Matematyka UJ

Stanisław Chmiela

4 marca 2012

1 Wprowadzenie do tematu odwrotności

Definicja Mamy liczbę $n \in \mathbb{N}$ oraz a takie, że $(a, n) = 1$. Powiemy, że b jest odwrotnością $a \pmod{n}$, jeśli $a \cdot b \equiv 1 \pmod{n}$.

Dowód Bierzemy reszty modulo n takie, że $(x_i, n) = 1$ dla $i = 1, \ldots, n$:

$$x_1, x_2, x_3, \ldots x_k$$

Przemnażamy je przez a:

$$ax_1, ax_2, ax_3, \ldots ax_k$$

Wiemy, że te reszty są cały czas parami różne. Aby to udowodnić, zauważmy, że:

$$ax_i \equiv ax_j \Rightarrow n \mid a\,(x_i - x_j) \Rightarrow n \mid x_i - x_j \Rightarrow i = j$$

Wniosek $a \cdot x_k \equiv 1 \pmod{n}$ dla pewnego k.

$$\frac{x}{a} \equiv x \cdot \frac{1}{a} \pmod{n}$$

Powinno być tak, że $\frac{a}{b} + \frac{c}{d} \equiv \frac{ad+bc}{bd}$. Można to udowodnić, ale nie będziemy tego robić. Musimy natomiast wiedzieć, że to działa.

Policzmy $\frac{2}{3} \pmod{5}$. Wiemy, że $x \cdot 3 \equiv 2 \pmod{5}$, więc $x \equiv 4 \pmod{5}$.

2 Rozwiązywanie zadań

2.1 Zadanie 1

Treść Wyznaczyć $\frac{15}{2} \pmod{7}$, $\frac{3}{4} \pmod{9}$, $\frac{2}{11} \pmod{16}$.

Rozwiązanie

Podpunkt $\frac{15}{2}$

$$x \cdot 2 \equiv 1 \pmod{7}$$

$$x \equiv 4 \pmod{7}$$

Podpunkt $\frac{3}{4}$

$$x \cdot 4 \equiv 3 \pmod 9$$

$$x \equiv 3 \pmod 9$$

Podpunkt $\frac{2}{11}$

$$x \cdot 11 \equiv 2 \pmod{16}$$

$$x \cdot 11 \equiv 66 \pmod{16}$$

$$x \equiv 6 \pmod{16}$$

Algorytm na liczenie reszt

Liczymy modulo p. Jeżeli $x \not\equiv 0$, to $x^{p-1} \equiv 1 \pmod p$. Wiemy wtedy, że $x^{p-2} \cdot x \equiv 1 \pmod p$.

Dowód tw. Wilsona

Treść Jeżeli p jest pierwsze, $(p-1)! \equiv -1 \pmod p$.

Rozwiązanie

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$$

Paruję x z $\frac{1}{x}$.

$$x \equiv \frac{1}{x} \pmod p \Rightarrow x^2 \equiv 1 \pmod p \Rightarrow p \mid (x-1)(x+1) \Rightarrow x \equiv \pm 1 \pmod p$$

2.2 Zadanie

Wyznacz wszystkie n, dla których istnieje $\{a_1, a_2, \ldots, a_n\}$ oraz $\{b_1, b_2, \ldots, b_n\}$ – permutacje reszt. Mamy też permutację reszt $a_1 + b_1, \ldots, a_n + b_n$. Z jednej strony wiemy, że to jest permutacja reszt.

$$(a_1 + b_1) + (a_2 + b_2) + \cdots + (a_n + b_n) \equiv 1 + 2 + \cdots + n - 1 \equiv \frac{n(n-1)}{2}$$

$$2(1 + 2 + \cdots + n - 1) \equiv \frac{n(n-1)}{n} \equiv 0$$

$$2 \not| n$$

2.3 Zadanie 2

Treść Liczby całkowite a i b są względnie pierwsze. Dowieść, że istnieje liczba naturalna n taka, że $ab \mid a^n + b^n - 1$.

Rozwiązanie

$$a^n + b^n \equiv (a+b)^n \equiv 1 \pmod{ab}$$

$$n = \varphi(ab)$$