Lista 4

Łukasz Magnuszewski

Zadanie 1

Z zadania 6 wiemy że $mn = gcd(m,n) * lcm(m,n)$ Przenosząc gcd na drugą stronę otrzymujemy wzór $\frac{mn}{gcd(m,n)} = lcm(m,n)$. Jedynym problemem jest to że wartość iloczyn m oraz n może przekroczyć zakres liczb całkowitych, pomimo tego że $lcm(m,n)$ leży w tym zakresie. Dlatego najpierw należy wykonać dzielenie a dopiero potem mnożenie: $\frac{m}{gcd(m,n)} * n$. Zakładając że pojedyncze operacje arytmetyczne na typie integer wykonywane są w czasie stałym, to złożoność tego algorytmu jest taka sama jak algorytmu gcd czyli $log((max(n,m))$.

Zadanie 4

Poniżej jest pseudokod algorytmu korzystającego z danych zależności

```
fun bin_gcd(x,y):
    if x == 0:
        return y
    if x % 2 == 0 && y % 2 == 0:
        return 2 * bin_gcd(x/2, y/2)
    if x % 2 && y % 2:
        return bin_gcd(max(x,y)-min(x,y),min(x,y))
    else:
        if y % 2 == 0:
            swap(x,y)
        return bin_gcd(x/2, y)
```

W momencie gdy obie liczby są parzyste to wiemy że dwójka na pewno będzie czynnikiem gcd, więc możemy pomnożyć przez dwa wynik algorytmu dla obu liczb podzielonych przez dwa. Do czasu gdy przynajmniej jedna będzie nieparzysta, i wtedy można skorzystać z danych zależności.

Złożoność

W przypadku gdy wywołanie funkcji wpadnie do pierwszego przypadku, to następuje koniec algorytmu. Jeśli zaś wpadnie do 2 lub 4 to zostanie wywołana funkcja rekurencyjnie z przynajmniej jednym argumentem zmniejszonym o połowę. Z kolei gdy wpadnie do 3 przypadku, czyli obie liczby są nieparzyste, to

wtedy $max(x, y) - min(x, y)$ będzie parzyste(różnica liczb nieparzystych. Więc wtedy kolejne wywołanie rekurencyjne wpadnie do 4 przypadku.

Czyli co maksymalnie dwa wywołania jeden z argumentów maleje o połowę, Czyli Złożoność tego algorytmu to $O(log(max(x, y)))$.

Zadanie 8

a)

Pokaż jeśli $2^n - 1$ jest liczbą pierwszą to n jest liczbą pierwszą. Załóżmy nie wprost że n jest złożone wtedy $n = ab$, gdzie $a, b > 1$. Użyjmy wzoru skróconego mnożenia na różnicę potęg

$$2^{ab} - 1^b = (2^a - 1) \sum_{i=0}^{b-1} (2^a)^i 1^{b-i-1}$$

jako że $a, b > 1$ to zarówno $2^a - 1$ oraz $\sum_{i=0}^{b-1} (2^a)^i 1^{b-i-1}$ są większe od 1. Czyli $2^n - 1$ ma dzielniki poza 1 i nią samą, czyli nie jest to liczba pierwsza. Sprzeczność!

b)

Pokaż jeśli $a^n - 1$ jest liczbą pierwszą to $a = 2$. Użyjmy wzoru skróconego mnożenia na różnicę potęg

$$a^n - 1 = (a - 1) \sum_{i=0}^{n-1} a^i 1^{n-i-1}$$

Załóżmy nie wprost że $a \neq 2$ Wtedy są 2 przypadki:

Jeśli $a \in 0, 1$ to wtedy całe wyrażenie jest albo zerem albo ujemne, czyli nie jest liczbą pierwszą. Sprzeczność!

Z kolei jeśli $a > 2$ to wtedy $a - 1 \geq 2$ oraz $\sum_{i=0}^{n-1} a^i 1^{n-i-1} \geq 2$ Czyli lewa strona równania ma dwa dzielniki nie będące nią samą oraz 1, czyli nie jest to liczba pierwsza. Sprzeczność!

c)

Pokaż jeśli $2^n + 1$ jest liczbą pierwszą to n jest potęgą dwójki. Załóżmy nie wprost że tak nie jest, wtedy $\exists n = p * q$ gdzie $p > 2, n > q > 0$ oraz p jest pierwsze.

Korzystając z tego że p jest nieparzyste(pierwsze i większe od dwóch) oraz wzorów skróconego mnożenia

$$2^n + 1 = (2^q)^p - (-1)^p = (2^q - (-1)) \sum_{i=0}^{p-1} (2^q)^i 1^{p-i-1}$$

Upraszczając jedynki wychodzi

$$(2^q+1)\sum_{i=0}^{p-1}(2^q)^i 1^{p-i-1}$$

Ale to oznacza że $(2^q+1)|(2^n+1)$, a wiemy także $q<n$ więc $(2^q+1)\neq(2^n+1)$ Czyli 2^n+1 ma dzielnik niebędący nią samą, ani jedynką, czyli nie jest to liczba pierwsza. Sprzeczność!

zadanie 6

a)

Załóżmy nie wprost że implikacja w prawą stronę nie zachodzi Czyli $k=gcd(m,n)$ oraz $\exists i : k_i \neq min(n_i, m_i)$. Bez straty ogólności przyjmijmy $n_i < m_i$. Rozpatrzmy 2 przypadki:

1: $k_i < n_i$

Ale wtedy istnieje lepszy kandydat na $gcd(n,m)$ taki że $b_j = k_j$ dla $j \neq i$ oraz $b_i = n_i$. Jest on dzielnikiem zarówno n jak i m oraz jest większy od k. Czyli k nie jest gcd. Sprzeczność!

2: $k_i > n_i$

Ale wtedy k nie jest dzielnikiem n. Sprzeczność!

Teraz udowodnijmy dowodem nie wprost implikację w drugą stronę. Czyli $\forall i, k_i = min(n_i, m_i)$ oraz $k \neq gcd(n,m) = g$, wtedy $\exists j, k_j \neq g_j$.

Rozpatrzmy 2 przypadki:

1: $k_j < g_j$

Ale wtedy $g_k > n_j, m_j$. Czyli g nie dzieli m, n. Czyli nie jest gcd. Sprzeczność!

2: $k_j > g_j$

Wtedy istnieje lepszy kandydat na gcd taki że $c_i = g_i$ dla $i \neq j$ oraz $c_j = k_j$. Wtedy c dzieli zarówno n jak i m. oraz $c > g$. Czyli g nie jest gcd. Sprzeczność!

b

Załóżmy nie wprost że implikacja w prawą stronę nie zachodzi. Czyli $k = lcm(n,m)$ oraz $\exists i, k_i \neq max(n_i, m_i)$ Bez straty ogólności. $n_i \geq m_i$. Wtedy mamy do rozważenia dwa przypadki:

1: $k_i < n_j$

Ale wtedy n nie jest dzielnikiem k, czyli k nie jest lcm. Sprzeczność!

2: $k_i > n_j$

Ale wtedy możemy stworzyć lepszego kandydata na lcm. $l_j = k_j$ dla $j \neq i$ oraz $l_i = n_i$. Wtedy $l < k$ oraz l jest wielokrotnością n, m. Czyli k nie jest lcm sprzeczność!.

Teraz udowodnijmy dowodem nie wprost implikację w drugą stronę. Wtedy $k \neq l = lcm(n, m)$ oraz $\forall, ik_i = max(n_i, m_i)$ czyli $\exists j, k_j \neq l_j$. Bez straty ogólności $n_j \geq m_j$. Rozpatrzmy dwa przypadki:

1: $l_j > n_j$

Ale wtedy możemy stworzyć lepszego kandydata na lcm takiego że $c_i = l_i$ dla $i \neq j$ oraz $c_j = n_j$ Jest on wielokrotnością n, m oraz jest mniejszy od l czyli $l \neq lcm(n, m)$. Sprzeczność!

1: $l_j < n_j$

Ale wtedy n nie jest dzielnikiem l czyli $l \neq lcm(n, m)$. Sprzeczność!

wnioski

Pokażmy że

$$nm = gcd(n, m)lcm(n, m)$$

Aby udowodnić tą równość wystarczy pokazać że $\forall i, L_i = P_i$, Gdzie L_i, P_i to odpowiednio reprezentacja lewej i prawej strony równania w układzie kolejnych liczb pierwszych.

Ustalmy dowolne i. Wtedy $L_i = n_i m_i$ oraz korzystając z poprzednich podpunktów $P_i = min(n_i, m_i)max(n_i, m_i)$. Bez straty ogólności $n_i \leq m_i$ wtedy $P_i = n_i m_i = L_i$ co było do pokazania.

Zadanie 14

a)

Załóżmy nie wprost że istnieje skończona ilość liczb pierwszych w postaci $3k + 2$. Wtedy tworzą one zbiór $K = \{2, p_1, ...p_r\}$ Wtedy jak weźmiemy $z = 2 + 3\prod_{i=1}^{r} p_i$, z nie jest podzielne przez żadną liczbą pierwszą z K. Bo dodajemy dwa do iloczynu. Wiemy też że $k \equiv 2 mod(3)$ Czyli $z = a * b$ gdzie $b = 3k + 2$ oraz jest pierwsze. Jest tak bo żeby liczba przystawała do 2 mod 3 to musi mieć przynajmniej jeden dzielnik pierwszy w takiej postaci, (dzielniki podzielne przez 3 nie mogą występować, a iloczyn samych czynników przystających do 1 będzie przystawał do 1). Ale b nie należy do Z bo wtedy nie dzieliłoby z. Czyli mamy sprzeczność!

b)

Załóżmy nie wprost że istnieje skończona ilość liczb pierwszych w postaci $4k+3$. Wtedy tworzą one zbiór $K = \{p_1, ...p_r\}$. Wtedy jak weźmiemy $z = 3+4\prod_{i=1}^{r} p_i$. To nie będzie one podzielne przez żadną liczbę z K. Ale z w swoim rozkładzie na czynniki pierwsze musi mieć przynajmniej jedną liczbę o reszcie 3 modulo 4(reszty 2,0 odpadają bo wtedy reszta na pewno nie będzie równa 3, Z kolei iloczyn samych liczb o reszcie 1 będzie miał resztę 1). Więc mamy liczbę pierwszą w postaci $4k+3$ nienależącą do zbioru K bo dzieli ona z czyli mamy Sprzeczność!

Zadanie 12

Jako że 25, 64, 27 są względnie pierwsze. To Układ kongruencji w zadaniu spełnia dokładnie jedna liczba na leżąca do przedziału $v = [1, 27 * 64 * 25]$(Chińskie twierdzenie o resztach). Czyli wystarczy znaleźć dowolne rozwiązanie i dodając wielokrotności $27 * 64 * 25$ sprowadzić je do przedziału v i wtedy będzie ono najmniejsze.

Korzystając z rozszerzonego algorytmu Euklidesa znajdźmy takie $x_1, y_1, x_2, y_2, x_3, y_3$ że $x_1 27 + y_1 25 * 64 = 1$ oraz $x_2 25 + y_2 27 * 64 = 1$ a także $x_3 64 + y_2 27 * 25 = 1$.

Wtedy jak weźmiemy $e_1 = y_1 * 25 * 64$ to wtedy $e_1 \equiv 0 mod(25 * 64) \wedge e_1 \equiv 1 mod(27)$. Analogicznie $e_2 = y_2 * 27 * 64$ to wtedy $e_2 \equiv 0 mod(27 * 64) \wedge e_3 \equiv 1 mod(25)$. Tak samo $e_3 = y_3 * 27 * 25$ to wtedy $e_3 \equiv 0 mod(27 * 25) \wedge e_3 \equiv 1 mod(64)$. Po wykonaniu obliczeń wychodzi $x_1 = -237, x_2 = 553, x_3 = -116, y_1 = 4, y_2 = -8, y_3 = 11, e_1 = 6400, e_2 = -13824, e_3 = 7425$. Teraz $x = 11 * e_1 + 13 * e_2 + 12 * e_3$ Spełnia układ kongruencji(bo współczynniki stojące przy e_1, e_2, e_3 wpływają tylko na pojedyncze równanie), ale niekoniecznie warunki zadania. $x = -20212$ Zaś $v = [1, 43200]$. Więc $s = -20212 + 43200 = 22988 \in v$ jest najmniejszą liczbą naturalną spełniającą układ kongruencji

Zadanie 7

a)

Implikacja w lewą stronę

Wiemy że $x \equiv y mod(m)$ w takim razie $\exists a, x = am + y$. Wymnażając przez z wychodzi $xz = amz + yz \equiv yz mod(mz)$. Ponieważ $amz \equiv 0 mod(mz)$, gdyż jest wielokrotnością modulo.

Implikacja w prawą stronę

Wiemy że $xz \equiv yz mod(mz)$ czyli $\exists a, xz = amz + yz$. Dzieląc obie strony przez z wychodzi $x = am + y \equiv y mod(m)$ Bo am to wielokrotność m.

b)

Implikacja w prawą stronę

Wiemy że $xz \equiv yzmod(m)$ czyli $\exists a, xz = am + yz$ Podzielmy teraz przez $gcd(m, z)$(możemy tak zrobić bo każdy wyraz jest podzielny przez $gcd(m, z)$, jest pomnożone albo przez m albo przez z) wychodzi: $\frac{xz}{gcd(m,z)} = \frac{am}{gcd(m,z)} + \frac{yz}{gcd(m,z)} \equiv \frac{yz}{gcd(m,z)} mod(\frac{m}{gcd(m,z)})$. Jako że $z > 0$ to pomnóżmy obie strony równania przez $\frac{z}{gcd(m,z)}$ wyjdzie wtedy $x \equiv ymod(\frac{m}{gcd(m,z)})$.

Implikacja w lewą stronę

Wiemy że $x \equiv ymod(\frac{m}{gcd(m,z)})$ czyli $\exists a, x = \frac{am}{gcd(m,z)} + y$. Pomnożmy teraz obie strony przez z. Wyjdzie wtedy $xz = \frac{azm}{gcd(m,z)} + yz = m\frac{az}{gcd(m,z)} + yz \equiv yzmod(m)$. Bo $m\frac{az}{gcd(m,z)}$ jest wielokrotnością m, ponieważ $\frac{az}{gcd(m,z)}$ jest całkowite, gdyż dzielimy z przez jego gcd z m. .

c)

Wiemy że $x \equiv ymod(mz)$ czyli $\exists a, x = amz + y \equiv ymod(m)$ gdyż $amz = (az)m \equiv 0mod(m)$.