Делимост на цели числа. Сравнения.

Започваме с изучаването на основните свойства на целите числа. Следващата теорема е една от основните и я излагаме без доказателство.

Теорема за деление с частно и остатък. *За всеки две числа $a, b \in \mathbb{Z}$, $b \neq 0$ съществуват единствени числа $q \in \mathbb{Z}$, наречено частно, и $r \in \mathbb{Z}$, наречено остатък, такива че $a = bq + r$ и $0 \leq r < |b|$.*

Ще казваме, че цялото число $b \neq 0$ *дели* цялото число a, ако съществува цяло число q, такова че $a = bq$ (т.е. при делението с частно и остатък имаме остатък $r = 0$). Означаваме $b \mid a$. Ако b не дели a пишем $a \nmid b$.

Свойства:

1. $a \mid a$ за всяко цяло число $a \neq 0$,
2. Ако $b \mid a$, то $|b| \leq |a|$. В частност, ако $b \mid a$ и $a \mid b$, то $a = \pm b$,
3. Ако $c \mid b$ и $b \mid a$, то $c \mid a$,
4. Ако b дели всяко от числата $a_1, a_2, \ldots, a_k$, а $t_1, t_2, \ldots, t_k$ са произволни цели числа, то

$$b \mid t_1 a_1 + t_2 a_2 + \cdots + t_k a_k.$$

Нека a и b са цели числа и поне едно от тях е различно от нула. Числото $d \in \mathbb{Z}$ е *най-голям общ делител (НОД)* на a и b, ако: $d \mid a$ и $d \mid b$ и ако числото d_1 дели a и b (т.е. е общ делител на a и b), то $d_1 \mid d$. В частност $|d_1| \leq |d|$. Ако d' също е НОД на a и b, то тогава едновременно $d' \mid d$ и $d \mid d'$, което означава, че $d' = \pm d$. За да въведем еднозначност на НОД ще считаме, че $d > 0$, т.е. $d \in \mathbb{N}$ и по този начин той ще бъде единствен. Означаваме $d = (a, b)$. За всеки две числа (поне едно от които е ненулево) може да се намери най-голям общ делител. Това става например с

Алгоритъм на Евклид:

Нека за простота считаме, че числата $a, b \in \mathbb{N}$ са такива, че $a \geq b$. От теоремата за деление с частно и остатък имаме, че

$$a = bq_1 + r_1$$

За числа $q_1, r_1 \in \mathbb{N}$ и $r_1 < b$. Сега делим b на r_1 с частно q_2 и остатък $r_2 < r_1$ така, че

$$b = r_1 q_2 + r_2.$$

По нататък имаме, че

$$r_1 = r_2 q_3 + r_3$$

за частно $q_3 \in \mathbb{N}$ и остатък $r_3 \in \mathbb{N}, r_3 < r_2$. Продължавайки по същия начин, делейки всеки остатък на следващия, след краен брой стъпки получаваме

$$r_{n-2} = r_{n-1} q_n + r_n$$

за естесвни числа $r_{n-2}, r_{n-1}, r_n, q_n$ като $r_n < r_{n-1}$ и

$$r_{n-1} = r_n q_{n+1}$$

за частно $q_{n+1} \in \mathbb{N}$. Алгоритъмът на евклид достига до край поради условието, наложено върху остатъците, от теоремата за деление $r_{i+1} < r_i$ за всяко $i = 1, 2, \ldots, n-1$. По този начин на последната стъпка неявно е изпълнено условието $r_{n+1} = 0 < r_n$ и алгоритъмът приключва т.к. вече е невъзможно да бъде намерено цяло неотрицателно число r_{n+2}, такова че $r_{n+2} < r_{n+1}$. Сега последното равенство дава, че $r_n \mid r_{n-1}$. Имайки предвид това от предпоследното равенство достигаме до заключението, че $r_n \mid r_{n-2}$. Сега продължавайки по обратния път от третото, второто и първото равенство получаваме респективно, че $r_n \mid r_1$, $r_n \mid b$ и $r_n \mid a$. Така получихме, че r_3 е общ делител на a и b. За да докажем, че r_3 е НОД на a и b взимаме произволен общ делител d на a и b. Тогава $d \mid a$ и $d \mid b$ и от първото равенство следва, че $d \mid r_1$. Продължавайки нататък по алгоритъма получаваме, че $d \mid r_2$, $d \mid r_3$, $\ldots$, $d \mid r_n$. По този начин доказахме, че наистина $r_n = (a, b)$. Знаменито следствие от Алгоритъма на Евклид е

Тъждество на Безу:

Ако $a, b \in \mathbb{Z}$ и $d = (a, b)$, то $\exists u, v \in \mathbb{Z} : ua + vb = d$. Това се вижда лесно от обратния ход на алгоритъма. За $d = r_3$ изразяваме първоначално

r_n чрез r_{n-1} и r_{n-2} от предпоследното равенство. По-нататък изразяваме r_{n-1} чрез r_{n-2} и r_{n-3} и т.н. към началото на алгоритъма, откъдето изразяваме r_2 чрез r_1 и b, а r_1 чрез b и a. По този всичко се свежда до изразяване на $d = r_n$ чрез a и b умножени с някакви цели числа, които полагаме да са u и v.

Ако за целите числа a и b е изпълнено $(a, b) = 1$, то те се наричат *взаимно прости*. В общия случай, когато $(a, b) = d$, то от определението на НОД имаме, че $d \mid a \Rightarrow a = da_1$ за $a_1 \in \mathbb{Z}$ и $d \mid b \Rightarrow b = db_1$ за $b_1 \in \mathbb{Z}$. Тогава за числата a_1, b_1 вече е изпълнено, че $(a_1, b_1) = 1$.

5. Ако $b \mid a_1a_2$ и $(b, a_1) = 1$, то $b \mid a_2$. Наистина, според тъждеството на Безу, съществуват числа $u, v \in \mathbb{Z}$, такива, че

$$ub + va_1 = 1.$$

Умножаваме двете страни по a_2, за да получим

$$ua_2b + va_1a_2 = a_2.$$

Понеже $b \mid a_1a_2$, то съществува цяло число a, такова че $a_1a_2 = ab$. Замествайки това в горното равенство получаваме

$$ua_2b + vab = a_2,$$

което означава, че трябва $b \mid a_2$.

6. Ако $b_1 \mid a$, $b_2 \mid a$ и $(b_1, b_2) = 1$, то тогава $b_1b_2 \mid a$. Наистина, имаме че $a = a_1b_1, a_1 \in \mathbb{Z}$. Тогава $b_2 \mid a_1b_1$ и от факта, че $(b_1, b_2) = 1$ следва, че $b_2 \mid a_1$, т.е. $a_1 = a_2b_2$. Сега вече $a = a_1b_1 = a_2b_1b_2$, което означава, че $b_1b_2 \mid a$.

Нека $p \in \mathbb{N}$ и $p > 1$. Казваме, че числото p е *просто*, ако единствените му делители са ± 1 и $\pm p$. Ако p не е просто, казваме че то е *съставно*. Ако $a \in \mathbb{Z}$ и p е просто число, то или $p \mid a$, или $(a, p) = 1$.

7. Ако p е просто число и $p \mid a_1a_2$, то или $p \mid a_1$, или $p \mid a_2$. Наистина, ако $p \mid a_1$, то всичко е доказано. Нека $p \nmid a_1$. Тогава $(p, a_1) = 1$ и според свойство 1 следва, че $p \mid a_2$.

Ясно е, че ако $n \in \mathbb{N}, n > 1$, то съществува просто число, такова че $p \mid n$. Ако n е просто, то тогава $p = n$. Ако n е съставно, то съществуват числа $n_1, n_2 \in \mathbb{N}$, такива че $n_1, n_2 > 1$ и $n = n_1 n_2$ и по индукция се вижда, че съществува просто число, което да дели n_1 и/или n_2, а оттам и n. Последователните прости числа се означават с

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \ldots$$

Теорема (Евклид). *Съществуват безбройно много прости числа.*

Доказателство. Да допуснем, че простите числа са n на брой ($n \in \mathbb{N}, n < \infty$). Нека това са числата $p_1, p_2, \ldots, p_n$. Да разгледаме тогава естественото число $P = p_1 p_2 \ldots p_n + 1$. Очевидно е, че $P > 1$ и тогава съществува просто число q, което да дели P. Тогава $q = p_i$ за някое фиксирано i между 1 и n. Сега $q \mid P$ и $q \mid p_1 p_2 \ldots p_n$, а оттам трябва да е изпълнено и $q \mid 1$, но това е невъзможно. Противоречието доказва теоремата. □

Следващата теорема разкрива най-фундаменталната роля на простите числа.

Основна теорема на аритметиката. *Всяко ествествно число $n > 1$ се разлага по единствен начин (с точност до реда на множителите) в произведение на прости числа.*

Доказателство. Съществуване: ще проведем доказтелството с индукция. Ако n е просто, то съществуването е доказано с $n = n$. Нека сега n е съставно и $n = n_1 n_2$ за естествени числа $n_1, n_2 > 1$. Правим индукционно предположение, че n_1 и n_2 се разлагат в произведение на прости числа. Тогава индукционната стъпка е изпълнена, т.к. n е произведение на n_1 и n_2, които се разлагат в произведение на прости числа. По-точно, ако $n_1 = p_1 p_2 \ldots p_n$ и $n_2 = q_1 q_2 \ldots q_m$ за $m, n \in \mathbb{N}$, са разлаганията на n_1 и n_2, то

$$n = p_1 p_2 \ldots p_n q_1 q_2 \ldots q_m$$

дава разлагане в прости числа на n. Сега твърдението за съществуване следва от принципа на математическата индукция.

Единственост: Нека предположим, че

$$n = p_1 p_2 \ldots p_r, \quad r \in \mathbb{N}$$

и

$$n = q_1 q_2 \dots q_s, \quad s \in \mathbb{N}$$

са две разлагания на n в произведение на прости множители. Тогава имаме, че е изпълнено

$$(*) \quad p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Нека без ограничение на общността $r \leq s$. Имаме, че $p_1 \mid q_q q_2 \dots q_s$ и следователно дели поне едно от числата $q_i, 1 \leq i \leq s$. Нека (след евентуално преномериране на индексите) това е числото q_1. Тогава $p_1 \mid q_1$, но т.к. q_1 е просто имаме, че

$$p_1 = q_1.$$

В такъв случай делим двете страни на $(*)$ на p_1 и получаваме

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Продължавайки същите разсъждения, след r на брой стъпки достигаме до

$$p_j = q_j \quad \text{за } j = 1, 2, \dots, r$$

и равенството

$$1 = q_{r+1} q_{r+2} \dots q_s.$$

Ако допуснем, че $r < s$, то горното равенство е невъзможно да бъде изпълнено в множеството на естествените числа. Следователно остава единствено $r = s$ и с това единствеността на разлагането (с точност до разместване на множителите) е доказана. □

Следствие. *Ако $n \in \mathbb{N}, n > 1$ и $p_1, p_2, \dots, p_t$ $(t \geq 1)$ са различните прости делители на n, то*

$$n = p_q^{k_1} p_2^{k_2} \dots p_t^{k_t},$$

където $k_i \in \mathbb{N}$ за $i = 1, 2, \dots, t$. Това разлагане се нарича канонично разлагане на числото n.

Пример:
За числото $n = 720$ имаме

$$n = 10.72 = 2.5.8.9 = 2.5.2^3.3^2.$$

Следователно $n = 2^4.3^2.5^1$.

Нека $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Казваме, че числото a *е сравнимо с* b *по модул* n, ако $n \mid a - b$. Записваме $a \equiv b (\mathrm{mod}\, n)$. Това определение е еквивалентно на свойството a и b да дават един и същи остатък при деление с n.

Свойства на сравненията:

1. $a \equiv a (\mathrm{mod}\, n), \forall a \in \mathbb{Z}$;

2. Ако $a \equiv b (\mathrm{mod}\, n)$, то и $b \equiv a (\mathrm{mod}\, n)$;

3. Ако $a \equiv b (\mathrm{mod}\, n)$ и $b \equiv c (\mathrm{mod}\, n)$, то $a \equiv c (\mathrm{mod}\, n)$. Наистина, $a - c = (a - b) + (b - c)$ и от $n \mid a - b$ и $n \mid b - c$ следва, че $n \mid a - c$, което означава, че $a \equiv c (\mathrm{mod}\, n)$.[1]

4. Ако $a \equiv b (\mathrm{mod}\, n)$, то $a + c \equiv b + c (\mathrm{mod}\, n), \forall c \in \mathbb{Z}$;

5. Ако $a \equiv b (\mathrm{mod}\, n)$, то $ac \equiv bc (\mathrm{mod}\, n), \forall c \in \mathbb{Z}$;

Нека

$$a_1 \equiv b_1, a_2 \equiv b_2, \ldots, a_k \equiv b_k \pmod{n}.$$

Тогава са изпълнени още свойствата:

6. $a_1 + a_2 + \cdots + a_k \equiv b_1 + b_2 + \cdots + b_k (\mathrm{mod}\, n)$;

7. $a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k (\mathrm{mod}\, n)$;

8. Ако $a \equiv b (\mathrm{mod}\, n)$ и $k \in \mathbb{N}$, то $a^k \equiv b^k (\mathrm{mod}\, n)$;

9. Ако $ka \equiv kb (\mathrm{mod}\, n)$ за някое $k \in \mathbb{Z}$, то $a \equiv b \left(\mathrm{mod}\, \frac{n}{(n,k)}\right)$. В частност, ако k и n са взаимно прости, то $a \equiv b (\mathrm{mod}\, n)$. Наистина, нека $d = (n, k)$. Тогава $n = dn_1, n_1 \in \mathbb{Z}$, $k = dk_1, k_1 \in \mathbb{Z}$ и $(n_1, k_1) = 1$. Сега $n \mid ka - kb$ означава $dn_1 \mid dk_1(a - b)$ или еквивалентното $n_1 \mid k_1(a - b)$, но понеже $(n_1, k_1) = 1$, то $n_1 \mid (a - b)$. Последното означава точно даденото свойство.

Пример:

Да се докаже, че числото $2^{70} + 3^{70}$ се дели на 13.

Имаме, че $2^6 = 64$. Понеже $65 = 5.13$ се дели на 13, то $64 \equiv -1 (\mathrm{mod}\, 13)$. Повдигаме двете страни на степен 11, за да получим, че $2^{66} \equiv -1 (\mathrm{mod}\, 13)$. Имаме още, че $2^4 = 16 \equiv 3 (\mathrm{mod}\, 13)$ и оттук $2^{70} \equiv -3 (\mathrm{mod}\, 13)$.

$3^3 = 27 \equiv 1 (\mathrm{mod}\, 13)$ (защото 26 се дели на 13). Повдигаме двете страни на сравнението на степен 23, за да получим, че $3^{69} \equiv 1 (\mathrm{mod}\, 13)$. Сега вече е ясно, че $3^{70} \equiv 3 (\mathrm{mod}\, 13)$.

[1] Тези три свойства заедно означават, че сравнимостта на числа е релация на еквивалентност.

Накрая имаме, че $2^{70} + 3^{70} = -3 + 3 = 0 (\mathrm{mod}\, 13)$, което означава, че $2^{70} + 3^{70}$ се дели на 13.

Нека n е произволно естествно число. С $\varphi(n)$ означаваме броя на всички естетвени числа, които са по-малки или равни на n и са взаимно прости с n. (Изображението

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N},$$

което на всяко число $n \in \mathbb{N}$ съпоставя числото $\varphi(n)$ се нарича *функция на Ойлер.*)

Например:

Очевидно $\varphi(1) = 1$.

$\varphi(6) = 2$, т.к. $(1, 6) = 1, (5, 6) = 1$ и няма друго $n \in \mathbb{N}$, такова че $n \leq 6$ и $(n, 6) = 1$.

За $n \geq 2$ е в сила

$$1 \leq \varphi(n) \leq n - 1.$$

Тогава $\varphi(n) = 1 \Leftrightarrow n = 2$ и $\varphi(n) = n - 1 \Leftrightarrow n$ е просто число.

Нека сега p е просто число, а $k \in \mathbb{N}$. Интересува ни $\varphi(p^k) =?$ Нека този път да преброим числата между 1 и p^k, които НЕ са взаимно прости с p^k. Понеже p е просто, то това са числата, които се делят на p. По-конкретно това са

$$p, 2p, 3p, \ldots, (p^{k-1} - 1)p, \underbrace{p^{k-1}p}_{=p^k}$$

и те са точно p^{k-1} на брой. В такъв случай числата, които са взаимно прости с p^k са $p^k - p^{k-1}$ на брой. Следователно $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

Важно свойство, с лесно доказателство, което няма да показваме тук е, че ако $a, b \in \mathbb{N}$ са взаимно прости, то

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Сега вече можем да докажем следната

Теорема. *Ако $n \in \mathbb{N}$ и $n > 1$ се разлага канонично като*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r},$$

то

$$\varphi(n) = p_1^{k_1-1}p_2^{k_2-1}\dots p_r^{k_r-1}(p_1-1)(p_2-1)\dots(p_r-1)$$

или еквивалентно [2]

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right).$$

Доказателство. Т.к. p_j за $1 \le j \le r$ са всичките различни прости числа, то те са две по две взаимно прости и от свойствата, които видяхме дотук имаме

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})\dots\varphi(p_r^{k_r})\\ &= p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1)\dots p_r^{k_r-1}(p_r-1)\end{aligned}$$

и това дава точно исканото разлагане. □

Пример:
$\varphi(720) =?$ Преди видяхме, че $720 = 2^4.3^2.5^1$ и следователно

$$\varphi(720) = 720\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 720\cdot\frac{8}{30} = 192.$$

Накрая ще споменем две важни теореми.
Нека $n \in \mathbb{N}$, $a \in \mathbb{Z}$ и $(a,n) = 1$. Тогава са в сила

Теорема на Ойлер-Ферма.

$$a^{\varphi(n)} \equiv 1(\mathrm{mod}\, n).$$

В частност, ако $n = p$ е просто число и $p \nmid a$, то

$$a^{p-1} \equiv 1(\mathrm{mod}\, p).$$

Теорема на Уилсън. *Ако p е просто число, то*

$$(p-1)! \equiv -1(\mathrm{mod}\, p).$$

[2] След изнасяне на p_i, $i = 1, 2, \dots, r$ пред скоби.