Zadania przygotowawcze z Teorii Liczb

Troche nizej znajduja sie wskazowki i rozwiazania. Wskazowki i rozwiazania do kazdego z trzech zadan umiescilem na oddzielnych stronach, zeby mozna bylo je robic bez stresu, ze czlowiek zobaczy przypadkiem inne rozwiazanie.

1. Udowodnij twierdzenie Wilsona mowiace, ze liczba naturalna n jest pierwsza wtedy i tylko wtedy, gdy $(n-1)! \equiv -1 \mod n$.

2. Udowodnij, ze iloczyn trzech kolejnych liczb naturalnych, z ktorych srodkowa jest szescianem liczby naturalnej jest podzielna przez 504.

3. Niech $n_1, \ldots, n_k$ parami wzglednie pierwsze oraz $a_1, \ldots, a_k$ takie, ze $0 \leq a_i < n_i$.
Chinskie Twierdzenie o resztach mowi, ze istnieje taka liczba a, ze $0 \leq a < \prod_{i=1}^{k} n_i$ oraz dla kazdego i zachodzi $a \equiv a_i \mod n_i$.
Wskaz konkretne a spelniajace te warunki.

Rozwiazanie 1

- najpierw udowodnij implikacje w prawo, jest prostsza
- zrob to nie wprost, zaloz, ze liczba n jest zlozona i pokaz, ze wowczas $(n-1)!$ nie przystaje do -1 modulo n
- jesli n jest zlozone, to daje sie przedstawic w postaci $n = p \cdot q$, gdzie $1 < p, q < n$
- jesli $p \neq q$, to po prostu w $(n-1)! = (n-1)(n-2)\ldots 2 \cdot 1$ wystepuja te wyrazy, czyli $n = p \cdot q | (n-1)!$
- zobaczmy teraz kiedy n jest zlozone, ale nie da sie go przedstawic w postaci $n = p \cdot q$, gdzie $p \neq q$. Musi byc wowczas $p = q$, czyli $n = p^2$. Jesli teraz $p \geq 3$, to w $(n-1)! = (p^2-1)!$ wystepuja wyrazy p oraz $2p$, czyli $n = p^2 | (n-1)!$. Jesli $p = 2$, to $n = 4$ i mamy $(4-1)! \equiv 2 \mod 4$, czyli $(4-1)! \not\equiv -1 \mod 4$
- czyli sprzecznosc, zadna liczba zlozona nie spelnia tego warunku
- dowodzimy teraz w lewo, niech n liczba pierwsza
- zauwazmy pewien fakt, mianowicie $\forall_{1 \leq a < n} \exists!_{1 \leq b < n} \; a \cdot b \equiv 1 \mod n$, gdzie przez $\exists!$ oznaczamy "istnieje dokladnie jeden", sprobujmy to pokazac
- rozwazmy zbior liczb $a \cdot b$ dla $1 \leq b < n-1$, czyli $a \cdot 1, a \cdot 2, \ldots, a \cdot (n-2), a \cdot (n-1)$. Zauwazmy, ze te liczby nie moga przyjac reszty 0 modulo n, gdyz n jest pierwsza. Liczb tych jest $n-1$, a mozliwych reszt modulo n (bez reszty 0) tez jest $n-1$. Pokazmy, ze kazda z liczby ak ma rozna reszte
- Przypuscmy, ze $ai \equiv aj \mod n$. Wowczas $n | (ai - aj) = a(i-j)$. Wowczas $n | a$ lub $n | (i-j)$. Jednak $a < n$, czyli musi byc $n | (i-j)$. Skoro $1 \leq i, j < n$, to jedyna mozliwosc to $i = j$. Zatem gdy $i \neq j$, to $ai \not\equiv aj \mod n$. Czyli innymi slowy wsrod liczb $a \cdot 1, \ldots, a \cdot (n-1)$ jest tylko dokladnie jedna o reszcie 1
- zatem dla kazdej liczby a istnieje jakas b do pary taka, ze $a \cdot b \equiv 1 \mod n$
- spojrzmy ktore liczby sa w parach z sama soba
- musi byc wowczas $a \cdot a \equiv 1 \mod n$, czyli $n | a^2 - 1 = (a-1)(a+1)$. Czyli $n | a-1$ lub $n | a+1$, czyli jedynie 1 oraz -1 to takie liczby
- zatem $(n-1)! = (n-1)(n-2)\ldots 2 \cdot 1 \equiv 1^{\frac{n-3}{2}} \cdot 1 \cdot (-1) = -1 \mod n$, gdzie druga rownosc wynika z tego, ze liczby tworza $\frac{n-3}{2}$ par, a poza parami pozostaja 1 oraz -1
- w ten sposob dowiedlismy tezy

Rozwiazanie 2

- $504 = 7 \cdot 8 \cdot 9$
- pokazemy oddzielnie dla 7, 8 i 9
- zauwazmy, ze nasza liczba to $(n^3 - 1)n^3(n^3 + 1) = n^3(n^6 - 1)$
- dla 7, jesli $7|n$, to OK, w przeciwnym razie mamy skorzystaj z tw. Eulera
- mamy $n \perp 7$ i z twierdzenia Eulera dostajemy $7|n^{\varphi(7)} - 1 = n^6 - 1$
- dla 8, jesli $2|n^3$, to OK, bo wowczas $2|n$, czyli $8|n^3$, w przeciwnym razie $2|n^3 - 1$, $2|n^3 + 1$ i przynajmniej jedna z nich dzieli 4, czyli OK
- dla 9, jesli $3|n^3$, to $3|n$ i OK, w przeciwnym razie skorzystaj z tw. Eulera
- mamy $n \perp 9$, wiec z twierdzenia Eulera $9|n^{\varphi(9)} - 1 = n^6 - 1$

Rozwiazanie 3

- zauwazmy, ze gdybysmy mieli liczby c_i takie, ze $c_i \equiv 1 \mod n_i$ oraz $c_i \equiv 0 \mod n_j$ dla $i \neq j$, to byloby juz latwo
- moglibysmy wowczas zrobic $a = (a_1 \cdot c_1 + a_2 \cdot c_2 + \ldots + a_k \cdot c_k) \mod n$ i a spelnia warunki zadania
- zatem zadanie sprowadza sie do znalezienia takich c_i
- najpierw znajdzmy liczbe d_i, ktora przystaje do zera modulo n_j, gdzie $j \neq i$ oraz nie do zera modulo n_i
- mozemy polozyc na przyklad $d_i = \frac{\prod_{i=1}^{k} n_i}{n_i}$
- skorzystajmy teraz z Malego Twierdzenia Fermata
- niech $c_i = d_i^{\varphi(n_i)}$, wowczas oczywiscie $c_i \equiv 0 \mod n_i$ oraz takze $c_i \equiv 1 \mod n_i$ (z MTF, gdyz $d_i \perp n_i$), to jest koniec zadania
- mozna tez znalezc inaczej liczby c_i, na przyklad powiedziec: oznaczmy $n = \prod_{i=1}^{k} n_i$, $n_i \perp \frac{n}{n_i}$, wiec niech $b_i = (\frac{n}{n_i})^{-1} \mod n_i$ oraz $c_i = d_i \cdot \frac{n}{n_i} \mod n$. Pozostaje sprawdzic, ze rzeczywiscie c_i jest OK.