# Делимост на числата.

Започваме да се занимаваме с основните свойства и операции с цели числа. Фундаментална роля играе

**Теорема за деление с частно и остатък.** *За всеки две цели числа* $a, b \in \mathbb{Z}$ *и* $b \neq 0$ *съществуват единствени цели числа* $q, r \in \mathbb{Z}$*, такива че*

$$a = bq + r$$

*и* $0 \leq r < |b|$.

И така, числото $q$, посочено в теоремата, се нарича частно, а числото $r$ – остатък. Когато делим цялото число $a$ на цялото ненулево число $b$ ще се стремим остатъкът $r$ да бъде цяло неторицателно число. Според теоремата $r$ не трябва да надминава модула на $b$. Все пак да отбележим, че е възможно делението да бъде извършено и с остатък $r$, изпълняващ условието $-|b| < r \leq 0$, но това няма да представлява интерес за нас.

**Задача 1.** *Извършете деление с частно и остатък за делимо* $a$ *и делител* $b$.

*1)* $a = 36, b = 8$*;*
*2)* $a = -36, b = 8$*;*
*3)* $a = 36, b = -8$*;*
*4)* $a = -36, b = -8$.

*Решение.* 1) Т.к. най-голямото кратно на 8, ненадминаващо 36 е $32 = 8.4$, а от своя страна $36 - 32 = 4$, то имаме, че

$$36 = 8.4 + 4.$$

2) Тук делимото и делителят имат различни знаци и затова може да мислим, че „се движим“ в отрицателната посока на числовата ос при

търсенето на частно. Най-голямото кратно на 8, което не надминава $-36$ е $-40 = 8.(-5)$ и $-36 - (-40) = 4$. Тогава

$$-36 = 8.(-5) + 4.$$

3) Отново търсим отрицателно частно. Най-голямото кратно на $-8$, което не надминава 36 отново е $32 = (-8).(-4)$. Очевидно имаме

$$36 = (-8).(-4) + 4.$$

4) Делимото и делителят имат еднакви знаци и очакваме частното да е положително. Очевидното решение, базирано на опита ни досега, е

$$-36 = (-8).5 + 4.$$

□

Да напоминим, че най-големият общ делител (НОД) на целите числа $a, b \in \mathbb{Z}$ е цяло число $d \in \mathbb{Z}$, което е общ делител, т.е. $d \mid a$ и $d \mid b$ и е най-голямо по модул. Последното означава, че всеки общ делител $d_1$ дели най-големия общ делител $d$. Бележим $d = (a, b)$.

Алгоритъм на Евклид за намиране на НОД е краен процес, който води до намирането на НОД за всеки две числа $a, b \in \mathbb{Z}$ стига (без ограничение на общността) $b \neq 0$. Правилото е следното:

1) делим $a$ на $b$ с частно $q$ и остатък $r$

$$a = bq + r;$$

2) ако $r = 0$ спираме – оказва се, че $b \mid a$ и тогава $(a, b) = b$; ако $r \neq 0$ делим $b$ на остатъка $r$ с частно $q_1$ и остатък $r_1$

$$b = q_1 r + r_1;$$

3) продължаваме да делим всеки предхден остатък $r_{i-1}$ на текущия $r_i$ с частно $q_{i+1}$ и следващ остатък $r_{i+1}$

$$r_{i-1} = q_{i+1} r_i + r_{i+1}, \quad i = 2, 3, \dots$$

докато не получим, че някой остаък е нулев, например $r_{n+1} = 0$. Последното задължително се члува след краен брой стъпки.

4) щом сме намерили нулев остатък $r_{n+1}$ спираме деленията (т.к. на 0 не се дели) и обявяваме остатъка $r_n$ за НОД на $a$ и $b$, т.е. $r_n = (a, b)$ е последният ненулев остатък.

**Задача 2.** *Намерете НОД на* 198 *и* 164.

*Решение.* Извършваме поредицата от деления, предписана от алгоритъма на Евклид и започваща с деление на 198 на 164. Имаме

$$\begin{aligned} 198 &= 164.1 + 34 \\ 164 &= 34.4 + 28 \\ 34 &= 28.1 + 6 \\ 28 &= 6.4 + 4 \\ 6 &= 4.1 + \boxed{2} \\ 4 &= 2.2 + 0 \end{aligned}$$

Последният ненулев остатък е 2 и следователно $(198, 164) = 2$. □

**Тъждество на Безу.** *Ако* $a, b \in \mathbb{Z}$ *и* $(a, b) = d$, *то съществуват числа* $u, v \in \mathbb{Z}$, *такива че*

$$ua + vb = d.$$

**Задача 3.** *Да се намерят цели числа* $u, v \in \mathbb{Z}$, *за които да е изпълнено*

$$u.198 + v.164 = 2.$$

*Решение.* Започваме „прочит“ на обратния ход на алгоритъма на Евклид, т.е. започваме да се движим от предпоследната към първата стъпка. Имаме, че

$$\boxed{2} = 6 - 4.$$

Оттук нататък на всяка стъпка заместваме по един от остатъците, продължавайки да се движим в обратната посока, докато стигнем до числата $a = 198$ и $b = 164$. И така, вече изразихме $\boxed{2}$. Следващата стъпка в обратната посока е да изразим

$$4 = 28 - 6.4.$$

Така получаваме

$$\boxed{2} = 6 - (28 - 6.4) = -28 + 5.6.$$

Следващата стъпка, движейки се отгоре надолу, е да изразим остатъка

$$6 = 34 - 28.$$

Така получаваме

$$\boxed{2} = -28 + 5.(34 - 28) = 5.34 - 6.28.$$

Издигайки се нагоре е време да изразим

$$28 = 164 - 34.4.$$

Това ни дава

$$\boxed{2} = 5.34 - 6.(164 - 34.4) = -6.164 + 29.34.$$

Поселдната стъпка на обратния ход естествно съвпада с първата стъпка на правия ход на алгоритъма. Изразяваме

$$34 = 198 - 164$$

и замествайки получаваме

$$\boxed{2} = -6.164 + 29.(198 - 164) = 29.198 - 35.164.$$

И така

$$29.198 - 35.164 = \boxed{2},$$

или с други думи $u = 29$ и $v = -35$ са търсените числа, за които става дума в тъждеството на Безу.

За да се уверим във верността на изчисленията си, правим проверката

$$29.198 - 35.164 = 5742 - 574 = 2.$$

$\square$

Да разгледаме линейното уравнение

$$ax + by = c$$

с неизвестни $x$ и $y$ и цели коефициенти $a, b, c \in \mathbb{Z}$, на което търсим само целочислени решения. Това е пример за диофантово уравнение от първа степен.

Ако $(a, b) = c$, то тъждеството на Безу ни гарантира съществуване на решение – двойката $(u, v)$.

Ако $(a, b) = d$ и $d \mid c$, то съществува $k \in \mathbb{Z}$, такова че $c = dk$. Тъждеството на Безу ни дава, че съществуват $u, v \in \mathbb{Z}$, такива че

$$a.u + b.v = d.$$

Сега ако умножим двете страни на горното равенство с $k$, то ще удовлетворим диофантовото уравнение

$$a(ku) + b(kv) = c$$

с решение двойката $(ku, kv)$.

Ако $(a, b) = d$ и $d \nmid c$, то не е трудно да се съобрази, че уравнението няма решение.

**Задача 4.** *Намерете решение на уравнението*

$$190x + 41y = 19.$$

*Решение.* Стратегията е да използваме алгоритъма на Евклид, за да намерим $(190, 41) = d$. След това тъждеството на Безу $190u + 41v = d$, ще ни помогне да намерим решение, ако то съществува. И така, с алгоритъма на Евклид намираме, че

$$(190, 41) = 1.$$

Очевидно $1 \mid 19$ и уравнението има решение. Проверяваме, че тъждеството на Безу е изпълнено с

$$190.(-11) + 41.51 = 1.$$

Сега, след умножение на двете страни с 19 получаваме, че

$$190.(-209) + 41.(969) = 19$$

или с други думи намерихме (частно) решение $(x_0, y_0) = (-209, 969)$. $\square$

Нека диофантовото уравнение $ax + by = c$ има решение. Може без ограничение да считаме, че $(a, b) = 1$ (Ако $(a, b) = d \neq 1$, то $d \mid c$ т.к. уравнението има решение. Тогава можем да разделим двете страни на $d$ и да получим еквивалентното уравнение $a_1x + b_1y = c_1$, където вече

$(a_1, b_1) = 1$.) Нека $(x_0, y_0)$ е едно частно решение. Тогава имаме, че са изпълнени

$$\begin{aligned} ax + by &= c \\ ax_0 + by_0 &= c. \end{aligned}$$

Изваждаме второто уравнение от първото и получаваме

$$a(x - x_0) + b(y - y_0) = 0$$

или еквивалентното

$$a(x - x_0) = b(y_0 - y).$$

Т.к. навсякъде работим с цели числа, последното равенство означава, че $b \mid a(x - x_0)$, но понеже $(a, b) = 1$, то всъщност $b \mid (x - x_0)$. Така $x - x_0 = kb$ за цялото число $k \in \mathbb{Z}$, т.е. $x = x_0 + kb$. Аналогично се вижда и че $y = y_0 - k'a$ за цяло число $k' \in \mathbb{Z}$. Замествайки теи изрази за $x$ и $y$ в уравнението получаваме

$$a(x_0 + kb) + b(y_0 - k'a) = c,$$

$$ax_0 + kab + by_0 - k'ab = c.$$

Понеже $(x_0, y_0)$ е частно решение, то

$$kab - k'ab = 0$$

или с други думи $k = k'$.

И така, ако вече сме открили частното решение $(x_0, y_0)$, то други частни решения се намират по формулите

$$\begin{aligned} x &= x_0 + kb, \\ y &= y_0 - k'a, \end{aligned}$$

където $k$ пробягва целите числа.

**Задача 5.** *Намерете три частни решения на диофантовото уравнение*

$$76x + 21y = 7.$$

*Решение.* По метода описан в Задача 4 намираме частното решение $(x_0, y_0) = (-56, 203)$. Сега, по формулите, които изведохме по-горе намираме още две частни решения за $k_1 = 2$ и $k_2 = 3$, а именно

$$x_1 = x_0 + k_1.b = -56 + 2.21 = -56 + 42 = -14,$$
$$y_1 = y_0 - k_1.a = 203 - 2.76 = 203 - 162 = 51.$$

и

$$x_2 = x_0 + k_2 b = -56 + 3.21 = 7,$$
$$y_2 = x_0 - k_2 a = 203 - 3.76 = -25.$$

□

**Задача 6.** *Покажете, че за всяко естествено число $n > 1$, числото $2^{2^n} + 1$ завършва на 7.*

*Решение.* Ясно е, че ако едно число завърша на 7, то при деление с 10, остатъкът отново ще е 7. Ще проведем индукция по $n$. Основа на индукцията: при $n = 2$ имаме

$$2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$$

и очевидно свойстовото е изпълнено.

Индукционно предположение: да допуснем, че свойството е вярно за всички естестени числа ненадминаващи $n$, т.е. $2^{2^k} + 1$ завършва на 7 за $2 \leq k \leq n$.

Индукционна стъпка: Ще докажем, че е вярно и при $k = n+1$. Наистина, $2^{2^{n+1}} + 1 = 2^{2^n.2} + 1$. Според индукционното предположени числото $2^{2^n} + 1$ завършва на 7, което означава, че

$$2^{2^n} + 1 = m.10 + 7$$

за цяло число $m \in \mathbb{Z}$. Тогава

$$2^{2^n 2} + 1 = (m.10 + 6)^2 + 1 = 100m^2 + 120m + 36 + 1 = 100k^2 + 120k + 37.$$

Оттук е очевидно, че свойстовото е изпълнено и за $k = n + 1$. □

Функцията
$$\varphi : \mathbb{N} \longrightarrow \mathbb{N},$$
която на всяко число $n \in \mathbb{N}$ съпоставя броя на числата, ненандминаващи $n$, означен с $\varphi(n)$, се нарича функция на Ойлер.

Свойства:
Ако $p$ е просто число, то $\varphi(p) = p - 1$.
Ако $p$ е просто и $k \in \mathbb{N}$, то $\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$.
Ако $(a, b) = 1$, то $\varphi(ab) = \varphi(a)\varphi(b)$.

От свойствата, казани дотук следва, че ако $a \in \mathbb{Z}$ и
$$a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$$
е каноничното разлагане на $a$ в произведение на прости множители, то
$$\begin{aligned}\varphi(a) &= \varphi(p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2}) \dots \varphi(p_n^{k_n}) \\ &= p_1^{k_1} \left(1 - \frac{1}{p_1}\right) p_2^{k_2} \left(1 - \frac{1}{p_2}\right) \dots p_n^{k_n} \left(1 - \frac{1}{p_n}\right) \\ &= a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_n}\right).\end{aligned}$$

**Задача 7.** *Намерете $\varphi(n)$ за $n = 196, n = 180$.*

*Решение.* Ще намерим каноничното разлагане на всяко от числата и ще приложим горната формула. Имаме, че
$$196 = 4.49 = 2^2.7^2.$$
Тогава
$$\varphi(196) = 2^2.7^2 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{7}\right) = 2^2.7^2 \cdot \frac{1}{2} \cdot \frac{6}{7} = 84.$$
Каноничното разлагане на 180 е
$$180 = 2^2 \cdot 3^2 \cdot 5$$
и тогава
$$\varphi(180) = 2^2 \cdot 3^2 \cdot 5 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 48.$$
$\square$

Нека $a, b \in \mathbb{Z}$, а $n \in \mathbb{N}$. Казваме, че числата $a$ и $b$ са сравними по модул $n$ и пишем $a \equiv b(\bmod n)$, ако $n \mid (a-b)$. Друг начин да изкажем същото е, ако $a$ и $b$ дават един и същи остатък при деление с $n$.

Свойства на сравненията

Ако $a \equiv b(\bmod n)$ и $c \equiv d(\bmod n)$, то $a \pm c \equiv b \pm d(\bmod n)$ и $ac \equiv bd(\bmod n)$.

За $\forall t \in \mathbb{Z}$ имаме, че $ta \equiv tb(\bmod n)$.

За $\forall k \in \mathbb{N}$ имаме, че $a^k \equiv b^k(\bmod n)$.

Ако $\alpha \equiv \beta(\bmod n)$ и $f(x) \in \mathbb{Z}[x]$, то $f(\alpha) \equiv f(\beta)(\bmod n)$.

**Теорема на Ойлер-Ферма.** *Ако $a \in \mathbb{Z}$, $n \in \mathbb{N}$ и $(a, n) = 1$ то $a^{\varphi(n)} \equiv 1(\bmod n)$. В частност, ако $p$ е просто число и $p \nmid a$, то $a^{p-1} \equiv 1(\bmod p)$.*

**Задача 8.** *Покажете, че* $641 \mid 2^{32} + 1$.

*Решение.* Ще покажем, че $2^{32} + 1 \equiv 0(\bmod 641)$.

Първи начин: използвайки свойствата на сравненията, последователно пресмятаме

$$\begin{aligned}
2 &\equiv 2(\bmod 641),\\
2^2 &\equiv 4(\bmod 641),\\
2^4 &\equiv 16(\bmod 641),\\
2^8 &\equiv 256(\bmod 641),\\
2^{16} &\equiv 256^2 \equiv 154(\bmod 641),\\
2^{32} &\equiv 640 \equiv -1(\bmod 641).
\end{aligned}$$

Към сравнението

$$2^{32} \equiv -1(\bmod 641)$$

добавяме очевидното сравнение

$$1 \equiv 1(\bmod 641)$$

и получаваме, че

$$2^{32} + 1 \equiv 0(\bmod 641).$$

Втори начин: имаме, че $640 = 2^7.5$. Това означава, че

$$2^7.5 \equiv -1 (\mathrm{mod}\, 641),$$
$$2^{14}.25 \equiv 1 (\mathrm{mod}\, 641),$$
$$2^{28}.625 \equiv 1 (\mathrm{mod}\, 641).$$

От последното сравнение и сравнението

$$2^4 \equiv 16 (\mathrm{mod}\, 641)$$

следва, че

$$2^{32}.625 \equiv 16 (\mathrm{mod}\, 641).$$

Имаме, че

$$625 \equiv -16 (\mathrm{mod}\, 641),$$

т.е.

$$2^{32}.(-16) \equiv 16 (\mathrm{mod}\, 641).$$

Т.к. $(16, 641) = 1$, то можем да разделеим двете страни на 16 и да получим

$$-2^{32} \equiv 1 (\mathrm{mod}\, 641).$$

Последното всъщност доказва разглежданото сравнение. □

**Задача 9.** *Намерете остатъка при делението на $7^{34}$ на 11.*

*Решение.* Достатъчно е да видим

$$7^{34} \equiv ? (\mathrm{mod}\, 11).$$

Понже $(7, 11) = 1$, то според теоретмата на Ойлер-Ферма получаваме, че $7^{\varphi(11)} = 7^{10} \equiv 1 (\mathrm{mod}\, 11)$. Повдигаме двете страни на трета степен и така

$$(*) \quad 7^{30} \equiv 1 (\mathrm{mod}\, 11).$$

За да достигнем до степен 34 проверяваме, че $7^2 = 49 \equiv 5 (\mathrm{mod}\, 11)$, а оттук

$$(**) \quad 7^4 \equiv 25 \equiv 3 (\mathrm{mod}\, 11).$$

Умножавайки почленно $(*)$ и $(**)$ получаваме, че

$$7^{34} \equiv 3 (\mathrm{mod}\, 11),$$

т.е. остатъкът при делението на $7^{34}$ на 11 е 3. □

**Задача 10.** *Решете сравненията:*

*1)*

$$2x^3 - 3x^2 + 2 \equiv 0(\operatorname{mod} 3);$$

*2)*

$$x^6 + 2x^5 - x^4 + 2x^3 - x^2 + x - 1 \equiv 0(\operatorname{mod} 5).$$

*Решение.* 1) Всевъзможните остатъци при деление на 3 са 0,1 и 2. Заместваме ги последователно в уравнението. Очевидно $x \equiv 0(\operatorname{mod} 3)$, т.е. числата от вида $z = 3k, k \in \mathbb{Z}$ не са решение на уравнението.

За $x \equiv 1(\operatorname{mod} 3)$, т.е. за числата от вида $x = 3k + 1, k \in \mathbb{Z}$ имаме, че

$$2 - 3 + 2 = 1 \equiv 1 \not\equiv 3(\operatorname{mod} 3)$$

и те не са решение на уравнението.

За числата от вида $x \equiv 2(\operatorname{mod} 3)$, т.е. от вида $x = 3k + 2, k \in \mathbb{Z}$ получаваме

$$16 - 12 + 2 = 6 \equiv 0(\operatorname{mod} 3)$$

и те са решения на уравнението.

2) Забелязваме, че някои от степенните показатели в сравнението надвишават модула 5. Тогава теоремата на Ойлер-Ферма би ни помогнала да намалим степента му. Очевидно кратните на 5 числа, т.е. $x \equiv 0(\operatorname{mod} 5)$ не са решения на сравнението. Т.к. 5 е просто число, то за всяко $x = 1, 2, 3, 4$ е в сила теоремата на Ферма и имаме, че

$$x^4 \equiv 1(\operatorname{mod} 5).$$

Умножавайки двете страни с $x$, получаваме

$$x^5 \equiv x(\operatorname{mod} 5)$$

и

$$x^6 \equiv x^2(\operatorname{mod} 5).$$

Като заместим тези резултати в сравнението понижаваме степента му и достигаме до еквивалентното сравнение

$$2x^3 + 3x - 2 \equiv 0(\operatorname{mod} 5).$$

Сега остава само последователно да се проверят отделните случаи. □

Да разгледаме сравненията от първа степен

$$ax \equiv b (\operatorname{mod} n),$$

където $x$ е неизвестен елемент. Ще разгледаме два подхода за неговото намиране.

Първият начин е да използваме теоремата на Ойлер-Ферма. Ако $(a, n) = 1$ (или ако можем да сведем уравнението до такова), то имаме че $a^{\varphi(n)} = 1$. Следователно, ако умножим двете страни на сравнението с $a^{\varphi(n)-1}$, ще получим директно решението

$$x \equiv a^{\varphi(n)-1} b (\operatorname{mod} n).$$

Вторият начин е да решим диофантовото уравнение, което следва от сравнението. По-конкретно, от определението за сравнимост имаме, че то е

$$ax - b \equiv ny, \quad y \in \mathbb{Z}$$

или записано в по-удобен вид

$$ax - ny = b.$$

Изслвдването на решенията на диофантовите уравнения, които разглеждахме, в комбинация със свойствата на сравненията ни помага да стигнем до следните заключения:

1. Ако $(a, n) = 1$, то сравнението има единствено решение;

2. Ако $(a, n) = d$ и $d \nmid b$, то сравнението няма решение;

3. Ако $(a, n) = d$ и $d \mid b$, то сравнението има $d$ на брой решения. При това, ако $x = x_0$ е едно решение, то всички решения се записват като $x = x_0 + k\frac{n}{d}$ за $k = 0, 1, \ldots, d-1$.

**Задача 11.** *Решете сравненията*

*1)* $5x \equiv 10 (\operatorname{mod} 8)$*;*

*2)* $29x + 3 \equiv 0 (\operatorname{mod} 12)$*;*

*3)* $13x \equiv 28 (\operatorname{mod} 31)$.

*Решение.* 1) Понеже $(5, 8) = 40 \nmid 10$ сравнението няма решение.

2) Имаме, че

$$\varphi(12) = 2^2 \cdot 3 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 2^2 \cdot 3 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$

Тогава след като умножим двете страни на сравнението с $29^3$ получаваме

$$x \equiv -3.29^3 \pmod{12}$$

и след необходимите пресмятания получаваме решението

$$x \equiv 9 \pmod{12}.$$

3) Т.к. $(13, 31) = 1$ сравнението има единствено решени. Свеждаме сравнението към диофантовото уравнение

$$13x - 31y = 28.$$

С алгоритъма на Евклид и тъждеството на Безу намираме, че

$$13.12 - 31.5 = 1.$$

Умножаваме двете страни с 28, за да получим

$$13.(12.28) - 31(2.28) = 28.$$

Оттук вече е ясно, че търсеното число е

$$x = 12.28 \equiv -5 \pmod{31}.$$

□

**Задача 12.** *Да се намерят послдните две цифри на числото* $783^{15}$.

*Решение.* Отговорът е просто решението на сравнението

$$786^{15} \equiv x \pmod{100}.$$

□