Teoria podzielności liczb całkowitych

Mariusz Strzelecki (szczeles@mat.umk.pl)

24 czerwca 2009

1 Teoria podzielności

Definicja 1.1. Jeśli $a, b, \in \mathbb{Z}$, to mówimy, że a *dzieli* b (piszemy $a|b$), jeśli istnieje $c \in \mathbb{Z}$ takie, że $b = ca$.

Przykład 1.2 (Własności podzielności)**.**

- $\forall_{a\in\mathbb{Z}} a|a$.
- Jeśli $a|b$ i $b|c$ to $a|c$.
- Jeśli $a|b$ i $b|a$ to $a = \pm b$.
- $\forall_{a\in\mathbb{Z}} 1|a$.
- $a|1 \iff a = \pm 1$.
- $\forall_{a\in\mathbb{Z}} a|0$.
- $0|a \iff a = 0$.
- Jeśli $a|b$ oraz $b \neq 0$, to $|a| \leqslant |b|$.
- Jeśli $a|b$ i $a|c$ to $a|b \pm c$ oraz $\forall_{k\in\mathbb{Z}} a|kc$. Ponadto, jeśli $am|bm$ i $m \neq 0$ to $a|b$.

2 Największy wspólny dzielnik

Definicja 2.1. Jeśli $a, b \in \mathbb{Z}$, to liczbę $d \in \mathbb{Z}$ nazywamy *największym wspólnym dzielnikiem liczb a i b* (będziemy oznaczać $d = (a, b)$), jeśli spełnione są następujące trzy warunki:

(1) $d \geqslant 0$,

(2) $d|a$ i $d|b$,

(3) jeśli $c|a$ i $c|b$, to $c|d$ (czyli d jest największą liczbą dzielącą a i b)

Uwaga 2.2 (o jednoznaczności NWD). Jeśli d i d' są największymi wspólnymi dzielnikami liczb a i b to z warunków (2) i (3) wynika, że $d|d'$ i $d'|d$, więc z własności podzielności i faktu, że NWD jest liczbą nieujemną mamy $d = d'$.

Przykład 2.3 (Własności NWD)**.**

$\forall_{a,b\in\mathbb{Z}}(a, b) = (b, a)$.

$\forall_{a,b\in\mathbb{Z}}(a, b) = (|a|, |b|)$.

$\forall_{a\in\mathbb{Z}}(a,a) = |a|$.

$\forall_{a\in\mathbb{Z}}(a,1) = 1$.

$\forall_{a\in\mathbb{Z}}(a,0) = |a|$.

Definicja 2.4. Mówimy, że liczby a i b są *względnie pierwsze*, jeśli $(a,b) = 1$.

Lemat 2.5 (Bardzo ważny lemat :-))**.** *Jeśli $a = qb + r$ dla $a, b, q, r \in \mathbb{Z}$ (zauważmy, że q i r nie muszą być wcale ilorazem i resztą z dzielenia, to dowolne liczby!), to $(a,b) = (b,r)$.*

Dowód. Wystarczy pokazać, że $c|a, b \iff c|b, r$ (ponieważ jeśli dowolny dzielnik tych dwóch liczb ma taką własność to w szczególności NWD też).
" $\Longrightarrow$ ". Jeśli $c|a, b$ to istnieją takie $k, l \in \mathbb{Z}$, że $a = kc$ i $b = lc$. Wtedy mamy równość $kc = lcq + r$. Dzieląc obie strony przez c dostaniemy $k = lq + \frac{r}{c}$, a ponieważ $k \in \mathbb{Z}$ i $lq \in \mathbb{Z}$, więc też $\frac{r}{c} \in \mathbb{Z}$, skąd mamy, że $c|r$.
" $\Longleftarrow$ ". Jeśli $c|b, r$ to istnieją takie $m, n \in \mathbb{Z}$, że $m = cb$ i $n = cr$, czyli $a = cbq + cr = c(bq + r)$, a ponieważ $bq + r \in \mathbb{Z}$, więc $a|c$. □

Twierdzenie 2.6 (O dzieleniu z resztą)**.** *Jeśli $a, b \in \mathbb{Z}$ oraz $b \neq 0$, to istnieją jednoznacznie wyznaczone $q, r \in \mathbb{Z}$ takie, że $a = qb + r$ i $0 \leqslant r < |b|$.*

Definicja 2.7. Liczby q i r z powyższego twierdzenia nazywamy odpowiednio *ilorazem (całkowitym) i resztą z dzielenia a przez b*. Resztę z dzielenia a przez b ($a, b \in \mathbb{Z}$, $b \neq 0$) oznaczamy a mod b.

Dowód. Takie liczby zawsze istnieją ponieważ q możemy wybrać tak, że

$$a = qb = min\{a - q'b | q' \in \mathbb{Z}, a - q'b \geqslant 0\}$$

oraz kładąc $r := a - qb$.
Dla dowodu jednoznaczności przyjmijmy, że istnieją q' i $r' \in \mathbb{Z}$ takie, że $a = a'b + r'$ oraz $0 \leqslant r' < |b|$. Wtedy $r - r' = a - qb - (a - q'b) = (q' - q)b$, skąd $b|r - r'$, a ponieważ $r < |b|$ i $r' < |b|$, więc $|r - r'| < |b|$. Stąd $r - r' = 0$, a zatem także $q - q' = 0$. □

3 Algorytm Euklidesa

Lemat 3.1. *Dla dowolnych $a, b \in \mathbb{Z}$ istnieje ich największy wspólny dzielnik.*

Dowód. Dowód będzie jednocześnie ukazaniem sposobu działania algorytmu Euklidesa.
Będzie on indukcyjny ze względu na $n = min(|a|, |b|)$.
Jeśli $n = 0$ to albo $a = 0$ i $(a,b) = |b|$ albo $b = 0$ i wtedy $(a,b) = |a|$. Załóżmy więc, że $n > 0$. Jeśli $|a| = |b| = n$ to $(a,b) = n$. W przeciwnym wypadku bez straty ogólności możemy założyć, że $|a| > |b| = n$ (w pseudokodzie jest to ten jeden if). Niech q i r będą ilorazem i resztą z dzielenia a przez b. Wiemy, że $(a,b) = (b,r)$, a przecież $min(|b|, |r|) = |r| < |b| = n$, zatem (a,b) istnieje. □

Uwaga 3.2 (O skomplikowaniu dowodu). Ten dowód wcale nie jest taki trudny, jak się wydaje, trzeba wyobrazić sobie wpierw działający algorytm. Dostaje on dwie liczby: a i b i sprawdza, czy są równe (bądź któraś z nich równa 0). Jeśli tak to kończy. Jeśli nie, to w kolejnym kroku rozważa **ostro mniejsze** liczby jako parametry (ale takie, że ich NWD jest taki sam jak poprzednich). Na pewno się kończy, bo jeśli któraś dojdzie do zera to algorytm się kończy.

Stwierdzenie 3.3. *Jeśli $a, b \in \mathbb{Z}$, to istnieją $p, q \in \mathbb{Z}$ takie, że $(a, b) = pa + qb$.*

Dowód. Dowód będzie bardzo podobny do poprzedniego, przestawia działania pewnego algorytmu, zwanego Rozszerzonym Algorytmem Euklidesa.
Indukcja ze względu na $n = min(a, b)$
Jeśli $n = 0$ to albo $a = 0$ i $(a, b) = |b| = 0 \cdot a + (sgn\, b) \cdot b$ albo $b = 0$ i wtedy $(a, b) = |a| = (sgn\, a) \cdot a + 0 \cdot b$. Załóżmy, że $n > 0$. Postępujemy dokładnie jak poprzednio: jeśli $|a| = n = |b|$ to $(a, b) = (sgn\, a) \cdot a + 0 \cdot b$. W przeciwnym wypadku możemy założyć bez straty ogólności, że $|a| > |b| = n$. Niech q i r będą ilorazem i resztą z dzielenia a przez b. Wtedy $min(|b|, |r|) = |r| < n$, więc na mocy założenia indukcyjnego istnieją $x, y \in \mathbb{Z}$ takie, że $(b, r) = xb + yr$. Wiemy też, że $(a, b) = (b, r) = ya + (x - yq)b$, co kończy dowód. □

Uwaga 3.4. Jeśli $a, b \in \mathbb{Z}$ to $(a, b)|pa + qb$ dla dowolnych $p, q \in \mathbb{Z}$.

Uwaga 3.5. Jeśli dla $a, b \in \mathbb{Z}$ istnieją $p, q \in \mathbb{Z}$ takie, że $1 = pa + qb$ to $(a, b) = 1$.

4 Liczby pierwsze

Definicja 4.1. Liczbę całkowitą p nazywamy *pierwszą*, jeśli $p > 1$ oraz $\nexists_{a \in \mathbb{Z} \wedge a \neq 1 \wedge a \neq p} a|p$. Oznaczymy zbiór liczb pierwszych jako $\mathbb{P} = \{p \in \mathbb{Z} \mid p \text{ jest pierwsza }\}$. Algorytm, który wykrywa wszystkie liczby pierwsze to znane wszystkim Sito Eratostenesa. Nie będę go przytaczał, bo wstyd :-)

Lemat 4.2 (O rozkładzie liczby całkowitej)**.** *Jeśli $n \in \mathbb{Z}, n > 1$ to istnieją $p_1, \ldots, p_k \in \mathbb{P}$ takie, że $n = p_1 \cdots p_k$.*

Dowód. Dowód znów będzie indukcyjny ze względu na n, tym razem bardzo prosty. Jeśli $n \in \mathbb{P}$ to w ogóle nie ma o czym mówić. Załóżmy zatem, że $n \notin \mathbb{P}$. Wtedy istnieją $n_1, n_2 \in \mathbb{Z}$ takie, że $1 < n_1, n_2 < n$ oraz $n_1 = p_1 \cdots p_k$ i $n_2 = q_1 \cdots q_l$. Wtedy $n = p_1 \cdots p_k \cdot q_1 \cdots q_l$, co kończy dowód. □

Twierdzenie 4.3 (Najkrótsze z możliwych twierdzień z najciekawszym dowodem)**.** $|\mathbb{P}| = \infty$.

Dowód. (A oto dowód made by Euklides) Pokażemy, że dla każdego podzbioru $P \subset \mathbb{P}$ skończonego (czyli $|P| < \infty$) istnieje $p \in \mathbb{P} \setminus P$. Jeśli $P = \emptyset$ to teza jest oczywista. Przypuśćmy, że $P = \{p_1, \ldots, p_n\}$. Jedynym wspólnym dzielnikiem liczb $p_1 \cdots p_n$ i $p_1 \cdots p_n + 1$ jest 1. Zatem żadna liczba pierwsza występująca w P nie jest dzielnikiem liczby $p_1 \cdots p_n + 1$. Ale $p_1 \cdots p_n + 1 > 1$, więc ma dzielnik p, który jest liczbą pierwszą. Oczywiście $p \notin \mathbb{P}$, co kończy dowód. □

Teraz udowodnimy kilka rzeczy w logicznej kolejności, które pozwolą nam sformułować Zasadnicze Twierdzenie Arytmetyki.

Lemat 4.4. *Jeśli $p \in \mathbb{P}$ i $p|ab$ dla $a, b \in \mathbb{Z}$ to $p|a$ lub $p|b$.*

Dowód. Przypuśćmy (bez straty ogólności), że $p \nmid a$. Wtedy $(a, p) = 1$, więc istnieją takie $m, n \in \mathbb{Z}$, że $1 = ma + np$. Ponadto, ponieważ $p|ab$, więc $\exists_k ab = pk$. Zatem mamy równość $b = mab + npb = m(ab) + p(nb) = m(pk) + p(nb) = p(mk + nb)$, a stąd $p|b$, co kończy dowód. □

Wniosek 4.5. Jeśli $p \in \mathbb{P}$ oraz $p|a_1 \cdots a_n$ dla $a_1, \ldots, a_n \in \mathbb{Z}$ to istnieje $i \in \{1, \ldots, n\}$ takie, że $p|a_i$.

Lemat 4.6. *Jeśli $p_1 \leqslant \cdots \leqslant p_k, q_1 \leqslant \cdots \leqslant q_l \in \mathbb{P}$ oraz $p_1 \cdots p_k = q_1 \cdots q_l$ to $k = l$ oraz $\forall_{i \in \{1,\ldots,k\}} p_i = q_i$*

Dowód. Dowód będzie indukcyjny ze względu na k. Jeśli $k = 1$ to teza jest oczywista. Załóżmy, że $k > 1$. Z poprzedniego wniosku wiemy, że istnieje $j \in \{1 \dots l\}$ takie, że $p_k | q_j$, a więc $p_k = q_j$. Wtedy $p_1 \cdots p_{k-1} = q_1 \cdots q_{j-1} q_{j+1} \cdots q_l$, więc z założenia indukcyjnego wynika, że $k - 1 = l - 1 (\implies k = l)$ oraz $p_i = q_i$ dla $i \in \{1, \dots, j-1\}$ i $p_i = q_{i+1}$ dla $i \in \{j, \dots, k-1\}$. Ponadto, jeśli $j < k = l$, to $p_k = q_j \implies p_k^{k-j} = q_j^{k-j} \iff p_k^{k-j} \geqslant p_{k-1} \cdots p_j = q_k \cdots q_{j+1} \geqslant q_j^{k-j} = p_k^{k-j}$, skąd $p_j = \cdots = p_k = q_j = \cdots = q_k$. □

Wniosek 4.7 (Zasadnicze Twierdzenie Arytmetyki). Jeśli $n \in \mathbb{Z}, n > 1$, to istnieją jednoznacznie wyznaczone $p_1 < \cdots p_k \in \mathbb{P}$ oraz $\alpha_1, \cdots, \alpha_k \in \mathbb{N}_+$ takie, że

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

Ktoś mógłby zadać sobie pytanie: ile jest liczb pierwszych? A my wiemy!

Twierdzenie 4.8. *Niech $\pi \colon \mathbb{R}_+ \to \mathbb{N}$ będzie funkcją zdefiniowaną wzorem: $\pi(x) := |\{p \in \mathbb{P} | p \leqslant x\}|$. Wówczas mamy:*

$$\lim_{n \to \infty} \frac{\pi(x)}{x/ln(x)} = 1.$$

5 Kongruencje!

Definicja 5.1. Niech $a, b, n \in \mathbb{Z}$ oraz $n \neq 0$. Mówimy, że *a przystaje do b modulo n* (piszemy $a \equiv b \pmod{n}$), jeśli $n | a - b$.

Lemat 5.2. *(Własności operatora $\equiv$)*

(1) Jeśli $a \equiv b \,(mod\ n)$ oraz $c \equiv d \,(mod\ n)$, to $a \pm c \equiv b \pm d \,(mod\ n)$ oraz $ac \equiv bd \,(mod\ n)$.

(2) Jeśli $ac \equiv bc \,(mod\ n)$ oraz $(c, n) = 1$, to $a \equiv b \,(mod\ n)$.

(3) $ma \equiv mb \,(mod\ mn) \iff a \equiv b \,(mod\ n)$

Stwierdzenie 5.3. *(Potrzebne do ChTwOR) Niech $a, b, n \in \mathbb{Z}, n \neq 0$ i niech $d = (a, n)$. Wówczas:*

- *$(\exists_{x \in \mathbb{Z}} ax \equiv b \,(mod\ n)) \iff d | b$.*
- *Jeśli $d | b$ oraz $ax \equiv b \,(mod\ n)$ i $ay \equiv b \,(mod\ n)$ dla $x, y \in \mathbb{Z}$ to wówczas $x \equiv y \,(mod\ \frac{n}{d})$.*

Dowód. Oczywiście, jeśli $d \not| b$ to $a = kd$ i $n = md$ dla pewnych $k, l \in \mathbb{Z}$, więc nie istnieje $x \in \mathbb{Z}$ taki, że $ax \equiv b \pmod{n}$. Przypuśćmy zatem że $d | b$. Wtedy przyjmując $a' = \frac{a}{d}, b' = \frac{b}{d}, n' = \frac{n}{d}$ mamy równoważność: $ax \equiv b \pmod{n} \iff a'x \equiv b' \pmod{n'}$. Zauważmy, że $(a', n') = 1$, więc istnieją $p, q \in \mathbb{Z}$ takie, że $1 = pa' + qn'$ i wtedy dla $x = pb'$ mamy $a'x \equiv b' \pmod{n'}$. Z drugiej zaś strony, jeśli $ay \equiv b \pmod{n}$ dla $y \in \mathbb{Z}$, to $a'y \equiv b' \pmod{n'}$ i $y \equiv (pa')y \equiv pb' \equiv x \pmod{n'}$ □

Twierdzenie 5.4. *Niech $m_1, \dots, m_k \in \mathbb{Z}$ będą parami względnie pierwsze i $b_1, \dots, b_k \in \mathbb{Z}$.*

(1) Istnieje $x \in \mathbb{Z}$ taki, że

$$x \equiv b_1 \,(mod\ m_1), \dots, x \equiv b_k \,(mod\ m_k)$$

(2) Dla $x, y \in \mathbb{Z}$ zachodzi

$$x \equiv b_1 \ (mod\ m_1), \ldots, x \equiv b_k \ (mod\ m_k)$$

oraz

$$y \equiv b_1 \ (mod\ m_1), \ldots, y \equiv b_k \ (mod\ m_k)$$

wtedy i tylko wtedy, gdy $x \equiv y \ (mod\ m_1 \cdots m_k)$

Dowód. Niech $n_i = \frac{m_1 \cdots m_k}{m_i}$ dla $i \in \{1, \ldots, k\}$. Z założeń wynika, że $(m_i, n_i) = 1$ dla wszystkich $i \in \{1, \ldots, k\}$, zatem dla każdego i istnieją $p_i, q_i \in \mathbb{Z}$ takie, że $1 = p_i m_i + q_i n_i$. Wtedy $x := b_1 q_1 n_1 + \cdots + b_k q_k n_k$ ma żądane własności. Druga część twierdzenia jest oczywista (wynika z elementarnych własności kongruencji). □

Uwaga 5.5. (Czyli jak używać ChTwOR?) Niech $a, b, m, n \in \mathbb{Z}, m, n > 1$. Niech $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ oraz $n = p_1^{\beta_1} \cdots p_k^{\beta_k}$ dla $p_1 < \cdots < p_k$ oraz $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \in \mathbb{N}(\cup 0!)$. Istnieje $x \in \mathbb{Z}$ taki, że $x \equiv a \pmod{m}$ i $x \equiv b \pmod{n}$ wtedy i tylko wtedy, gdy $a \equiv b \pmod{p_i^{min(\alpha_i, \beta_i)}}$ dla wszystkich $i \in \{1, \ldots, k\}$.
Jeśli powyższy warunek jest spełniony, to powyższy układ kongruencji jest równoważny układowi:

$$x \equiv c_i \pmod{p_i^{max(\alpha_i, \beta_i)}}, i \in \{1, \ldots, k\},$$

gdzie $c_i = \begin{cases} a & \alpha_i \geqslant \beta_i \\ b & \alpha_i < \beta_i \end{cases}$