Необходимые факты из теории чисел

Выполнила студентка БПИ213,

Галкина Таисия

Основные понятия:

- Пусть даны три целых числа a, b и m. Говорят, что a сравнимо с b по модулю m если разность a - b делится на m. Записывают это так: $a \equiv b \pmod{m}$. Число m называется модулем сравнения.
- Для фиксированного m каждый класс эквивалентности по этому отношению обладает в точности одним представителем в множестве чисел от 0 до m - 1.
- Сравнения (по одному и тому же модулю) можно складывать, вычитать и перемножать. Таким образом, множество Z/mZ является коммутативным кольцом, т.е. классы вычетов можно складывать, вычитать и перемножать (причем результат не зависит от того, какие представители классов эквивалентности используются), и эти операции удовлетворяют обычным аксиомам ассоциативности, коммутативности, существования противоположного элемента и т. д.

Алгоритм Евклида (Нахождение наибольшего общего делителя)

Пусть a и b положительные целые числа и $a > b$, чтобы найти их НОД поделим с остатком a на b:

$a = bq_0 + r_1,\ 0 \le r_1 < b$

Поделим b на r: $b = r_1q_1 + r_2,\ 0 < r_2 < r_1$

Если r_1 не делится на r_2, то $r_1 = r_2q_2 + r_3,\ 0 < r_3 < r_2$

Деление продолжается, пока новый остаток не окажется делителем предыдущего. Последний ненулевой остаток и является наибольшим общим делителем a и b.

$a = bq_0 + r_1,$

$b = r_1q_1 + r_2,$

. . . . . .

$r_{n-2} = r_{n-1}q_{n-1} + r_n,$

$r_{n-1} = r_nq_n$

$(a, b) = r_n$ ■

Следствие:

Пусть $d = (a, b)$, где $a > b$. Тогда существуют такие целые числа u и v, что $d = ua + bv$. Другими словами, НОД двух чисел можно представить в виде линейной комбинации этих чисел с целыми коэффициентами.

Доказательство:

Будем проходит последовательность равенств в алгоритме Евклида снизу вверх и последовательно выражать d через все ранние остатки. В конце получим выражение d через a и b ■

Замечание

Обратимыми по умножению являются те элементы из Z/mZ, представители которых взаимно просты с m, т.е. числа a, для которых существует такое b, что $ab \equiv 1 \pmod{m}$. Это те и только те числа a, для которых $(a, m) = 1$.

Доказательство:

Если бы $d = (a, m)$ и $d > 1$, то ни для какого b сравнение $ab \equiv 1 \pmod{m}$ не могло бы выполняться, так как в противном случае d делил бы a - 1 и, следовательно, $1 \vdots d$.

Обратно, если $(a, m) = 1$, то можно считать, что $a < m$. Тогда в соответствии со следствием существуют целые числа u и v, для которых $u + v = 1$. Полагая $b = u$, получаем, что $1 - au = 1 - ab \vdots m$ ■

Малая теорема Ферма

Теорема:
Пусть $p \in \mathbb{P}$, $a \in \mathbb{Z}$ и $(a, p) = 1$, тогда $a^{p-1} \equiv 1 \pmod p$, если $(a, p) \neq 1$, то $a^p \equiv a \pmod p$.

Доказательство:
Рассмотрим сначала первую часть теоремы.
Докажем, что $0a, 1a, \ldots, (p-1)a$ образуют полную систему вычетов.
Пусть $i \cdot a \equiv j \cdot a \pmod p$, тогда $a \cdot (i-j) \equiv 0 \pmod p$. Поскольку a и p взаимно просты, то $p \vdots (i-j)$, так как i и j меньше p, это возможно лишь в случае $i = j$. Значит числа a, $2a$,…, $(p-1)a$ являются некоторой перестановкой чисел 1, 2,…, $p-1$. Значит произведение первого набора сравнимо по модулю с произведением второго набора, то есть $a^{p-1}(p-1)! \equiv (p-1)! \,(mod\ m)$. Получаем $(p-1)!\,(a^{p-1}-1) \equiv 0\ (mod\ m)$. Поскольку $\big((p-1)!, p\big) = 1$, то $(a^{p-1}-1) \vdots p$.
Если a делится на p, то случай тривиальный, поскольку обе части сравнимы с 0 по модулю p ■

Следствие:

Пусть $d = (a, b)$, где $a > b$. Тогда существуют такие целые числа u и v, что $d = ua + bv$. Другими словами, НОД двух чисел можно представить в виде линейной комбинации этих чисел с целыми коэффициентами.

Доказательство:

Будем проходит последовательность равенств в алгоритме Евклида снизу вверх и последовательно выражать d через все ранние остатки. В конце получим выражение d через a и b ■

Замечание

Обратимыми по умножению являются те элементы из Z/mZ, представители которых взаимно просты с m, т.е. числа a, для которых существует такое b, что $ab \equiv 1 \pmod{m}$. Это те и только те числа a, для которых $(a, m) = 1$.

Доказательство:

Если бы $d = (a, m)$ и $d > 1$, то ни для какого b сравнение $ab \equiv 1 \pmod{m}$ не могло бы выполняться, так как в противном случае d делил бы a - 1 и, следовательно, $1 \vdots d$.

Обратно, если $(a, m) = 1$, то можно считать, что $a < m$. Тогда в соответствии со следствием существуют целые числа u и v, для которых $u + v = 1$. Полагая $b = u$, получаем, что $1 - au = 1 - ab \vdots m$ ■

Функция Эйлера

Определение:

Пусть $m \in \mathbb{N}$, $m > 1$. Тогда $\varphi(m)$ – количество натуральных чисел, меньших m и взаимно простых с m.

Утверждение:

$$\varphi(p^{\alpha}) = p^{\alpha-1}(p-1), \text{ где } p \in \mathbb{P} \text{ и } \alpha \in \mathbb{N}$$

Доказательство:

Заметим, что среди числе от 1 до p^{α} ровно $p^{\alpha-1}$ чисел, что делятся на p: p, $2p$,…, $p^{\alpha-1} \cdot p$.

Значит среди чисел от 1 до p^{α} не делятся на p : $p^{\alpha-1}(p-1)$ ■

Теорема:

$\varphi(mn) = \varphi(m) \cdot \varphi(n)$, если $(m, n) = 1$(то есть выполняется мультипликативность)

Доказательство:

Рассмотрим числа от 1 до mn таким образом:

1	2	… m
m+1	m+2	… 2m
…		
m(n-1)+1	m(n-1)+2	… mn

Обратим внимание на случайный столбец:

r	В этом столбце полная система вычетов по модулю n. Пусть не так, тогда выполняется равенство:
$r+m$	$r+mx \equiv r+my \pmod m$, где НУО $0 \le x < y \le n-1$
…	То есть $m(y-x) \vdots n \Rightarrow y-x \vdots n$ (?!)
$r+m(n-1)$	

Тогда r,…, $r+m(n-1)$ дают все остатки от деления на n ровно по 1 разу, из которых $\varphi(n)$ взаимно простых с n.

Заметим, что если $(m, r) \neq 1$, то все числа в столбце не взаимно просты с m, значит они не взаимно просты с mn. Тогда подобных столбцов $\varphi(m)$.

Итого у нас $\varphi(m)$ столбцов, где $\varphi(n)$ чисел, взаимно простых с n. Значит, в таблице $\varphi(m)\varphi(n)$ чисел взаимно простых с mn. Получается, что $\varphi(mn) = \varphi(m)\varphi(n)$ ■

Следствие:

Пусть $n =$, тогда $\varphi(n) = ($

Теорема Эйлера:

$m \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, m) = 1$
Тогда

Доказательство:

- приведенная система вычетов по модулю m, то есть $s = \varphi(m)$

Так как $(a, m) = 1$, то a - тоже полная система вычетов по модулю m

Тогда:

$\Rightarrow \equiv 1 \pmod{m} \Rightarrow \equiv 1 \pmod{m}$ ■

Китайская теорема об остатках

Пусть требуется решить систему сравнений о различным модулям:

$x \equiv a_1 \ (mod\ m_1)$

$x \equiv a_2 \ (mod\ m_2)$

…

$x \equiv a_r \ (mod\ m_r)$

Причем любые два модуля взаимно просты. Тогда эта система разрешима и любые два решения сравнимы по модулю $M = m_1 \cdot \ldots \cdot m_r$

Доказательство:

Единственность по модулю M:

Пусть x' и x'' – два решения система, положим $x = x' - x''$. Тогда x сравним с 0 по любому модулю m_i, значит и по модулю M.

Как найти решение:

Пусть $M_i = \frac{M}{m_i}$. Заметим, что $(m_i, M_i) = 1$, тогда существует такое n_i, что $M_i \cdot n_i \equiv 1 \pmod{m_i}$

Положим, что $x = \sum_i a_i M_i n_i$.

Тогда для каждого i все слагаемые в этой сумме, за исключением i-го, делятся на m_i, так как $M_j \vdots m_i$ для всех $i \neq j$. Таким образом, для каждого i имеем $x \equiv a_i M_i n_i \equiv a_i \pmod{m_i}$ ■

Алгоритм быстрого возведения в степень

Дано: число b, модуль m. Хоти найти $b^n \pmod m$

Пусть $n_0, \ldots, n_{k-1}$ - цифры двоичной записи числа n, a – промежуточный результат умножения.

Если $n_0 = 1$, заменим a на b, иначе $a = 1$. Далее возведем b в квадрат и скажем, что $b_1 \equiv b^2 \pmod m$. Если $n_1 = 1$, умножим a на b_1, иначе a останется таким же. Далее возведем b_1 в квадрат и скажем, что $b_2 \equiv {b_1}^2 \pmod m$. И так далее. После k-1 шага $a \equiv b^n \pmod m$.