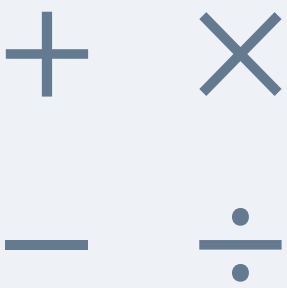


Арифметика остатков

Еще раз вспомним:

Как записать, что d - остаток от деления числа a на число b:

$$a = a_1 \cdot b + d, \text{ где}$$

$a_1, a \in \mathbb{Z}$!

$b \in \mathbb{N}$

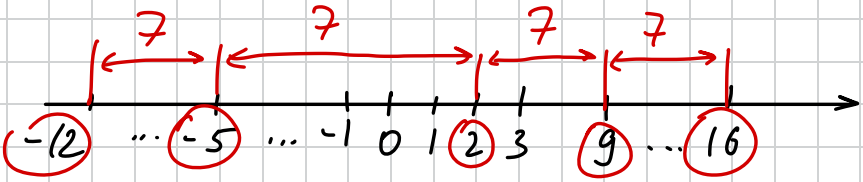
$d \in \{0, 1, 2, \dots, b-1\}$

остаток не бывает отрицательным!

Например: $100 = 14 \cdot 7 + 2$

$-100 = -15 \cdot 7 + 5$

Давайте посмотрим как на числовой оси располагаются числа, которые при делении на 7 дают остаток 2.



Т.е. все эти числа имеют что-то одинаковое (остаток от деления на 7) => нужно научиться это записывать

Опр 1: $a \equiv b \pmod m$ или $a \equiv_m b$, если a и b имеют одинаковый остаток при делении на m.

Читается как: a сравнимо с b по модулю m

Например: $16 \equiv -12 \pmod 7$

$16 \equiv_7 -12$

Как мы ранее выяснили: если числа имеют одинаковый остаток при делении на m, то на числовой оси расстояние м/у ними $= m$. Переформулируем это по-математически и докажем.

Лемма: $a \equiv b \pmod m \Leftrightarrow a - b \vdots m$

▲

$\boxed{\Rightarrow}$ $a = k_1 m + d_1$, где $k_1 \in \mathbb{Z}$, $d_1 \in \{0, 1, \dots, m-1\}$

$b = k_2 m + d_1$, где $k_2 \in \mathbb{Z}$, $d_1 \in \{0, 1, \dots, m-1\}$

Вычитаем одно из другого:

$$\underbrace{a - b}_{\vdots m} = \underbrace{(k_1 - k_2) m}_{\Leftarrow \vdots m}$$

$\Leftarrow$ $a = k_1 m + d_1$, где $k_1 \in \mathbb{Z}$, $d_1 \in \{0, 1, \dots, m-1\}$

$b = k_2 m + d_2$, где $k_2 \in \mathbb{Z}$, $d_2 \in \{0, 1, \dots, m-1\}$

Вычтем:

$$\underbrace{a-b}_{\vdots m} = \underbrace{(k_1-k_2)m}_{\vdots m} + \underbrace{d_1-d_2}_{\vdots m} \Rightarrow$$

но: $d_1 - d_2 \in \{-(m-1), \dots, 0, \dots, (m-1)\}$

из этих чисел только 0 делится на m

$\Rightarrow d_1 = d_2$ ■

Свойства сравнения по модулю:

Св-во 1°: Если $a \equiv_m b$, $c \equiv_m d$, то $a+c \equiv_m b+d$, $a-c \equiv_m b-d$ и $!a \cdot c \equiv_m b \cdot d!$

▲

1) Покажем, что $(a+c)-(b+d) \vdots m$, тогда, по лемме выше, получим что $a+c \equiv_m b+d$

$$a+c-b-d = \underbrace{(a-b)}_{\vdots m} + \underbrace{(c-d)}_{\vdots m} \vdots m$$

2) Аналогично для $(a-c)-(b-d)$

3) Для $ac \equiv_m bd$ аналогичная идея:

$$ac - bd = ac - bd + bc - bc = \underbrace{(a-b)c}_{\vdots m} - b\underbrace{(c-d)}_{\vdots m} \vdots m$$

■

! Следствие (из св-ва 1°): Если $a \equiv_m b \overset{1°}{\Rightarrow} a^2 \equiv_m b^2, \dots$

$\dots, a^k \equiv_m b^k$

Св-во 2°: Если $k \in \mathbb{Z}$ и $a \equiv_m b$, то $ka \equiv_m kb$

Св-во 3°: Если $m = a \cdot b$ и $N \equiv_m r$, то

$N \equiv_a r$ и $N \equiv_b r$

▲

$N \equiv_m r \overset{\text{Лемма}}{\Leftrightarrow} N - r \vdots m \Leftrightarrow \exists k : N = km + r$

Тогда $N = kab + r$

То есть $N - r \vdots a$, т.к. $N - r = kb \cdot a$ и

$N - r \vdots b$, т.к. $N - r = ka \cdot b$

■

№1 Найдите остаток при делении 1) 2^{2018} на 15
2) 2^{2018} на 17

1) Какая степень двойки не сильно отличается от 15? : $2^4 = 16 \equiv_{15} 1$

Тогда, по следствию из св-ва 1°: $16^k \equiv_{15} 1^k = 1$

обратите внимание, что 1 - последний остаток, т.к. $1^k = 1$

Тогда: $2^{2018} = 2^2 \cdot 2^{2016} = 4 \cdot (2^4)^{504} \equiv_{15} 4 \cdot 1^{504} = 4$

То есть остатки у 2^{2018} и 4 при делении на 15 совпадают $\Rightarrow$ Отв.: 4

2) Опять же - нам нужно найти число, такое что $\equiv_{15} 1$ или $\equiv_{15} (-1)$ (чтобы легко решить)

Найти число $\equiv_{15} 1$ в степенях двойки сложно. Вспомним про отрицательные числа

$$2^4 = 16 \equiv_{17} -1$$

Тогда $16^k \equiv_{17} (-1)^k$ и $2^{2018} \equiv_{17} 4 \cdot (-1)^{504} = 4$

$\Rightarrow$ Отв: 4

№2 Найдите остаток от деления 521^{637} на 17

1) Упростим основание: $521 \mid 17$, $51 \mid 30$, остаток 11

$$521 \equiv_{17} 11 \equiv_{17} -6$$

Еще раз - из опр-я $\equiv_{17}$ - все эти числа имеют одинаковые остатки при делении на 17

Тогда $521^{637} \equiv_{17} -6^{637}$

2) Найдем степень 6-ки, которая имеет небольшой остаток при делении на 17: $6^2 = 36 \equiv_{17} 2$

Тогда: $-6^{637} = -6 \cdot (6^2)^{318} \equiv_{17} -6 \cdot 2^{318} \Rightarrow$

Вспоминаем: $2^4 \equiv_{17} -1$

$$\Rightarrow -6 \cdot 2^{318} = -6 \cdot 2^2 \cdot (2^4)^{79} \equiv_{17} -6 \cdot 4 \cdot (-1)^{79} = 24$$

$318 = 79 \cdot 4 + 2$

3) То есть 521^{637} и 24 имеют одинаковый остаток при делении на 17

Ответ: 7

Признаки делимости

Рассмотрим число $N = \overline{a_n \dots a_1 a_0}$

Как еще его можно записать?

$$N = a_0 + 10 \cdot \overline{a_n \dots a_2 a_1}$$

Вспомним, что $10 : 2,5,10$, т.е. $10 \underset{2,5,10}{\equiv} 0$. Тогда по св-ву 1°:

$$N \underset{2,5,10}{\equiv} a_0$$

Признак делимости на 2,5,10:

Если последняя цифра числа делится на 2,5,10, то и все число делится на 2,5,10.

Аналогично, N можно представить в виде:

$$N = \overline{a_1 a_0} + 100 \overline{a_n \dots a_2}$$

$:4, 25, 20, 50, 100$

2,5 - уже изучили

Аналогично получаем

$$N \underset{\substack{4,25,20\\50,100}}{\equiv} \overline{a_1 a_0} \Rightarrow$$ признак делимости на 4, 25, 100, 20, 50

Можно продолжать "отсчитывать" по одной цифре и получать признаки делимости на любой делитель 1000, 10000 и т.д.

Теперь представим N как:

$$N = a_0 + 10a_1 + 10^2 a_2 + \ldots + 10^n a_n \quad (*)$$

По какому модулю 10 имеет маленький остаток? (Лучше всего "1", т.к. $1^n = 1$ и можно применять следствие из 1°):

$$10 \equiv 1 \pmod{\substack{9\\3}}$$

9 это хорошо, т.к. $9 = 10 - 1$

Тогда равенство (*) по mod 9 или mod 3:

$$N \equiv a_0 + 1^1 a_1 + 1^2 a_2 + \ldots + 1^n a_n$$

$$N \equiv a_0 + \ldots + a_n \pmod{\substack{9\\3}}$$

Признак делимости на 3, 9:

Если сумма цифр числа делится на 3, 9, то и все число делится на 3, 9

Вспомним, что еще хорошо сравнивать числа с (-1), т.к. $(-1)^2 = 1$, $(-1)^3 = -1$, ...; А по какому модулю сравнимы 10 и -1?

$$10 \equiv -1 \pmod{10+1=11}$$

Тогда:

$$N = a_0 + 10a_1 + 10^2 a_2 + \ldots + 10^n a_n \underset{11}{\equiv} a_0 + (-1)^1 a_1 + (-1)^2 a_2 + \ldots + (-1)^n a_n = a_0 - a_1 + a_2 - a_3 + \ldots + (-1)^n a_n$$

Признак делимости на 11

начиная с "+" - "справа"

Если знакочередующаяся сумма цифр числа делится на 11, то и все число делится на 11.

Аналогично можно сделать, заметив что $100 \underset{99}{\underset{13}{\equiv}} 1$,

тогда

$$N = \overline{a_1 a_0} + 100\,\overline{a_3 a_2} + 100^2\,\overline{a_5 a_4} + \ldots \underset{99}{\underset{13}{\equiv}} \overline{a_1 a_0} + \overline{a_3 a_2} + \ldots$$

↑ такое обычно редко нужно

Можно еще попробовать $100 \underset{101}{\equiv} -1$, но 101 простое ⇒

⇒ не дает нам интересных делителей

Попробуем разбить на группы по 3:

$$N = \overline{a_2 a_1 a_0} + 1000\,\overline{a_5 a_4 a_3} + \ldots$$

Как всегда: $1000 \equiv 1 \pmod{999}$: $999 = 9 \cdot 111 =$

$= \underbrace{9 \cdot 3}_{\text{уже изучили}} \cdot 37 \Rightarrow 1000 \underset{37}{\equiv} 1$ ⇒ получаем признак делимости на 37

↑ неинтересно

НО! $1000 \equiv -1 \pmod{1001}$, причем

$1001 = 7 \cdot 11 \cdot 13$, то есть $1000 \underset{7,13}{\equiv} -1$

11 - уже изучили

То есть

$$N \underset{7,13}{\equiv} \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \ldots - \ldots + \ldots$$

↑

Признак делимости на 7, 13:

Число делится на 7, 13, если на 7, 13 делится знакочередующаяся сумма групп по 3 цифры. (См. выше)

Таким образом, мы вывели признаки делимости на все числа до 17