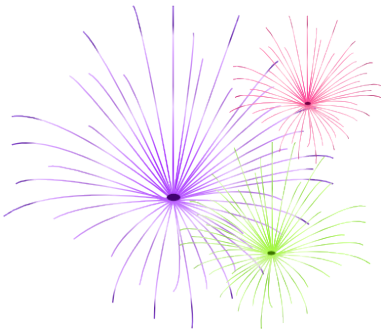

Teoria liczb — powtórka

czyli kolejny fascynujący tytuł.

Joachim Jelisiejew

12 grudnia 2011

1.1 Powtórzenie teorii

Reszty modulo n Cel: chcemy stwierdzić, czy równanie ma rozwiązanie w liczbach całkowitych. Moglibyśmy sprawdzić wszystkie, ale jest ich nieskończenie wiele... Natomiast reszt z dzielenia przez n jest skończenie wiele, więc możemy sprawdzić wszystkie.

Na resztach da się sensownie działać: jeżeli $a \equiv b$ i $c \equiv d$ (wszystko $\mod n$) to

$$a+c \equiv b+d \mod n \quad a-c \equiv b-d \mod n, \quad ac \equiv bd \mod n, \quad a^m \equiv b^m \mod n \text{ dla każdego } m \in \mathbb{Z}_+$$

Z dzieleniem trzeba ostrożnie: mamy $2 \cdot 2 \equiv 4 \cdot 2 \mod 4$, ale $2 \not\equiv 4 \mod 4$. Jednak:

$$\text{jeżeli } NWD(a,n) = 1 \text{ i } ak \equiv al \mod n, \text{ to } k \equiv l \mod n.$$

Udowodniliśmy także

Twierdzenie 1.1 (Małe twierdzenie Fermata)**.** *Jeżeli p jest liczbą pierwszą, a a jest całkowite, to*

$$a^p \equiv a \mod p.$$

Jeżeli $p \not| a$, to $a^{p-1} \equiv 1 \mod p$, innymi słowy $a \cdot a^{p-2} \equiv 1 \mod p$, więc a^{p-2} możemy NIEFORMALNIE (na razie) traktować jako "$a^{-1} \mod p$". Kiedyś może pokażemy, że to ma sens, a jeśli nie, to na studiach.

1.2 Zadania

Zadanie 1

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*).

Podaj przykład, że bez założenia, że p jest pierwsza, teza zadania nie byłaby prawdziwa.

Zadanie 2

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 $\{0, 1, -1\}$. Co można powiedzieć o 5 potęgach, 6 potęgach itd.?

Zadanie 3

Udowodnij, że równanie $x^3 - y^3 = 2012$ nie ma rozwiązań w liczbach całkowitych x, y.

Wskazówka: skorzystać z wyniku poprzedniego zadania.

Zadanie 4

Udowodnij, że równanie $x^5 - y^5 = 2010$ nie ma rozwiązań w liczbach całkowitych x, y.

Wskazówka: skorzystać z wyniku poprzedniego poprzedniego zadania.

Zadanie 5

Niech $p > 3$ będzie liczbą pierwszą, udowodnić, że

$$p \big| 6^{p-2} + 3^{p-2} + 2^{p-2} - 1.$$

(bardzo nieformalnie znaczy to: $1/6 + 1/2 + 1/3 - 1 = 0$.) trzeba skorzystać z twierdzenia Fermata, więc trzeba wymnożyć przez coś...