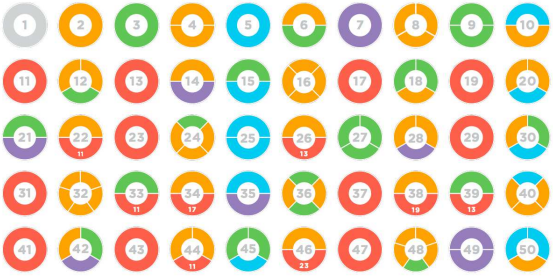


LICZBY PIERWSZE

ARKADIUSZ MĘCEL

Warsztaty KFndD „**Elementy teorii liczb i kryptografii**”,
Wydział Matematyki, Informatyki i Mechaniki UW, 3 XII 2022 r.

Definicja liczby pierwszej

Liczbę całkowitą $p > 1$ nazywamy:

- **pierwszą**, jeśli jej dodatnimi dzielnikami są tylko 1 oraz p,
- **złożoną**, jeśli nie jest liczbą pierwszą.

Zbiór wszystkich liczb całkowitych oznaczamy przez $\mathbb{Z}$.
Zbiór wszystkich liczb pierwszych oznaczamy przez $\mathbb{P}$.

Dla liczby naturalnej $n \geq 1$ przez p_n oznaczamy n-tą kolejną liczbę pierwszą.

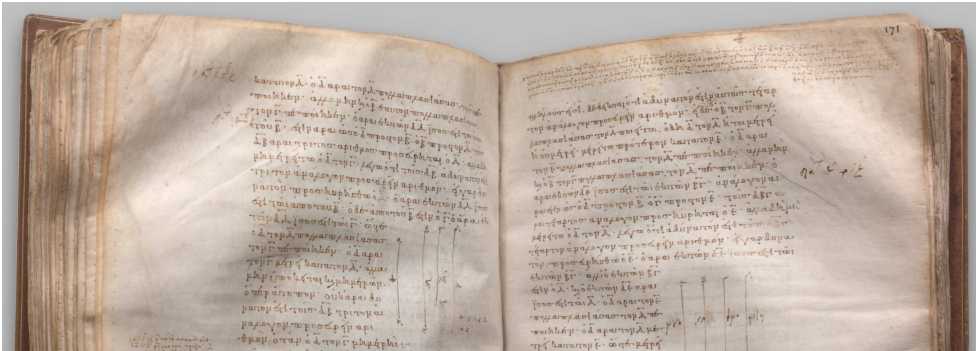
Przykłady

$$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \quad p_{20} = 71, \quad p_{2 \cdot 10^{17}} = 8512677386048191063$$

Twierdzenie Euklidesa (ok -300 r.) — *Elementy*, księga IX, Stwierdzenie 20

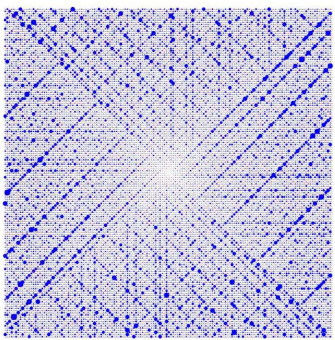
Jest więcej liczb pierwszych niż jakakolwiek ustalona ilość liczb pierwszych.

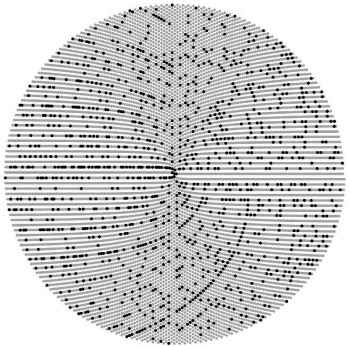
Niech a, b, c będą liczbami pierwszymi. Twierdzę, że istnieje więcej liczb pierwszych niż a, b, c. W tym celu rozważmy liczbę $d = abc + 1$.
Albo jest ona pierwsza albo ma czynnik pierwszy....

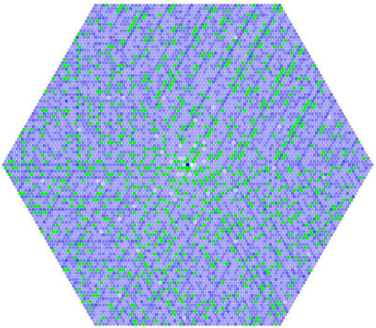


Główne pytanie

Jak rozmieszczone są wśród liczb naturalnych liczby pierwsze?







Czytaj też: Barbara Biły, *Trójkąt Klaubera i spirala Ulama od kuchni*, https://minut.polsl.pl/articles/A-20-001.pdf

Główne pytanie

Jak rozmieszczone są wśród liczb naturalnych liczby pierwsze?

- Euklides — liczb pierwszych jest nieskończenie wiele, ale w $\mathbb{N}$ są dowolnie duże *dziury* — ciągi kolejnych liczb złożonych (wrócimy do tego).
- Euler — suma odwrotności wszystkich kolejnych liczb naturalnych oraz suma odwrotności wszystkich liczb pierwszych są nieskończone

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots=\infty, \quad \frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\ldots=\infty$$

ale sumy częściowe rosną *bardzo wolno*:

  - suma odwrotności n pierwszych liczb naturalnych rośnie jak $log(n)$ – czyli mniej więcej jak liczba cyfr liczby n,
  - druga suma rośnie mniej więcej jak $\log(\log(n))$ — suma sumy cyfr liczby n.

- Legendre, Gauss — ile jest liczb pierwszych nie większych od n? Liczbę tą oznaczamy przez $\pi(n)$. Znowu *przeczuwa się* związek z liczbą cyfr n:

$$\pi(10^1) = 4$$
$$\pi(10^2) = 25$$
$$\pi(10^3) = 168$$
$$\pi(10^4) = 1229$$
$$\pi(10^5) = 9592$$
$$\pi(10^6) = 78498$$
$$\pi(10^7) = 664579$$
$$\pi(10^8) = 5761455$$
$$\pi(10^9) = 50847534$$
$$\pi(10^{10}) = 455052511$$
$$\pi(10^{11}) = 4118054813$$

Intuicje te były wielkim wyzwaniem dla XIX-wiecznych matematyków: Legendre'a, Gaussa, Czebyszewa, Riemanna, Rozwiązali je — w postaci tzw. **twierdzenia o liczbach pierwszych** Hadamard i niezależnie de la Vallee Poussin (1896).

Cel. Twierdzenie Czebyszewa (1850), inaczej: postulat Bertranda

Dla każdej liczby naturalnej $n \geq 2$ istnieje taka liczba pierwsza p, że:

$$n < p < 2n.$$



Oglądać będziemy dowód 19-letniego Paula Erdősa z 1932 roku.

CZĘŚĆ I

DZIELNIKI PIERWSZE I SILNIE

Adrien-Marie Legendre (1752-1833)

Notacja sigma-pi dla sum i iloczynów

Suma liczb $a_1, \ldots, a_n$ indeksowanych liczbami k ze zbioru od $\{1, \ldots, n\}$:

$$\sum_{k=1}^{n} a_k := a_1 + a_2 + a_3 + \ldots + a_n.$$

Iloczyn liczb $a_1, \ldots, a_n$ indeksowanych liczbami k ze zbioru od $\{1, \ldots, n\}$:

$$\prod_{k=1}^{n} a_k := a_1 \cdot a_2 \cdot a_3 \cdot \ldots \cdot a_n.$$

Przykłady

$$\sum_{k=1}^{10} \frac{1}{k} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10},$$

$$\sum_{k=1}^{n} k^2 = 1^2 + 2^2 + 3^3 + \ldots + n^2,$$

$$\prod_{k \leq n} k = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n.$$

Definicja liczby $n!$ (czytaj: n silnia)

Niech $n \geq 0$ będzie liczbą całkowitą. Określamy

$$n! = \begin{cases} 0, & \text{dla } n = 0 \\ 1, & \text{dla } n = 1 \\ 1 \cdot 2 \cdot \ldots \cdot n, & \text{dla } n > 1. \end{cases}$$

Przykłady

- $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$
- $5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$
- $6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$

Definicja liczby $n!$ (czytaj: n silnia)

Niech $n \geq 0$ będzie liczbą całkowitą. Określamy

$$n! = \begin{cases} 0, & \text{dla } n = 0 \\ 1, & \text{dla } n = 1 \\ 1 \cdot 2 \cdot \ldots \cdot n, & \text{dla } n > 1. \end{cases}$$

Proste własności

- $(n+1)! = (n+1) \cdot n!$
- $n \cdot n! = (n+1)! - n!$
- $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$

Uwaga — liczba $n!$ ma *małe* dzielniki pierwsze

Niech $n \geq 2$ będzie liczbą całkowitą. **Dzielnikami pierwszymi** liczby $n!$ mogą być jedynie liczby nie większe niż n, czyli:

$$2, 3, \ldots, n.$$

Dowód. Na mocy twierdzenia o **jednoznaczności** rozkładu liczby całkowitej $n > 1$ na czynniki pierwsze mamy następującą własność (można ją dowodzić inaczej).

Fakt

Niech $p \in \mathbb{P}$ oraz niech $a, b \in \mathbb{Z}$. Wówczas:

$$p \mid ab \quad \Longrightarrow \quad (p \mid a \quad \text{lub} \quad p \mid b).$$

Problem

Niech $n \geq 2$ będzie liczbą całkowitą oraz niech p będzie liczbą pierwszą. Wyznaczyć największą potęgę całkowita liczby p, która jest dzielnikiem n, to znaczy — liczbę całkowitą k taką, że

$$p^k \mid n \quad \text{oraz} \quad p^{k+1} \nmid n$$

Liczbę k oznaczamy przez $v_p(n)$ (jest to tzw. wykładnik p-adyczny liczby n).

Przykłady

- $v_3(24) = v_3(2^3 \cdot 3) = 1$,
- $v_5(400) = v_5(2^4 \cdot 5^2) = 4$,
- $v_2(6!) = v_2(1 \cdot \mathbf{2} \cdot 3 \cdot \mathbf{4} \cdot 5 \cdot \mathbf{6}) = 4$.

Zadanie. Niech n będzie liczbą naturalną. Znaleźć najwyższą potęgę liczby 2 będącą dzielnikiem liczby

$$(n+1)(n+2)\cdot\ldots\cdot 2n.$$

Zadanie. Niech n będzie liczbą naturalną. Znaleźć najwyższą potęgę liczby 2 będącą dzielnikiem liczby

$$(n+1)(n+2)\cdot\ldots\cdot 2n.$$

Rozwiązanie. Rozważana liczba równa jest ilorazowi

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

Zadanie. Niech n będzie liczbą naturalną. Znaleźć najwyższą potęgę liczby 2 będącą dzielnikiem liczby

$$(n+1)(n+2)\cdot\ldots\cdot 2n.$$

Rozwiązanie. Rozważana liczba równa jest ilorazowi

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

Przedstawiamy powyższą liczbę w postaci ilorazu iloczynów:

$$\frac{1\cdot 2\cdot 3\cdot\ldots\cdot 2n}{1\cdot 2\cdot 3\cdot\ldots\cdot n} = 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot\frac{2\cdot 4\cdot 6\cdot\ldots\cdot 2n}{1\cdot 2\cdot 3\cdot\ldots\cdot n} = 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot 2^n.$$

Zadanie. Niech n będzie liczbą naturalną. Znaleźć najwyższą potęgę liczby 2 będącą dzielnikiem liczby

$$(n+1)(n+2)\cdot\ldots\cdot 2n.$$

Rozwiązanie. Rozważana liczba równa jest ilorazowi

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

Przedstawiamy powyższą liczbę w postaci ilorazu iloczynów:

$$\frac{1\cdot 2\cdot 3\cdot\ldots\cdot 2n}{1\cdot 2\cdot 3\cdot\ldots\cdot n} = 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot\frac{2\cdot 4\cdot 6\cdot\ldots\cdot 2n}{1\cdot 2\cdot 3\cdot\ldots\cdot n} = 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)\cdot 2^n.$$

Zatem

$$v_2((n+1)(n+2)\cdot\ldots\cdot 2n) = n.$$

Ćwiczenie. Własności v_p

Niech p będzie liczbą pierwszą, zaś a, b niech będą liczbami całkowitymi. Wówczas:

- $a \mid b$ wtedy i tylko wtedy, gdy $v_p(a) \leq v_p(b)$, dla dowolnej $p \in \mathbb{P}$,
- $v_p(a \cdot b) = v_p(a) + v_p(b)$,
- $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$,
- $v_p(a^n) = n \cdot v_p(a)$,
- $v_p(NWD(a,b)) = \min\{v_p(a), v_p(b)\}$,
- $v_p(NWW(a,b)) = \max\{v_p(a), v_p(b)\}$,
- $v_p(a \pm b) \geq \min\{v_p(a), v_p(b)\}$, a równość zachodzi, gdy $v_p(a) \neq v_p(b)$.

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

- Mamy:

$$v_p(n!) = v_p(1) + v_p(2) + \ldots + v_p(n).$$

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

- Mamy:
$$v_p(n!) = v_p(1) + v_p(2) + \ldots + v_p(n).$$
- Jeśli m nie jest wielokrotnością p, to $v_p(m) = 0$. Zatem:

$$\boxed{v_p(n!) = v_p(p) + v_p(2p) + \ldots + v_p(kp),}$$

gdzie k — największa liczba całkowita nie większa niż $\frac{n}{p}$.

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

- Mamy:
$$v_p(n!) = v_p(1) + v_p(2) + \ldots + v_p(n).$$
- Jeśli m nie jest wielokrotnością p, to $v_p(m) = 0$. Zatem:
$$\boxed{v_p(n!) = v_p(p) + v_p(2p) + \ldots + v_p(kp),}$$
gdzie k — największa liczba całkowita nie większa niż $\frac{n}{p}$.
- Największą liczbę całkowitą nie większą niż $x \in \mathbb{R}$ oznaczamy przez $[x]$. Zatem liczba liczb naturalnych $k \leq n$ takich, że $v_p(k) \geq 1$ wynosi:
$$\left[\frac{n}{p}\right].$$

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

- Mamy:
$$v_p(n!) = v_p(1) + v_p(2) + \ldots + v_p(n).$$
- Jeśli m nie jest wielokrotnością p, to $v_p(m) = 0$. Zatem:
$$\boxed{v_p(n!) = v_p(p) + v_p(2p) + \ldots + v_p(kp),}$$
gdzie k — największa liczba całkowita nie większa niż $\frac{n}{p}$.
- Liczba liczb naturalnych $k \leq n$ takich, że $v_p(k) \geq 2$ wynosi:
$$\left[\frac{n}{p^2}\right].$$

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

- Mamy:
$$v_p(n!) = v_p(1) + v_p(2) + \ldots + v_p(n).$$
- Jeśli m nie jest wielokrotnością p, to $v_p(m) = 0$. Zatem:
$$\boxed{v_p(n!) = v_p(p) + v_p(2p) + \ldots + v_p(kp),}$$
gdzie k — największa liczba całkowita nie większa niż $\frac{n}{p}$.
- Liczba liczb naturalnych $k \leq n$ takich, że $v_p(k) \geq 3$ wynosi:
$$\left[\frac{n}{p^3}\right].$$

Niech $n \geq 1$ będzie liczbą naturalną oraz $p \in \mathbb{P}$. Chcemy wyznaczyć

$$v_p(n!).$$

Jeśli $k \leq n$ oraz $v_p(k) = s$, to owe s kopii liczby p wchodzących do rozkładu na czynniki pierwsze liczby $k \leq n$ wliczamy do sumy $v_p(1) + \ldots + v_p(n)$ poprzez s kroków:

- raz, gdy liczymy k jako liczbę która spełnia $v_p(k) \geq 1$,
- raz, gdy liczymy k jako liczbę która spełnia $v_p(k) \geq 2$,
- raz, gdy liczymy k jako liczbę która spełnia $v_p(k) \geq 3$,
- $\vdots$
- raz, gdy liczymy k jako liczbę która spełnia $v_p(k) \geq s$,

Formuła Legendre'a

Niech n będzie liczbą całkowitą dodatnią oraz p – liczbą pierwszą. Wówczas:

$$v_p(n!) = \sum_{k=1}^{s} \left[\frac{n}{p^k}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + \left[\frac{n}{p^s}\right],$$

gdzie s jest największą liczbą całkowitą taką, że $p^s \leq n$.

Przykład 1.

$$v_5(2020!) = \left[\frac{2020}{5}\right] + \left[\frac{2020}{25}\right] + \left[\frac{2020}{125}\right] + \left[\frac{2020}{625}\right] = 404 + 80 + 16 + 3 = 503.$$

Uwaga. Dla dowolnej dodatniej liczby naturalnej mamy $v_2(n) > v_5(n)$, więc liczba zer stojących na końcu zapisu dziesiętnego liczby naturalnej n wynosi $v_5(n!)$

Przykład 2. Nie istnieje liczba naturalna n, dla której $2^n \mid n!$

- Pokażemy, że dla każdego $n > 0$ mamy $v_2(2^n) > v_2(n!)$.

Przykład 2. Nie istnieje liczba naturalna n, dla której $2^n \mid n!$

- Pokażemy, że dla każdego $n > 0$ mamy $v_2(2^n) > v_2(n!)$.
- Ze wzoru Legendre'a

$$v_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \ldots + \left[\frac{n}{2^s}\right],$$

gdzie $2^s \leq n < 2^{s+1}$.

Przykład 2. Nie istnieje liczba naturalna n, dla której $2^n \mid n!$

- Pokażemy, że dla każdego $n > 0$ mamy $v_2(2^n) > v_2(n!)$.
- Ze wzoru Legendre'a

$$v_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \ldots + \left[\frac{n}{2^s}\right],$$

  gdzie $2^s \leq n < 2^{s+1}$.
- A zatem mamy $v_2(n!) \leq \frac{n}{2} + \frac{n}{2^2} + \ldots + \frac{n}{2^s} = \frac{n}{2}\left(1 + \frac{1}{2} + \ldots + \frac{1}{2^{s-1}}\right)$.

Przykład 2. Nie istnieje liczba naturalna n, dla której $2^n \mid n!$

- Pokażemy, że dla każdego $n > 0$ mamy $v_2(2^n) > v_2(n!)$.
- Ze wzoru Legendre'a

$$v_2(n!) = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \ldots + \left[\frac{n}{2^s}\right],$$

  gdzie $2^s \leq n < 2^{s+1}$.
- A zatem mamy $v_2(n!) \leq \frac{n}{2} + \frac{n}{2^2} + \ldots + \frac{n}{2^s} = \frac{n}{2}\left(1 + \frac{1}{2} + \ldots + \frac{1}{2^{s-1}}\right)$.
- Ze wzoru skróconego mnożenia $a^s - 1 = (a-1)(a^{s-1} + a^{s-2} + \ldots + a + 1)$:

$$1 + \frac{1}{2} + \ldots + \ldots + \frac{1}{2^{s-1}} = \frac{1 - \frac{1}{2^s}}{1 - \frac{1}{2}} = 2 - \frac{1}{2^{s-1}}.$$

  zatem mamy:

$$v_2(n!) \leq \frac{n}{2}\left(2 - \frac{1}{2^{s-1}}\right) < n = v_2(2^n).$$

Przykład 3. Dla dowolnych liczb naturalnych n, m liczba

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

jest calkowita.

Przykład 3. Dla dowolnych liczb naturalnych n, m liczba

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

jest calkowita.

- Pokażemy, że dla dowolnej liczby pierwszej p zachodzi nierówność:

$$v_p(n! \cdot m!) = v_p(n!) + v_p(m!) \leq v_p((m+n)!).$$

Przykład 3. Dla dowolnych liczb naturalnych n, m liczba

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

jest calkowita.

- Pokażemy, że dla dowolnej liczby pierwszej p zachodzi nierówność:

$$v_p(n! \cdot m!) = v_p(n!) + v_p(m!) \leq v_p((m+n)!).$$

- Niech s będzie liczbą naturalną taką, że $p^s \leq m+n < p^{s+1}$. Wtedy

$$\begin{aligned}
v_p(m!) &= \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \ldots + \left[\frac{m}{p^s}\right] \\
v_p(n!) &= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots + \left[\frac{n}{p^s}\right] \\
v_p((m+n)!) &= \left[\frac{m+n}{p}\right] + \left[\frac{m+n}{p^2}\right] + \ldots + \left[\frac{m+n}{p^s}\right]
\end{aligned}$$

Przykład 3. Dla dowolnych liczb naturalnych n, m liczba

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

jest całkowita.

- Pokażemy, że dla dowolnej liczby $1 \leq r \leq s$ mamy:

$$\left[\frac{m}{p^r}\right] + \left[\frac{n}{p^r}\right] \leq \left[\frac{m+n}{p^r}\right]$$

Przykład 3. Dla dowolnych liczb naturalnych n, m liczba

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

jest całkowita.

- Pokażemy, że dla dowolnej liczby $1 \leq r \leq s$ mamy:

$$\left[\frac{m}{p^r}\right] + \left[\frac{n}{p^r}\right] \leq \left[\frac{m+n}{p^r}\right]$$

- Dla dowolnych $x, y \in \mathbb{R}$ mamy jednak $[x] \leq x,$ oraz $\quad [y] \leq y$, zatem

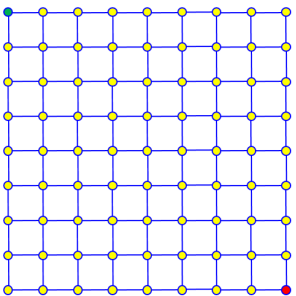
$$[x] + [y] \leq x + y.$$

  Skoro jednak $[x] + [y]$ jest całkowita, to

$$[x] + [y] \leq [x + y].$$

CZĘŚĆ II

LICZBA $\binom{2n}{n}$ I JEJ DZIELNIKI PIERWSZE



Ile jest dróg *w prawo i w dół* z lewego górnego rogu do prawego dolnego?

Kluczowa uwaga

Każda liczba pierwsza p spełniająca nierówność $n < p < 2n$ jest dzielnikiem liczby

$$\binom{2n}{n} = \frac{2n!}{n! \cdot n!}.$$

Dowód. Mamy:

$$\frac{(2n)!}{n! \cdot n!} = \frac{n! \cdot (n+1)(n+2)\ldots 2n}{n! \cdot n!} = \frac{(n+1)(n+2)\ldots 2n}{n!}.$$

Żadna liczba pierwsza p spełniająca $n < p < 2n$ nie jest dzielnikiem $n!$

Każda taka liczba wchodzi do rozkładu $\frac{(2n)!}{n! \cdot n!}$ dokładnie raz.

Pytanie. Czy jest możliwe, że $\binom{2n}{n}$ jest iloczynem tylko liczb pierwszych od 2 do n?

Wyznaczymy $x_p = v_p\binom{2n}{n}$.

Wyznaczymy $x_p = v_p\binom{2n}{n} = v_p((2n)!) - v_p(n! \cdot n!) = v_p((2n)!) - 2v_p(n!)$.

Z wzoru Legendre'a jest to suma postaci:

$$\sum_k \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Wyznaczymy $x_p = v_p\binom{2n}{n} = v_p((2n)!) - v_p(n! \cdot n!) = v_p((2n)!) - 2v_p(n!)$.

Z wzoru Legendre'a jest to suma postaci:

$$\sum_k \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Dla każdego k mamy:

$$0 \leq \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2.$$

Wyznaczymy $x_p = v_p\binom{2n}{n} = v_p((2n)!) - v_p(n! \cdot n!) = v_p((2n)!) - 2v_p(n!)$.

Z wzoru Legendre'a jest to suma postaci:

$$\sum_k \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Dla każdego k mamy:

$$0 \leq \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2.$$

Zatem

- każdy powyższy składnik równy jest 0 lub 1,

Wyznaczymy $x_p = v_p\binom{2n}{n} = v_p((2n)!) - v_p(n! \cdot n!) = v_p((2n)!) - 2v_p(n!)$.

Z wzoru Legendre'a jest to suma postaci:

$$\sum_k \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Dla każdego k mamy:

$$0 \leq \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2.$$

Zatem

- każdy powyższy składnik równy jest 0 lub 1,
- x_p szacuje się przez maksymalne k,

Wyznaczymy $x_p = v_p\binom{2n}{n} = v_p((2n)!) - v_p(n! \cdot n!) = v_p((2n)!) - 2v_p(n!)$.

Z wzoru Legendre'a jest to suma postaci:

$$\sum_k \left(\left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] \right).$$

Dla każdego k mamy:

$$0 \leq \left[\frac{2n}{p^k} \right] - 2 \left[\frac{n}{p^k} \right] < \frac{2n}{p^k} - 2 \left(\frac{n}{p^k} - 1 \right) = 2.$$

Zatem

- każdy powyższy składnik równy jest 0 lub 1,
- x_p szacuje się przez maksymalne k,
- a zatem otrzymujemy szacowanie $p^{x_p} \leq 2n$.

Wyznaczymy $x_p = v_p\binom{2n}{n} = v_p((2n)!) - v_p(n! \cdot n!) = v_p((2n)!) - 2v_p(n!)$.

Wniosek

Niech $x_p = v_p\binom{2n}{n}$. Wówczas:

- $x_p \leq 1$, dla $p > \sqrt{2n}$,
- $x_p = 0$, dla p nieparzystych większych od $\frac{2}{3}n$ i nie większych od n.

Wyznaczymy $x_p = v_p\binom{2n}{n}$.

Wniosek

Niech $x_p = v_p\binom{2n}{n}$. Wówczas:

- $x_p \leq 1$, dla $p > \sqrt{2n}$,
- $x_p = 0$, dla p nieparzystych większych od $\frac{2}{3}n$ i nie większych od n.

Dowód.

- Jeśli $p > \sqrt{2n}$, to $p^2 > 2n$. A zatem w tym przypadku maksymalne k takie, że $p^k \leq 2n$ równe jest 1.

Wyznaczymy $x_p = v_p\binom{2n}{n}$.

Wniosek

Niech $x_p = v_p\binom{2n}{n}$. Wówczas:

- $x_p \leq 1$, dla $p > \sqrt{2n}$,
- $x_p = 0$, dla p nieparzystych większych od $\frac{2}{3}n$ i nie większych od n.

Dowód.

- Jeśli $p > \sqrt{2n}$, to $p^2 > 2n$. A zatem w tym przypadku maksymalne k takie, że $p^k \leq 2n$ równe jest 1.
- Jeśli $p \geq 3$ oraz zachodzi warunek $2n < 3p \leq 3n$, to
  - w iloczynie $(2n)!$ są tylko dwie wielokrotności p, więc $v_p((2n)!) = 2$,
  - liczba $n!$ ma czynnik p, więc $v_p(n! \cdot n!) = 2$.

Jak zatem oszacować można rozkład $\binom{2n}{n}$ na czynniki pierwsze?

Jak zatem oszacować można rozkład $\binom{2n}{n}$ na czynniki pierwsze?

$$\binom{2n}{n} \leq \prod_{2 \leq p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p,$$

przy czym po prawej stronie mamy:

- iloczyn potęg k_i dzielników pierwszych p_i od 2 do nie dalej niż $\sqrt{2n}$, przy czym zawsze:

$$p_i^{k_i} \leq 2n \qquad \text{, bo} \quad k_i = v_{p_i}\binom{2n}{n},$$

Jak zatem oszacować można rozkład $\binom{2n}{n}$ na czynniki pierwsze?

$$\binom{2n}{n} \leq \prod_{2 \leq p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p,$$

przy czym po prawej stronie mamy:

- iloczyn potęg k_i dzielników pierwszych p_i od 2 do nie dalej niż $\sqrt{2n}$, przy czym zawsze:
$$p_i^{k_i} \leq 2n \qquad \text{, bo} \qquad k_i = v_{p_i}\binom{2n}{n},$$
- iloczyn tych liczb pierwszych, które są większe niż $\sqrt{2n}$ a nie większe niż $\frac{2}{3}n$, wchodzących do rozkładu $\binom{2n}{n}$ z wykładnikiem **co najwyżej** 1,

Jak zatem oszacować można rozkład $\binom{2n}{n}$ na czynniki pierwsze?

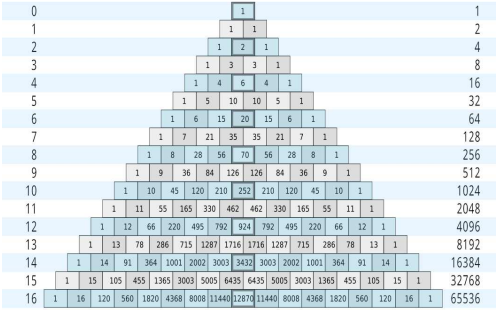
$$\binom{2n}{n} \leq \prod_{2 \leq p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p,$$

przy czym po prawej stronie mamy:

- iloczyn potęg k_i dzielników pierwszych p_i od 2 do nie dalej niż $\sqrt{2n}$, przy czym zawsze:
$$p_i^{k_i} \leq 2n \qquad \text{, bo} \qquad k_i = v_{p_i}\binom{2n}{n},$$
- iloczyn tych liczb pierwszych, które są większe niż $\sqrt{2n}$ a nie większe niż $\frac{2}{3}n$, wchodzących do rozkładu $\binom{2n}{n}$ z wykładnikiem **co najwyżej** 1,
- iloczyn tych liczb pierwszych, które są większe od n, a mniejsze od $2n$ — takie, o które pyta postulat Bertranda. Jeśli takie p istnieje, to $x_p = 1$.

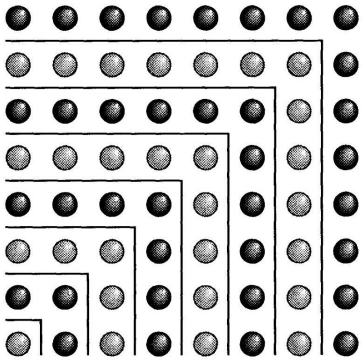
CZĘŚĆ III

SZACOWANIE LICZB POSTACI 4^n

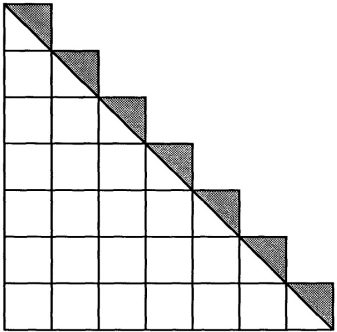


Suma elementów w co drugim wierszu jest potęgą 4.

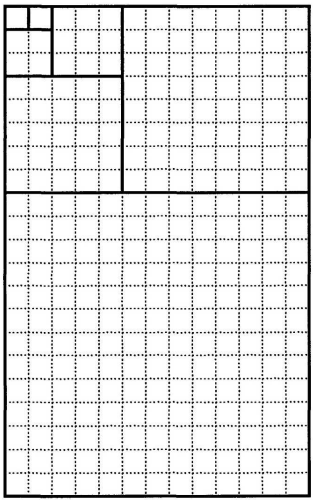
Zagadka 1. Ułóż wzór opisujący poniższy rysunek.



Zagadka 2. Ułóż wzór opisujący poniższy rysunek.



Zagadka 3. Ułóż wzór opisujący poniższy rysunek.



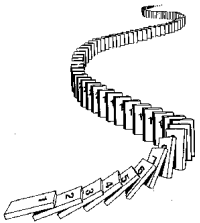
Zasada indukcji matematycznej (mocnej)

Niech $T(1), T(2), T(3), \ldots$ — zdania ponumerowane l. naturalnymi. Jeśli

(i) $T(1)$ jest zdaniem prawdziwym,

(ii) dla każdego $k \in \mathbb{N}$ prawdziwość zdań $T(1), T(2), \ldots, T(k)$ implikuje prawdziwość zdania $T(k+1)$,

to zdanie $T(n)$ jest prawdziwe, dla każdej liczby naturalnej $n \geq 1$.



Zasada indukcji matematycznej (mocnej)

Niech $T(1), T(2), T(3), \ldots$ — zdania ponumerowane l. naturalnymi. Jeśli

(i) $T(1)$ jest zdaniem prawdziwym,

(ii) dla każdego $k \in \mathbb{N}$ prawdziwość zdań $T(1), T(2), \ldots, T(k)$ implikuje prawdziwość zdania $T(k+1)$,

to zdanie $T(n)$ jest prawdziwe, dla każdej liczby naturalnej $n \geq 1$.

Przykład

- zdanie $T(1)$ postaci $1 = \frac{1 \cdot 2}{2}$,
- zdanie $T(2)$ postaci $1 + 2 = \frac{2 \cdot 3}{2}$,
- zdanie $T(3)$ postaci $1 + 2 + 3 = \frac{3 \cdot 4}{2}$,
- ...
- zdanie $T(k)$ postaci $1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$.

Zasada indukcji matematycznej (mocnej)

Niech $T(1), T(2), T(3), \ldots$ — zdania ponumerowane l. naturalnymi. Jeśli

(i) $T(1)$ jest zdaniem prawdziwym,

(ii) dla każdego $k \in \mathbb{N}$ prawdziwość zdań $T(1), T(2), \ldots, T(k)$ implikuje prawdziwość zdania $T(k+1)$,

to zdanie $T(n)$ jest prawdziwe, dla każdej liczby naturalnej $n \geq 1$.

Przykład

- zdanie $T(1)$ mówiące, że $1 = \frac{1 \cdot 2}{2}$ jest prawdziwe,
- zakładając prawdziwość zdania $T(k)$ pokażmy prawdziwość zdania $T(k+1)$:

$$\underbrace{1 + 2 + \ldots + k}_{\text{stosujemy } T(k)} + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

Zadanie. Pokaż, że dla dowolnego naturalnego $n \geq 1$ zachodzi nierówność:

$$2^n \geq n + 1.$$

Zadanie. Pokaż, że dla dowolnego naturalnego $n \geq 1$ zachodzi nierówność:

$$2^n \geq n + 1.$$

Dowód indukcyjny. Zdanie $T(k)$: zachodzi nierówność $2^k \geq k + 1$.

- Baza indukcji. Dla $k = 1$ mamy równość.

Zadanie. Pokaż, że dla dowolnego naturalnego $n \geq 1$ zachodzi nierówność:

$$2^n \geq n + 1.$$

Dowód indukcyjny. Zdanie $T(k)$: zachodzi nierówność $2^k \geq k + 1$.

- Baza indukcji. Dla $k = 1$ mamy równość.
- Krok indukcyjny. Załóżmy, że $2^k > k + 1$. Pokażmy, że $2^{k+1} > k + 2$.

Zadanie. Pokaż, że dla dowolnego naturalnego $n \geq 1$ zachodzi nierówność:

$$2^n \geq n + 1.$$

Dowód indukcyjny. Zdanie $T(k)$: zachodzi nierówność $2^k \geq k + 1$.

- Baza indukcji. Dla $k = 1$ mamy równość.
- Krok indukcyjny. Załóżmy, że $2^k > k + 1$. Pokażmy, że $2^{k+1} > k + 2$.
- Mamy:

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot (k + 1) = 2k + 2 > k + 2.$$

Zadanie. Pokaż, że dla dowolnego naturalnego $n \geq 1$ zachodzi nierówność:

$$2^n \geq n + 1.$$

Dowód indukcyjny. Zdanie $T(k)$: zachodzi nierówność $2^k \geq k + 1$.

- Baza indukcji. Dla $k = 1$ mamy równość.
- Krok indukcyjny. Załóżmy, że $2^k > k + 1$. Pokażmy, że $2^{k+1} > k + 2$.
- Mamy:

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot (k + 1) = 2k + 2 > k + 2.$$

- Pokazaliśmy zatem, że implikacja $T(k) \Rightarrow T(k + 1)$ zachodzi dla każdego k. Skoro zarówno baza, jak i krok indukcyjny są prawdziwe, rozważana nierówności zachodzi dla każdego naturalnego $n \geq 1$.

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

- Zdanie $T(k)$ — zachodzi nierówność $p_k < 2^{2^k}$.

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

- Zdanie $T(k)$ — zachodzi nierówność $p_k < 2^{2^k}$.
- Oczywiście $T(1)$ jest prawdą: $p_1 = 2 < 2^{2^1}$.

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

- Zdanie $T(k)$ — zachodzi nierówność $p_k < 2^{2^k}$.
- Oczywiście $T(1)$ jest prawdą: $p_1 = 2 < 2^{2^1}$.
- Załóżmy, że zdania $T(1), \ldots, T(k)$ są prawdziwe. Mamy wtedy

$$p_1 < 2^{2^1}, \quad p_2 < 2^{2^2}, \quad \ldots, \quad p_k < 2^{2^k}.$$

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

- Zdanie $T(k)$ — zachodzi nierówność $p_k < 2^{2^k}$.
- Oczywiście $T(1)$ jest prawdą: $p_1 = 2 < 2^{2^1}$.
- Załóżmy, że zdania $T(1), \ldots, T(k)$ są prawdziwe. Mamy wtedy

$$p_1 < 2^{2^1}, \quad p_2 < 2^{2^2}, \quad \ldots, \quad p_k < 2^{2^k}.$$

- Mnożąc te wszystkie nierówności stronami:

$$p_1 p_2 \ldots p_k + 1 \leq 2^{2^1} \cdot 2^{2^2} \cdot \ldots \cdot 2^{2^k} = 2^{2^1+2^2+\ldots+2^k} = 2^{2^{k+1}-2} < 2^{2^{k+1}}.$$

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

- Zdanie $T(k)$ — zachodzi nierówność $p_k < 2^{2^k}$.
- Oczywiście $T(1)$ jest prawdą: $p_1 = 2 < 2^{2^1}$.
- Załóżmy, że zdania $T(1), \ldots, T(k)$ są prawdziwe. Mamy wtedy
$$p_1 < 2^{2^1}, \quad p_2 < 2^{2^2}, \quad \ldots, \quad p_k < 2^{2^k}.$$
- Mnożąc te wszystkie nierówności stronami:
$$p_1 p_2 \ldots p_k + 1 \leq 2^{2^1} \cdot 2^{2^2} \cdot \ldots \cdot 2^{2^k} = 2^{2^1+2^2+\ldots+2^k} = 2^{2^{k+1}-2} < 2^{2^{k+1}}.$$
- Każdy dzielnik pierwszy p liczby $p_1 p_2 \ldots p_k + 1$ spełnia $p < 2^{2^{k+1}}$. Żadna z liczb $p_1, \ldots, p_k$ nie jest dzielnikiem pierwszym liczby $p_1 p_2 \ldots p_k + 1$.

Zadanie. Pokaż, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^n}$.

- Zdanie $T(k)$ — zachodzi nierówność $p_k < 2^{2^k}$.
- Oczywiście $T(1)$ jest prawdą: $p_1 = 2 < 2^{2^1}$.
- Załóżmy, że zdania $T(1), \ldots, T(k)$ są prawdziwe. Mamy wtedy

$$p_1 < 2^{2^1}, \quad p_2 < 2^{2^2}, \quad \ldots, \quad p_k < 2^{2^k}.$$

- Mnożąc te wszystkie nierówności stronami:

$$p_1 p_2 \ldots p_k + 1 \leq 2^{2^1} \cdot 2^{2^2} \cdot \ldots \cdot 2^{2^k} = 2^{2^1+2^2+\ldots+2^k} = 2^{2^{k+1}-2} < 2^{2^{k+1}}.$$

- Każdy dzielnik pierwszy p liczby $p_1 p_2 \ldots p_k + 1$ spełnia $p < 2^{2^{k+1}}$. Żadna z liczb $p_1, \ldots, p_k$ nie jest dzielnikiem pierwszym liczby $p_1 p_2 \ldots p_k + 1$.
- A zatem jednym z dzielników pierwszych liczby $p_1 p_2 \ldots p_k + 1$ jest p_{k+1}, co kończy krok indukcyjny. Szacowanie to jest nieefektywne.

Zadanie. Dla dowolnej liczby naturalnej $n > 1$ zachodzą nierówności

$$\frac{4^n}{2n} \leq \binom{2n}{n} < 4^n.$$

Zadanie. Dla dowolnej liczby naturalnej $n > 1$ zachodzą nierówności

$$\frac{4^n}{2n} \leq \binom{2n}{n} < 4^n.$$

Dowód.

- Z jednej strony mamy

$$2n \cdot \binom{2n}{n} = \frac{(2n)! \cdot 2n}{n! \cdot n!} = \underbrace{\frac{2}{1} \cdot \frac{3}{1} \cdot \frac{4}{2} \cdot \frac{5}{2} \cdots \frac{2n-2}{n-1} \cdot \frac{2n-1}{n-1} \cdot \frac{2n}{n} \cdot \frac{2n}{n}}_{2n}.$$

- każdy z $2n$ ułamków jest większy lub równy od 2, więc iloczyn jest $\geq 2^{2n} = 4^n$.

Zadanie. Dla dowolnej liczby naturalnej $n > 1$ zachodzą nierówności

$$\frac{4^n}{2n} \leq \binom{2n}{n} < 4^n.$$

Dowód.

- Z jednej strony mamy

$$2n \cdot \binom{2n}{n} = \frac{(2n)! \cdot 2n}{n! \cdot n!} = \underbrace{\frac{2}{1} \cdot \frac{3}{1} \cdot \frac{4}{2} \cdot \frac{5}{2} \cdots \frac{2n-2}{n-1} \cdot \frac{2n-1}{n-1} \cdot \frac{2n}{n} \cdot \frac{2n}{n}}_{2n}.$$

- każdy z $2n$ ułamków jest większy lub równy od 2, więc iloczyn jest $\geq 2^{2n} = 4^n$.

Dowód drugiej nierówności będzie analogiczny.

Zadanie. Dla dowolnej liczby naturalnej $n > 1$ zachodzą nierówności

$$\frac{4^n}{2n} \leq \binom{2n}{n} < 4^n.$$

Dowód (cd.) Mamy:

$$\begin{aligned}\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} &= 2^n \cdot \frac{n! \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2n-1}{n! \cdot n!} \\ &= 2^n \cdot \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2n-1}{n!} \\ &< 2^n \cdot \frac{2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n}{n!} = 4^n\end{aligned}$$

Zadanie. Dla dowolnej liczby naturalnej $n > 1$ zachodzą nierówności

$$\frac{4^n}{2n} \leq \binom{2n}{n} < 4^n.$$

Dowód (cd.) Mamy:

$$\begin{aligned}\binom{2n}{n} = \frac{(2n)!}{n! \cdot n!} &= 2^n \cdot \frac{n! \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2n-1}{n! \cdot n!} \\ &= 2^n \cdot \frac{1 \cdot 3 \cdot 5 \cdot \ldots \cdot 2n-1}{n!} \\ &< 2^n \cdot \frac{2 \cdot 4 \cdot 6 \cdot \ldots \cdot 2n}{n!} = 4^n\end{aligned}$$

Uwaga. Analogicznie pokazujemy, że dla $n > 1$:

$$\binom{2n+1}{n} < 4^n.$$

Wniosek

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych p spełniających nierówność $n < p < 2n$ jest mniejszy od 4^n.

To jest prawda, bo

$$\prod_{n<p<2n} p \leq \binom{2n}{n} < 4^n.$$

Wniosek

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych p spełniających nierówność $n < p < 2n$ jest mniejszy od 4^n.

Znacznie lepszy wniosek

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych nie większych niż n można oszacować z góry przez 4^{n-1}, tzn.

$$\prod_{p \leq n} p \leq 4^{n-1}.$$

Wniosek

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych p spełniających nierówność $n < p < 2n$ jest mniejszy od 4^n.

Znacznie lepszy wniosek

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych nie większych niż n można oszacować z góry przez 4^{n-1}, tzn.

$$\prod_{p \leq n} p \leq 4^{n-1}.$$

Dowód korzysta z zasady indukcji (a nie korzysta z wniosku wyżej!). Gdy $k = 2$ otrzymujemy $2 \leq 4$. Załóżmy, że fakt ten jest prawdziwy dla pewnego $k > 2$.

Twierdzenie

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych nie większych niż n można oszacować z góry przez 4^{n-1}, tzn. $\prod_{p \leq n} p \leq 4^{n-1}$.

Dowód. Wystarczy założyć, że $k = 2m + 1 \in \mathbb{P}$. Mamy:

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p < 2m+1} p.$$

Twierdzenie

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych nie większych niż n można oszacować z góry przez 4^{n-1}, tzn. $\prod_{p \leq n} p \leq 4^{n-1}$.

Dowód. Wystarczy założyć, że $k = 2m+1 \in \mathbb{P}$. Z zał. indukcyjnego dla $m+1 < k$:

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p < 2m+1} p \leq 4^m \cdot \prod_{m+1 < p < 2m+1} p$$

Twierdzenie

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych nie większych niż n można oszacować z góry przez 4^{n-1}, tzn. $\prod_{p \leq n} p \leq 4^{n-1}$.

Dowód. Wystarczy założyć, że $k = 2m+1 \in \mathbb{P}$. Z zał. indukcyjnego dla $m+1 < k$:

$$\prod_{p \leq 2m+1} p = \prod_{p \leq m+1} p \cdot \prod_{m+1 < p < 2m+1} p \leq 4^m \cdot \prod_{m+1 < p < 2m+1} p$$

Druga kluczowa uwaga wynikająca z rozważania liczb pierwszych p od $m+1$ do $2m+1$, które dzielą $(2m+1)!$, ale nie $m!$ lub $(m+1)!$: zachodzi nierówność

$$\prod_{m+1 < p < 2m+2} p \leq \binom{2m+1}{m} < 4^m.$$

Twierdzenie

Dla każdej liczby naturalnej $n > 1$ iloczyn wszystkich liczb pierwszych nie większych niż n można oszacować z góry przez 4^{n-1}, tzn. $\prod_{p \le n} p \le 4^{n-1}$.

Dowód. Wystarczy założyć, że $k = 2m+1 \in \mathbb{P}$. Z zał. indukcyjnego dla $m+1 < k$:

$$\prod_{p \le 2m+1} p = \prod_{p \le m+1} p \cdot \prod_{m+1 < p < 2m+1} p \le 4^m \cdot \prod_{m+1 < p < 2m+1} p$$

Druga kluczowa uwaga wynikająca z rozważania liczb pierwszych p od $m+1$ do $2m+1$, które dzielą $(2m+1)!$, ale nie $m!$ lub $(m+1)!$: zachodzi nierówność

$$\prod_{m+1 < p < 2m+2} p \le \binom{2m+1}{m} < 4^m.$$

Zatem całość szacuje się przez $4^m \cdot 4^m = 4^{2m} = 4^{k-1}$, co daje krok indukcyjny.

CZĘŚĆ IV

DOWÓD POSTULATU BERTRANDA

Bill Gates i Warren Buffet. Duża paletka symbolizuje *grube*szacowania, które zaraz wykonamy.

Następujące liczby są pierwsze
i każda następna jest mniejsza niż dwukrotność poprzedniej:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001, 7993, 15973, 23333.$$

Wniosek

Przykład: każdy przedział $(n, 2n]$ dla $n \leq 23328$ zawiera jedną z powyższych 17 liczb pierwszych. A zatem hipoteza Bertranda działa dla $n \leq 23328$.

Wiemy, że:

$$\binom{2n}{n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p,$$

przy czym po prawej stronie mamy:

- iloczyn potęg k_i liczb pierwszych p_i mniejszych od $\sqrt{2n}$, przy czym zawsze:
$$p_i^{k^i} \leq 2n,$$
- iloczyn tych liczb pierwszych, które są większe niż $\sqrt{2n}$ a nie większe niż $\frac{2}{3}n$, wchodzących do rozkładu $\binom{2n}{n}$ z wykładnikiem **co najwyżej** 1,
- iloczyn tych liczb pierwszych, które są większe od n, a mniejsze od $2n$ — takie, o które pyta postulat Bertranda. Jeśli takie p istnieje, to $x_p = 1$.

A zatem

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p,$$

przy czym po prawej stronie mamy:

- iloczyn potęg k_i liczb pierwszych p_i mniejszych od $\sqrt{2n}$, przy czym zawsze:
$$p_i^{k^i} \leq 2n,$$
- iloczyn tych liczb pierwszych, które są większe niż $\sqrt{2n}$ a nie większe niż $\frac{2}{3}n$, wchodzących do rozkładu $\binom{2n}{n}$ z wykładnikiem **co najwyżej** 1,
- iloczyn tych liczb pierwszych, które są większe od n, a mniejsze od $2n$ — takie, o które pyta postulat Bertranda. Jeśli takie p istnieje, to $x_p = 1$.

Załóżmy, wbrew tezie Postulatu, że trzeci iloczyn równy jest 1.

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Mamy teraz:

- jeśli $p_i \leq \sqrt{2n}$, to $p_i^{k_i} \leq 2n$, czyli:

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p,$$

bowiem liczb p_i jest nie więcej niż $\sqrt{2n}$.

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Mamy teraz:

- jeśli $p_i \leq \sqrt{2n}$, to $p_i^{k_i} \leq 2n$, czyli:

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p,$$

  bowiem liczb p_i jest nie więcej niż $\sqrt{2n}$.

- Na mocy „lepszego wniosku" wiemy, że:

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq \prod_{p \leq \frac{2}{3}n} p \leq 4^{\frac{2}{3}n}.$$

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

W rezultacie

$$4^n \leq (2n)^{\sqrt{2n}+1} \cdot 4^{\frac{2}{3}n} \iff 2^{2n} \leq (2n)^{3(1+\sqrt{2n})}$$

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

W rezultacie

$$4^n \leq (2n)^{\sqrt{2n}+1} \cdot 4^{\frac{2}{3}n} \iff 2^{2n} \leq (2n)^{3(1+\sqrt{2n})}$$

Jak się okazuje, gdy n jest „dostatecznie duże", powyższa nierówność nie jest prawdziwa. Korzystając ze znanej nam nierówności $k + 1 \leq 2^k$ mamy:

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

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

W rezultacie

$$4^n \leq (2n)^{\sqrt{2n}+1} \cdot 4^{\frac{2}{3}n} \iff 2^{2n} \leq (2n)^{3(1+\sqrt{2n})}$$

Jak się okazuje, gdy n jest „dostatecznie duże", powyższa nierówność nie jest prawdziwa. Korzystając ze znanej nam nierówności $k + 1 \leq 2^k$ mamy:

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

Mamy więc:

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

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Mamy wreszcie $18 < 2\sqrt{2n}$, dla $n \geq 50$, więc

$$2^{2n} = 2^{18 \cdot \sqrt[6]{2n}(1+\sqrt{2})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}}.$$

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Mamy wreszcie $18 < 2\sqrt{2n}$, dla $n \geq 50$, więc

$$2^{2n} = 2^{18 \cdot \sqrt[6]{2n}(1+\sqrt{2})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}}.$$

Warunek $2n < 20(2n)^{\frac{2}{3}}$ daje $(2n)^{\frac{1}{3}} < 20$, czyli $n < 4000$.

A zatem trzeci iloczyn liczb pierwszych od n do $2n$ nie może być równy 1 dla $n \geq 4000$. Dowód twierdzenia Czebyszewa jest zakończony.

Przypuśćmy zatem, że

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p.$$

Mamy wreszcie $18 < 2\sqrt{2n}$, dla $n \geq 50$, więc

$$2^{2n} = 2^{18 \cdot \sqrt[6]{2n}(1+\sqrt{2})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{\frac{2}{3}}}.$$

Warunek $2n < 20(2n)^{\frac{2}{3}}$ daje $(2n)^{\frac{1}{3}} < 20$, czyli $n < 4000$.

A zatem trzeci iloczyn liczb pierwszych od n do $2n$ nie może być równy 1 dla $n \geq 4000$. Dowód twierdzenia Czebyszewa jest zakończony.

Uwaga. Szacując bardzo podobnie jak wyżej można pokazać, że w każdym przedziale $(n, 2n)$ jest w istocie $\frac{\sqrt{2n}}{2}$ liczb pierwszych.

Uwaga. Szacując bardzo podobnie jak wyżej można pokazać, że w każdym przedziale $(n, 2n)$ jest w istocie

$$\frac{\sqrt{2n}}{2}$$

liczb pierwszych.

Uwaga. Szacując bardzo podobnie jak wyżej można pokazać, że w każdym przedziale $(n, 2n)$ jest w istocie

$$\frac{\sqrt{2n}}{2}$$

liczb pierwszych.

Rzeczywiście, każda taka liczba pierwsza szacuje się przez $2n$, a nierówność:

$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot (2n)^{\sqrt{2n}/2}$$

nie jest prawdziwa dla $2n \geq 900$. Dla pozostałych n sprawdzamy ręcznie.

Uwaga. Szacując bardzo podobnie jak wyżej można pokazać, że w każdym przedziale $(n, 2n)$ jest w istocie

$$\frac{\sqrt{2n}}{2}$$

liczb pierwszych.

Rzeczywiście, każda taka liczba pierwsza szacuje się przez $2n$, a nierówność:

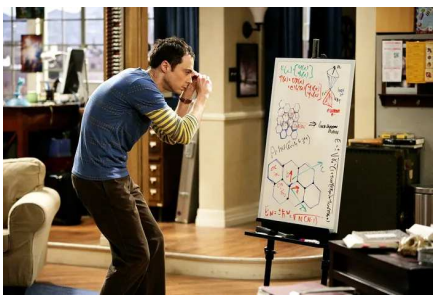
$$\frac{4^n}{2n} \leq \prod_{p_i \leq \sqrt{2n}} p_i^{k_i} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot (2n)^{\sqrt{2n}/2}$$

nie jest prawdziwa dla $2n \geq 900$. Dla pozostałych n sprawdzamy ręcznie.

Przykład: dla $n \geq 8$ mamy $\sqrt{2n}/2 \geq 2$, czyli w przedziale $(n, 2n)$ leżą co najmniej dwie liczby pierwsze (i nie lepiej: dla $n = 8$ i $2n = 16$ są to: 11, 13).
Już dla $n \geq 9$ między n oraz $2n$ są już co najmniej 3 liczby pierwsze.

CZĘŚĆ V

WNIOSKI, PYTANIA, PROBLEMY



Sheldon Cooper przy tablicy, kadr z serialu *The Big Bang Theory*

Przykładowe zastosowania

Zadanie. Każda liczba naturalna większa od 7 jest sumą liczb pierwszych i ewentualnie liczby 1, przy czym każdy składnik może być użyty tylko raz.

Zadanie. Liczba $n!$ nie jest k-tą potęgą liczby całkowitej, dla $k > 1$.

Zadanie. Dla każdej całkowitej liczby dodatniej k istnieją co najmniej trzy różne liczby pierwsze mające dokładnie k cyfr.

Zadanie. Pokaż, że jeśli m oraz n są dodatnimi liczbami całkowitymi, to :

$$\frac{1}{m} + \frac{1}{m+1} + \ldots + \frac{1}{m+n} \notin \mathbb{Z}.$$

Twierdzenie Czebyszewa nie jest traktowane jako *kanon olimpijski*. Te i znacznie więcej zadań opartych o twierdzenie Czebyszewa znaleźć można na przykład w poniższym artykule w Crux Mathematicorum: https://cms.math.ca/wp-content/uploads/crux-pdfs/CRUXv42n4.pdf.

Przykładowe zastosowania

Zadanie. Każda liczba naturalna n jest sumą liczb pierwszych, przy czym każdy składnik może być użyty tylko raz.

Zadanie. Liczba $n!$ nie jest k-tą potęgą liczby całkowitej, dla $k > 1$.

Zadanie. Dla każdej całkowitej liczby dodatniej k istnieją co najmniej trzy różne liczby pierwsze mające dokładnie k cyfr.

- Dla $1 \leq n \leq 7$ teza jest jasna. Załóżmy, że istnieje liczba całkowita większa od 7, która nie rozkłada się na sumę parami różnych liczb pierwszych. Weźmy najmniejszą taką liczbę n. Między $n/2$, a n są co najmniej...
- Każdy dzielnik pierwszy $n!$ jest liczbą od 1 do n. Między $n/2$, a n jest liczba pierwsza p i oczywiście $2p > n$, czyli $v_p(n!) = 1$. Nie może to być potęga.
- **Wskazówka.** Popatrz na liczby $10^{k-1}, 2 \cdot 10^{k-1}, 4 \cdot 10^{k-1}, 8 \cdot 10^{k-1}$.

Twierdzenie Sylvestera (1892)

Iloczyn kolejnych k liczb całkowitych większych niż k jest podzielny przez liczbę pierwszą większą niż k.

Uwaga. Dowodząc twierdzenie Czebyszewa kluczowe jest pokazanie, że iloczyn $(n+1)(n+2)\cdots 2n$ ma dzielnik pierwszy większy od n.

Twierdzenie Erdősa-Selfridge'a (1966 — otwarty 150 lat)

Nie istnieją $n, m, k, s \in \mathbb{Z}_+$, gdzie $k, s \geq 2$, że $(n+1)(n+2)\ldots(n+k) = m^s$.

Twierdzenie Erdősa

Dla każdej dodatniej liczby całkowitej k istnieje liczba $N \in \mathbb{N}$ taka, że dla liczb naturalnych $n > N$ istnieje co najmniej k liczb pierwszych między n oraz $2n$.

Problem Sierpińskiego (1958)

Czy dla każdej liczby naturalnej $n \geq 1$ oraz dowolnej liczby naturalnej $k \leq n$ pomiędzy liczbami kn oraz $(k+1)n$ znajduje się liczba pierwsza?

- dla $k = 1$ to jest postulat Bertranda,
- dla $k = 2$ jest elementarny dowód Bachraoui (2006): M. El Bachraoni, *Primes in the Interval [2n,3n]*, Int. J. Contemp. Math. Sciences (13) 2006, 617-621. https://www.researchgate.net/publication/267076371_Primes_in_the_interval_2n3n,
- dla $k = 3$ jest wynik Luo (2011), oraz Nagury dla $k = 5$ (1957).

Sformułowanie hipotezy jest w artykule Schinzel A., Sierpiński W., *Sur certaines hypotheses concernant les nombres premiers,* Acta Arithm., 4, (1958), 185-208 (strona 206, hipoteza H1 z komentarzami), http://matwbn.icm.edu.pl/ksiazki/aa/aa4/aa432.pdf.

Problem Legendre'a

Czy dla każdej liczby naturalnej $n \geq 1$ pomiędzy liczbami n^2 oraz $(n+1)^2$ znajduje się liczba pierwsza?

Problem ten nosi nazwisko Legendre'a z uwagi na to, że popełnił on w 1798 roku brzemienny w skutkach błąd próbując udowodnić twierdzenie o istnieniu nieskończenie wielu liczb pierwszych w dowolnym ciągu arytmetycznym o względnie pierwszym pierwszym pierwszym wyrazie i różnicy. Wynik ten pokazał w pełni dopiero Dirichlet w roku 1838. Jeden ze skutków błędu Legendre'a objawił się w pracach A. Desbovesa, który wywiódł z niego, że między kolejnymi kwadratami jest liczba pierwsza. Z czasem problem stał się sławny (jeden z tzw. problemów Landau). Problem ten do dziś wydaje się poza zasięgiem. W 1937 roku Ingham udowodnił, że dla dostatecznie dużych n istnieje liczba pierwsza pomiędzy n^3 oraz $(n+1)^3$.

Źródło. W. Narkiewicz, *The Development of Prime Number Theory*, https://link.springer.com/chapter/10.1007/978-3-662-13157-2_2.