Liczby pierwsze Mersenne'a i Fermata

Liczby dwumianowe $N = a^n \pm b^n$

Tak zwane *liczby dwumianowe* $N = a^n \pm b^n$ łatwo poddają się faktoryzacji. Wynika to z wzorów (polecam sprawdzenie!)

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}\right)$$

a także (zmieniamy $b \to (-b)$, ale n *musi* być liczbą nieparzystą

$$a^n + b^n = (a+b)\left(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1}\right).$$

Kładąc teraz $a \to a^m$, $b \to b^m$ — na przykład w pierwszym wzorze dostaniemy

$$a^{mn} - b^{mn} = (a^m - b^m)\left(a^{(n-1)m} + a^{(n-2)m}b^m + \ldots + a^m b^{m(n-2)} + b^{m(n-1)}\right).$$

na przykład dla $N = 10^9 - 3^9 = 999\,980\,317$ mamy $10 - 3 = 7$ i $10^3 - 3^3 = 7 \cdot 139$, co daje $N = 7 \cdot 19 \cdot 139 \cdot 54\,091$.
Podobnie – do samodzielnego zrobienia – można rozłożyć na czynniki $N = 10^9 + 3^9$.

Liczby dwumianowe $N = b^n - 1$

zachodzi twierdzenie ...

dla $b \perp m$; $a, c > 0$; jeżeli

$b^a \equiv 1 \bmod m$ i $b^c \equiv 1 \bmod m \to b^d \equiv 1 \bmod m, \quad d = (a, c)$.

(dowód podamy przy rachunku kongruencji — $a \equiv k \bmod m$ oznacza: reszta z dzielenia a przez m równa jest k.)

...z którego wynika kolejne twierdzenie

Jeżeli liczba pierwsza p dzieli N — $p \mid b^n - 1$ to

(1) albo $p \mid b^d - 1$, gdzie $d \mid n$; albo

(2) $p \equiv 1 \bmod n$. Dla $p > 2$ i dla $n = 2k + 1$ mamy $p \equiv 1 \bmod 2n$.

Na przykład jeżeli liczba $2^{11} - 1$ ma mieć dzielnik p to na mocy ostatniego twierdzenia $p = k \cdot 22 + 1$ – rzeczywiście $2047 = 23 \cdot 89$.

a liczba $2^{13} - 1$ – czy ma dzielnik p? Kandydatami mogą być tylko $p = k \cdot 26 + 1$ i to mniejsze od $\sqrt{N} \approx 90$. Wszystkie trzy kandydatki 27, 53 i 79 nie dzielą N z czego wynika, że N jest liczbą pierwszą!

Liczby Mersenne'a ...

to szczególny przypadek wzorów z poprzedniej strony. Są to liczby

$$M_n = 2^n - 1$$

i były one przedmiotem intensywnych studiów, głównie w kontekście *liczb doskonałych*. Jak już wspomnieliśmy, każda liczba Mersenne'a będąca liczbą pierwszą określa pewną liczbę doskonałą, które to liczby stanowiły przed wiekami i przez całe wieki obiekt przeróżnych dywagacji pseudo-matematycznych.

Dla złożonego wykładnika $n = rs$ liczba Mersenne'a musi też być liczbą złożoną (wynika to z relacji z poprzedniej strony!). Aby liczba Mersenna była liczbą pierwszą wykładnik n musi być liczbą pierwszą

$$M_p = 2^p - 1.$$

Rzeczywiście dla $p = 2, 3, 5, 7$ a potem dla $13, 17, 19$ liczby M_p są liczbami pierwszymi, ale liczba $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ jest liczbą złożoną (wiedziano już o tym w 16 w.). Wraz ze wzrostem p mamy tych liczb pierwszych M_P coraz to mniej; jeszcze 50 lat temu znano ich poniżej dwudziestki.

Ciekawy jest niesłychanie „rozwój świadomości” nt. tych liczb.
Sam Mersenne w swoich *Cogitata Physico-Mathematica* (1644) autorytatywnie stwierdza, że M_p są „pierwsze” dla $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ a złożone dla pozostałych $p \leqslant 257$. (O 17 i 19 wiedziano już na początku 17 w. – Cataldi).
Braciszek Mersenne nie wyjaśnił podstaw swoich stwierdzeń.
Czy były to tylko domysły?
Liczba M_{127} to – bagatela 39 cyfr, a M_{257} – 78.
Następne uściślenia zawdzięczamy Eulerowi. Potwierdził on „pierwszość” M_{31}, sugerował (błędnie – potem poprawił się) także „pierwszość” M_{41} i M_{47}.
Jasny obraz sytuacji dla $p \leqslant 257$ pojawił się dopiero . . . 300 lat po publikacji Mersenne’a. M. popełnił tylko (aż?) 5 błędów; liczby M_{61}, M_{89} i M_{107} są pierwsze, natomiast M_{67} i M_{257} – złożone.
Faktoryzację M_{67} przedstawił Cole (1903) na posiedzeniu $\mathcal{AMS}$ (chociaż już w 1876 Lucas stwierdził, przy pomocy opracowanego przez siebie testu, że nie jest to liczba pierwsza – ale nie potrafił znaleźć rozkładu). $(193\,707\,721 \times 761\,838\,257\,287)$;
faktoryzację M_{257} przedstawił Krajczyk (1903).

Wraz z nadejściem ery komputerów (początek lat 1960) trochę ich przybyło, ale nie tak znowu wiele. W latach 1995-6 rozpoczęto akcje Great Internet Search (for) Mersenne Primes (GIMPS) i do chwili obecnej dorobiono się (listopad 2006) 44-ej liczby Mersenne'a (a dziesiątej w ramach GIMPS).
Jest to $M_{32\,582\,657} = 2^{32\,582\,657} - 1$ – w sumie 9 808 358 cyfr.
Jej bezpośrednia poprzedniczka to $M_{30402457} = 2^{30402457} - 1$ – skromne maleństwo , którego zapis dziesiętny miałby ponad dwie trzecie miliona cyfr mniej!
Niestety, liczba 44-ta też ma w swoim zapisie mniej niż 10 milionów cyfr – dla odkrywcy liczby z – przynajmniej – 10 milionami cyfr czeka nagroda 100 000 $.
Na wszelki wypadek podaję adres strony.
Na następnej stronie stan obecny!!

Stan A. D. 2016 – mamy już 49 liczb Mersenne'a

In 2008, on August 23rd, a UCLA computer discovered the 45th known Mersenne prime, $2^{43\,112\,609}-1$ a mammoth 12 978 189 digit number!

In 2013, on September 6th, the 46th known Mersenne prime, $2^{37\,156\,667}-1$, a 11 185 272 digit number was found by Hans-Michael Elvenich in Langenfeld near Cologne, Germany!

This was the first Mersenne prime to be discovered out of order since Colquitt and Welsh discovered $2^{110\,503}-1$ in 1988.

...

On January 25th (2014), prolific GIMPS contributor Dr. Curtis Cooper discovered the 48th known Mersenne prime, $2^{57\,885\,161}-1$, a 17 425 170 digit number. This find shatters the previous record prime number of 12 978 189 digits, also a GIMPS prime, discovered over 4 years ago. The discovery is eligible for a 3 000 GIMPS research discovery award.

Do chwili obecnej...

(styczeń 2016; znowu Curtis Cooper) znaleziono 49-tą liczbę Mersenne'a (piętnasta (!)w ramach GIMPS).
Jest to $M_{74\,207\,281} = 2^{74\,207\,281}-1$ – w sumie 22 338 618 cyfr.
Ale to 45 liczba Mersenne'a zdobyła nagrodę! (ponad 11 milionów cyfr!).
Odkrywca (GIMPS!) to Hans-Michael Elvenich.

Rozmieszczenie liczb Mersenne'a ...

Funkcja π dla liczb Mersenne'a z bardzo dobrą dokładnością jest określona jako

$$\pi_M(x) \approx \frac{e^\gamma}{\ln 2} \ln(\ln x).$$

Z tego to wzoru wynika, że ilość liczb Mersenne'a w przedziale $(x, 2x)$ wynosi w przybliżeniu e^γ; gdzie γ to stała Eulera-Mascheroniego, n.b. bardzo ciekawa liczba.
Można też wykazać, że prawdopodobieństwo że dana M_q jest liczbą pierwszą to

$$\pi\left(M_q \text{ jest liczba pierwszą }\right) = \frac{e^\gamma}{\ln 2} \frac{\ln aq}{\ln 2},$$

gdzie

$$a = \begin{cases} 2 & q \mod 4 = 3 \\ 6 & q \mod 4 = 1 \end{cases}$$

Liczby Fermata

Liczby postaci

$$N_n = 2^n + 1$$

potrafimy bez trudu rozłożyć na czynniki jeżeli $n = ab$ i (przynajmniej) jeden z tych czynników jest liczbą nieparzystą – np. b.

$$2^n + 1 = (2^a)^b + 1 = (2^a + 1)\left(2^{a(b-1)} - 2^{a(b-2)} + 2^{a(b-3)} \ldots - 2^a + 1\right).$$

Jeżeli więc liczba N_n miałaby być liczba pierwszą to wykładnik n nie może zawierać w sobie nieparzystych czynników – $n = 2^t$. Takie właśnie liczby nazywamy *liczbami Fermata*

$$\boxed{F_t = 2^{2^t} + 1.}$$

Pierwsze liczby F: $F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65\,537$ są liczbami pierwszymi i P.F. optymistycznie uważał, że znalazł sposób – niezawodny – na generowanie liczb pierwszych.

Euler (1739) wykazał, że $F_5 = 2^{32} + 1 = 641 \cdot 6700417$.

Przy okazji udowodnił, że każdy ewentualny dzielnik pierwszy (!) liczby Fermata F_t musi mieć postać $p = 2^{t+2}k + 1; \quad k \in N$.
Tak więc dla $t = 5$ dzielnik $p = 64k + 1\,(k = 10)$.
W 150 (!) lat później znaleziono rozkład
$F_6 = 2^{64} + 1 = 274\,177 \cdot 67\,280\,421\,310\,721$.
i znowu po prawie 100 (!) latach później znaleziono rozkłady F_7 i F_8; potem znaleziono rozkłady F_9 i F_{10} i F_{11} (1990-1996).
Rozkład liczby F_{12} nie jest ciągle do końca poznany (wiemy, że jest to liczba złożona), tak zresztą jak i kolejny tuzin liczb Fermata.

Liczby Fermata – relacje rekurencyjne

Z wzoru definiującego liczby Fermata łatwo wyprowadzamy związek

$$F_{t+1} = (F_t - 1)^2 + 1$$

albo

$$F_{t+1} - 2 = F_t(F_t - 2).$$

Ten ostatni wzór generuje dość ciekawą zależność

$$F_{t+1} - 2 = F_0 F_1 \dots F_t,$$

a więc

$$F_{t-s} \mid (F_{t+1} - 2), \qquad 0 \leqslant s \leqslant t.$$

Łatwo stąd wywnioskować, że

$$F_{t-s} \perp F_{t+1}, \qquad 0 \leqslant s \leqslant t$$

– liczby Fermata są względnie pierwsze.

Liczby Fermata – różne drobiazgi

Nie wiemy, czy ...

- ... istnieje nieskończenie wiele liczb pierwszych Fermata.
- ... istnieje nieskończenie wiele liczb złożonych Fermata.
- ... każda liczba Fermata jest bezkwadratowa.

Ile cyfr ma $F_{73} = 2^{2^{73}} + 1$? korzystamy z $2^{10} = 1024 > 10^3$.

$$2^{2^{73}} = 2^{16 \cdot 2^{69}} > 2^{10 \cdot 2^{69}} = \left(2^{10}\right)^{2^{69}} > \left(10^3\right)^{2^{69}} >$$
$$\left(10^2\right)^{2^{69}} = (10)^{2^{70}} = \left(10^{2^{10}}\right)^7 > \left(10^{10^3}\right)^7 = (10)^{10^{21}}.$$

strona A4 – 2 000 cyfr; książka 500 stron – 10^6 cyfr;
biblioteka – 10^5 książek — 10^{11} cyfr
10 miliardów bibliotek.