MAŁE TWIERDZENIE FERMATA

Lemat. Jeśli p jest liczbą pierwszą oraz $0 < k < p$, to

$$p \mid \binom{p}{k}. \quad \spadesuit$$

Lemat. Jeśli p jest liczbą pierwszą, to

$$(a+b)^p \equiv a^p + b^p \pmod{p}. \quad \spadesuit$$

Twierdzenie 1. Jeśli p jest liczbą pierwszą, to

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

Dowód. Indukcja względem a.
- $a = 1$ — oczywiste;
- krok indukcyjny:

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}. \quad \spadesuit$$

Wniosek. Jeśli p jest liczbą pierwszą, to każda liczba $a \in \mathbb{Z}_p$ jest pierwiastkiem wielomianu $X^p - X$.

TWIERDZENIE LAGRANGE'A

Twierdzenie 2. Wielomian stopnia n ma co najwyżej n pierwiastków w ciele $\mathbb{Z}_p$ (uwzględniając krotności pierwiastków).

Dowód. Niech r będzie pierwiastkiem wielomianu $W(X)$ stopnia n. Wtedy

$$W(X) = (X - r) \cdot V(X),$$

gdzie $V(X)$ jest wielomianem stopnia $n-1$. Każdy pierwiastek wielomianu $V(X)$ jest też pierwiastkiem wielomianu $W(X)$. Wybieramy dowolny pierwiastek s wielomianu $V(X)$ i otrzymujemy

$$W(X) = (X - r)(X - s) \cdot U(X),$$

gdzie $U(X)$ jest wielomianem stopnia $n - 2$. I tak dalej... $\spadesuit$

Wniosek. W ciele $\mathbb{Z}_p$ każdy pierwiastek wielomianu $X^p - X$ jest pierwiastkiem jednokrotnym. $\spadesuit$

ROZWIĄZYWANIE KONGRUENCJI

(1) Umiemy już rozwiązywać kongruencje liniowe.

(2) Umiemy też stwierdzić, czy kongruencja kwadratowa

$$x^2 \equiv a \pmod{p}$$

ma rozwiązanie, gdy p jest liczbą pierwszą.

(3) Teraz chcemy nauczyć się **rozwiązywać**

(3a) najpierw kongruencje kwadratowe,
(3b) a potem kongruencje wyższych stopni.

Fakt. Problem
- **dane:** liczby całkowite dodatnie a, b, c;
- **pytanie:** czy istnieje liczba całkowita dodatnia $x < c$ taka, że

$$x^2 \equiv a \pmod{b}$$

jest problemem NP-zupełnym. (Manders, Adleman, 1978)

OBLICZANIE PIERWIASTKÓW KWADRATOWYCH

Dana jest liczba pierwsza p oraz liczba całkowita a taka, że

$$\left(\frac{a}{p}\right) = 1.$$

Chcemy znaleźć liczbę d taką, że

$$d^2 \equiv a \pmod{p}.$$

Przypomnienie: jeśli $p \equiv 3 \pmod{4}$, to wystarczy przyjąć

$$d = a^{\frac{p+1}{4}} \,\mathbf{mod}\, p.$$

Jeśli $p \equiv 5 \pmod{8}$, to też łatwo znajdujemy rozwiązanie. Wiemy, że

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Zatem

$$a^{\frac{p-1}{4}} \equiv \pm 1 \pmod{p}.$$

Mamy dwa przypadki.

Przypadek 1.

$$a^{\frac{p-1}{4}} \equiv 1 \pmod{p}.$$

Wtedy kładziemy

$$d = a^{\frac{p+3}{8}} \mathbin{\mathbf{mod}} p$$

i otrzymujemy

$$d^2 \equiv a^{\frac{p+3}{4}} = a^{\frac{p-1}{4}} \cdot a \equiv a \pmod{p}.$$

Przypadek 2.

$$a^{\frac{p-1}{4}} \equiv -1 \pmod{p}.$$

Wtedy kładziemy

$$d = 2a \cdot (4a)^{\frac{p-5}{8}} \mathbin{\mathbf{mod}} p.$$

Ponieważ $p \equiv 5 \pmod{8}$, więc

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

czyli

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Zatem

$$d^2 \equiv 4a^2 \cdot (4a)^{\frac{p-5}{4}} = \ldots = 2^{\frac{p-1}{2}} \cdot a^{\frac{p+3}{4}} = 2^{\frac{p-1}{2}} \cdot a^{\frac{p-1}{4}} \cdot a \equiv (-1) \cdot (-1) \cdot a = a \pmod{p}.$$

Pozostaje przypadek najtrudniejszy, gdy

$$p \equiv 1 \pmod{8}.$$

Przypominamy:

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

(1) Znajdujemy nieresztę n modulo p. Mamy wtedy

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

czyli

$$n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

(2) Kładziemy

$$e := 0; \quad w := \frac{p-1}{2}, \quad b := 2.$$

Wtedy

$$2 \mid e, \quad w = \frac{p-1}{b}, \quad a^w \equiv n^{ew} \pmod{p}.$$

(3) Dopóki $2 \mid w$ powtarzaj:

$w := w \,\mathbf{div}\, 2$
jeśli $a^w \not\equiv n^{ew} \pmod{p}$, **to** $e := e + b$
$b := 2b$

Warunek

$$2 \mid e, \quad w = \frac{p-1}{b}, \quad a^w \equiv n^{ew} \pmod{p}$$

jest niezmiennikiem pętli.

Jest oczywiste, że

$$2 \mid e, \quad w = \frac{p-1}{b}.$$

Niech e, w, b na początku pętli takie, że

$$w = \frac{p-1}{b}, \quad a^w \equiv n^{ew} \pmod{p}.$$

Niech

$$w' = \frac{w}{2}.$$

Wtedy

$$a^{2w'} \equiv n^{2ew'} \pmod{p}.$$

Stąd albo

$$a^{w'} \equiv n^{ew'} \pmod{p}$$

i wtedy kładziemy $e' = e$, albo

$$a^{w'} \equiv -n^{ew'} \pmod{p}$$

i wtedy kładziemy $e' = e + b$.

W tym przypadku

$$n^{e'w'} = n^{(e+b)w'} = n^{ew'} \cdot n^{bw'}.$$

Ale $bw = p - 1$, skąd

$$bw' = \frac{p-1}{2}.$$

Zatem

$$n^{bw'} = n^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Stąd

$$n^{e'w'} \equiv -n^{ew'} \pmod{p},$$

czyli

$$a^{w'} \equiv n^{e'w'} \pmod{p}.$$

W obu przypadkach mamy więc

$$a^{w'} \equiv n^{e'w'} \pmod{p},$$

co kończy dowód niezmiennika.

Teraz liczba w jest nieparzysta. Kładziemy

$$c := a \cdot n^{-e}$$

oraz

$$d := n^{\frac{e}{2}} \cdot c^{\frac{w+1}{2}}$$

w ciele $\mathbb{Z}_p$. Wówczas

$$\begin{aligned} d^2 &= n^e \cdot c^{w+1} = n^e \cdot a^{w+1} \cdot n^{-e(w+1)} = \\ &= n^e \cdot a^{w+1} \cdot n^{-ew-e} = n^{-ew} \cdot a^{w+1} = n^{-ew} \cdot a^w \cdot a \equiv \\ &\equiv n^{-ew} \cdot n^{ew} \cdot a = a \pmod{p}. \end{aligned}$$

PRZYKŁAD

Niech $p = 113$. Wtedy $p - 1 = 2^4 \cdot 7$. Znajdujemy niereszt̨ę n modulo 113:

$$\left(\frac{3}{113}\right) = \left(\frac{113}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

więc możemy przyjąć $n = 3$. Niech wreszcie $a = 13$. Wtedy

$$\left(\frac{13}{113}\right) = \left(\frac{113}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{3^2}{13}\right) = 1,$$

więc a jest resztą kwadratową modulo 113. Szukamy liczby d takiej, że

$$d^2 \equiv 13 \pmod{113}.$$

Przyjmujemy

$$e = 0, \quad w = 56, \quad b = 2.$$

Wtedy

$$13^{56} \equiv 1 \pmod{113}$$

oraz

$$3^0 \equiv 1 \pmod{113},$$

czyli

$$13^w \equiv n^{ew} \pmod{113}.$$

Krok 1. Przyjmujemy
$$w = 56\,\mathbf{div}\,2 = 28.$$
Wtedy
$$13^{28} \equiv -1 \pmod{113}$$
oraz
$$3^{0} \equiv 1 \pmod{113}.$$
Zatem
$$13^{w} \not\equiv 3^{ew} \pmod{113},$$
więc kładziemy $e = 0 + b = 2$. Wreszcie kładziemy $b = 4$.

Krok 2. Przyjmujemy
$$w = 28\,\mathbf{div}\,2 = 14.$$
Wtedy
$$13^{14} \equiv 15 \pmod{113}$$
oraz
$$3^{28} \equiv 98 \pmod{113}.$$
Zatem
$$13^{w} \not\equiv 3^{ew} \pmod{113},$$
więc kładziemy $e = 2 + b = 6$. Wreszcie kładziemy $b = 8$.

Krok 3. Przyjmujemy
$$w = 14\,\mathbf{div}\,2 = 7.$$
Wtedy
$$13^{7} \equiv 69 \pmod{113}$$
oraz
$$3^{42} \equiv 69 \pmod{113}.$$
Zatem
$$13^{w} \equiv 3^{ew} \pmod{113},$$
więc pozostawiamy $e = 6$ bez zmian. Wreszcie kładziemy $b = 16$. Liczba w jest już nieparzysta, więc kończymy pętlę.

Teraz
$$3^{-1}\,\mathbf{mod}\,113 = 38,$$
skąd otrzymujemy
$$3^{-6}\,\mathbf{mod}\,113 = 82.$$
Zatem
$$c = a \cdot n^{-e} = 13 \cdot 82\,\mathbf{mod}\,113 = 49.$$
Wreszcie
$$d = n^{\frac{e}{2}} \cdot c^{\frac{w+1}{2}} = 3^{3} \cdot 49^{4}\,\mathbf{mod}\,113 = 37.$$

Łatwo sprawdzamy, że

$$37^2 \equiv 13 \pmod{113}.$$

Mamy zatem dwa pierwiastki z 13 modulo 113: 37 oraz 76.

KONGRUENCJE KWADRATOWE

Rozwiążemy kongruencję kwadratową

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

gdzie p jest liczbą pierwszą nieparzystą.

Zakładamy oczywiście, że a nie dzieli się przez p.

Zatem mnożąc obie strony kongruencji przez $4a$ otrzymamy kongruencję równoważną:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}.$$

Następnie dodajemy i odejmujemy b^2 i wprowadzamy oznaczenie $\Delta = b^2 - 4ac$:

$$4a^2x^2 + 4abx + b^2 - b^2 + 4ac \equiv 0 \pmod{p},$$

czyli

$$(2ax + b)^2 \equiv \Delta \pmod{p}.$$

Teraz mamy trzy przypadki.

Przypadek 1. Δ jest resztą kwadratową modulo p. Wtedy istnieje liczba d taka, że

$$d^2 \equiv \Delta \pmod{p}.$$

Wtedy albo

$$2ax + b \equiv d \pmod{p},$$

albo

$$2ax + b \equiv -d \pmod{p}.$$

Stąd otrzymujemy dwa pierwiastki:

$$x = (-b + d) \cdot (2a)^{-1} \quad \text{oraz} \quad x = (-b - d) \cdot (2a)^{-1}$$

w ciele $\mathbb{Z}_p$.

Przypadek 2. $\Delta \equiv 0 \pmod{p}$. Wtedy

$$(2ax+b)^2 \equiv 0 \pmod{p},$$

czyli

$$2ax+b \equiv 0 \pmod{p}.$$

Kongruencja ma jeden pierwiastek

$$x = (-b) \cdot (2a)^{-1}$$

w ciele $\mathbb{Z}_p$.

Przypadek 3. Δ jest nieresztą kwadratową modulo p. Wtedy kongruencja

$$ax^2+bx+c \equiv 0 \pmod{p}$$

nie ma rozwiązania.

ROZWIĄZYWANIE KONGRUENCJI WYŻSZYCH STOPNI

Rozwiążemy kongruencję

$$x^5+10x^4+2x^3+8x^2+7x+10 \equiv 0 \pmod{3773}.$$

Oznaczmy

$$W(x) = x^5+10x^4+2x^3+8x^2+7x+10.$$

Najpierw rozkładamy na czynniki liczbę 3773:

$$3773 = 343 \cdot 11 = 7^3 \cdot 11.$$

Kongruencja

$$W(x) \equiv 0 \pmod{3773}$$

jest równoważna układowi kongruencji

$$\begin{cases} W(x) \equiv 0 \pmod{7^3} \\ W(x) \equiv 0 \pmod{11} \end{cases}$$

Rozwiążemy każdą z tych kongruencji osobno. Najpierw zajmiemy się kongruencją

$$x^5+10x^4+2x^3+8x^2+7x+10 \equiv 0 \pmod{11}.$$

Pokażemy na tym przykładzie algorytm ogólny rozwiązywania kongruencji modulo p, gdzie p jest liczbą pierwszą.

Najpierw znajdujemy (za pomocą algorytmu Euklidesa)

$$\mathrm{NWD}(W(x), x^p - x),$$

czyli w naszym przypadku

$$\mathrm{NWD}(x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10, x^{11} - x).$$

Otóż

$$\begin{aligned}
&(x^{11} - x) : (x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10) = \\
&\qquad\qquad (x^6 + x^5 + 10x^4 + 9x^2 + 1) \ \text{ r. } \ (5x^4 + x^3 + x^2 + 3x + 1), \\
&(x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10) : (5x^4 + x^3 + x^2 + 3x + 1) = \\
&\qquad\qquad (9x + 9) \ \text{ r. } \ (6x^3 + 5x^2 + 4x + 1), \\
&(5x^4 + x^3 + x^2 + 3x + 1) : (6x^3 + 5x^2 + 4x + 1) = (10x + 1) \ \text{ r. } \ 0.
\end{aligned}$$

Zatem

$$\mathrm{NWD}(x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10, x^{11} - x) = 6x^3 + 5x^2 + 4x + 1.$$

Po podzieleniu (w $\mathbb{Z}_{11}$) przez 6 otrzymamy:

$$\mathrm{NWD}(x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10, x^{11} - x) = x^3 + 10x^2 + 8x + 2.$$

Teraz wielomian $W(x)$ zastępujemy wielomianem

$$V(x) = x^3 + 10x^2 + 8x + 2.$$

Z własności wielomianu $x^{11} - x$ wynika, że wielomiany $W(x)$ i $V(x)$ mają te same pierwiastki w ciele $\mathbb{Z}_{11}$, z tym tylko, że wielomian $V(x)$ ma wyłącznie pierwiastki jednokrotne. Krotności pierwiastków wielomianu $W(x)$ można już łatwo wyznaczyć.

Jeśli stopień wielomianu $V(x)$ jest równy 1 lub 2, to kongruencję

$$V(x) \equiv 0 \pmod{p}$$

rozwiązujemy za pomocą znanych metod.

Jeśli stopień wielomianu $V(x)$ jest równy co najmniej 3, to losujemy liczbę a i znajdujemy

$$D(x) = \mathrm{NWD}((x + a)^{\frac{p-1}{2}} - 1, V(x)).$$

Przypuśćmy, że x jest pierwiastkiem wielomianu $V(x)$ oraz $x + a$ jest resztą kwadratową modulo p. Wtedy x jest też pierwiastkiem wielomianu

$$(x + a)^{\frac{p-1}{2}} - 1,$$

a zatem jest też pierwiastkiem otrzymanego największego wspólnego dzielnika $D(x)$.

Przypuśćmy teraz, że x jest pierwiastkiem wielomianu $V(x)$ oraz $x+a$ jest nieresztą kwadratową modulo p. Wtedy x nie jest pierwiastkiem wielomianu

$$(x+a)^{\frac{p-1}{2}}-1,$$

a zatem nie jest też pierwiastkiem $D(x)$.

Zauważmy, że dla losowo wybranej liczby a prawdopodobieństwo tego, że dla każdego pierwiastka x wielomianu $V(x)$ liczba $x+a$ jest resztą kwadratową modulo p (lub że dla każdego takiego x liczba $x+a$ jest nieresztą) jest w przybliżeniu równe 2^{-n}, gdzie n jest stopniem wielomianu $V(x)$.

Zatem istnieje duża szansa na to, że po pewnym czasie wylosujemy taką liczbę a, że dla niektórych pierwiastków x liczby $x+a$ są resztami kwadratowymi modulo p, a dla innych są nieresztami. Wtedy otrzymany największy wspólny dzielnik $D(x)$ jest dzielnikiem właściwym wielomianu $V(x)$.

W takim przypadku wywołujemy rekurencyjnie procedurę znajdowania pierwiastków oddzielnie dla wielomianu $D(x)$ i dla wielomianu $V(x):D(x)$.

Zauważmy, że dla małych liczb p opłaca się przeszukać całe ciało $\mathbb{Z}_p$. Zatem ten algorytm będziemy stosować przede wszystkim wtedy, gdy liczba p jest duża i stopień wielomianu $W(x)$ (a zatem i $V(x)$) jest mały. Wtedy opłaca się wyznaczać największy wspólny dzielnik

$$D(x)=\mathrm{NWD}(x^{\frac{p-1}{2}}-1, V(x+a))$$

i rozkładać w ten sposób na czynniki wielomian $V(x+a)$. Rozkład wielomianu $V(x)$ otrzymujemy wtedy przez podstawienie $x-a$ w miejsce x.

PRZYKŁAD

Przypominamy, że

$$V(x)=x^3+10x^2+8x+2.$$

Niech $a=2$. Wtedy

$$V(x+2)=x^3+5x^2+5x=x\cdot(x^2+5x+5).$$

Wtedy oczywiście

$$V(2)=0,$$

czyli $x=2$ jest pierwiastkiem wielomianu $V(x)$. Ponieważ

$$(x^5-1):(x^2+5x+5)=x^3+6x^2+9x+2,$$

więc oba pozostałe pierwiastki wielomianu $V(x)$ są resztami kwadratowymi modulo 11 lub oba są nieresztami kwadratowymi modulo 11.

Niech $a = 3$. Wtedy

$$V(x+3) = x^3 + 8x^2 + 7x = x \cdot (x^2 + 8x + 7).$$

Wtedy oczywiście

$$V(3) = 0,$$

czyli $x = 3$ jest pierwiastkiem wielomianu $V(x)$. Ponieważ

$$(x^5 - 1) : (x^2 + 8x + 7) = (x^3 + 3x^2 + 2x + 7) \ \text{ r. } \ (7x + 5)$$

oraz

$$(x^2 + 8x + 7) : (7x + 5) = 8x + 8,$$

więc otrzymujemy rozkład

$$x^2 + 8x + 7 = (7x + 5)(8x + 8),$$

czyli

$$x^2 + 8x + 7 = (x + 7)(x + 1).$$

Zatem

$$V(x+3) = x(x+1)(x+7),$$

skąd łatwo otrzymujemy pierwiastki wielomianu $V(x)$:

$$x = 2, \quad x = 3, \quad x = 7.$$

Niech $a = 4$. Wtedy

$$V(x+4) = x^3 + 4x + 5.$$

Ponieważ

$$(x^5 - 1) : (x^3 + 4x + 5) = (x^2 + 7) \ \text{ r. } \ (6x^2 + 5x + 8)$$

oraz

$$(x^3 + 4x + 5) : (6x^2 + 5x + 8) = 2x + 2,$$

więc otrzymujemy rozkład

$$x^3 + 4x + 5 = (6x^2 + 5x + 8)(2x + 2) = (x^2 + 10x + 5)(x + 1).$$

Rozkładając trójmian kwadratowy na czynniki otrzymujemy

$$V(x+4) = (x+1)(x+2)(x+8),$$

skąd łatwo dostajemy pierwiastki wielomianu $V(x)$:

$$x = 2, \quad x = 3, \quad x = 7.$$

Niech $a = 7$. Wtedy

$$V(x + 7) = x(x^2 + 9x + 9).$$

Jednym pierwiastkiem jest 7. Mamy też

$$\mathrm{NWD}(x^5 - 1, x^2 + 9x + 9) = 1,$$

więc nie otrzymujemy dalszego rozkładu.

Niech $a = 9$. Wtedy

$$\mathrm{NWD}(x^5 - 1, V(x + 9)) = V(x + 9),$$

więc to losowanie zakończyło się całkowitym niepowodzeniem.

Teraz rozwiązujemy kongruencję

$$x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10 \equiv 0 \pmod{7}.$$

Nie będziemy powtarzać tu rozumowania takiego jak w przypadku modułu 11; zauważmy od razu, że pierwiastkami są liczby 4 i 5.

Pokażemy, w jaki sposób z tych dwóch pierwiastków możemy otrzymać pierwiastki kongruencji

$$x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10 \equiv 0 \pmod{343}$$

(przypominamy, że $343 = 7^3$).

Twierdzenie 3. Niech

$$W(x) = a_n x^n + \ldots + a_1 x + a_0$$

będzie wielomianem o współczynnikach całkowitych. Wtedy istnieje wielomian $r(x, h)$ o współczynnikach całkowitych taki, że

$$W(x + h) = W(x) + W'(x) \cdot h + r(x, h) \cdot h^2.$$

Zamiast dowodu. Tezę możemy uzyskać łatwo ze wzoru Taylora lub rozwijając każde wyrażenie postaci

$$(x + h)^k$$

ze wzoru dwumianowego Newtona i grupując następnie wyrazy zawierające h i wyrazy zawierające h^i dla $i \geq 2$. ♠

LEMAT HENSLA

Twierdzenie 4. Niech p będzie liczbą pierwszą i niech $W(x)$ będzie wielomianem stopnia n o współczynnikach całkowitych. Załóżmy, że współczynnik stojący przy najwyższej potędze x nie jest podzielny przez p (czyli wielomian $W(x)$ jest wielomianem stopnia n w $\mathbb{Z}_p[x]$). Jeśli istnieje liczba całkowita x_1 taka, że

$$W(x_1) \equiv 0 \pmod{p}$$

oraz

$$W'(x_1) \not\equiv 0 \pmod{p},$$

to dla każdej liczby $k \geq 2$ istnieje liczba całkowita x_k taka, że

$$W(x_k) \equiv 0 \pmod{p^k}$$

oraz

$$x_k \equiv x_{k-1} \pmod{p^{k-1}}.$$

Dowód. Indukcja względem k. Najpierw konstruujemy x_2. Szukamy x_2 w postaci

$$x_2 = x_1 + pt$$

dla pewnej liczby całkowitej t. Z poprzedniego twierdzenia wynika, że

$$W(x_1 + pt) = W(x_1) + W'(x_1) \cdot pt + r(x_1, pt) \cdot p^2$$

dla pewnego wielomianu $r(x, y)$ o współczynnikach całkowitych. Zatem

$$W(x_1 + pt) \equiv W(x_1) + W'(x_1) \cdot pt \pmod{p^2}.$$

Stąd wynika, że

$$W(x_1 + pt) \equiv 0 \pmod{p^2}$$

wtedy i tylko wtedy, gdy

$$W(x_1) + W'(x_1) \cdot pt \equiv 0 \pmod{p^2}.$$

Wiemy jednak, że

$$W(x_1) \equiv 0 \pmod{p}.$$

Zatem $W(x_1)$ dzieli się przez p. Stąd wynika, że kongruencja

$$W(x_1) + W'(x_1) \cdot pt \equiv 0 \pmod{p^2}$$

jest równoważna kongruencji

$$\frac{W(x_1)}{p} + W'(x_1) \cdot t \equiv 0 \pmod{p}.$$

Ta kongruencja ma zaś dokładnie jedno rozwiązanie modulo p, gdyż liczba $W'(x_1)$ nie dzieli się przez p. Rozwiązując tę kongruencję znajdujemy t, a następnie

$$x_2 = x_1 + pt.$$

Następnie szukamy x_3 w postaci

$$x_3 = x_2 + p^2 t$$

dla pewnej liczby całkowitej t. Tak jak poprzednio

$$W(x_2 + p^2 t) = W(x_2) + W'(x_2) \cdot p^2 t + r(x_2, p^2 t) \cdot p^4$$

dla pewnego wielomianu $r(x, y)$ o współczynnikach całkowitych.

Zatem

$$W(x_2 + p^2 t) \equiv W(x_2) + W'(x_2) \cdot p^2 t \pmod{p^3}.$$

Stąd wynika, że

$$W(x_2 + p^2 t) \equiv 0 \pmod{p^3}$$

wtedy i tylko wtedy, gdy

$$W(x_2) + W'(x_2) \cdot p^2 t \equiv 0 \pmod{p^3}.$$

Wiemy jednak, że

$$W(x_2) \equiv 0 \pmod{p^2}.$$

Zatem $W(x_2)$ dzieli się przez p^2. Stąd wynika, że kongruencja

$$W(x_2) + W'(x_2) \cdot p^2 t \equiv 0 \pmod{p^3}$$

jest równoważna kongruencji

$$\frac{W(x_2)}{p^2} + W'(x_2) \cdot t \equiv 0 \pmod{p}.$$

Ta kongruencja ma zaś dokładnie jedno rozwiązanie modulo p, gdyż

$$W'(x_2) \equiv W'(x_1) \not\equiv 0 \pmod{p}.$$

Rozwiązując tę kongruencję znajdujemy t, a następnie

$$x_3 = x_2 + p^2 t$$

i tak dalej. ♠

Niech teraz

$$W(x) = x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10.$$

Wtedy

$$W'(x) = 5x^4 + 40x^3 + 6x^2 + 16x + 7.$$

Niech wreszcie $x = 4$.

Zauważamy, że
$$W'(4) \equiv 3 \pmod 7$$
oraz
$$W(4) \equiv 7 \pmod{49}.$$
Zatem
$$\frac{W(4)}{7} \equiv 1 \pmod 7.$$
Mamy $x_1 = 4$ i szukamy
$$x_2 = x_1 + 7t = 4 + 7t.$$
Rozwiązujemy kongruencję
$$\frac{W(x_1)}{7} + W'(x_1) \cdot t \equiv 0 \pmod p,$$
czyli
$$1 + 3t \equiv 0 \pmod 7.$$
Otrzymujemy rozwiązanie $t = 2$, skąd dostajemy
$$x_2 = 4 + 7 \cdot 2 = 18.$$
Teraz szukamy x_3 w postaci
$$x_3 = x_2 + 49t = 18 + 49t.$$
Rozwiązujemy kongruencję
$$\frac{W(x_2)}{49} + W'(x_2) \cdot t \equiv 0 \pmod 7.$$
Zauważamy, że
$$W(18) \equiv 147 \pmod{343},$$
czyli
$$\frac{W(18)}{49} \equiv 3 \pmod 7.$$
Również
$$W'(18) \equiv W'(4) \equiv 3 \pmod 7.$$
Nasza kongruencja ma więc postać
$$3 + 3t \equiv 0 \pmod 7.$$
Rozwiązaniem tej kongruencji jest $t = 6$. Zatem
$$x_3 = 18 + 49 \cdot 6 = 312.$$

W podobny sposób dla $x_1 = 5$ otrzymujemy

$$x_2 = 12$$

i wreszcie

$$x_3 = 208.$$

Wreszcie rozwiązujemy kongruencję

$$x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10 \equiv 0 \pmod{3773}.$$

Przypominamy, że

$$3773 = 7^3 \cdot 11.$$

Zatem kongruencja

$$W(x) \equiv 0 \pmod{3773}$$

jest równoważna układowi kongruencji

$$\begin{cases} W(x) \equiv 0 \pmod{7^3} \\ W(x) \equiv 0 \pmod{11} \end{cases}$$

Takie układy rozwiązujemy korzystając z chińskiego twierdzenia o resztach. Rozwiążmy najpierw układ w postaci ogólnej:

$$\begin{cases} x \equiv a \pmod{7^3} \\ x \equiv b \pmod{11} \end{cases}$$

Ponieważ

$$11 \cdot 156 \equiv 1 \pmod{343} \text{ oraz } 6 \cdot 343 \equiv 1 \pmod{11},$$

więc rozwiązaniem ogólnym jest

$$x \equiv 11 \cdot 156 \cdot a + 6 \cdot 343 \cdot b \pmod{3773},$$

czyli

$$x \equiv 1716a + 2058b \pmod{3773}.$$

Teraz rozwiązujemy sześć układów kongruencji:

$$\begin{cases} x \equiv 208 \pmod{7^3} \\ x \equiv 2 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 208 \pmod{7^3} \\ x \equiv 3 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 208 \pmod{7^3} \\ x \equiv 7 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 312 \pmod{7^3} \\ x \equiv 2 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 312 \pmod{7^3} \\ x \equiv 3 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 312 \pmod{7^3} \\ x \equiv 7 \pmod{11} \end{cases}$$

Rozwiązania znajdujemy korzystając z otrzymanego wzoru ogólnego. Najpierw zauważmy, że

$$1716 \cdot 208 \equiv 2266 \pmod{3773}$$

oraz

$$1716 \cdot 312 \equiv 3399 \pmod{3773},$$

a także

$$2058 \cdot 2 \equiv 343 \pmod{3773},$$
$$2058 \cdot 3 \equiv 2401 \pmod{3773}$$

oraz

$$2058 \cdot 7 \equiv 3087 \pmod{3773}.$$

Stąd dostajemy rozwiązania naszych sześciu układów:

$$x \equiv 2266 + 343 = 2609 \pmod{3773},$$
$$x \equiv 2266 + 2401 = 4667 \equiv 894 \pmod{3773},$$
$$x \equiv 2266 + 3087 = 5353 \equiv 1580 \pmod{3773},$$
$$x \equiv 3399 + 343 = 3742 \pmod{3773},$$
$$x \equiv 3399 + 2401 = 5800 \equiv 2027 \pmod{3773},$$
$$x \equiv 3399 + 3087 = 6486 \equiv 2713 \pmod{3773}$$

Ostatecznie rozwiązaniami kongruencji

$$x^5 + 10x^4 + 2x^3 + 8x^2 + 7x + 10 \equiv 0 \pmod{3773}$$

są liczby

$$894, \quad 1580, \quad 2027, \quad 2609, \quad 2713, \quad 3742.$$

TWIERDZENIE WILSONA

Twierdzenie 5. (Wilson) Jeśli p jest liczbą pierwszą, to

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

Dowód. Dla $p = 2$ dowód jest oczywisty. Załóżmy więc, że p jest liczbą nieparzystą.

Łączymy liczby a takie, że $1 < a < p-1$ w pary: liczbę a w parze z liczbą b taką, że

$$ab \equiv 1 \pmod{p}.$$

Ponieważ $1 < a < p-1$, więc $a \neq b$.

Wtedy $(p-1)!$ jest iloczynem następujących liczb:
- liczby 1,
- liczby -1,
- iloczynów liczb z takich par $\{a, b\}$.

Iloczyn liczb w każdej parze przystaje do 1 modulo p, zatem liczba $(p-1)!$ przystaje do $1 \cdot (-1) \cdot 1$ modulo p, czyli do -1. ♠

Prawdziwe jest również twierdzenie odwrotne:

Twierdzenie 6. Jeśli $n > 0$ oraz

$$(n-1)! \equiv -1 \pmod{n},$$

to n jest liczbą pierwszą.

Dowód. Przypuśćmy, że $a \mid n$ oraz $1 < a < n$. Wtedy oczywiście

$$a \mid (n-1)!$$

Ale

$$n \mid (n-1)! + 1,$$

więc

$$a \mid (n-1)! + 1.$$

Stąd

$$a \mid 1,$$

sprzeczność. ♠

To nie jest dobry test pierwszości ze względu na bardzo dużą złożoność obliczeniową: wymaga $O(n(\log_2 n)^2)$ działań na bitach.

Przypomnienie:

Twierdzenie 7. (Małe twierdzenie Fermata) Jeśli p jest liczbą pierwszą, to

$$a^p \equiv a \pmod{p}. \quad ♠$$

Wniosek. Jeśli p jest liczbą pierwszą oraz $p \not| \, a$, to

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

PRZYKŁADY

Zauważmy, że
$$2^{63} \not\equiv 2 \pmod{63}.$$
Mianowicie
$$2^{63} = 2^{60} \cdot 2^3 = \left(2^6\right)^{10} \cdot 2^3 = 64^{10} \cdot 8 \equiv 1^{10} \cdot 8 = 8 \not\equiv 2 \pmod{63}.$$
Zatem 63 nie jest liczbą pierwszą. (Tego można dowieść prościej!)

Podobnie
$$2^{847} \not\equiv 2 \pmod{847}.$$
Mianowicie, stosując metodę podnoszenia do kwadratu, otrzymujemy:
$$\begin{aligned}
2^1 &\equiv 2 \pmod{847}\\
2^2 &\equiv 4 \pmod{847}\\
2^4 &\equiv 16 \pmod{847}\\
2^8 &\equiv 256 \pmod{847}\\
2^{16} &\equiv 317 \pmod{847}\\
2^{32} &\equiv 543 \pmod{847}\\
2^{64} &\equiv 93 \pmod{847}\\
2^{128} &\equiv 179 \pmod{847}\\
2^{256} &\equiv 702 \pmod{847}\\
2^{512} &\equiv 697 \pmod{847}
\end{aligned}$$
Teraz
$$\begin{aligned}
2^{847} &\equiv 697 \cdot 702 \cdot 93 \cdot 256 \cdot 16 \cdot 4 \cdot 2 \equiv\\
&\equiv 282 \pmod{847}.
\end{aligned}$$
Zatem 847 też jest liczbą złożoną. Tego też można dowieść prościej.

LICZBY PSEUDOPIERWSZE

Hipoteza. (Tzw. „twierdzenie Chińczyków”): Jeśli
$$2^n \equiv 2 \pmod{n},$$
to n jest liczbą pierwszą.

Niestety ta hipoteza jest fałszywa. Przykład: niech $n = 341$. Wtedy
$$n = 341 = 11 \cdot 31.$$

Jednocześnie
$$2^{10} \equiv 1 \pmod{11},$$
skąd otrzymujemy
$$2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \pmod{11}.$$
Również
$$2^5 = 32 \equiv 1 \pmod{31},$$
skąd wynika, że
$$2^{340} = (2^5)^{68} \equiv 1^{68} = 1 \pmod{31}.$$
Zatem
$$2^{340} \equiv 1 \pmod{341}$$
lub równoważnie
$$2^{341} \equiv 2 \pmod{341}.$$

Oczywiście $2^{341} \bmod 341$ można obliczyć bezpośrednio tak samo jak w poprzednim przykładzie.

Definicja. Liczbę n nazywamy **liczbą pseudopierwszą** przy podstawie b wtedy i tylko wtedy, gdy jest złożona oraz
$$b^n \equiv b \pmod{n}.$$
Interesują nas podstawy b takie, że $\mathrm{NWD}(b,n) = 1$. Mianowicie będziemy wykorzystywać liczby pseudopierwsze do sprawdzania, czy dana liczba n jest pierwsza. Jeśli zaś $\mathrm{NWD}(b,n) > 1$, to od razu znajdujemy dzielnik właściwy liczby n.

Jeśli $\mathrm{NWD}(b,n) = 1$, to kongruencja
$$b^n \equiv b \pmod{n}$$
jest równoważna kongruencji
$$b^{n-1} \equiv 1 \pmod{n}.$$

Przykłady liczb pseudopierwszych przy podstawie 2:

$$\begin{array}{cccccccc}
341, & 561, & 645, & 1105, & 1387, & 1729, & 1905, & 2047, \\
2465, & 2701, & 2821, & 3277, & 4033, & 4369, & 4371, & 4681, \\
5461, & 6601, & 7957, & 8321, & 8481, & 8911, & & \ldots
\end{array}$$

Są to wszystkie takie liczby mniejsze od 10000. Jest ich 22.

Wśród liczb mniejszych od 10^{10} jest 455052512 liczb pierwszych i tylko 14884 liczb pseudopierwszych przy podstawie 2.

To były przykłady liczb pseudopierwszych nieparzystych. Są także liczby pseudopierwsze parzyste: najmniejszą jest 161038.

Twierdzenie 8. Istnieje nieskończenie wiele liczb pseudopierwszych przy podstawie 2.

Zamiast dowodu. Można pokazać, że jeśli liczba n jest złożona, nieparzysta oraz

$$2^n \equiv 2 \pmod{n},$$

to liczba $m = 2^n - 1$ ma te same własności. ♠

Testowanie złożoności.

Jeśli liczba n jest nieparzysta oraz

$$2^n \not\equiv 2 \pmod{n},$$

to liczba n jest złożona.

Ten test nie wyjaśnia, czy liczba n jest złożona w przypadku liczb pseudopierwszych – a jest ich nieskończenie wiele!

LICZBY CARMICHAELA

Można próbować zmienić podstawę.

Niech $n = 341$. Weźmy $b = 7$. Wtedy

$$7^3 = 343 \equiv 2 \pmod{341}$$

oraz

$$2^{10} = 1024 \equiv 1 \pmod{341}.$$

Zatem

$$7^{340} = (7^3)^{113} \cdot 7 \equiv 2^{113} \cdot 7 = (2^{10})^{11} \cdot 2^3 \cdot 7 \equiv 1^{11} \cdot 56 = 56 \pmod{341}.$$

Zatem liczba 341 jest złożona.

Pytanie. Czy dla liczby złożonej n można zawsze dobrać podstawę b taką, że

$$b^n \not\equiv b \pmod{n}?$$

Definicja. Liczbę n nazywamy **liczbą Carmichaela** wtedy i tylko wtedy, gdy jest złożona oraz dla każdej liczby b takiej, że $\mathrm{NWD}(b, n) = 1$ zachodzi kongruencja

$$b^n \equiv b \pmod{n}.$$

Inaczej mówiąc, liczbą Carmichaela nazywamy liczbę n pseudopierwszą przy każdej podstawie b względnie pierwszej z n.

PRZYKŁADY

Niech $n = 561$. Wtedy $n = 3 \cdot 11 \cdot 17$. Niech $\mathrm{NWD}(b, n) = 1$. Wtedy

$$b^2 \equiv 1 \pmod{3},$$

skąd otrzymujemy

$$b^{560} = (b^2)^{280} \equiv 1 \pmod{3};$$

następnie

$$b^{10} \equiv 1 \pmod{11},$$

skąd dostajemy

$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11};$$

wreszcie

$$b^{16} \equiv 1 \pmod{17},$$

skąd wynika, że

$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$

Zatem

$$b^{560} \equiv 1 \pmod{561}.$$

Liczba 561 jest więc liczbą Carmichaela.

Twierdzenie 9. Niech $n = q_1 \cdot \ldots \cdot q_m$, gdzie $q_1, \ldots, q_m$ są różnymi liczbami pierwszymi. Jeśli

$$(q_i - 1) \mid (n - 1)$$

dla $i = 1, \ldots, m$, to liczba n jest liczbą Carmichaela. ♠

Przykład. Liczba $n = 6601$ jest liczbą Carmichaela. Mianowicie

$$6601 = 7 \cdot 23 \cdot 41$$

oraz

$$6 \mid 6600, \quad 22 \mid 6600, \quad 40 \mid 6600.$$

Prawdziwe jest też twierdzenie odwrotne:

Twierdzenie 10. Niech n będzie liczbą Carmichaela. Wtedy istnieją różne liczby pierwsze $q_1, \ldots, q_m$, gdzie $m \geq 3$ takie, że

$$n = q_1 \cdot \ldots \cdot q_m$$

oraz

$$(q_i - 1) \mid (n - 1)$$

dla $i = 1, \ldots, m$. ♠

Wiadomo też, że istnieje nieskończenie wiele liczb Carmichaela.

TEST MILLERA

Przypomnienie: jeśli p jest liczbą pierwszą oraz

$$x^2 \equiv 1 \pmod{p},$$

to

$$x \equiv 1 \pmod{p} \text{ lub } x \equiv -1 \pmod{p}.$$

Zastosujmy to twierdzenie do wykazania, że liczba 561 (będąca liczbą Carmichaela) jest liczbą złożoną. Niech $b = 5$. Wtedy

$$\mathrm{NWD}(5, 561) = 1$$

oraz wiemy, że

$$5^{560} \equiv 1 \pmod{561}.$$

Ale $560 = 2 \cdot 280$. Zatem

$$5^{560} = (5^{280})^2 \equiv 1 \pmod{561}.$$

Można sprawdzić, że

$$5^{280} \equiv 67 \pmod{561}.$$

Zatem liczba 561 nie jest pierwsza.

To połączenie małego twierdzenia Fermata z twierdzeniem o pierwiastkach kwadratowych z jedności pozwoliło sprawdzić, że liczba 561 jest złożona. Ten test można jeszcze bardziej poprawić.

Test. Niech n będzie liczbą nieparzystą dodatnią. Niech

$$n - 1 = 2^s \cdot t,$$

gdzie t jest liczbą nieparzystą. Oczywiście $s \geq 1$. Niech następnie b będzie liczbą dodatnią taką, że

$$\mathrm{NWD}(b, n) = 1.$$

Mówimy, że liczba n spełnia **test Millera** przy podstawie b wtedy i tylko wtedy, gdy albo

$$b^t \equiv 1 \pmod{n},$$

albo
$$b^{2^j\cdot t}\equiv -1 \pmod n$$
dla pewnego $j=0,1,\ldots,s-1$.

Twierdzenie 11. Jeśli n jest liczbą pierwszą, to n spełnia test Millera przy dowolnej podstawie b takiej, że
$$\mathrm{NWD}(b,n)=1.$$

Dowód. Niech
$$x_k=b^{2^{s-k}\cdot t}$$
dla $k=0,1,\ldots,s$. Wtedy
$$x_0=b^{n-1} \quad \text{oraz} \quad x_k=x_{k+1}^2$$
dla $k=0,1,\ldots,s-1$. Zauważmy, że
$$x_0\equiv 1 \pmod n.$$
Zatem
$$x_1^2\equiv 1 \pmod n,$$
skąd wynika, że
$$x_1\equiv \pm 1 \pmod n.$$
Jeśli
$$x_1\equiv -1 \pmod n,$$
to liczba n spełnia test Millera przy podstawie b. Jeśli
$$x_1\equiv 1 \pmod n,$$
to
$$x_2^2\equiv 1 \pmod n$$
i wtedy
$$x_2\equiv \pm 1 \pmod n$$
i tak dalej. Jeśli dla któregokolwiek k dostaniemy
$$x_k\equiv -1 \pmod n,$$
to liczba n spełnia test Millera. Jeśli natomiast dla każdego k mamy
$$x_k\equiv 1 \pmod n,$$
to w szczególności
$$x_s\equiv 1 \pmod n.$$
Ale
$$x_s=b^t,$$

skąd otrzymujemy

$$b^t \equiv 1 \pmod{n},$$

co oznacza, że liczba n spełnia test Millera. ♠

LICZBY SILNIE PSEUDOPIERWSZE

Definicja. Liczbę całkowitą dodatnią n nazywamy **liczbą silnie pseudopierwszą** przy podstawie b, jeśli jest złożona oraz spełnia test Millera przy podstawie b.

Przykład. Niech $n = 2047$. Wtedy liczba n jest złożona:

$$2047 = 23 \cdot 89.$$

Następnie

$$n - 1 = 2046 = 2^1 \cdot 1023.$$

Niech $b = 2$. Wtedy

$$2^{2046} = (2^{11})^{186} = (2048)^{186} \equiv 1^{186} = 1 \pmod{2047}$$

oraz

$$2^{1023} = (2^{11})^{93} \equiv 1^{93} = 1 \pmod{2047}.$$

Zatem liczba 2047 jest silnie pseudopierwsza przy podstawie 2. Można sprawdzić, że liczba 2047 nie jest silnie pseudopierwsza przy podstawie 3.

Twierdzenie 12. Jeśli n jest liczbą silnie pseudopierwszą przy podstawie b to jest też liczbą pseudopierwszą przy podstawie b.

Dowód. Zauważmy, że jeśli $j \leq s - 1$, to 2^{s-j} jest liczbą parzystą i stąd

$$b^{n-1} = (b^{2^j \cdot t})^{2^{s-j}} \equiv (\pm 1)^{2^{s-j}} = 1 \pmod{n}.$$

Zatem

$$b^{n-1} \equiv 1 \pmod{n}. \quad ♠$$

Twierdzenie 13. Istnieje nieskończenie wiele liczb silnie pseudopierwszych przy podstawie 2.

Zamiast dowodu. Można pokazać, że jeśli liczba n jest pseudopierwsza przy podstawie 2, to liczba $2^n - 1$ jest silnie pseudopierwsza przy podstawie 2. ♠

Dla małych liczb n test Millera jest znakomitym testem pierwszości. Sprawdzono bowiem, że:

- najmniejszą liczbą silnie pseudopierwszą przy podstawie 2 jest 2047;

- najmniejszą liczbą silnie pseudopierwszą przy podstawach 2 i 3 jest 1373653;
- najmniejszą liczbą silnie pseudopierwszą przy podstawach 2, 3 i 5 jest 25326001;
- najmniejszą liczbą silnie pseudopierwszą przy podstawach 2, 3, 5 i 7 jest 3215031751.

Wśród liczb $n < 25 \cdot 10^9$ jedyną liczbą silnie pseudopierwszą przy podstawach 2, 3, 5 i 7 jest liczba 3215031751.

Z uogólnionej hipotezy Riemanna wynika, że ten test jest też znakomitym testem dla dowolnych liczb n. Jeśli bowiem liczba n jest złożona, to nie spełnia testu Millera dla pewnej podstawy b takiej, że

$$b < 70(\log_2 n)^2.$$

TEST MILLERA – RABINA

Nie ma liczb analogicznych do liczb Carmichaela dla liczb silnie pseudopierwszych. Tzn. nie istnieje liczba n silnie pseudopierwsza przy każdej podstawie b względnie pierwszej z n. Można pokazać więcej.

Twierdzenie 14. Jeśli n jest liczbą nieparzystą złożoną, to liczba n spełnia test Millera dla co najwyżej $\frac{n-1}{4}$ podstaw b takich, że $1 \leq b \leq n-1$.

To twierdzenie daje test probabilistyczny. Dla danej liczby n losujemy liczbę b taką, że $1 \leq b \leq n-1$. Jeśli

$$\mathrm{NWD}(b, n) > 1,$$

to liczba n jest oczywiście złożona (a nawet znaleźliśmy jej dzielnik). Jeśli

$$\mathrm{NWD}(b, n) = 1,$$

to przeprowadzamy test Millera. Jeśli liczba n nie spełnia testu Millera, to jest złożona (ale tym razem nie znamy jej dzielnika). Jeśli zaś liczba n spełnia test Millera, to losujemy następną liczbę b.

Prawdopodobieństwo tego, że liczba złożona spełnia test Millera przy wybranej losowo liczbie b, jest równe 4^{-1}. Zatem prawdopodobieństwo tego, że liczba n przejdzie pomyślnie przez k testów przy k wybranych losowo podstawach b, jest równe 4^{-k}. Dla $k = 50$ to prawdopodobieństwo jest praktycznie równe zeru.