8ВМ, спецкурс, занятие 18
13 января 2023
Деление по модулю

Научимся говорить о сравнениях на немного другом языке.

Зафиксируем модуль m. Отношение сравнимости по модулю m является отношением эквивалентности, поэтому все целые числа можно разбить на классы эквивалентности. Иными словами, можно разложить все целые числа в m «ящиков» в зависимости от остатка от деления на m.

$\ldots, -2m,$ $-m, \mathbf{0}, m,$ $2m, 3m, \ldots$	$\ldots, 1-2m,$ $1-m, \mathbf{1}, m+1,$ $2m+1, \ldots$	$\ldots, 2-2m,$ $2-m, \mathbf{2}, m+2,$ $2m+2, \ldots$	$\ldots$	$\ldots, -1-m,$ $-1, \boldsymbol{m-1}, 2m-1,$ $3m-1, \ldots$

Внутри каждого ящика все элементы сравнимы друг с другом по модулю m, а элементы из разных ящиков не сравнимы.

Через $[a]$ будем обозначать *класс* числа a (то есть ящик, где лежит a). Один и тот же класс можно обозначить разными способами, например $[0]=[m]$, а $[m-1]=[-1]$. Равенство классов — это все равно что сравнимость элементов по модулю: $[a]=[b]$ означает, что $a \equiv b \pmod m$.

Классы можно складывать. Чтобы сложить классы A и B нужно взять какое-то число a из A, какое-то число b из B, и результатом этого сложения станет класс, в котором лежит $a+b$. То есть, $[a]+[b]=[a+b]$.

Важно, что результат не зависит от того, какие именно числа мы берем из каждого класса. Действительно, пусть вместо a мы взяли c из класса A, а вместо b мы взяли d из класса B. Тогда $a \equiv c \pmod m$ и $b \equiv d \pmod m$. Но тогда $a+b \equiv c+d \pmod m$, и $c+d$ попадет в тот же класс, что и $a+b$.

Аналогичным образом, классы можно вычитать и умножать: $[a]-[b]=[a-b]$ и $[a]\cdot[b]=[ab]$. А вот возводить в степень класса нельзя. Например, $[1]=[4]$ по модулю 3. Но при этом $[2^1]=[2]$, а $[2^4]=[16]=[1]$. Значит, определить, что такое $2^{[1]}$, мы не можем.

Определение. Множество всех классов по модулю m обозначается $\mathbb{Z}_m$. Оно состоит из m элементов:

$$\mathbb{Z}_m = \{[0], [1], [2], \ldots, [m-1]\}$$

Эти элементы можно складывать, вычитать и умножать.

Множество, любые два элемента которого можно складывать, вычитать и умножать, называется *кольцом*. Множество $\mathbb{Z}_m$ называется *кольцом остатков* по модулю m.

Замечание. *Решить сравнение* по модулю m — это значит «решить уравнение в множестве $\mathbb{Z}_m$». Иными словами, найти все классы, которым может принадлежать переменная.

Например, пусть нужно решить сравнение $x^2 \equiv 1 \pmod 8$. Это все равно что решить уравнение $[x]^2=1$ в множестве классов $\mathbb{Z}_8$. Решениями являются $[x]=[1]$, $[x]=[3]$, $[x]=[5]$, $[x]=[7]$. Иными словами, $x \equiv 1 \pmod 8$, $x \equiv 3 \pmod 8$, $x \equiv 5 \pmod 8$ или $x \equiv 7 \pmod 8$.

Для решения уравнений нам очень часто приходится делить. Но как делить классы друг на друга?

Определение. Разделить класс $[b]$ на класс $[a]$ (разделить b на a по модулю m) — значит найти такой класс $[x]$, что $[a]\cdot[x]=[b]$ (то есть решить сравнение $ax\equiv b \pmod m$).

Предложение. Пусть $k\neq 0$. Тогда

$$ka \equiv kb \pmod{km} \Longleftrightarrow a \equiv b \pmod m.$$

Иными словами, можно домножить или сократить обе половины сравнения и его модуль на множитель k.

Но можно ли домножать и сокращать сравнения, не трогая модуль? Домножать можно, это было доказано на прошлой лекции. А вот сокращать можно не всегда. Действительно, $2\equiv 12 \pmod{10}$, но $1\not\equiv 6 \pmod{10}$.

Предложение. Пусть НОД$(k, m)=1$. Тогда сравнения по модулю m можно сокращать на k:

$$ka \equiv kb \pmod m \Longrightarrow a \equiv b \pmod m.$$

Следствие. Если НОД$(k, m)=1$ и $a\not\equiv b \pmod m$, то $ka\not\equiv kb \pmod m$.

Следствие. Пусть НОД$(k, m)=1$. Тогда все числа $0k$, $1k$, $2k$, $3k$, ..., $(m-1)k$ дают разные остатки по модулю m. Поскольку тут m чисел, и остатков тоже m, то эти числа дают все остатки по одному разу.

Иными словами, $[0k]$, $[1k]$, $[2k]$, ..., $[(m-1)k]$ — это все элементы множества $\mathbb{Z}_m$ (только, возможно, в перепутанном порядке).

Следствие. Если a взаимно просто с модулем m, то можно *делить* на a по модулю m. Чтобы поделить b на a найдем среди чисел $0a$, $1a$, $2a$, ..., $(m-1)a$ то единственное число xa, которое сравнимо с b по модулю m.

Получится, что $xa\equiv b \pmod m$, а значит можно сказать, что $x\equiv b : a \pmod m$.

Теперь научимся делить быстро. Чтобы поделить $[b]$ на $[a]$, нужно решить сравнение $ax\equiv b \pmod m$. Иными словами, мы ищем такие x, что $ax-b \,\vdots\, m$. Значит, $ax-b=my$ и $ax-my=b$.

Это *линейное диофантово уравнение*. Поскольку a и m взаимно просты, то у него есть целые решения x и y. Мы умеем их искать (достаточно только x и только одного).

Наконец, есть еще один способ делить по модулю, покажем его на примере. Пусть надо разделить 5 на 17 по модулю 31.

$$17x \equiv 5 \pmod{31} \text{ (сравнение, которое надо решить)}$$

$$31x \equiv 0 \pmod{31} \text{ (верно при всех } x\text{)}$$
$$34x \equiv 10 \pmod{31} \text{ (умножаем первое на 2)}$$
$$3x \equiv 10 \pmod{31} \text{ (разность двух предыдущих)}$$
$$18x \equiv 60 \equiv -2 \pmod{31} \text{ (умножаем на 6)}$$
$$x \equiv -7 \pmod{31} \text{ (из последнего вычитаем первое)}$$

Таким образом, $[5]:[17]=[-7]=[24]$ по модулю 31.

Следствие. По простому модулю можно делить на любое число (не сравнимое с 0).

То есть, если p — простое число, то элементы множества $\mathbb{Z}_p$ можно делить друг на друга (только не на 0). Такое множество, элементы которого складывать, вычитать, умножать и делить, называется *полем*.

1 Пусть НОД$(a, m) = d$ и b не делится на d. Докажите, что сравнение $ax \equiv b \pmod{m}$ не имеет решений.

2 Пусть $xy \equiv 0 \pmod{m}$.

a Докажите, что если m — простое число, то $x \equiv 0 \pmod{m}$ или $y \equiv 0 \pmod{m}$.

b Докажите, что если m не является простым числом, то x и y могут быть оба не сравнимы с 0.

3 Решите сравнения:

a $7x \equiv 2 \pmod{13}$;

b $334x \equiv 123 \pmod{1001}$;

c $1543x \equiv 2023 \pmod{29}$;

d $4x \equiv 2 \pmod{22}$;

e $36x \equiv 15 \pmod{51}$.

4 Решите квадратные сравнения:

a $x^2 + 3 \equiv 0 \pmod{19}$;

b $x^2 + 3x \equiv 15 \pmod{17}$;

c $x^2 + 1533x \equiv 1527 \pmod{1543}$;

d $x^2 - 4 \equiv 0 \pmod{15}$.

5 Известно, что x^2 оканчивается на 001. На какие три цифры может оканчиваться x?

6 a Пусть p — простое число. Поскольку по модулю p можно делить на что угодно, кроме 0, то все ненулевые остатки можно разбить на пары обратных: остатку a в пару дадим такой остаток b, что $ab \equiv 1 \pmod{p}$. Какие числа окажутся в паре сами с собой?

b (**Теорема Вильсона**) Докажите, что $(p-1)! \equiv -1 \pmod{p}$.

c Докажите, что если n не простое, то $(n-1)! \not\equiv -1 \pmod{n}$. С чем в этом случае сравнимо $(n-1)!$ по модулю n?

Следующие задачи не обязательно используют деление по модулю

7 Докажите, что сумма квадратов пяти последовательных чисел не может быть полным квадратом.

8 Докажите, что уравнение $15x^2 - 7y^2 = 9$ не имеет решений в целых числах.

9 Найдите все такие натуральные m и n, что $1! + 2! + \cdots + n! = m^2$.