Dlaczego reszty $\mod p$ są fajne? Krótkie przypomnienie teorii liczb

KÓŁKO I LO BIAŁYSTOK

6 LUTEGO 2012

1.1 Ogólnorozwojowa teoria

Oznaczmy przez $\mathbb{Z}_n$ zbiór reszt $\mod n$, który można uznawać za $\{0, 1, 2, \ldots, n-1\}$.

Porównanie $\mathbb{Q}$ i $\mathbb{Z}_p$, gdzie jest p pierwsza. Poniżej $x, y \in \mathbb{Q}, a, b \in \mathbb{Z}$.

$\mathbb{Q}$	$\mathbb{Z}_p$
jeżeli $x \cdot y = 0$, to $x = 0$ lub $y = 0$	jeżeli $a \cdot b \equiv 0 \mod p$ to $a \equiv 0 \mod p$ lub $b \equiv 0 \mod p$
jeżeli $x \neq 0$, to istnieje $x^{-1} \in \mathbb{Q}$ takie, że $x \cdot x^{-1} = 1$	jeżeli $a \not\equiv 0 \mod p$, to istnieje $b \in \mathbb{Z}$ takie, że $a \cdot b \equiv 1 \mod p$. Możemy to b oznaczać "$a^{-1} \mod p$"
$x^{-1}+y^{-1} = (x+y)\cdot(xy)^{-1}$ i ogólnie wszystkie działania zachowują się tak, jak wiemy	$a^{-1} + b^{-1} \equiv (a+b) \cdot (ab)^{-1} \mod p$ i ogólnie wszystko jest dobrze, tylko trzeba pamiętać, że nie istnieje nic takiego jak $p^{-1} \mod p$ albo $(2p)^{-1} \mod p$.

Dlaczego ten punkt widzenia opłaca się?

Przykład 1.1. *Udowodnij, że jeżeli p jest pierwsza, a $a \in \mathbb{Z}$ niepodzielna przez p, to $\{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$ dają różne reszty z dzielenia przez p.*

Rozwiązanie.

Wiemy, że $a \not\equiv 0 \mod p$.

Rozważamy liczby $\{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$. Chcemy pokazać, że one dają różne reszty $\mod p$. Więc mnożymy je wszystkie przez $a^{-1} \mod p$. Otrzymujemy liczby $\{0, 1, 2, \ldots, p-1\}$ które dają różne reszty. A więc i oryginalne liczby dawały różne reszty.

To jest TYLKO intuicyjne porównanie!!

Wiemy, że $a \neq 0$.

Rozważamy liczby $\{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$. Chcemy pokazać, że są one parami różne. Więc mnożymy je wszystkie przez a^{-1}. Otrzymujemy liczby $\{0, 1, 2, \ldots, p-1\}$ które są różne. A więc i oryginalne liczby były różne.

ZADANIE 1

Jeżeli $p > 3$ jest liczbą pierwszą to $p \big| 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

DLACZEGO jest potrzebne założenie $p > 3$?

ZADANIE 2

Jeżeli $p > 5$ jest pierwsze, to $p \big| 2^{p-2} + 5^{p-2} - 7 \cdot 10^{p-2}$.

ZADANIE 3

Uzasadnij, że jeśli $p > 2$ jest pierwsze, to $p \big| 2^{p-2} + (p-2)^{p-2}$.

Uzasadnij, że jeśli $p > 40$ jest pierwsze, to $p \big| 2^{p-40} + (p-2)^{p-40}$.

1.2 Praktyka — nieskończone schodzenie lub minimalne rozwiązanie.

ZADANIE 4

Znajdź wszystkie rozwiązania równania $8x^4 + 4y^4 + 2z^4 = t^4$ w liczbach całkowitych nieujemnych.

ZADANIE 5

Znajdź wszystkie rozwiązania równania $x^2 + y^2 + z^2 + u^2 = 2xyzu$ w liczbach $\mathbb{N}_+$.

Zadanie 6
Udowodnij, że 7 nie da się przedstawić w postaci sumy trzech kwadratów liczb wymiernych dodatnich.

Zadanie 7
Udowodnij, że liczba postaci $4^n(8k-1)$, gdzie $k, n \in \mathbb{N}_+$ nie może być przedstawiona jako suma 1, 2 lub 3 kwadratów liczb naturalnych dodatnich.

Zadanie 8
Udowodnić, że dla dowolnych dodatnich liczb całkowitych $x_1, \cdots, x_{2011}, y_1, \cdots, y_{2011}$ iloczyn

$$(2x_1^2 + 3y_1^2) \cdot (2x_2^2 + 3y_2^2) \cdot \cdots \cdot (2x_{2011}^2 + 3y_{2011}^2)$$

nie jest kwadratem liczby całkowitej.

Zadanie 9
Ciąg $a_1, ..., a_n$ $(a_i \in \mathbb{N}_+)$ zamieniamy na ciąg postaci

$$\frac{a_1 + a_2}{2}, \frac{a_2 + a_3}{2}, \cdots, \frac{a_{n-1} + a_n}{2}, \frac{a_n + a_1}{2},$$

ten ciąg zmieniamy analogicznie itd. Udowodnij, że po pewnej liczbie takich operacji albo otrzymany ciąg będzie stały, albo będzie on zawierać wyrazy niecałkowite.