21. Małe twierdzenie Fermata i jego zastosowanie w kryptografii.

Małe twierdzenie Fermata (wersja 1): Dla dowolnej liczby pierwszej p i liczby całkowitej a

$$p \mid a^p - a \ .$$

Małe twierdzenie Fermata (wersja 2): Dla dowolnej liczby pierwszej p i liczby całkowitej a względnie pierwszej z p

$$p \mid a^{p-1} - 1 \ .$$

Idea dowodu.

Ponieważ dla $1 \leqslant i \leqslant p-1$ liczba $\binom{p}{i}$ jest podzielna przez p, więc dla dowolnych liczb całkowitych b, c mamy

$$(b+c)^p = b^p + c^p + \sum_{i=1}^{p-1} \binom{p}{i} b^i c^{p-i} \equiv b^p + c^p \pmod{p} \ .$$

Przez indukcję otrzymujemy

$$a^p = \underbrace{(1+1+1+...+1+1)^p}_{a} \equiv \underbrace{1^p+1^p+1^p+...+1^p+1^p}_{a} = a \pmod{p}$$

dla a dodatnich oraz

$$(-a)^p \equiv -a^p \equiv -a \pmod{p}$$

dla a ujemnych.

Uwaga.

Nie każda liczba spełniająca tezę małego twierdzenia Fermata jest pierwsza. Liczby złożone spełniające małe twierdzenie Fermata są zwane liczbami Carmichaela (czyt. karmajkla) i jest ich nieskończenie wiele.

Twierdzenie Eulera (wersja powszechnie używana): Dla dowolnej liczby naturalnej n i liczby całkowitej a względnie pierwszej z n

$$n \mid a^{\varphi(n)} - 1 \ ,$$

gdzie

$$\varphi(p^k) = (p-1)p^{k-1}$$

dla liczby pierwszej p oraz

$$\varphi(st) = \varphi(s)\varphi(t)$$

dla liczb względnie pierwszych s i t.

Twierdzenie Eulera (wersja wzmocniona): Dla dowolnej liczby naturalnej n i liczby całkowitej a względnie pierwszej z n

$$n|a^{\psi(n)}-1 \ ,$$

gdzie

$$\psi(p^k)=(p-1)p^{k-1}$$

dla liczby pierwszej nieparzystej p,

$$\psi(2)=1, \quad \psi(4)=\psi(8)=2, \quad \psi(2^k)=2^{k-2} \qquad \text{dla} \quad k\geqslant 4$$

oraz

$$\psi(st)=\mathrm{NWW}(\psi(s),\psi(t))$$

dla liczb względnie pierwszych s i t.

Twierdzenie Eulera dla potęg liczb pierwszych dowodzimy indukcyjnie. Krok indukcyjny przebiega następująco. Jeśli liczba a jest względnie pierwsza z p oraz

$$a^{(p-1)p^{k-1}}\equiv 1 \pmod{p^k} \ ,$$

to $a^{(p-1)p^{k-1}}$ jest postaci cp^k+1, skąd

$$a^{(p-1)p^k}=(cp^k+1)^p\equiv 1+cp^k\binom{p}{1}+c^2p^{2k}\binom{p}{2}+$$
$$+\text{inne wyrazy podzielne przez } p^{k+1}\equiv 1 \pmod{p^{k+1}} \ .$$

Wniosek: Dla $n\geqslant 3$ i a względnie pierwszego z n

$$a^{\varphi(n)/2}\equiv \pm 1 \pmod{n} \ .$$

Jeśli n jest potęgą liczby pierwszej nieparzystej lub podwojoną potęgą liczby pierwszej nieparzystej, to

$$a^{\varphi(n)}-1=\left(a^{\varphi(n)/2}+1\right)\left(a^{\varphi(n)/2}-1\right)\equiv 0 \pmod{n} \ ,$$

skąd wynika, że jeden z czynników iloczynu $\left(a^{\varphi(n)/2}+1\right)\left(a^{\varphi(n)/2}-1\right)$ jest podzielny przez n.

Dla $n=4$ teza wniosku jest oczywista.

Gdy n jest potęgą dwójki większą od 4, to

$$a^{\psi(n)}=a^{\varphi(n)/2}\equiv 1 \pmod{n} \ .$$

Gdy n nie jest potęgą liczby pierwszej, ani podwojoną potęgą liczby pierwszej, tezę wniosku otrzymujemy z podzielności $\psi(n)|\frac{\varphi(n)}{2}$; wówczas $a^{\varphi(n)/2}\equiv 1 \pmod{n}$.

Uwaga

$7^4\equiv 1 \pmod{15}$, ale to nie znaczy, że $7^2\equiv \pm 1 \pmod{15}$.

561. Dla podanej liczby n obliczyć $\varphi(n)$ oraz $\psi(n)$

a) $n=24$

b) $n=27$

c) $n=32$

d) $n=63$

e) $n=91$

f) $n=105$

g) $n=2520$

1105. Wskazać największą liczbę naturalną d, która dla dowolnej liczby naturalnej n jest dzielnikiem liczby n^6-n^2.

1729. Wskazać największą liczbę naturalną d, która dla dowolnej liczby naturalnej n jest dzielnikiem liczby $n^{16}-n^4$.

2465. Które liczby naturalne n spełniają podzielność

$$n|a^{\psi(n)+1}-a$$

dla dowolnej liczby całkowitej a?

2821. Czy dla dowolnej liczby całkowitej a zachodzi podzielność

$$n|a^k-a\,,$$

jeżeli

a) $n=7$, $k=13$

b) $n=15$, $k=5$

c) $n=15$, $k=9$

d) $n=21$, $k=7$

e) $n=28$, $k=7$

f) $n=105$, $k=25$

6601. Dla podanej liczby naturalnej n wskazać taką liczbę naturalną $k>1$, aby podzielność

$$n|a^k-a$$

była prawdziwa dla dowolnej liczby całkowitej a.

a) $n=35$

b) $n=55$

c) $n=77$

d) $n=91$

e) $n=899$

f) $n=1155$

8911. Dla podanych liczb naturalnych n oraz s wskazać taką liczbę naturalną d, że dla dowolnej liczby $a\in\{0,1,2,\ldots,n-1\}$ zachodzi

$$b^d\equiv a(\mathrm{mod}\, n)\,,$$

gdzie

$$b\equiv a^s(\mathrm{mod}\, n)\,.$$

a) $n=55$, $s=3$, $d=\ldots$

b) $n=85$, $s=3$, $d=\ldots$

c) $n=91$, $s=5$, $d=\ldots$

d) $n=667=23\cdot 29$, $s=3$, $d=\ldots$

e) $n=667=23\cdot 29$, $s=5$, $d=\ldots$

f) $n=10403$, $s=13$, $d=\ldots\ldots\ldots$ (wymaga co najmniej kalkulatora)

10585. Wskazać taką liczbę naturalną $r<55$, że

$$r^3\equiv 2(\mathrm{mod}\, 55)\,.$$

15841. Wskazać taką liczbę naturalną $r<115$, że

$$r^5\equiv 2(\mathrm{mod}\, 115)\,.$$

29341. Wskazać taką liczbę naturalną $r<133$, że

$$r^{11}\equiv 2(\mathrm{mod}\, 133)\,.$$

41041. Wskazać taką liczbę naturalną $r<133$, że

$$r^{11}\equiv 3(\mathrm{mod}\, 133)\,.$$

46657. Wskazać taką liczbę naturalną $r<5461=43\cdot 127$, że

$$r^{23}\equiv 2(\mathrm{mod}\, 5461)\,.$$

Zajęcia z Matematyki Elementarnej B
są współfinansowane przez Unię Europejską
w ramach Europejskiego Funduszu Społecznego.