Podzielność liczb; liczby pierwsze

Tabele faktoryzacji liczb

- 1659, Zurych – J.H. Rahn *Teusche Algebra* czynniki pierwsze liczb do 24 000 (nieparzyste, niepodzielne przez 5).
- 1668, Londyn – John Pell (1610-1685)
  rozszerzenie tablic do 100 000.
- J. J. Lambert (1728-1777), niemiecki matematyk i fizyk; zainicjował „szeroką akcję" tworzenia tabel rozkładu liczb na czynniki pierwsze;
- 1776, Wiedeń – Anton Felkel – do 408 000 (w rękopisie znacznie dalej) ale . . . wydruk skonfiskowano i z papieru sporządzono . . . naboje (wojna z Turkami)
- XIX w., Chernac, Burckhardt, Crelle, Glaisher, Dase – do 10^7; publikacje w oddzielnych tomach dla każdego miliona
- J.P. Kulik (Praga) (1773–1863) – tablice rozkładu na czynniki pierwsze aż do 100 000 000
  (rękopis złożony w bibliotece cesarskiej w Wiedniu)
- 1909 – Derrick Norman Lehmer *Factor Table for the First Ten Million* – tablice rozkładu na czynniki pierwsze.
- od ca. 1952 roku nastała era komputerów;

Metoda faktoryzacji Fermata

Podstawowa metoda rozkładu na czynniki opiera się na pomyśle

$$n = x^2 - y^2 = (x - y)(x + y), \tag{1}$$

a więc dla $n = ab;\ b \geqslant a$ musi zachodzić $a = x - y,\ b = x + y,$ czyli $x = \dfrac{b + a}{2}$ i $y = \dfrac{b - a}{2}$.

Jak znaleźć x i y? Z (1) mamy

$x^2 = n + y^2, \quad \to x^2 > n, \quad \to x \geqslant \sqrt{n}.$

Podstawiamy kolejno za x liczby większe od $\sqrt{n}$; sprawdzamy czy $\Delta(x) = x^2 - n$ jest kwadratem.

rozkład 13 837

$\left\lfloor \sqrt{13\,837} \right\rfloor = 117; \quad \Delta(118) = 118^2 - 13\,837 = 87;$

$\Delta(119) = 119^2 - 13\,837 = 324 = 18^2.$

$13\,837 = (119 - 18)(119 + 18) = 101 \cdot 137$

Metoda faktoryzacji Fermata, c.d.

Udało nam się znaleźć faktoryzację bardzo szybko, bo ... a było bliskie b
– wtedy $y \approx 0$ i $x \approx \sqrt{n}$ (oczywiście musi być ciut większe)
Ale mamy drogę na skróty: $\Delta(x) = x^2 - n \qquad x \to x+1.$ Mamy:
$\Delta(x+1) = \Delta(x) + 2x + 1; \quad \Delta(x+2) =$
$\Delta(x+1) + 2x + 3; \quad \Delta(x+3) = \Delta(x+2) + 2x + 5; \quad \ldots.$

Przykład Fermata $n = 2\,027\,651\,281$.
$1 + \lfloor \sqrt{n} \rfloor = 45\,030$. Au travail!

$$n = 2\,027\,651\,281 \qquad 1 + \lfloor \sqrt{n} \rfloor = 45\,030$$

$x = 45030$	$x^2 - n = 49619$	$x = 45035$	$x^2 - n = 499944$
	$2x + 1 = \underline{90061}$		$2x + 11 = \underline{90071}$
31	139680	36	590015
	$2x + 3 = \underline{90063}$		$2x + 13 = \underline{90073}$
32	229743	37	680088
	$2x + 5 = \underline{90065}$		$2x + 15 = \underline{90075}$
33	319808	38	770163
	$2x + 7 = \underline{90067}$		$2x + 17 = \underline{90077}$
34	409875	39	860240
	$2x + 9 = \underline{90069}$		$2x + 19 = \underline{90079}$
35	499944	40	950319
			$2x + 21 = \underline{90081}$
		$x = 45041$	$x^2 - n = 1040400$

$1040400 = 1020^2$.

$n = (45041 - 1020) \cdot (45041 + 1020) = 46061 \cdot 44021$.

Metoda jest do użycia, jeżeli różnica dwóch czynników liczby n, $(x + y) - (x - y) = 2y$ jest niewielka – bo wtedy szybko ją zobaczymy.

Metoda faktoryzacji Eulera

Pierwsze pomysły...

2 sierpnia 1641, M. Frénicle de Berry, pracownik francuskiej mennicy, w liście do Fermata proponuje aby wykorzystać fakt, że

$$221 = 10^2 + 11^2 = 5^2 + 14^2$$

do rozkładu liczby 221 na czynniki. Mersenne znał chyba też tę metodę, ale dopiero Euler „rozpracował" ją do końca.

Metoda faktoryzacji Eulera

Mamy: $N = a^2 + b^2 = c^2 + d^2$. Liczba N jest nieparzysta; jedna z liczb (a, b) i jedna z liczb (c, d) też są nieparzyste. Niech to będą a i c. Zauważmy: z nieparzystości a wynika $a^2 = 4n + 1$, ale wiemy, że $4 \mid b^2$ a więc $\boxed{N = 4M + 1}$.

Z założenia wyjściowego wynika $(a - c)(a + c) = (d - b)(d + b)$.
Oznaczmy $k = ((a - c), (d - b))$.

$$a - c = kl, \quad d - b = km; \quad l \perp m.$$

Ponieważ $a - c$ jest – jak i $d - b$ – liczbą parzystą to k musi też być liczbą parzystą.
Podstawiamy: $kl(a + c) = km(d + b); \quad \rightarrow l(a + c) = m(d + b)$.
Wynika stąd, że $m \mid (a + c)$ (bo $l \perp m$!), a więc $(a + c) = mn;\ n \in \mathbb{Z}$.
Po podstawieniu mamy
$l(mn) = m(d + b), \quad \rightarrow d + b = ln, \quad \rightarrow n \mid (d + b)$.
W takim razie $n = (a + c, d + b)$ i musi być liczbą parzystą, bo $a + c$ i $d + b$ są parzyste.

Metoda faktoryzacji Eulera, c.d

Nasza faktoryzacja to

$$N = \left[\left(\frac{k}{2}\right)^2 + \left(\frac{n}{2}\right)^2\right](m^2 + l^2).$$

$$\frac{1}{4}\left[(km)^2 + (kl)^2 + (mn)^2 + (nl)^2\right] =$$

$$\frac{1}{4}\left[(d-b)^2 + (a-c)^2 + (a+c)^2 + (d+b)^2\right] =$$

$$\ldots = \frac{1}{4}\left[2a^2 + 2b^2 + 2c^2 + 2d^2\right] = N \qquad \square$$

Przykład: N= 221

$$\begin{array}{lll} a = 11 & a - c = 6 & k = (a-c, d-b) = 2 \\ b = 10 & a + c = 16 & l = (a-c)/k = 3 \\ c = 5 & d - b = 4 & m = (d-b)/k = 2 \\ d = 14 & d + b = 24 & n = (d+b)/k = 8 \end{array}$$

$$N = \left[\left(\frac{2}{2}\right)^2 + \left(\frac{8}{2}\right)^2\right](2^2 + 3^3) = 17 \cdot 13.$$

Metoda faktoryzacji Eulera, c.d

Przykład: N= 2501

Nawet komputer zauważy

$$N = 50^2 + 1^2$$

A drugi rozkład? Poszukaj jest bardzo blisko...

Przykład Eulera: N= 1 000 009

do zrobienia samodzielnie ...

Metoda faktoryzacji Eulera, koniec

Metoda Eulera opiera się – jak widać to było z przykładów – na fakcie, że każda liczba złożona da się przedstawić jako suma dwóch kwadratów, i to na dwa różne sposoby.
„Przy okazji" Euler udowodnił także, jedno z wielu „twierdzeń" Fermata:

Twierdzenie Fermata

Każda liczba pierwsza $p = 4n + 1$ daje się przedstawić *w jeden i tylko jeden sposób* w postaci sumy dwóch kwadratów:

$$p = 4n + 1 = \boxed{?}^2 + \boxed{?}^2.$$

dla liczb poniżej 100:

$$\begin{array}{llll} 5 = 2^2 + 1 & 13 = 3^2 + 1 & 17 = 4^2 + 1 & 29 = 5^2 + 2^2 \\ 37 = 6^2 + 1 & 41 = 5^2 + 4^2 & 53 = 7^2 + 2^3 & 61 = 6^2 + 5^2 \\ 73 = 8^2 + 3^2 & 89 = 5^2 + 8^2 & 97 = 9^2 + 4^2 & \end{array}$$

Metody faktoryzacji, uwagi ogólne

Przy szukaniu czynników pamiętajmy, że dużo informacji możemy uzyskać z ostatniej cyfry (ostatnich dwóch, trzech cyfr). Dla ostatniej określonej – oto jakie mogą być ostatnie cyfry czynników:

1	$(1,1)$	$(9,9)$	$(3,7)$
3	$(1,3)$	$(7,9)$	
7	$(1,7)$	$(3,9)$	
9	$(1,9)$	$(3,3)$	$(7,7)$