Teoria liczb II

1. *Algorytm Euklidesa*
Algorytm Euklidesa jest algorytmem obliczającym $NWD(a,b)$ dla $a,b \in \mathbb{N}$. Jest zdecydowanie szybszy niż popularnie stosowany algorytm rozkładania liczb na czynniki pierwsze i patrzenia, które są wspólne.
Załóżmy bez straty ogólności, że $a > b$. Algorytm opiera się na spostrzeżeniu, że $NWD(a,b) = NWD(b, a \mod b)$. Zauważmy, że $a \mod b = a - b[\frac{a}{b}]$. A zatem jeśli $d \mid a$ i $d \mid b$, to $d \mid a - b[\frac{a}{b}]$, czyli $d \mid a \mod b$. Podobnie jeśli $d \mid a - b[\frac{a}{b}]$ i $d \mid b$, to $d \mid a$. A zatem zbiór wspólnych dzielników a i b jest taki sam, co zbiór wspólnych dzielników b i $a \mod b$, a więc i największe elementy w tych zbiorach są równe.
Skoro wiemy, że $NWD(a,b) = NWD(b, a \mod b)$, to możemy kontynuować tę operację aż do otrzymania 0. Wtedy ostatnia otrzymana niezerowa liczba to właśnie $NWD(a,b)$.

Przykład: NWD(87,72)=NWD(72,15)=NWD(15,12)=NWD(12,3)=NWD(3,0)=3

2. *Dla każdych $a,b \in \mathbb{N}$ istnieją takie $x,y \in \mathbb{Z}$, że $ax + by = NWD(a,b)$.*
Dowód: można pokazać przez indukcję, że każda otrzymana w algorytmie Euklidesa liczba jest postaci $ak + bl$, gdzie $k,l \in \mathbb{N}$. Na pewno $a = a \cdot 1 + b \cdot 0$, b podobnie, więc początek indukcji jest. Jeśli w pewnym momencie mamy $c = ak_1 + bl_1$ i $d = ak_2 + bl_2$, to wtedy $c \mod d = c - d[\frac{c}{d}] = ak_1 + bl_1 - (ak_2 + bl_2) \cdot e$, gdzie $e \in \mathbb{Z}$, więc $c \mod d$ też postaci $ak + bl$. Zatem na końcu dojdziemy do $NWD(a,b)$, które też będzie tej postaci.

Zauważmy, że w tej sytuacji mamy, że gdy $a \perp b$ to istnieją $x,y \in \mathbb{Z}$ takie, że $ax + by = 1$.

3. $NWD(a,b) \cdot NWW(a,b) = a \cdot b$
Dowód: rozpatrzmy pewną liczbę pierwszą p i wykładnik, w którym występuje z lewej i z prawej strony. Jeśli $p \nmid a$ i $p \nmid b$, to sprawa jest prosta, wykładniki to odpowiednio 0 i 0, czyli są równe. Jeśli $p \nmid a$, a $p \mid b$, to powiedzmy, że maksymalny wykładnik p w b to α. Wtedy w $NWD(a,b)$ wykładnik jest 0, a w $NWW(a,b)$ - α. A zatem również się sumuje. Gdy obie liczby są podzielne przez p w potęgach odpowiednio α i β, to wykładnik przy $NWD(a,b)$ będzie $\min(\alpha,\beta)$, a przy $NWW(a,b)$ będzie $\max(\alpha,\beta)$, a więc także po obu stronach wykładniki sumują się do tej samej liczby. Skoro p była dowolną liczbą pierwszą, to znaczy, że liczby po obu stronach są faktycznie równe.

4. *Ciąg Fibonacciego*
Ciąg Fibonacciego definiuje się następująco: $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$. Warto znać jego pierwsze kilka wartości - $0,1,1,2,3,5,8,13,21,34,55,\ldots$ - pomaga to dostrzec ciąg Fibonacciego w zadaniach, które w treści wcale go nie mają, a zauważenie, że tak naprawdę mowa o tym ciągu praktycznie rozwiązuje zadanie. Ciąg ten posiada sporo ciekawych własności, niektóre z nich to:

1. $NWD(F_{n+1}, F_n) = 1$

Możemy zastosować algorytm Euklidesa i dostajemy: $NWD(F_{n+1}, F_n) = NWD(F_n, F_{n-1}) = \ldots = NWD(F_2, F_1) = NWD(F_1, F_0) = NWD(1,0) = 1$

2. $F_n^2 = F_{n-1}F_{n+1} + (-1)^{n+1}$

Dowodzimy poprzez indukcję.
Początek: $F_1 = F_2 \cdot F_0 + 1$, zgadza się.
Krok: $F_{n+1}^2 = F_{n+1}(F_n + F_{n-1}) = F_nF_{n+1} + F_{n+1}F_{n-1} = F_nF_{n+1} + F_n^2 + (-1)^{n+1+1} = F_n(F_{n+1} + F_n) + (-1)^{n+2} = F_nF_{n+2} + (-1)^{n+2}$

3.$n \mid m \Rightarrow F_n \mid F_m$

Rozpatrujemy reszty modulo F_n. $F_0 \equiv 0, F_1 \equiv 1, F_2 \equiv 1, F_3 \equiv 2 \ldots F_n \equiv 0$, więc jeśli $F_{n+1} \equiv k$, to $F_{n+2} \equiv k, F_{n+3} \equiv 2k \ldots F_{2n} \equiv F_n \cdot k \equiv 0$. Podobnie $F_{3n} \equiv 0$ itd.

Warto zauważyć, że mając dane 2 kolejne wyrazy ciągu możemy się cofać, czyli znajdować poprzednie wyrazy, tzn. 2 kolejne wyrazy tego ciągu określają cały ciąg.

Konsekwencją tego jest, że reszty modulo k dla każdego $k \in \mathbb{N}$ powtarzają się, czyli jeżeli wystąpił już kiedyś wyraz np. podzielny przez k, to będzie ich nieskończenie wiele.

Istnieje wzór jawny na ciąg Fibonacciego, tak zwany wzór Bineta:

$$F_n = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^n$$

Warto wiedzieć, że taki istnieje, ale nie koniecznie trzeba go znać.

5. *Liczb pierwszych jest nieskończenie wiele*
Dowód: Dowód przeprowadzimy nie wprost. Przypuśćmy, że jest skończenie wiele liczb pierwszych, niech będą to: $p_1, p_2, \ldots, p_n$. Rozważmy liczbę $p = p_1p_2p_3 \ldots p_n + 1$. Zauważmy, że $p_1 \nmid p, p_2 \nmid p \ldots p_n \nmid p$, a zatem p dzieli się tylko przez 1 i przez samą siebie, więc jest liczbą pierwszą. Dodatkowo p jest większa od wszystkich p_i, więc wcześniej rozpatrywane liczby nie były wszystkimi liczbami pierwszymi, w ten sposób doszliśmy do sprzeczności.

6. *Małe twierdzenie Fermata*

Niech p będzie liczbą pierwszą, $n \in \mathbb{N}, p \nmid n$. Wtedy zachodzi $n^p \equiv n \mod p$ (inna wersja: $n^{p-1} \equiv 1 \mod p$).

Dowód: Rozpatrzmy zbiór $A = \{n, 2n, 3n, \ldots, (p-1)n\} \mod p$. Pokażemy, że $A = \{1, 2, \ldots, p-1\}$. Najpierw zauważmy, że wszystkie liczby postaci $in \mod p$ są z zakresu od 1 do $p-1$, bo $n \perp p$ oraz $i \perp p$. Oprócz tego wszystkie te liczby są różne. Przypuśćmy, że $in \mod p = jn \mod p$. Wtedy $p \mid in - jn$, czyli $p \mid n(i-j)$. Jednak $p \perp n$, więc $p \mid i-j$. Skoro $1 \leqslant i, j \leqslant p-1$, to $i - j = 0$, czyli $i = j$. A zatem każde dwie liczby tej postaci są różne. Mamy więc $\{n, 2n, \ldots, (p-1)n\} \mod p = \{1, 2, \ldots, p-1\} \mod p$. Po wymnożeniu stronami dostajemy: $n^{p-1}(p-1)! \equiv (p-1)! \mod p$, jednak $(p-1)! \perp p$, więc $n^{p-1} \equiv 1 \mod p$, c.n.d.

7. *Tw. Eulera*

Niech $n \in \mathbb{N}, a \perp n$, wtedy $a^{\varphi(n)} \equiv 1 \mod n$.

Najpierw wyjaśnijmy, że $\varphi(n)$ jest liczbą liczb względnie pierwszych z n mniejszych od n, $\varphi(n) = |\{1 \leqslant k \leqslant n : k \perp n\}|$. Zauważmy, że jeśli p jest liczbą pierwszą, to $\varphi(p) = p - 1$, bo wszystkie liczby mniejsze od p są z nią względnie pierwsze, a $\varphi(p^k) = p^{k-1} * (p-1)$, bo nie są z nią względnie pierwsze tylko liczby podzielne przez p, czyli co p-ta. Jednocześnie jeżeli $a \perp b$, to $\varphi(ab) = \varphi(a)\varphi(b)$, w ten sposób można już obliczyć $\varphi(n)$ dla każdego $n \in \mathbb{N}$.
Zwróćmy uwagę, że małe twierdzenie Fermata jest szczególnym przypadkiem twierdzenia Eulera, gdyż $\varphi(p) = p - 1$. Przejdźmy teraz do dowodu tw. Eulera, będzie on bardzo podobny do dowodu małego tw. Fermata.

Dowód: niech $A = \{ka : 1 \leqslant k \leqslant n, k \perp n\} \mod n$. Pokażemy, że $A = \{k : 1 \leqslant k \leqslant n, k \perp n\} \mod n = B$. Każda liczba $ka \mod n$ są z zakresu od 1 do $n-1$ i na dodatek są względnie pierwsze z n, bo $k \perp n$ i $a \perp n$. Poza tym jeśli $ka \mod n = la \mod n$, to $n \mid a(k-l)$, czyli $n \mid k - l$, czyli $k = l$. Zatem $\prod_{k\in A} ka \equiv \prod_{k\in A} k \mod n$, z czego wynika, że $a^{\varphi(n)} * \prod_{k\in A} k \equiv \prod_{k\in A} k \mod n$. Jednak ponieważ $\prod_{k\in A} k \perp n$, to $a^{\varphi(n)} \equiv 1 \mod n$, c.n.d.

8. *Chińskie tw. o resztach*

Niech $n_1, n_2, \ldots, n_k \in \mathbb{N}, n_i \perp n_j$ dla $i \neq j, a_1, a_2, \ldots, a_k \in \mathbb{N}$. Wtedy istnieje dokładnie jedna liczba $a \in \{0, 1, \ldots, n_1 n_2 \ldots n_k - 1\}$ taka, że $a \equiv a_i \mod n_i$.

Dowód: zauważmy, najpierw, że możliwych układów reszt modulo $n_1, n_2, \ldots, n_k$ jest $n_1 n_2 \ldots n_k$. Zauważmy też że dla każdej liczby z przedziału od 0 do $n_1 n_2 \ldots n_k - 1$ układ reszt, które daje ona modulo n_i jest różny. Gdyby x i y dawały ten sam układ reszt, to $n_1 \mid x - y, n_2 \mid x - y, \ldots, n_k \mid x - y$, czyli $n_1 n_2 \ldots n_k \mid x - y$, a to dla x i y z naszego przedziału możliwe jest tylko przy $x = y$. A zatem wszystkie układy reszt są przyjmowane i to każdy dokladnie raz, czyli jakkolwiek sobie nie wybierzemy żądanego układu znajdziemy dokładnie jedną liczbę w naszym przedziale realizującą te reszty, c.n.d.

9. *Tw. Wilsona*

$n \in \mathbb{N}, n > 1$ jest liczbą pierwszą wtedy i tylko wtedy gdy $(n-1)! \equiv -1 \mod n$

Dowód:
„$\Leftarrow$” Najpierw dowodzimy w lewo.
Dowodzimy nie wprost. Załóżmy, że n jest złożone. A zatem $n = p_1 \cdot p_2, n > p_1, p_2 > 1$. Wtedy $p_1 \mid (n-1)!$, więc $(n-1)!$ nie jest względnie pierwszy z n. Sprzeczność.
„$\Rightarrow$” Teraz dowodzimy w prawo.
Liczba p jest pierwsza, więc dla każdego k istnieje odwrotność modulo p, czyli $\bigwedge k \bigvee l : k \cdot l \equiv 1 \mod n$. Tylko dwie liczby są w parze ze sobą, są to 1 oraz $p-1$, gdyż aby $p \mid x^2 - 1$ potrzeba, by $p \mid (x+1)(x-1)$, czyli $p \mid (x-1)$ lub $p \mid (x+1)$. Liczb od 1 do $p-1$ jest parzyście wiele, więc wszystkie dobiorą się w pary, czyli $(p-1)! \equiv 1 \mod p$.