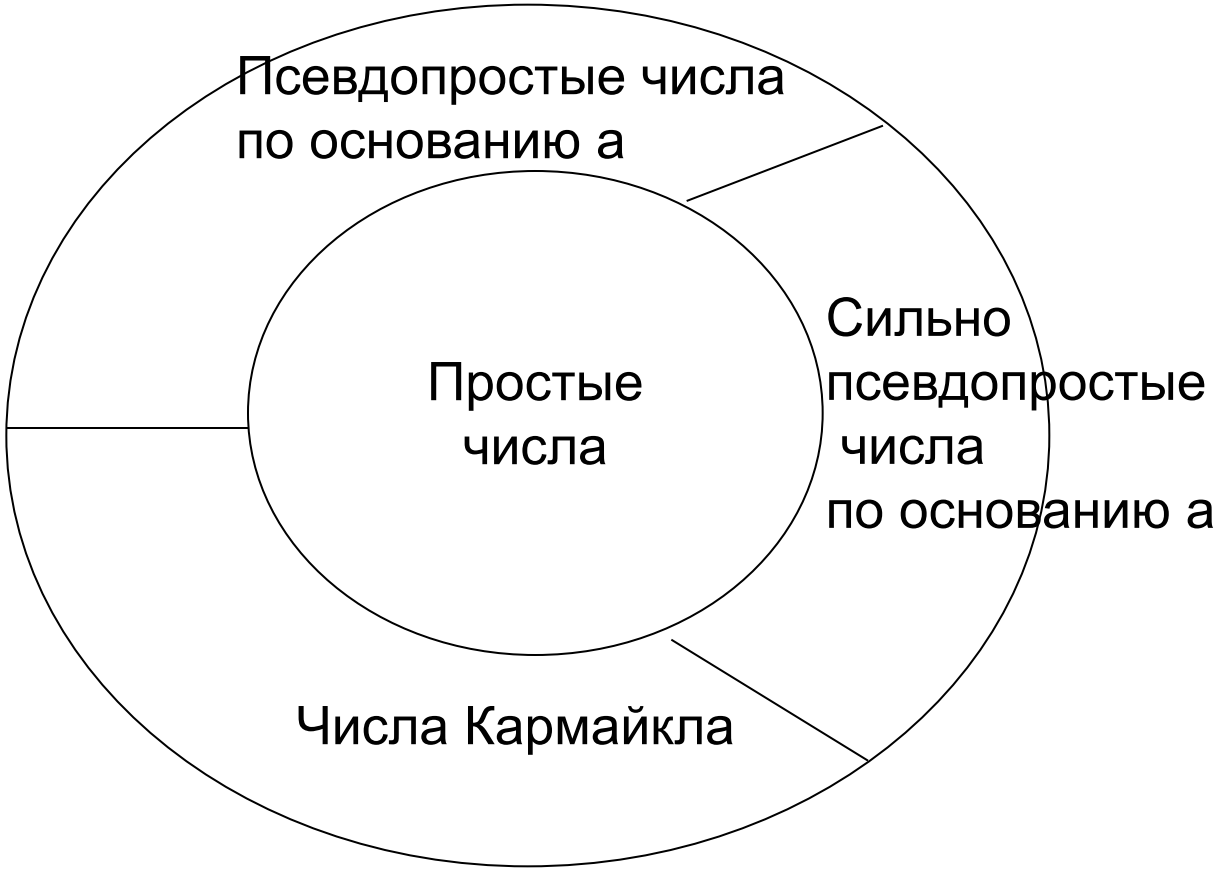
Тест Ферма

Пример. n=341, b=2.
$2^{340}=(2^{10})^{34}\text{mod}341=(1024(\text{mod}341))^{10}(\text{mod}341)=1$.
Но с другой стороны $341=31\cdot 11$, т.е. число составное.

Для любого b имеется бесконечно много **псевдопростых чисел,** однако их относительное количество не такое уж большое. Так для b=2 существует всего 21853 псевдопростых чисел среди чисел от 1 до $25\cdot 10^9$.

Особый случай составляют составные числа, условия т. Ферма для которых выполняются при любом b. Это **числа Кармайкла.**
Всего имеется 2163 числа Кармайкла в диапазоне 1 до $25\cdot 10^9$, а в диапазоне 1 до $1\cdot 10^5$ всего 16 таких чисел: 561,1105,1729….75361. В тесте Ферма эти числа не

Простые числа



нечетное. a – произвольное целое число.1≤a ≤n-1 взаимно простое с n.

- Число n называется сильно псевдопростым по основанию a, если $a^r \equiv 1 (\mathrm{mod} n)$ или если существует такое целое j, $0 \le j \le s-1$, что
- Пусть число *n* нечетное и $n-1=2^s r$, где *r* — нечетное. a – произвольное целое число.1≤a ≤n-1 взаимно простое с n.
- Число n называется сильно псевдопростым по основанию a, если $a^r \equiv 1 (\mathrm{mod} n)$ или если существует такое целое j, $0 \le j \le s-1$, что $a^{2^j r} \equiv -1 (\mathrm{mod}\, n)$

Тест Рабина- Миллера -

- Тест-Рабина-Миллера позволяет отсеять часть псевдопростых чисел

Вероятность ошибки для Теста Рабина-Миллера

$P(n\text{-составное}) < (1/4)^k$

Тест Миллера - Рабина

Пусть число n нечетное и $n - 1 = 2^s r$, где r — нечетное. Если n простое, то для любого $a \geq 2$, взаимно простого с n, выполняется условие. Разложим a^{n-1}-1 на множители

$$a^{n-1} - 1 = a^{2^s r} - 1 = (a^{2^{s-1} r} - 1)(a^{2^{s-1} r} + 1) =$$

$$= (a^{2^{s-2} r} - 1)(a^{2^{s-2} r} + 1)(a^{2^{s-1} r} + 1) = \ldots =$$

$$= (a^{2r} - 1)(a^{2r} + 1)\ldots(a^{2^{s-2} r} + 1)(a^{2^{s-1} r} + 1) =$$

$$= (a^{r} - 1)(a^{r} + 1)(a^{2r} + 1)\ldots(a^{2^{s-2} r} + 1)(a^{2^{s-1} r} + 1)$$

В последнем произведении хотя бы одна из скобок делится на n, то есть либо $ar \equiv 1 \pmod{n}$, либо среди чисел ar, $a2r$, …, $a2^{s-1}r$ найдется сравнимое с −1 по модулю n.

Вероятность ошибки для Теста Рабина-Миллера

$$P(\text{n-составное}) \leq (1/4)^k$$