Kongruencje II

JOACHIM JELISIEJEW
12 grudnia 2011

ZADANIE (MAŁE TWIERDZENIE FERMATA) 1
Niech p będzie liczbą pierwszą, a a będzie liczbą całkowitą niepodzielną przez p.

1. Udowodnij, że liczby $\{0 \cdot a, 1 \cdot a, \ldots, (p-1) \cdot a\}$ dają różne reszty z dzielenia przez p.
2. Udowodnij *małe twierdzenie Fermata*:
$$a^{p-1} \equiv 1 \mod p.$$
3. Wywnioskuj, że **dla wszystkich** liczb całkowitych a zachodzi $a^p \equiv a \mod p$.

ZADANIE 2
Uzasadnij, że jeśli $NWD(a, 105) = 1$ to $7 \big| a^6 - 1, \quad 3 \big| a^2 - 1, \quad 5 \big| a^4 - 1$.
Pokaż, że jeśli $NWD(a, 105) = 1$ to $105 \big| a^{12} - 1$.

ZADANIE 3
Pokaż, że jeżeli p jest pierwsza, to jedynymi rozwiązaniami równania $x^2 \equiv 1 \mod p$ są $1 \mod p$ i $-1 \mod p$ (*tzn. każda liczba całkowita x spełniająca $x^2 \equiv 1$, przystaje do 1 lub -1 modulo p*).
Pokaż, że bez założenia, że p jest pierwsza, teza zadania nie byłaby prawdziwa.

ZADANIE 4
Udowodnij, że jeśli p jest pierwsza, a a całkowita niepodzielna przez p, to
$$a^{\frac{p-1}{2}} \equiv 1 \mod p \text{ lub } a^{\frac{p-1}{2}} \equiv -1 \mod p.$$
Wywnioskuj, że sześciany liczb całkowitych dają z dzielenia przez 7 reszty ze zbioru $\{0, 1, -1\}$.

ZADANIE 5
Uzasadnij, że równanie $7^n = x^3 + 2y^3$ nie ma rozwiązań w liczbach całkowitych dodatnich x, y, n.

ZADANIE 6
Oblicz, jakie reszty dają kwadraty liczb całkowitych przy dzieleniu przez 3 (użyj zadania 2.) i przez 4. Pokaż, że równania $3^n = x^2 + y^2$ i $4^n = x^2 + y^2$ nie mają rozwiązań w liczbach całkowitych dodatnich x, y, n.