

03.02.2025

Арифметика по модулю. Алгоритм Евклида. Цепные дроби. Вычеты.

Филиппов Михаил Витальевич

m.filippov@g.nsu.ru

89232283872

Императивное программирование, 2024-2025

N * Новосибирский
государственный
университет
***НАСТОЯЩАЯ НАУКА**

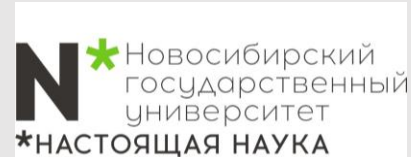


Давайте познакомимся



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

**Арифметика по
модулю**

25 минут

**Алгоритм
Евклида**

20 минут

Цепные дроби

25 минут

Сравнения

20 минут

План лекции

**Арифметика по
модулю**

25 минут

**Алгоритм
Евклида**

20 минут

Цепные дроби

25 минут

Сравнения

20 минут

Пример 1

```
bool checkSubarraySum(int* nums, int numsSize, int k) {  
}
```

Дан целочисленный массив **nums** и целое число **k**, вернуть, **true** если **nums** есть хороший подмассив, или **false** в противном случае .

Хороший подмассив — это подмассив, в котором:

- его длина составляет **не менее двух** , и
- сумма элементов подмассива кратна **k**.

Обратите внимание , что *подмассив* — это непрерывная часть массива.

Целое число **x** является кратным, если **k** существует целое число, **n** такое что **x = n * k**. **0** всегда кратно **k**

Пример 1:

Ввод: `nums = [23, 2, 4, 6, 7]`, `k = 6`

Вывод: `true`

Пояснение: `[2, 4]` — это непрерывный подмассив размера 2, сумма элементов которого равна 6.

Пример 2:

Ввод: `nums = [23, 2, 6, 4, 7]`, `k = 6`

Вывод: `true`

Пояснение: `[23, 2, 6, 4, 7]` — это непрерывный подмассив размера 5, сумма элементов которого составляет 42.

Число 42 кратно 6, поскольку $42 = 7 * 6$, а 7 — целое число.

Пример 3:

Ввод: `nums = [23,2,6,4,7]`, `k = 13`

Вывод: `false`

Ограничения:

- $1 \leq \text{nums.length} \leq 10^5$
- $0 \leq \text{nums}[i] \leq 10^9$
- $0 \leq \text{sum}(\text{nums}[i]) \leq 2^{31} - 1$
- $1 \leq k \leq 2^{31} - 1$

Пример 1

Сумма всех подмассивов чтобы найти и проверить делимость, какое это время?

$O(n^2)$

вычисление суммы для каждого подмассива сколько занимает?

$O(n)$

Таким образом, общая временная сложность равна $O(n^3)$

Префиксные суммы особенно полезны для вычисления суммы подмассивов. Сумма подмассива, начинающегося с индекса $i + 1$ и заканчивающегося j (включительно), вычисляется по формуле $\text{префикс}_j - \text{префикс}_i$, где префикс_i обозначает префиксную сумму до индекса i .

Надо, $(\text{prefix}[j] - \text{prefix}[i]) \% k = 0$.

$\text{prefix}[j] = Q1 \cdot k + R1$, $\text{prefix}[i] = Q2 \cdot k + R2$

$0 = (\text{prefix}[j] - \text{prefix}[i]) \% k = (Q1 \cdot k + R1 - Q2 \cdot k - R2) \% k = ((Q1 - Q2) \cdot k + R1 - R2) \% k = 0$

Очевидно, что $(Q1 - Q2) \cdot k$ кратно k

Следовательно, $(R1 - R2) \% k = 0$, то есть так как $R1$ и $R2 < k$, то $R1 = R2$

Пример 1

Поскольку нас интересует только модуль суммы префикса, мы начинаем с целого числа, `prefixMod` чтобы сохранить остаток от `prefixSum` с `k` постепенно. Мы можем найти самый длинный подмассив, который удовлетворяет вышеуказанным условиям, вычислив разницу между текущим индексом и первым индексом со значением `prefixMod`.

`nums` =

1	5	2	1	5	2	1	3
---	---	---	---	---	---	---	---

`k` = 5

`prefixSum` =

0	1	6	8	9	14	16	17	20
---	---	---	---	---	----	----	----	----

 Остаток от деления берем разницы

`prefixMod` =

0	1	1	3	4	4	1	2	0
---	---	---	---	---	---	---	---	---

 -> длина больше 1 – не берем

 -> Оба решения верны.

Пример 1

```
#include <unordered_map>
#include <algorithm>
#include <vector>
bool checkSubarraySum(std::vector<int> &nums, int k) {
    int prefixMod = 0;
    std::unordered_map<int, int> modSeen;
    modSeen[0] = -1;
    for (int i = 0; i < nums.size(); i++) {
        prefixMod = (prefixMod + nums[i]) % k;
        if (modSeen.find(prefixMod) != modSeen.end())
            // ensures that the size of subarray is atleast 2
            if (i - modSeen[prefixMod] > 1)
                return 1;
        else
            // mark the value of prefixMod with the current index.
            modSeen[prefixMod] = i;
    }
    return 0;
}
```

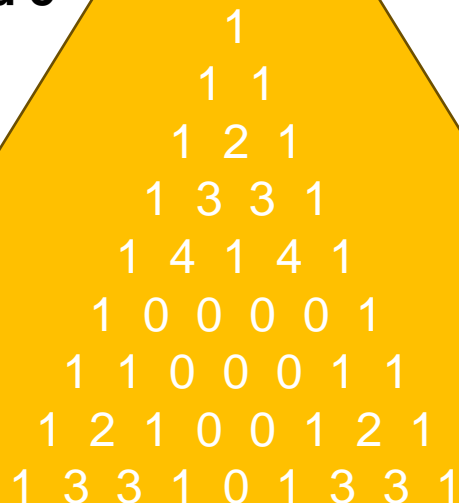

Пример 2

как вычислить $C(n, k) \bmod M$?

$C(n, k)$ - биномиальный коэффициент

$$C(n, k) = \frac{n!}{k! (n - k)!}$$

$\bmod 5$



```

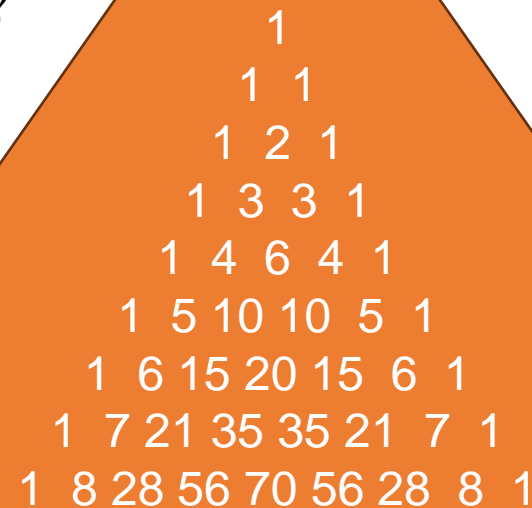
      1
     1 1
    1 2 1
   1 3 3 1
  1 4 1 4 1
 1 0 0 0 0 1
1 1 0 0 0 1 1
1 2 1 0 0 1 2 1
1 3 3 1 0 1 3 3 1
  
```

$$C(1, 1) = \frac{1!}{1! (1 - 1)!} = 1$$

$$C(8, 1) = \frac{8!}{1! (8 - 1)!} = 8$$

$$C(8, 5) = \frac{8!}{5! (8 - 5)!} = 56$$

$$C(1000, 674) \bmod 5 = ?$$



```

      1
     1 1
    1 2 1
   1 3 3 1
  1 4 6 4 1
 1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1
1 8 28 56 70 56 28 8 1
  
```

Чтобы вычислить треугольник Паскаля до n , нужно потратить $O(n^3)$ времени и памяти.

Если всегда брать сразу остаток от деления, то все числа фиксированного размера, длинная арифметика не нужна, время и память $O(n^2)$.

Пример 3

Вычисляем $10! \bmod 11$

В лоб!

$$10! \bmod 11 = 3\,628\,800 \% 11 = 10$$

А если не в лоб

$$1 \% 11 = 1$$

$$1 \cdot 2 \cdot 3 \cdot 4 \% 11 = 22 \% 11 = 2$$

$$4! \cdot 5 \% 11 = 2 \cdot 5 \% 11 = 10$$

$$5! \cdot 6 \% 11 = 10 \cdot 6 \% 11 = 5$$

$$6! \cdot 7 \% 11 = 5 \cdot 7 \% 11 = 2$$

$$7! \cdot 8 \% 11 = 2 \cdot 8 \% 11 = 5$$

$$8! \cdot 9 \% 11 = 5 \cdot 9 \% 11 = 1$$

$$9! \cdot 10 \% 11 = 1 \cdot 10 \% 11 = 10$$

Аналогично можно вычислить, например $x^3 - 17x^2 + 4x - 156$ по модулю $(10^9 + 7)$ при $x = 123456789$.

Чтобы вычислить "влоб" значение многочлена, нужны целые числа, вмещающие до 10^{27} --- в 64-битные не входит.

А если каждый промежуточный результат сразу брать по модулю $10^9 + 7$, тогда хватает 64-битных чисел.



Чётные и нечётные числа

Числа бывают чётные и нечётные. Чётные делятся на 2 без остатка, а нечётные дают остаток 1. Другими словами, чётные числа имеют вид $2k$ для целых k , а нечётные $2k + 1$, тоже при целых k .

Пример, число 0 чётное ($0 = 2 \cdot 0$), а число -3 нечётное ($-3 = 2 \cdot (-2) + 1$).

+	Ч	Н
Ч	Ч	Н
Н	Н	Ч

×	Ч	Н
Ч	Ч	Ч
Н	Ч	Н

Пример 2, если мы складываем чётное и нечётное число, то получаем $2k + (2l + 1) = 2(k + l) + 1$, то есть нечётное число. А если мы умножаем два нечётных числа, то получаем $(2k + 1)(2l + 1) = 4kl + 2k + 2l + 1 = 2(2kl + k + l) + 1$, то есть нечётное число.

Преподаватель со студентом играют в игру: каждый пишет на бумажке число, не говоря его другому, потом они открывают эти числа, и если произведение четное, студент получает 2, а если нечётное, то 5. Честная ли это игра?



Деление на 3 и остатки

Попробуем составить аналогичные таблицы сложения и умножения для чисел, делящихся и не делящихся на 3. Тут сразу же возникает проблема: мы не знаем, что сказать про сумму двух чисел, не делящихся на 3. Она может делиться на 3 (например, $1 + 5 = 6$), а может и не делиться (например, $2 + 5 = 7$). Дело в том, что не делящиеся на 3 числа могут быть двух видов: одни дают остаток 1 (имеют вид $3k + 1$ при целом k), а другие дают остаток 2 (имеют вид $3k + 2$).

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Каждую клеточку в этой таблице несложно проверить.

Пример,

$$(3k + 1) + (3l + 2) = 3(k + l) + 3 = 3(k + l + 1) + 0$$

и

$$(3k + 2)(3l + 2) = 9kl + 6k + 6l + 4 = 3(3kl + 2k + 2l + 1) + 1.$$



Деление с остатком

Определение: Пусть $a, b \in \mathbf{Z}$. Число a делится на число b если найдется такое число $q \in \mathbf{Z}$, что $a = qb$. Синонимы: a кратно b ; b – делитель a .

Запись: $a : b$ или $b \mid a$.

В этом случае говорят также $\langle a$ кратно $b \rangle$, и $\langle b$ является делителем числа $a \rangle$.

В этом определении можно было бы сказать: \langle если частное a/b целое \rangle , но этим бы исключался случай $b = 0$, который формально допустим по нашему определению. Правда, особого смысла в нём всё равно нет: единственное число, которое делится на 0, это число 0. Определение допускает также отрицательные a и b : скажем, число -6 делится на -2 (а также и на 2), всего у него 8 делителей, если считать и положительные, и отрицательные.

Что это за делители?

Впрочем, обычно, говоря о количестве делителей у положительного целого числа, имеют в виду только положительные делители (считая единицу и само число).

Пример: $30 = 2 \cdot 3 \cdot 5$; $210 = 2 \cdot 3 \cdot 5 \cdot 7$?

Говорить о кратных можно не только для целых чисел, но и для отрезков: один отрезок кратен другому, если второй укладывается в первом целое число раз, то есть если отношение (длина первого)/(длина второго) целое.

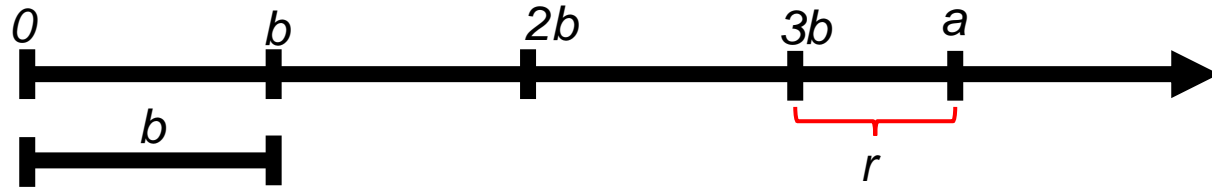


Деление с остатком

Теорема. Для данного целого отличного от нуля числа b , всякое целое число a единственным образом представимо в виде

$$a = bq + r, \text{ где } 0 \leq r < |b|.$$

Доказательство. Ясно, что одно представление числа a равенством $a = bq + r$ мы получим, если возьмем bq равным наибольшему кратному числа b , не превосходящему a



Тогда, очевидно, $0 \leq r < |b|$. Докажем единственность такого представления. Ну пусть $a = bq + r$ и $a = bq_1 + r_1$ — два таких представления. Значит $0 = a - a = b(q - q_1) + (r - r_1)$. Здесь 0 делится на b ; $b(q - q_1)$ делится на b , следовательно $(r - r_1)$ обязано делиться на b . Так как $0 \leq r < b$ и $0 \leq r_1 < b$, то $(r - r_1) < b$ и $(r - r_1)$ делится на b , значит $(r - r_1)$ равно нулю, а, значит и $(q - q_1)$ равно нулю, т.е. два таких представления совпадают. ■

Определение. Число q называется неполным частным, а число r — остатком от деления a на b .

Деление с остатком

!. Если два числа a и b делятся на третье число c , то и их сумма и разность делятся на это c .

Доказательство:

В самом деле, если $a = kc$ и $b = lc$, то $a + b = (k + l)c$ и $a - b = (k - l)c$.

!. Для делимости произведения достаточно делимости одного из сомножителей: если a делится на c , то и ab делится на c , каково бы ни было (целое) b . В самом деле, если $a = kc$, то $ab = k(bc) = (kb)c$.

С этого момента:

Пусть x , y - произвольные целые числа, и мы знаем их остатки:

$$a = x \bmod m \quad b = y \bmod m$$

Тогда можно зная только остатки (и не зная полностью числа) найти:

$$(x + y) \bmod m = a [+] b$$

$$(x - y) \bmod m = a [-] b$$

$$(x * y) \bmod m = a [*] b$$

Здесь $[+]$, $[-]$ и $[*]$ обозначают операции сложения, вычитания и умножения "по модулю". Их легко реализовать в программе:

```
a [+] b  return (a + b) % m;
```

```
a [-] b  return (a - b + m) % m;    //не забываем, что остаток от деления отрицательного  
числа на положительное в C обычно отрицательный!
```

```
a [*] b  return (a * b) % m;        //если a, b, m 32-битные, то нужно привести один из  
множителей к 64-битному типу, иначе будет переполнение
```

Деление с остатком

Можно заметить, что операции по модулю ведут себя во многом так же, как такие же операции над обычными целыми числами.

В частности:

$$a [+] b = b [+] a$$

//коммутативность сложения

$$a [+] (b [+] c) = (a [+] b) [+] c$$

//ассоциативность сложения

$$a [+] 0 = a$$

//прибавление нуля ничего не меняет

$$a [-] b [+] b = a$$

//вычитание обратно сложению

$$a [*] b = b [*] a$$

//коммутативность умножения

$$a [*] (b [*] c) = (a [*] b) [*] c$$

//ассоциативность умножения

$$a [*] 1 = a$$

//умножение на один ничего не меняет

$$(a [+] b) [*] c = (a [*] c) [+] (b [*] c)$$

//дистрибутивность

Если рассмотреть множество остатков с этими операциями:

$$\langle \{0, 1, 2, \dots, m-1\}, [+], [*] \rangle = \mathbb{Z}_m$$

Это называется кольцо вычетов по модулю m .

Определение. Множество целых чисел называют *идеалом*, если вместе с любыми двумя числами оно содержит их сумму и разность, и вместе с любым числом оно содержит все его кратные. Используя эту терминологию, можно сказать, что для любого s множество всех кратных числа s является идеалом. (Множество натуральных чисел)



Деление с остатком - примеры

Примеры:

- Докажите, что произведение любых трёх последовательных целых чисел делится на 3.

$$a + (a + 1) + (a + 2) = 3a + 3$$

- Докажите, что число $a^3 - a$ делится на 3 при любом целом a .

$$a^3 - a = a(a - 1)(a + 1)$$

- Известно, что a, b, c, d - положительные целые числа, и $ab = cd$. Докажите, что если a делится на c , то d делится на b .

$$a = kc$$

$$kcb = cd$$

$$d = kb$$

- Числа a и b целые, причём $2a + 3b$ делится на 7. Докажите, что $a + 5b$ также делится на 7.

$$2a \equiv -3b \pmod{7}$$

$$8a \equiv -12b \pmod{7}$$

$$a \equiv 2b \pmod{7}$$

$$a + 5b \equiv 2b + 5b \equiv 7b \equiv 0 \pmod{7}$$

- Д/З** Положительное целое число a чётно, но не делится на 4. Покажите, что количество (положительных) чётных делителей a равно количеству (положительных) нечётных делителей a .

План лекции

**Арифметика по
модулю**

25 минут

**Алгоритм
Евклида**

20 минут

Цепные дроби

25 минут

Сравнения

20 минут

Быстрое возведение в степень

Как вычислить $a^n = ?$

Предположим, что необходимо возвести число a в степень n .
Можно также рассматривать задачу о возведении в степень n элементах группы (G, \times)

Влоб: $a \cdot a \cdot a \cdot a \cdot a \dots a$ - работает примерно за n умножений.

Пример:

$$n = 169$$

$$a^{169} = a^{(128+32+8+1)} = a^{128} \cdot a^{32} \cdot a^8 \cdot a^1$$

$$a^1 = a$$

$$a^2 = a^1 \cdot a^1$$

$$a^4 = a^2 \cdot a^2$$

$$a^8 = a^4 \cdot a^4$$

$$a^{16} = a^8 \cdot a^8$$

$$a^{32} = a^{16} \cdot a^{16}$$

$$a^{64} = a^{32} \cdot a^{32}$$

$$a^{128} = a^{64} \cdot a^{64}$$

Получили вычисление a^{169} за 10 умножений.



Быстрое возведение в степень

Следующий алгоритм позволяет вычислять x^n за $O(\log n)$ умножений.

Алгоритм. Бинарный алгоритм возведения в степень

Вход: Элемент x группы G , натуральное $n = (n_{l-1} \dots n_0)_2$.

Выход: $x^n \in G$.

1. Полагаем $y \leftarrow 1, i \leftarrow l - 1$.
2. Пока $i > 0$ повторяем шаги 3-5.
3. $y \leftarrow y^2$
4. Если $n_i = 1$, то $y \leftarrow xy$
5. $i \leftarrow i - 1$.

Этот алгоритм основан на равенстве

$$x^{(n_{l-1} \dots n_{i+1} + n_i)_2} = \left(x^{(n_{l-1} \dots n_{i+1})_2} \right)^2 \cdot x^{n_i}$$

и выполняет возведение в степень за $b(n) = l + v(n) - 1$ умножений, где $v(n)$ – вес Хемминга числа n , то есть число единиц в двоичном представлении n .

Замечание. Говорят, что алгоритм работает за квазилинейное время, если на входных данных длины время его работы допускает оценку

$$T(n) = O(n \log^k n)$$

для некоторой константы k . Шёнхаге и Штрассен построили вариант алгоритма быстрого умножения, которые работают за квазилинейное время:

$$M(n) = O(n \log n \log \log n).$$



Быстрое возведение в степень

Время работы:

1) В Z длина числа растёт линейно с показателем степени, а умножение занимает квадратичное время.

Если оценивать время возведений в квадрат, оно будет:

$$T = (Cn/2)^2 + (Cn/4)^2 + (Cn/8)^2 + \dots + 1 = O(n^2)$$

Даже просто на последнем возведении в квадрат уже тратится $O(n^2)$ времени.

Если перемножать влоб, то тоже будет работать за $O(n^2)$ --- никакой выгоды!

2) В Z_n все остатки входят в наш тип данных, значит все умножения требуют $O(1)$ времени.

Общее время работы $O(\log n)$ - намного лучше времени $O(n)$ тривиального алгоритма.

Одно из основных приложений для быстрого возведения в степень - вычисление обратного по модулю.

Остаток x называется обратным по модулю к a , если $a [\cdot] x = 1$. Пишется: $x = \text{inv}(a)$.

Если у нас есть обратный элемент, то мы можем на него "делить":

$$a [/] b = a [\cdot] \text{inv}(b)$$

Причём будет верно обычное свойство:

$$a [/] b [\cdot] b = a$$



Алгоритм Евклида

Определение 2.2. Наибольшим общим делителем (НОД) целых чисел a_1, \dots, a_n называется наибольший из их общих делителей. НОД чисел a_1, \dots, a_n обозначается (a_1, \dots, a_n) .

Если наибольший общий делитель чисел a_1, \dots, a_n равен 1, то эти числа называются взаимно простыми.

Теорема 2.2 (Алгоритм Евклида). Пусть m_0 и m_1 - целые числа, $m_1 > 0$, $m_1 \nmid m_0$ и $d = (m_1, m_0)$. Тогда для некоторого $k > 1$ найдутся целые числа a_0, a_1, \dots, a_{k-1} и m_2, \dots, m_k такие, что $m_1 > m_2 > m_3 > \dots > m_k > 0$, $a_k > 1$, и

$$\left\{ \begin{array}{l} m_0 = m_1 a_1 + m_2 \\ m_1 = m_2 a_2 + m_3 \\ m_2 = m_3 a_3 + m_4 \\ \dots \dots \dots \\ m_{k-2} = m_{k-1} a_{k-1} + m_k \\ m_{k-1} = m_k a_k \end{array} \right.$$

При этом $m_k = d$.



Алгоритм Евклида

Как получается: легко видеть, что:

$$(a, b) = (b, a)$$

$$(a, 0) = a$$

$$(a, b) = (a-b, b)$$

Отсюда вытекает простой алгоритм Евклида:

вычитаем из большего числа меньшее, пока одно из них не станет нулём.

Пример: $\gcd(35, 90) = (90, 35) = (55, 35) = (20, 35) = (35, 20) = (15, 20) = (20, 15) = (5, 15) = (15, 5) = (10, 5) = (5, 5) = (5, 0) = 5$

На примере $a = 109, b = 3$ заметим, что время работы этого алгоритма $O(a + b)$.

Ускорим: будем делать все подряд идущие вычитания за одну операцию:

$$(a, b) = (a - q \cdot b, b) = (a \% b, b)$$

Получается более канонический алгоритм Евклида:

$$(a, b) = (b, a \% b) = \dots = (a, 0) = a$$

(продолжаем цепочку, пока не будет $b = 0$)

Можно легко реализовать рекурсивно:

```
int gcd(int a, int b) { return (b == 0 ? a : gcd(b, a%b)); }
```

Итоговое время: $O(\log(a + b))$ (**Доказательство – ДЗ**)



Алгоритм Евклида

Следствие. Наибольший общий делитель двух чисел можно представить в виде линейной комбинации этих чисел с целыми коэффициентами: для некоторых u и v выполняется равенство:

$$m_0u + m_1v = d.$$

Доказательство. Достаточно по индукции проверить, что для любого i от $k-1$ до 0 существуют числа u_i, v_i такие, что $u_im_i + m_{i+1}v_i = d$, где $d = (m_1, m_0)$.

При $i = 0$ получаем утверждение следствия.

Процесс последовательного нахождения пар (u_i, v_i) называется расширенным алгоритмом Евклида.

"Расширенный алгоритм Евклида" находит целые числа x и y , такие что:

$$a \cdot x + b \cdot y = \gcd(a, b)$$

Здесь:

- a и b задаются как входные данные,
- $\gcd(a, b)$ находит в том числе обычный алгоритм Евклида,
- x и y - дополнительные выходные данные расширенного алгоритма



Алгоритм Евклида

Для этого пишем рекурсивный алгоритм:

$\text{Euclid}(a, b) \rightarrow (g, x, y) \quad //g = \text{gcd}(a, b)$

Как работает расширенный алгоритм:

1) Если $b = 0$, то тривиально находим x, y и g .

2) Вызываем рекурсивно: $\text{Euclid}(b, a \% b) \rightarrow (g_1, x_1, y_1)$

3) По полученным из рекурсии значениям g_1, x_1 и y_1 восстанавливаем g, x, y , которые возвращаем наружу.

То к обычному алгоритму Евклида добавился пересчёт решения на выходе из рекурсии.

Чтобы понять, как пересчитывать, запишем уравнения для рекурсивного вызова:

$b \cdot x + r \cdot y = g = \text{gcd}(b, r) \quad //r = a \% b \text{ --- остаток}$

Мы уже знаем, что $g = \text{gcd}(b, r) = \text{gcd}(a, b) = g_1$.

Кроме того, остаток r можно выразить так:

$r = a - q \cdot b \quad //q \text{ - частное при делении } a \text{ на } b$

Подставляем это выражение в уравнение и перегруппировываем слагаемые:

$$b \cdot x + (a - q \cdot b) \cdot y = g$$

$$b \cdot x + a \cdot y - q \cdot b \cdot y = g$$

$$a \cdot y + b \cdot x - b \cdot q \cdot y = g$$

$$a \cdot y + b \cdot (x - q \cdot y) = g$$

Значит решение уравнения можно получить по формулам:

$$x_1 = y \qquad y_1 = x - q \cdot y$$

Алгоритм Евклида

Расширенный алгоритм Евклида можно применить для поиска обратного по модулю.

Если $\text{gcd}(a, m) = 1$ (взаимно просты), то запустив алгоритм найдем:

$$a \cdot x + b \cdot m = 1$$

Это равенство по модулю m выглядит так:

$$a [\cdot] x = 1$$

То есть $x = \text{inv}(a)$ --- обратный элемент.

Время работы $O(\log m)$, отлично работает даже для непростых m .

Кроме того, алгоритм возвращает $\text{gcd}(a, m)$, так что можно заодно узнать, есть обратный или нет.



Теорема Ламе

Следующее утверждение любопытно тем, что это редкий случай, когда, по существу, используется десятичная система счисления.

Теорема (Ламе). Пусть k - число шагов в алгоритме Евклида, применённом к числам m_0 и m_1 ($m_0 > m_1$) и $q = L_{10}(m_1)$ - количество цифр в десятичной записи числа m_1 . Тогда

$$k \leq 5q.$$

Лемма. Пусть алгоритм Евклида, примененный к числам m_0 и m_1 , состоит из k шагов. Тогда $m_1 \geq F_{k+1}$. F – число Фибоначчи.

Доказательство. Так как $m_k \geq 1$ и $a_{k-1} > 1$, то можно записать неравенства

$$m_k \geq F_2 = 1, m_{k-1} \geq F_3 = 2.$$

Далее, по индукции, легко проверить неравенство

$$m_{k-j} \geq F_{j+2} \quad (j = 0, 1, \dots, k).$$

Утверждение леммы получается из оценки подстановкой $j = k - 1$.

Следствие. Если в алгоритме Евклида $m_1 < F_{n+1}$, то для числа шагов k выполняется оценка $k \leq n - 1$.



Теорема Ламе

Лемма. При любом целом $q \geq 0$ выполняется неравенство $L_{10}(F_{5q+2}) \geq q + 1$.

Доказательство. При $q = 0, 1, 2$ утверждение леммы легко проверить непосредственно:

n	1	2	3	4	5	6	7	8	9	10	11	12
F_n	1	1	2	3	5	8	13	21	34	55	89	144

Для доказательства леммы покажем сначала, что при $s \geq 2$ существует не более 5 чисел Фибоначчи, имеющих s цифр. Пусть F_n - первое из чисел Фибоначчи, имеющее s цифр. Тогда из неравенства $F_n < 2F_{n-1}$ находим, что

$$F_n \geq 10^{s-1} \quad (1)$$

$$F_{n-1} > 0.5F_n$$

Покажем, что $L_{10}(F_{n+5}) > s + 1$. Из неравенств (1) получаем:

$$F_{n+1} = F_n + F_{n-1} > 1.5F_n > 1.5 \cdot 10^{s-1}$$

$$F_{n+2} = F_{n+1} + F_n > 2.5 \cdot 10^{s-1}$$

$$F_{n+3} = F_{n+2} + F_{n+1} > 4 \cdot 10^{s-1},$$

$$F_{n+4} = F_{n+3} + F_{n+2} > 6.5 \cdot 10^{s-1}$$

$$F_{n+5} = F_{n+4} + F_{n+3} > 10.5 \cdot 10^{s-1} > 10^s,$$

поэтому

$$L_{10}(F_{n+5}) \geq s + 1.$$

Следовательно, после увеличения номера на 5 количество цифр в записи чисел Фибоначчи обязательно увеличивается, что и доказывает лемму.

Теорема Ламе

Доказательство теоремы Ламе. Обозначим через q количество цифр в числе m_1 . По лемме

$$L_{10}(m_1) = q < L_{10}(F_{5q+2}).$$

Отсюда заключаем, что $m_1 < F_{5q+2}$. Теперь утверждение теоремы получается непосредственно из следствия к лемме.

Замечание. Можно доказать более точное утверждение: при $s > 2$ количество s -значных чисел Фибоначчи равно 4 или 5.

Следствие. Пусть $T(n)$ - максимальное время работы алгоритма Евклида, когда на вход подаются данные размера n . Тогда $T(n) = O(\log^3 n)$.

Домашняя задача. Докажите, что на самом деле сложность алгоритма Евклида допускает более точную оценку, а именно $T(n) = O(\log^2 n)$.

Замечание. Кнут и Шёнхаге предложили варианты алгоритма Евклида, которые работают за квазилинейное время. Наилучшая на сегодняшний день оценка - $T(n) = O(M(n) \log n) = O(n \log^2 n \log \log n)$.



Основная теорема арифметики

Теорема (Основная теорема арифметики). Всякое натуральное число, большее 1 может быть разложено в произведение простых чисел, и это разложение единственно с точностью до порядка множителей.

Лемма. Пусть $(a, b) = 1$ и $a \mid bc$. Тогда $a \mid c$.

Доказательство. Из условия $(a, b) = 1$, согласно следствию, найдутся целые u и v такие, что $au + bv = 1$. Тогда в равенстве $asu + bcv = c$ левая часть делится на a , значит, и правая часть делится на a , т. е. $a \mid c$.

Доказательство основной теоремы арифметики. Существование разложения на простые множители проверяется по индукции. Для доказательства единственности воспользуемся леммой. Предположим, что существуют натуральные числа, обладающие разными разложениями на простые множители. Выберем из них наименьшее число

$$n = p_1^{a_1} \dots p_s^{a_s} = q_1^{b_1} \dots q_t^{b_t}$$

С одной стороны, из минимальности n следует, что $p_1 \neq q_1$. С другой стороны

$$p_1 \mid p_1^{b_1} \dots p_t^{b_t}$$

и применяя последовательно лемму с $a = p_1$ и $b = q_1$, приходим к тому, что $p_1 \mid 1$.

Основная теорема арифметики

Замечание. Существует более короткое доказательство основной теоремы арифметики, не опирающееся на лемму. Однако оно, как и алгоритм Евклида, использует метод спуска. Пусть n - наименьшее число, обладающее неоднозначным разложением на простые множители:

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$$

Без ограничения общности можем также предполагать, что $p_1 > q_1$. Тогда мы можем предъявить меньшее число $n' = n - q_1 p_2 \dots p_s$, которое также допускает два различных разложения на простые:

$$n' = (p_1 - q_1) p_2 \dots p_s = q_1 (q_2 \dots q_t - p_2 \dots p_s)$$

Эти два разложения различны, поскольку простое число q_1 входит во второе, но не входит в первое.



Уравнение $ax + by = c$

Алгоритм Евклида позволяет не только вычислять наибольший общий делитель, но и находить общее решение в целых числах линейного уравнения $ax + by = c$.

Очевидно, что для разрешимости этого уравнения необходимо выполнения условия $(a, b) \mid c$. В этом случае, полагая $d = (a, b)$, $a = da_1$, $b = db_1$, $c = dc_1$, уравнение $ax + by = c$ мы можем заменить эквивалентным уравнением $a_1x + b_1y = c_1$, в котором коэффициенты a_1 и b_1 уже взаимно просты. Поэтому будем предполагать, что стоит задача описать все решения уравнения в целых числах при условии, что $(a, b) = 1$.

Теорема. Пусть $(a, b) = 1$, целые u и v таковы, что выполняется равенство $au + bv = 1$. Тогда общее решение уравнения $ax + by = c$ имеет вид

$x_k = x_0 + b_k$, $y_k = y_0 - a_k$, где k - произвольное целое, и $(x_0, y_0) = (cu, cv)$.

Доказательство. Числа, задаваемые равенствами, удовлетворяют уравнению $ax + by = c$. Проверим, что у этого уравнения нет других решений. Если (x, y) - произвольное решение, то вычитая из равенства $ax + by = c$ равенство $ax_0 + by_0 = c$, получаем, что $a(x - x_0) = -b(y - y_0)$. Так как $(a, b) = 1$, то разность $x - x_0$ должна делиться на b . Следовательно для некоторого целого k будет выполняться равенство $x - x_0 = bk$. Но тогда $y - y_0 = -a_k$, и значит, решение (x, y) лежит в серии решений $x_k = x_0 + b_k$, $y_k = y_0 - a_k$.

С геометрической точки зрения равенства означают, что все целые точки (x, y) , лежащие на прямой $ax + by = c$ получаются из некоторой точки (x_0, y_0) навекторы, кратные вектору $(b, -a)$.

План лекции

**Арифметика по
модулю**

25 минут

**Алгоритм
Евклида**

20 минут

Цепные дроби

25 минут

Сравнения

20 минут

Цепные дроби

Цепными дробями называются выражения вида

$$a_0 + \frac{b_0}{a_1 + \frac{b_1}{a_2 + \dots}}$$

Они бывают конечными и бесконечными. Мы ограничимся рассмотрением классических цепных дробей, для которых $b_0 = b_1 = \dots = 1$.

Определение. Бесконечной цепной дробью называется выражение вида

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{\ddots}{\frac{1}{a_n + \dots}}}}$$

в котором a_0 - целое, a_1, \dots, a_n, \dots - натуральные числа. Числа $a_0, a_1, \dots, a_n, \dots$, как и в случае конечных цепных дробей, называются неполными частными дробей.

Цепные дроби

Для цепной дроби $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$ будем использовать обозначение $[a_0; a_1, a_2, \dots]$.

Мы докажем, что всякое действительное число единственным образом (с небольшой оговоркой) раскладывается в цепную дробь. При этом рациональным числам будут соответствовать конечные цепные дроби, а иррациональным - бесконечные. Алгоритм разложения числа α в цепную дробь очень прост. Число записывается в виде $\alpha = a_0 + r_0 = a_0 + 1/\alpha_1$, где $a_0 = [\alpha]$, $r_0 = \{\alpha\}$, $\alpha_1 = 1/r_0$, после чего та же процедура применяется к числу α_1 . На шаге с номером k в разложении

$$\alpha = [a_0; a_1, a_2, \dots, a_{k-1}, a_k]$$

число $\alpha_k = a_k + r_k$, где $\alpha_k = [a_k]$, $r_k = \{\alpha_k\}$, заменяется на $\alpha_k + 1/\alpha_{k+1}$, где $\alpha_{k+1} = 1/r_k$. Процесс обрывается, если на некотором шаге (быть может нулевом) остаток оказывается равен нулю.

Примеры. Например, если $\alpha = \sqrt{2}$, то $a_0 = 1$, $r_0 = \sqrt{2} - 1$, $\alpha_1 = \sqrt{2} + 1$:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + 1/(\sqrt{2} + 1)$$

На следующем шаге возникает то же число $\sqrt{2} + 1$, т.е. процесс закликивается:

$$\sqrt{2} = 2 + (\sqrt{2} - 1) = 2 + 1/(\sqrt{2} + 1)$$

Таким образом $\sqrt{2} = [1; 2, \dots, 2, \dots] = [1; \bar{2}]$.

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 1, 6, 1, 1, 8, 1, 1, 10, \dots]$$

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \dots]$$

Цепные дроби

Определение. Бесконечная цепная дробь $\alpha = [a_0; a_1, a_2, \dots]$ называется периодической, если существуют такие натуральные числа m и t , что для любого $k > m$ выполняется равенство $a_{k+t} = a_k$. Будем записывать такую дробь в виде

$$\alpha = [a_0; a_1, a_2, \dots, a_m, \overline{a_{m+1}, \dots, a_{m+t}}]$$

Набор чисел $(a_{m+1}, \dots, a_{m+t})$ называется периодом, а t - его длиной. (Подразумевается при этом, что период выбирается с наименьшей возможной длиной.)

Набор чисел $(a_0; a_1, a_2, \dots, a_m)$ называется предпериодом.

Дробь вида $\alpha = [\overline{a_0, \dots, a_{t-1}}]$ называется чисто периодической.

Рассмотренные примеры чисел с периодическими разложениями в цепные дроби являются частными случаями более общего результата, принадлежащего Лагранжу.

Определение. Число называется квадратичной иррациональностью, если оно является иррациональным корнем некоторого квадратного уравнения с целыми коэффициентами.

Теорема (Теорема Лагранжа). Число разлагается в периодическую цепную дробь тогда и только тогда, когда оно является квадратичной иррациональностью.

Прежде чем отождествлять иррациональные числа с бесконечными цепными дробями, последним надо будет придать смысл чисел. Для этого понадобится сначала изучить свойства конечных цепных дробей.

Конечные цепные дроби

Определение. Пусть a_0 - целое, a_1, a_2, \dots, a_n - натуральные. Конечной цепной (непрерывной) дробью называется выражение

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots \frac{1}{a_n}}}}$$

которое обозначается $[a_0; a_1, a_2, \dots, a_n]$. Если $n > 0$, то дополнительно требуем, что $a_n > 1$.

Числа a_1, a_2, \dots, a_n называются неполными частными дроби.

Замечание. Требование $a_{n-1} > 2$ является необходимым для того, чтобы представление всякого рационального числа в виде конечной цепной дроби (??) было единственным.

Пример $2 = 1 + 1/1$

показывает, что это требование отбросить нельзя. Любое другое рациональное число также можно записать двумя способами:

$$[a_0; a_1, a_2, \dots, a_{n-1}] = [a_0; a_1, a_2, \dots, a_{n-1} - 1, 1].$$

Но следует отметить, что в некоторых задачах наоборот удобнее требовать, чтобы последнее неполное частное a_{n-1} равнялось бы 1.

Конечные цепные дроби

Теорема. Всякое рациональное число представимо в виде конечной цепной дроби, причем такое представление единственно.

Доказательство. Каждый шаг разложения числа $\alpha = m_0/m_1$ в цепную дробь находится во взаимно однозначном соответствии с шагом алгоритма Евклида, применённом к числам m_0 и m_1 :

$$\frac{m_0}{m_1} = \alpha_0 + \frac{m_2}{m_1}, \frac{m_1}{m_2} = \alpha_1 + \frac{m_3}{m_2}, \dots$$

Значит, процесс разложения числа α в цепную дробь закончится за конечное число шагов.

Для доказательства единственности предположим, что существуют две конечные цепные дроби, равные другу:

$$\alpha = [a_0; a_1, \dots, a_s] = [b_0; b_1, \dots, b_t].$$

Будем предполагать, что среди всех таких разложений выбраны самые короткие ($s \leq t$ и s - наименьшее возможное). Тогда $a_0 \neq b_0$ (иначе на них можно было бы сократить). Но, по определению конечных цепных дробей $\alpha = a_0 + r_0 = b_0 + w_0$, где $0 < r_0, w_0 < 1$. Значит $|r_0 - w_0| < 1$ и равенство $a_0 + r_0 = b_0 + w_0$ невозможно.

Полученное противоречие и доказывает теорему.

Основная задача, которую решают цепные дроби - это построение хороших рациональных приближений к данному числу. Такие приближения получаются, если цепную дробь $\alpha = [a_0; a_1, \dots, a_k, \dots]$ оборвать на некотором месте.

Подходящие дроби

Определение. Числа

$$\frac{p_k}{q_k} = [a_0; a_1, a_2, \dots, a_k] \quad (k \geq 0)$$

называются подходящими дробями к цепной дроби.

Например, $\frac{p_0}{q_0} = \frac{a_0}{1}, \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}, \frac{p_2}{q_2} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1},$

Теорема. Числители и знаменатели подходящих дробей – это последовательности $\{p_n\}, \{q_n\}$, которые задаются начальными условиями

$$p_0 = a_0, \quad p_1 = a_0 a_1 + 1, \quad q_0 = 1, \quad q_1 = a_1$$

и рекуррентными соотношениями

$$p_n = a_n p_{n-1} + p_{n-2}, \quad q_n = a_n q_{n-1} + q_{n-2} \quad (n \geq 2).$$

Замечание. В некоторых случаях бывает полезным доопределить дробь $\frac{p_{-1}}{q_{-1}} = \frac{1}{0}$. Тогда рекуррентные соотношения будут выполняться уже начиная с $n = 1$.

Замечание. Подходящие дроби удобно вычислять, заполняя таблицу вида

a_k		a_0	a_1	a_2	...
p_k	1	a_0	p_1	p_2	...
q_k	0	1	q_1	q_2	...

a_k		1	2	2	2	2	2
p_k	1	1	3	7	17	41	99
q_k	0	1	2	5	12	29	70

Например, если для числа $\sqrt{2}$ мы хотим найти пятую подходящую дробь (напомним, что их нумерация начинается с нуля), то такая таблица будет иметь вид

Подходящие дроби

Для доказательства теоремы мы ненадолго забудем, что числа p_k и q_k определялись как числители и знаменатели подходящих дробей. Вместо этого мы будем считать, что они задаются начальными условиями. Сначала мы докажем, что p_k/q_k - несократимые дроби, а потом проверим равенства

$\frac{p_k}{q_k} = [a_0; a_1, a_2, \dots, a_k] \ (k \geq 0)$. Из этого будет следовать доказательство теоремы.

Лемма. Последовательности $\{p_n\}$, $\{q_n\}$, заданные начальными условиями

$$p_0 = a_0, \ p_1 = a_0 a_1 + 1, \ q_0 = 1, \ q_1 = a_1$$

и рекуррентными соотношениями

$$p_n = a_n p_{n-1} + p_{n-2}, \ q_n = a_n q_{n-1} + q_{n-2} \ (n \geq 2).$$

связаны соотношением

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1} \quad (k > 1).$$

В частности, $(p_k, q_k) = 1$.

Доказательство. При $k = 1$ равенство следует из начальных условий. Далее оно проверяется по индукции. Если считать, что равенство выполнено, то

$$p_{k+1} q_k - p_k q_{k+1} = (a_k p_k + p_{k-1}) q_k - p_k (a_k q_k + q_{k-1}) = -(p_k q_{k-1} - p_{k-1} q_k) = (-1)^{k+2}$$

Доказательство теоремы. Будем считать, что последовательности $\{p_n\}$, $\{q_n\}$ заданы начальными условиями и рекуррентными соотношениями.

Подходящие дроби

Покажем, что для всех $k > 0$ выполняется равенство

$$\frac{p_k}{q_k} = [a_0; a_1, a_2, \dots, a_k]$$

При $k = 0, 1$ оно выполняется по определению. Если это равенство уже доказано для некоторого k , то

$$[a_0; a_1, a_2, \dots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}$$

Заменяя в этом равенстве a_k на $a_k + \frac{1}{a_{k+1}}$ приходим к соотношениям

$$\begin{aligned} \left[a_0; a_1, a_2, \dots, a_k + \frac{1}{a_{k+1}} \right] &= [a_0; a_1, a_2, \dots, a_k, a_{k+1}] = \frac{\left(a_k + \frac{1}{a_{k+1}} \right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}} \right) q_{k-1} + q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} = \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}} \end{aligned}$$

Из взаимной простоты чисел p_{k+1} и q_{k+1} следует, что $(k + 1)$ -ая подходящая дробь это и есть дробь $\frac{p_{k+1}}{q_{k+1}}$

Свойства подходящих дробей

Лемма. Числители и знаменатели подходящих дробей обладают следующими свойствами:

$$1^\circ. p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k \quad (k \geq 2);$$

$$2^\circ. \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k+1}}{q_k q_{k-1}} \quad (k \geq 1);$$

$$3^\circ. \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}} \quad (k \geq 2);$$

$$4^\circ. q_1 < q_2 < \dots < q_n < \dots;$$

$$5^\circ. \frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots \leq \frac{p_n}{q_n} \leq \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1};$$

$$6^\circ. \frac{p_{2k}}{q_{2k}} < \frac{p_{2l+1}}{q_{2l+1}} \quad (k, l \geq 0);$$

Доказательство. Свойство 1° вытекает из рекуррентных соотношений и равенства $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1} (k > 1)$:

$$p_k q_{k-2} - p_{k-2} q_k = (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2} (a_k q_{k-1} + q_{k-2}) = a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) = (-1)^k a_k$$

Равенство 2° получается из $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$ делением на $q_k q_{k-1}$.

Равенство 3° в свою очередь получается из 1° делением на $q_k q_{k-2}$.

Свойство 4° является очевидным следствием рекуррентного соотношения, которому удовлетворяет последовательность $\{q_k\}$.

Свойство 5° следует из 2° и 3° .

Свойство 6° - непосредственное следствие свойства 5° .

Доказанные свойства позволяют понять, насколько хорошим приближениями являются подходящие дроби.

Пока мы докажем этот результат для приближений рациональных чисел, но будет справедлив и для приближений подходящими дробями произвольных действительных чисел.

Свойства подходящих дробей

Теорема (о приближении рациональных чисел подходящими дробями).

Пусть $\frac{p_k}{q_k}$ - подходящая дробь к числу Q . Тогда

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k^2}$$

Доказательство. Если α совпадает с дробью $\frac{p_k}{q_k}$, то утверждение теоремы очевидно. Если же $\frac{p_k}{q_k}$ - не последняя подходящая дробь, то, согласно свойству 5°, α лежит на отрезке между $\frac{p_k}{q_k}$ и $\frac{p_{k+1}}{q_{k+1}}$, и поэтому

$$\left| \alpha - \frac{p_k}{q_k} \right| \leq \left| \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} \right| = \frac{1}{q_k q_{k+1}} \leq \frac{1}{a_{k+1} q_k^2} \leq \frac{1}{q_k^2}$$



Свойства подходящих дробей

Замечание. Если для числа α определена подходящая дробь $\frac{p_{k+2}}{q_{k+2}}$, то α лежит за пределами отрезка с концами $\frac{p_k}{q_k}$ и $\frac{p_{k+2}}{q_{k+2}}$. Этот аргумент позволяет оценивать точность приближения подходящими дробями снизу:

$$\left| \alpha - \frac{p_k}{q_k} \right| \geq \left| \frac{p_{k+2}}{q_{k+2}} - \frac{p_k}{q_k} \right| = \frac{a_{k+2}}{q_k q_{k+2}} = \frac{a_{k+2}}{q_k (a_{k+2} q_{k+1} + q_k)} > \frac{1}{q_k (q_{k+1} + q_k)}$$

Если подходящая дробь $\frac{p_{k+2}}{q_{k+2}}$ не определена, то это неравенство всё равно остаётся справедливым, поскольку

$$\left| \alpha - \frac{p_k}{q_k} \right| = \left| \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} \right| = \frac{1}{q_k q_{k+1}} > \frac{1}{q_k (q_{k+1} + q_k)}$$

Таким образом справедливы двусторонние оценки, отличающиеся не более чем в два раза.

$$\frac{1}{q_k (q_{k+1} + q_k)} \leq \left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}}$$

Замечание. Ранее мы находили частное решение уравнения $ax + by = 1$ путём применения расширенного алгоритма Евклида к числам a и b . Из равенства $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k+1}$ ($k > 1$) следует, что эту процедуру можно проинтерпретировать следующим образом. Сначала мы находим разложение $a/b = [a_0; a_1, a_2, \dots, a_n]$, затем отбрасываем последнее неполное частное, сворачиваем получившуюся цепную дробь $[a_0; a_1, a_2, \dots, a_{n-1}]$, и присваиваем переменным x и y значения $x = (-1)^{n+1} q_{n-1}$, $y = (-1)^n p_{n-1}$.

Бесконечные цепные дроби

Рациональные числа можно задавать самыми разными способами. Например, одно и то же число можно записать в виде отношения двух целых чисел a/b , можно в виде систематической дроби в позиционной системе счисления с некоторым основанием $q > 1$. Причем эта дробь может оказаться конечной, а может – бесконечной периодической, в зависимости от выбора q .

Мы рассмотрели еще один способ - представление конечной цепной дробью. Распространим его на все действительные числа. Ранее мы уже рассмотрели алгоритм, который позволяет произвольное действительное число разлагать в цепную дробь. Прежде чем мы станем отождествлять цепные дроби с числами, нам потребуется доказать сходимость бесконечных цепных дробей. Кроме этого, понадобится также проверить взаимную однозначность этих соответствий, то есть показать, что цепная дробь, построенная по числу α , будет сходиться именно к этому же числу α .

Определение. Бесконечная цепная дробь $[a_0; a_1, a_2, \dots, a_{k-1}, \dots]$, называется сходящейся, если существует предел ее подходящих дробей

$$\lim_{k \rightarrow \infty} \frac{p_k}{q_k} = \alpha$$

При этом предел α называется величиной данной бесконечной цепной дроби.

Теорема. Каждому иррациональному числу соответствует единственная бесконечная цепная дробь, имеющая это число своим значением.

Бесконечные цепные дроби

Лемма. Пусть $n > 0$ и $\alpha = [a_0; a_1, a_2, \dots, a_n, \alpha']$. Тогда

$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

В частности, α лежит правее всех подходящих дробей с чётными номерами и левее всех подходящих дробей с нечётными номерами.

Доказательство. Из рекуррентных соотношений следует, что то

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n + p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})} = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

Доказательство теоремы. Пусть число α раскладывается в бесконечную цепную дробь $[a_0; a_1, a_2, \dots, a_k, \dots]$. Покажем, что эта дробь сходится к α . По лемме число α лежит в каждом из отрезков $\left[\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}}\right]$ ($k \geq 0$). Но это система вложенных отрезков, длина которых стремится к нулю. Согласно принципу вложенных отрезков Кантора эта система отрезков имеет одну общую точку, которая не может быть ничем иным как числом α .

Для доказательства единственности предположим, что

$$\alpha = [a_0; a_1, a_2, \dots, a_n, \dots] = [a'_0; a'_1, a'_2, \dots, a'_n, \dots]$$

причём эти дроби могут быть как конечными, так и бесконечными. Тогда $a_0 = [\alpha] = a'_0$. Если уже установлено, что $a_i = a'_i$ при $i = 0, 1, \dots$, то $p_i = p'_i$, $q_i = q'_i$ ($i = 0, 1, \dots, n$), и по формуле

$$\alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} = \frac{\alpha'_{n+1}p_n + p_{n-1}}{\alpha'_{n+1}q_n + q_{n-1}}$$

откуда $\alpha_{n+1} = \alpha'_{n+1}$. То есть данные дроби полностью совпадают.

Приближение чисел подходящими дробями

Следствие. Для подходящих дробей к бесконечной цепной дроби α выполняются неравенства, доказанные нами ранее для конечных цепных дробей:

$$\frac{1}{q_k(q_{k+1} + q_k)} \leq \left| \alpha - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}}$$

Теорема (теорема Лежандра). Пусть α - действительное число,

$$\alpha - \frac{p}{q} = \frac{\theta}{q^2}$$

и p'/q' - предпоследняя подходящая дробь к числу p/q . Тогда p/q будет подходящей дробью к числу α тогда и только тогда, когда

$$|\theta| \leq \frac{q}{q + q'}$$

(Если $\alpha = [a_0; a_1, a_2, \dots, a_{n-1}, a_n]$ - рациональное число, то для справедливости этого утверждения к множеству подходящих дробей нужно добавить еще одну - $[a_0; a_1, a_2, \dots, a_{n-1}, a_n - 1]$.)

Эта теорема, в частности, означает, что достаточно хорошие приближения могут быть только подходящими дробями.

Приближение чисел подходящими дробями

Следствие. Если

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2q^2}$$

то $\frac{p}{q}$ - подходящая дробь к числу α .

Доказательство теоремы Лежандра. Пусть p/q - подходящая дробь к числу α и p''/q'' - следующая подходящая дробь. Тогда, согласно ограничивающему неравенству,

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{2qq''} \leq \frac{1}{q(q + q')}$$

что и дает нужную оценку величины Θ .

Возможен также случай, когда p/q - последняя подходящая дробь к числу α и дроби p''/q'' не существует. Тогда $\left| \alpha - \frac{p}{q} \right| = 0$ и нужное неравенство также выполняется.

Докажем утверждение теоремы в другую сторону. Пусть

$$\frac{p}{q} = [a_0; a_1, a_2, \dots, a_n], \frac{p'}{q'} = [a_0; a_1, a_2, \dots, a_{n-1},]$$

Приближение чисел подходящими дробями

Будем дополнительно предполагать, что из двух разложений p/q в цепную дробь (с единицей на конце и с не единицей на конце) выбрано то, для которого знак совпадает со знаком числа $(-1)^n$, т.е. $(-1)^n \Theta > 0$.

Если $\alpha = p/q$, то утверждение тривиально. Заметим, что число не может совпадать ни с одной из подходящих дробей к p/q . Действительно, если α - подходящая дробь, то $q_j < q$, но неравенства

$$\frac{1}{qq_j} \leq \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q(q+q')}$$

приводят к тому, что $q_j > q + q'$. Значит, для некоторого α' будет выполняться равенство

$$\alpha = [a_0; a_1, a_2, \dots, a_n, \alpha']$$

Согласно лемме,

$$\alpha - \frac{p}{q} = \frac{(-1)^n}{q(q\alpha' + q')} = \frac{\theta}{q^2}$$

Отсюда следует, что

$$|\theta| \leq \frac{q}{q\alpha' + q'} \text{ и } \frac{q}{q\alpha' + q'} \leq \frac{1}{q(q+q')}$$

Значит, $q\alpha' + q' > 0$, $q\alpha' + q' > q + q'$ и $\alpha' \geq 1$. Теперь из равенства $\alpha = [a_0; a_1, a_2, \dots, a_n, \alpha']$ следует, что p/q есть подходящая дробь к числу

Теорема Маркова - Гурвица

Теорема. Пусть $\varphi = \frac{1+\sqrt{5}}{2}$. Тогда существует бесконечно много дробей $\frac{p}{q}$ для которых выполняется неравенство

$$\left| \varphi - \frac{p}{q} \right| \leq \frac{1}{\sqrt{5}q^2}$$

Но при любом $c > \sqrt{5}$ неравенство

$$\left| \varphi - \frac{p}{q} \right| \leq \frac{1}{cq^2}$$

имеет лишь конечное число решений.

Доказательство. Из теоремы Лежандра следует, что решениями неравенства могут быть лишь подходящие дроби к числу φ . Из леммы, применённой к разложению $\varphi = [1; 1, 1, \dots, 1, \varphi]$, следует, что

$$\left| \varphi - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n(q_n\varphi - q_{n-1})} = \frac{1}{q_n^2 \left(\varphi - \frac{q_{n-1}}{q_n} \right)}$$

Число $\frac{q_{n-1}}{q_n}$ есть подходящая дробь к φ значит,

$$\frac{q_{n-1}}{q_n} = \frac{1}{\varphi} + \varepsilon_n$$

где $|\varepsilon_n| < 1/q_n^2 \rightarrow 0$ при $n \rightarrow \infty$.

Теорема Маркова - Гурвица

Таким образом

$$\left| \varphi - \frac{p_n}{q_n} \right| = \frac{1}{q_n(q_n\varphi - q_{n-1})} = \frac{1}{q_n^2 \left(\varphi + \frac{1}{\varphi} + \varepsilon_n \right)} = \frac{1}{q_n^2(\sqrt{5} + \varepsilon_n)}$$

Утверждение теоремы следует из того, что $\{\varepsilon_n\}$ - стремящаяся к нулю знакопеременная последовательность.

Доказанное нами утверждение - часть теоремы Маркова - Гурвица.

Теорема (Теорема Маркова - Гурвица). Для любого действительного α найдется бесконечно много дробей p/q таких, что

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{\sqrt{5}q^2}$$

Константу $\sqrt{5}$, фигурирующую в неравенстве, нельзя заменить большим числом.

Существенное уточнение этой теоремы было дано А. А. Марковым. Он доказал, что если из множества действительных чисел исключить числа, эквивалентные φ

(числа называются эквивалентными, если их разложения в цепную дробь начиная с некоторого места совпадают), то для всех оставшихся чисел α неравенство

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{cq^2}$$

будет иметь бесконечно много решений с константой $c = \sqrt{8}$. Это значение наилучшее, т.к. эту константу нельзя улучшить для чисел, эквивалентных серебряному сечению $\alpha = 1 + \sqrt{2}$.

Теорема Маркова - Гурвица

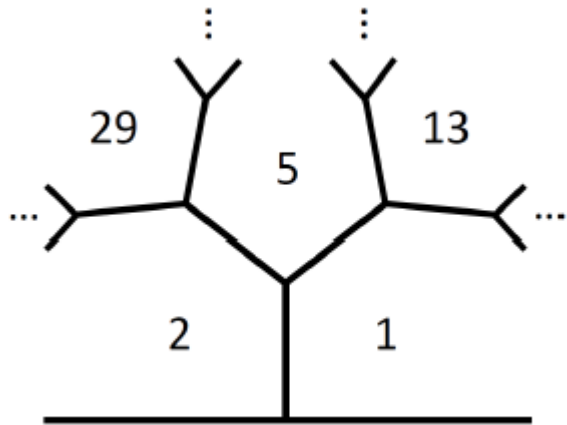
Если отбросить их, то для всех оставшихся неравенство будет уже выполняться с константой $c = \frac{\sqrt{221}}{5}$, и т. д. Возникающие здесь числа представляют собой спектр Маркова:

$$\sqrt{5}, \sqrt{8}, \frac{\sqrt{221}}{5}, \frac{\sqrt{1517}}{13}$$

Он имеет вид

$$\left\{ \frac{\sqrt{9m^2 - 4}}{m} : m \in M \right\}$$

Здесь $M = \{1, 2, 5, 13, 29, 34, \dots\}$ - множество чисел, возникающих в решениях уравнения Маркова $m^2 + m_1^2 + m_2^2 = 3mm_1m_2$
то есть в тройках $(1, 1, 1), (1, 1, 2), (1, 2, 5), (1, 5, 13), (2, 5, 29), (1, 13, 34), \dots$



Дерево Марковских троек

План лекции

**Арифметика по
модулю**

25 минут

**Алгоритм
Евклида**

20 минут

Цепные дроби

25 минут

**Сравнения
(начало)**

20 минут

Сравнение по модулю

Если два числа a и b дают одинаковые остатки при делении на положительное число N , то говорят, что они *сравнимы* по модулю N , и пишут $a \equiv b \pmod{N}$.

Эквивалентное определение: a и b сравнимы по модулю N , если разность $a - b$ делится на N . (В самом деле, если они дают одинаковый остаток r , то $a = kN + r$, $b = lN + r$, и $a - b = kN - lN = (k - l)N$. Наоборот, если $a - b = mN$, и b даёт остаток r , то $b = lN + r$ и $a = (a - b) + b =$

$mN + lN + r = (m + l)N + r$, то есть a даёт тот же остаток r .)

Можно сказать, что при данном N все целые числа разбиваются на N классов в зависимости от остатков по модулю N : два числа в одном классе сравнимы, а числа в разных классах - нет.



Сравнение по модулю

Важное свойство сравнений: чтобы узнать, в какой класс попадет сумма или произведение двух чисел, достаточно знать, в каком классе лежат слагаемые или сомножители: если одно из слагаемых (один из сомножителей) изменить на кратное N , то сумма (произведение) тоже изменится на кратное N .

В самом деле, если к одному из слагаемых прибавить kN , то к сумме тоже прибавится kN , аналогично для разности. С произведением: $(a + kN)b = ab + kbN \equiv ab \pmod{N}$.

Благодаря этому свойству в выражении, содержащем операции сложения и умножения (или возведение в целую степень, которое сводится к многократному умножению), можно заменять слагаемые или сомножители на сравнимые по модулю N - если результат нам важен лишь по модулю N . Например, можно найти $2^{100} \bmod 7$ (остаток от деления 2^{100} на 7): поскольку $2^3 = 8 \equiv 1 \pmod{7}$, то $2^{99} \equiv (2^3)^{33} \equiv 1^{33} = 1 \pmod{7}$, так что $2^{100} \equiv 2^{99} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{7}$.



Сравнение по модулю

Сравнения по модулю (пусть не под таким названием) часто встречаются в быту. Скажем, циферблат показывает количество прошедших часов по модулю 12, а также количество минут по модулю 60. Измеряя углы в градусах, мы фактически измеряем число градусов по модулю 360.

Последняя цифра (для положительного целого числа) сравнима в этом числе по модулю 10, а две последние цифры - по модулю 100. В музыке двенадцать полутонов составляют целую октаву, и потом названия нот (до, до диез и так далее) повторяются.

Известный признак делимости на 9 (число делится на 9 тогда и только тогда, когда его сумма цифр делится на 9) можно обобщить и сказать, что число и его сумма цифр сравнимы по модулю 9. Это легко следует из наших рассуждений. Скажем, для четырёхзначного числа:

$abcd = 1000a + 100b + 10c + d \equiv 1a + 1b + 1c + 1d = a + b + c + d \pmod{9}$, поскольку $10 \equiv 1 \pmod{9}$ и, следовательно, 10^2 , $10^3, \dots$ все сравнимы с 1 по модулю 9.



Сравнение по модулю

Если мы хотим представить себе наглядно числа по модулю N , можно вообразить кольцевое шоссе длиной в N километров: на нём километровые столбы будут $0, 1, 2, \dots, N - 1$, далее идёт столб N , который на том же месте, где 0 , затем $N + 1$ на том же месте, где 1 , и так далее. Можно пойти в другую сторону и поставить столб -1 на том же месте, где $N - 1$: это соответствует тому, что $(N - 1) \equiv (-1) \pmod{N}$.

Для действительных (не целых) чисел равенство дробных частей можно назвать сравнением по модулю 1. Точнее говоря, целой частью числа x называют наибольшее целое число, не превосходящее x ; целую часть обозначают обычно $\lfloor x \rfloor$. Разницу $x - \lfloor x \rfloor$ называют дробной частью и иногда обозначают $\{x\}$. Числа с одинаковой дробной частью отличаются на целое число единиц; можно сказать, что они <сравнимы по модулю 1>. Обратите внимание, что с отрицательными числами та же ситуация: $\lfloor -2.3 \rfloor = -3$ и $\{-2.3\} = 0.7$.



Таблицы сложения и умножения по модулю N

Мы уже видели таблицы сложения и умножения по модулю 2 и 3. Теперь мы знаем, что аналогичную таблицу можно составить по любому модулю. Например, по модулю 10 получатся таблицы сложения и умножения, которые получаются из обычных, если оставить только последнюю цифру:

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

×	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Скажем, $7 \times 8 = 56$, поэтому в восьмой клетке седьмого ряда мы пишем $56 \bmod 10 = 6$.



Обратимые элементы по модулю N

Остаток (вычет) по модулю N называется обратимым, если в произведении с каким-то другим остатком он даёт 1. Другими словами, а обратим, если уравнение $ax = 1$ имеет решение, то есть если в строке a таблицы умножения встречается единица.

В самом деле, обозначим через a^{-1} элемент, который в произведении с a даёт единицу. (Пока мы не знаем, что такой только один, так что обозначим какой-то.) Положим $x = a^{-1}b$. Тогда $ax = a(a^{-1}b) = (aa^{-1})b = 1 \cdot b = b$, так что одно решение уравнения $ax = b$ мы нашли. Оно будет единственным: если $ax = b$, то $a^{-1}(ax) = a^{-1}b$, но $a^{-1}(ax) = (a^{-1}a)x = 1 \cdot x = x$, так что для x есть только одна возможность.

Остаётся выяснить, какие элементы (остатки, вычеты) обратимы по модулю N . Решив задачу в начале этого раздела, мы знаем, что по модулю 10 это будут 1, 3, 7, 9.



Обратимые элементы по модулю N

Теорема. *Обратимыми по модулю N являются те и только те остатки, которые взаимно просты с N .*

Взаимно простыми называются числа, которые не имеют общего делителя, не считая 1.

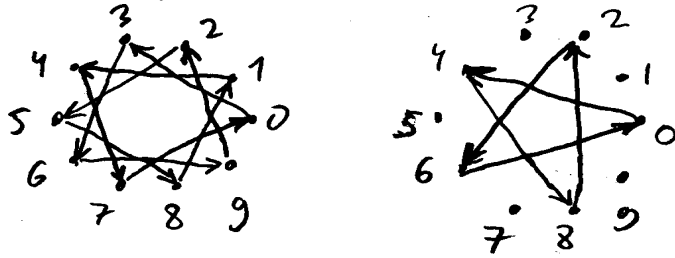
Например, по модулю 10 отпадают все чётные числа (у которых общий делитель 2), а также число 5 (общий делитель 5), остаются как раз 1, 3, 7, 9.

В частности, если N простое (не разлагается в произведение меньших чисел), то общим делителем могут быть только 1 и N , так что все остатки, кроме нуля, взаимно просты с N и обратимы. Для простого модуля всё как в обычной алгебре: делить можно на всё кроме нуля. (Математики выражают это словами: вычеты по простому модулю p образуют *поле*.)



Обратимые элементы по модулю N

Теорема. Обратимыми по модулю N являются те и только те остатки, которые взаимно просты с N .



Теперь легко доказать простую часть утверждения: если N и шаг a имеют общий делитель d , то элемент a необратим (мы не попадём в соседнюю остановку). В самом деле, будем отмечать остановки через $d, 2d, 3d$ и так далее от начальной. Поскольку N делится на d , то мы дойдём до N -й (то есть начальной) остановки, пройдя весь круг. Если a кратно d , то a -автобус будет останавливаться только в выделенных остановках, и в соседнюю никогда не попадёт.

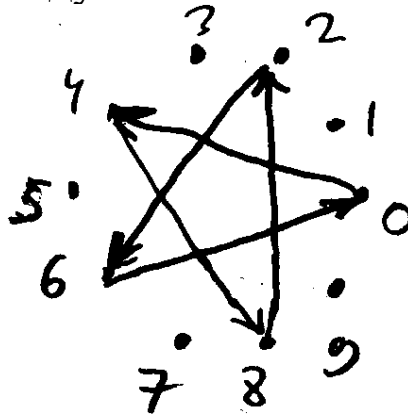
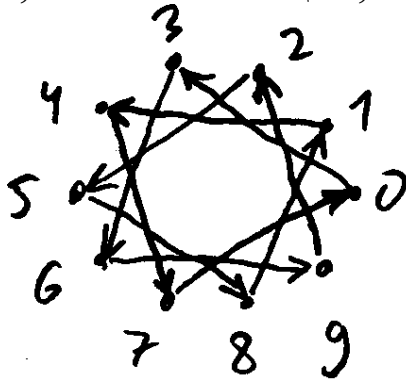
Осталось доказать сложную часть утверждения: если N и шаг a не имеют общих делителей, то все остановки будут обслужены. Прежде чем это сделать, мы ненадолго отвлечёмся и сделаем несколько простых замечаний об ориентированных графах.



Обратимые элементы по модулю N

Прежде чем доказывать эту теорему, представим себе наглядно, что означает обратимость остатка a . Для этого вспомним, что остатки по модулю N можно расположить на круговом шоссе длины N , как автобусные остановки. Запустим маршрут автобуса, которые делает остановки каждые a километров: у него первая остановка будет в a , вторая в $a + a = 2a$, третья в $3a$ (всё по модулю N , естественно). Обратимость означает, что таким странным способом все остановки будут обслужены (в строке таблицы умножения встретятся все остатки).

Вот две картинки, показывающие, что по модулю 10 остаток 3 будет обратимым, а остаток 4 нет:



в первом случае мы проходим все остановки, а во втором не все (только чётные).

Перестановки, ориентированные графы и циклы

Мы только что доказали, что всякий остаток a , взаимно простой с N , имеет обратный. Но как этот обратный найти? Можно пробовать все возможности по очереди. При небольших N это реально, но что делать, если, скажем $N = 5704689200685129054721$. Для начала переформулируем нашу задачу более симметричным образом. Мы хотим решить сравнение $ax \equiv b \pmod{N}$. Это сравнение означает, что разность $b - ax$ должна быть целым числом, кратным N , то есть должна равняться Ny при каком-то y . Таким образом, нам надо решить в целых числах уравнение $ax + Ny = b$. Здесь a , N , y - известные целые числа, и мы ищем целые x и y , при которых левая часть равна правой. Найдя их, мы можем про y забыть, а x будет решением.

Уравнения, в которых нам нужны целые решения, называются *диофантовыми*, в честь другого древнего грека - Диофанта. (Он, правда, не такой древний, как Евклид, и жил уже после Р.Х.)

Теорема 3. Пусть a , b , c - произвольные целые числа. Уравнение $ax + by = c$ имеет целочисленное решение тогда и только тогда, когда число c кратно $\text{НОД}(a, b)$.

Опять в одну сторону это очевидно: если d есть (наибольший) общий делитель a и b , то $ax + by$ всегда делится на d , так что уравнение может иметь решение только при c , кратном d . Интересно обратное утверждение. ДЗ

Перестановки, ориентированные графы и циклы

Мы только что доказали, что всякий остаток a , взаимно простой с N , имеет обратный. Но как этот обратный найти? Можно пробовать все возможности по очереди. При небольших N это реально, но что делать, если, скажем $N = 5704689200685129054721$. Для начала переформулируем нашу задачу более симметричным образом. Мы хотим решить сравнение $ax \equiv b \pmod{N}$. Это сравнение означает, что разность $b - ax$ должна быть целым числом, кратным N , то есть должна равняться Ny при каком-то y . Таким образом, нам надо решить в целых числах уравнение $ax + Ny = b$. Здесь a , N , y - известные целые числа, и мы ищем целые x и y , при которых левая часть равна правой. Найдя их, мы можем про y забыть, а x будет решением.

Уравнения, в которых нам нужны целые решения, называются *диофантовыми*, в честь другого древнего грека - Диофанта. (Он, правда, не такой древний, как Евклид, и жил уже после Р.Х.)

Теорема 3. Пусть a , b , c - произвольные целые числа. Уравнение $ax + by = c$ имеет целочисленное решение тогда и только тогда, когда число c кратно $\text{НОД}(a, b)$.

Опять в одну сторону это очевидно: если d есть (наибольший) общий делитель a и b , то $ax + by$ всегда делится на d , так что уравнение может иметь решение только при c , кратном d . Интересно обратное утверждение. ДЗ