

Делимость

Теорема 1.

Операция делимости рефлексивна:

$$a : a .$$

Теорема 2.

Операция делимости транзитивна:

Если $a : b$ и $b : c$, то $a : c$.

Теорема 3.

Делимость антисимметрична:

Если $a : b$ и $b : a$, то либо: $a=b$, либо $a=-b$.

Теорема 4.

Если $a : b$ и $|b| > |a|$, то $a=0$.

Следствие. Если $a : b$ и $a \neq 0$, то $|a| \geq |b|$.

Теорема 5.

Для того чтобы $a : b$, необходимо и достаточно, чтобы $|a| : |b|$

На основании этой теоремы в дальнейшем достаточно ограничиваться рассмотрением случая, когда делитель положительное число.

Теорема 6.

Если $a_1 : b$, $a_2 : b$, ..., $a_n : b$, то $(a_1 + a_2 + \dots + a_n) : b$

Следствие. Если сумма двух чисел и одно из них делится на некоторое число b , то на b делится и другое слагаемое.

Теорема 7.

(о делении с остатком). Для произвольных чисел a и b ($b > 0$) существуют и единственны такие числа q и r , что: $a = b \cdot q + r$, причем $0 \leq r < b$.

Теорема 8.

Простых чисел бесконечно много.

Наибольший общий делитель чисел a , b обозначается через (a, b) . Если $(a, b) = 1$, то числа a , b называются **взаимно простыми**.

Теорема 9.

Если a и p - натуральные числа, причем число p простое,

то либо $a : p$, либо a и p взаимно просты .

Всякое число, делящееся одновременно на числа a и b называется **общим кратным** чисел a и b .

Теорема 10.

Если M - общее кратное a и b , а m - их наименьшее общее кратное, то $M : m$.

Теорема 11.

Наименьшее общее кратное взаимно простых чисел равно их произведению.

Следствие. Для того чтобы число a делилось на взаимно простые числа b и c , необходимо и достаточно, чтобы оно делилось на их произведение.

Теорема 12.

Если $ab : c$, причем числа b и c взаимно простые, то $a : c$.

Теорема 13.

Если произведение нескольких сомножителей делится на простое число p , то хотя бы один из сомножителей делится на p .

Следствие. Если p - простое и $0 < k < p$, то число

$$C_p^k = \frac{1 \cdot 2 \dots (p-1)p}{1 \cdot 2 \dots (k-1) \cdot k \cdot 1 \cdot 2 \dots (p-k-1)(p-k)}$$

делится на p .

Теорема 14.

(основная теорема арифметики)

Всякое целое положительное число, кроме единицы, может быть представлено в виде произведения простых сомножителей и притом единственным способом:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$$

произведение стоящее в правой части называется **каноническим разложением** числа a .

Теорема 15.

Для того чтобы числа a и b были взаимно простыми, необходимо и достаточно, чтобы ни один из простых сомножителей, входящих в каноническое разложение числа a , не входил в каноническое разложение числа b .

Теорема 16.

Пусть

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$$

каноническое разложение числа a . Тогда для делимости $b : a$ необходимо и достаточно, чтобы:

$$b : p_1^{\alpha_1}, b : p_2^{\alpha_2}, \dots, b : p_r^{\alpha_r}$$

из теорем 15,16 вытекает, что делимость на произведение нескольких взаимно простых чисел равносильна делимости на каждое из них.

Теорема 17.

Пусть

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$$

каноническое разложение числа a . Тогда для делимости $a : b$ необходимо и достаточно, чтобы каноническое разложение числа b имело вид:

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_r^{\beta_r}$$

, где:

$$0 \leq \beta_1 \leq \alpha_1,$$

$$0 \leq \beta_2 \leq \alpha_2,$$

...

$$0 \leq \beta_r \leq \alpha_r$$

Теорема 18.

Пусть m и t - натуральные числа. Тогда m можно представить в виде такого произведения $m = m_1 \cdot m_2$, что $(m_1, t) = 1$ (взаимно просты) и найдется такое k , для которого $t^k : m_2$.

τ -функция

Число различных делителей числа a (включая 1 и само число a), с каноническим разложением:

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}$$

, равно:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_r + 1)$$

Теорема 19.

Для того чтобы числа a и b были равноостаточны при делении на m , необходимо и достаточно, чтобы $(a - b) : m$.

Следствие. Если числа a и b равноостаточны при делении на m , и $m : d$, то a и b равноостаточны при делении на d

Теорема 20.

Если при делении на m числа a_1, a_2, \dots, a_n равноостаточны числам b_1, b_2, \dots, b_n , то равноостаточными будут суммы $a_1 + a_2 + \dots + a_n$ и $b_1 + b_2 + \dots + b_n$

Следствие. Если при делении на m числа a и b равноостаточны, то такими же являются и степени a^n и b^n при любом натуральном n .

равноостаточные при делении на m числа a и b называют также сравнимыми по модулю m . Это обозначается так:

$$a \equiv b(\text{mod } m)$$

а сама эта формула называется сравнением. Сравнимость двух чисел по некоторому фиксированному модулю m , или что тоже самое, их равноостаточность при делении на m , также является некоторым отношением связывающим целые числа.

Свойства этого отношения:

1. Рефлексивность:

$$a \equiv a(\text{mod } m).$$

2. Симметричность: если

$$a \equiv b(\text{mod } m), \text{ то } b \equiv a(\text{mod } m)$$

3. Транзитивность: если

$$a \equiv b(\bmod m), \text{ и } b \equiv c(\bmod m), \text{ то } a \equiv c(\bmod m)$$

4. Число классов вычетов по модулю m равно m .

5. Если $a \equiv b(\bmod m)$ и $c \equiv d(\bmod m)$, то $a + c \equiv b + d(\bmod m)$

6. Если $a \equiv b(\bmod m)$ и $c \equiv d(\bmod m)$, то $ac \equiv bd(\bmod m)$

теорема Вильсона

Для того чтобы число p было простым, необходимо и достаточно, чтобы:

$$(p-1)! + 1 = 1 \cdot 2 \cdot \dots \cdot (p-1) + 1$$

делилось на p .

Если некоторое отношение обладает свойствами рефлексивности, симметричности и транзитивности, то оно называется **отношением эквивалентности** (или эквивалентным отношением). Простейший пример - отношение равенства.

Теорема 24.

Малая теорема Ферма (МТФ).

[YouTube, Савватеев]

Если число p простое, то $a^p - a \div p$.

или в форме сравнения:

$$a^{p-1} \equiv 1(\bmod p)$$

$$(p, a) = 1$$

Следствие. Если p простое и a не делится на p , то $a^{p-1} - 1$ делится на p , т.к. $a^p - a = a(a^{p-1} - 1)$

Пример. Пусть $p=13$ - любое простое и $a=1,2,3,4,5,6,7,8,9,10,11,12$ не делятся на 13, по МТФ: $a^{p-1} - 1$ делится на p , или, что тоже самое: a^{p-1} всегда дает остаток равный 1, при делении на p

Функция Эйлера

Пусть натуральное число m имеет каноническое разложение:

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

$$\varphi(m) = p_1^{\alpha_1-1}(p_1-1) \cdot p_2^{\alpha_2-1}(p_2-1) \cdot \dots \cdot p_k^{\alpha_k-1}(p_k-1)$$

функция Эйлера, определяет число взаимно простых с m чисел меньших m .

$$\text{Другая форма: } \varphi(m) = m \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_k}\right)$$

$$\text{Для простых чисел: } \varphi(p) = p - 1,$$

и таким образом на графике $\varphi(m)$ простые числа - экстремумы(максимумы), а числа с наибольшим числом делителей - экстремумы минимумы.

[питон-блокнот, график]

Пример. Пусть $m=41580$, найдем $\varphi(m), \tau(m)$

Каноническое разложение числа 41580	
$m := 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 41580$	
$p1 := 2$	$\alpha1 := 2$
$p2 := 3$	$\alpha2 := 3$
$p3 := 5$	$\alpha3 := 1$
$p4 := 7$	$\alpha4 := 1$
$p5 := 11$	$\alpha5 := 1$
число взаимно простых с m чисел, меньших m	
$\varphi := m \cdot \left(1 - \frac{1}{p1}\right) \cdot \left(1 - \frac{1}{p2}\right) \cdot \left(1 - \frac{1}{p3}\right) \cdot \left(1 - \frac{1}{p4}\right) \cdot \left(1 - \frac{1}{p5}\right) = 8640$	
$\varphi := p1^{\alpha1-1} \cdot (p1-1) \cdot p2^{\alpha2-1} \cdot (p2-1) \cdot p3^{\alpha3-1} \cdot (p3-1) \cdot p4^{\alpha4-1} \cdot (p4-1) \cdot p5^{\alpha5-1} \cdot (p5-1) = 8640$	
число делителей m включая единицу и само m	
$\tau := (\alpha1+1) \cdot (\alpha2+1) \cdot (\alpha3+1) \cdot (\alpha4+1) \cdot (\alpha5+1) = 96$	
это будут следующие числа	
[1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 14, 15, 18, 20, 21, 22, 27, 28, 30, 33, 35, 36, 42, 44, 45, 54, 55, 60, 63, 66, 70, 77, 84, 90, 99, 105, 108, 110, 126, 132, 135, 140, 154, 165, 180, 189, 198, 210, 220, 231, 252, 270, 297, 308, 315, 330, 378, 385, 396, 420, 462, 495, 540, 594, 630, 660, 693, 756, 770, 924, 945, 990, 1155, 1188, 1260, 1386, 1485, 1540, 1890, 1980, 2079, 2310, 2772, 2970, 3465, 3780, 4158, 4620, 5940, 6930, 8316, 10395, 13860, 20790, 41580]	

вычисление $\varphi(41580), \tau(41580)$.

Теорема 25.

При взаимно простых m_1 и m_2 имеет место равенство:

$$\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$$

Теорема 26.

(теорема Эйлера). Если числа a и m взаимно просты, то:

$$a^{\varphi(m)} - 1 \div m$$

или в форме сравнения:

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

$$(a, m) = 1$$

Теорема 27.

Если числа a и m взаимно просты, а числа k_1 и k_2 равноостаточны при делении на $\varphi(m)$, то числа a^{k_1} и a^{k_2} равноостаточны при делении на m .

Теорема 28.

Если числа a и b взаимно просты, то уравнение

$$ax + by = c$$

всегда разрешимо в целых числах, и целыми его решениями будут все пары чисел (x_t, y_t) , где

$$x_t = ca^{\varphi(b)-1} + b \cdot t$$

$$y_t = c \frac{1 - a^{\varphi(b)}}{b} - at$$

t - любое целое число .

Теорема 29.

Пусть m взаимно просто с 10 и k равноостаточно с $10^{\varphi(m)-1}$ при делении на m . Тогда числа:

$$10a + b \text{ и } a + kb$$

равноделимы на m .

(т.е. либо оба делятся на m , либо оба не делятся на m) .