Алгоритмы и структуры данных

Лекция 18
Числа.

Сергей Леонидович Бабичев

Делимость. Простые числа.

Делимость

Definition (НОД)

Наибольший общий делитель чисел $a, b \in \mathbb{N}$ есть наибольшее из всех таких чисел $c \in \mathbb{N}$, которое $a \vdots c, b \vdots c$ и обозначается $\gcd(a, b)$.

Definition (НОК)

Наименьшее общее кратное чисел $a, b \in \mathbb{N}$ есть наименьшее из всех таких чисел $c \in \mathbb{N}$, которое $c \vdots a, c \vdots b$ и обозначается $\operatorname{lcm}(a, b)$.

Алгоритм Евклида

- Операция $\gcd$ коммутативна.
- Определение Евклида:

$$\gcd(a,b) = \begin{cases} a, \text{ если } b = 0 \\ b, \text{ если } a = 0 \\ \gcd(b, a-b), \text{ если } a > b \\ \gcd(b-a, a) \text{ иначе} \end{cases}$$

Definition (Простое число)

Число $a \in \mathbb{N}, a > 1$ есть *простое* если $\nexists b \in N : (1 < b < a) \wedge (a \vdots b)$.

Theorem (Количество простых чисел)

Множество простых чисел счётно и бесконечно.

Доказательство.

Рассмотрим число $p_1 p_2 \dots p_l + 1$, где p_l — последнее простое число. □

Theorem (Теорема Дирихле)

Множество, образованное числами $b \in \mathbb{N}_0$ и числами вида $ak + b, a \in \mathbb{N}, b \in \mathbb{Z}$ содержит бесконечное множество простых чисел, если $\gcd(a, b) = 1$.

Theorem (Основная теорема арифметики)

Каждое число $n \in \mathbb{N}, n > 1$ может быть однозначно записано как

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

где $p_i \in \mathbb{P}, p_i \neq p_j$ при $i \neq j$. Такое обозначение при $p_1 < p_2 < \cdots < p_s$ называется каноническим.

Corollary (Делимость чисел)

Число

$$a = p_1^{\alpha_1} \times p_2^{\alpha 2} \times \cdots \times p_n^{\alpha_n}$$

делится на

$$b = q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_m^{\beta_m}$$

в том и только в том случае, если $Q \subset P$ и каждый из коэффициентов при соответствующих показателях степеней при q меньше или равен соответствующему показателю при p.

Следствия ОТА

- Пусть $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}, \alpha_i \geqslant 0$ и $M = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n} \beta_i \geqslant 0$.

$$\gcd(M, N) = p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \cdots \times p_n^{\min(\alpha_n, \beta_n)}.$$

$$\operatorname{lcm}(M, N) = p_1^{\max(\alpha_1, \beta_1)} \times p_2^{\max(\alpha_2, \beta_2)} \times \cdots \times p_n^{\max(\alpha_n, \beta_n)}.$$

- Отсюда, в частности, следует формула:

$$\gcd(M, N) \times \operatorname{lcm}(M, N) = M \times N$$

.

Задача. Определить количество натуральных делителей числа x.

Задача. Определить количество натуральных делителей числа x.
Решение:

- Выпишем каноническое представление x.

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

  В каждый делитель числа в разложении может входить делитель p_i с кратностью от 0 до α_i.
- Следовательно, общее количество делителей будет

$$\prod_{i=1}^{n} \alpha_i + 1$$

Теорема Ферма

Если p — простое число, a — целое число, то $a^p - a$ кратно p.

$$\boxed{\forall p \in \mathbb{P}, \forall a \in \mathbb{Z} : a^p - a \vdots p}$$

Теорема Ферма: другая формулировка

Для числа $k \in \mathbb{Z}$ и числа $p \in \mathbb{P}$ таких, что $k \not\vdots p$ верно
$k^{p-1} \pmod{p} \equiv 1$

Доказательство: так как остатки от деления на p чисел $k, 2 \cdot k, \ldots, (p-1) \cdot k$ есть перестановка чисел $1, 2, \cdot, p-1$, то

$$k \cdot 2k \cdot \ldots \cdot (p-1)k \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p},$$

из чего следует

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

$(p-1)!$ и p взаимно просты $\rightarrow$ можно сократить обе части на $(p-1)!$, получив искомое.

Теорема Ферма: а что, если число p — не простое?

- Среди остатков появятся нули.
- Наше доказательство не пройдёт.
- Попробуем выяснить, что будет, если p — не простое.

Таблицы умножения по модулю

Давайте составим таблицу умножения всех чисел от 1 до $p-1$ по модулю p.

- p — простое число. Пусть $p = 7$..

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Мы уже доказали, что в каждой строке встретятся все числа от 1 до $p-1$.
Какие ещё свойства?

Таблицы умножения по модулю

- p — составное число. Пусть $p = 6$.

$\times$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

- Есть строки и столбцы, содержащие нули. Вычеркнем их.

$\times$	1	5
1	1	5
5	5	1

Таблицы умножения по модулю

- p — составное число. Пусть $p = 8$.

$\times$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	0	2
7	7	6	5	4	3	2	1

- Вычеркнем строки и столбцы, содержащие нули.

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Таблицы умножения по модулю

- Для чего мы сокращаем таблицы?

Таблицы умножения по модулю

- Для чего мы сокращаем таблицы?
- Чтобы обобщить теорему Ферма не только на простые числа.
- Что содержится в сокращённых таблицах при составных n?

Таблицы умножения по модулю

- Для чего мы сокращаем таблицы?
- Чтобы обобщить теорему Ферма не только на простые числа.
- Что содержится в сокращённых таблицах при составных n?
- Каждая строка или столбец содержит все взаимно простые с n числа.
- Строки различаются только порядком.
- Перемножим числа в строке k.

$$ka_1ka_2 \dots ka_r \equiv a_1a_2 \dots a_r \pmod{p}$$

$$(k^r - 1)a_1a_2 \dots a_r \equiv 0 \pmod{p}$$

- Так как $(k^r - 1)a_1a_2 \dots a_r$ делится на p, а все a_i взаимно просты с p, то

$$\boxed{k^r - 1 \equiv 0 \pmod{p}}$$

Теорема Эйлера

$$k^r - 1 \equiv 0 \pmod{p}$$

- Что такое r в этой формуле?
- r — число чисел, меньших p и взаимно простых с p.
- Это — теорема Эйлера.

> Для взаимно простых целого числа k и натурального числа p верно, что
>
> $$k^{\varphi(p)} - 1 \equiv 0 \pmod{p}$$

- Здесь p — не обязательно простое число.
- Функция Эйлера $\varphi(p)$ есть число чисел, меньших p и взаимно простых с p.

Функция Эйлера

Исследуем эту замечательную функцию.

- Для p — простого числа, функция $\varphi(p) = p - 1$.
- Рассмотрим p^m, где p — простое число.
- Все числа $p, 2p, 3p, \ldots, p^m - p$ имеют с p^m общие делители. Таких чисел $p^{m-1} - 1$.
- По основной теореме арифметики (ОТА), других делителей у p^m нет.
- По ОТА все остальные числа от 1 до $p^m - 1$ — взаимно простые с p^m.
- Итого: $\varphi(p^m) = p^m - 1 - (p^{m-1} - 1) = p^m \left(1 - \frac{1}{p}\right)$.

Функция Эйлера

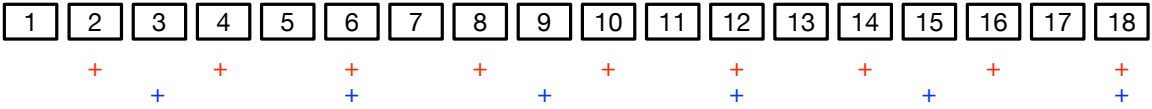
Чему равна $\varphi(18)$?

- Это — число чисел от 1 до 18, не делящихся ни на 2 ни на 3.
- На 2 делится 9 чисел.
- На 3 делится 6 чисел.
- Правда ли, что $\varphi(18) = 18 - 9 - 6 - 1$?

Функция Эйлера

Чему равна $\varphi(18)$?

- Это — число чисел от 1 до 18, не делящихся ни на 2 ни на 3.
- На 2 делится 9 чисел.
- На 3 делится 6 чисел.
- Правда ли, что $\varphi(18) = 18 - 9 - 6 - 1$?
- Нет, мы вычеркнули числа 6 и 12 дважды.
- Их надо вернуть.
- $\varphi(18) = 18 - 9 - 6 - 1 + 2 = 6$
- Это — формула включений/исключений.



Функция Эйлера

- Есть ли другой?
- Да. Используя следующую теорему:

> Функция Эйлера обладает свойством мультипликативности: для взаимно простых m и n верно:
>
> $$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

Следствие из теоремы:
Если число $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, то

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k})$$

или

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

Китайская теорема об остатках

Theorem (Китайская теорема об остатках)

Пусть $p_1, p_2, \ldots, p_k$ — попарно различные простые числа и пусть $P = p_1 \cdot p_2 \cdot \ldots \cdot p_k$. Тогда существует единственное неотрицательное решение по модулю P системы уравнений

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \ldots \\ x \equiv a_k \pmod{p_k} \end{cases}$$

Задача. Решить систему:

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

Задача. Решить систему:

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

Решение: [Наивное]
Составим таблицу остатков от деления на 3 и 5.

$x \pmod 5 \backslash x \pmod 3$	0	1	2
0	0	10	5
1	6	1	11
2	12	7	2
3	3	13	8
4	9	4	14

Найдём пересечение столбца с заголовком 2 и строки с заголовком 1.
Это 11. Значит, $x = 11 + 15t, t \in \mathbb{Z}$.

Китайская теорема об остатках

Решение: [Правильное]

- Что значит решить такую систему?
- С чего начинать решение?
- Начнём с первого уравнения.
- Если

$$x \equiv 2 \pmod 3,$$

то

$$x = 3k + 2,$$

где $k \in \mathbb{Z}$.

- Подставим во второе уравнение.

$$3k + 2 \equiv 1 \pmod 5$$

Обратные числа в модулярной арифметике.

- Нам нужно определить, на какое число нужно умножить p, чтобы получился остаток 1 по модулю m.
- Это — обратное число в поле вычетов.
- Его можно найти через *расширенный алгоритм Евклида* или через *малую теорему Ферма*.

Обратные числа в модулярной арифметике.

- Имея обратное число p^{-1} по модулю m, мы можем решать любые системы вида $ax + by = c$.

$$ax = c - by$$
$$ax = c \pmod{b}$$
$$x = c \cdot a^{-1} \pmod{b}$$

.

Китайская теорема об остатках: решение уравнения

Дорешаем уравнение

$$3k + 2 \equiv 1 \pmod 5,$$

- $3k = (1 - 2) \pmod 5 = 4 \pmod 5$
- Установим, что $3^{-1} \pmod 5 = 2$.
- Действительно, $(3 \cdot 2) \pmod 5 = 1$.
- Тогда $k = (3^{-1} \cdot 4) \pmod 5 = (2 \cdot 4) \pmod 5 = 3$.
- Подстановкой в уравнение убеждаемся, что мы правы.
- Подставляем в уравнение $x = 3k + 2$ получаем $x = 11$.

Использование КТО на практике

- Выберем n простых чисел $p_i, i = 1, n$.
- $P = \prod_{i=1}^{n} p_i$.
- КТО гласит, что

$$\forall x \in [0 \dots P)\ \exists \{a_1, a_2, \dots, a_n\} : 0 \leqslant a_i < p_i \text{ и } a_i \equiv x \pmod{p_i}.$$

- Существует биекция $x \Leftrightarrow \{a_1, \dots, a_n\}$.
- Исследуем свойства кортежей $\{a_1, \dots, a_n\}$

Использование КТО на практике

Для $x \Leftrightarrow \{a_1, \ldots, a_n\}$ и $y \Leftrightarrow \{b_1, \ldots, b_n\}, x, y \in [0, P)$:

- $x + y \equiv \{(a_1 + b_1) \pmod{p_1}, \ldots, (a_n + b_n) \pmod{p_n}\} \pmod{P}$
- $x - y \equiv \{(a_1 - b_1) \pmod{p_1}, \ldots, (a_n - b_n) \pmod{p_n}\} \pmod{P}$
- $x \cdot y \equiv \{(a_1 \cdot b_1) \pmod{p_1}, \ldots, (a_n \cdot b_n) \pmod{p_n}\} \pmod{P}$

- Каждый кортеж — представитель x в непозиционной системе счисления по основаниям $\{p_1, \ldots, p_n\}$.
- Над кортежами производятся те же операции сложения, вычитания, умножения.
- Сложность всех этих операций $\Theta(n) \rightarrow$ арифметика КТО применима для реализации длинных чисел.

Длинные числа и КТО

- Выбираются n простых чисел, образующих непозиционную систему счисления (*систему вычетов*).
- В ней представимы все числа $0 \leqslant x < \prod_{i=1}^{n} p_i$.
- Перевод любого числа в систему есть нахождение n остатков.
- Перевод числа из системы счисления надо автоматизировать.
- Для этого имеется *алгоритм Гарнера*.

Алгоритм Гарнера

Задача: кортежу $\{a_1, \ldots, a_n\}$ в системе вычетов $\{p_1, \ldots, p_n\}$ найти представителя x.

- Пока всё было не очень автоматизировано. Поставим вычисления на поток.
- Будем искать разложение x в сумму:

$$x = x_0 + p_1 \cdot x_1 + p_1 \cdot p_2 \cdot x_2 + \cdots + p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot x_{n-1} \tag{1}$$

Известно, что

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \ldots \\ x \equiv a_n \pmod{p_n} \end{cases} \tag{2}$$

Подставим уравнение (1) в первое уравнение из (2).

Алгоритм Гарнера

$$x_0 + p_1 \cdot x_1 + p_1 \cdot p_2 \cdot x_2 + \cdots + p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot x_{n-1} \equiv a_1 \pmod{p_1} \qquad (3)$$

Отсюда следует $x_0 = a_1$.
Подставим уравнение (1) во второе уравнение из (2)

$$a_1 + p_1 \cdot x_1 + p_1 \cdot p_2 \cdot x_2 + \cdots + p_1 \cdot p_2 \cdot \cdots \cdot p_{n-1} \cdot x_{n-1} \equiv a_2 \pmod{p_2} \qquad (4)$$

Отсюда, так как мы в поле вычетов по каждому из p_i:

$$x_0 + p_1 \cdot x_1 \equiv a_2 \pmod{p_2}$$
$$p_1 \cdot x_1 \equiv a_2 - x_0 \pmod{p_2}$$
$$x_1 \equiv (a_2 - x_0) \cdot {p_1}^{-1} \pmod{p_2}$$

Введём обозначение $r_{i,j} = p_i^{-1} \pmod{p_j}$.
Тогда

$$x_1 \equiv (a_2 - x_0) \cdot r_{1,2} \pmod{p_2}$$

Алгоритм Гарнера

$$x_1 \equiv (a_2 - x_0) \cdot r_{1,2} \pmod{p_2}$$

Подстановка x_1 в третье уравнение 2 даёт:

$$x_0 + x_1 \cdot p_1 + x_2 \cdot p_2 \equiv a_3 \pmod{p_3}$$

$$x_1 \cdot p_1 + x_2 \cdot p_1 \cdot p_2 \equiv a_3 - x_0 \pmod{p_3}$$

Домножаем на $r_{1,3}$:

$$x_1 \cdot p_1 \cdot r_{1,3} + x_2 \cdot p_1 \cdot p_2 \cdot r_{1,3} \equiv (a_3 - x_0) \cdot r_{1,3} \pmod{p_3}$$

$$x_1 + x_2 \cdot p_2 \equiv (a_3 - x_0) \cdot r_{1,3} \pmod{p_3}$$

$$x_2 \cdot p_2 \equiv (a_3 - x_0) \cdot r_{1,3} - x_1 \pmod{p_3}$$

Домножаем на $r_{2,3}$:

$$x_2 \cdot p_2 \cdot r_{2,3} = x_2 \equiv ((a_3 - x_0) \cdot r_{1,3} - x_1) \cdot r_{2,3} \pmod{p_3}$$

Алгоритм Гарнера: рекуррента

$$x_n \equiv (((a_{n+1} - x_0) \cdot r_{1,n+1} - x_1) \cdot r_{2,n+1}) - x_2 \ldots \pmod{p_{n+1}}$$

Другая запись при раскрытии скобок:

$$x_n = \frac{a_{n+1} - (x_0 + x_1 \cdot p_1 + x^2 \cdot p_1 \cdot p_2 + \cdots + x_{n-1} \cdot p_1 \cdot p_2 \ldots p_{n-1})}{p_1 \cdot p_2 \cdot \cdots \cdot p_n} \pmod{p_{n+1}}$$

Символ Лежандра

Definition (Символ Лежандра)

Символ Лежандра $\left(\frac{a}{m}\right)$

$$\left(\frac{a}{m}\right) = \begin{cases} 1, \text{ если } a - \text{ квадратичный вычет по модулю } m \\ -1, \text{ если } a - \text{ квадратичный невычет по модулю } m \\ 0, \text{ если } a \vdots m \end{cases}$$

Формула Эйлера:

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

Свойства символа Лежандра

1. Для $a \equiv b \pmod{m}$ верно $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$;
2. $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right) \cdot \left(\frac{b}{m}\right)$;
3. $\left(\frac{1}{m}\right) = 1$;
4. $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$;
5. $\left(\frac{a^2}{m}\right) = 1$.
6. Для $m = p_1 \cdot p_2 \cdot \ldots \cdot p_k, p_i > 2$, где p_i могут совпадать, верен символ Якоби

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

- Это — обобщение символа Лежандра на произвольные m.

Задача. Для большого n-чанкового числа x определить, является ли оно полным квадратом. Сложность операций сложения двух n-чаковых чисел $\Theta(n)$, операций умножения — $\Theta(n^2)$. Операции извлечения квадратного корня — нет. Придумайте способ, как для очень большого числа запросов получать ответы максимально быстро. Полагаем, что число правильных квадратов во входящей последовательности невелико.

Задача. Для большого n-чанкового числа x определить, является ли оно полным квадратом. Сложность операций сложения двух n-чаковых чисел $\Theta(n)$, операций умножения — $\Theta(n^2)$. Операции извлечения квадратного корня — нет. Придумайте способ, как для очень большого числа запросов получать ответы максимально быстро. Полагаем, что число правильных квадратов во входящей последовательности невелико.

Решение:

- Поймём, что сложность нахождения остатка от операции деления n-чанкового числа на короткое $\Theta(n)$.
- Составим таблицы $M_{i,j} = \left(\frac{a}{p_i}\right)$ для всех $a \in \mathbb{Z}_{p_i}$ по модулям $p_1, p_2, \ldots, p_k \in \mathbb{P}$.
- Для каждого проверяемого числа x находим $x \bmod p_i$.
- Если табличное значение равно -1, то число — не точный квадрат.
- Если число не являлось точным квадратом, то каждая проверка завершит работу с вероятностью 0.5.
- После k проверок вероятность, точного квадрата будет 2^{-k}.

Подгруппы

- В поле вычетов по модулю p для каждого элемента a существует обратный по операции умножения: $ax \equiv 1 \pmod{p}$.
- Если S образует группу по операции $\circ$, $S' \subseteq S$ и S' образует группе по операции $\circ$, то S' — *подгруппа группы S по операции $\circ$*.
- Пример — множество чётных чисел — подгруппа $\mathbb{Z}$ по операции сложения.

Theorem (Существование подгруппы)

Если S — конечная группа по операции $\circ$, S' — непустое подмножество S такое, что $a \circ b \in S'$, то S' — подгруппа S по операции $\circ$.

Theorem (Лагранжа)

Если S — конечная группа по операции $\circ$, S' — подгруппа S по операции $\circ$, то $|S| \vdots |S'|$.

Генераторы подгрупп

Здесь и далее речь идёт о группах по операции $\circ$.

- Для элемента $a \in S$ определим все элементы, которые из него могут получиться.
- $a^{(k)} = \underbrace{a \circ a \cdots \circ a}_{k}$
- Введём обозначение $\langle a \rangle$ для такой подгруппы.
- Порядок элемента в подгруппе $\langle a \rangle$ называемый (a) есть минимальное $k \in \mathbb{N}_1 : a^{(k)} = e$.

Theorem (Порядок группы)

Для любой конечной группы S *и* $\forall a \in S \quad (a) = |\langle a \rangle|$.

Задача. Хеш-таблица использует открытую адресацию с рехешированием. Для вновь пришедшего ключа вычисляется $h = H(key) \bmod S$, где S — размер таблицы. Если позиция h занята, вычисляется $h1 = H1(key) \bmod S$. После это делаются попытки вставить ключ в позиции $(h + h1) \bmod S$, $(h + 2 \cdot h1) \bmod S$, $(h + 3 \cdot h1) \bmod S$ — до успеха. Каким условиям должны удовлетворять S, h и $h1$, чтобы множество возможных точек вставки ключа было максимальным?

Порядки мультипликативных групп

Здесь и далее речь идёт о группах $\mathbb{Z}_m$ по операции умножения.
Свойства групп и их порядков:

1. Если $a \equiv b \pmod{m}$, то $(a) = (b)$.
2. Числа $a^0, a_1, \ldots, a_k - 1$ различны по модулю m, $k = (a)$.
3. $\varphi(m) \vdots (a)$.
4. Если $a^n \equiv 1 \pmod{m}$ то $m \vdots (a)$.
5. Если $a^k \equiv a^l \pmod{m}$, то $k \equiv l \pmod{(a)}$.
6. В поле вычетов по модулю p для каждого элемента a существует обратный по операции умножения: $ax \equiv 1 \pmod{p}$.

Первообразные корни и дискретные логарифмы

Definition (Первообразный корень)

Число a есть *первообразный корень по модулю* m, если $(a) = \varphi(m)$.

- Пусть p — фиксированное простое число, g — некоторый первообразный корень по модулю p.
- g^0, g^1, g^2, g^{p-2} образуют приведённую систему вычетов по модулю p.
- Для всякого $a \in \mathbb{Z}_p$ найдётся такое $l \in [0, p-1)$, что $a = g^l \pmod{p}$.
- l — *дискретный логарифм* числа a по основанию g и модулю p.

$$l =_g a$$

Алгоритм Диффи-Хеллмана

- Имеются два несекретных числа:
  - p — простое число;
  - g — первообразный корень по модулю p.
- Основан на том, что $g^{ab} \bmod p = g^{ba} \bmod p$ и невозможности за разумное время по известным $g^a \bmod p$ и $g^b \bmod p$ вычислить $g^{ab} \bmod p$ при больших p, a, b.
  Задача дискретного логарифмирования трудноразрешима.

Алгоритм Диффи-Хеллмана

- A и B хотят взаимно получить число, известное лишь им.
- Они выбрали $p = 13, g = 6$.
  - A выбирает произвольно приватный ключ $a = 10$.
  - A вычисляет $A' = g^a \bmod p = 6^{10} \bmod 13 = 4$ и посылает его B.
  - B выбирает произвольно приватный ключ $b = 3$.
  - B вычисляет $B' = g^b \bmod p = 6^3 \bmod 13 = 8$ и посылает его A
  - A вычисляет $s = B'^a \bmod p = 8^{10} \bmod 13 = 12$.
  - B вычисляет $s = A'^b \bmod p = 4^3 \bmod 13 = 12$.
- s — искомый секрет, известный лишь двоим.
- Всё остальное может быть известно всем.

Алгоритм RSA

1. Находится пара больших простых чисел P и Q
2. $N = P \cdot Q$.
3. $Z = (P-1)(Q-1)$.
4. Выбирается $E : \gcd(E, Z) = 1$.
5. Вычисляется $D : D = E^{-1} \pmod{Z}$
6. Пара $P = E, N$ — публичный ключ.
7. Пара $S = D, N$ — приватный (секретный) ключ.

$C_i = M_i^E \bmod N$ — шифрование
$M_i = C_i^d \bmod N$ — дешифрование