Teoria liczb

5 czerwca 2018

1 Twierdzenia

Twierdzenie 1 (Zasada szufladkowa Dirichleta)
Mamy n szufladek i przynajmniej $nk+1$ przedmiotów. Wówczas w którejś szufladce będzie przynajmniej $k+1$ przedmiotów.

Wniosek 1.1 (k=1)
Mamy $n+1$ przedmiotów, które wkładamy do n szufladek. Wówczas w którejś szufladce będą przynajmniej 2 przedmioty.

Wniosek 1.2
Mamy n szufladek i m przedmiotów. Wówczas istnieje szufladka w której jest przynajmniej $\left\lfloor \frac{m-1}{n} \right\rfloor + 1$ przedmiotów.

Twierdzenie 2 (Małe twierdzenie Fermata)

$$p \in \mathbb{P} \wedge NWD(a,p) = 1 \implies a^{p-1} \equiv 1 \pmod{p}$$

Lemat 1

$$\{ka \pmod{p} : k \in \{0,1,\ldots,p-1\}\} = \{0,1,\ldots,p-1\}$$

Dowód 1
Załóżmy nie wprost, że $\exists_{k<l} ka \equiv la \pmod{p}$.
Wówczas $(l-k)a \equiv 0 \pmod{p}$
Ale $(l-k) \in \{1,2,\ldots,p-1\} \implies (l-k) \nmid p$.
Sprzeczność.

Lemat 2

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Dowód 2

$$L = \prod_{k=1}^{p-1} ka = a \times 2a \times \cdots \times (p-1)a = a^{p-1}(p-1)!$$

$$R = \prod_{k=1}^{p-1} k = (p-1)!$$

Wystarczy pokazać, że $\forall_i a_i \equiv b_i \pmod n \implies \prod_i a_i \equiv \prod_i b_i \pmod n$*.*

Zauważmy, że $\forall_i a_i \equiv c_i \pmod n$*, gdzie* $c_i \in \{0, 1, \dots, n-1\}$*.*
Stąd $\forall_i \exists_p a_i = pn + c_i$ *Oznaczmy te* p *przez* p_i*.*
Wówczas $L = \prod_i (p_i n + c_i) \equiv \prod_i c_i \pmod n = R$ *. (Po wymnożeniu wszystkie wyrazy, mają zero lub więcej niż jedno* n*. Jedynym wyrazem który nie zawiera* n *jest* $\prod_i c_i$*.)*

Lemat 3

$$\forall_{\substack{a,b,c \in \{1,\dots,p-1\} \\ a<b}} ac \equiv bc \pmod p \implies a \equiv b \pmod p$$

Przy założeniu, że $p \in \mathbb{P}$*.*

Dowód 3
$ac \equiv bc$
$\implies \exists_t (bc - ac) = pt$
$\implies (b-a)c = pt$
(Zachodzi również $c \nmid p \implies c \mid t$*).*
$\implies (b-a) = p\frac{t}{c} \implies a \equiv b \pmod p$

Dowód 4 (Małego twierdzenia Fermata)
Dzielimy obustronnie przez $1, \dots, p-1$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod p \implies a^{p-1} \equiv 1 \pmod p$$

2 Funkcja phi Eulera

$\varphi(n)$ mówi ile jest liczb względnie pierwszych z n w zbiorze $\{1, \dots, n\}$

$$\varphi(n) := \{i \in \{1, \dots, n\} : NWD(i, n) = 1\}$$

$$\varphi(n) = \begin{cases} p^k - p^{k-1} & n = p^k, p \in \mathbb{P} \\ \prod_{i=1}^{m} \varphi(p_i^{k_i}), & n = \prod_{i=1}^{m} p_i^{k_i}, \forall_i p_i n \in \mathbb{P}, k_i > 0 \end{cases}$$

W szczególności:
$p \in \mathbb{P} \implies \varphi(p) = p - 1$
$n = 1 \implies \varphi(n) = 1$
$n = 4 \implies \varphi(n) = 2$

Dowód 5 ($n = p^k$)
Rozpatrzmy $NWD(ip + j, p), i \in \{0, 1, \ldots, p^{k-1} - 1\}, j \in \{1, 2, \ldots, p\}$
$NWD(ip + j, p) = 1 \iff NWD(j, p) = 1 \iff j \in \{1, 2, \ldots, p - 1\}$
Takich liczb jest $|\{0, 1, \ldots, p^{k-1} - 1\} \times \{1, 2, \ldots, p - 1\}| = p^{k-1}(p - 1)$

Lemat 4
$\{a_0 \mod n, a_1 \mod n, \ldots, a_{n-1} \mod n\} = \{0, 1, \ldots, n - 1\}$
$\implies \forall_{c \in \mathbb{N}} \{a_0 + c \mod n, a_1 + c \mod n, \ldots, a_{n-1} + c \mod n\} = \{0, 1, \ldots, n-1\}$
Po prostu przesuwamy liczby cyklicznie o 1 c razy.

Dowód 6 ($NWD(m, n) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$)
Niech $a_{i,j} := im + j, i \in \{0, 1, \ldots, n - 1\}, j \in \{1, 2, \ldots, m\}$
$NWD(a_{i,j}, mn) = 1 \iff NWD(a_{i,j}, n) = 1 \wedge NWD(a_{i,j}, m) = 1$

Rozpatrzmy wartości kolumnami. $NWD(j, m) = 1 \iff \forall_i NWD(a_{i,j}, m) = 1$
(Wszystkie wartości w j-tej kolumnie są względnie pierwsze z m, o ile j jest względnie pierwsze z m).

Niech $S(j)$ *oznacza zbiór wartości w k-tej kolumnie.*
$S(j) := \{a_{i,j} \mod n : i \in \{0, 1, \ldots, n - 1\}$
$S(0) = \{0, m, 2m, \ldots, (n - 1)m\} = \{0, 1, \ldots, n - 1\}$
Z lematu wynika, że $S(j) = \{0, 1, \ldots, n - 1\}$.

W każdej z $\varphi(m)$ *kolumn dokładnie* $\varphi(n)$ *wartości jest względnie pierwszych z n. Stąd* $\varphi(nm) = \varphi(n)\varphi(m)$

Twierdzenie 3 (Twierdzenie Eulera)

$$NWD(a, m) = 1 \implies a^{\varphi(m)} \equiv 1 \pmod m$$

3 Zadania

1. Załóżmy, że maksymalna liczba włosów na głowie wynosi 500.000. Udowodnić, że spośród dowolnej populacji 3.141.592 mieszkańców, da się wybrać 7 (ale nie zawsze 8) osób takich, które mają równą liczbę włosów na głowie.

2. Szybkie potęgowanie http://pl.spoj.com/problems/PA05˙POT/

3. Znaleźć wartość funkcji Eulera http://www.spoj.com/problems/ETF

4. Znaleźć odwrotność modulo $p \in \mathbb{P}$. (Będzie to potrzebne w algorytmie Karpa-Rabina)
   Odwrotność modulo p liczby m to liczba c, taka że $mc \equiv 1 \pmod p$ Zwyczajowo c oznaczamy poprzez m^{-1}.

Uwaga. Poniższe równości nie muszą być prawdziwe, gdy $p \notin \mathbb{P}$.

$$m \equiv a^k \pmod p$$
$$m * m^{-1} \equiv 1 \pmod p$$
$$a^k * m^{-1} \equiv 1 \pmod p$$
$$a^{p-1-k} \equiv a^{p-1-k} * a^k * m^{-1} \equiv a^{p-1} * m^{-1} \equiv m^{-1} \pmod p$$
$$m^{-1} \equiv a^{p-1-k} \pmod p$$

4 Źródła

1. https://forthright48.blogspot.com/2015/09/euler-totient-or-phi-function.html

2. https://en.wikipedia.org/wiki/Pigeonhole˙principle