Arytmetyka modularna

Kajetan Ramsza

Grudzień 2023

1 Teoria

Uwaga. W całym skrypcie liczba p oznacza liczbę pierwszą

1.1 Szybka powtórka kongruencje

- dla $k \in \mathbb{Z}$, $p \perp k$: $a \equiv_p b \Leftrightarrow ak \equiv_p bk$
- przechodność: $a \equiv b \cap b \equiv c \Rightarrow a \equiv c$
- $a \equiv b \Rightarrow a^n \equiv b^n$
- $a^{p-1} \equiv_p 1$ dla $a \in \mathbb{Z}_+$, $a \perp p$ (małe tw. Fermata)
- $a^{\phi(m)} \equiv_m 1$ dla $a \in \mathbb{Z}_+$, $a \perp m$ (tw. Eulera)

1.2 Twierdzenie Wilsona

$$(p-1)! \equiv_p -1$$

1.3 Ciało $\mathbb{F}_p$

Uwaga, nie trzeba się bać to tylko oznaczenie żebyście wiedzieli jak coś nazwać i wiedzieli o co chodzi jak ktoś tego użyje

Jak mówimy, że pracujemy nad ciałem $\mathbb{F}_p$ oznacza to po prostu:

- wszystkie nasze liczby sprowadzamy do liczb ze zbioru $\{0, 1, 2, \ldots, p-1\}$ (reszta z dzielenia)
- wszystkie działania (mnożenie, dodawanie i odejmowanie) mają domyślnie reszte z dzielenia po wykonaniu działania
- Różni się jedynie dzielenie — jest to mnożenie przez odwrotność liczby

1.4 Własności

Poniższe funkcje f nad ciałem $\mathbb{F}_p$ są permutacjami:

- $f(x) = x + k$ dla dowolnego $k \in \mathbb{Z}$
- $f(x) = x \cdot k$ dla dowolnego $k \in \mathbb{Z}, k \perp p$ (w szczególności $f(x) = -x$)
- Czyli po prostu: $f(x) = a \cdot x + b$ dla $a, b \in \mathbb{Z}$, $a \perp p$
- $f(x) = \begin{cases} \frac{1}{x} & x \neq 0 \\ 0 & x = 0 \end{cases}$

1.5 Generatory

Zwane inaczej pierwiastkami pierwotnymi

Liczbę g nazywamy **pierwiastkiem pierwotnym modulo** m jeśli zachodzi równość zbiorów $\pmod m$

$$\{g, g^1, g^2, \ldots, g^{\phi(m)-1}, g^{\phi(m)}\} = \{x \mid 1 \le x \le m-1, x \perp m\}$$

Zatem dla liczb pierwszych g jest pierwiastkiem pierwotnym modulo p jeśli zbiory są równe nad ciałem $\mathbb{F}_p$:

$$\{g, g^1, g^2, \ldots, g^{p-2}, g^{p-1}\} = \{1, 2, 3, \ldots, p-1\}$$

Dla każdej liczby pierwszej istnieje $\phi(p-1)$ pierwiastków pierwotnych, w szczególności, co najważeniejsze, zawsze istnieje conajmniej jeden.

1.5.1 Własności

Niech a będzie dowolną liczbą ze zbioru $\{1, 2, 3, \ldots, p-1\}$, a g generatorem modulo p

- $g^k \equiv g^{l(p-1)+k}$, dla każdego $k, l \in \mathbb{Z}$
- Istnieje takie $k \in \{1, 2, \ldots, p-1\}$, że $a \equiv g^k$
- Dla nieparzystych p, $g^{\frac{p-1}{2}} \equiv -1$
- Zatem, jeśli $a \equiv g^k$ to $-a \equiv -g^k \equiv g^k \cdot g^{\frac{p-1}{2}} \equiv g^{k+\frac{p-1}{2}}$

2 Zadania

Na rozgrzewkę

- Udowodnij, że dla dowolnego pierwszego p oraz $k \in \{0, 1, 2, \ldots, p\}$
$$\binom{p-1}{k} \equiv_p (-1)^k$$
- Korzystając z poprzedniego zadania udowodnij, że
$$\frac{(p-1)!}{k!(p-k)!} \equiv_p (-1)^k \cdot \frac{(p-1)!}{k}$$

Uwaga. Gdy mówimy o podzielności ułamków mamy na myśli podzielność licznika skróconego ułamka

1. Udowodnij, że dla dowolnego pierwszego $p > 2$
$$p \mid 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$
2. Udowodnij, że dla dowolnego pierwszego $p > 3$
$$p^2 \mid 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$
3. Udowodnij, że dla dowolnego pierwszego $p > 3$ i $k = \lfloor \frac{2p}{3} \rfloor$
$$p^2 \mid \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}$$
4. Udowodnij, że dla dowolnego pierwszego $p > 2$
$$p^4 \mid \left(1 + p\sum_{k=1}^{p-1} \frac{1}{k}\right)^2 - 1 + p^2 \sum_{k=1}^{p-1} k^{-2}$$
5. Niech p będzie nieparzystą liczbą pierwszą. Udowodnij, że
$$p^2 \mid 2^p - 2 \iff p \mid \frac{(p-1)!}{1 \cdot 2} + \frac{(p-1)!}{3 \cdot 4} + \frac{(p-1)!}{(p-2) \cdot (p-1)}$$