UŁAMKI ŁAŃCUCHOWE

Zastosujmy algorytm Euklidesa do liczb 62 i 23:

$$\begin{aligned} 62 &= 2 \cdot 23 + 16, \\ 23 &= 1 \cdot 16 + 7, \\ 16 &= 2 \cdot 7 + 2, \\ 7 &= 3 \cdot 2 + 1. \end{aligned}$$

Inaczej:

$$\begin{aligned} \tfrac{62}{23} &= 2 + \tfrac{16}{23} &&= 2 + \tfrac{1}{23/16}, \\ \tfrac{23}{16} &= 1 + \tfrac{7}{16} &&= 1 + \tfrac{1}{16/7}, \\ \tfrac{16}{7} &= 2 + \tfrac{2}{7} &&= 2 + \tfrac{1}{7/2}, \\ \tfrac{7}{2} &= 3 + \tfrac{1}{2}. \end{aligned}$$

Składając razem te równości otrzymamy:

$$\begin{aligned} \tfrac{62}{23} &= 2 + \cfrac{1}{23/16} = \\ &= 2 + \cfrac{1}{1 + \cfrac{1}{16/7}} = \\ &= 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{7/2}}} = \\ &= 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}}. \end{aligned}$$

Ułamek postaci

$$\frac{62}{23} = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{2}}}}$$

nazywamy **ułamkiem łańcuchowym**.

Ogólnie, **ułamkiem łańcuchowym** nazywamy ułamek postaci

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}},$$

gdzie $a_0, a_1, \ldots, a_n$ są liczbami rzeczywistymi takimi, że

$$a_1, \ldots, a_n > 0.$$

Taki ułamek łańcuchowy oznaczamy wygodniejszym symbolem

$$[a_0; a_1, \ldots, a_n].$$

Zatem

$$\frac{62}{23} = [2; 1, 2, 3, 2].$$

Ułamek łańcuchowy nazywamy **arytmetycznym**, jeśli wszystkie liczby $a_0, a_1, \ldots, a_n$ są całkowite.

LICZBY WYMIERNE

Twierdzenie 1. Każdy ułamek łańcuchowy arytmetyczny przedstwia liczbę wymierną. ♠

Twierdzenie 2. Każda liczba wymierna daje się przedstawić w postaci ułamka łańcuchowego arytmetycznego.

Dowód. Stosujemy algorytm Euklidesa tak jak w przykładzie na początku wykładu. ♠

Przedstawienie liczby wymiernej w postaci ułamka łańcuchowego nie jest jednoznaczne. Mianowicie z równości

$$a_n = (a_n - 1) + \frac{1}{1}$$

wynika, że jeśli $a_n > 1$, to

$$[a_0; a_1, \ldots, a_{n-1}, a_n] = [a_0; a_1, \ldots, a_{n-1}, a_n - 1, 1].$$

Na przykład

$$\frac{62}{23} = [2; 1, 2, 3, 2] = [2; 1, 2, 3, 1, 1].$$

Twierdzenie 3. Każda liczba wymierna ma dokładnie dwa różne przedstawienia w postaci ułamków łańcuchowych arytmetycznych: jedno mające parzystą liczbę wyrazów i drugie mające nieparzystą liczbę wyrazów. Dokładnie jedno z nich kończy się jedynką. ♠

REDUKTY

Definicja. Dany jest ułamek łańcuchowy

$$[a_0; a_1, a_2, \ldots, a_n].$$

Wtedy **reduktem** tego ułamka łańcuchowego nazywamy każdy ułamek łańcuchowy postaci

$$R_k = [a_0; a_1, a_2, \ldots, a_k]$$

dla $k = 0, 1, 2, \ldots, n$.

Twierdzenie 4. Niech $a_0, a_1, a_2, \ldots, a_n \in \mathbb{R}$ oraz

$$a_1, a_2, \ldots, a_n > 0.$$

Definiujemy ciągi $p_0, p_1, p_2, \ldots, p_n$ oraz $q_0, q_1, q_2, \ldots, q_n$ wzorami:

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_0 a_1 + 1 & q_1 &= a_1 \\ p_k &= a_k p_{k-1} + p_{k-2} & q_k &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

dla $k = 2, 3, \ldots, n$. Wtedy k-ty redukt R_k jest dany wzorem

$$R_k = [a_0; a_1, a_2, \ldots, a_k] = \frac{p_k}{q_k}.$$

Dowód. Indukcja względem k. ♠

PRZYKŁAD

Wiemy, że

$$\frac{62}{23} = [2; 1, 2, 3, 2].$$

Obliczamy wyrazy ciągów p_i oraz q_i:

$$\begin{aligned} p_0 &= 2 & q_0 &= 1 \\ p_1 &= 2 \cdot 1 + 1 = 3 & q_1 &= 1 \\ p_2 &= 2 \cdot 3 + 2 = 8 & q_2 &= 2 \cdot 1 + 1 = 3 \\ p_3 &= 3 \cdot 8 + 3 = 27 & q_3 &= 3 \cdot 3 + 1 = 10 \\ p_4 &= 2 \cdot 27 + 8 = 62 & q_4 &= 2 \cdot 10 + 3 = 23. \end{aligned}$$

Wtedy kolejne redukty wynoszą:

$$\begin{aligned}
R_0 &= \frac{p_0}{q_0} = \frac{2}{1} = 2, \\
R_1 &= \frac{p_1}{q_1} = \frac{3}{1} = 3, \\
R_2 &= \frac{p_2}{q_2} = \frac{8}{3}, \\
R_3 &= \frac{p_3}{q_3} = \frac{27}{10}, \\
R_4 &= \frac{p_4}{q_4} = \frac{62}{23}.
\end{aligned}$$

WŁASNOŚCI REDUKTÓW

Twierdzenie 5. Niech k-tym reduktem ułamka łańcuchowego

$$[a_0; a_1, a_2, \ldots, a_n]$$

będzie

$$R_k = \frac{p_k}{q_k},$$

gdzie p_k i q_k są zdefiniowane tak jak w poprzednim twierdzeniu. Wtedy

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}.$$

Dowód. Indukcja względem k. ♠

Przykład. Dla ułamka łancuchowego

$$\frac{62}{23} = [2; 1, 2, 3, 2]$$

mamy:

$$\begin{aligned}
p_0 q_1 - p_1 q_0 &= 2 \cdot 1 - 3 \cdot 1 = 2 - 3 = -1, \\
p_1 q_2 - p_2 q_1 &= 3 \cdot 3 - 8 \cdot 1 = 9 - 8 = 1, \\
p_2 q_3 - p_3 q_2 &= 8 \cdot 10 - 27 \cdot 3 = 80 - 81 = -1, \\
p_3 q_4 - p_4 q_3 &= 27 \cdot 23 - 62 \cdot 10 = 621 - 620 = 1.
\end{aligned}$$

Wniosek. Liczby p_k i q_k są względnie pierwsze. ♠

DALSZE WŁASNOŚCI

Twierdzenie 6. Niech $R_k = \frac{p_k}{q_k}$ będzie k-tym reduktem ułamka łańcuchowego

$$[a_0; a_1, a_2, \ldots, a_n].$$

Wtedy

$$R_k - R_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}}$$

dla $k = 1, 2, \ldots, n$. Także

$$R_k - R_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}}$$

dla $k = 2, 3, \ldots, n$. ♠

Wniosek. Niech R_k będzie k-tym reduktem ułamka łańcuchowego

$$[a_0; a_1, a_2, \ldots, a_n].$$

Wtedy

$$R_0 < R_2 < R_4 < \ldots < R_5 < R_3 < R_1.$$

Dowód. Zauważmy, że

$$\operatorname{sgn}(R_k - R_{k-2}) = \operatorname{sgn}((-1)^k)$$

oraz

$$\operatorname{sgn}(R_k - R_{k-1}) = \operatorname{sgn}((-1)^{k-1}),$$

skąd wynikają wszystkie nierówności. ♠

PRZYKŁAD

Dla ułamka

$$\frac{62}{23} = [2; 1, 2, 3, 2]$$

mamy:

$$\begin{aligned}
R_0 &= \frac{2}{1} = 2, \\
R_1 &= \frac{3}{1} = 3, \\
R_2 &= \frac{8}{3} = 2,3333\ldots, \\
R_3 &= \frac{27}{10} = 2,7, \\
R_4 &= \frac{62}{23} = 2,6956\ldots.
\end{aligned}$$

Wtedy

$$2 < 2,3333\ldots < 2,6956\ldots < 2,7 < 3,$$

czyli

$$R_0 < R_2 < R_4 < R_3 < R_1.$$

UŁAMKI ŁAŃCUCHOWE NIESKOŃCZONE

Twierdzenie 7. Niech będzie dany ciąg nieskończony

$$a_0, a_1, a_2, \ldots, a_n, \ldots$$

liczb całkowitych takich, że

$$a_1, a_2, \ldots > 0.$$

Określmy następnie k-ty redukt wzorem

$$R_k = [a_0; a_1, a_2, \ldots, a_k].$$

Wtedy istnieje granica

$$\lim_{k\to\infty} R_k = \alpha. \quad \spadesuit$$

Definicja. Granicę α określoną w powyższym twierdzeniu nazywamy **nieskończonym ułamkiem łańcuchowym arytmetycznym**. Oznaczamy ją symbolem

$$[a_0; a_1, a_2, \ldots, a_n, \ldots].$$

Twierdzenie 8. Niech

$$a_0, a_1, a_2, \ldots \in \mathbb{Z} \ \text{ oraz } \ a_1, a_2, \ldots > 0.$$

Wtedy liczba

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots]$$

jest niewymierna. $\spadesuit$

ROZWIJANIE LICZB NIEWYMIERNYCH

Twierdzenie 9. Niech α będzie liczbą niewymierną. Definiujemy dwa ciągi liczb rzeczywistych wzorami:

$$\alpha_0 = \alpha, \qquad a_0 = \lfloor \alpha_0 \rfloor,$$

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}, \qquad a_{k+1} = \lfloor \alpha_{k+1} \rfloor$$

dla $k = 0, 1, 2, 3, \ldots$. Wtedy

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots]. \quad \spadesuit$$

Przykład. Niech $\alpha = \sqrt{2}$. Wtedy mamy:

$$\begin{aligned} \alpha_0 &= \sqrt{2}, & a_0 &= \lfloor\sqrt{2}\rfloor = 1, \\ \alpha_1 &= \frac{1}{\sqrt{2}-1} = \sqrt{2}+1, & a_1 &= \lfloor\sqrt{2}+1\rfloor = 2, \\ \alpha_2 &= \frac{1}{\sqrt{2}+1-2} = \sqrt{2}+1, & a_2 &= \lfloor\sqrt{2}+1\rfloor = 2 \end{aligned}$$

i tak dalej w nieskończoność.

Zatem

$$\sqrt{2} = [1; 2, 2, 2, 2, 2, \ldots].$$

WŁASNOŚCI UŁAMKÓW NIESKOŃCZONYCH

Twierdzenie 10. Rozwinięcie liczby niewymiernej na ułamek łańcuchowy nieskończony jest jednoznaczne. Jeśli

$$\alpha = [a_0; a_1, a_2, \ldots, a_n \ldots] = [b_0; b_1, b_2, \ldots, b_n, \ldots],$$

to

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \quad \ldots, \quad a_n = b_n, \ldots \quad \spadesuit$$

Wiemy już, że kolejne redukty są przybliżeniami liczby α. Na przykład dla ułamka

$$\sqrt{2} = [1; 2, 2, 2, 2, \ldots]$$

mamy

$$\begin{aligned} R_0 &= [1] = 1, \\ R_1 &= [1; 2] = \frac{3}{2} = 1,5, \\ R_2 &= [1; 2, 2] = \frac{7}{5} = 1,4, \\ R_3 &= [1; 2, 2, 2] = \frac{17}{12} = 1,41666\ldots, \\ R_4 &= [1; 2, 2, 2, 2] = \frac{41}{29} = 1,4137931\ldots \end{aligned}$$

i tak dalej.

Twierdzenie 11. Jeśli $R_k = \frac{p_k}{q_k}$ jest k-tym reduktem ułamka łańcuchowego

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots],$$

to

$$|\alpha - R_k| < \frac{1}{q_k^2}. \quad \spadesuit$$

Twierdzenie 12. Jeśli $R_k = \frac{p_k}{q_k}$ jest k-tym reduktem ułamka łańcuchowego

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots]$$

i jeśli r i s są liczbami całkowitymi takimi, że $s > 0$ oraz

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

to $s \geq q_{k+1}$. $\spadesuit$

Twierdzenie 13. Jeśli $R_k = \frac{p_k}{q_k}$ jest k-tym reduktem ułamka łańcuchowego

$$\alpha = [a_0; a_1, a_2, \ldots, a_n, \ldots]$$

i jeśli r i s są liczbami całkowitymi takimi, że $s > 0$ oraz

$$\left|\alpha - \frac{r}{s}\right| < \left|\alpha - \frac{p_k}{q_k}\right|,$$

to $s \geq q_{k+1}$. $\spadesuit$

Można pokazać, że jeśli ułamek $\frac{r}{s}$ jest wystarczająco dobrym przybliżeniem liczby α, to jest pewnym reduktem jej rozwinięcia łańcuchowego.

PRZYKŁADY

Wiemy już, że

$$\sqrt{2} = [1; 2, 2, 2, 2, \ldots].$$

Kolejnymi reduktami są

$$1, \quad \frac{3}{2}, \quad \frac{7}{5}, \quad \frac{17}{12}, \quad \frac{41}{29}, \ldots$$

Zatem na przykład:

- ułamek $\frac{7}{5}$ jest najlepszym przybliżeniem $\sqrt{2}$ z mianownikiem mniejszym od 12,

- ułamek $\frac{17}{12}$ jest najlepszym przybliżeniem $\sqrt{2}$ z mianownikiem mniejszym od 29 i tak dalej.

Można sprawdzić, że

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, \ldots].$$

Kolejnymi reduktami są

$$3, \quad \frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}, \quad \frac{103993}{33102}, \ldots$$

Zatem:

- ułamek $\frac{22}{7}$ jest najlepszym przybliżeniem π z mianownikiem mniejszym od 106,
- ułamek $\frac{355}{113}$ jest najlepszym przybliżeniem π z mianownikiem mniejszym od 33102 i tak dalej.

RÓWNANIE PELLA

Przyjrzyjmy się kolejnym reduktom ułamka łańcuchowego

$$\sqrt{2} = [1; 2, 2, 2, 2, \ldots].$$

- Dla reduktu $\frac{3}{2}$ mamy
$$3^2 - 2 \cdot 2^2 = 9 - 8 = 1;$$
- dla reduktu $\frac{7}{5}$ mamy
$$7^2 - 2 \cdot 5^2 = 49 - 50 = -1;$$
- dla reduktu $\frac{17}{12}$ mamy
$$17^2 - 2 \cdot 12^2 = 289 - 288 = 1;$$
- dla reduktu $\frac{41}{29}$ mamy

$$41^2 - 2 \cdot 29^2 = 1681 - 1682 = -1$$

i tak dalej.

W ten sposób otrzymujemy rozwiązania równań diofantycznych postaci

$$x^2 - 2y^2 = \pm 1.$$

Definicja. Równanie diofantyczne postaci

$$x^2 - dy^2 = 1,$$

gdzie d nie jest kwadratem liczby całkowitej, nazywamy **równaniem Pella**.

UŁAMKI ŁAŃCUCHOWE OKRESOWE

Niech $\alpha = \sqrt{7}$. Znajdziemy rozwinięcie liczby α na ułamek łańcuchowy. Mamy kolejno:

$$\begin{aligned}
\alpha_0 &= \sqrt{7}, & a_0 &= \lfloor\sqrt{7}\rfloor = 2,\\
\alpha_1 &= \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}, & a_1 &= \left\lfloor\tfrac{\sqrt{7}+2}{3}\right\rfloor = 1,\\
\alpha_2 &= \frac{1}{\frac{\sqrt{7}+2}{3}-1} = \frac{\sqrt{7}+1}{2}, & a_2 &= \left\lfloor\tfrac{\sqrt{7}+1}{2}\right\rfloor = 1,\\
\alpha_3 &= \frac{1}{\frac{\sqrt{7}+1}{2}-1} = \frac{\sqrt{7}+1}{3}, & a_3 &= \left\lfloor\tfrac{\sqrt{7}+1}{3}\right\rfloor = 1,\\
\alpha_4 &= \frac{1}{\frac{\sqrt{7}+1}{3}-1} = \sqrt{7}+2, & a_4 &= \lfloor\sqrt{7}+2\rfloor = 4,\\
\alpha_5 &= \frac{1}{\sqrt{7}+2-4} = \frac{\sqrt{7}+2}{3}, & a_5 &= \left\lfloor\tfrac{\sqrt{7}+2}{3}\right\rfloor = 1.
\end{aligned}$$

Zauważmy, że

$$\alpha_5 = \alpha_1,$$

a więc kolejne wyrazy obu ciągów będą się okresowo powtarzać:

$$\alpha_5 = \alpha_1, \quad \alpha_6 = \alpha_2, \quad \alpha_7 = \alpha_3, \quad \alpha_8 = \alpha_4, \ldots$$

Zatem

$$\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots] = [2; \overline{1, 1, 1, 4}].$$

INNY PRZYKŁAD

Spróbujmy w drugą stronę. Niech

$$\alpha = [2; 3, 2, 3, 2, 3, 2, \ldots] = [2; \overline{3, 2}] = [\overline{2; 3}].$$

Wtedy mamy

$$\begin{aligned}\alpha &= 2+\frac{1}{[3;2,3,2,3,2,3,\ldots]} = \\ &= 2+\cfrac{3}{1+\cfrac{1}{[2;3,2,3,2,3,2,\ldots]}} = \\ &= 2+\cfrac{3}{1+\cfrac{1}{\alpha}} = \end{aligned}$$

Zatem

$$\alpha-2=\frac{\alpha}{3\alpha+1},$$

skąd dostajemy

$$3\alpha^2-6\alpha-2=0.$$

A więc

$$\alpha=\frac{3+\sqrt{15}}{3} \quad \text{lub} \quad \alpha=\frac{3-\sqrt{15}}{3}.$$

Ale $\alpha>0$, więc ostatecznie

$$\alpha=\frac{3+\sqrt{15}}{3}.$$

NIEWYMIERNOŚCI KWADRATOWE

Definicja. Liczbę niewymierną α nazywamy **niewymiernością kwadratową**, jeśli jest pierwiastkiem równania kwadratowego

$$Ax^2+Bx+C=0$$

o współczynnikach całkowitych.

Twierdzenie 14. Liczba niewymierna α jest niewymiernością kwadratową wtedy i tylko wtedy, gdy istnieją liczby całkowite a, b i c takie, że

$$\alpha=\frac{a+\sqrt{b}}{c}$$

oraz b nie jest kwadratem liczby całkowitej. ♠

Definicja. Jeśli liczba

$$\alpha=\frac{a+\sqrt{b}}{c}$$

jest niewymiernością kwadratową, to liczbę

$$\alpha' = \frac{a-\sqrt{b}}{c}$$

nazywamy **liczbą sprzężoną** z liczbą α.

Twierdzenie 15. Jeśli niewymierność kwadratowa α jest pierwiastkiem równania kwadratowego

$$Ax^2 + Bx + C = 0$$

o współczynnikach całkowitych, to drugim pierwiastkiem tego równania jest liczba α'. ♠

TWIERDZENIE LAGRANGE'A

Twierdzenie 16. Liczba niewymierna α ma rozwinięcie okresowe na ułamek łańcuchowy wtedy i tylko wtedy, gdy jest niewymiernością kwadratową. ♠

Algorytm. Dana jest niewymierność kwadratowa

$$\alpha = \frac{a+\sqrt{b}}{c}.$$

Najpierw kładziemy

$$P_0 = a|c|, \quad Q_0 = c|c|, \quad d = bc^2.$$

Wtedy

$$\alpha = \frac{P_0+\sqrt{d}}{Q_0} \quad \text{oraz} \quad Q_0 \mid (d-P_0^2).$$

Następnie definiujemy

$$\begin{aligned} \alpha_k &= \frac{P_k+\sqrt{d}}{Q_k}, \\ a_k &= \lfloor \alpha_k \rfloor, \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{d-P_{k+1}^2}{Q_k}. \end{aligned}$$

Uwaga: Można pokazać, że $Q_k \mid (d-P_{k+1}^2)$.
Wreszcie:

$$\alpha = [a_0; a_1, a_2, \ldots, a_k, \ldots].$$

PRZYKŁAD

Niech $\alpha = \frac{3+\sqrt{7}}{2}$. Wtedy $d = 28$ i następnie

$$\begin{array}{lllllll}
P_0 & = & 6, & \qquad & Q_0 & = & 4, \\
\alpha_0 & = & \frac{6+\sqrt{28}}{4} & & a_0 & = & \lfloor\frac{6+\sqrt{28}}{4}\rfloor = 2, \\
\\
P_1 & = & 2, & & Q_1 & = & 6, \\
\alpha_1 & = & \frac{2+\sqrt{28}}{6} & & a_1 & = & \lfloor\frac{2+\sqrt{28}}{6}\rfloor = 1, \\
\\
P_2 & = & 4, & & Q_2 & = & 2, \\
\alpha_2 & = & \frac{4+\sqrt{28}}{2} & & a_2 & = & \lfloor\frac{4+\sqrt{28}}{2}\rfloor = 4, \\
\\
P_3 & = & 4, & & Q_3 & = & 6, \\
\alpha_3 & = & \frac{4+\sqrt{28}}{6} & & a_3 & = & \lfloor\frac{4+\sqrt{28}}{6}\rfloor = 1, \\
\\
P_4 & = & 2, & & Q_4 & = & 4, \\
\alpha_4 & = & \frac{2+\sqrt{28}}{4} & & a_4 & = & \lfloor\frac{2+\sqrt{28}}{4}\rfloor = 1, \\
\\
P_5 & = & 2, & & Q_5 & = & 6, \\
\alpha_5 & = & \frac{2+\sqrt{28}}{6} & & a_5 & = & \lfloor\frac{2+\sqrt{28}}{6}\rfloor = 1.
\end{array}$$

Zauważmy, że

$$P_5 = P_1 \text{ oraz } Q_5 = Q_1.$$

Zatem rozwinięcie będzie okresowe z okresem długości 4:

$$\frac{3+\sqrt{7}}{2} = [2; 1, 4, 1, 1, 1, 4, 1, 1, \ldots] = [2; \overline{1, 4, 1, 1}].$$

JESZCZE KILKA WŁASNOŚCI

Definicja. Ułamek łańcuchowy jest ułamkiem okresowym **czystym**, jeśli

$$[a_0; a_1, a_2, \ldots] = [\overline{a_0; a_1, a_2, \ldots, a_n}].$$

Przykład. Ułamek

$$\alpha = \frac{3+\sqrt{15}}{3} = [3; 2, 3, 2, 3, 2, 3, 2, \ldots] = [\overline{3; 2}]$$

jest czysty; natomiast ułamek

$$\sqrt{7} = [2; 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \ldots] = [2; \overline{1, 1, 1, 4}]$$

nie jest czysty.

Twierdzenie 17. Niewymierność kwadratowa α ma rozwinięcie na ułamek łańcuchowy okresowy czysty wtedy i tylko wtedy, gdy

$$\alpha > 1 \quad \text{oraz} \quad -1 < \alpha' < 0.$$

Na zakończenie podamy postać rozwinięcia pierwiastków kwadratowych. Mianowicie, jeśli D nie jest kwadratem liczby całkowitej, to

$$\sqrt{D} = [a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}].$$

Przykłady:

$$\begin{aligned}
\sqrt{31} &= [5; \overline{1, 1, 3, 5, 3, 1, 1, 10}], \\
\sqrt{53} &= [7; \overline{3, 1, 1, 3, 14}], \\
\sqrt{73} &= [8; \overline{1, 1, 5, 5, 1, 1, 16}], \\
\sqrt{94} &= [9; \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}],
\end{aligned}$$

ROZKŁADANIE LICZB NA CZYNNIKI PIERWSZE

Zagadnienie odróżniania liczb pierwszych od złożonych i rozkładanie tych ostatnich na ich czynniki pierwsze uchodzi za najważniejsze i o dużym praktycznym znaczeniu w arytmetyce. ... Sama powaga nauki zdaje się wymagać, aby dołożyć wszelkich możliwych starań do rozwiązania tak eleganckiego i tak słynnego zagadnienia.

Gauss (1801)

NIECO HISTORII

Fermat przypuszczał, że każda liczba postaci

$$F_n = 2^{2^n} + 1$$

jest liczbą pierwszą. Liczby

$$\begin{aligned}
F_0 &= 2^1 + 1 = 3, \\
F_1 &= 2^2 + 1 = 5, \\
F_2 &= 2^4 + 1 = 17, \\
F_3 &= 2^8 + 1 = 257, \\
F_4 &= 2^{16} + 1 = 65537
\end{aligned}$$

rzeczywiście są pierwsze (i Fermat to wiedział).

Euler wykazał, że każdy dzielnik liczby F_n (dla $n \geq 2$) ma postać

$$k \cdot 2^{n+2} + 1$$

i w ten sposób wykazał, że

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417.$$

Zauważmy, że

$$641 = 5 \cdot 2^7 + 1.$$

Hipoteza Fermata okazała się (jak dotychczas wiadomo) bardzo nietrafna: nie znamy żadnej innej liczby pierwszej F_n poza wymienionymi wyżej, ale nie wiemy, czy takie istnieją, czy nie. Problemem jest natomiast znalezienie rozkładu tych liczb, o których już wiadomo, że są złożone.

E. Lucas udowodnił, że liczba F_6 jest złożona, a w 1880 r. F. Landry (w wieku 82 lat) znalazł rozkład

$$F_6 = 2^{64} + 1 = 18446744073709551617 = 274177 \cdot 67280421310721.$$

Wiemy również, że Clausen w liście do Gaussa z 1 stycznia 1856 r. podał ten rozkład.

Następną liczbę Fermata rozłożono na czynniki dopiero w 1970 r. Największą liczbą Fermata, której rozkład znamy, jest F_{11}, ale nie znamy rozkładu liczby F_{10}. Wiemy tylko, że

$$F_{10} = 455925777 \cdot 6487031809 \cdot C291,$$

gdzie Cm oznacza liczbę złożoną mającą m cyfr (w zapisie dziesiętnym). Wiemy również, że liczby do F_{22} są złożone.

Próbowano też rozkładać na czynniki liczby Mersenne'a. W październiku 1903 roku na posiedzeniu AMS w Nowym Yorku F. N. Cole wygłosił referat pt. *O rozkładzie na czynniki dużych liczb.* Cole, który zawsze był małomówny, bez słowa wykonał na tablicy wszystkie działania, by obliczyć 2^{67}, a następnie pracowicie odjął jedynkę. Następnie, na innej części tablicy, wykonał mnożenie

$$193707721 \cdot 761838257287.$$

Okazało się, że wyniki były zgodne... Cole bez słowa usiadł. Nie było pytań, ale publiczność zgotowała prelegentowi owację.

OSZACOWANIE TRUDNOŚCI

W 1874 roku W. Stanley Jevons stwierdził, że tylko on będzie znał czynniki pierwsze liczby 10-cyfrowej

$$8616460799.$$

Ok. 1925 roku Bancroft Brown już znał te czynniki:

$$8616460799 = 96079 \cdot 89681.$$

W 1967 roku J. Brillhart i J. Selfridge stwierdzili, że:

... w ogólności nie można oczekiwać niczego prócz frustracji przy rozkładaniu na czynniki liczby mającej 25 cyfr lub więcej, nawet przy obecnej szybkości komputerów.

W 1976 roku R. Guy stwierdził:

Będę zdziwiony, jeśli ktoś będzie potrafił przed końcem tego wieku rozkładać na czynniki liczby mające 80 cyfr i nie mające specjalnej postaci.

W 1977 roku, w artykule na temat RSA opublikowanym w *Scientific American* R. Rivest oszacował, że rozłożenie na czynniki wybranej przez autorów liczby 129-cyfrowej będzie wymagało więcej niż „40 kwadrylionów lat", nawet jeśli użyje się komputera szybszego od wszystkich istniejących. Tę liczbę rozłożono na czynniki w 1994 roku.

MOC OBLICZENIOWA

Jednostką mocy obliczeniowej będzie mips-year (1 rok pracy komputera wykonującego milion operacji na sekundę): jest to rok pracy komputera DEC VAX 11/780.

Rekordy rozkładu na czynniki:

rok	liczba cyfr
1964	20
1974	45
1984	71
1994	129
1999	155

Moc obliczeniowa wykorzystana do rekordowego rozkładu:

rok	mips-years
1974	$0,001$
1984	$0,1$
1994	5000
1999	8000

Rozkład 129-cyfrowej liczby RSA-129 (jeden z najbardziej spektakularnych) trwał ponad 8 miesięcy. Główna część pracy była wykonana przez ok. 600 ochotników z ponad 20 krajów. Obliczenia zostały dokończone przez superkomputer.

ALGORYTM ρ POLLARDA

Niech $f : S \to S$ będzie „losową" funkcją, gdzie S jest zbiorem mającym n elementów. Definiujemy ciąg

$$x_0, x_1, x_2, \ldots$$

elementów zbioru S wzorem rekurencyjnym

$$x_{i+1} = f(x_i)$$

dla $i \geq 0$.

Fakt. Oczekiwana długość „ogona" i oczekiwana długość cyklu wynosi $\sqrt{\pi n/8}$. ♠

Niech p będzie dzielnikiem pierwszym liczby n. Definiujemy ciąg

$$x_0 = 2, \quad x_{i+1} = f(x_i) = x_i^2 + 1 \operatorname{\mathbf{mod}} p.$$

Za pomocą algorytmu Floyda szukamy m takiego, by

$$x_m \equiv x_{2m} \pmod{p}.$$

Wtedy

$$\mathrm{NWD}(x_m - x_{2m}, n) > 1.$$

Jeśli również

$$\mathrm{NWD}(x_m - x_{2m}, n) < n,$$

to znaleźliśmy nietrywialny dzielnik liczby n.

ALGORYTM I PRZYKŁAD

Algorytm.

Dane: liczba złożona n;

Wynik: nietrywialny dzielnik p liczby n;

(1) $a := 2$, $b := 2$;

(2) powtarzaj:

(2.1) $a := a^2 + 1 \,\mathbf{mod}\, n$, $b := b^2 + 1 \,\mathbf{mod}\, n$, $b := b^2 + 1 \,\mathbf{mod}\, n$;
(2.2) $d := \mathrm{NWD}(a - b, n)$;

(2.3) jeśli $1 < d < n$, to zwróć wynik $p = d$.

Weźmy przykład: $n = 455459$. Kolejne kroki algorytmu wyglądają następująco:

a	b	d
5	26	1
26	2871	1
677	179685	1
2871	155260	1
44380	416250	1
179685	43670	1
121634	164403	1
155260	247944	1
44567	68343	743

Stąd otrzymujemy rozkład $455459 = 743 \cdot 613$.

UWAGI

Zakładając, że wybrana funkcja f działa losowo, oczekiwany czas działania algorytmu Pollarda wynosi $O(\sqrt{p})$, czyli $O(n^{1/4})$.

W przypadku niepowodzenia funkcję f zastępujemy inną, np.

$$f(x) = x^2 + c$$

dla $c \neq 0, -2$.

Istnieją ulepszenia algorytmu Pollarda, np. metoda pochodząca od Brenta. Polega ona na tym, że w każdym kroku obliczamy tylko jedną wartość funkcji f i następnie obliczamy $\mathrm{NWD}(x_i, x_{2^m-1})$, gdzie liczby m oraz i spełniają nierówności

$$2^{m+1} - 2^m \leq i \leq 2^{m+1} - 1.$$

Ta wersja algorytmu Pollarda jest ok. 24% szybsza od oryginalnej.

METODA FERMATA

Niech n będzie liczbą złożoną nieparzystą. Zamiast rozkładu liczby n na czynniki

$$n = a \cdot b$$

szukamy rozkładu na różnicę kwadratów:

$$n = t^2 - s^2.$$

To jest równoważne.

Na ogół badamy liczby postaci $t^2 - n$, gdzie $t > \lfloor\sqrt{n}\rfloor$ i sprawdzamy, czy któraś z tych liczb jest pełnym kwadratem.

Niech na przykład $n = 200819$. Wtedy

$$\lfloor\sqrt{200819}\rfloor = 448.$$

Następnie

$$\begin{aligned} 449^2 - 200819 &= 782, \\ 450^2 - 200819 &= 1681 = 41^2. \end{aligned}$$

Zatem

$$200819 = 450^2 - 41^2 = (450 - 41)(450 + 41) = 409 \cdot 491.$$

Ta metoda daje szybko wynik, jeśli oba czynniki liczby n są „bliskie siebie”.

UOGÓLNIENIA

Możemy również szukać takich liczb t i s, dla których

$$t^2 - kn = s^2,$$

gdzie k jest niedużą liczbą naturalną. Wtedy

$$kn = t^2 - s^2 = (t + s)(t - s)$$

i nietrywialny dzielnik n możemy znaleźć obliczając

$$\mathrm{NWD}(t + s, n).$$

Niech na przykład $n = 141467$. Wtedy

$$\lfloor\sqrt{3 \cdot 141467}\rfloor = 651.$$

Szybko znajdujemy rozkład:

$$655^2 - 3 \cdot 141467 = 68^2.$$

Wtedy

$$\mathrm{NWD}(655 + 68, 141467) = 241,$$

skąd dostajemy

$$141467 = 241 \cdot 587.$$

Metoda bezpośrednia dałaby rozkład dopiero po 38 próbach:

$$\lfloor \sqrt{141467} \rfloor = 376$$

oraz

$$414^2 - 141467 = 173^2.$$

BAZY ROZKŁADU

Wybieramy zbiór $S = \{p_1, p_2, \ldots, p_t\}$ liczb pierwszych. Czasami przyjmujemy, że $p_1 = -1$ (następne liczby są nadal liczbami pierwszymi). Zbiór S nazywamy **bazą rozkładu**.

Szukamy par liczb (a_i, b_i) spełniających następujące dwa warunki:

(1) $a_i^2 \equiv b_i \pmod{n}$;

(2) $b_i = \prod\limits_{j=1}^{t} p_j^{e_{ij}}$, gdzie $e_{ij} \geq 0$.

Zatem każda liczba b_i rozkłada się na czynniki pierwsze należące do wybranej bazy rozkładu S. Liczba $p_1 = -1$ jest wybrana dlatego, że czasami wygodnie jest rozpatrywać ujemne liczby b_i.

Następnie znajdujemy pary

$$(a_{i_1}, b_{i_1}), (a_{i_2}, b_{i_2}), \ldots, (a_{i_k}, b_{i_k})$$

takie, że iloczyn

$$b = b_{i_1} \cdot b_{i_2} \cdot \ldots \cdot b_{i_k}$$

jest pełnym kwadratem: $b = c^2$. Niech następnie

$$a = a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_k}.$$

Wtedy

$$a^2 \equiv c^2 \pmod{n}.$$

Jeśli

$$a \not\equiv \pm c \pmod{n},$$

to $\mathrm{NWD}(a+c,n)$ jest nietrywialnym dzielnikiem liczby n.

Jeśli natomiast

$$a \equiv \pm c \pmod{n},$$

to wybieramy inny zbiór par $(a_{i_1}, b_{i_1}), \ldots, (a_{i_k}, b_{i_k})$ lub inny zbiór par mających własności (1) i (2).

Ten opis algorytmu rozkładu jest niekompletny z trzech powodów:

(i) nie wiadomo, w jaki sposób wybrać bazę rozkładu; w szczególności nie wiadomo, ile liczb pierwszych do niej wziąć;

(ii) nie wiadomo, w jaki sposób szukać par (a_i, b_i) spełniających warunki (1) i (2);

(iii) nie wiadomo, w jaki sposób wybierać pary, dla których iloczyn liczb b_i jest kwadratem.

Dość łatwo odpowiedzieć na pytanie (iii). Mianowicie, jeśli

$$b_i = \prod_{j=1}^{t} p_j^{e_{ij}},$$

to tworzymy wektor zerojedynkowy

$$(e_{i1} \,\mathbf{mod}\, 2, e_{i2} \,\mathbf{mod}\, 2, \ldots, e_{it} \,\mathbf{mod}\, 2).$$

Wybieramy następnie takie pary, dla których suma odpowiednich wektorów jest wektorem zerowym. Widzimy, że w tym celu wystarczy wziąć zbiór wektorów liniowo zależny nad ciałem $\mathbb{Z}_2$. To możemy zrobić za pomocą eliminacji Gaussa. Wystarczy, by liczba par była większa od t.

Odpowiedź na pytanie (ii) jest trudniejsza. Jedną z wielu metod jest wybieranie losowo liczb a_i i rozkładanie liczb b_i na czynniki. Zauważmy, że nie musimy stosować tu żadnego specjalnego algorytmu rozkładu: wystarczy sprawdzić, czy otrzymana liczba b_i jest iloczynem liczb pierwszych należących do bazy rozkładu S. To daje tzw. **algorytm Dixona**.

Inny pomysł polega na wybieraniu liczb a_i w taki sposób, by otrzymana liczba b_i była odpowidnio mała. Można na przykład brać liczby a_i bliskie liczbom

$$\lfloor \sqrt{kn} \rfloor$$

dla małych wartości k i dla każdej takiej liczby a_i wybrać liczbę b_i o najmniejszej wartości bezwzględnej i przystającą do a_i^2 modulo n.

Jeszcze inny pomysł polega na wykorzystaniu ułamków łańcuchowych. Pomysł ten jest przypisywany jeszcze Legengre'owi, a na pewno jest znany od lat 30-tych XX wieku. Algorytm ten nie nadaje się jednak do obliczeń „ręcznych", więc znalazł zastosowanie dopiero wtedy, gdy zaczęto używać komputerów do obliczeń teorioliczbowych. Za pomocą tego algorytmu Morrison i Brillhart w 1970 roku (publikacja z 1975 r.) rozłożyli na czynniki liczbę F_7, mającą 39 cyfr.

UŁAMKI ŁAŃCUCHOWE

Przypomnimy algorytm rozwijania niewymierności kwadratowej na ułamek łańcuchowy:

Algorytm. Dana jest liczba naturalna N.

$$\alpha = \frac{a+\sqrt{b}}{c}.$$

Najpierw kładziemy

$$P_0 = 0, \quad Q_0 = 1.$$

Wtedy

$$\sqrt{N} = \frac{P_0+\sqrt{N}}{Q_0} \text{ oraz } Q_0 \mid (N - P_0^2).$$

Następnie definiujemy

$$\begin{aligned} \alpha_k &= \frac{P_k+\sqrt{N}}{Q_k}, \\ a_k &= \lfloor \alpha_k \rfloor, \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= \frac{N - P_{k+1}^2}{Q_k}. \end{aligned}$$

Uwaga: Można pokazać, że $Q_k \mid (N - P_{k+1}^2)$.

Wreszcie:

$$\sqrt{N} = [a_0; a_1, a_2, \ldots, a_k, \ldots].$$

UPROSZCZENIA ALGORYTMU

Oznaczmy $g = \lfloor\sqrt{N}\rfloor$. Wtedy

$$\left\lfloor \frac{P_k + \sqrt{N}}{Q_k} \right\rfloor = \left\lfloor \frac{P_k + g}{Q_k} \right\rfloor.$$

Następnie

$$P_k + g = a_k \cdot Q_k + r_k, \quad 0 \leq r_k < Q_k.$$

W ten sposób obliczamy a_k i r_k.

Teraz

$$P_{k+1} = a_k Q_k - P_k = P_k + g - r_k - P_k = g - r_k,$$

skąd dostajemy

$$P_{k+1} + g = 2g - r_k.$$

W ten sposób obliczamy $P_{k+1} + g$. Zauważmy, że zamiast P_k możemy zawsze obliczać $P_k + g$.

Wreszcie można pokazać, że

$$\frac{N - P_k^2}{Q_k} = Q_{k-1},$$

skąd wynika, że

$$Q_{k+1} = \frac{N - P_{k+1}^2}{Q_k} = \ldots = Q_{k-1} + a_k(r_k - r_{k-1}).$$

W ten sposób obliczamy Q_{k+1}.

Można dowieść, że zachodzą następujące nierówności:

$$0 < P_k + g < 2\sqrt{N}, \quad 0 < Q_k < 2\sqrt{N}.$$

Liczniki reduktów obliczamy ze wzoru rekurencyjnego

$$p_k = a_k p_{k-1} + p_{k-2}.$$

Mianowniki q_k nie będą potrzebne do dalszych obliczeń, więc nie musimy ich obliczać. Liczniki będą potrzebne tylko modulo N.

Twierdzenie 18. Przy powyższych oznaczeniach

$$p_k^2 - N q_k^2 = (-1)^{k-1} Q_{k+1}. \quad \spadesuit$$

PRZYKŁAD

Niech $n = 197209$. Wtedy

$$\sqrt{197209} = [444; 12, 6, 23, 1, 5, 3, 1, 26, 6, 2, 36, \ldots].$$

Popatrzmy na dwa redukty. Pierwszy to:

$$[444; 12, 6, 23] = \frac{750943}{1691}.$$

W tym przypadku otrzymujemy kongruencję

$$750943^2 \equiv 720 \pmod{197209},$$

czyli

$$159316 \equiv 720 \pmod{197209}.$$

Drugi to:

$$[444; 12, 6, 23, 1, 5, 3, 1, 26, 6].$$

W tym przypadku dostaniemy

$$133218 \equiv 405 \pmod{197209}.$$

Teraz mamy

$$720 = 2^4 \cdot 3^2 \cdot 5$$

oraz

$$405 = 3^4 \cdot 5.$$

Zatem

$$720 \cdot 405 = 2^4 \cdot 3^6 \cdot 5^2 = (2^2 \cdot 3^3 \cdot 5)^2 = 540^2.$$

A więc

$$(159316 \cdot 133218)^2 \equiv 540^2 \pmod{197209},$$

czyli

$$126308^2 \equiv 540^2 \pmod{197209}.$$

Wreszcie

$$\mathrm{NWD}(126308 + 540, 197209) = 991,$$

skąd dostajemy

$$197209 = 199 \cdot 991.$$

BAZY ROZKŁADU – PRZYPOMNIENIE

Wybieramy bazę rozkładu $S = \{p_1, p_2, \ldots, p_t\}$. Przyjmujemy, że $p_1 = -1$, a następne liczby są liczbami pierwszymi.

Szukamy par liczb (a_i, b_i) spełniających następujące dwa warunki:

(1) $a_i^2 \equiv b_i \pmod{n}$;

(2) $b_i = \prod_{j=1}^{t} p_j^{e_{ij}}$, gdzie $e_{ij} \geq 0$.

Następnie znajdujemy pary $(a_{i_1}, b_{i_1}), (a_{i_2}, b_{i_2}), \ldots, (a_{i_k}, b_{i_k})$ takie, że iloczyn

$$b = b_{i_1} \cdot b_{i_2} \cdot \ldots \cdot b_{i_k}$$

jest pełnym kwadratem: $b = c^2$. Niech następnie

$$a = a_{i_1} \cdot a_{i_2} \cdot \ldots \cdot a_{i_k}.$$

Wtedy

$$a^2 \equiv c^2 \pmod{n}.$$

Jeśli

$$a \not\equiv \pm c \pmod{n},$$

to $\mathrm{NWD}(a + c, n)$ jest szukanym dzielnikiem liczby n. W przeciwnym przypadku wybieramy inny zbiór par $(a_{i_1}, b_{i_1}), \ldots, (a_{i_k}, b_{i_k})$ lub inny zbiór par mających własności (1) i (2).

SITO KWADRATOWE

Rozkładamy na czynniki liczbę n. Niech $m = \lfloor \sqrt{n} \rfloor$. Bierzemy wielomian

$$W(x) = (x + m)^2 - n.$$

Zauważmy, że

$$W(x) \approx x^2 + 2mx,$$

a więc dla małych (w porównaniu z n) wartości x wartość wielomianu jest mała, a zatem może rozłożyć się na małe czynniki pierwsze.

Dla $x = 0, \pm 1, \pm 2, \pm 3, \ldots$ obliczamy

$$a_i = x + m$$

oraz

$$b_i = W(x) = (x+m)^2 - n.$$

Wtedy

$$a_i^2 = (x+m)^2 \equiv b_i \pmod{n}.$$

Zauważmy również, że jeśli $p \mid b_i$, to

$$(x+m)^2 \equiv n \pmod{p},$$

a więc n jest resztą kwadratową modulo p. Zatem do bazy rozkładu można brać tylko liczby pierwsze p takie, że $\left(\frac{n}{p}\right) = 1$. Ponieważ $W(x)$ może być liczbą ujemną, więc do bazy rozkładu bierzemy również $p_1 = -1$.

PRZYKŁAD

Niech $n = 24961$. Wtedy $m = 157$. Bierzemy bazę rozkładu

$$S = \{-1, 2, 3, 5, 13, 23\}.$$

Zauważmy, że liczby 7, 11, 17 i 19 wykluczyliśmy, gdyż dla tych liczb p liczba n nie jest resztą kwadratową modulo p.

A oto wyniki obliczeń dla wybranych wartości x:

i	x	$W(x)$	rozkład $W(x)$	a_i	$\overrightarrow{e_i}$
1	0	-312	$-2^3 \cdot 3 \cdot 13$	157	$(1,1,1,0,1,0)$
2	1	3	3	158	$(0,0,1,0,0,0)$
3	-1	-625	-5^4	156	$(1,0,0,0,0,0)$
4	2	320	$2^6 \cdot 5$	159	$(0,0,0,1,0,0)$
5	-2	-936	$-2^3 \cdot 3^2 \cdot 13$	155	$(1,1,0,0,1,0)$
6	4	960	$2^6 \cdot 3 \cdot 5$	161	$(0,0,1,1,0,0)$
7	-6	-2160	$-2^4 \cdot 3^3 \cdot 5$	151	$(1,0,1,1,0,0)$

Zauważmy, że

$$\overrightarrow{e_1} + \overrightarrow{e_2} + \overrightarrow{e_5} = \overrightarrow{0}.$$

Wtedy

$$a = (a_1 \cdot a_2 \cdot a_5) \,\mathbf{mod}\, n = 936$$

oraz

$$b = 2^6 \cdot 3^4 \cdot 13^2,$$

czyli

$$c = 2^3 \cdot 3^2 \cdot 13 \,\mathbf{mod}\, n = 24025.$$

Mamy
$$a^2 \equiv c^2 \pmod{n},$$
ale również
$$a \equiv -c \pmod{n}.$$
Zatem ten zestaw wektorów liniowo zależnych nie dał rozkładu liczby n na czynniki.

Mamy też
$$\overrightarrow{e_3} + \overrightarrow{e_6} + \overrightarrow{e_7} = \overrightarrow{0}.$$
Wtedy
$$a = (a_3 \cdot a_6 \cdot a_7) \,\mathbf{mod}\, n = 23405$$
oraz
$$b = 2^{10} \cdot 3^4 \cdot 5^6,$$
czyli
$$c = 2^5 \cdot 3^2 \cdot 5^3 \,\mathbf{mod}\, n = 13922.$$
Mamy
$$a^2 \equiv c^2 \pmod{n},$$
oraz
$$a \not\equiv -c \pmod{n}.$$
Tym razem
$$\mathrm{NWD}(23405 - 13922, 24961) = \mathrm{NWD}(9483, 24961) = 109,$$
skąd dostajemy rozkład
$$24961 = 109 \cdot 229.$$

PRZESIEWANIE

Istotą algorytmu **sita kwadratowego** jest nie to, w jaki sposób generujemy pary (a_i, b_i), ale to, w jaki sposób rozkładamy liczby b_i na czynniki.

Większość z nich nie rozkłada się na czynniki należące do wybranej bazy rozkładu; próba faktoryzacji jest ewidentną stratą czasu. Co więcej, próba dzielenia przez kolejne liczby p_j jest na ogół stratą czasu.

Okazuje się, że możemy z góry przewidzieć, które liczby będą się dzielić przez liczbę p_i. Zauważmy, że dla dowolnego wielomianu $W(x)$ mamy równoważność
$$W(x) \equiv 0 \pmod{p} \quad \Leftrightarrow \quad W(x + kp) \equiv 0 \pmod{p}.$$

Zatem, jeśli x_1 i x_2 są dwoma różnymi pierwiastkami wielomianu $W(x)$ modulo p (dla przypomnienia: $W(x)$ jest wielomianem kwadratowym), to wszytkie pierwiastki tego wielomianu modulo p są wyrazami dwóch ciągów arytmetycznych:

$$x_1 + kp \text{ oraz } x_2 + kp$$

(dla $k \in \mathbb{Z}$). I tylko te liczby będziemy dzielić przez p.

PRZYKŁAD

Powroćmy do naszego przykładu. Dla przypomnienia:

$$\begin{aligned} n &= 24961, \\ m &= \lfloor\sqrt{24961}\rfloor = 157, \\ S &= \{-1, 2, 3, 5, 13, 23\}, \\ W(x) &= (x+m)^2 - n. \end{aligned}$$

Umieszczamy w tablicy S (czyli w sicie) wartości wielomianu $W(x)$ dla $x = -11, \ldots, 15$.

Następnie rozwiązujemy kongruencje postaci

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

dla $p = 3, 5, 13, 15$. Otrzymujemy rozwiązania:

p	x_1	x_2
3	0	1
5	2	4
13	0	11
23	15	16

Teraz przesiewamy. Najpierw dla x parzystych (wtedy liczba $W(x)$ jest też parzysta) dzielimy $S[x]$ przez 2 tyle razy, ile się da.

Potem dla x takich, że

$$x \equiv 0 \pmod{3} \text{ lub } x \equiv 1 \pmod{3}$$

dzielimy $S[x]$ przez 3 (też tyle razy, ile się da).

Robimy to samo dla

$$x \equiv 2 \pmod{5} \text{ lub } x \equiv 4 \pmod{5},$$

dla

$$x \equiv 0 \pmod{13} \text{ lub } x \equiv 11 \pmod{13}$$

i wreszcie dla

$$x \equiv 15 \pmod{23} \text{ lub } x \equiv 16 \pmod{23}.$$

Oczywiście w innej tablicy zapamiętujemy, ile razy podzieliliśmy przez każdą liczbę z bazy rozkładu. Można też rozwiązywać kongruencje modulo p^k dla coraz większych k; to jeszcze bardziej przyspieszy algorytm.

Wyniki przesiewania (tzn. tylko dzielenia, bez zapamiętanych wykładników potęg liczb p_i) są zawarte w następującej tabeli:

x	$W(x)$	2	3	5	13	23
−11	−3645		−5	−1		
−10	−3352	−419				
−9	−3057		−1019			
−8	−2760	−345	−115	−23		−1
−7	−2461					−107
−6	−2160	−135	−5	−1		
−5	−1857		−619			
−4	−1552	−97				
−3	−1245		−415	−83		
−2	−936	−117	−13		−1	
−1	−625			−1		
0	−312	−39	−13		−1	
1	3		1			
2	320	5		1		
3	639		71			
4	960	15	5	1		
5	1283					
6	1608	201	67			
7	1935		215	43		
8	2264	283				
9	2595		865	173		
10	2928	183	61			
11	3263				251	
12	3600	225	25	1		
13	3939		1313		101	
14	4280	535		107		
15	4623		1541			67

ZŁOŻONOŚĆ OBLICZENIOWA

Definiujemy funkcję

$$L_q[\alpha, c] = \exp((c + o(1))(\ln q)^\alpha (\ln \ln q)^{1-\alpha}).$$

Przy optymalnym wyborze parametrów (wielkość bazy rozkładu oraz wielkość sita) algorytm sita kwadratowego działa w czasie $O(L_n[\frac{1}{2}, 1])$.

Odkryty kilka lat temu algorytm **sita ciał liczbowych** (general number sieve field, w skrócie GNFS) działa w czasie $O(L_n[\frac{1}{3}, c])$ dla stałej $c = (\frac{64}{9})^{\frac{1}{3}} \approx 1,923$.

Specjalna wersja tego algorytmu (special number field sieve, w skrócie SNFS), która jest wykorzystywana do rozkładu liczb postaci $n = r^k - s$ dla małych r i $|s|$, działa w czasie $O(L_n[\frac{1}{3}, c])$ dla stałej $c = (\frac{32}{9})^{\frac{1}{3}} \approx 1,526$.