## TWIERDZENIE CZEBYSZEWA

**Twierdzenie 1.** (Czebyszew) Dla każdej liczby $n$ istnieje liczba pierwsza $p$ taka, że

$$n < p \leq 2n.$$

**Dowód.** Szacujemy współczynnik dwumianowy $\binom{2n}{n}$ tak, by zauważyć, że jeśli nie ma on dzielnika pierwszego $p$ spełniającego nierówności $n < p \leq 2n$, to byłby on „za mały". Dowód przebiega w kilku krokach.

**Krok 1.** Dowodzimy dla $n < 4000$, Wystarczy sprawdzić, że każda liczba z następującej listy jest pierwsza oraz każda (oprócz pierwszej) jest mniejsza od podwojonej poprzedniej:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001.$$

Możemy zatem założyć, że $n \geq 4000$.

**Krok 2.** Dowodzimy przez indukcję, że

$$\prod_{p \leq x} p \leq 4^{x-1}, \quad \text{dla} \quad x \geq 2.$$

(1) Wystarczy dla $x = q$, gdzie $q$ pierwsza.
(2) $q = 2$ oczywiste.
(3) $q = 2m + 1$. Wtedy

$$\prod_{p \leq 2m+1} p = \left( \prod_{p \leq m+1} p \right) \cdot \left( \prod_{m+1 < p \leq 2m+1} p \right) \leq 4^m \cdot \binom{2m+1}{m} \leq 4^m \cdot 2^{2m} = 4^{2m}.$$

Nierówność

$$\prod_{p \leq m+1} p \leq 4^m$$

wynika z założenia indukcyjnego; nierówność

$$\prod_{m+1 < p \leq 2m+1} p \leq \binom{2m+1}{m}$$

wynika stąd, że liczby pierwsze $p$ spełniające nierówność $m + 1 < p \leq 2m + 1$ występują w liczniku ułamka

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m! \cdot (m+1)!}$$

i nie występują w mianowniku; nierówność

$$\binom{2m+1}{m} \leq 2^{2m}$$

wynika stąd, że

$$\binom{2m+1}{m} = \frac{1}{2}\cdot\left(\binom{2m+1}{m} + \binom{2m+1}{m+1}\right) \le \frac{1}{2}\cdot 2^{2m+1} = 2^{2m}.$$

**Krok 3.** Twierdzenie Legendre'a.
Wykładnik potęgi, w której liczba $p$ występuje w rozwinięciu $n!$ wynosi

$$\sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor.$$

**Dowód.** Wśród czynników w iloczynie $n! = 1\cdot 2\cdot\ldots\cdot n$ jest $\lfloor\frac{n}{p}\rfloor$ podzielnych przez $p$, $\lfloor\frac{n}{p^2}\rfloor$ podzielnych przez $p^2$ itd.

**Krok 4.** Wykładnik potęgi, w której liczba $p$ występuje we współczynniku dwumianowym $\binom{2n}{n}$ wynosi

$$\sum_{k=1}^{r}\left(\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\cdot\left\lfloor\frac{n}{p^k}\right\rfloor\right),$$

gdzie $r = \max\{k:\ p^k \le 2n\}$. Każdy składnik jest równy 0 lub 1:

$$\left\lfloor\frac{2n}{p^k}\right\rfloor - 2\cdot\left\lfloor\frac{n}{p^k}\right\rfloor < \frac{2n}{p^k} - 2\left(\frac{n}{p^k}-1\right) = 2.$$

Zatem ten wykładnik jest nie większy od $r$. W szczególności ta potęga $p$ jest nie większa od $2n$. Zatem, jeśli $p > \sqrt{2n}$, to $p$ występuje w potędze pierwszej.

**Krok 5.** Jeśli $\frac{2}{3}n < p \le n$, to $p$ nie jest dzielnikiem $\binom{2n}{n}$. Jeśli bowiem $3p > 2n$, to w liczniku ułamka

$$\frac{(2n)!}{n!\cdot n!}$$

występują dokładnie dwie liczby podzielne przez $p$, mianowicie $p$ i $2p$. W mianowniku $p$ występuje dwukrotnie, więc się skróci.

**Krok 6.** Zatem

$$\binom{2n}{n} \le \left(\prod_{p\le\sqrt{2n}} 2n\right)\cdot\left(\prod_{\sqrt{2n}<p\le\frac{2}{3}n} p\right)\cdot\left(\prod_{n<p\le 2n} p\right).$$

Jeśli nie istnieje liczba pierwsza $p$ spełniająca nierówności $n < p \le 2n$, to ostatniego iloczynu po prostu nie ma. Pierwszy iloczyn jest nie większy od $(2n)^{\sqrt{2n}}$. Drugi iloczyn jest nie większy od $4^{\frac{2}{3}n}$ (krok 2). Zatem

$$\binom{2n}{n} \le (2n)^{\sqrt{2n}}\cdot 4^{\frac{2}{3}n}.$$

**Krok 7.** Zauważmy, że współczynnik dwumianowy $\binom{2n}{n}$ jest największy spośród

$$\binom{2n}{0}+\binom{2n}{2n},\binom{2n}{1},\binom{2n}{2},\ldots,\binom{2n}{2n-1}.$$

Zatem jest większy od średniej arytmetycznej:

$$\binom{2n}{n}\geq\frac{2^{2n}}{2n}$$

Stąd wynika, że $\frac{4^n}{2n}\leq(2n)^{\sqrt{2n}}\cdot 4^{\frac{2}{3}n}$, czyli $4^{\frac{n}{3}}\leq(2n)^{1+\sqrt{2n}}$.

**Krok 8.** Z nierówności $2^m>m+1$ wynika, że

$$2n=(\sqrt[6]{2n})^6<(\lfloor\sqrt[6]{2n}\rfloor+1)^6<2^{6\lfloor\sqrt[6]{2n}\rfloor}\leq 2^{6\sqrt[6]{2n}}.$$

Zatem

$$2^{2n}=4^n=(4^{\frac{n}{3}})^3\leq(2n)^{3(1+\sqrt{2n})}<2^{18\sqrt[6]{2n}(1+\sqrt{2n})}.$$

Ale $n\geq 4000$. Zatem $18<2\sqrt{2n}$, więc

$$2^{2n}<2^{\sqrt[6]{2n}(18+18\sqrt{2n})}=2^{20\sqrt[6]{2n}\sqrt{2n}}=2^{20(2n)^{2/3}}.$$

Stąd dostajemy $2n<20(2n)^{\frac{2}{3}}$, czyli $(2n)^3<20^3\cdot(2n)^2$. Zatem $2n<8000$, czyli $n<4000$, sprzeczność. ♠

---

## TEST LUCASA-LEHMERA

**Twierdzenie 2.** Niech $p$ będzie liczbą pierwszą nieparzystą. Definiujemy następujący ciąg liczb:

$$r_1=4,\quad r_k=(r_{k-1}^2-2)\,\mathbf{mod}\,M_p\quad\text{dla } k\geq 2\quad.$$

Wówczas liczba Mersenne'a $M_p$ jest pierwsza wtedy i tylko wtedy, gdy

$$r_{p-1}=0.$$

**Dowód.** Oznaczmy: $n=2^p-1$. Niech $q$ będzie dowolnym dzielnikiem pierwszym liczby $n$. Weźmy wielomian

$$f(X)=X^2-2^{\frac{p+1}{2}}\cdot X-1.$$

Niech $\alpha,\beta\in GF(q^2)$ będą pierwiastkami wielomianu $f(X)$.

Zauważmy, że jeśli $\Delta$ jest resztą kwadratową modulo $q$, to

$$\alpha,\beta\in\mathbb{Z}_q\ \text{ oraz }\ \mathbb{Z}_q\subseteq GF(q^2).$$

Jeśli natomiast $\Delta$ jest nieresztą kwadratową modulo $q$, to

$$\alpha, \beta \in \mathbb{Z}_q(\sqrt{\Delta}) \quad \text{oraz} \quad \mathbb{Z}_q(\sqrt{\Delta}) = GF(q^2).$$

Zauważmy następnie, że

$$\alpha + \beta = 2^{\frac{p+1}{2}} \quad \text{oraz} \quad \alpha\beta = -1.$$

Korzystając z powyższych równości dowodzimy przez indukcję, że

$$r_k \equiv \alpha^{2^k} + \beta^{2^k} \pmod{q}.$$

- Niech $k = 1$. Wtedy

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 2^{p+1} + 2 \equiv 4 = r_1 \pmod{n}.$$

- Załóżmy, że

$$\alpha^{2^k} + \beta^{2^k} \equiv r_k \pmod{n}.$$

  Wtedy

$$\alpha^{2^{k+1}} + \beta^{2^{k+1}} = (\alpha^{2^k} + \beta^{2^k})^2 - 2\alpha^{2^k}\beta^{2^k} \equiv r_k^2 - 2 \cdot (-1)^{2^k} = r_k^2 - 2 \equiv r_{k+1} \pmod{n}.$$

Załóżmy teraz, że $n$ jest liczbą pierwszą, czyli $q = n$. Zauważamy, że $\Delta$ jest wtedy nieresztą kwadratową modulo $n$. Mianowicie $\Delta = 2^{p+1} + 4 \equiv 6 \pmod{n}$ oraz

$$\left(\frac{6}{n}\right) = \left(\frac{2}{n}\right) \cdot \left(\frac{3}{n}\right).$$

Następnie

$$\left(\frac{2}{n}\right) = 1,$$

bo $(2^{\frac{p+1}{2}})^2 = 2^{p+1} \equiv 2 \pmod{n}$. Z drugiej strony

$$\left(\frac{3}{n}\right) = -\left(\frac{n}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Zatem

$$\left(\frac{6}{n}\right) = -1.$$

Stąd wynika, że wielomian $f(X)$ jest nierozkładalny nad ciałem $\mathbb{Z}_n$, a więc

$$\alpha, \beta \notin \mathbb{Z}_p.$$

Weźmy automorfizm Frobeniusa

$$\tau : GF(n^2) \to GF(n^2)$$

określony wzorem $\tau(x) = x^n$.

Wtedy $\tau(\alpha)$ jest pierwiastkiem wielomianu $f(X)$. Ponieważ $\tau(x) = x \Leftrightarrow x \in \mathbb{Z}_n$, więc $\tau(\alpha) \neq \alpha$. Zatem $\alpha^n = \beta$. Podobnie $\beta^n = \alpha$.

Stąd otrzymujemy

$$r_p \equiv \alpha^{2^p} + \beta^{2^p} = \alpha^{n+1} + \beta^{n+1} = 2\alpha\beta = -2 \pmod{n}.$$

Ale $r_p \equiv r_{p-1}^2 - 2 \pmod{n}$, więc

$$r_{p-1} \equiv 0 \pmod{n}.$$

Niech teraz $n$ będzie liczbą złożoną i załóżmy, że

$$r_{p-1} \equiv 0 \pmod{n}.$$

Niech $q$ będzie dzielnikiem pierwszym liczby $n$ takim, że $q^2 \leq n$. Wtedy $r_{p-1} \equiv 0 \pmod{q}$, czyli

$$\alpha^{2^{p-1}} + \beta^{2^{p-1}} = 0.$$

Zatem

$$\alpha^{2^p} + (\alpha\beta)^{2^{p-1}} = 0,$$

skąd dostajemy

$$\alpha^{2^p} = -1.$$

Stąd wynika, że rząd elementu $\alpha$ w grupie multyplikatywnej ciała $GF(q^2)$ jest równy $2^{p+1}$. Zatem $2^{p+1} \mid q^2 - 1$, co jest niemożliwe, gdyż wtedy

$$n < 2^{p+1} \leq q^2 - 1 < q^2 \leq n. \quad \spadesuit$$