Odwrotne twierdzenie Fermata

Przypomnijmy ...

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

Zachodzi naturalne pytanie ...

... czy z faktu $a^{m-1} \equiv 1 \pmod{m}$ wynika, że $m = p$? Niekoniecznie.

Wprawdzie, jeszcze przed 25 wiekami chińscy matematycy uważali, że podzielność przez n liczby $2^n - 2$ jest równoznaczna z pierwszością n (jeszcze trzysta trzydzieści lat temu zgadzał się z tym sam Leibniz), ale Sarrus (francuski spec od algebry, Strasbourg, 1819) pokazał, że $2^{340} \equiv 1 \pmod{341}$, mimo że $341 = 11 \cdot 31$.
Rzeczywiście: $2^{10} - 1 = 1023 = 3 \cdot 341$ dzieli $(2^{340} - 1)$ (bo $10 \mid 340$).
Podobnie mamy $3^{90} \equiv 1 \pmod{91}$, mimo że $91 = 7 \cdot 13$.

Wprowadzając pewne dodatkowe ograniczenie można sformułować ...

twierdzenie Lucasa (odwrotne do twierdzenia Fermata):

Jeżeli, dla pewnej liczby a zachodzi kongruencja $a^{m-1} \equiv 1 \pmod{m}$, natomiast *nie zachodzi* dla żadnego t; $0 < t < m - 1$ to moduł m jest liczbą pierwszą.

Dowód: z warunków twierdzenia wynika, że rząd liczby a modulo m jest równy $m-1$, a więc jest równy maksymalnej wartości $\phi(m)$, która to wartość dla modułu złożonego $m = p_1 \dots p_r$ wynosi

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_r}\right)$$

a więc zachodzi

$$\phi(m) \leqslant m\left(1 - \frac{1}{p_1}\right) = m - \frac{m}{p_1} \leqslant m - 1,$$

czyli dla $\phi(m) = m - 1$ liczba m *musi* być liczba pierwszą. Badając ewentualne spełnianie kongruencji $a^{t-1} \equiv 1 \pmod{t}$ dla $t;\ 0 < t < m-1$ wystarczy się oczywiście ograniczyć do wykładników, które są dzielnikami $m-1$.

twierdzenie Lucasa (zmodyfikowane)

Jeżeli liczby $q_1, q_2, \dots, q_s$ są dzielnikami liczby $m-1$ i – dla dowolnego a zachodzi $a^{m-1} \equiv 1 \pmod{m}$, a nie zachodzi żadna z kongruencji

$$a^{\frac{m-1}{q_i}} \equiv 1 \pmod{m}, \qquad i = 1, \dots, s$$

to liczba m jest liczbą pierwszą.

przykład

Jak praktycznie badać spełnianie kongruencji $a^{m-1} \equiv 1 \pmod{m}$
– na przykład dla $m = 143$? Wybieramy zwykle małe a
– na przykład 2 i dla $m - 1 = 142$ konstruujemy pierwszą kolumnę tabeli (każdy następny wiersz to podłoga z poprzednika/2)

142	$2^{116} \equiv -29$		
71	$2^{025} \equiv 23$	46	
35	$3^{481} \equiv 49$	$98 \equiv -45$	(mod 143)
17	$900 \equiv 42$	$84 \equiv -59$	
8	$256 \equiv -30$		
4	16		
2	4		
1	2		

Drugą kolumnę wypełniamy od dołu; podnosimy do kwadratu i (ewentualnie) domnażamy przez dwa.

Okazuje się, że 142-ga potęga dwójki nie przylega do 1 modulo 143; wnioskujemy, że 143 nie jest liczbą pierwszą.
Jeszcze przed epoką komputerów, Lehmer i Poulet zbudowali tabele wszystkich *liczb złożonych* m, spełniających $a^{m-1} \equiv 1 \pmod{m}$ dla m sięgających do . . . 100 milionów, podając dla każdej z nich (jakiś) czynnik pierwszy.

Prawdopodobne liczby pierwsze i liczby pseudopierwsze

Definicja

Liczba naturalna $n > 1$ jest *prawdopodobną liczbą pierwszą przy podstawie* b jeżeli

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

Jeżeli liczba taka jest złożona, to nazywamy ją *liczbą pseudopierwszą przy podstawie* b. Czasem używa się określeń: prawdopodobne (pseudopierwsze) liczby Fermata, przy podstawie b.

Tak więc liczba $n = 341$ jest liczbą pseudopierwszą przy podstawie 2; podobnie liczba $n = 91$ jest liczbą pseudopierwszą przy podstawie 3.
Co ciekawe, istnieją liczby n, tzw. *liczby Carmichaela*, które spełniają kogruencję $b^{n-1} \equiv 1 \pmod{n}$ przy *dowolnej* podstawie b, $b \perp n$.
Taką liczbą jest liczba $n = 561 = 3 \cdot 11 \cdot 17$. Wynika to z małego twierdzenia Fermata i chińskiego twierdzenia o resztach:

$b^2 \equiv 1 \pmod{3} \Rightarrow b^{560} = (b^2)^{280} \equiv 1 \pmod{3}$,
$b^{10} \equiv 1 \pmod{11} \Rightarrow b^{560} = (b^{10})^{56} \equiv 1 \pmod{11}$,
$b^{16} \equiv 1 \pmod{17} \Rightarrow b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}$.
a więc $b^{560} \equiv 1 \pmod{(3 \cdot 11 \cdot 17)}$ dla wszystkich $b \perp 561 = 3 \cdot 11 \cdot 17$.

Liczby Carmichaela

Twierdzenie

Spełnienie kongruencji $b^{n-1} \equiv 1 \pmod{n}$ dla *dowolnej* podstawy $b, b \perp n$ będzie możliwe, wtedy i tylko wtedy, gdy $\lambda(n) \mid n-1$, albo

$$n \equiv 1 \pmod{\lambda(n)}.$$

I rzeczywiście: dla liczby Carmichaela 561 mamy

$$\lambda(561) = [\phi(3), \phi(11), \phi(17)] = [2, 10, 16] = 80; \quad 561 \equiv 1 \pmod{80}.$$

Kolejne twierdzenie ...

Liczba Carmichaela musi być liczbą nieparzystą i musi mieć przynajmniej trzy czynniki pierwsze:

$$n = \prod_{k=1}^{K} p_k, \quad K \geqslant 3,$$

gdzie wszystkie nieparzyste p_k, $k = 1, \ldots, K$ spełniają warunek $\lambda(p_k) \mid (n-1)$, czyli $p_k - 1 \mid (n-1)$ dla każdego $1 \leqslant k \leqslant K$.

Dowód: Z kongruencji $n \equiv 1 \pmod{()\lambda(n)}$ wynika, że $(n, \lambda(n)) = 1$.
Funkcja Carmichaela, jest, dla $n > 2$ zawsze parzysta,
a więc n musi być nieparzyste.
Funkcja Carmichaela $\lambda(n)$ jest też zawsze podzielna przez $\phi(p^\alpha)$,
gdzie p^α jest czynnikiem n. Ale $\phi(p^\alpha) = p^{\alpha-1}(p-1)$, czyli dla $\alpha > 1$
istniałby wspólny dzielnik n i $\lambda(n)$ – liczba p.
Nie mogą więc w rozkładzie kanonicznym n występować potęgi
czynniki pierwszych wyższe od pierwszej.

Pozostaje wykazać, że $n \neq p_1 p_2$. Wówczas bowiem
$\lambda(n) = [p_1 - 1, p_2 - 1]$
i z kongruencji $n \equiv 1 \pmod{\lambda(n)}$ wynika, że liczba

$$n - 1 = p_1 p_2 - 1 = (p_1 - 1)p_2 + p_2 - 1$$

musi być podzielna przez $p_1 - 1$ – co będzie możliwe (patrz wyżej)
wtedy i tylko wtedy, gdy $p_1 - 1 \mid p_2 - 1$. Analogicznie dowodzimy, że
musi zachodzić $p_2 - 1 \mid p_1 - 1$ – a to oznacza, że $p_1 = p_2$.