KONGRUENCJE

PASJONACI MATEMATYKI

$$\forall, \exists, \Rightarrow, \Leftrightarrow, \vee, \wedge.$$

1. Definicje i przykłady

Przypomnienie: a daje resztę r przy dzieleniu przez n, jeżeli $a = qn + r$, gdzie $r \in \{0, 1, \ldots, n-1\}$, $q \in \mathbb{Z}$.

Definicja 1.1. Mówimy, że $a \equiv b \pmod{n}$, jeżeli $n|a-b$ (równoważnie jeżeli a oraz b dają tą samą resztę przy dzieleniu przez n).

Fakt 1.2. *Kongruencje o tym samym module można dodawać, odejmować i mnożyć stronami.*

Przykłady:

- jaką resztę daje 2^{101} przy dzieleniu przez 5?

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8 \equiv 3, 2^4 \equiv 1 \pmod{5}.$$

  Zatem $2^{101} = (2^4)^{25} \cdot 2 = 1 \cdot 2 \equiv 2 \pmod{5}$.
- Liczba dzieli się przez 9 wtw. gdy jej suma cyfr dzieli się przez 9:
  Mamy $10 \equiv 1 \pmod{9}$, zatem:

$$n = n_0 + 10n_1 + \ldots + 10^k \cdot n_k \equiv n_0 + 1 \cdot n_1 + 1 \cdot n_2 + \ldots + 1 \cdot n_k \pmod{9}.$$

Fakt 1.3. *Niech $a, n \in \mathbb{Z}$. Wtedy istnieje $b \in \mathbb{Z}$ takie, że $a \cdot b \equiv 1 \pmod{n}$ (odwrotność multyplikatywna) wtw. gdy $a \cdot b \equiv 1 \pmod{n}$.*

Twierdzenie 1.4 (Małe Twierdzenie Fermata)**.** *$p \in \mathbb{P}$, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.*

Wniosek 1.5. *$p \in \mathbb{P}$, $a \in \mathbb{Z} \Rightarrow a^p \equiv a \pmod{p}$.*

Definicja 1.6. $\mathbb{Z}/n := \{0, 1, \ldots, n-1\}$ z działaniami dodawania i mnożenia modulo n.

Fakt 1.7. *Jeżeli $p \in \mathbb{P}$, $a \cdot b \equiv 0 \pmod{p}$, to $a \equiv 0 \pmod{p}$ lub $b \equiv 0 \pmod{p}$.*

Przykład 1.8. $2 \cdot 3 \equiv 0 \pmod{6}$*, ale* $2, 3 \not\equiv 0 \pmod{6}$.

Twierdzenie 1.9. *Dla każdej liczby pierwszej p istnieje $g \in \mathbb{Z}/p$ (generator modulo p) takie, że:*

$$\mathbb{Z}/p = \{0\} \cup \{g^0, g^1, \ldots, g^{p-2}\}.$$

Przykład 1.10. $\mathbb{Z}/5 = \{2^0 \pmod{5}, 2 \pmod{5}, 2^2 \pmod{5}, 2^3 \pmod{5}, 2^4 \pmod{5}\}$

Problem otwarty: czy 2 jest generatorem mod p dla nieskończenie wielu $p \in \mathbb{P}$?

2. Reszty kwadratowe

Niech:

$$\mathbb{F}_p[x] = \text{ wielomiany o współczynnikach z } \mathbb{F}_p = \{a_0 + a_1 x + \ldots + a_n x^n : a_i \in \mathbb{F}_p\}.$$

Uwaga: czy $f(x) := x^p - x = 0$? Z jednej strony, dla każdego $a \in \mathbb{F}_p$ mamy $f(a) = 0$. Z drugiej strony – f ma niezerowe współczynniki! Ale **wielomian** to wyrażenie formalne – z definicji jest równy zero tylko wtedy, gdy wszystkie współczynniki ma zerowe. Nie mylić z funkcją wielomianową!
Okazuje się, że wielomian stopnia n nad $\mathbb{F}_p$ ma maksymalnie n pierwiastków. Przykład:

$$x^p - x \equiv x \cdot (x-1) \cdot \ldots \cdot (x-(p-1)) \pmod{p}.$$

(np. $x^3 - x = x \cdot (x-1) \cdot (x-2) \pmod 3$). Jak i po co rozwiązywać równania wielomianowe modulo p?
Po co: jeżeli chcemy pokazać, że równanie nie ma rozwiązania całkowitego, wystarczy pokazać, że nie ma rozwiązania modulo p!
Równanie liniowe: $ax + b \equiv 0 \pmod p$ wtw. gdy $x \equiv -a^{-1} \cdot b \pmod p$.
Równanie kwadratowe: które elementy $\mathbb{F}_p$ są kwadratami?

Definicja 2.1. a jest resztą kwadratową mod p wtw. gdy $a \equiv b^2 \pmod p$ dla pewnego b.

Przykład 2.2. *Reszty kwadratowe modulo 7:* $\{0, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \equiv \{0, 1, 2, 4\} \pmod 7$.

Fakt 2.3. *Dla $p \in \mathbb{P}$, $p > 2$, istnieje $\frac{p-1}{2}$ niezerowych reszt kwadratowych i $\frac{p-1}{2}$ niereszt kwadratowych.*

Dowód. Reszty kwadratowe:

$$\{1^2, 2^2, \ldots, (p-1)^2\} \equiv \{1^2, 2^2, 3^2, \ldots, (\frac{p-1}{2})^2\} \pmod p.$$

Istotnie: $a^2 \equiv b^2 \pmod p$ wtw gdy $a \equiv \pm b \pmod p$. □

Wniosek 2.4. *Jeżeli g jest generatorem, to niezerowe reszty kwadratowe to $\{g^n : 2|n\}$, zaś niereszty kwadratowe to $\{g^n : 2 \nmid n\}$.*

Dowód. Liczby $\{g^n : n = 0, 2, 4, \ldots, p-1\}$ muszą być wszystkimi resztami kwadratowymi. Zatem pozostałe to niereszty! □

Przykład 2.5. *3 – generator mod 7:* $1, 3^2 \equiv 2, 3^4 \equiv 4$ *– kwadraty.*

Definicja 2.6.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p|a, \\ 1, & p \nmid a, a \text{ jest resztą kwadratową}, \\ -1, & a \text{ jest niereszą kwadratową}. \end{cases}$$

Fakt 2.7.

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Dowód. Zauważmy, że $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$, zatem $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Jeżeli $a \equiv b^2$ jest resztą kwadratową, to $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$. Zatem wielomian $x^{\frac{p-1}{2}} - 1$ ma przynajmniej $\frac{p-1}{2}$ pierwiastków. Więcej mieć nie może! Niereszty kwadratowe muszą zatem spełniać $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Wniosek 2.8.

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{a \cdot b}{p}\right).$$

Jeżeli a, b są nieresztami kwadratowymi mod p, to $a \cdot b$ jest resztą kwadratową.

Dowód.

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{a \cdot b}{p}\right) \pmod{p}.$$

□

Twierdzenie 2.9 (prawo wzajemności reszt kwadratowych)**.** *$p, q \in \mathbb{P}$, $p, q > 2 \Rightarrow$*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

oraz $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Przykład 2.10.

$$\left(\frac{6}{47}\right) = \left(\frac{2}{47}\right) \cdot \left(\frac{3}{47}\right) = (-1)^{\frac{47^2-1}{8}} \cdot (-1)^{\frac{3-1}{2}\frac{47-1}{2}} \left(\frac{47}{3}\right) = 1 \cdot (-1) \cdot \left(\frac{2}{3}\right) = 1.$$