8В, спецкурс, занятие 17

19 января 2024

Деление по модулю

Определение. *Разделить b на a по модулю m* – это найти такой x, что $xa \equiv b \pmod m$.

Предложение. Пусть $k \neq 0$. Тогда

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

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 $\text{НОД}(k, m) = 1$. Тогда сравнения по модулю m можно сокращать на k:

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

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

Следствие. Пусть $\text{НОД}(k, m) = 1$. 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.

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. Нам 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.

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

$$31x \equiv 0 \pmod{31} \text{ (верно при всех } x)$$

$$34x \equiv 10 \pmod{31} \text{ (умножаем первое на 2)}$$

$$3x \equiv 10 \pmod{31} \text{ (разность двух предыдущих)}$$

$$18x \equiv 60 \equiv -2 \pmod{31} \text{ (умножаем на 6)}$$

$$x \equiv -7 \pmod{31} \text{ (из последнего вычитаем первое)}$$

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

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

2$^{\vee}$ 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 (ответ дайте в виде «x сравнимо с... по исходному модулю»):

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

b$^{\vee}$ $1543x \equiv 2024 \pmod{29}$;

c$^{\vee}$ $331x \equiv 123 \pmod{1001}$;

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?

Будем говорить, что остаток b *обратный* к остатку a по модулю m (пишем $b = a^{-1}$), если $ab \equiv 1 \pmod m$. Остатки, у которых есть обратные, называются *обратимыми.*

6 a Пусть p – простое число. Какие остатки по модулю p обратимы? Разобьем все обратимые остатки на пары обратных. Какие остатки оказались 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?

7 Трудолюбивая Вероника сложила сто дробей: $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{100}$ и получила в итоге несократимую дробь $\frac{m}{n}$. Докажите, что m делится на 101.

8 Число q простое. Докажите, что $(2q-1)! - q$ делится на q^2.

9* (**Теорема Вольстенхольма**) Пусть $p \geq 5$ – простое число.

a Сложили $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$, получили несократимую дробь $\frac{m}{n}$. Докажите, что m делится на p.

b Сложили $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$, получили несократимую дробь $\frac{m}{n}$. Докажите, что m делится на p^2.

c Вспомните, что $C_{2n}^n = (C_n^0)^2 + (C_n^1)^2 + \cdots + (C_n^n)^2$.

d Докажите, что $C_{2p}^p \equiv 2 \pmod{p^3}$.

Тут две независимые задачи: a-b и a-c-d. За каждую из них ставится отдельная звездочка.