CYKLICZNOŚĆ $\mathbb{Z}_p^*$
I Uniwersytecki Obóz Olimpiady Matematycznej

Michał Szachniewicz

grudzień 2016, Bardo

Def.: Zbiór $\{1, 2, \ldots, p-1\}$ będziemy nazywać $\mathbb{Z}_p^*$.

1. Pokaż, że dla dowolnego $x \in \mathbb{Z}_p^*$ istnieje taka potęga d, że $p|x^d - 1$.
2. Pokaż, że jeśli d jest najmniejszą potęgą, że dla liczby pierwszej p i liczby naturalnej x zachodzi $p|x^d - 1$, to $d|p-1$ (taką liczbę d nazywamy rzędem x). By to zrobić wykonaj napierw dwa kroki:
   (a) wykaż małe twierdzenie Fermata: dla liczby pierwszej p oraz x, że $(x, p) = 1$, zachodzi $p|x^{p-1} - 1$;
   (b) pokaż, że $(x^a - 1, x^b - 1) = x^{(a,b)} - 1$.
3. Pokaż, że dla dowolnego x, rzędu d, elementy zbioru $\{1, x, x^2, \ldots, x^{d-1}\}$ są różne i każdy spełnia równanie $y^d \equiv 1 \pmod{p}$.
4. Pokaż, że w świecie $\mathbb{Z}_p^*$ każdy wielomian stopnia d ma co najwyżej d rozwiązań. Możesz zacząć od pokazania, że jeśli w tym świecie λ jest pierwiastkiem wielomianu W, to $W(x) = (x-\lambda)\cdot Q(x)$ dla pewnego wielomianu Q.
5. Z poprzednich zadań wywnioskuj, że jesli $x \in \mathbb{Z}_p^*$ jest elementem rzędu d, to zbiór wszystkich elementów tego rzędu zawiera się w zbiorze $\{1, x, x^2, \ldots, x^{d-1}\}$.

Def.: Niech φ będzie funkcją zdefiniowaną w następujący sposób:

$$\varphi(n) = |\{1 \leq k \leq n \mid (k, n) = 1\}|$$

Jest to tak zwana funkcja Eulera.

6. Wykaż, że w zbiorze wspomnianym w zadaniu 5. istnieje dokładnie $\varphi(d)$ elementów rzędu d. Wywnioskuj z tego, że jeśli zbiór $\mathcal{R}(d) = \{k \in \mathbb{Z}_p^* \mid \text{rząd } k \text{ to } d\}$ jest niepusty, to ma dokładnie $\varphi(d)$ elementów.
7. Pokaż, że dla każdego n naturalnego zachodzi:

$$n = \sum_{d|n} \varphi(d)$$

Wskazówka: możesz rozważyć relację $x \sim y$ zachodzącą gdy $(x, n) = (y, n)$, na zbiorze $\{1, 2, \ldots, n\}$.

8. Zauważ, że:

$$\mathbb{Z}_p^* = \bigcup_{d|p-1} \mathcal{R}(d)$$

Czy zbiory $\mathcal{R}(d)$ sa rozłączne?

9. Pokaż, że gdyby dla pewnego dzielnika $d|p-1$, zbiór $\mathcal{R}(d)$ byłby pusty, to $\mathbb{Z}_p^*$ miałby mniej niż $p-1$ elementów, co prowadzi do sprzeczności. Wywnioskuj z tego, że jeśli $d|p-1$, to $|\mathcal{R}(d)| = \varphi(d)$.
10. Pokaż, że istnieje w $\mathbb{Z}_p^*$ element g rzędu $p-1$, taki, że $\{1, g, g^2, \ldots, g^{p-2}\} = \mathbb{Z}_p^*$.
11. Niech p będzie liczbą pierwszą. Pokaż, że:

$$1^k + 2^k + \ldots + (p-1)^k = \begin{cases} 0 \pmod{p} & \text{gdy } p-1 \nmid k, \\ -1 \pmod{p} & \text{gdy } p-1 \mid k. \end{cases}$$

12. Pokaż, że jeśli $p = 4k+1$ jest liczbą pierwszą, to istnieje liczba a, taka, że $p|a^2 + 1$.
13. Pokaż, że dla liczb pierwszych postaci $4k+3$ powyższe twierdzenie nie zachodzi.