Teoria liczb 7

28 maja 2017

We have seen that the sequence of prime numbers $2, 3, 5, 7, \ldots$ is infinite. To see that the size of its gaps is not bounded, let $N := 2 \cdot 3 \cdot 5 \cdots p$ denote the product of all prime numbers that are smaller than $k + 2$, and note that none of the k numbers

$$N + 2, N + 3, N + 4, \ldots, N + k, N + (k + 1)$$

is prime, since for $2 \leq i \leq k + 1$ we know that i has a prime factor that is smaller than $k + 2$, and this factor also divides N, and hence also $N + i$. With this recipe, we find, for example, for $k = 10$ that none of the ten numbers

$$2312, 2313, 2314, \ldots, 2321$$

is prime.

But there are also upper bounds for the gaps in the sequence of prime numbers. A famous bound states that "the gap to the next prime cannot be larger than the number we start our search at." This is known as Bertrand's postulate, since it was conjectured and verified empirically for $n < 3\,000\,000$ by Joseph Bertrand. It was first proved for all n by Pafnuty Chebyshev in 1850. A much simpler proof was given by the Indian genius Ramanujan. Our Book Proof is by Paul Erdős: it is taken from Erdős' first published paper, which appeared in 1932, when Erdős was 19.

Bertrand's postulate.
For every $n \geq 1$, there is some prime number p with $n < p \leq 2n$.

Proof. We will estimate the size of the binomial coefficient $\binom{2n}{n}$ carefully enough to see that if it didn't have any prime factors in the range $n < p \leq 2n$, then it would be "too small." Our argument is in five steps.

(1) We first prove Bertrand's postulate for $n < 4000$. For this one does not need to check 4000 cases: it suffices (this is "Landau's trick") to check that

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

is a sequence of prime numbers, where each is smaller than twice the previous one. Hence every interval $\{y : n < y \leq 2n\}$, with $n \leq 4000$, contains one of these 14 primes.

(2) Next we prove that

$$\prod_{p \le x} p \;\le\; 4^{x-1} \qquad \text{for all real } x \ge 2, \tag{1}$$

where our notation — here and in the following — is meant to imply that the product is taken over all *prime* numbers $p \le x$. The proof that we present for this fact uses induction on the number of these primes. It is not from Erdős' original paper, but it is also due to Erdős (see the margin), and it is a true Book Proof. First we note that if q is the largest prime with $q \le x$, then

$$\prod_{p \le x} p = \prod_{p \le q} p \qquad \text{and} \qquad 4^{q-1} \le 4^{x-1}.$$

Thus it suffices to check (1) for the case where $x = q$ is a prime number.

For $q = 2$ we get "$2 \leq 4$," we proceed to consider odd primes $q = 2m + 1$. (Here we may assume, by induction, that (1) is valid for all integers x in the set $\{2, 3, \ldots, 2m\}$.) For $q = 2m + 1$ we split the product and compute

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

All the pieces of this "one-line computation" are easy to see. In fact,

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

holds by induction.

The inequality

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

follows from the observation that $\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$ is an integer, where the primes that we consider all are factors of the numerator $(2m+1)!$, but not of the denominator $m!(m+1)!$. Finally

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

holds since

$$\binom{2m+1}{m} \text{ and } \binom{2m+1}{m+1}$$

are two (equal!) summands that appear in

Legendre's theorem

The number $n!$ contains the prime factor p exactly

$$\sum_{k\geq 1}\left\lfloor \frac{n}{p^k}\right\rfloor$$

times.

■ **Proof.** Exactly $\left\lfloor \frac{n}{p}\right\rfloor$ of the factors of $n! = 1\cdot 2\cdot 3\cdots n$ are divisible by p, which accounts for $\left\lfloor \frac{n}{p}\right\rfloor$ p-factors. Next, $\left\lfloor \frac{n}{p^2}\right\rfloor$ of the factors of $n!$ are even divisible by p^2, which accounts for the next $\left\lfloor \frac{n}{p^2}\right\rfloor$ prime factors p of $n!$, etc. □

(3) From Legendre's theorem (see the box) we get that $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ contains the prime factor p exactly

$$\sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right)$$

times. Here each summand is at most 1, since it satisfies

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

and it is an integer. Furthermore the summands vanish whenever $p^k > 2n$. Thus $\binom{2n}{n}$ contains p exactly

$$\sum_{k\geq 1}\left(\left\lfloor \frac{2n}{p^k}\right\rfloor - 2\left\lfloor \frac{n}{p^k}\right\rfloor\right) \;\leq\; \max\{r : p^r \leq 2n\}$$

times. Hence the largest power of p that divides $\binom{2n}{n}$ is not larger than $2n$. In particular, primes $p > \sqrt{2n}$ appear at most once in $\binom{2n}{n}$.

Furthermore — and this, according to Erdős, is the key fact for his proof — primes p that satisfy $\frac{2}{3}n < p \leq n$ do not divide $\binom{2n}{n}$ at all! Indeed, $3p > 2n$ implies (for $n \geq 3$, and hence $p \geq 3$) that p and $2p$ are the only multiples of p that appear as factors in the numerator of $\frac{(2n)!}{n!n!}$, while we get two p-factors in the denominator.

Examples such as
$\binom{26}{13} = 2^3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19 \cdot 23$
$\binom{28}{14} = 2^3 \cdot 3^3 \cdot 5^2 \cdot 17 \cdot 19 \cdot 23$
$\binom{30}{15} = 2^4 \cdot 3^2 \cdot 5 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
illustrate that "very small" prime factors $p < \sqrt{2n}$ can appear as higher powers in $\binom{2n}{n}$, "small" primes with $\sqrt{2n} < p \leq \frac{2}{3}n$ appear at most once, while factors in the gap with $\frac{2}{3}n < p \leq n$ don't appear at all.

(4) Now we are ready to estimate $\binom{2n}{n}$. For $n \geq 3$, using an estimate from page 12 for the lower bound, we get

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

and thus, since there are not more than $\sqrt{2n}$ primes $p \leq \sqrt{2n}$,

$$4^n \leq (2n)^{1+\sqrt{2n}} \cdot \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p \quad \text{for} \quad n \geq 3. \qquad (2)$$

(5) Assume now that there is no prime p with $n < p \leq 2n$, so the second product in (2) is 1. Substituting (1) into (2) we get

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

or

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

which is false for n large enough! In fact, using $a + 1 < 2^a$ (which holds for all $a \geq 2$, by induction) we get

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\lfloor \sqrt[6]{2n} \rfloor + 1\right)^6 < 2^{6\left\lfloor \sqrt[6]{2n} \right\rfloor} \leq 2^{6\sqrt[6]{2n}}, \tag{4}$$

and thus for $n \geq 50$ (and hence $18 < 2\sqrt{2n}$) we obtain from (3) and (4)

$$2^{2n} \leq (2n)^{3\left(1+\sqrt{2n}\right)} < 2^{\sqrt[6]{2n}\left(18+18\sqrt{2n}\right)} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

This implies $(2n)^{1/3} < 20$, and thus $n < 4000$. □

Zbiór $\mathbb{Z}$ liczb całkowitych z wyróżnionymi elementami 0,1 oraz z działaniami dodawania i mnożenia liczb naturalnych jest pierścieniem: dla dowolnych liczb całkowitych x, y, z

$$x + y = y + x \qquad \textit{(przemienność dodawania)}$$
$$x + (y + z) = (x + y) + z \qquad \textit{(łączność dodawania)}$$
$$0 + x = x + 0 = x \qquad \textit{(element neutralny dodawania)}$$
$$x + (-x) = -x + x = 0 \qquad \textit{(element przeciwny dla dodawania)}$$
$$x \cdot y = y \cdot x \qquad \textit{(przemienność mnożenia)}$$
$$x \cdot (y \cdot z) = (x \cdot y) \cdot z \qquad \textit{(łączność mnożenia)}$$
$$1 \cdot x = x \cdot 1 = x \qquad \textit{(element neutralny mnożenia)}$$
$$x \cdot (y + z) = x \cdot y + x \cdot z \qquad \textit{(rozdzielność mnożenia względem dodawania)}$$

Liczby całkowite.

Dla każdych dwóch liczb całkowitych a, b jeśli tylko $b \neq 0$, to istnieją jednoznacznie określone liczby całkowite i oraz r spełniające warunek:

$$a = i \cdot b + r \qquad i \qquad 0 \leq r < |b| .$$

Podzielność liczb całkowitych. Jeśli resztą z dzielenia liczby całkowitej a przez b jest 0, to mówimy, że a *dzieli się przez* b, albo że b *jest dzielnikiem* a, albo że a *jest wielokrotnością* b. Zapisujemy to symbolami następująco: $b|a$. Podzielność liczb całkowitych jest relacją.

DEFINICJA *Dla liczb całkowitych* a, b :

$b|a$ *wtedy i tylko wtedy, gdy istnieje taka liczba całkowita* i, *że* $a = i \cdot b$.

$$b|a \Leftrightarrow \exists_{i \in \mathbb{Z}} \left[a = i \cdot b\right].$$

TWIERDZENIE *Dla dowolnych liczb całkowitych* a, b, c*:*

$a|a$ *(zwrotność relacji podzielności)*

$(a|b \wedge b|c) \Rightarrow a|c$ *(przechodniość relacji podzielności)*

$(a|b \wedge b|a) \Rightarrow (a = b \vee a = -b)$ *(częściowa antysymetria)*

$a|0$;

$1|a$;

$a|b \Rightarrow a|bc$;

$(a|b \wedge a|c) \Rightarrow a|(b + c)$.

Reszty i kongruencje. Załóżmy, że jest ustalona liczba całkowita n, $n > 1$ i interesuje nas podzielność przez n, albo ogólniej i dokładniej: reszty z dzielenia przez n. W takiej sytuacji liczbę n będziemy nazywać modułem (w domyśle: podzielności).

Określimy funkcję $r_n : \mathbb{Z} \longrightarrow \{0, 1, 2, ..., n-1\}$:

$r_n(a)$ jest resztą z dzielenia liczby a przez n

$$r_n(a) = a - n \cdot \left\lfloor \frac{a}{n} \right\rfloor .$$

Dla danego modułu n zbiór $\{0, 1, 2, ..., n-1\}$
możliwych reszt z dzielenia przez n będziemy oznaczać symbolem $\mathbb{Z}_n$:

$$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}.$$

DEFINICJA $x = r_n(a) \quad \Leftrightarrow \quad (x \in \mathbb{Z}_n \wedge n|(a-x)).$

TWIERDZENIE

(1) $n|(a-b) \Leftrightarrow r_n(a) = r_n(b)$;
(2) $r_n(r_n(a)) = r_n(a)$;
(3) $r_n(a+b) = r_n(r_n(a) + r_n(b))$;
(4) $r_n(a \cdot b) = r_n(r_n(a) \cdot r_n(b))$.

DEFINICJA *Dla dowolnych liczb całkowitych* a, b: $\quad a \equiv b (\mathrm{mod}\, n) \;\Leftrightarrow\; n|(a-b).$

TWIERDZENIE *Dla dowolnych liczb całkowitych* a, b, c, d:

a) $a \equiv b (\mathrm{mod}\, n) \Leftrightarrow r_n(a) = r_n(b)$;

b) $a \equiv a (\mathrm{mod}\, n)$; *(zwrotność relacji kongruencji)*

c) $a \equiv b (\mathrm{mod}\, n) \Rightarrow\; b \equiv a (\mathrm{mod}\, n)$; *(symetryczność relacji kongruencji)*

d) $(a \equiv b (\mathrm{mod}\, n) \wedge b \equiv c (\mathrm{mod}\, n)) \Rightarrow\; a \equiv c (\mathrm{mod}\, n)$; *(przechodniość kongruencji)*

e) $a \equiv b (\mathrm{mod}\, n) \Rightarrow\; a + c \equiv b + c (\mathrm{mod}\, n)$;

f) $(a \equiv b (\mathrm{mod}\, n) \wedge c \equiv d (\mathrm{mod}\, n)) \Rightarrow\; a + c \equiv b + d (\mathrm{mod}\, n)$;

g) $a \equiv b (\mathrm{mod}\, n) \Rightarrow\; a \cdot c \equiv b \cdot c (\mathrm{mod}\, n)$;

h) $(a \equiv b (\mathrm{mod}\, n) \wedge c \equiv d (\mathrm{mod}\, n)) \Rightarrow\; a \cdot c \equiv b \cdot d (\mathrm{mod}\, n)$.

DEFINICJA *Niech n będzie liczbą naturalną, a $a_1, a_2, \ldots, a_n$ niech będą liczbami całkowitymi.*

$$(a_1, a_2, \ldots, a_n) = \left\{ \sum_{i=1}^{n} a_i x_i : x_1, x_2, \ldots, x_n \in \mathbb{Z} \right\}.$$

W szczególności $(a) = \{y \in \mathbb{Z} : a \mid y\}$ w przypadku $n = 1$. Na przykład $(1) = (-1) = \mathbb{Z}$.

LEMAT *Zbiór $(a_1, a_2, \ldots, a_n)$ zawiera każdą z liczb $a_1, a_2, \ldots, a_n$, jest zamknięty ze względu na dodawanie i wraz z każdą liczbą zawiera jej wszystkie wielokrotności.*

LEMAT *Dla każdych dwóch liczb całkowitych $a, b \in \mathbb{Z}$ istnieje taka liczba naturalna d, że $(a, b) = (d)$.*

DEFINICJA *Wspólnym dzielnikiem liczb całkowitych a, b nazywamy każdą taką liczbę całkowitą x, która jest dzielnikiem a i jednocześnie jest dzielnikiem liczby b. Największym wspólnym dzielnikiem (a, b) liczb całkowitych a, b nazywamy liczbę naturalną d spełniającą warunki:*

$$d|a \wedge d|b$$

$$(x \mid a \wedge x \mid b) \Rightarrow x \mid d.$$

LEMAT *Dla dowolnych liczb całkowitych a, b jeśli $(a, b) = (d)$ i $d > 0$, to $d = (a, b)$.*

DEFINICJA *Dwie liczby całkowite a i b są względnie pierwsze $\Leftrightarrow$ jedynymi wspólnymi dzielnikami liczb a i b są liczby 1 i -1.*

Innymi słowy liczby całkowite a i b są względnie pierwsze $\Leftrightarrow (a, b) = 1$

TWIERDZENIE *Załóżmy, że $a \mid bc$ i $(a, b) = 1$. Wtedy $a \mid c$.*

WNIOSEK *Jeśli p jest liczbą pierwszą, to* $v_p(ab) = v_p(a) + v_p(b)$.

Własności wykładnika p-adycznego.

przyjmujemy następujące umowy:

dla każdej liczby całkowitej x zachodzi nierówność $x < \infty$,
dla każdej liczby całkowitej x zachodzą równości $x + \infty = \infty + x = \infty$,
$\infty + \infty = \infty$,
dla każdej liczby naturalnej n zachodzą równości $n \cdot \infty = \infty \cdot n = \infty$.

TWIERDZENIE *Dla każdej liczby pierwszej p i dowolnych liczb całkowitych a, b*

a) $v_p(a) \geq 0$;
b) $v_p(a) = \infty \Leftrightarrow a = 0$;
c) $v_p(a) = 0 \Leftrightarrow p \nmid a$;
d) $v_p(ab) = v_p(a) + v_p(b)$ *(pełna addytywność);*
e) $a|b \Leftrightarrow \underset{p \in \mathbf{P}}{\forall} [v_p(a) \leq v_p(b)]$;
f) $v_p(a+b) \geq \min(v_p(a), v_p(b))$;
g) $v_p(a+b) > \min(v_p(a), v_p(b)) \Rightarrow v_p(a) = v_p(b)$;
h) dla dowolnych liczb naturalnych n, m

$$v_p(a^n) = n v_p(a) \ \ i$$

$$\underset{x \in \mathbb{Z}}{\exists} [x^n = m] \Leftrightarrow \underset{p \in \mathbf{P}}{\forall} [n | v_p(m)] .$$

DEFINICJA *Najmniejszą wspólną wielokrotnością liczb całkowitych a, b nazywamy liczbę naturalną $w = NWW(a, b)$ spełniającą warunki*

$$a|w \wedge b|w$$
$$(a|x \wedge b|x) \Rightarrow w|x.$$

TWIERDZENIE *Dla każdej liczby pierwszej p*

$$\begin{aligned} v_p(NWD(a,b)) &= \min(v_p(a), v_p(b)), \\ v_p(NWW(a,b)) &= \max(v_p(a), v_p(b)). \end{aligned}$$

To twierdzenie mozna sformułować w postaci wzorów:

$$\begin{aligned} NWD(a,b) &= \prod_{p\in\mathbf{P}} p^{\min(v_p(a),v_p(b))} \\ NWW(a,b) &= \prod_{p\in\mathbf{P}} p^{\max(v_p(a),v_p(b))}, \end{aligned}$$

które są użyteczne, jeśli znamy rozkłady liczb a i b na czynniki pierwsze:

$$\begin{aligned} 60984 &= 2^3 \cdot 3^2 \cdot 7 \cdot 11^2 \\ 714285 &= 3^3 \cdot 5 \cdot 11 \cdot 13 \cdot 37 \end{aligned}$$

$NWD(60984, 714285) =$

$$\begin{aligned} &= 2^{\min(3,0)} \cdot 3^{\min(2,3)} \cdot 5^{\min(0,1)} \cdot 7^{\min(1,0)} \cdot 11^{\min(2,1)} \cdot 13^{\min(0,1)} \cdot 37^{\min(0,1)} \\ &= 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^1 \cdot 13^0 \cdot 37^0 \\ &= 3^2 \cdot 11 = 99. \end{aligned}$$

albo krócej: $NWD(60984, 714285) = 3^{\min(2,3)} \cdot 11^{\min(2,1)} = 3^2 \cdot 11 = 99$;

$NWW(60984, 714285) =$

$$\begin{aligned} &= 2^{\max(3,0)} \cdot 3^{\max(2,3)} \cdot 5^{\max(0,1)} \cdot 7^{\max(1,0)} \cdot 11^{\max(2,1)} \cdot 13^{\max(0,1)} \cdot 37^{\max(0,1)} \\ &= 2^3 \cdot 3^3 \cdot 5^1 \cdot 7^1 \cdot 11^2 \cdot 13^1 \cdot 37^1 \\ &= 439999560. \end{aligned}$$

UWAGA $\min(x,y) + \max(x,y) = x + y$ *(tzn. dla danych liczb* x, y *suma mniejszej z nich i większej z nich jest sumą danych liczb), co oznacza, że* $NWW(a,b) \cdot NWD(a,b) = ab$. *Aby obliczać najmniejszą wspólną wielokrotność dwóch liczb, wystarczy umieć obliczać najwiekszy wspólny dzielnik i iloczyn.*

TWIERDZENIE *Dla każdej liczby naturalnej n*

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

Rozwiązywanie kongruencji.

TWIERDZENIE *Niech m będzie liczbą naturalną większą od 1. Dla dowolnych liczb całkowitych a, b, c, d:*

$a)$ $a \equiv a (\mathrm{mod}\, m)$; *(zwrotność relacji kongruencji)*

$b)$ $a \equiv b (\mathrm{mod}\, m) \Rightarrow b \equiv a (\mathrm{mod}\, m)$; *(symetryczność relacji kongruencji)*

$c)$ $(a \equiv b (\mathrm{mod}\, m) \wedge b \equiv c (\mathrm{mod}\, m)) \Rightarrow a \equiv c (\mathrm{mod}\, m)$; *(przechodniość kongruencji)*

$d)$ $a \equiv b (\mathrm{mod}\, m) \Rightarrow a + c \equiv b + c (\mathrm{mod}\, m)$;

$e)$ $(a \equiv b (\mathrm{mod}\, m) \wedge c \equiv d (\mathrm{mod}\, m)) \Rightarrow a + c \equiv b + d (\mathrm{mod}\, m)$;

$f)$ $a \equiv b (\mathrm{mod}\, m) \Rightarrow a \cdot c \equiv b \cdot c (\mathrm{mod}\, m)$;

$g)$ $c \neq 0 \Rightarrow a \equiv b (\mathrm{mod}\, m) \Leftrightarrow a \cdot c \equiv b \cdot c (\mathrm{mod}\, c \cdot m)$;

$h)$ $(a \equiv b (\mathrm{mod}\, m) \wedge c \equiv d (\mathrm{mod}\, m)) \Rightarrow a \cdot c \equiv b \cdot d (\mathrm{mod}\, m)$.

TWIERDZENIE *Dla dowolnej liczby naturalnej $m > 1$:*

a) dla dowolnej liczby naturalnej k i dowolnych liczb całkowitych a, b

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow a^k \equiv b^k (\mathrm{mod}\, m);$$

b) dla dowolnego wielomianu $f(X)$ zmiennej X o współczynnikach całkowitych

$$a \equiv b (\mathrm{mod}\, m) \Rightarrow f(a) \equiv f(b) (\mathrm{mod}\, m);$$

c) dla dowolnej liczby naturalnej n i dla dowolnego wielomianu $f(X_1, X_2, \ldots, X_n)$ i dowolnych układów liczb całkowitych $(a_1, a_2, \ldots, a_n)$ i $(b_1, b_2, \ldots, b_n)$

$$\underset{i \in \{1,2,\ldots,n\}}{\forall} [a_i \equiv b_i (\mathrm{mod}\, m)] \Rightarrow f(a_1, a_2, \ldots, a_n) \equiv f(b_1, b_2, \ldots, b_n) (\mathrm{mod}\, m).$$

DEFINICJA 10.1. *Rozwiązania* $(a_1, a_2, \ldots, a_n)$ *i* $(b_1, b_2, \ldots, b_n)$ *kongruencji*

$$f(X_1, X_2, \ldots, X_n) \equiv 0 (\mathrm{mod}\, m)$$

są równoważne, gdy $\underset{i \in \{1,2,\ldots,n\}}{\forall} [a_i \equiv b_i (\mathrm{mod}\, m)]$.

PRZYKŁAD 6. *Sprawdzenie wszystkich możliwości dowodzi, że jedynymi mniejszymi od* 15 *rozwiązaniami kongruencji*

$$6X \equiv 3 (\mathrm{mod}\, 15)$$

są $3, 8$ *i* 13. *Rozwiązanie* 18 *jest równoważne rozwiązaniu* 3.

TWIERDZENIE 11.1. *Niech m będzie liczbą naturalną większą od 1. Dla dowlnych liczb całkowitych a, b oznaczmy $d = NWD(a, m)$. Wtedy*
a) kongruencja $ax \equiv b (\mathrm{mod}\, m)$ ma rozwiązanie $\Leftrightarrow d|b$;
b) jeśli $d|b$ to kongruencja $ax \equiv b (\mathrm{mod}\, m)$ ma dokładnie d rozwiązań;
c) jeśli c jest rozwiązaniem kongruencji $ax \equiv b (\mathrm{mod}\, m)$, czyli jeśli $ac \equiv b (\mathrm{mod}\, m)$, to wszystkimi rozwiązaniami kongruencji $ax \equiv b (\mathrm{mod}\, m)$ są

$$c, c + \frac{m}{d}, c + \frac{2m}{d}, \ldots, c + \frac{(d-1)m}{d}.$$

Wniosek 11.2. $NWD(a,m) = 1 \Rightarrow$ *kongruencja* $ax \equiv b(\mathrm{mod}\, m)$ *ma dokładnie jedno rozwiązanie.*

Wniosek 11.3. *Dla liczby pierwszej* p *i liczby całkowitej* a *nie dzielącej się przez* p *kongruencja* $ax \equiv b(\mathrm{mod}\, p)$ *ma dokładnie jedno rozwiązanie.*

Wniosek 11.4. $\underset{x\in\mathbb{Z}_m}{\exists}\,[ax = 1] \Leftrightarrow NWD(a,m) = 1.$

Wniosek 11.5. *Pierścień* $\mathbb{Z}_m$ *jest ciałem* $\Leftrightarrow$ m *jest liczbą pierwszą.*

Definicja 11.1. *Element* a *pierścienia* R *nazywamy elementem odwracalnym (albo jednością) gdy* a *ma element odwrotny w pierścieniu* R.
Zbiór wszystkich elementów odwracalnych pierścienia R *oznaczamy symbolem* R^* *albo* $U(R)$.

Przykład 9. $a \in R^* \Leftrightarrow a|1 \Leftrightarrow \underset{b\in R}{\forall}\,[a|b] \Leftrightarrow (a) = R.$

Przykład 10. *Pierścień* R *jest ciałem* $\Leftrightarrow R^* = R \setminus \{0\}.$

Przykład 11. $\mathbb{Z}^* = \{1, -1\}$.

Przykład 12. $R[X]^* = R^*$.

Przykład 13. *Wniosek 11.4 oznacza, że*

$$\mathbb{Z}_m^* = \{a \in \{0, 1, 2, \ldots, m-1\} : NWD(a, m) = 1\}.$$

Warto zauważyć, że dla dowolnego pierścienia R zbiór R^* z wyróżnionym elementem 1 i działaniem mnożenia jest grupą. W szczególności iloczyn elementów odwracalnych pierścienia jest elementem odwracalnym: $(ab)^{-1} = b^{-1}a^{-1}$ bo

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1.$$

Liczba elementów odwracalnych pierścienia $\mathbb{Z}_m$ była badana na długo przed pojawieniem się pojęcia pierścienia.

Definicja 11.2. *Funkcja Eulera* $\varphi : \mathbb{N} \to \mathbb{N}$ *określona jest nastepująco:*

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(n) &= |\mathbb{Z}_n^*| \ \ dla\ n > 1. \end{aligned}$$

Równoważne sformułowanie:

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(n) &= \text{liczba liczb naturalnych mniejszych od } n \text{ i względnie pierwszych z } n \text{ dla } n > 1. \end{aligned}$$

Przykład 14. *Jeśli* p *jest liczbą pierwszą, to* $\varphi(p) = p - 1$.

PRZYKŁAD 15. *Jeśli m jest liczbą złożoną, to $\varphi(m) < m - 1$.*

PRZYKŁAD 16. *Jeśli p jest liczbą pierwszą, a k jest liczbą naturalną, to* $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$:
$NWD(a, p^k) > 1 \Leftrightarrow p|a$; *sposród liczb* $0, 1, 2, \ldots, p^k - 1$ *przez* p *dzielą się tylko*

$$0 \cdot p, 1 \cdot p, 2 \cdot p, \ldots, (p^{k-1} - 1)p$$

i jest ich p^{k-1}. *Pozostałe* $p^k - p^{k-1}$ *liczb nie dzieli się przez* p, *wiec są one względnie pierwsze z liczbą* p^k.

TWIERDZENIE 11.6 (twierdzenie Eulera).

$$NWD(a,m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m).$$

DOWÓD. Z założenia wynika, że $a \in \mathbb{Z}_m^*$. Ponumerujmy elementy grupy $\mathbb{Z}_m^*$:

$$\mathbb{Z}_m^* = \{b_1, b_2, \ldots, b_{\varphi(m)}\}.$$

Wszystkie wyrazy ciągu $(ab_1, ab_2, \ldots, ab_{\varphi(m)})$ po pierwsze są elementami grupy $\mathbb{Z}_m^*$, a po drugie są parami różne: jeśli pomnożyć równość

$$ab_i = ab_j$$

stronami przez a^{-1}, to okaże się, że $b_i = b_j$, więc $i = j$. Każdy element odwracalny występuje w tym ciągu: $b_i = a(a^{-1}b_i)$, a $a^{-1}b_i$ jest elementem odwracalnym, więc musi być jednym z elementów b_j. Wobec tego ciąg $(ab_1, ab_2, \ldots, ab_{\varphi(m)})$ jest permutacją ciągu $(b_1, b_2, \ldots, b_{\varphi(m)})$. Wynika z tego równość iloczynów

$$ab_1 ab_2 \cdots ab_{\varphi(m)} = b_1 b_2 \cdots b_{\varphi(m)},$$

bo te iloczyny różnią się najwyżej kolejnością czynników, a więc i równość

$$a^{\varphi(m)} b_1 b_2 \cdots b_{\varphi(m)} = b_1 b_2 \cdots b_{\varphi(m)}.$$

Po pomnożeniu stronami przez element odwrotny do $b_1 b_2 \cdots b_{\varphi(m)}$ uzyskujemy jako wniosek równość $a^{\varphi(m)} = 1$.

TWIERDZENIE 11.7 (małe twierdzenie Fermata). *Dla dowolnej liczby pierwszej p i dowolnej liczby całkowitej a*
a) $p \nmid a \Rightarrow a^{p-1} \equiv 1 (\mathrm{mod}\, p)$;
b) $a^p \equiv a (\mathrm{mod}\, p)$.

Układy kongruencji, twierdzenie chińskie o resztach.

Jeden z najważniejszych faktów, dotyczących układów kongruencji względem różnych modułów, mający szereg uogólnień, był systematycznie używany w podręczniku matematyki pióra Suń Czy (w angielskiej transkrypcji: Sun Tsy) z III w. ne. I samo twierdzenie, i jego uogólnienia noszą nazwę chińskiego twierdzenia o resztach, co jest wyraźną przesłanką na rzecz wniosku, że fakt, iż kultura europejska jest podsumowaniem osiągnięć całego swiata i pochodzących z wielu tysiacleci, jest znany od dawna, choć ignorowany. Samo twierdzenie pojawia się (w postaci opisu metody rozwiązywania zadań) w dziele *Gamita* Aryabhaty I (476 - ok. 550). Metodę opisuje również Brahmagupta (598 - ok. 660). W Europie dopiero astronom Bianchini szukał liczb, które przy dzieleniu przez 17, 13, 10 dają odpowiednio reszty 15, 11, 3. To zadanie rozwiązał mu Regimontanus (Johannes Miller, 16 VI 1736 - 6 VII 1476): wykazał, że najmniejszą taką liczbą naturalną jest 1103 i że każde inne rozwiązanie jest sumą 1103 i wielokrotności liczby $17 \cdot 13 \cdot 10 = 2210$

Sformułowanie twierdzenia poprzedzimy udowodnieniem dwóch prostych lematów.

LEMAT 12.1. *Dla dowolnych liczb całkowitych $m, a_1, a_2, \ldots, a_l$ jeśli każda z liczb $a_1, a_2, \ldots, a_l$ jest względnie pierwsza z m, to ich iloczyn $a_1 a_2 \cdots a_l$ jest względnie pierwszy z m.*

DOWÓD. Należy wykazać, że $NWD(a_1 a_2 \cdots a_l, m) = 1$. Gdyby jakaś liczba pierwsza p dzieliła ten największy wspólny dzielnik, to dzieliłaby liczbę m oraz iloczyn $a_1 a_2 \cdots a_l$. Dzieląc iloczyn, musiałaby dzielić któryś z jego czynników, np. a_i. Ale wtedy dzieliłaby $NWD(a_i, m)$, wbrew założeniu, że a_i i m są względnie pierwsze. ∎

LEMAT 12.2. *Dla dowolnych liczb całkowitych $n, a_1, a_2, \ldots, a_t$ jeśli $a_1, a_2, \ldots, a_t$ są parami względnie pierwsze, oraz są dzielnikami liczby n, to ich iloczyn $a_1 a_2 \cdots a_t$ jest dzielnikiem liczby n.*

DOWÓD. Indukcja względem t. Dla $t = 1$ należy dowieść implikacji $a_1|n \Rightarrow a_1|n$, która jest logicznie prawdziwa. Załóżmy indukcyjnie, że dowodzone twierdzenie jest prawdziwe dla $t = k$ i załóżmy, że $a_1, a_2, \ldots, a_{k+1}$ są parami względnie pierwszymi dzielnikami liczby n. Na mocy poprzedniego lematu z tego, że a_{k+1} jest względnie pierwsze z każdą z liczb $a_1, a_2, \ldots, a_k$ wynika, że względnie pierwsze są a_{k+1} i iloczyn $a_1 a_2 \cdots a_k$. Wobec tego istnieją liczby całkowite r, s takie, że

$$ra_{k+1} + sa_1 a_2 \cdots a_k = 1.$$

Pomnożenie tej równości stronami przez n daje w wyniku równość

$$ra_{k+1}n + sa_1 a_2 \cdots a_k n = n.$$

Z założenia indukcyjnego wynika, że $a_1 a_2 \cdots a_k | n$; zatem $a_1 a_2 \cdots a_k a_{k+1} | ra_{k+1}n$. Z założenia $a_{k+1}|n$ wynika podzielność $a_1 a_2 \cdots a_k a_{k+1} | sa_1 a_2 \cdots a_k n$. Iloczyn $a_1 a_2 \cdots a_k a_{k+1}$ dzieli oba składniki po lewej stronie równości, dzieli więc ich sumę, czyli dzieli liczbę n. ∎

TWIERDZENIE 12.3 (twierdzenie chińskie o resztach). *Jeśli $m_1, m_2, \ldots, m_t$ są parami względnie pierwszymi liczbami całkowitymi, a $b_1, b_2, \ldots, b_t$ dowolnymi liczbami całkowitymi, a*

$$U : \begin{cases} x \equiv b_1 (\mathrm{mod}\, m_1) \\ x \equiv b_2 (\mathrm{mod}\, m_2) \\ \qquad \vdots \\ x \equiv b_t (\mathrm{mod}\, m_t) \end{cases}$$

jest układem kongruencji, to
a) układ U zawsze ma rozwiązanie $x \in \mathbb{Z}$;
b) każde dwa rozwiązania układu U przystają do siebie modulo $m_1 m_2 \cdots m_t$.

Dowód. a) Oznaczmy $m = m_1 m_2 \cdots m_t$ i $n_i = \frac{m}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_t$. To, że czynniki tego iloczynu są względnie pierwsze z m_i - na podstawie pierwszego lematu - oznacza, że $NWD(m_i, n_i) = 1$, a zatem istnieją (dla każdego i) liczby całkowite r_i, s_i takie, że $r_i m_i + s_i n_i = 1$. Oznaczmy

$$e_i = s_i n_i = 1 - r_i m_i.$$

Dla dowolnego numeru j są dwie możliwości: albo $j \neq i$, zatem $m_j | n_i$ i $m_j | s_i n_i = e_i$, albo $j = i$ i $e_i = 1 - r_i m_i \equiv 1 (\mathrm{mod}\, m_i)$. Niech

$$x = \sum_{k=1}^{t} b_k e_k.$$

Dla dowolnego numeru i

$$\begin{aligned} x &\equiv \sum_{k=1}^{t} b_k e_k \equiv \sum_{k=1}^{i-1} b_k e_k + b_i e_i + \sum_{k=i+1}^{t} b_k e_k \\ &\equiv \sum_{k=1}^{i-1} b_k \cdot 0 + b_i \cdot 1 + \sum_{k=i+1}^{t} b_k \cdot 0 \equiv b_i (\mathrm{mod}\, m_i). \end{aligned}$$

Zatem $x = \sum_{k=1}^{t} b_k e_k$ jest rozwiązaniem układu U.

b) Niech x i y będą dwoma rozwiązaniami układu kongruencji U. Wtedy dla każdego numeru i

$$m_i | x - y.$$

Liczby m_i są parami względnie pierwsze, więc - na mocy drugiego lematu - ich iloczyn m dzieli $x - y$. ∎

$$NWD(n,m) = 1 \Rightarrow \varphi(nm) = \varphi(n)\varphi(m).$$

Jeśli $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_l^{a_l}$ *jest rozkładem liczby* n *na czynniki pierwsze, to*

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_l}).$$

Rozmieszczenie liczb pierwszych.

Już Euklides wykazał, że jest nieskończenie wiele liczb pierwszych.

TWIERDZENIE 13.1. *Zbiór* $\mathbf{P}$ *wszystkich liczb pierwszych jest zbiorem nieskończonym.*

DOWÓD. Niech $A = \{p_1, p_2, \ldots, p_n\}$ będzie dowolnym niepustym, skończonym zbiorem liczb pierwszych. Wtedy istnieje liczba pierwsza q nie należąca do tego zbioru:
niech $m = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1$. Każda z liczb $p_1, p_2, ..., p_n$ jest większa lub równa 2, więc $m > 1$ - liczba m nie może być ani zerem, ani jedynką. W takim razie liczba m ma rozkład na czynniki pierwsze, w którym występuje conajmniej jedna liczba pierwsza q. Liczba q jest pierwsza i $q \mid m$. W takim razie liczba q nie może być elementem zbioru A, bo dla każdego numeru i

$$m \equiv 1 (\mathrm{mod}\, p_i) \text{ i } m \equiv 0 (\mathrm{mod}\, q).$$

Gdyby zbiór $\mathbf{P}$ wszystkich liczb pierwszych był skończony, to powyższa konstrukcja pozwalałaby zbudować liczbę pierwszą, która do niego nie należy. ∎

TWIERDZENIE 13.2. *Dla każdej liczby naturalnej k istnieje ciąg kolejnych liczb naturalnych długości k, którego wszystkie wyrazy są liczbami złożonymi.*

DOWÓD. Np. ciąg $(k+1)!+2, (k+1)!+3, \ldots, (k+1)!+(k+1)$. ∎

TWIERDZENIE 13.3. *Szereg* $\sum_{n=1}^{\infty} \frac{1}{p_n}$ *odwrotności liczb pierwszych jest rozbieżny.*

C. F. Gauss otrzymał w prezencie na piętnaste urodziny tablice matematyczne. Analizując zamieszczoną w nich tablicę liczb pierwszych zauważył pewną regularność, która skłoniła go do określenia następującej funkcji:

DEFINICJA 13.1.

$$\pi(x) = \textit{liczba liczb pierwszych} \leq x \textit{ dla } x \in \mathbb{R}$$

Rozumowanie Gaussa ilustruje tabelka:

x	$\pi(x)$	$\frac{x}{\pi(x)}$	przyrost
10	4	2,5	2,5
100	25	4,0	1,5
1000	168	6,0	2,0
10 000	1 229	8,1	2,1
100 000	9 592	10,4	2,3
1 000 000	78 498	12,7	2,3
10 000 000	664 579	15,0	2,3
100 000 000	5 761 455	17,4	2,4
1000 000 000	50 847 534	19,7	2,3
10 000 000 000	455 052 512	22,0	2,3
⋮	⋮	⋮	⋮

W tabeli widać, że ze wzrostem wartości x do kolejnej potęgi dziesiątki iloraz $\frac{x}{\pi(x)}$ wzrasta o około $2,3$. Co to za tajemnicza liczba $2,3$? Zauważmy, że $\ln 10 = 2,3$, zatem $\ln 10^n = 2,3 \cdot n$ czyli jeśli x rośnie dziesięciokrotnie, to $\ln x$ rośnie o liczbę $2,3$. Niewielki błąd względny

$$\frac{\left(\frac{10x}{\pi(10x)} - \frac{x}{\pi(x)}\right) - (\ln(10x) - \ln x)}{10x}$$

przy zastąpieniu przyrostów funkcji $\frac{x}{\pi(x)}$ przez przyrosty funkcji $\ln x$ skłonił Gaussa do wysunięcia przypuszczenia, że

$$\frac{x}{\pi(x)} \approx \ln x \text{ czyli } \frac{x}{\ln x} \approx \pi(x)$$

gdzie przybliżona równość oznacza równość asymptotyczną, tzn. że błąd względny tego przybliżenia dąży do zera ze wzrostem x. Twierdzenie to zostało sformułowane po raz pierwszy i sprawdzone do $x = 3\ 000\ 000$ (ręcznie!) przez Gaussa, o czym świadczy jego list do matematyka i astronoma J. F. Encke z 1793 roku.

TWIERDZENIE 13.4 (Twierdzenie o liczbach pierwszych).

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

Twierdzenie o liczbach pierwszych zostało udowodnione w 1896 roku (niezależnie) przez J. Hadamarda i C. de la Vallée-Poussina.

TWIERDZENIE 13.5. *(P. L. Czebyszew) Istnieją liczby rzeczywiste* c_1 *i* $c_2 > 0$ *takie, że dla każdej liczby rzeczywistej* $x \geq 2$

$$c_2 \frac{x}{\ln x} < \pi(x) < c_1 \frac{x}{\ln x}.$$

Czebyszew udowodnił również, że $c_1 \leq 1,11$ i $c_2 \geq 0,89$.
Udowodnimy twierdzenie Czebyszewa dla nieco "gorszych" stałych $c_1 = 1,7$ i $c_2 = \frac{2}{3}$.

Z twierdzenia Czebyszewa wynika między innymi, że

$$\pi(2n) - \pi(n) > \frac{89}{100}\frac{2n}{\ln(2n)} - \frac{111}{100}\frac{n}{\ln n} > 0$$

dla dużych n. Dokładniej:

TWIERDZENIE 13.6 (Postulat Bertranda). *Dla $n > 1$ między n a $2n$ leży co najmniej jedna liczba pierwsza.*

Podobnie można udowodnić, że

Dla $n > 5$ między n a $2n$ leżą co najmniej dwie liczby pierwsze.

WNIOSEK 13.8. *Dla każdej liczby naturalnej l istnieje co najmniej sześć liczb pierwszych, mających l cyfr w dziesiętnym układzie pozycyjnym.*

DOWÓD. $10^l, 2 \cdot 10^l, 4 \cdot 10^l, 8 \cdot 10^l$ wszystkie mają po l cyfr i między każdymi dwoma leżą co najmniej dwie liczby pierwsze. ∎

Przybliżenie funkcji $\pi(x)$ dane przez Twierdzenie o liczbach pierwszych było wielokrotnie poprawiane. Na przykład Legendre zauważył (empirycznie), że lepsze przybliżenie ma postać

$$\pi(x) \approx \frac{x}{\ln x - 1,08366}.$$

Riemann podał dwa przybliżenia funkcji $\pi(x)$ nieco trudniejszymi do obliczenia funkcjami:

$$\begin{aligned} \mathrm{Li}(x) &= \int_2^x \frac{dt}{\ln t} \text{ (tzw. logarytm całkowy)} \\ R(x) &= \mathrm{Li}(x) - \sum_{n=2}^{\infty} \frac{\mathrm{Li}(\sqrt[n]{x})}{n} = 1 + \sum_{n=1}^{\infty} \frac{1}{n\zeta(n+1)} \frac{(\ln x)^n}{n!}. \end{aligned}$$

Mianowicie Riemann udowodnił, że

$$\begin{aligned} \pi(x) &\approx \mathrm{Li}(x) \\ \pi(x) &\approx R(x) \end{aligned}$$

x	$x/\ln(x)$	$\mathrm{Li}(x)$	$R(x)$	$\pi(x)$
100 000 000	5 428 681	5 762 209	5 761 552	5 761 455
200 000 000	10 463 628	11 079 974	11 079 090	11 078 937
300 000 000	15 369 409	16 253 409	16 252 355	16 252 325
400 000 000	20 194 905	21 337 378	21 336 185	21 336 326
500 000 000	24 962 408	26 356 832	26 355 517	26 355 867
600 000 000	29 684 688	31 326 045	31 324 622	31 324 703
700 000 000	34 370 013	36 254 242	36 252 719	36 252 931
800 000 000	39 024 157	41 147 862	41 146 248	41 146 179
900 000 000	43 651 379	46 011 648	46 009 949	46 009 215
1 000 000 000	48 254 942	50 849 234	50 847 455	50 847 534

Warto odnotować wynik Rossera i Schoenfelda z 1962 roku:

TWIERDZENIE 13.9. *Dla $x > 66$ zachodzą nierówności:*

$$\frac{x}{\ln x - \frac{1}{2}} < \pi(x) < \frac{x}{\ln x - \frac{3}{2}}.$$

Wyznaczanie liczb pierwszych. Już w starożytności znana była metoda wyznaczania liczb pierwszych znana obecnie jako *sito Erastotenesa*. Polega ona na tym, że z ciągu liczb naturalnych > 1 i mniejszych od M wykreślamy najpierw wszystkie liczby parzyste > 2, następnie wszystkie liczby podzielne przez 3 większe od 3, itd. Liczby, które pozostaną są liczbami pierwszymi mniejszymi od M. Metoda ta rozwinęła się w bogatą teorię określaną jako metody sita.

Poszukiwane były wzory dające liczby pierwsze jako wartości pewnych wyrażeń. Od razu należy powiedzieć, że nie jest znany wzór dający wszystkie liczby pierwsze, który miałby praktyczny a nie spektakularny charakter.

Warto w tym miejscu wspomnieć o wielomianie Eulera $f(x) = x^2 + x + 41$, który ma jako wartości liczby pierwsze dla $x \in \{1, \ldots, 39\}$.

TWIERDZENIE 13.10. *Nie istnieje wielomian jednej zmiennej o współczynnikach całkowitych, którego wartości dla wszystkich liczb naturalnych są liczbami pierwszymi.*

13.2.1. *Liczby Mersenne'a.* Większość rekordów stanowią liczby pierwsze postaci $M_k = 2^k - 1$. Liczby tej postaci nazywamy *liczbami Mersenne'a*.

STWIERDZENIE 13.11. *Jeśli liczba Mersenne'a $M_k = 2^k - 1$ jest liczbą pierwszą, to k jest liczbą pierwszą.*

TWIERDZENIE 13.12. *Niech p będzie nieparzystą liczbą pierwszą oraz niech ciąg S_n będzie określony następująco:*

$$S_1 = 4, \quad S_{n+1} = S_n^2 - 2 \text{ dla } n = 1, 2, \ldots$$

Wtedy liczba $M_p = 2^p - 1$ jest liczbą pierwszą wtedy i tylko wtedy, gdy M_p dzieli S_{p-1}.

Oczywiście zamiast wyrazów ciągu S_n obliczamy ich reszty z dzielenia przez M_p. Liczby pierwsze Mersenne'a są ściśle związane z parzystymi liczbami doskonałymi. Przypomnijmy, że - za Euklidesem - *liczbę naturalną n nazywamy doskonałą, gdy jest równa sumie swoich dzielników naturalnych mniejszych od n.*

Prawdziwe jest nastepujące twierdzenie pochodzące od **Eulera**.

TWIERDZENIE 13.13. *Liczba parzysta n jest doskonała wtedy i tylko wtedy, gdy n jest postaci $n = 2^{k-1}(2^k - 1)$, gdzie $M_k = 2^k - 1$ jest liczbą pierwszą.*

13.2.3. *Liczby Fermata.* Fermat w liście do Frenicle de Bessy w 1640 r. wyraził przypuszczenie, wszystkie liczby postaci $F_n = 2^{2^n}+1$ są liczbami pierwszymi (liczby tej postaci nazywamy *liczbami Fermata*). Dla początkowych wyrazów tego ciągu jest to prawdą - liczby:

$$\begin{aligned} F_0 &= 2^{2^0}+1 = 3, \\ F_1 &= 2^{2^1}+1 = 5, \\ F_2 &= 2^{2^2}+1 = 17, \\ F_3 &= 2^{2^3}+1 = 257, \\ F_4 &= 2^{2^4}+1 = 65537 \end{aligned}$$

są pierwsze. Zauważmy, że kolejne liczby Fermata rosną bardzo szybko:

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

Jednakże L. Euler w 1733 r. pokazał, że F_5 jest liczbą złożoną i wskazał jej dzielnik właściwy 641.

$$F_5 = 2^{2^5}+1 = 429467297 = 641 \cdot 6700417.$$

Istnieje hipoteza, że F_n, *dla każdego* $n \geq 5$ *jest złożona.*

Prawdziwe jest twierdzenie pochodzące od Gaussa:

TWIERDZENIE 13.15. *n-kąt foremny ($n > 2$) jest konstruowalny przy pomocy cyrkla i linijki wtedy i tylko wtedy, gdy liczba n jest postaci $n = 2^k p_1 \dots p_r$, gdzie $k \geq 0$, $r \geq 0$ oraz $p_1, \dots, p_r$ są parami różnymi liczbami pierwszymi Fermata.*

Podstawowe własności grup. Rzędy grup, podgrup i elementów grupy.

Przypomnijmy, że grupą nazywamy system algebraiczny $G = (G; e; \circ)$ złożony ze zbioru G, wyróżnionego elementu $e \in G$ i działania $\circ : G \times G \to G$ spełniających następujące aksjomaty:

G1 $\underset{x\in G}{\forall}\underset{y\in G}{\forall}\underset{z\in G}{\forall}[x \circ (y \circ z) = (x \circ y) \circ z]$

G2 $\underset{x\in G}{\forall}[x \circ e = e \circ x = x]$

G3 $\underset{x\in G}{\forall}\underset{x'\in G}{\exists}[x \circ x' = x' \circ x = e]$

Jeśli dodatkowo dla każdych elementów $x, y \in G$ zachodzi równość

$$x \circ y = y \circ x$$

to grupę G nazywamy przemienną (albo abelową).

TWIERDZENIE 15.1 (Prawo skracania). *Jeśli G jest grupą, to dla każdych $x, y, z \in G$*

$$x \circ y = x \circ z \Rightarrow y = z$$

$$y \circ x = z \circ x \Rightarrow y = z.$$

Podstawowe funkcje arytmetyczne; wzór Möbiusa na odwracanie

DEFINICJA 16.1. *Funkcją arytmetyczną nazywamy funkcję określoną na zbiorze liczb naturalnych* $\mathbb{N}$ *i przyjmującą wartości w zbiorze liczb zespolonych* $\mathbb{C}$. *Zbiór wszystkich funkcji arytmetycznych oznaczamy symbolem* $\mathbb{A}$.

Dla każdej ze znanych nam funkcji (wykładnik p-adyczny v_p ograniczony do zbioru liczb naturalnych, funkcja Eulera φ) rozszerzamy przeciwdziedzinę, aby można było te funkcje uważać za funkcje arytmetyczne. Zatem przykładami funkcji arytmetycznych są:

- dla każdej liczby pierwszej p funkcja $v_p : \mathbb{N} \to \mathbb{C}$; $v_p(n) = \sup\{\alpha \in \mathbb{N} : p^\alpha \mid n\}$;
- funkcja Eulera

$$\varphi : \mathbb{N} \to \mathbb{C};$$

$$\varphi(n) = \begin{cases} 1 & \text{gdy } n = 1 \\ |\{x \in \{1, 2, 3, ..., n-1\} : NWD(x, n) = 1\}| & \text{gdy } n > 1 \end{cases};$$

- funkcja podająca n-tą liczbę pierwszą $p_n : \mathbb{N} \to \mathbb{C}$;
- funkcja podająca n-tą liczbę Fermata $F_n = 2^{2^n} + 1$;
- funkcja podająca n-tą liczbę Mersenne'a $M_n = 2^n - 1$;
- funkcja tożsamościowa $id : \mathbb{N} \to \mathbb{C}$; $id(n) = n$;
- funkcja potęgowa o wykładniku k $id^k : \mathbb{N} \to \mathbb{C}$; $id^k(n) = n^k$;
- logarytm naturalny $\ln : \mathbb{N} \to \mathbb{C}$; $\ln(n) = x \Leftrightarrow e^x = n$;
- funkcja stała równa 1, którą oznaczymy $\mathbf{1} : \mathbb{N} \to \mathbb{C}$; $\mathbf{1}(n) = 1$;
- funkcja stała równa 0, którą oznaczymy $\mathbf{0} : \mathbb{N} \to \mathbb{C}$; $\mathbf{0}(n) = 0$;
- funkcja $I : \mathbb{N} \to \mathbb{C}$ określona wzorem $I(n) = \begin{cases} 1 & \text{gdy } n = 1 \\ 0 & \text{gdy } n > 1 \end{cases}$.