ЛЕКЦИЯ 15. МОДУЛЬНАЯ АРИФМЕТИКА

ТЕОРИЯ ДЕЛИМОСТИ

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

Определение 1. Для положительных целых чисел a и b существуют и единственны неотрицательные целые числа q (*целое частное*) и r (*остаток*), где $0 \le r \le b$ такие что

$$a = bq + r.$$

Определение 2. *Наибольшим общим делителем* a и b называют такое положительное число $d = НОД(a,b)$, что

1) $d \mid a, d \mid b$
2) d – наибольшее из таких чисел

Определение 3. *Наименьшим общим кратным* a и b называют такое положительное число $c = НОК(a,b)$, что

3) $c \vdots a, c \vdots b$
4) c – наименьшее из таких чисел

Теорема. $НОК(a,b) = \dfrac{a \cdot b}{НОД(a,b)}$.

Доказательство: позже.

АЛГОРИТМ ЕВКЛИДА

<pre>while a!=b:
    if a>b:
        a -= b
    else:
        b -=a
print(a)</pre>
	<pre>while b>0:
	    r = a % b
	    a, b = b, r
	print(a)</pre>

медленный вариант	быстрый вариант

Пример: НОД(42,30) =6

42=30*1+12

30=12*2+6

12=6*2+0

ЛИНЕЙНОЕ ПРЕДСТАВЛЕНИЕ НОД

ТЕОРЕМА 3.32. Наибольший общий делитель положительных целых чисел a и b существует. Такой наибольший общий делитель может быть записан в виде

$$u \cdot a + v \cdot b$$

для некоторых целых чисел u и v. Кроме того, наибольший общий делитель — это наименьшее положительное целое число такого вида.

ДОКАЗАТЕЛЬСТВО. Пусть S — множество всех положительных целых чисел, имеющих форму $na + mb$. Пусть $d = ua + vb$ — наименьший элемент множества S. Тогда $d \leq a$, т.к. $a = 1 \cdot a + 0 \cdot b$ принадлежит S. Кроме того, $a = qd + r$ для некоторых q и r, где $q > 0$ и $0 \leq r < d$. Итак, $a = q(ua + vb) + r$. Решая относительно r, получаем, $r = (1 - qu)a + (-v)qb$, так что r принадлежит S или $r = 0$. Но r меньше, чем d, которое, в свою очередь, является наименьшим элементом множества S, так что $r = 0$. Поэтому $d \mid a$. Аналогично, $d \mid b$. Если c — произвольный делитель чисел a и b, то по теореме 3.24 часть (в) $c \mid d$, поскольку $d = ua + vb$. Следовательно, d — наибольший общий делитель чисел a и b. ■

Найти линейное представление НОД можно из алгоритма Евклида, двигаясь по нему *в обратную сторону*.

Следствие. НОД(a,b) делится на любой другой общий делитель a,b (иногда это свойство берут в качестве определения НОД).

Пример:

6 = 30 – 12*2 = 30 – (42 – 30*1)*2 = 30*3 + 42*(-2)

ВЗАИМНО ПРОСТЫЕ ЧИСЛА

Определение. Числа a и b называются *взаимно простыми*, если НОД(a,b)=1.

Теорема. Числа a и b взаимно просты т. и т.д., когда найдутся такие целые u и v, что

$$au + bv = 1.$$

Доказательство: из теоремы о линейном представлении НОД.

ПРОСТЫЕ ЧИСЛА

Определение. Целое число, большее 1, называется *простым*, если оно делится только на 1 и на себя. Целое число, большее 1, называется *составным*, если оно не простое.

ТЕОРЕМА 3.40. (Евклид) Существует бесконечно много простых чисел.

ДОКАЗАТЕЛЬСТВО. Допустим, что существует только конечное число простых чисел, например, $p_1, p_2, \ldots, p_k$. Рассмотрим целое число $(p_1 p_2 \cdots p_k) + 1$. Предположим, что p_r — некоторое простое число, и $p_r \mid ((p_1 p_2 \cdots p_k) + 1)$. Но тогда $p_r \mid (p_1 p_2 \cdots p_k)$, откуда следует, что $p_r \mid 1$, а это приводит к противоречию, т.к. $p_r > 1$. Следовательно, $(p_1 p_2 \cdots p_k) + 1$ — простое число, что, в свою очередь, также является противоречием, т.к. этого числа нет среди указанной конечной совокупности простых чисел. Таким образом, наше предположение о том, что существует конечное число простых чисел, ложно, поэтому простых чисел должно быть бесконечно много. ■

Постулат Бертрана или теорема Чебышёва: при любом n>2 в интервале от n до 2n найдётся простое число.

Сформулировал и проверил для n<=3 000 000 Бертран, а доказал Чебышёв.

ПРОВЕРКА НА ПРОСТОТУ

ТЕОРЕМА 3.41. Если положительное целое число n является составным, то n имеет простой делитель p такой, что $p^2 \leq n$.

ДОКАЗАТЕЛЬСТВО. Пусть p — наименьший простой делитель числа n. Если n раскладывается на множители r и s, то $p \leq r$ и $p \leq s$. Следовательно, $p^2 \leq rs = n$. ■

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

ТЕОРЕМА 3.46. (Основная теорема арифметики) Любое положительное целое число, большее, чем 1, либо является простым, либо может быть записано в виде произведения простых чисел, причем это произведение единственно с точностью до порядка сомножителей.

ТЕОРЕМА 3.49. Пусть $a = p_1^{a(1)} p_2^{a(2)} p_3^{a(3)} \cdots p_k^{a(k)}$ и $b = p_1^{b(1)} p_2^{b(2)} p_3^{b(3)} \cdots p_k^{b(k)}$, где p_i — простые числа, которые делят либо a, либо b, и некоторые показатели степени могут быть равны 0. Пусть $m(i) = \min(a(i), b(i))$ и $M(i) = \max(a(i), b(i))$ для $1 \leq i \leq k$. Тогда

$$\text{НОД}(a, b) = p_1^{m(1)} p_2^{m(2)} p_3^{m(3)} \cdots p_k^{m(k)}$$

и

$$\text{НОК}(a, b) = p_1^{M(1)} p_2^{M(2)} p_3^{M(3)} \cdots p_k^{M(k)}.$$

Следствие. $НОК(a,b) = \dfrac{a \cdot b}{НОД(a,b)}$.

Пример:

Применим теорему 3.49 в случае, когда $a = 195000$ и $b = 10435750$. Разложения на простые множители чисел a и b имеют вид

$$a = 2^3 3^1 5^4 13^1 \qquad \text{и} \qquad b = 2^1 5^3 13^3 19^1 .$$

Таким образом,

$$\begin{aligned}
\text{НОД}(195000, 10435750) &= 2^{\min(3,1)} 3^{\min(1,0)} 5^{\min(4,3)} 13^{\min(1,3)} 19^{\min(0,1)} = \\
&= 2^1 3^0 5^3 13^1 19^0 = 2^1 5^3 13^1 = 3250, \\
\text{НОК}(195000, 10435750) &= 2^{\max(3,1)} 3^{\max(1,0)} 5^{\max(4,3)} 13^{\max(1,3)} 19^{\max(0,1)} = \\
&= 2^3 3^1 5^4 13^3 19^1 = 626145000 .
\end{aligned}$$

ТЕОРИЯ СРАВНЕНИЙ

СРАВНЕНИЯ

ОПРЕДЕЛЕНИЕ 3.51. Пусть n — положительное целое число. Целое число a ***сравнимо*** с целым числом b по модулю n, что обозначается $a \equiv b \pmod{n}$, если n делит $(a - b)$.

ТЕОРЕМА 3.52. Отношение $\equiv$ для фиксированного n является отношением эквивалентности на множестве целых чисел. Это означает, что

а) $a \equiv a \pmod{n}$ для каждого целого числа a;

б) если $a \equiv b \pmod{n}$, то $b \equiv a \pmod{n}$ для целых чисел a и b;

в) если $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n}$, то $a \equiv c \pmod{n}$.

СВОЙСТВА СРАВНЕНИЙ

ТЕОРЕМА 3.54. Отношение сравнимости обладает следующими свойствами:

а) если $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$, то $a + c \equiv b + d \pmod{n}$ и $ac \equiv bd \pmod{n}$;

б) если $a \equiv b \pmod{mn}$, то $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$.

в) к обеим частям сравнения можно прибавлять (вычитать) одно и то же число;

г) обе части сравнения можно домножать на одно и то же число;

д) если a сравнимо с b, то и a^k сравнимо с b^k;

е) обе части сравнения можно делить на число, **взаимно простое с модулем**;

ж) можно делить a,b,m на любое число (например, на их НОД).

ВЫЧЕТЫ

Определение 1. Каждый класс эквивалентности называется *классом вычетов по модулю n* и обозначается

$$[a]_n = \{b : b \equiv a (\operatorname{mod} n)\}.$$

Определение 2. Множество всех вычетов обозначается Z_n и называется *кольцом вычетов по модулю n*.

На множестве Z_n можно определить операции сложения и умножения. Если $[a]$ — класс вычетов по модулю n, содержащий a, и $[b]$ — класс вычетов по модулю n, содержащий b, то сложение и умножение определим соотношениями

$$[a] \oplus [b] = [a + b] = [[a + b]]_n,$$
$$[a] \odot [b] = [a \cdot b] = [[a \cdot b]]_n,$$

Когда и так понятно, что речь идёт о вычетах, часто используют сокращённую запись, принятую в «обычной» арифметике, и вместо $[a]\oplus[b]$ пишут $a+b$, а вместо $[a]\odot[b]$ - просто ab.

Вычисляя все возможные суммы и произведения (а их конечное число!), можно создать *таблицы сложения и умножения* в $\mathbb{Z}_n$. При различных n они будут обладать различными интересными свойствами.

Пример 1. Таблицы сложения и умножения в $\mathbb{Z}_5$:

$a+b$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a \cdot b$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Вопрос: какие свойства вы можете заметить у этих таблиц?

Пример 2. Таблица умножения в $\mathbb{Z}_4$:

$a \cdot b$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Можно заметить, что в этой таблице появились т.н. *делители нуля*: $2 \cdot 2 = 0$ (т.е. при умножении ненулевых чисел можем получить 0!).

ПОЛНАЯ И ПРИВЕДЁННАЯ СИСТЕМЫ ВЫЧЕТОВ

Определение 1. *Полной системой вычетов* по модулю n называется такое множество чисел $\{r_1, r_2, ..., r_n\}$, в котором все числа r_i выбраны из разных классов эквивалентности.

Определение 2. *Первичная или каноническая система вычетов* по модулю n: $\{0, 1, ..., n-1\}$.

Определение 3. *Приведённая система вычетов* по модулю n – такое подмножество полной системы вычетов, в котором все числа **взаимно просты** с n.

Приведённая система вычетов образует *мультипликативную подгруппу* в кольце вычетов: это значит, что каждый приведённый вычет имеет обратный по умножению (при этом остальные вычеты обратных не имеют!). Другими словами, в приведённой системе вычетов *возможно деление*.

ТЕОРЕМА 3.65. Пусть n — положительное целое число и $\{r_1, r_2, \ldots, r_k\}$ — полная [приведенная] система вычетов по модулю n. Если a — целое число, взаимно простое с n, то $\{ar_1, ar_2, \ldots, ar_k\}$ — также полная [приведенная] система вычетов.

Пример 1. Приведённая система вычетов в Z_5: {1,2,3,4}.

$$1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4$$

Пример 2. Приведённая система вычетов в Z_4: {1,3}.

$$1^{-1} = 1, 3^{-1} = 3$$