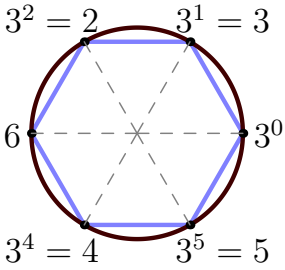
$\{1,2,3,4,5,6\} \mod 7 \Rightarrow$



Generator

1.1 Teoria

Twierdzenie (Istnienie generatora) *Niech p będzie liczbą pierwszą. Istnieje liczba całkowita g, taka, że potęgi g dają wszystkie niezerowe reszty z dzielenia przez p, tzn.*

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

Wniosek *Dla g,p jak wyżej jeżeli $g^n \equiv 1 \mod p$ to $p-1 \mid n$.*

Wniosek *Dla dowolnej liczby pierwszej p nie ma liczby $n < p-1$ takiej, że $x^n \equiv 1 \mod p$ dla każdego x niepodzielnego przez p — "małe twierdzenie Fermata jest optymalne".*

1.2 Zadania bez generatora

1. Zadanie
   Udowodnij, że równanie $3x^2 + 2 = y^2$ nie ma rozwiązań w liczbach całkowitych.

2. Zadanie
   Udowodnij, że równanie $7x^3 + 2 = y^3$ nie ma rozwiązań w liczbach całkowitych.

3. Zadanie
   (twierdzenie Wilsona)

   Niech p będzie liczbą pierwszą większą od 2.

   (a) Pokaż, że jedynymi rozwiązaniami równania $x^2 \equiv 1 \mod p$ są liczby x dające resztę -1 lub 1 z dzielenia przez p.

   (b) Przypomnij sobie, że dla każdej liczby całkowitej $a \in \{1,2,\ldots,p-1\}$ istnieje dokładnie jedna liczba b ze zbioru $\{1,2,\ldots,p-1\}$ taka, że $ab \equiv 1 \mod p$, którą oznaczam a^{-1}. Udowodnij, że przy tak przyjętych oznaczeniach $(a^{-1})^{-1} = a$.

   (c) Wywnioskuj, że jeżeli $x \equiv x^{-1} \mod p$ to $x \equiv 1$ lub $x \equiv -1$.

   (d) Uzasadnij, że
   $$(p-1)! \equiv -1 \cdot 1 = -1 \mod p.$$
   grupując elementy iloczynu po lewej w pary (x, x^{-1}).

   (e) Policz, że (zupełnym przypadkiem) to samo zachodzi dla $p = 2$.

4. Zadanie
   Niech p będzie liczbą pierwszą większą od 2.

   Uzasadnić, że istnieje dokładnie $\frac{p+1}{2}$ reszt kwadratowych $\mod p$ tzn. zbiór $\{0^2, 1^2, \ldots, (p-1)^2\}$ ma dokładnie $\frac{p+1}{2}$ elementów.

5. Zadanie
   Uzasadnij, że jeżeli $p > 2$ jest pierwsze, a n takie, że $NWD(n, p-1) = 1$, to
   $$a^n \equiv b^n \mod p \text{ implikuje } a \equiv b \mod p.$$

   Wskazówka użyj małego twierdzenia Fermata.

6. Zadanie
Uzasadnij (bez użycia teorii generatora!), że jeżeli p jest nieparzystą liczbą pierwszą, a $NWD(n, p-1) = 1$ to

$$p \Big| 1^n + 2^n + \cdots + (p-1)^n.$$

Wskazówka: skorzystaj z poprzedniego zadania, by zobaczyć, że liczby $1^n, 2^n, \ldots, (p-1)^n$ są różne.

Ile wynosi $1^n + 2^n + \cdots + (p-1)^n$ gdy $p - 1 \Big| n$?

1.3 * Zadania na generator

1. Zadanie
Korzystając z tego, że 2 jest generatorem dla liczby 29 znajdź, bez zgadywania, rozwiązania równania $x^7 \equiv 1 \mod 29$.

2. Zadanie
Udowodnij, że dla 8 nie istnieje odpowiednik generatora tzn. taka liczba g, że $\{g \mod 8, g^2 \mod 8, g^3 \mod 8, g^4 \mod 8\} = \{1, 3, 5, 7\}$.

3. Zadanie
Niech p będzie pierwsze, a n będzie liczbą całkowitą niepodzielną przez $p-1$. Udowodnić, że

$$p \Big| 1^n + 2^n + \cdots + (p-1)^n.$$

Ile wynosi $1^n + 2^n + \cdots + (p-1)^n$ jeżeli $p - 1 \Big| n$?

4. Zadanie
Liczba $p > 2$ jest pierwsza.

Wielomian $P(x) = a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$ jest taki, że p nie dzieli $P(a) - P(b)$ o ile a, b są całkowite i $p \nmid a - b$. Wykazać, że $p | a_{p-1}$.

   (a) Wykaż, że $\{P(0) \mod p, P(1) \mod p, \ldots, P(p-1) \mod p\} = \{0, 1, \ldots, p-1\}$.

   (b) Zakonkluduj, że $p \Big| P(0) + \cdots + P(p-1)$.

   (c) Rozpisz współczynniki i policz, że właśnie udowodniłeś, że $p \Big| a_{p-1}$.

5. Zadanie
Niech p będzie liczbą pierwszą większą od 2.

Uzasadnić, że istnieje dokładnie $\frac{p+1}{2}$ reszt kwadratowych $\mod p$ tzn. zbiór $\{0^2, 1^2, \ldots, (p-1)^2\}$ ma dokładnie $\frac{p+1}{2}$ elementów.

6. Zadanie
Niech p będzie liczbą pierwszą. Wtedy a^k może daje dokładnie $\frac{p-1}{NWD(k,p-1)} + 1$ różnych reszt $\mod p$.