Ciało $\mathbb{Z}_p$ - skrypt

DEF. Ciało - trójka $(A, +, \cdot)$ w którym dwa działania wykonywane są na elementach ze zbioru A, posiadają elementy neutralne, każdy element ma element odwrotny dodawania i każdy oprócz elementu neutralnego dodawania ma element odwrotny mnożenia. W ciele $\mathbb{Z}_p$ ponadto $A = \{0, 1, \ldots, p-1\}$ i dodawanie i mnożenie odbywa się modulo p, więc na przykład jest przemienne.

WŁ1. Dla każdego $t \in A$ oraz $k \in A$, gdzie $k \neq 0$ istnieje takie $s \in A$, że $s \cdot t = k$. (w szczególnym przypadku dla $k = 1$ jest to istnienie odwrotności)

DEF. Resztą kwadratową modulo p nazywamy takie $a \in A$, że istnieje $t \in A$, że $t^2 = a$.

1. Pokazać, że reszt kwadratowych jest $\frac{p+1}{2}$.

2. Pokazać, że $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1(modp)$

WŁ2. Wielomiany w ciele $\mathbb{Z}_p$ działają tak samo jak w liczbach rzeczywistych - jeśli wielomian dla pewnego k daje zero, to mogę go podzielić przez $(x-k)$. (tw. Bezout)

1. Jeśli mamy wielomian kwadratowy $W(x)$ o współczynnikach całkowitych i $p > 3$ pierwsze oraz $p|W(0), W(1), W(2)$, to $W(x)$ jest tożsamośiowo podzielny przez p.

WŁ3. Zachodzi małe tw. Fermata - $a^{p-1} \equiv 1(modp)$.

1. Ile może być wówczas $a^{\frac{p-1}{2}}$?

2. Pokazać, że jeśli $\sigma(a)$ - najmniejsza liczba dodatnia, że $a^{\sigma(a)} \equiv 1(modp)$, to $\sigma(a)|p-1$. ($\sigma(a)$ - rząd a modulo p)

DEF. $(\frac{a}{p})$ - symbol Legendre'a, daje 1, gdy jest resztą kwadratową i (-1) gdy nie jest.

1. Pokazać, że $(\frac{a}{p}) = a^{\frac{p-1}{2}}$.

2. Pokazać, że $\sum_{i=1}^{p-1}(\frac{i}{p}) = 0$.

WŁ4. Własności symbolu Legendre'a:

- $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$
- a, b - pierwsze: $(\frac{a}{b})(\frac{b}{a}) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$ (prawo wzajemności)
- $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$

1. Pokazać, że jeśli liczba pierwsza p jest postaci $3k+2$, to wszystkie reszty sześcienne są różne.

WŁ5. Twierdzenie o generatorze - istnieje takie $g \in A$, że dla niego $\sigma(g) = p-1$, czyli przemnażając g przez siebie uzyskujemy wszystkie rórne liczby aż po $p-1$ krokach uzyskamy 1. Zatem A mogę przedstawić jako $\{0\} \cup \{g^0, g^1, \ldots, g^{p-2}\}$.

0. Pokazać, że generator nie jest resztą kwadratową.

1. Pokazać, że dla dowolnego $1 \leqslant k \leqslant p-2$ zachodzi:

$$p|1^k + 2^k + \ldots + (p-1)^k$$

.

2. Pokazać, że $1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv -1(modp)$

ZADANIA NA KONIEC

1. Pokazać, że dla każdego n postaci $4m^2 - 5$ istnieją takie $a, b \in \mathbb{Z}^+$, że ciąg f_i określony następująco $f_0 = a, f_1 = b, f_{i+2} = f_{i+1} + f_i$, nie ma wyrazów podzielnych przez n.

2. Niech $q|\frac{p^p-1}{p-1}$, gdzie p, q są liczbami pierwszymi nieparzystymi. Pokazać, że $p|q-1$.

3. k-tą liczbą Fermata nazywamy liczbę postaci $F_k = 2^{2^k} + 1$. Pokazać, że jeśli dla $n > 0$ zachodzi $F_n|3^{\frac{F_n-1}{2}} + 1$, to F_n jest pierwsze.