FAKT: Każda liczba naturalna ma rozkład na czynniki pierwsze.

TWIERDZENIE: Rozkład na czynniki pierwsze jest jednoznaczny.

Dowód: Załóżmy nie wprost, że liczby z niejednoznacznym rozkładem istnieją i n jest najmniejszą taką liczbą:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$
$$n = q_1 \cdot q_2 \cdot \ldots \cdot q_l$$

1° $\forall_{i,j}\ p_i \neq q_j$, bo gdyby $p_1 = q_1$, to $\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_l$

Co przeczy założeniu, że n jest najmniejsze z kilkoma rozkładami (różnymi).

2° Rozszerzony algorytm Euklidesa zastosowany dla p_1, q_1 wylicza $x, y \in \mathbb{Z}$ takie, że $xp_1 + yq_1 = 1$.

$$xp_1 + yq_1 = 1 \qquad / \cdot p_2 p_3 \cdot \ldots \cdot p_k$$

$$x\cancel{p_1 p_2} \cdots p_k + y q_1 p_2 \cdots p_k = p_2 p_3 \cdots p_k = n'$$

$$q_1 \mid x q_1 \cdots q_l + y q_1 p_2 \cdots p_k = p_2 p_3 \cdots p_k = n'$$

Zatem $n' = \frac{n}{p_1}$ ma rozkład, w którym występuje q_1: $n' = q_1 r_1 \cdots r_s$, więc n' ma dwa różne rozkłady. ($n' = p_2 p_3 \cdots p_k = q_1 r_1 \cdots r_s$). Sprzeczność z założeniem, że n jest najmniejszą taką liczbą.

TWIERDZENIE: Liczb pierwszych jest nieskończenie wiele.

Dowód: Załóżmy nie wprost, że $p_1 \ldots p_n$ to wszystkie liczby pierwsze. Liczba $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1$ ma jakiś rozkład na czynniki pierwsze i w tym rozkładzie nie występują $p_1 \ldots p_n$, zatem $p_1 \ldots p_n$ nie są jedynymi liczbami pierwszymi, co jest sprzeczne z naszym założeniem.

PROBLEM: Wygeneruj losową k-cyfrową liczbę pierwszą.

ROZWIĄZANIE: Wylosuj k-cyfrową liczbę naturalną i sprawdź czy jest ona pierwsza.

$\pi(n)$ - ilość liczb pierwszych w przedziale $[1, n)$

$$\pi(n) \sim \frac{n}{\ln n}$$

Z tego wzoru wynika, że losowa liczba k-cyfrowa jest pierwsza z prawdopodobieństwem $\Theta\left(\frac{1}{k}\right)$, czyli dla np. $k=1000$ będziemy mieć liczby pierwsze co około 1000.

TWIERDZENIE CZEBYSZEWA

$$\pi(n) = \Theta\left(\frac{n}{\log n}\right)$$

Dowód: $\pi(n) = O\left(\frac{n}{\log n}\right)$

Lemat: $\prod_{p \leq n} p \leq 4^n$ (p - liczby pierwsze), dowód lematu przez indukcję po n:

1° Dla małych n można łatwo sprawdzić bezpośrednio.

2° Krok indukcyjny (wystarczy pokazać dla nieparzystych n):

$$\prod_{p \leq n} p = \prod_{p \leq \frac{n+1}{2}} p \cdot \prod_{\frac{n+1}{2} < p \leq n} p = 4^{\frac{n+1}{2}} \cdot 4^{\frac{n-1}{2}} \leq 4^n$$

Z założenia indukcyjnego $\prod_{p \leq \frac{n+1}{2}} p \leq 4^{\frac{n+1}{2}}$.

to jest liczba naturalna

$$\prod_{\frac{n+1}{2} < p \leq n} p \leq \binom{n}{\frac{n+1}{2}} = \frac{\left(\frac{n+1}{2}+1\right)\cdots(n-1)\,n}{\left(n-\left(\frac{n+1}{2}\right)\right)!} = \frac{\left(\left(\frac{n+1}{2}\right)+1\right)\cdots(n-1)\,n}{\left(\frac{n-1}{2}\right)!}$$

$$2\binom{n}{\frac{n+1}{2}} \leq \binom{n}{\frac{n+1}{2}} + \binom{n}{\frac{n-1}{2}} \leq \sum_{k=0}^{n} \binom{n}{k} = 2^n \Rightarrow \binom{n}{\frac{n+1}{2}} \leq 2^{n-1} = 4^{\frac{n-1}{2}}$$

Pokażemy jak z lematu wynika, że $\pi(n) = O\left(\frac{n}{\log n}\right)$. Niech $k = \pi(n)$.

$$\overbrace{k!}^{1\cdot 2\cdot 3\cdot\ldots} \leq \overbrace{\prod_{p\leq n} p}^{\leq 2\cdot 3\cdot 5\cdot\ldots} \leq 4^n \Rightarrow k! \leq 4^n. \Rightarrow \left(\frac{k}{2}\right)^{\left(\frac{k}{2}\right)} \leq 4^n$$

nie ma różnicy czy mamy $<, \leq$

$$\left(\frac{k}{2}\right)^{\left(\frac{k}{2}\right)} \leq k!$$

$$\frac{k}{2}\log\frac{k}{2} \leq \log 4^n = 2n$$

Pokażemy, że z tego wynika $k = O\left(\frac{n}{\log n}\right)$:

1° $k \leq 2\sqrt{n}$

2° $k > 2\sqrt{n} \Rightarrow \log\frac{k}{2} \geq \log\sqrt{n} = \frac{\log n}{2} \Rightarrow$

$$\Rightarrow \frac{k}{2}\cdot\frac{\log n}{2} \leq \frac{k}{2}\log\frac{k}{2} \leq 2n \Rightarrow k \leq \frac{8n}{\log n}$$

Mając dokładną wartość k wiemy, że $k \leq \max\left\{2\sqrt{n}, \frac{8n}{\log n}\right\} = O\left(\frac{n}{\log n}\right)$.

Teraz pokażemy, że $\pi(n) = \Omega\left(\frac{n}{\log n}\right)$:

$$\frac{1}{4^n} \geq \int_0^1 x^n(1-x)^n dx \left(= \int_0^1 \underbrace{(x(1-x))^n}_{\max = \frac{1}{4^n}} dx\right) = \int_0^1 (a_{2n}x^{2n} + a_{2n-1}x^{2n-1} + a_1 x + a_0)\, dx =$$

$s \geq 1$ (aby całka była dodatnia)

$$= \frac{a_{2n}}{2n+1} + \frac{a_{2n-1}}{2n} + \ldots + \frac{a_1}{2} + \frac{a_0}{1} = \frac{s}{NWW(1,2,\ldots,2n+1)} > 0$$

Stąd: $\frac{1}{4^n} \geq \frac{1}{NWW(1,2,\ldots,2n+1)} \Rightarrow 4^n \leq NWW(1,2,\ldots,2n+1)$

$$NWW(1,2,\ldots,N) = 2^{\lfloor \log_2 N\rfloor}\cdot 3^{\lfloor \log_3 N\rfloor}\cdot 5^{\lfloor \log_5 N\rfloor}\cdot\ldots\cdot p^{\lfloor \log_p N\rfloor}, \text{ gdzie } p = \max\{p : p \leq n\}$$

$$\underbrace{2n}_{\log 4^n} \leq \log NWW(1,2,\ldots,2n+1) = \sum_{p\leq 2n+1} \log p \cdot \lfloor \log_p(2n+1)\rfloor =$$

$$= \sum_{p\leq 2n+1} \log p \cdot \left\lfloor \frac{\log(2n+1)}{\log p}\right\rfloor \leq \pi(2n+1)\cdot\log(2n+1)$$

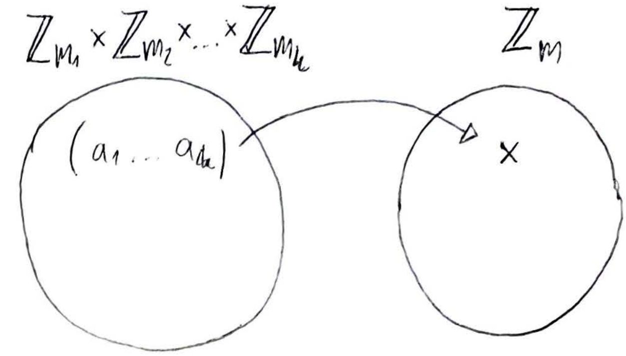
$$2n \leq \pi(2n+1)\log(2n+1) \Rightarrow \frac{2n}{\log(2n+1)} \leq \pi(2n+1) \Rightarrow \pi(N) = \Omega\left(\frac{n}{\log n}\right)$$

Chińskie twierdzenie o resztach

Niech $m_1, \dots, m_k \in \mathbb{N}$ i $(\forall i,j \ i \neq j)(m_i \perp m_j)$, $m = m_1 m_2 \dots m_k$.

Dla dowolnych $a_1, \dots, a_k$: $a_i \in \mathbb{Z}_{m_i}$ istnieje dokładnie jedna reszta $x \in \mathbb{Z}_m$ taka, że spełniony jest układ kongruencji:

$$
\begin{aligned}
x &\equiv a_1 \bmod m_1 \\
x &\equiv a_2 \bmod m_2 \\
&\dots \\
x &\equiv a_k \bmod m_k
\end{aligned}
$$



Dowód: Najpierw pokażemy istnienie takiego x dla dowolnej krotki $(a_1 \dots a_k)$.

$$x' = a_1 \frac{m}{m_1}\left(\left(\frac{m}{m_1}\right)^{-1} \bmod m_1\right) + \dots + a_k \frac{m}{m_k}\left(\left(\frac{m}{m_k}\right)^{-1} \bmod m_k\right)$$

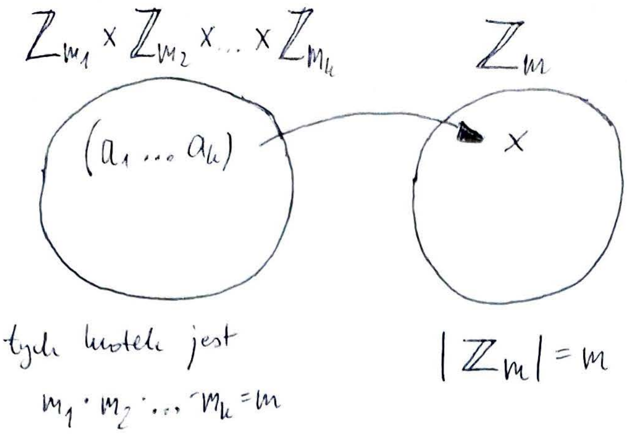
Pokażemy, że x' spełnia powyższy układ kongruencji (chociaż niekoniecznie $x' \in \mathbb{Z}_m$). Dla dowolnego i mamy:

$$a_i \underbrace{\frac{m}{m_i}\left(\left(\frac{m}{m_i}\right)^{-1} \bmod m_i\right)}_{1} \equiv a_i \bmod m_i$$

oraz gdy $i \neq j$:

$$a_j \left(\frac{m}{m_j}\right)\left(\left(\frac{m}{m_j}\right)^{-1} \bmod m_j\right) \equiv 0 \bmod m_i$$

Jako że $x' \in \mathbb{Z}$, to $x = x' \bmod m$.



Ta funkcja jest różnowartościowa ze zbioru m-elementowego w inny zbiór m-elementowy, więc jest ona bijekcją.

Funkcja Eulera

$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ ← zbiór reszt n

$\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : x^{-1} \bmod n \text{ istnieje}\} = \{x \in \mathbb{Z}_n : x \perp n\}$ ← zbiór elementów odwracalnych

$\varphi(n) = |\mathbb{Z}_n^*|$

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k} \Rightarrow \varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$\varphi(p) = p - 1$

$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$

$m_i = p_i^{n_i}$

Niech $n = p_1^{n_1} \cdot p_2^{n_2} \cdot \ldots \cdot p_k^{n_k}$, wtedy $x \perp n \Leftrightarrow \forall i \; p_i \perp x \Leftrightarrow$

$$\Leftrightarrow \quad \forall i \; x \underset{p_i^{n_i}}{\equiv} a_i : a_i \in \mathbb{Z}_{p_i^{n_i}} \text{ i } a_i \perp p_i^{n_i} \quad (a_i \equiv x \bmod p_i^{n_i})$$

Liczba układów $(a_1 \ldots a_k)$ spełniających warunki $\forall i \; a_i \perp p_i^{n_i}$ wynosi:

$$\varphi(p_1^{n_1}) \cdot \varphi(p_2^{n_2}) \cdot \ldots \cdot \varphi(p_k^{n_k})$$

Zatem $\varphi(n) = \varphi(p_1^{n_1}) \cdot \varphi(p_2^{n_2}) \cdot \ldots \cdot \varphi(p_k^{n_k}) = p_1^{n_1}\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot p_k^{n_k}\left(1 - \frac{1}{p_k}\right) =$

$$= \underbrace{p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}}_{n} \cdot \left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right)$$