2. Podstawy matematyczne

2.1 Liczby całkowite i kongruencje

Omówimy krótko kongruencje w zbiorze liczb całkowitych Z oraz podstawowe własności kongruencji. Kongruencje mają podstawowe znaczenie dla algorytmów kryptograficznych.

Resztę z dzielenia liczby $a \in Z$ przez $m \in Z$ oznaczamy symbolem $a \pmod m$ lub symbolem $[a]_m$.

Definicja kongruencji. Niech $a, b, m \in Z$. Mówimy, że „liczba a przystaje do b modulo m" wtedy i tylko wtedy, gdy $m \mid (a-b)$ czyli liczba $a-b$ jest podzielna przez m. Fakt ten zapisujemy symbolicznie jako

$$a \equiv b \pmod m$$

i nazywamy krótko kongruencją (zarówno fakt jak i zapis). Bezpośrednio z definicji wynika, że jeśli $a \equiv b \pmod m$ to istnieje takie $k \in Z$, że $a = b + k \ m$.

Własności kongruencji

$$(n_1 + n_2 + \ldots + n_k) \pmod m = (n_1 \pmod m + n_2 \pmod m + \ldots + n_k \pmod m) \pmod m$$

Kongruencje (względem tego samego modułu m) można dodawać, odejmować i mnożyć stronami. Kongruencje można również mnożyć i dzielić obustronnie (jeśli dzielenie jest wykonalne) przez liczbę całkowitą względnie pierwszą z modułem $m \in N$, $m \geq 2$.

Fakt Jeśli $a, b \in Z$ to istnieją takie liczby całkowite $k_1, k_2 \in Z$, że

$$k_1 a + k_2 b = NWD(a,b) \qquad (*)$$

Dowód.
1.Oczywiście, jeśli $a \mid b$ lub $b \mid a$ to równość (*) zachodzi.

2.Rozważmy teraz przypadek gdy a nie dzieli b oraz b nie dzieli a. Wówczas postępując jak w algorytmie Euklidesa obliczenia $NWD(a,b)$ dostajemy (oznaczając $r_{-1} \overset{ozn}{=} a, r_0 \overset{ozn}{=} b$) w kolejnych dzieleniach z resztą:

(1) $\quad r_{-1} = q_1 r_0 + r_1$ czyli $r_1 = r_{-1} - q_1 \cdot r_0$

(2) $r_0 = q_2 r_2 + r_2$ czyli $r_2 = r_0 - q_2 \cdot r_1$

.

.

.

(n-1) $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$ czyli $r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2}$

(n) $r_{n-2} = q_n r_{n-1} + r_n$ czyli $r_n = r_{n-2} - q_n \cdot r_{n-1}$

gdzie $n \in N, n \geq 2, r_i$ dla $i = 1,2,...,n$ są resztami a q_i dla $i = 1,2,...,n$ są ilorazami w kolejnych dzieleniach z resztą.

Reszta r_n jest przy tym pierwszą zerującą się resztą. Zerowanie się reszty jest regułą stopu algorytmu Euklidesa. Ponieważ jak łatwo zauważyć kolejne reszty $r_1, r_2, ..., r_n$ maleją tzn. $r_1 > r_2 > ... > r_n$ więc reguła stopu musi w końcu zadziałać po pewnej liczbie kroków n. Przy powyższych oznaczeniach mamy:

$$NWD(a,b) = NWD(r_{-1}, r_0) = r_{n-1}$$

3.Patrząc na równość (n-1) widzimy, że $NWD(a,b) = r_{n-1}$ jest kombinacją liniową reszt r_{n-3} i r_{n-2}. Dokładnie, istnieją takie $\alpha, \beta \in Z$, że:

$$\alpha \cdot r_{n-3} + \beta \cdot r_{n-2} = NWD(a,b)$$

4.Korzystając z równości (n-2) na r_{n-2} stwierdzamy, że istnieją takie $\alpha', \beta' \in Z$, że

$$\alpha' \cdot r_{n-4} + \beta' \cdot r_{n-3} = NWD(a,b)$$

Postępując tak dalej (tzn. korzystając ze wzoru na r_{n-3} itd.) dostajemy w końcu, że istnieją takie $k_1, k_2 \in Z$, że

$$k_1 \cdot r_{-1} + k_2 \cdot r_0 = NWD(a,b)$$

czyli

$$k_1 a + k_2 b = NWD(a,b)$$

■

Funkcja Eulera

Funkcję Eulera $\varphi : N \to N$ definiuje się tak: $\varphi(n)$ dla $n \in N, n \geq 2$ jest liczbą liczb naturalnych mniejszych od n i względnie pierwszych z n ($n, m \in N$ są względnie pierwsze jeśli $NWD(n,m) = 1$). Można więc napisać: $\varphi(n) = card\{m \in N; m \leq n, NWD(m,n) = 1\}$.

Łatwo wykazać, że dla każdej liczby pierwszej p mamy

$$\varphi(p) = p - 1$$

oraz dla każdego $k \in N$ i każdej liczby p liczby pierwszej mamy

$$\varphi(p^k) = p^{k-1}(p-1).$$

Jeśli $a, b \in N$ są względnie pierwsze, to $\varphi(a,b) = \varphi(a)\varphi(b)$.

Ogólnie dla

$$\varphi(p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}) = p_1^{k_1-1}(p_1-1) \cdot p_2^{k_2-1} \cdot (p_2-1) \cdot \ldots \cdot p_r^{k_r-1}(p_r-1)$$

lub równoważnie

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

gdzie $p_1 < p_2 < \ldots < p_r$ są liczbami pierwszymi oraz $k_1, k_2, \ldots, k_r \in N$. Z reguły przyjmujemy dodatkowo, że $\varphi(1) = 1$ i wówczas funkcja Eulera zdefiniowana jest dla wszystkich argumentów naturalnych, tzn. $\varphi : N \to N$.

Małe twierdzenie Fermata

Dla dowolnej liczby pierwszej p i dowolnej liczby całkowitej $a \in Z$ takiej, że $NWD(p,a)=1$ (co jest równoważne z faktem, że p nie dzieli liczby całkowitej a) prawdziwa jest kongruencja

$$a^{p-1} \equiv 1 \pmod{p}.$$

lub równoważnie dla dowolnej liczby $a \in Z_p, a \neq 0$ mamy $a^{p-1} = 1$ (mnożenie w ciele Z_p)

Dowód. Wynika bezpośrednio z twierdzenia Eulera i z faktu, że $\varphi(p) = p - 1$.■

Twierdzenie Eulera.

Twierdzenie Eulera jest ważnym często wykorzystywanym w kryptografii twierdzeniem.

Twierdzenie (twierdzenie Eulera). Dla dowolnej liczby całkowitej a względnie pierwszej z $n \in N, n \geq 2$ prawdziwa jest kongruencja

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n),$$

gdzie $\varphi : N \to N$ jest funkcją Eulera lub równoważnie dla dowolnej liczby $a \in Z_n, a \neq 0$ i takiej, że $NWD(a,n) = 1$ mamy $a^{\varphi(n)} = 1$ (mnożenie w pierścieniu Z_n)

Dowód. Nietrudny dowód tego twierdzenia można znaleźć w każdym podręczniku elementarnej teorii liczb. ■

Małe twierdzenie Fermata jest prostym wnioskiem z twierdzenia Eulera.

Reszty i niereszty kwadratowe.

Niech $a \in Z_n^*$, liczba a nazywa się resztą kwadratową modulo n lub kwadratem modulo n, jeśli istnieje takie $x \in Z_n^*$, że $x^2 \equiv a (\mathrm{mod}\, n)$. Jeśli takie x nie istnieje, to a jest nazywane nieresztą kwadratową modulo n. Zbiór wszystkich reszt kwadratowych modulo n, oznaczony jest przez Q_n, a zbiór wszystkich niereszt kwadratowych modulo n oznaczany jest przez $\overline{Q}_n$. Zauważmy, że z definicji $0 \notin Z_n^*$ i stąd $0 \notin Q_n$ i $0 \notin \overline{Q}_n$.

Symbole Legendre`a i Jacobiego.

Symbol Legendre`a jest pomocny w sprawdzaniu czy liczba całkowita $a \in Z$ jest resztą kwadratową modulo liczba pierwsza $p$. Symbol Legendre`a $\left(\frac{a}{p}\right)$ dla $a \in Z$ i nieparzystej liczby pierwszej p zdefiniowany jest następująco:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ jesli } p|a \\ 1 \text{ jesli } a \in Q_p \\ -1 \text{ jesli a} \in \overline{Q}_p \end{cases}$$

Własności symbolu Legendre`a. Niech $a, b \in Z$ i p będzie nieparzystą liczbą pierwszą, wówczas:

a) $$\left(\frac{a}{b}\right) \equiv a^{(p-1)/2} (\mathrm{mod}\, p)$$

W szczególności $\left(\frac{1}{p}\right) = 1$ i $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, zatem $-1 \in Q_p$ jeśli $p \equiv 1(\mathrm{mod}\, 4)$ oraz $-1 \in Q_p$ jeśli $p \equiv 3(\mathrm{mod}\, 4)$.

b) $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

zatem jeśli $a \in Z_p^*$, to $\left(\frac{a^2}{p}\right) = 1$.

c) Jeśli $a \equiv b(\mathrm{mod}\, p)$, to $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

d) $$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$

Zatem $\left(\frac{2}{p}\right) = 1$ jeśli $p \equiv 1(\mathrm{mod}\, 8)$ lub $p \equiv 7(\mathrm{mod}\, 8)$ oraz $\left(\frac{2}{p}\right) = -1$ jeśli $p \equiv 3(\mathrm{mod}\, 8)$ lub $p \equiv 5(\mathrm{mod}\, 8)$.

e) Prawo wzajemności dla reszt kwadratowych. Jeśli q jest różną od p nieparzystą liczbą pierwsza, to

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}.$$

Innymi słowy $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ poza przypadkiem, gdy $p \equiv 3(\mathrm{mod}\, 4)$ i $q \equiv 3(\mathrm{mod}\, 4)$, w którym $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Symbol Jacobiego.

Symbol Jacobiego jest uogólnieniem symbolu Legendre`a na $n \in N$ nieparzyste (nie wymagamy pierwszości n). Definicja symbolu Jacobiego jest następująca. Niech $n \in N, n \geq 3$ będzie liczbą nieparzystą z rozkładem na czynniki pierwsze $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, wówczas symbol Jacobiego $\left(\frac{a}{n}\right)$ jest zdefiniowany jako

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} ... \left(\frac{a}{p_k}\right)^{e_k}.$$

Łatwo zauważyć, że jeśli n jest liczbą pierwszą, to symbol Jacobiego jest dokładnie symbolem Legendre`a.

Własności symbolu Jacobiego

. Niech $m, n \in N, m, n \geq 3$ i m, n niech będą nieparzyste wówczas dla każdego $a, b \in Z$ mamy

a) $\left(\frac{a}{n}\right) = 0,1$ lub -1 a ponadto $\left(\frac{a}{n}\right) = 0$ wtedy i tylko wtedy $NWD(a,n) \neq 1$.

b) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$, zatem jeśli $a \in Z_n^*$, to $\left(\frac{a^2}{n}\right) = 1$.

c) $\left(\frac{a}{m \cdot n}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$,

d) $a \equiv b (\mathrm{mod}\, n)$, to $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$,

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

f) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$, zatem

$\left(\frac{-1}{n}\right) = 1$ jeśli $n \equiv 1 (\mathrm{mod}\, 4)$ oraz:

$\left(\frac{-1}{n}\right) = -1$ jeśli $n \equiv 3 (\mathrm{mod}\, 4)$,

g) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$ zatem

$\left(\frac{2}{n}\right) = 1$ jeśli $n \equiv 1 \text{ lub } 7 \pmod 8$ oraz

$\left(\frac{2}{n}\right) = -1$ jeśli $n \equiv 3 \text{ lub } 5 \pmod 8$

h) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$ zatem

$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ chyba, że m i n przystają do 3 modulo 4, kiedy to $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

Algorytm obliczania symbolu Jacobiego

Prosty, rekurencyjny algorytm obliczania symbolu Jacobiego $\left(\frac{a}{n}\right)$ (i symbolu Legendre`a) jest następujący:

JACOBI(a, n) ; obliczanie $\left(\frac{a}{n}\right)$

WEJŚCIE: nieparzysta liczba całkowita $n \geq 3$ i $a \in < 0, n-1 >$

WYJŚCIE: symbol Jacobiego $\left(\frac{a}{n}\right)$ (a jeśli n jest liczbą pierwszą – symbol Legendre`a)

---

1. **if** $a = 0$ **then** $\left(\frac{a}{n}\right) := 0$
2. **if** $a = 1$ **then** $\left(\frac{a}{n}\right) := 1$
3. Przedstaw a w postaci $a = 2^e a_1$, gdzie a_1 jest nieparzyste, oraz $e \in N \cup \{0\}$.
4. **if** e parzysta **then** $s := 1$ **else begin**

   if $n \equiv 1 \text{ lub } 7 \pmod 8$ **then** $s := 1$

   if $n \equiv 3 \text{ lub } 5 \pmod 8$ **then** $s := -1$

   end

5. **if** $n \equiv 3 (\mathrm{mod}\, 4)$ i $a_1 \equiv 3 (\mathrm{mod}\, 4)$ **then** $s := -s$

6. $n_1 := n (\mathrm{mod}\, a_1)$

7. **if** $a_1 = 1$ then $\left(\frac{a}{n}\right) := s$ **else** $\left(\frac{a}{n}\right) := s \cdot \mathrm{JACOBI}\ (n_1, a_1)$.

Uwaga. Powyższy algorytm wykorzystuje do obliczania $\left(\frac{a}{n}\right)$ następujący wzór wynikający bezpośrednio z podanych wyżej własności symbolu Jacobiego.

$$\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right)\left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n (\mathrm{mod}\, a_1)}{a_1}\right)(-1)^{(a_1-1)(n-1)/4}$$

Liczby pseudopierwsze.

Jeśli $n \in N$ jest nieparzystą liczbą złożoną, spełniającą kongruencję $a^{n-1} \equiv 1 (\mathrm{mod}\, n)$ dla pewnego $a \in <2, n-1>$, to nazywamy ją pseudopierwszą przy podstawie *a*. Na przykład *n*=91 jest liczbą pseudopierwszą przy podstawie *a*=3, ponieważ $NWD(n,a) = 1$, *n* jest liczbą nieparzystą i $3^{90} \equiv 1 (\mathrm{mod}\, 91)$, ale nie jest pseudopierwsza przy podstawie 2, ponieważ $2^{90} \equiv 64 (\mathrm{mod}\, 91)$.

Istnieje nieskończenie wiele liczb pseudopierwszych przy podstawie *a*.

Liczby silnie pseudopierwsze przy podstawie a

Niech $n \in N$ będzie liczbą złożoną nieparzystą i niech $n-1 = 2^s \cdot d$, gdzie $s, d \in N$ i d jest nieparzyste oraz $s \geq 1$. Niech ponadto $a \in N$ spełnia warunki $1 < a < n$ i $NWD(a,n) = 1$. Liczbę *n* nazywamy silnie pseudopierwszą przy podstawie *a*, jeżeli

$$a^d \equiv 1 (\mathrm{mod}\, n)$$

albo

$$a^{2^r d} \equiv -1 (\mathrm{mod}\, n)$$

dla pewnego $r \in <0, s-1>$

Uwaga. Oczywiście jeśli n jest silnie pseudopierwsza przy podstawie a, to

$$a^{n-1} \equiv 1 \pmod{n} .$$

Ponadto nie musimy zakładać, w definicji, że $NWD(a,n)=1$, ponieważ jeśli $NWD(a,n)>1$, to nie zachodzi kongruencja $a^{n-1} \equiv 1 \pmod{n}$.

Liczby Carmichaela

Liczba Carmichaela (czyt. karmajkla) jest to liczba złożona $n \in N$, taka, że dla każdej liczby $a \in <2, n-1>$ takiej, że $NWD(a,n)=1$ mamy:

$$a^{n-1} \equiv 1 (\mathrm{mod}\, n)$$

Przykład. Liczba $n = 561 = 3 \cdot 11 \cdot 17$ jest liczbą Carmichaela. Jest to najmniejsza liczba Carmichaela.■

Twierdzenie. Istnieje nieskończenie wiele liczb Carmichaela i każda liczba Carmichaela jest iloczynem co najmniej trzech różnych liczb pierwszych.

Algorytm Millera-Rabina testowania pierwszości liczby $n \in N$.

Zauważmy, że mając testowaną liczbę $n \in N$ w zapisie NKB, możemy łatwo rozpoznać czy liczba n jest parzysta czy nie. Wystarczy sprawdzić wartość najmniej znacznego bitu. Jeśli ten bit jest równy 0, to liczba jest parzysta. Żeby nie komplikować opisu algorytmu od razu zakładamy, że dane wejściowe w algorytmie Millera–Rabina stanowią liczby $n \in N, n \geq 3$ nieparzyste. Algorytm Millera–Rabina jest następujący

---

Miller–Rabin (n, t) ; wersja pierwsza algorytmu Millera-Rabina

WEJŚCIE: testowana nieparzysta liczba $n \in N, n \geq 3$ i parametr t określający prawdopodobieństwo pomyłki orzeczenia „testowana liczba n jest pierwsza".

WYJŚCIE: odpowiedź „ n jest liczbą złożoną" lub „n jest liczbą pierwszą".

---

1. Zapisz liczbę $n-1$ w postaci $n-1 = 2^s r$, gdzie $s, r \in N$ i r jest liczbą nieparzystą.

2. **for** $i := 1$ **to** t **do begin**

2.1 wybierz losowo liczbę $a \in < 2, n-2 >$;

2.2 Oblicz $y = a^r \pmod n$ (np. wykorzystując algorytm iterowanego podnoszenia do kwadratu).

2.3 **if** $y \neq 1 \pmod n$ and $y \neq n-1 \pmod n$ **then**

begin

$j := 1$

while $j \leq s-1$ and $y \neq n-1 \pmod n$ **do**

begin

oblicz $y := y^2 \pmod n$

if $y = 1$ **then** „n jest liczbą złożoną i stop”

$j := j+1$

end

if $y \neq n-1$ **then** „ n jest liczbą złożoną i stop”.

end

end

3. Wyprowadź komunikat „ n jest liczbą pierwszą” i stop.

Miller–Rabin (n, t) ; wersja druga algorytmu Millera-Rabina

WEJŚCIE: testowana nieparzysta liczba $n \in N, n \geq 3$ i parametr t określający prawdopodobieństwo pomyłki orzeczenia „testowana liczba n jest pierwsza”.

WYJŚCIE: odpowiedź „ n jest liczbą złożoną” lub „n jest liczbą pierwszą”.

---

1. Zapisz liczbę $n-1$ w postaci $n-1 = 2^s r$, gdzie $s, r \in N$ i r jest liczbą nieparzystą.

2. **for** $i := 1$ **to** t **do begin**

2.1 wybierz losowo liczbę $a \in < 2, n-2 >$;

2.2 $m := (n-1)/2$

2.3 $j := s$

2.4 **while** $j > 0$ **begin**

2.5 Oblicz $y = a^m \pmod n$ (np. wykorzystując algorytm iterowanego podnoszenia do kwadratu).

if $y \neq 1 \pmod n$ and $y \neq n-1 \pmod n$ **then** „n jest liczbą złożoną i stop”

if $y = n-1 \pmod n$ **then** $j = 0$ **else begin** $j := j-1$; $m := m/2$ **end**

end

end

3. Wyprowadź komunikat „ *n* jest liczbą pierwszą” i stop.

Algorytm Millera-Rabina jest klasycznym przykładem tzw. algorytmu probabilistycznego. Istotą algorytmu probabilistycznego jest udzielanie odpowiedzi na postawione pytanie z zastrzeżeniem, że udzielona odpowiedź może być z pewnym bardzo małym prawdopodobieństwem np. prawdopodobieństwem $\frac{1}{2^{100}}$ błędna. Z reguły algorytmy probabilistyczne są znacznie szybsze niż algorytmy deterministyczne rozwiązujące ten sam problem.

W przypadku algorytmu Millera-Rabina odpowiedź "*n* jest liczbą złożoną" jest pewna natomiast odpowiedź "*n* jest liczbą pierwszą" może być błędna z prawdopodobieństwem błędu nie większym od $\frac{1}{4^t}$, gdzie liczba $t \in N$ jest parametrem wejściowym algorytmu określającym liczbę losowań liczby $a \in < 2, n-2 >$ (tzw. podstawy).

Istnieje deterministyczna wersja algorytmu Millera-Rabina oparta na tzw. hipotezie GRH (Generalised Riemann Hypothesis).

2.2 Grupy, pierścienie

Działania i algebry

Działanie. Niech A będzie niepustym zbiorem a n liczbą naturalną. *Działanie n–argumentowe* (lub operacja n-argumentowa) w zbiorze A, to dowolne odwzorowanie $f : \underbrace{A \times A \times ... \times A}_{n} \to A$. Element $f(a) \in A$ dla $a \in A^n$ nazywamy *wynikiem tego działania*.

Dodatkowo przez działanie 0 – argumentowe rozumiemy dowolny wyróżniony element zbioru A. Najczęściej mamy do czynienia z działaniami 0, 1 i 2 argumentowymi.

Mówimy, że podzbiór $B \subset A$ jest zamknięty ze względu na działanie $f : \underbrace{A \times A \times ... \times A}_{n} \to A$ jeśli dla każdego $(a_1, a_2, ..., a_n) \in B^n$ mamy $f(a_1, a_2, ..., a_n) \in B$. Zamkniętość podzbioru $B \subset A$ ze względu na działanie 0-argumentowe oznacza, że wyróżniony element należy do zbioru B.

Działania dwuargumentowe nazywamy krótko działaniami i oznaczamy zwykle takimi symbolami jak $+, \circ, \otimes, \oplus, /$ itp. a wynik działania na parze $(a_1, a_2) \in A^2$ oznaczamy symbolem $a_1 + a_2$, $a_1 \circ a_2$, $a_1 \otimes a_2$ itd.

Działanie dwuargumentowe $\circ$ nazywamy *przemiennym*, jeśli dla każdego $a, b \in A$ mamy

$$a \circ b = b \circ a$$

Działanie dwuargumentowe $\circ$ nazywamy *łącznym*, jeśli dla każdego $a, b, c \in A$ mamy

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Element neutralny (jedynka lub element jednostkowy) działania $\circ$. Element $1 \in A$ nazywamy elementem neutralnym lub jedynką lub też elementem jednostkowym działania $\circ$ jeśli $1 \circ a = a \circ 1 = a$ dla każdego $a \in A$.

Fakt. Element jednostkowy ustalonego działania dwuargumentowego $\circ$ może być tylko jeden.

Dowód. Załóżmy, że istnieją dwa różne takie elementy. Prowadzi to do sprzeczności a więc może istnieć tylko jeden element jednostkowy dla danego działania■

Działania zdefiniowane wyżej nazywają się również działaniami wewnętrznymi. Jeśli mamy dwa niepuste zbiory K i A to dowolne odwzorowanie $o_e : K \times A \to A$ nazywamy działaniem zewnętrznym.

Algebra. Układ uporządkowany $(A, o_1, o_2, ..., o_n)$, gdzie A jest zbiorem, a $o_1, o_2, ..., o_n$ działaniami, nazywa się algebrą. Jeśli wiemy z jakimi działaniami mamy do czynienia mówimy po prostu algebra A.

Algebry nazywamy też "*algebrami ogólnymi* lub "*algebrami abstrakcyjnymi*". Z pojęciem algebry związane są ściśle pojęcia *podalgebry*, *homomorfizmu algebr* i *izomorfizmu algebr*.

Podalgebra algebry $(A, o_1, o_2, ..., o_n)$. Niech $(A, o_1, o_2, ..., o_n)$ będzie algebrą a zbiór $B \subset A$ niech będzie zamknięty ze względu na działania $o_1, o_2, ..., o_n$ oraz niech dla każdego $i \in <1, n>$: $o_i' \stackrel{df}{=} o_i$ jeśli działanie o_i jest zeroargumentowe oraz $o_i' \stackrel{df}{=} o_i | B^{n_i}$ o ile działanie nie jest zeroargumentowe (gdzie n_i jest liczbą argumentów działania o_i).
W tej sytuacji algebrę $(B, o_1', o_2', ..., o_n')$ nazywamy podalgebrą algebry $(A, o_1, o_2, ..., o_n)$. Mówimy też często w uproszczeniu, że B jest podalgebrą algebry A.

Oczywiście każdy podzbiór $B \subset A$ zamknięty ze względu na działania $o_1, o_2, ..., o_n$ wyznacza podalgebrę algebry $(A, o_1, o_2, ..., o_n)$.

Homomorfizm algebr. Niech będą dane 2 algebry $(A, o_1, o_2, ..., o_n)$ i $(A, o_1', o_2', ..., o_n')$ tego samego typu tzn. takie, że dla każdego $i \in <1, n>$ liczby argumentów działania o_i oraz o_i' są jednakowe. Odwzorowanie $h: A_1 \to A_2$ nazywamy homomorfizmem algebr $(A, o_1, o_2, ..., o_n)$ i $(A, o_1', o_2', ..., o_n')$ jeśli dla każdego $i \in <1, n>$ i dla każdego $(a_1, a_2, ..., a_{n_i}) \in A_1^{n_i}$ (gdzie n_i jest liczbą argumentów działania i) mamy

$$h(o_i(a_1, a_2, ..., a_{n_i})) = o_i'(h(a_1), h(a_2), ..., h(a_{n_i}))$$

Izomorfizm algebr Homomorfizm różnowartościowy i na nazywamy izomorfizmem algebr.

Przykład. Szczególnymi przypadkami algebry są półgrupa, monoid, grupa, grupa abelowa, pierścień, ciało i algebra Boole'a. Niektóre z tych algebr poznamy dokładniej w dalszym ciągu.■

Czasami wprowadza się w (bardzo bliskie pojęciowo algebrze abstrakcyjnej ale nieco ogólniejsze) pojęcie *struktury algebraicznej* jako n-tki uporządkowanej (w skład tej n-tki wchodzi rodzina zbiorów niepustych oraz rodzina działań wewnętrznych i zewnętrznych). Przykładem struktury algebraicznej jest przestrzeń liniowa $(V, K, +, \cdot)$, gdzie V jest zbiorem wektorów, K ciałem, plus oznacza dodawanie wektorów a kropka oznacza działanie mnożenia przez skalar.

Półgrupy, monoidy

Półgrupa to niepusty zbiór A z dwuargumentowym działaniem łącznym $o : A \times A \to A$.

Dokładniej jest to para uporządkowana (A, o) taka, że zbiór A jest niepusty a działanie $o : A \times A \to A$ jest działaniem dwuargumentowym łącznym tzn. dla każdego $a, b, c \in A$ mamy

$$a \circ (b \circ c) = (a \circ b) \circ c$$

Działanie zdefiniowane w półgrupie nazywa się najczęściej mnożeniem.

Fakt.(który warto znać)
W dowolnej półgrupie $(A, \circ)$ z łączności działania wynika, że wartość $(...((a_1 \circ a_2) \circ a_3) \circ ...a_{n-1}) \circ a_n$ dla $a_1, a_2, ..., a_n \in A$ nie zależy od rozmieszczenia nawiasów. Możemy więc pisać: $a_1 \circ a_2 \circ ... \circ a_n$.

Dowód. Dowód tego faktu jest indukcyjny ■

Monoid to półgrupa z elementem jednostkowym więc jest to trójka uporządkowana $(G, \cdot, 1)$ z działaniem $\cdot : G \times G \to G$ spełniającym dwa warunki

1) warunek łączności; tzn. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ dla każdego $x, y, z \in G$.

2) istnienie elementu jednostkowego w zbiorze G

Istnienie jedynki oznacza, że istnieje taki element $1 \in A$, że $1 \circ a = a \circ 1 = a$ dla każdego $a \in A$.

W monoidzie możemy zdefiniować relację podzielności. Jeśli $a = b \cdot c$ to piszemy $b|c$ i czytamy b dzieli a .

Przykład. Zbiór V^* (wszystkich słów nad ustalonym alfabetem V) z konkatenacją jest monoidem. Jedynką w V^* jest słowo puste ε . Łączność konkatenacji jest oczywista.■

Grupy i logarytmy dyskretne w grupach

Definicja grupy. Monoid $(G, \circ)$ posiadający tę własność, że dla każdego $a \in A$ istnieje taki element $b \in A$, że $a \circ b = b \circ a = 1$ nazywamy *grupą*. Upraszczając mówimy, że G jest grupą.

Element b z powyższej definicji nazywamy elementem odwrotnym do a i oznaczamy symbolem a^{-1} tzn. $b = a^{-1}$.

Inaczej mówiąc grupą nazywamy system algebraiczny $(G,\circ)$ z dwuargumentowym działaniem $\circ\cdot : G \times G \to G$ spełniającym 3 warunki

1) łączność

2) istnieje jedynki w zbiorze G

3) istnienie elementu odwrotnego (de facto aksjomat 3 wprowadza nowe działanie) $a \to a^{-1}$

Grupę nazywamy grupą skończoną jeśli ma skończoną liczbę elementów. Ilość elementów w grupie nazywamy *rzędem grupy* i oznaczamy symbolem $|G|$. Podzbiór grupy G, który jest grupą ze względu na to samo działanie grupowe nazywamy podgrupą grupy G. Homomorfizm grup i izomorfizm grup definiujemy tak jak w każdej algebrze.

Generator grupy Generator g grupy G to taki element grupy dla którego $G = \{g^k; k \in N\}$. Jeśli grupa ma generator to nazywamy ją cykliczną.

Rząd elementu grupy Rząd k elementu a grupy G to najmniejsza taka liczba naturalna n taka , że $a^n = 1$ a więc

$$k = \min\{k \in N; a^k = 1\}$$

Jeśli działanie grupowe jest przemienne to taką grupę nazywamy *grupą abelową lub grupą przemienną.*

Grupy cykliczne to z definicji grupy mające generator. Oczywiście każda grupa cykliczna jest abelowa.

Twierdzenie. (twierdzenie Lagrange'a**)** Dla grup skończonych rząd podgrupy jest dzielnikiem rzędu grupy.

Wniosek. Rząd elementu grupy jest dzielnikiem rzędu grupy.

Twierdzenie (Cayleya)
Każda grupa rzędu n jest izomorficzna z pewną podgrupą grupy symetrycznej S_n.

Uwaga. S_n jest „całkiem sporą" grupą bo rząd S_n jest równy $n!$.

Przykład 1. Podstawowym przykładem grupy jest zbiór liczb całkowitych $(Z,+)$ ze zwykłym działaniem dodawania jako działaniem grupowym. $(Z,+)$ jest grupą abelową. ■

Przykład 2.
Zbiór liczb rzeczywistych $(R,+)$ ze zwykłym działaniem dodawania jest grupą. Podobnie zbiór $(R.\setminus\{0\},\cdot)$ z działaniem mnożenia jest grupą abelową.

Podobnie zbiór liczb Q wymiernych z dodawaniem i zbiór liczb zespolonych C z dodawaniem są grupami abelowymi. ■

Przykład 3.
Rozważmy zbiór liczb $Z_m = \{0,1,2,...,m-1\}$. Ważnym przykładem grupy jest grupa $(Z_m,\oplus_m)$ liczb modulo *m*, gdzie $m \in N, m \geq 2$ z działaniem sumy modulo *m* jako działaniem grupowym. Jest to grupa abelowa.

Grupą abelową jest również $(Z_m \setminus\{0\},\otimes_m)$ (gdzie $m \in N, m \geq 2$) o ile $m = p$, gdzie *p* jest liczbą pierwszą. Działaniem grupowym. jest tu iloczyn modulo *m* . Jeśli *m* nie jest liczbą pierwszą to $(Z_m \setminus\{0\},\otimes_m)$ jest tylko półgrupą z 1.■

Przykład 4. Zbiór liczb $Z_p^* = \{1,2,..., p-1\}$, z działaniem mnożenia modulo *p* jest grupą abelową. ■

Przykład 5. Przykładem grupy nieabelowej jest $(S_n,\circ)$, gdzie S_n jest zbiorem wszystkich permutacji zbioru *n* elementowego a działanie "$\circ$" superpozycją odwzorowań. ■

Przykład 6. Zbiory Q\{0}, R\{0}, C\{0} z działaniem mnożenia liczb są grupami abelowymi. ■

Przykład 7.
Zbiór wszystkich liczb naturalnych względnie pierwszych z liczbą naturalną *n,* $n \geq 2$ jest grupą (por. następny podrozdział) ze względu na mnożenie modulo *n.* Grupę tę oznaczamy symbolem *G(n*). Liczba elementów w grupie *G(n*) jest oczywiście równa $\varphi(n)$. ■

Niech *P* będzie podgrupą grupy *G*. Jeśli $|P| = p^k$ dla pewnego $k \in N$ i liczby pierwszej *p* to mówimy, że *P* jest *p* podgrupą grupy *G*. Każdą grupę mającą p^k elementów nazywamy *p*-grupą.

Logarytmy dyskretne w grupach. Jeśli $g \in G$ jest ustalonym elementem grupy G i $a \in G$ pewnym wybranym elementem to każdą liczbę $n \in N \cup \{0\}$ taką, że $g^n = a$ nazywamy logarytmem dyskretnym z elementu a przy podstawie g i ten fakt zapisujemy również jako $\log_g a = n$. Najczęściej jako g przyjmujemy generator grupy G.

Uwaga: Jeśli $g \in G$ jest generatorem grupy G tzn. grupa G jest cykliczna i n jest rzędem grupy G to funkcja $\log_b : G \ni y \to \log_b y \in Z_n$ jest izomorfizmem grupy G i grupy addytywnej pierścienia Z_n.

Pierścienie

Definicja *pierścienia,* jest następująca Niech w niepustym zbiorze P będą określone 2 działania, $+ : P \times P \to P$ i $\cdot : P \times P \to P$ zwane odpowiednio dodawaniem i mnożeniem oraz niech będą wyróżnione 2 elementy 0 i 1 zwane zerem i jedynką pierścienia. Czwórkę uporządkowaną $(P,+,\cdot,0,1)$ nazywamy pierścieniem jeśli spełnione są dla każdego $a,b,c \in P$ następujące warunki:

1) $a+b=b+a$ (przemienność dodawania)
2) $a+(b+c)=(a+b)+c$ (łączność dodawania)
3) $a+0=0+a=a$ (0 jest elementem zerowym pierścienia)
4) dla każdego $a \in P$ istnieje $a' \in P$, że $a+a'=a'+a=0$ (istnienie elementu przeciwnego)

5) $a \cdot b = b \cdot a$ (przemienność mnożenia)
6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (łączność mnożenia)
7) $a \cdot 1 = 1 \cdot a = a$ (1 jest jedynką pierścienia)
8) $a(b+c) = a \cdot b + a \cdot c$ oraz $(b+c)a = ba + ca$ (rozdzielność mnożenia względem dodawania)

Ściślej, układ $(P,+,\cdot,0,1)$ spełniający powyższe warunki nazywamy zwykle pierścieniem przemiennym z jednością a pierścieniem nazywa się układ $(P,+,\cdot,0)$ spełniający tylko warunki 1), 2), 3), 4) 7) i 8). Innymi słowy pierścień to grupa abelowa z mnożeniem spełniającym warunki 6) i 8).

Jeśli dodatkowo spełniony jest warunek 5) to pierścień nazywamy przemiennym. Pierścień przemienny zatem to taki pierścień w którym działanie mnożenia jest przemienne

Jeśli dodatkowo spełnione są warunki 5) i 7) to pierścień nazywamy pierścieniem przemiennym z 1.

Ponieważ w dalszym ciągu będziemy mieli do czynienia tylko z pierścieniami przemiennymi z jedynką będziemy je krótko nazywać pierścieniami.

Krótko: pierścieniem nazywamy algebrę $(P,+,\cdot,0)$ taką, że $(P,0,+)$ jest grupą abelową a działanie mnożenia $\cdot : P \times P \to P$ jest łączne i rozdzielne względem dodawania

(prawostronnie i lewostronnie) tzn. spełnione są aksjomaty grupy abelowej i następujące 2 warunki $a(b+c)=a\cdot b+a\cdot c$ oraz $(b+c)a=ba+ca$ dla każdego $a,b,c\in P$.

Często dla uproszczenia sformułowań pierścieniem nazywamy również sam zbiór P.

Zauważmy, że nie zakładamy, że zero i jedynka to różne elementy. Jeśli jednak tak jest to pierścień składa się z jednego tylko elementu. Jest to tzw. pierścień zerowy.

Pojęcia podpierścienia, homomorfizmu i izomorfizmu pierścieni wprowadza się w teorii pierścieni analogicznie jak w przypadku algebr.

Przykład 1. Zbiór liczb całkowitych Z ze zwykłymi działaniami dodawania i mnożenia jest pierścieniem (przemiennym z 1). ■

Przykład 2. Zbiór liczb $Z_m=\{0,1,...,m-1\}$ $(m\in N, m\geq 2)$ jest pierścieniem z działaniami sumy modulo m i mnożenia modulo m. Jest to tzw. pierścień reszt modulo m. Sumę modulo m oznaczamy symbolem $\oplus$ lub $\oplus_m$. Zapis $x\oplus_m y$ oznacza resztę z dzielenia zwykłej sumy $x+y$ liczb całkowitych przez m. Podobnie iloczyn modulo m oznaczamy symbolem $\otimes$ lub $\otimes_m$. Zapis $x\otimes_m y$ oznacza resztę z dzielenia zwykłego iloczynu liczb całkowitych przez m. Wprowadza się też często 2 zapisy na oznaczenie reszty z dzielenia przez liczby całkowitej x przez m : x (mod m) oraz $[x]_m$. Jeśli $m=p$ gdzie p jest liczbą pierwszą to Z_p jest ciałem. ■

Dzielniki zera

Definicja dzielnika zera. Element a pierścienia przemiennego P nazywa się dzielnikiem zera, gdy istnieje taki różny od zera element $b\in P$, że $ab=0$. Jeśli $a\cdot b=0$ i $a,b\neq 0$ to a i b nazywamy (właściwymi) dzielnikami zera.

Przykład 1 0 jest dzielnikiem zera■

Przykład 2 W pierścieniu Z_5 liczby 5 i 2 są dzielnika mi zera ponieważ $5\otimes_{10} 2=0$.■

Niezerowy pierścień przemienny z 1 nazywamy dziedziną całkowitości, jeśli nie ma w nim właściwych dzielników zera tzn. dla każdego $a,b\in P$ jeśli $ab=0$ to $a=0$ lub $b=0$. Mówimy krótko dziedzina całkowitości to pierścień bez dzielników 0.

Ideały

Definicja ideału. Niepusty podzbiór I pierścienia P nazywamy ideałem jeśli

1) I jest zamknięty ze względu na dodawanie

2) Jeśli $a\in I$ i $x\in P$ to $a\cdot x\in I$

Łatwo sprawdzić, że z warunku 1) wynika, że I jest grupą abelową ze względu na dodawanie. Można więc powiedzieć, że ideał pierścienia P to taki niepusty podzbiór $I \subset P$, który jest grupą abelową ze względu na dodawanie i dla każdego $a \in I$ i każdego $x \in P$ mamy $a \cdot x \in I$.

Przykład Zbiór nZ jest ideałem w pierścieniu liczb całkowitych Z.■

Twierdzenie

Niech $a \in Z_m$ wówczas NWD(a,m)=1 wtedy i tylko wtedy, gdy istnieją takie liczby $k_1, k_2 \in Z$, że

$$k_1 a + k_2 m = 1,$$

Dowód. $\Leftarrow$ Implikacja w tym kierunku jest oczywista.
$\Rightarrow$ Wynika z rozszerzonego algorytmu Euklidesa. ■

Elementy odwracalne w pierścieniu Z_m scharakteryzowane są następującym twierdzeniem.

Twierdzenie

Element $a \in Z_m$ jest odwracalny w Z_m wtedy i tylko wtedy, gdy NWD(a,m)=1

Dowód. $\Leftarrow$ Załóżmy, że $NWD(a,m)=1$, wówczas (na mocy wykazanego powyżej twierdzenia) istnieją takie liczby całkowite $k_1, k_2 \in Z$, *że* $k_1 a + k_2 m = 1$, skąd po obłożeniu obu stron tej równości homomorfizmem modulo m dostajemy $[k_1 a]_m = 1$ i dalej $[k_1]_m \otimes_m [a]_m = 1$ zatem $[k_1]_m$ jest szukaną odwrotnością elementu *a.*
$\Rightarrow$ Jeśli element a jest odwracalny to istnieje taki element $b \in Z_m$, że $b \otimes_m a = 1$ a zatem istnieje takie $k \in Z$, że $ba + km = 1$ liczby a i m muszą więc być względnie pierwsze w przeciwnym bowiem razie ich wspólny czynnik musiałby dzielić prawą stronę równania $ba + km = 1$ co jest niemożliwe.■

2.3 Ciała skończone

W tym podrozdziale zdefiniujemy pojęcie ciała (ang. field, fran. le corp, nm. Korp) i omówimy podstawowe własności ciał.

Ciało to algebra $(K,+,\cdot,0,1)$ z dwoma działaniami dwuargumentowymi, działaniem dodawania $+:K\times K\to K$ i działaniem mnożenia $\cdot:K\times K\to K$ oraz dwoma wyróżnionymi elementami 0 i 1.

Ciała oznacza się z reguły symbolami *K, L, F* a tzw. ciała skończone o q elementach symbolem F_q lub $GF(q)$ (litera *K* sugeruje wykorzystanie francuskiej lub niemieckiej nazwy ciała, *F* nazwy angielskiej *a GF* jest skrótem od Galois field).

Ciało może mieć skończoną albo nieskończoną ilość elementów. Mówimy krótko "ciała skończone" i "ciała nieskończone".

Szczególną uwagę zwrócimy na ciała skończone czyli ciała o skończonej ilości elementów. Szczególnie ważne są ciała skończone w kryptografii, kodach korekcyjnych i cyfrowym przetwarzaniu sygnałów. W niniejszym podrozdziale zostaną również omówione pierwiastki z jedności i pierwiastki pierwotne z jedności.

Definicja ciała Pierścień przemienny z jednością $(K,+,\cdot,0,1)$ taki, że $0\neq 1$ spełniający warunek

$$\forall_{x\in K, x\neq 0}\ \exists_{y\in K}\ xy=1$$

nazywa się ciałem.

Inaczej mówiąc ciało to z definicji taki pierścień przemienny z jednością taki, że $0\neq 1$, i w którym dla każdego niezerowego elementu istnieje element odwrotny. Jeśli ciało K ma skończoną ilość elementów to nazywamy je ciałem skończonym jeśli nieskończoną to nazywamy je ciałem nieskończonym . Z definicji ciała wynika, że ciało ma co najmniej 2 elementy.

Podciało ciała i rozszerzenie ciała, ciało proste

Definicja. Niech K będzie ciałem. Podzbiór L ciała K nazywamy podciałem ciała K jeśli $0,1\in L$ i w podzbiorze L są wykonalne działania dodawania, odejmowania, mnożenia i dzielenia przez elementy różne od 0. Z kolei K nazywamy rozszerzeniem ciała L.

Definicja. Ciało proste K to takie ciało które nie zawiera żadnego podciała właściwego tzn. nie ma takiego podciała L ciała K, że $L\subset K$ i $L\neq K$.

Fakt. Jedynym (z dokładnością do izomorfizmu) ciałem skończonym prostym jest ciało Z_p a jedynym (z dokładnością do izomorfizmu) ciałem nieskończonym prostym jest ciało liczb wymiernych Q.

Charakterystyka ciała

Definicja. Niech K będzie ciałem. Charakterystyka ciała K to najmniejsza liczba naturalna n o tej własności, że:

$$\underbrace{1+1+...+1}_{n}=0$$

co zapisujemy również jako $n1=0$. Jeśli takiej liczby naturalnej nie ma to przyjmujemy że charakterystyka ciała jest równa 0. Charakterystykę ciała K oznaczamy przez char K.

Twierdzenie Charakterystyka ciała K jest zawsze liczbą pierwszą p lub równa się 0. Charakterystyka ciała skończonego jest zawsze liczbą pierwszą.

Dowód. Załóżmy, że char K =n i $n=m_1m_2$, gdzie $m_1,m_2\in N$ a więc $n\cdot 1=(m_1m_2)\cdot 1=0$. Z łączności dodawania i rozdzielności mnożenia względem dodawania w ciele K mamy $(m_1m_2)\cdot 1=(m_1\cdot 1)(m_2\cdot 1)$, zatem

$$(m_1\cdot 1)(m_2\cdot 1)=0 \qquad (*)$$

Jeśli $m_1<n$ to z definicji charakterystyki dostajemy, że $m_1\cdot 1\neq 0$, zatem istnieje element odwrotny $(m_1\cdot 1)^{-1}$ do $m_1\cdot 1$. Mnożąc lewostronnie równość (*) przez $(m_1\cdot 1)^{-1}$ dostajemy $m_2\cdot 1=0$, ponieważ jednak $1\le m_2\le n$ to biorąc pod uwagę definicję charakterystyki ciała musimy mieć $m_2=n$. Wynika stąd, że liczba
n nie jest podzielna przez żadną liczbę różną od n i 1 a zatem jest liczbą pierwszą. ■

Uwaga 1. Każde ciało skończone K ma oczywiście charakterystykę skończoną. Zatem charakterystyka ciała skończonego K jest zawsze liczbą pierwszą p. Oczywiście każde rozszerzenie skończonego ciała K ma tę samą charakterystykę. Jednak liczba elementów ciała K nie musi być równa charakterystyce tego ciała czyli na ogół $card\ K\neq char\ K$. Istnieją jednak ciała nieskończone o charakterystyce skończonej.

Uwaga 2. Każde ciało charakterystyki 0 jest nieskończone.

Przykład 1. Jeżeli p jest liczbą pierwszą to pierścień $Z_p=\{0,1,2,...,p-1\}$ jest ciałem. Nazywamy je ciałem liczb modulo p (i oznaczamy też symbolem $GF(p)$ lub F_p). Oczywiście jest to ciało skończone o charakterystyce p. ■

Przykład 2. Zbiór liczb wymiernych Q, zbiór liczb rzeczywistych R, zbiór liczb zespolonych C są przykładami ciał nieskończonych o charakterystyce 0. ■

Przykład 3. Ciała $GF(2^8)$ i $GF(2^n)$ to ciała skończone o charakterystyce 2. ■

Przykład 4. Ciała liczbowe $Q(\sqrt{2}) \overset{df}{=} \{a+b\sqrt{2}; a,b \in Q\}$ i $Q(\sqrt{3}) = \{a+b\sqrt{3}; a,b \in Q\}$. są nieskończonymi ciałami o charakterystyce 0. Ciało liczb wymiernych Q jest podciałem tych ciał..

Przykład 5. Ciało skończone $GF(p^k)$ ma charakterystykę p. Pokażemy później jak zbudowane jest takie ciało i że jest ono jedynym ciałem (z dokładnością do izomorfizmu) o p^k elementach.

Twierdzenie Każde ciało skończone ma p^k elementów, gdzie p jest pewną liczbą pierwszą. Dokładniej jeśli q oznacza liczbę elementów ciała skończonego K to istnieje takie $k \in N$ i liczba pierwsza p, że $q = p^k$.

Dowód. Dowód można znaleźć np. w [10] ■

Twierdzenie Dla każdej liczby pierwszej p i dowolnej liczby $k \in N$ istnieje ciało o $q = p^k$ elementach.
Dowód. Dowód można znaleźć np. w [10] ■

Konstrukcja uniwersalnego ciała o $q = p^k$ elementach

Twierdzenie Każde ciało skończone F_q o $q = p^k$ elementach jest izomorficzne z ciałem $F_q[x]/(f)$, gdzie f jest dowolnym unormowanym wielomianem stopnia k o współczynnikach w ciele F_q nierozkładalnym w pierścieniu $F_q[x]$.
Dowód. Dowód można znaleźć np. w [10] ■

Twierdzenie Niech p będzie liczbą pierwszą oraz $k \in N$. Każde 2 ciała skończone o o takiej samej liczbie elementów są izomorficzne.

Dowód. Dowód można znaleźć np. w [9] i [10] ■

Uwaga. Możemy więc powiedzieć mając ustaloną liczbę pierwszą p i $k \in N$, że z dokładnością do izomorfizmu istnieje dokładnie jedno ciało o $q = p^k$ elementach. Oznaczamy to ciało symbolem F_q lub $GF(p^k)$

2. 4 Chińskie Twierdzenie o Resztach

Chińskie twierdzenie o resztach (ang. Chinese Remainder Theorem) to bardzo przydane w praktyce twierdzenie. Chińskie twierdzenie o resztach jest lematem, który wykorzystamy m.in. w dowodzie poprawności działania szyfru RSA. Chińskie twierdzenie o resztach jest również często wykorzystywane w cyfrowym przetwarzaniu sygnałów i arytmetyce cyfrowej. W najprostszej wersji jest to twierdzenie o istnieniu i jednoznaczności rozwiązania układu kongruencji $x \equiv x_i \pmod{m_i}$ dla każdego $i=1,2,...,n$.

Twierdzenie 2.1. *(klasyczne sformułowanie chińskiego twierdzenia o resztach dla pierścienia liczb całkowitych Z)*

Załóżmy, że liczby naturalne $m_1, m_2,...m_n$ większe od jedynki są parami względnie pierwsze (tzn. dla każdego $i \neq j$ mamy $\text{NWD}(m_i, m_j) = 1$) wówczas dla dowolnych n liczb całkowitych $x_1, x_2,...x_n \in Z$ układ kongruencji liniowych (*)

$$\begin{aligned} &x \equiv x_1 \pmod{m_1} \\ &x \equiv x_1 \pmod{m_2} \\ &..... \\ &x \equiv x_i \pmod{m_n} \end{aligned} \qquad (*)$$

ma tylko jedno rozwiązanie x w zbiorze $< 0, M-1 >$, gdzie $M = m_1 \cdot m_2 \cdot ...m_n$. Rozwiązanie to dane jest wzorem

$$x = \left[\sum_{i=1}^{n} k_i x_i \right]_M$$

gdzie k_i dla i=1,2,3,...,n są liczbami całkowitymi spełniającymi następujące warunki

$$\begin{aligned} &k_i \equiv 1 \pmod{m_i} \text{ dla } i=1,2,3...,n \\ &k_i \equiv 0 \pmod{m_j} \text{ dla } i \neq j \end{aligned} \qquad (**)$$

Dowód. Pełne rygorystyczne dowody można znaleźć m.in. w pracach [4] i [8]■

Literatura

[1] H.Rasiowa; Wstęp do matematyki;PWN,Warszawa
[2] A.Białynicki- Birula; Algebra; PWN,Warszawa
[3] A.Białynicki- Birula; Zaryss Algebry, PWN, Warszawa
[4] D.E. Knuth; The Art of Computer Programming; Addison-Wesley, London 1998.
(jest przekład polski: D.E. Knuth; Sztuka programowania; WNT, 2002).
[5] B.Schneier; Kryptografia dla praktyków; WNT, 2002.
[6] A. Menezes, P. Oorschot, S. Vanstone; Handbook of Applled Cryptography; CRC Press Inc., 1997. (treść jest na stronie: http://cacr.math.uwaterloo.ca/hac)
[7] N.Koblitz; A Course in Number Theory and Cryptography; Springer Verlag, New York 1994. (jest przekład polski p.t. Wykład z teorii liczb i kryptografii; WNT, Warszawa 1995.)
[8] W. Narkiewicz; Teoria liczb; PWN 1990.
[9] V. Shoup; A computational Introduction to Number Theory and Algebra; www.shoup.net/ntb
[10] J.Browkin; Teoria ciał; PWN, Warszawa 1977.

Zadania

Zadanie 1
Obliczyć wartość funkcji Eulera: a) $\varphi(5358)$, b) $\varphi(3458)$, c) $\varphi(2^{1000})$

Rozwiązanie
1.Skorzystamy z ogólnego wzoru na wartość funkcji Eulera. Jeśli $n = p_1^{k_1} p_2^{k_2} \cdot ... \cdot p_r^{k_r}$, gdzie $p_1 < p_2 < ... < p_n$ są liczbami pierwszymi a $k_1, k_2, ..., k_r \in N$, to :

$$\varphi(n) = \varphi(p_1^{k_1} p_2^{k_2} \cdot ... \cdot p_r^{k_r}) = p_1^{k_1 - 1}(p_1 - 1) p_2^{k_2 - 1}(p_2 - 1) \cdot ... \cdot p^{k_r - 1}(p_r - 1)$$

2.Ad a) $n = 5358 = 2 \cdot 3 \cdot 19 \cdot 47$ i 2,3,19,47 są liczbami pierwszymi, zatem

$\varphi(n) = \varphi(5358) = 1 \cdot 2 \cdot 18 \cdot 46$

3.Ad b) $n = 3458 = 2 \cdot 7 \cdot 13 \cdot 19$ i 2,7,13,19 są liczbami pierwszymi, zatem:

$\varphi(n) = \varphi(3458) = 1 \cdot 6 \cdot 12 \cdot 18 = 1296$

4.Ad c) $\varphi(2^{1000}) = 2^{999}$ ■

Zadanie 2
Pokazać, że $\limsup_{n \to \infty} \frac{\varphi(n)}{n} = 1$

Rozwiązanie
Jeśli wybierzemy z ciągu $(\frac{\varphi(n)}{n})_{n=1}^{\infty}$ podciąg $(\frac{\varphi(n_k)}{n_k})_{k=1}^{\infty}$ taki, że dla $k = 1,2,3,...$ liczba n_k jest kolejną liczbą pierwszą, to mamy:

1) dla każdego $n \in N$; $\frac{\varphi(n)}{n} \leq 1$

2) $\frac{\varphi(n_k)}{n_k} = \frac{n_k - 1}{n_k} \to 1$ dla $k \to \infty$

Zatem istotnie $\limsup_{n \to \infty} \frac{\varphi(n)}{n} = 1$. ■

Zadanie 3

Pokazać, że dla $x, a \in Z$ i $n \in N, n \geq 2$ mamy $x \equiv a (\mathrm{mod}\, n)$ wtedy i tylko wtedy gdy $[x]_n \equiv a (\mathrm{mod}\, n)$.

Rozwiązanie

1. Wynikanie w prawo. Jeśli $x \equiv a (\mathrm{mod}\, n)$, to istnieje takie $k \in Z$, że $x - a = kn$, zatem $x = a + kn$ i z własności homomorfizmu $[\cdot]_n : Z \to Z_n$ dostajemy $[x]_n = [a]_n$ skąd oczywiście mamy $[x]_n \equiv a (\mathrm{mod}\, n)$.

2. Wynikanie w lewo. Z faktu, że $[x]_n \equiv a (\mathrm{mod}\, n)$ wynika, że istnieje takie $j \in Z$, że $x = [x]_n + jn$, zatem $x - jn \equiv a (\mathrm{mod}\, n)$, a więc $x \equiv a (\mathrm{mod}\, n)$. ■

Zadanie 4

Niech f będzie funkcją kwadratową określoną dla $x \in R$ wzorem $f(x) = x^2 + 6x + 8$.

Odpowiedzieć na pytania:

1) Czy dla każdej liczby naturalnej *n* liczba $f(n)$ jest podzielna przez 3 ?

2) Czy jeżeli liczba naturalna *n* nie jest podzielna przez 3 to liczba $f(n)$ jest podzielna przez 3 ?

Zadanie 5

Wykazać małe twierdzenie Fermata. Jeśli *p* jest liczbą pierwszą, zaś *a* liczbą całkowitą to $a^p \equiv a \,(\mathrm{mod}\, p)$. W szczególności jeżeli *p* nie dzieli *a*, to $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$.

Rozwiązanie

Dowód można przeprowadzić indukcyjnie względem $a \in N$. Wynika stąd natychmiast prawdziwość twierdzenia dla $a \in Z$. Dla $a = 1$ twierdzenie oczywiście zachodzi. Jeśli zachodzi dla pewnego *a*, to zachodzi dla *a* +1. Istotnie ze wzoru na dwumian Newtona dla dowolnego ciała i założenia indukcyjnego mamy:

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \,(\mathrm{mod}\, p)$$

Zatem na mocy zasady indukcji skończonej wzór $a^p \equiv a \,(\mathrm{mod}\, p)$ prawdziwy jest dla każdego $a \in N$ a stąd również dla każdego $a \in Z$. Załóżmy teraz, że *p* nie dzieli *a*. Kongruencja $a^p \equiv a \,(\mathrm{mod}\, p)$ oznacza, że w ciele Z_p

$$[a]_p^p = [a]_p \qquad (**)$$

a ponieważ $NWD(p,a)=1$, więc również $NWD(p,[a]_p)=1$ (por zad. xx) i istnieje w Z_p element odwrotny $[a]_p^{-1}$. Mnożąc teraz równość (**) stronami przez $[a]_p^{-1}$ dostajemy $[a]_p^{p-1}=1$ co oznacza, że $a^{p-1}\equiv 1 \pmod p$. ■

Zadanie 2.6
Znaleźć wszystkie liczby pierwsze *p* dla których liczba $1!+2!+3!+...+p!$ jest kwadratem liczby naturalnej.

Rozwiązanie
1.Zauważmy, że dla *p*=2, tak nie jest ale dla *p*=3 tak jest ponieważ $1!+2!+3!=3^2$. Liczba *p*=3 jest jednak jedyną taką liczbą, że $1!+2!+3!+...+p!$ jest kwadratem liczby naturalnej.

2. Istotnie, zauważmy, że kwadrat liczby naturalnej musi kończyć się w zwykłym zapisie dziesiętnym jedną z cyfr 0,1,4,5,6,9 (wszystkie możliwości dla $k^2 \pmod{10}$) natomiast suma $1!+2!+3!+...+p!$ modulo 10 dla $p\geq 5$ jest równa 3 ponieważ $n!\pmod{10}=0$ dla każdego $n\geq 5$ oraz $1!+2!+3!+4!=33$.

3. Zatem liczby dla liczb pierwszych $p\geq 5$ liczby $(1!+2!+3!+...+p!)\pmod{10}$ i $k^2 \pmod{10}$ (dla dowolnego naturalnego $k\in N$) są różne a więc również różne są liczby $1!+2!+3!+...+p!$ oraz k^2. ■

Zadanie 7
Niech *p* będzie ustaloną liczbą pierwszą. Wykazać, że liczba naturalna $\underbrace{111...1}_{p\text{ cyfr}}\underbrace{222...2}_{p\text{ cyfr}}...\underbrace{999...9}_{p\text{ cyfr}}-123456789$ dzieli się przez *p*.

Rozwiązanie
1.Mamy wykazać, że dla dowolnej ustalonej liczby *p* mamy

$$\underbrace{111...1}_{p\text{ cyfr}}\underbrace{222...2}_{p\text{ cyfr}}...\underbrace{999...9}_{p\text{ cyfr}}-123456789\equiv 0 \ (\bmod p)$$

lub równoważnie

$$\underbrace{111...1}_{p\text{ cyfr}}\underbrace{222...2}_{p\text{ cyfr}}...\underbrace{999...9}_{p\text{ cyfr}}\equiv 123456789 \ (\bmod \mathrm{p}) \qquad (1)$$

Oznaczając liczbę $\underbrace{111...1}_{p\text{ cyfr}}\underbrace{222...2}_{p\text{cyfr}}...\underbrace{999...9}_{p\text{ cyfr}}$ przez *a* możemy kongruencje (1) zapisać również jako $\varphi_p(a)$ = 123456789, gdzie $Z \ni x \to \varphi_p(x)=[x]_p \in Z_p$ jest homomorfizmem pierścieni *Z* i Z_p a $[x]_p$ resztą z dzielenia *x* przez *p*.

Zauważmy, że ze wzoru na sumę postępu geometrycznego wynika, że

$$b_0 \overset{ozn}{=} \underbrace{999...9}_{p} = 9(10^{p-1} + 10^{p-2} + ... + 10^1 + 10^0) = 9\frac{10^p - 1}{9}$$

$$b_1 \overset{ozn}{=} \underbrace{888...8}_{p} = 8(10^{p-1} + 10^{p-2} + ... + 10^1 + 10^0 = 8\frac{10^p - 1}{9} \qquad (2)$$

.
.
.

$$b_8 \overset{ozn}{=} \underbrace{11...1}_{p} = 1(10^{p-1} + 10^{p-2} + ... + 10^1 + 10^0) = 1\frac{10^p - 1}{9}$$

zatem

$$a = b_8 \cdot 10^{8p} + b_7 \cdot 10^{7p} + ... + b_0 \cdot 10^0 =$$

$$= \frac{10^p - 1}{9} \cdot 10^{8p} + 2 \cdot \frac{10^p - 1}{9} \cdot 10^{7p} + 3 \cdot \frac{10^p - 1}{9} \cdot 10^{6p} + ... + 8 \cdot \frac{10^p - 1}{9} \cdot 10^p + 9 \cdot \frac{10^p - 1}{9} =$$

$$= \frac{10^p - 1}{9}(10^{8p} + 2 \cdot 10^{7p} + ... + 9 \cdot 10^0)$$

Zwróćmy uwagę, że $b_8 = \frac{10^p - 1}{9}$ jest liczbą naturalną.

2. Z małego twierdzenia Fermata mówiącego, że dla każdej liczby pierwszej p i dowolnej liczby całkowitej nie będącej wielokrotnością p mamy $a^{p-1} \equiv 1 \pmod{p}$ wynika, że

$$10^{p-1} \equiv 1 \pmod{p} \qquad (3)$$

ale również $$10 \equiv 10 \pmod{p} \qquad (4)$$

Mnożąc kongruencje (3) i (4) stronami dostajemy $10^p \equiv 10 \pmod{p}$ czyli $\varphi_p(10^p) = [10]_p$.
Zatem dla dowolnego $k \in N$ mamy (z mnożenia kongruencji stronami)

$$10^{kp} \equiv 10^k$$

a z własności homomorfizmu $\varphi_p : Z \to Z_p$

$$\varphi_p(10^{kp}) = [10]_p^k \text{ (potęgowanie mamy w } Z_p) \qquad (5)$$

Korzystając z (5) i własności homomorfizmu φ_p mamy dalej

$$\varphi_p(a) = \varphi_p(\frac{10^p - 1}{9} \cdot (10^{8p} + 2 \cdot 10^{7p} + ... + 9 \cdot 10^0)) =$$

$$= \varphi_p(\frac{10^p - 1}{9})(\varphi_p(10^{8p}) \oplus_p 2 \otimes_p \varphi_p(10^{7p}) \oplus_p ... \oplus 9 \otimes_p \varphi_p(10^0)) =$$

$$= \varphi_p(\frac{10^p - 1}{9})(1 \otimes [10]_p^8 \oplus_p 2 \otimes_p [10]_p^7 \oplus_p ... \oplus_p 9) =$$

$$= \varphi_p(\frac{10^p - 1}{9})\varphi_p(123456789) = \varphi_p(\frac{10^p - 1}{9} \cdot 123456789)$$

Chwyt jak w rachunku operatorowym: ”obłóż homomorfizmem φ_p, wykonaj działania po stronie Z_p i cofnij się do Z”.

3. Korzystając z własności homomorfizmu φ_p i z wyników punktu 2 mamy:

$$\varphi_p(a - 123456789) = \varphi_p(a) -_p \varphi_p(123456789) =$$

$$= \varphi_p(\frac{10^p - 1}{9} \cdot 123456789) -_p \varphi_p(123456789) =$$

$$= \varphi_p(\frac{10^p - 1}{9} \cdot 123456789 - 123456789) =$$

$$= \varphi_p(123456789 \cdot (\frac{10^p - 1}{9} - 1)) =$$

$$= \varphi_p(1234567879 \cdot \frac{10^p - 1}{9})$$

Zauważamy, że liczba 123456789 jest podzielna przez 9, ponieważ suma cyfr jest podzielna przez 9 (porównaj zadanie xx); zatem ze wzoru (2) dostajemy

$$\varphi(a - 123456789) = \varphi_p(\frac{123456789}{9} \cdot (10^p - 10)) = \varphi_p(\frac{123456789}{9})\varphi_p(10^p - 10) =$$

$$= \varphi_p(\frac{123456789}{9}) \cdot 0 = 0$$

Co kończy dowód.

Do rozwiązania zadania potrzebne nam były takie rzeczy:
- małe twierdzenie Fermata
- własności homomorfizmu $\varphi_p : Z \to Z_p$

wzór na sumę postępu geometrycznego. .■
-

Zadanie 2.8

Wyznaczyć 2 liczby sąsiadujące, z przecinkiem w rozwinięciu dziesiętnym liczby $(\sqrt{2}+\sqrt{3})^{1980}$.

Rozwiązanie

1. Zauważmy, że $(\sqrt{3}+\sqrt{2})(\sqrt{3}-\sqrt{3})=3-2=1$ oraz $\sqrt{3}+\sqrt{2}>3$ zatem $(\sqrt{2}+\sqrt{3})^{1980}$ to „ bardzo duża" liczba, większa od 3^{1980} a $(\sqrt{3}-\sqrt{2})^{1980}$ to „bardzo mała" liczba, mniejsza od $\frac{1}{3^{1980}}=\frac{1}{27^{405}}<\frac{1}{10^{405}}$.

Liczba $(\sqrt{2}+\sqrt{3})^{1980}$ ma więc co najmniej 405 zer (w zapisie dziesiętnym) za przecinkiem.

2.Oczywiście mamy

$$(\sqrt{2}+\sqrt{3})^{1980}=$$
$$=\underbrace{\binom{1980}{0}\sqrt{2}^{1980}+\binom{1980}{1}\sqrt{2}^{1980-1}\sqrt{3}+\binom{1980}{2}\sqrt{2}^{1980-2}\sqrt{3}^{2}+\ldots+\binom{1980}{1980}\sqrt{3}^{1980}}_{1981\ \ wyrazów}=a+b$$

$$(\sqrt{3}-\sqrt{2})^{1980}=\binom{1980}{0}\sqrt{2}^{1980}-\binom{1980}{1}\sqrt{2}^{1980-1}\sqrt{3}+\binom{1980}{2}\sqrt{2}^{1980-2}\sqrt{3}^{2}-\ldots+\binom{1980}{1980}\sqrt{3}^{1980}=a-b$$

gdzie
$$a=\sum_{i=1}^{990}\binom{1980}{2i}2\cdot 990-i\cdot 3$$
$$b=\sum_{i=1}^{990}\binom{1980}{2i-1}2^{(990-i)}3^{i-1}\sqrt{6}$$

3. Liczba a jest oczywiście liczbą naturalną. Obliczamy pierwszą cyfrę (od prawej strony) w dziesiętnym zapisie liczby a. Oczywiście jest ona równa $[a]_{10}$. Obliczamy $[a]_{10}$ czyli $\varphi_{10}(a)$.

Zauważamy, że $\varphi_{10}(2^k)$ dla $k\in N$ może być równe tylko 2,4,8,6 a $\varphi_{10}(3^k)$ dla $k\in N$ może być równe tylko 3,9,7,1 oraz $\varphi_{10}(2^k)=\varphi_{10}(2^{[k]4})$ i $\varphi_{10}(3^k)=\varphi_{10}(3^{[k]4})$

Zatem korzystając z własności homomorfizmu φ_{10} mamy

$$\varphi_{10}(2^{990-i}\cdot 3^i)=\varphi_{10}(2^{990-i})\otimes_{10}\varphi_{10}(3^i)=\varphi_{10}(2^{[990-i]4}\otimes_{10}\varphi_{10}(3^{[i]4})$$

Konkretnie dla $i=0$ $\varphi_{10}(2^{990})=\varphi_{10}(2^{[990]4})=\varphi_{10}(2^2)=4$

$i=990$ $\varphi_{10}(3^{990})=\varphi_{10}(3^{[990]4})=\varphi_{10}(3^2)=9$

Dla $i=1$ $\varphi_{10}(2^{990-1}\cdot 3)=\varphi_{10}(2^{989})\otimes_{10}\varphi_{10}(3)=2\otimes_{10}3=6$

$$i=2 \qquad \varphi_{10}(2^{990-2}\cdot 3^2)=\varphi_{10}(2^{988})\otimes_{10}\varphi_{10}(3^2)=6\otimes_{10}9=4$$
$$i=3 \qquad \varphi_{10}(2^{990-3}\cdot 3^3)=\varphi_{10}(2^{987})\otimes_{10}\varphi_{10}(3^3)=8\otimes_{10}7=6$$
$$i=4 \qquad \varphi_{10}(2^{990-4}\cdot 3^4)=\varphi_{10}(2^{986})\otimes_{10}\varphi_{10}(3^4)=4\otimes_{10}1=4$$

i oczywiście dla następnych *i* aż do *i* = 989 mamy tak samo, tzn.

$\varphi_{10}(2^{990-i}\cdot 3^i)=4$ dla i parzystych, a dokładnie *i*=0,2,...,988

$\varphi_{10}(2^{990-i}\cdot 3^i)=6$ dla i=1,3,...,989

Teraz po tych wstępnych obliczeniach możemy policzyć $\varphi_{10}(a)$

$$\varphi_{10}(a)=\varphi_{10}(\sum_{i=0}^{990}\binom{1980}{2i}2^{990-i}3^i)=\sum_{i=0}^{990}\binom{1980}{2i}\varphi_{10}(2^{990-i}3^i)$$ (sumowanie modulo 10)

UWAGA! Warto zwrócić uwagę na to, że wielokrotność elementu pierścienia *m·a* nie jest tym samym co mnożenie w pierścieniu *a·b.*

Sumowanie po prawej stronie oznacza sumowanie w Z_{10}, a mnożenie liczby $x\in Z_{10}$ przez liczbę naturalną k, czyli k oznacza: $k\cdot x\overset{df}{=}\underbrace{x\oplus_{10}x\oplus_{10}...\oplus x}_{k}$

Ogólne mnożenie dowolnego elementu pierścienia x ∈ p przez liczbę całkowitą, k ∈ *Z* definiujemy jako m x $\overset{df}{=}\underbrace{x+x+...+x}_{m}$ a ponadto zachodzą wzory *k(-x)=-kx*

(-k*x* to zapis –(kx))

Korzystając z faktu, że w Z_{10} -4=6 oraz w dowolnym pierścieniu dla każdego *m, n* ∈ Z i $x\in Z_{10}$ mamy *m(-x)=-mx, (m +n) x = m x + n x* dostajemy

$$\varphi_{10}(a)=\binom{1980}{0}\ 4\oplus_{10}\binom{1980}{2}6\oplus_{10}\binom{1980}{4}4\oplus_{10}...\oplus_{10}\binom{1980}{1978}6\oplus_{10}\binom{1980}{1980}9=$$
$$=\binom{1980}{0}4\oplus_{10}\binom{1980}{2}6\oplus_{10}\binom{1980}{4}4\oplus_{10}...\oplus_{10}\binom{1980}{1978}6\oplus_{10}\binom{1980}{1980}4\oplus_{10}5=$$
$$=\binom{1980}{0}4-_{10}\binom{1980}{2}4\oplus_{10}\binom{1980}{4}4-_{10}...-_{10}\binom{1980}{1978}4\oplus\binom{1980}{1980}4\oplus_{10}5=$$
$$=(\binom{1980}{0}-\binom{1980}{2}+\binom{1980}{4}-...-\binom{1980}{1978}+\binom{1980}{1980})4\oplus_{10}5$$

Obliczymy liczbę L

$$L\overset{df}{=}\binom{1980}{0}-\binom{1980}{2}+\binom{1980}{4}-...-\binom{1980}{1978}+\binom{1980}{1980}$$

Zauważmy, że:

$$(1+i)^{1980}=\binom{1980}{0}+\binom{1980}{1}i+\binom{1980}{2}i^2+\binom{1980}{3}i^3+\binom{1980}{4}i^4+...+\binom{1980}{1980}i^{1980}$$

Zatem L=Re $((1+i)^{1980}) = \binom{1980}{0} - \binom{1980}{2} + \binom{1980}{4} + \ldots + \binom{1980}{1980}$

Jednocześnie $(1+i)^{1990} = (\sqrt{2})^{1990}(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^{1990} = -2^{990}$

Zatem $\varphi_{10}(a) = -2^{990}4 \oplus_{10} 5 = 2^{990}6 \oplus_{10} 5$

Zauważmy, że w Z_{10} dodanie do siebie 5-ciu szóstek daje zero, zatem:

$2^{990}6 = \varphi_5(2^{990}) \cdot 6 = (\varphi_5(2))^{990}6$

gdzie podnoszenie do potęgi wykonywane jest w pierścieniu Z_5.

Obliczmy $(\varphi_5(2))^{990}$ w Z_5, zauważmy jednak, że w Z_5 mamy $2^1 = 2,\ 2^2 = 4, 2^3 = 3,\ 2^4 = 1$ zatem w Z_5 dostajemy $2^{990} = 2^{[990]4} = 2^2 = 4$

Zatem w Z_{10} $2^{990}6 = 4 \cdot 6 = 4$ (*)

Obliczmy teraz φ_{10}(a). Uwzględniając równość (*) dostrzegamy, że

$\varphi_{10}(a) = \varphi_5(2^{990})6 \oplus_{10} 5 = 4 \oplus_{10} 5 = 9$

zatem

$\varphi_{10}(a) = \binom{1980}{0}4 \oplus_{10} \binom{1980}{2}6 \oplus_{10} \binom{1980}{4}4 \oplus_{10} \ldots \oplus_{10} \binom{1980}{1978}6 \oplus_{10} \binom{1980}{1980}9 = 4 \oplus_{10} 9 = 3$

Istotnie, wszystkie liczby $\binom{1980}{2i}$ dla *i*=1,2,...,989 („cały środek wyrażenia”) podzielne są przez 5, a łatwo zauważyć, że:

$\underbrace{6 \oplus_{10} 6 \oplus_{10} 6 \oplus 6 \oplus 6}_{5} = 0$ oraz $\underbrace{4 \oplus_{10} 4 \oplus_{10} 4 \oplus_{10} 4 \oplus_{10} 4}_{5} = 0$

Stwierdziliśmy w punkcie 1, że liczby a i b są „prawie równe”, a ściślej a> b, a jest naturalna Oraz różnica a- b to liczba z co najmniej 400 zerami po przecinku; wynika stąd, że liczba po przecinku w b musi być 9, a liczba przed przecinkiem w b, liczbą o 1 mniejsza od pierwszej skrajnej cyfry w zapisie dziesiętnym liczby a.
Po dodaniu więc a i b:

a = ...9,00...
b = ...8,99...

dostajemy a+ b = ...7,9... czyli pierwsza cyfra przed przecinkiem w zapisie dziesiętnym liczby a + b = $(\sqrt{2}+\sqrt{3})^{1980}$ jest równa 7, a pierwsza za przecinkiem jest równa 9.

Drugi sposób rozwiązania zadania:

1. Początek taki jak w punkcie pierwszym sposobu pierwszego.

2. Zauważmy, że korzystając ze wzoru na dwumian Newtona mamy:

$$(\sqrt{2}+\sqrt{3})^{1980} = ((\sqrt{2}+\sqrt{3})^2)^{990} = (5+2\sqrt{6})^{990} =$$
$$= \binom{990}{0}5^{990} + \binom{990}{1}5^{990-1}\cdot(2\sqrt{6}) + \binom{990}{2}5^{990-2}(2\sqrt{6})^2 + \ldots + \binom{990}{989}5(2\sqrt{6})^{984} + \binom{990}{990}(2\sqrt{6})^{990} = a+b$$

gdzie

$$a = \sum_{i=0}^{495} \binom{990}{2i}5^{990-2i}\cdot 2^{2i}6^{i}$$

$$b = \sum_{i=1}^{494} \binom{990}{2i-1}5^{990-2i+1}\cdot 2^{2i-1}(\sqrt{6})^{2i-1}$$

i jednocześnie podobnie rozumując dla $(\sqrt{2}-\sqrt{3})^{1980}$ dostajemy $(\sqrt{2}-\sqrt{3})^{1980}$ = a – b

3. Obliczamy φ_{10}(a), korzystając z tego, że $\varphi_{10}: Z \to Z_{10}$ jest homomorfizmem

$$\varphi_{10}(a) = \varphi_{10}(\sum_{i=0}^{495} \binom{990}{2i}5^{90-2i}\cdot(4\cdot 6)^i) = \varphi_{10}(\sum_{i=0}^{495} \binom{990}{2i}25^{495-i}24^i) =$$
$$= \sum_{i=0}^{495} \binom{990}{2i}\varphi_{10}(25^{495-i}) \otimes_{10} \varphi_{10}(24^i) = \sum_{i=0}^{495} \binom{990}{2i}5^{495-i} \otimes_{10} 4^i \qquad (**)$$

4.Zauważmy, że w Z_{10} $5^{495} = 5$ (dowolna potęga 5^k dla $k \in N$ jest równa 5) oraz ponieważ w Z_{10} mamy $4^3 = 4$ zatem $4^{495} = 4^{[495]2} = 4$.

Jednocześnie w Z_{10} mamy $5 \otimes_{10} 4 = 0$, zatem wszystkie składniki w (**) oprócz „skrajnych” tzn. 5^{495} i 4^{495} są równe zero, zatem

$$\varphi_{10}(a) = \sum_{i=0}^{495} \binom{990}{2i}5^{495-i} \otimes_{10} 4^i = 5 \oplus_{10} 4 = 9$$

5.Rozumując identyczne jak w sposobie 1 rozwiązania zadania stwierdzamy, że przed przecinkiem w dziesiętnym zapisie liczby $(\sqrt{2}+\sqrt{3})^{1980}$ mamy cyfrę 7, a za przecinkiem 9.

Uwaga. Sposób drugi rozwiązania zadania jest nieco prostszy, bo nie musimy obliczać sumy

$$\binom{1980}{0} - \binom{1980}{2} + \binom{1980}{4} - \ldots + \binom{1980}{1980}$$

ale rozumowanie jest mniej naturalne. Łatwo wpaść na pomysł, by podnieść liczbę $(\sqrt{2}+\sqrt{3})$ do potęgi 1980, a trudniej, że lepiej byłoby najpierw obliczyć $(\sqrt{2}+\sqrt{3})^2$ a potem dopiero podnieść tę liczbę do potęgi 990. .■

Zadanie 9

Pokazać, że dla każdego $a,b \in Z$ mamy $NWD(a,b)\cdot NWW(a,b) = |ab|$

Rozwiązanie

Zauważmy, że $NWD(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdot p_2^{\min(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\min(\alpha_n,\beta_n)}$ oraz

$NWW(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdot p_2^{\max(\alpha_2,\beta_2)} \cdot \ldots \cdot p_n^{\max(\alpha_n,\beta_n)}$

$NWD(a,b)\cdot NWW(a,b) = |ab|$ zatem $NWD(a,b)\cdot NWW(a,b) = |ab|$

Zadanie 10

Pokazać, że jeśli *m, n* $\in Z$ czyli m i n są dowolnymi liczbami całkowitymi to

$$NWD(m, n) = 1 \text{ wtedy i tylko wtedy gdy } NWD\,([m]_n, n) = 1$$

Rozwiązanie:

Przeprowadzimy dowód nie wprost. Załóżmy, że $NWD\,([m]_n, n) \neq 1$, zatem istnieje takie $d \in Z,\ d > 1$, że:

$$[m]_n = k_1 \cdot d \qquad (1)$$

$$n = k_2 \cdot d \qquad (2)$$

dla pewnych $k_1, k_2 \in Z$.

Oczywiście dla pewnego $k \in Z$ mamy $m = [m]_n + k \cdot n$, zatem z (1) i (2) dostajemy

$$m = [m]_n + k \cdot n = k_1 d + k \cdot k_2 \cdot d \qquad (3)$$

Z (2) i (3) wynika, że liczby *m* i *n* są podzielne przez $d > 1$ co jest sprzeczne z założeniem, że *NWD (m, n) = 1*. ■

Zadanie 11

Znaleźć trzy ostatnie cyfry liczby 2^{1000}.

Rozwiązanie

Rozumujemy tak. Wyznaczenie trzech ostatnich cyfr sprowadza się do znalezienia trzycyfrowej liczby *n* takiej, że: $2^{1000} \equiv n \pmod{1000}$. Obliczamy kolejno:

$2^{10} \equiv 1024 \equiv 24 \pmod{1000}$

$2^{20} \equiv (2^{10})^{10} \equiv 24^2 \pmod{1000}$ czyli $2^{20} \equiv 576 \pmod{1000}$

$2^{40} \equiv (2^{20})^2 \equiv 576^2 = 3311776 \equiv 776 \pmod{1000}$

$2^{80} \equiv (2^{40})^2 \equiv 776^2 = 602176 \equiv 176 \pmod{1000}$

$2^{240} \equiv (2^{80})^3 \equiv 176^3 = 5451776 \equiv 776 \,(\mathrm{mod}\, 1000)$
$2^{480} \equiv (2^{240})^2 \equiv 776^2 = 602176 \equiv 176 \,(\mathrm{mod}\, 1000)$
$2^{500} \equiv 2^{480} \cdot 2^{20} \equiv 176 \cdot 576 = 101376 \,(\mathrm{mod}\, 1000)$
$2^{1000} \equiv 376^2 141376 \equiv 376 \,(\mathrm{mod}\, 1000)$
Ostatecznie 2^{1000} kończy się na 376 .■

Zadanie 12

Pokazać, że jeśli *NWD(a,n)*>1 to to teza twierdzenia Eulera $a^{\varphi(n)} \equiv 1 \,(\mathrm{mod}\, n)$ nie zachodzi.

Rozwiązanie

1. Niech $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, gdzie $p_i \neq p_j$ dla $i \neq j$ i $\alpha_i \in N$. Zauważmy, że z chińskiego twierdzenia o resztach wynika (por. zad. xx), że

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$$

wtedy i tylko wtedy, gdy dla każdego $i = 1,2,...,k$

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, p_i^{\alpha_i})$$

2. Wystarczy więc pokazać, że któraś z kongruencji $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, p_i^{\alpha_i})$ nie zachodzi.. Niech $d = NWD(a,n)$ i p_i dzieli d pokażemy, że

$$a^{\varphi(n)} \equiv 0 \,(\mathrm{mod}\, p_i^{\alpha_i})$$

Wystarczy w tym celu pokazać, że dla ustalonego α_i mamy:

$$(p_i)^{\varphi(p_i^{\alpha_i})} \equiv 0 \,(\mathrm{mod}\, p_i^{\alpha_i}) \qquad (*)$$

czyli

$$p_i p_i^{\alpha_i - 1}(p_i - 1) \equiv 0 \,(\mathrm{mod}\, p_i^{\alpha_i}) \qquad (**)$$

Jak łatwo sprawdzić $p_i^{\alpha_i - 1}(p_i - 1) \geq \alpha_i$. Wynika stąd, że lewa strona (**) jest wielokrotnością $p_i^{\alpha_i}$ a więc kongruencja (**) zachodzi. Podnosząc obie strony kongruencji (**) do potęgi α_i dostajemy $p_i^{\alpha_i p_i^{\alpha_i - 1}(p_i - 1)} \equiv 0 \pmod{p_i^{\alpha_i}}$. Mnożąc tę kongruencję stronami przez kongruencje postaci $p_j^{\alpha_j p_j^{\alpha_i - 1}(p_j - 1)} \equiv b_j \pmod{p_i^{\alpha_i}}$ dla $j \neq i$ i pewnych

$b_j \in Z$ dostajemy $a^{\varphi(n)} \equiv 0 \pmod{p_i^{\alpha_i}}$.

Uwaga. Zauważmy, że dowodzony fakt jest równoważny zdaniu: jeśli teza twierdzenia Eulera $a^{\varphi(m)} \equiv 1 \pmod{n}$ zachodzi, to $NWD(a,m) = 1$. Uzyskaliśmy zatem metodę sprawdzania czy liczby $a, m \in N$ są względnie pierwsze czy nie. Bezpośrednie obliczenie $NWD(a,m)$ szybką wersją algorytmu Euklidesa (np. tzw. algorytmem Steina) jest jednak znacznie szybsze i łatwiejsze do realizacji układowej. ■

Zadanie 2.13
Obliczyć $2^{10^6} \pmod{77}$ czyli $[2^{10^6}]_{77}$ lub co na jedno wychodzi 2^{10^6} w pierścieniu Z_{77}.

Rozwiązanie

1.Korzystając z twierdzenia Eulera (lub bezpośrednio wyników zadania xx), mamy: jeśli $a \in Z$ i $m \in N$ i $NWD\ (a,m)=1$ to $a^n \equiv a^{[n]_{\varphi(n)}} \pmod{m}$ lub $a^n = a^{[n]_{\varphi(n)}}$ w pierścieniu Z_m zatem ponieważ $NWD(2,77)=1$, więc mamy

$$2^{10^6} \equiv 2^{[10^6]_{\varphi(77)}} \pmod{77}$$

2.Obliczamy $\varphi(77) = \varphi(7 \cdot 11) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60$ a następnie obliczamy $10^6 \pmod{\varphi(77)}$, czyli w innej notacji $[10^6]_{\varphi(77)}$.

$$10^6 \pmod{\varphi(77)} = 10^6 \pmod{60} = 40$$

1. Musimy więc obliczyć $2^{40} \pmod{77}$.

$$2^{40} \pmod{77} = (2^8)^5 \pmod{77} = (256)^5 \pmod{77} =$$
$$= ([256]_{77})^5 \pmod{77} = 25^5 \pmod{77} = ((25)^2)^2 \cdot 25 \pmod{77} =$$
$$= ([625]_{77})^2 \cdot 25 \pmod{77} = 9^2 \cdot 25 \pmod{77} =$$
$$= 81 \cdot 25 \pmod{77} = [81]_{77} \cdot 25 \pmod{77} = 4 \cdot 25 \pmod{77} = 100 \pmod{77} = 23$$

Czyli ostatecznie $2^{10^6} \equiv 23 \pmod{77}$. Można również obliczyć $2^{40} \pmod{77}$ tak

$$2^{[10^6]_{60}} = 2^{40} = (2^{10})^4 = ([1024]_{77})^4 = 23^4 = 23^2 \otimes_{77} 23^2 = [529]_{77} \otimes_{77} [529]_{77} =$$
$$= (-10) \otimes_{77} (-10) = [100]_{77} = 23$$

4.Powyżej przeprowadzone obliczenia można nieco uprościć wykorzystując do obliczenia $2^{40} \pmod{77}$ chińskie twierdzenie o resztach. Z twierdzenia tego wynika, że $x = 2^{40} \pmod{77}$ jest jedynym rozwiązaniem w zbiorze <0,76> układu kongruencji

$x \equiv 2^{40} \pmod{7}$ (*)
$x \equiv 2^{40} \pmod{11}$ (**).

Do prawych stron kongruencji (*) i (**) można zastosować identyczną metodę postępowania jak poprzednio, otrzymując:

$$x \equiv 2^{40} \pmod{7} = 2^{[40]_{\varphi(7)}} \pmod{7}$$

i ponieważ $\varphi(7) = 6$ oraz $40 = 6 \cdot 6 + 4$ dostajemy

$$2^{[40]_{\varphi(7)}} \pmod{7} = 2^{[40]_6} \pmod{7} = 2^4 \pmod{7} = 2 .$$

W podobny sposób obliczamy $2^{40} \pmod{11}$.

$2^{40} \pmod{11} = 2^{[40]_{\varphi(11)}} \pmod{11}$ i ponieważ $\varphi(11) = 10$ oraz $40 = 3 \cdot 11 + 7$ mamy dalej $2^{[40]_{\varphi(11)}} \pmod{11} = 2^{[40]_{10}} \pmod{11} = 2^0 \pmod{11} = 1$. Zatem układ kongruencji (*) i (**) można zapisać następująco

$x \equiv 2 \pmod{7}$
$x \equiv 1 \pmod{11}$ (***)

Wiemy z chińskiego twierdzenia o resztach, że rozwiązanie układu kongruencji (***) jest jedyne w zbiorze <0,76>. Pierwszą kongruencję tego układu spełniają z tego zbioru liczby postaci $2 + k \cdot 7$ dla $k = 0,1,2,...,10$ czyli 2,9,16,23,30,37,44,51,58,65,75.

Drugą kongruencję tego układu spełniają ze zbioru <0,76> liczby postaci $1 + k \cdot 11$ dla $k = 0,1,2,...,6$ czyli 1,11,12,23,34,45,56,67. Widać, że liczba x= 23 jako jedyna spełnia obie kongruencje układu (***). Ostatecznie więc $10^{10^6} \pmod{77} = 2^{40} \pmod{77} = 23$.■

Zadanie 14
Znaleźć wszystkie rozwiązania następujących kongruencji:
1) $3x \equiv 4 \pmod 7$
2) $3x \equiv 4 \pmod{12}$
3) $9x \equiv 12 \pmod{21}$
4) $27x \equiv 25 \pmod{256}$
5) $27x \equiv 72 \pmod{900}$
6) $103x \equiv 612 \pmod{676}$

Rozwiązanie:
1. Jeśli $a \equiv b \pmod n$, to również $[a]_n \equiv [b]_n \pmod n$ (*). Jeśli pomnożymy obie strony kongruencji 1) przez 5, to dostajemy $15x \equiv 20 \pmod 7$ czyli korzystając z (*) $[x] \equiv 6 \pmod 7$ co daje następujące rozwiązanie kongruencji 1):
$x = 6 + k \cdot 7, \text{gdzie } k \in Z$

2. Łatwo sprawdzić, że kongruencja 2) nie ma rozwiązań, podstawiając x=0,1,2,...,11. Gdyby istniało $x \in Z$, dla którego kongruencja 2) byłaby prawdziwa, to istniałoby również $[x]_{12}$ spełniające tę kongruencję.

3. Jeśli mamy moduły $m_1, m_2, ..., m_n$ względnie pierwsza parami, to $a \equiv b \pmod{m_1, m_2, ..., m_n}$ wtedy i tylko wtedy $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}, ..., a \equiv b \pmod{m_n}$. Zatem kongruencja 3) równoważna jest 2 kongruencjom $9x \equiv 12 (\mathrm{mod}\, 7)$ i $9x \equiv 12 (\mathrm{mod}\, 3)$. Dla drugiej kongruencji rozwiązaniami są wszystkie całkowite $x \in Z$. Pierwsza natomiast jest równoważna kongruencji $2x \equiv 5 (\mathrm{mod}\, 7)$. Jeśli pomnożymy przez 4 obustronnie powyższą kongruencję, dostajemy $x \equiv 6 (\mathrm{mod}\, 7)$, czyli $x = 6 + k \cdot 7, \text{gdzie } k \in Z$. Ostatecznie więc rozwiązaniem kongruencji 6 są liczby $x = 6 + k \cdot 7, \text{gdzie } k \in Z$.

4. Sposób rozwiązania kongruencji 4 może być analogiczny jak w przypadku kongruencji 1. Ponieważ $NWD(27,256) = NWD(3 \cdot 9, 2^8) = 1$ można więc znaleźć element odwrotny do 27 w pierścieniu Z_{256}. Mnożąc obie strony kongruencji 4 przez ten element dostajemy rozwiązanie. W celu obliczenia elementu odwrotnego do 27 w pierścieniu Z_{256} możemy wykorzystać rozszerzony algorytm Euklidesa, znajdując takie liczby $a, k \in Z$, że $a \cdot 27 + k \cdot 256 = NWD(27,256) = 1$

5. Rozwiązanie pozostałych kongruencji pozostawiamy Czytelnikowi. .■

Zadanie 15

Udowodnić, że liczba naturalna jest podzielna przez 3 wtedy i tylko wtedy, gdy suma jej cyfr jest podzielna przez 3. Tak jest, jeśli liczba naturalna zapisana jest w zapisie wagowym z waga W =10, czyli w zapisie dziesiętnym. Dla jakich innych wag. W powyższe twierdzenie jest prawdziwe. Jak można warunek podzielności przez 3 sformułować dla zapisu trójkowego.

Rozwiązanie

1.Rozważmy liczbę $a = a_n a_{n-1} ... a_0$ (w zapisie dziesiętnym). Następujące kongruencje są równoważne.

$$a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... a_1 \cdot 10 + a_0 \equiv 0 \,(\mathrm{mod}\, 3) \quad (*)$$

$$[a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... a_1 \cdot 10 + a_0]_3 \equiv 0 \,(\mathrm{mod}\, 3)$$

$$[[a_n]_3 \cdot [10^n]_3 + [a_{n-1}]_3 \cdot [10^{n-1}]_3 + ... + [a_0]_3] \equiv 0 \,(\mathrm{mod}\, 3)$$

$$[[a_n]_3 + [a_{n-1}]_3 + ... + [a_0]_3]_3 \equiv 0 \,(\mathrm{mod}\, 3)$$

ponieważ $[10^k]_3 = \underbrace{[10]_3 \cdot ... \cdot [10]_3}_{k} = 1$

$$[a_n + a_{n-1} + ... + a_0]_3 \equiv 0 \pmod 3$$

$$a_n + a_{n-1} + ... + a_0 \equiv 0 \,(\mathrm{mod}\, 3) \quad (**)$$

Kongruencja (*) jest równoważna stwierdzeniu, że liczba a jest podzielna przez 3, a kongruencja (**), że suma jej cyfr dziesiętnych jest podzielna przez 3.

2. Widać, że istotę w powyższym rozumowaniu stanowi fakt, że $[10]_3 = 1$. Zatem analogiczny dowód można przeprowadzić dla wag postaci $W = k \cdot 3 + 1$, gdzie $k \in N$, gdyż dla tych wag mamy $[W]_3 = 1$.

3. W przypadku zapisu trójkowego czyli W=3 warunkiem koniecznym i dostatecznym podzielności przez 3 jest zero na najmniej znaczącej pozycji. Ogólniej w przypadku, gdy $W = k \cdot 3$, gdzie $k \in N$ warunkim koniecznym i dostatecznym podzielności przez 3 jest podzielność przez 3 liczby na najmniej znaczącej pozycji. ■

Zadanie 16
Udowodnić następujący warunek podzielności przez 9. Liczba naturalna jest podzielna przez 9, wtedy i tylko wtedy, gdy suma jej cyfr podzielna jest przez 9. Tak jest w zapisie dziesiętnym tzn. w zapisie z wagą *W*=10. Dla jakich innych wag $W \geq 2$ powyższy fakt jest prawdziwy.

Rozwiązanie
1. Przeprowadzamy dla liczby $a = a_n, a_{n-1}, a_{n-2}, ..., a_0$ (w zapisie dziesiętnym) takie samo rozumowanie jak w zadaniu xx zastępując kongruencję mod 3, kongruencjami mod 9 i zastępując homomorfizm $Z \ni x \to [x]_3 \in Z_3$ homomorfizmem $Z \ni x \to [x]_9 \in Z_9$. Istotę stanowi w tym rozumowaniu równość $[10]_9 = 1$.
2. Rozumowanie z punktu 1 pozostaje niezmienione, jeśli wagi są postaci $W = k \cdot 9 + 1$, gdzie $k \in N$, ponieważ dla tych wag mamy $[W]_9 = 1$. ■

Zadanie 17
Udowodnić następujące twierdzenie, tzw. twierdzenie Wilsona. Jeśli *p* jest liczbą pierwszą, to $(p-1)! \equiv -1 \pmod{p}$.

Rozwiązanie
Twierdzenie Wilsona jest prostym wnioskiem z małego twierdzenia Fermata. Z małego twierdzenia Fermata wynika bowiem, że liczby $1,2,..., p-1$ są pierwiastkami równania $x^{p-1} -_p 1 = 0$ w ciele Z_p, gdzie $-_p$ oznacza odejmowanie modulo *p* (lub co na jedno wychodzi rozwiązaniami kongruencji $x^{p-1} - 1 \equiv 0 \pmod{p}$). Zatem z twierdzenia Bezout dla ciała Z_p dostajemy:

$$x^{p-1} -_p 1 = (x -_p 1) \otimes_p (x -_p 2) \otimes_p ... \otimes_p (x -_p (p-1))$$

Porównując wyrazy wolne dostajemy: $-1 = [(-1)^{p-1} \cdot (p-1)!]_p$

Zatem $(p-1)! \equiv -1 \pmod{p}$

Uwaga. Zauważmy, że twierdzenie Wilsona podaje pewną charakterystykę liczb pierwszych. Dokładniej , niech $N_0 \in N, N_0 > 1$ wówczas:

liczba N_0 jest pierwsza wtedy i tylko wtedy gdy $(N_0 - 1)! \equiv -1 \pmod{N_0}$.

Istotnie, jeśli liczba $N_0 \in N, N_0 > 1$ nie jest pierwsza, to $N_0 = mn$ dla pewnych $m, n \in < 2, N_0 - 1 >$ zatem *m* i *n* dzielą N_0 oraz $(N_0 - 1)!$ skąd $(N_0 - 1)! \equiv 0 \pmod{N_0}$, a więc kongruencja $(N_0 - 1)! \equiv -1 \pmod{N_0}$ nie zachodzi.

Jednak charakteryzacja liczb pierwszych podana w twierdzeniu Wilsona nie ma praktycznego znaczenia przy badaniu pierwszości liczby N_0, ponieważ nie jest znany algorytm szybkiego obliczania liczby N_0, np. w log N_0 krokach. .■

Zadanie 18

Pokazać, że jeśli $NWD(a,n)=1$ (czyli $a,n\in N$ są względnie pierwsze) to z faktu, że $ax\equiv ay\,(\mathrm{mod}\,n)$ wynika, że $x\equiv y\,(\mathrm{mod}\,n)$.

Krótko: kongruencje można dzielić obustronnie przez element względnie pierwszy z n. Znaleźć taki przykład, że $ax\equiv ay\,(\mathrm{mod}\,n)$ a kongruencja $x\equiv y\,(\mathrm{mod}\,n)$ nie zachodzi.

Rozwiązanie

1.Jeśli $NWD(a,n)=1$, to jak wynika z rozszerzonego algorytmu Euklidesa istnieją takie liczby $a',k'\in Z$, że

$$a'\cdot a+k'\cdot n=NWD(a,n)=1 \qquad (*).$$

2.Kongruencja $ax\equiv ay\,(\mathrm{mod}\,n)$ jest równoważna równości $ax-ay=k\cdot n$ dla pewnego $k\in Z$ lub równości $a(x-y)=k\cdot n$ dla pewnego $k\in Z$. Pomnóżmy obie strony ostatniej równości przez $a'\in Z$ z p. 1. dostajemy wówczas

$$a'a(x-y)=a'k\cdot n$$

Z równości (*) mamy teraz $a'a=1-k'n$ i dalej $(1-k'n)(x-y)=a'k\cdot n$, zatem $x-y=k'(x-y)\cdot n+a'k\cdot n$, a więc $x\equiv y\,(\mathrm{mod}\,n)$.

3.Przykład jest następujący $3\cdot 4\equiv 3\cdot 8\,(\mathrm{mod}\,12)$ i oczywiście kongruencja $4\equiv 8\,(\mathrm{mod}\,12)$ nie zachodzi.■