Patryk Maciąg 331542 Lista 3

Zad. 11.

a) $\gcd(448, 721) = 721x + 448y$, $x, y \in \mathbb{Z}$

721	448
448	$721 - 448 = 273$
273	$448 - 273 = 175$
175	$273 - 175 = 98$
98	$175 - 98 = 77$
77	$98 - 77 = 21$
21	$77 - 3 \cdot 21 = 14$
14	$21 - 14 = 7$
7	$14 - 2 \cdot 7 = 0$

$\gcd(448, 721) = 7$

$\gcd(448, 721) = 7 =$
$= 21 - 14 = 21 - (77 - 3 \cdot 21) =$
$= 4 \cdot 21 - 77 =$
$= 4 \cdot (98 - 77) - 77 =$
$= 4 \cdot 98 - 5 \cdot 77 =$
$= 4 \cdot 98 - 5 \cdot (175 - 98) =$
$= 9 \cdot 98 - 5 \cdot 175 =$
$= 9 \cdot (273 - 175) - 5 \cdot 175 =$
$= 9 \cdot 273 - 14 \cdot 175 =$
$= 9 \cdot 273 - 14(448 - 273) =$
$= 23 \cdot 273 - 14 \cdot 448 =$
$= 23 \cdot (721 - 448) - 14 \cdot 448 =$
$= 23 \cdot 721 - 37 \cdot 448$

$x = 23 \quad y = -37$

b) $x, y \in \mathbb{Z}$, $333x + 1234y = 1$
333^{-1} w $\mathbb{Z}_{1234}$ = ?

1234	333
333	$1234 - 333 = 235$
235	$333 - 235 = 98$
98	$235 - 2 \cdot 98 = 39$
39	$98 - 2 \cdot 39 = 20$
20	$39 - 20 = 19$
19	$20 - 19 = 1$
1	$1 - 1 = 0$

$\gcd(333, 1234) = 1 = 20 - 19 =$
$= 20 - (39 - 20) = 2 \cdot 20 - 39 =$
$= 2 \cdot (98 - 2 \cdot 39) - 39 =$
$= 2 \cdot 98 - 5 \cdot 39 = 2 \cdot 98 - 5 \cdot (235 - 2 \cdot 98) =$
$= 12 \cdot 98 - 5 \cdot 235 =$
$= 12 \cdot (333 - 235) - 5 \cdot 235 =$
$= 12 \cdot 333 - 17 \cdot 235 =$
$= 12 \cdot 333 - 17 \cdot (1234 - 3 \cdot 333) =$
$= 63 \cdot 333 - 17 \cdot 1234$

$x = 63 \quad y = -17$

$333 \cdot x \bmod 1234 = 1$ ↔ $63 \cdot 333 - 17 \cdot 1234 = 1$

$\Rightarrow 333^{-1} \equiv 63 \pmod{1234}$

c) $-69^{-1} \bmod 1313$

$(1313 - 69)x + 1313y = \gcd(1313, 1244)$

1313	1244
1244	$1313 - 1244 = 69$
69	$1244 - 18 \cdot 69 = 2$
2	$69 - 34 \cdot 2 = 1$
1	$1 - 1 = 0$

$\gcd(1313, 1244) = 1 = 69 - 34 \cdot 2 =$
$= 69 - 34 \cdot (1244 - 18 \cdot 69) =$
$= 613 \cdot 69 - 34 \cdot 1244 =$
$= 613 \cdot (1313 - 1244) - 34 \cdot 1244 =$
$= 613 \cdot 1313 - 647 \cdot 1244$

$x = -647 \quad y = 613$

$x = 666 \pmod{1313}$

Zad. 4.

$f(x, k, n)$:

jeśli $k = 0$ zwróć 1

w.p.p. $t \leftarrow f(x, \lfloor \frac{k}{2} \rfloor, n)$

jeśli $k \bmod 2 = 0$: zwróć $t^2 \bmod n$

w.p.p. zwróć $(t^2 \cdot x) \bmod n$

liczba mnożeń:

$T(k) = T(\lfloor \frac{k}{2} \rfloor) + c = T(\lfloor \frac{k}{4} \rfloor) + 2c = T(\lfloor \frac{k}{8} \rfloor) + 3c =$

$\ldots = T(\lfloor \frac{k}{2^t} \rfloor) + c \cdot t = T(\lfloor \frac{k}{2^{\log_2 k}} \rfloor) + c \log_2 k$

$T(1) = 0$

Zad. 10.

Zał. $a, b \in \mathbb{N}$

$x, y \in \mathbb{Z} \setminus \{0\}$

$ax + by = 1$

Teza: $\gcd(a,b) = \gcd(a,y) = \gcd(x,b) = \gcd(x,y)$

D-d nie wprost

Niech $\gcd(a,b) > 1$ (to może być dowolne gcd)

$g = \gcd(a,b)$, $\exists_{a',b' \in \mathbb{Z}}\ a = ga' \wedge b = gb'$

$1 = ax + by = ga'x + gb'y = g(a'x + b'y)$

ale $g > 1 \wedge g \in \mathbb{Z}$

Sprzeczność!

(Największy dzielnik dwóch liczb całkowitych jest równy 1, jeśli obie są równe 1.) ∎

1) gdyby $x, y < 0$

$1 = ax + by \leq 1 \cdot (-1) + 1 \cdot (-1) = -2$

$1 \leq -2$

Sprzeczność!

2) gdyby $x, y > 0$

$1 = ax + by \geq 1 \cdot 1 + 1 \cdot 1 = 2$

$1 \geq 2$

Sprzeczność!

Zad. 12.

Teza: $\gcd(F_{n-1}, F_n) = 1$.

D-d)

Baza dla $n=1$ $\gcd(F_0, F_1) = \gcd(0,1) = 1$ ok.

dla $n=2$ $\gcd(F_1, F_2) = \gcd(1,1) = 1$ ok.

Zał. że $\forall_{n_0<n}\ \gcd(F_{n_0-1}, F_{n_0}) = 1$

Pokazujemy dla $n>2$:

$\gcd(F_{n-1}, F_n) = \gcd(F_{n-2}+F_{n-3}, F_{n-1}+F_{n-2}) =$

$= \gcd(F_{n-2}+F_{n-3}, F_{n-2}) = \gcd(F_{n-3}, F_{n-2}) \overset{zał}{=} 1$ ∎

($\gcd(a,b) = \gcd(a, a-b)$ dowód na wykładzie)

Teza: $\gcd(F_m, F_n) = F_{\gcd(m,n)}$

D-d) indukcja po n

$\gcd(F_m, F_0) = F_m = F_{\gcd(m,0)}$ ok.

Zał. $\forall_{n_0<n}\ \gcd(F_m, F_{n_0}) = F_{\gcd(m,n_0)}$

Pokazujemy dla n (bez straty ogólności zał. $m \leq n$):

(lemat: $F_{n+m} = F_n F_{m+1} + F_{n-1} F_m$ dowód na wykładzie nr 2)

$\gcd(F_m, F_n) = \gcd(F_m, F_m F_{(n-m+1)} + F_{m+1} F_{n-m}) =$

$= \gcd(F_m, F_m F_{n-m} + F_{m+1} F_{n-m}) = \gcd(F_m, F_{n-m}(F_m + F_{m+1})) =$

$= \gcd(F_m, F_{n-m} F_{m+1}) = \gcd(F_m, F_{n-m}(F_{m-1} + F_m)) =$

$= \gcd(F_m, F_{n-m} F_{m-1}) \overset{*}{=} \gcd(F_m, F_{n-m}) \overset{zał}{=} F_{\gcd(m,n-m)} =$

$= F_{\gcd(m,n)}$ ∎

* $b \perp c \Rightarrow \gcd(ab, c) = \gcd(a, c)$

Patrycja Maciąg 331542 Lista 3

Zad. 13.

$a \perp b$, $a > b$, $0 \leq m < n$

Teza: $\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$

D-d indukcja po n

dla $n = 1 \to \gcd(a^m - b^m, a^1 - b^1) = a - b = a^{\gcd(m,1)} - b^{\gcd(m,1)}$ ok.

Zał. $\forall_{n_0 < n} \gcd(a^m - b^m, a^{n_0} - b^{n_0}) = a^{\gcd(m,n_0)} - b^{\gcd(m,n_0)}$

Pokażmy dla n:

$$\gcd(a^m - b^m, a^n - b^n) \overset{zał.}{=} \gcd(a^m - b^m, a^{m+k} - b^{m+k}) =$$

$$= \gcd(a^m - b^m, (a^{m+k} - a^m b^k) + (a^m b^k - b^{m+k})) =$$

$$= \gcd(a^m - b^m, a^m(a^k - b^k) + b^k(a^m - b^m)) =$$

$$= \gcd(a^m - b^m, a^m(a^k - b^k)) \overset{a^m - b^m \perp a^m}{\overset{*}{=}} \gcd(a^m - b^m, a^k - b^k) =$$

$$\overset{zał.}{=} a^{\gcd(m,k)} - b^{\gcd(m,k)} = a^{\gcd(m, n-m)} - b^{\gcd(m, n-m)} =$$

$$= a^{\gcd(m,n)} - b^{\gcd(m,n)}$$

□

Lemat * $a \perp b \Rightarrow \gcd(ac, b) = \gcd(c, b)$

D-d

$g_1 = \gcd(ac, b) = ac x_1 + b y_1$

$g_2 = \gcd(c, b) = c x_2 + b y_2$

$\gcd(a, b) = 1 = ax + by$ →

$ax + by = 1$

$axy_2 + byy_2 = y_2$

$ax(x_2 + ax by_2 + byy_2 = y_2$

$ac(xx_2) + b(axy_2 + yy_2) = y_2$

$gcd(ac, b) = y_1 \Rightarrow y_1 | y_2$

$ax + by = 1$

$axy_1 + byy_1 = y_1$

$a^2x(x_1 + axby_1 + byy_1 = y_1$

$c(a^2xx_1) + b(axy_1 + yy_1) = y_1$

$gcd(c, b) = y_2 \Rightarrow y_2 | y_1$

$y_1 | y_2 \wedge y_2 | y_1 \Rightarrow y_1 = y_2$ ∎

Zad. 14.

~~Zał. nie wprost~~

D-d nie wprost

Zał. że istnieje takie n, dla którego nie istnieje ~~potęga~~ n-cyfrowa potęga 2 z najbardziej znaczącą cyfrą równą 1.

Wtedy $\exists_k \; 2^k < 10^{n-1} \wedge 2^{k+1} \geq 2 \cdot 10^{n-1}$

(2^{k+1} ← następna potęga)

$\Downarrow$

$2^k < 10^{n-1} \wedge 2^k \geq 10^{n-1}$

Sprzeczność!

Czyli zawsze istnieje taka potęga, dla dow. n.

Dowód jednoznaczności:

2^k – najmniejsza (taka) liczba n-cyfrowa z 1 na początku

$2^k \geq 10^{n-1}$

$2^{k+1} \geq 2 \cdot 10^{n-1}$ Następna potęga ma już 2 na początku.

Czyli nie istnieją k_1 i k_2 takie, że: $(k_1 \neq k_2)$

$10^{n-1} \leq 2^{k_1} < 2 \cdot 10^n$

$10^{n-1} \leq 2^{k_2} < 2 \cdot 10^n$ ∎

Zad. 1. $n \geq 1$

Teza: $f(n) = \sum_{k=1}^{n} \lceil \log_2 k \rceil = n + f(\lfloor \frac{n}{2} \rfloor) + f(\lceil \frac{n}{2} \rceil)$ ✓ -1

Dowód

$$f(n) = \sum_{k=1}^{n} \lceil \log_2 k \rceil = \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 (2k) \rceil + \sum_{k=1}^{\lceil \frac{n}{2} \rceil} \lceil \log_2 (2k-1) \rceil =$$

$$= \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil 1 + \log_2 k \rceil + \sum_{k=1}^{\lceil \frac{n}{2} \rceil} \lceil 1 + \log_2 \left(k - \frac{1}{2}\right) \rceil =$$

$$= \underbrace{\lfloor \frac{n}{2} \rfloor + \lceil \frac{n}{2} \rceil}_{n} + \underbrace{\sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \lceil \log_2 k \rceil}_{f(\lfloor \frac{n}{2} \rfloor)} + \sum_{k=2}^{\lceil \frac{n}{2} \rceil} \lceil \log_2 \left(k - \frac{1}{2}\right) \rceil =$$

$$= n + f(\lfloor \tfrac{n}{2} \rfloor) - 1 + \sum_{k=2}^{\lceil \frac{n}{2} \rceil} \lceil \log_2 \left(k - \frac{1}{2}\right) \rceil =$$

$$= n - 1 + f(\lfloor \tfrac{n}{2} \rfloor) + f(\lceil \tfrac{n}{2} \rceil) \quad \blacksquare$$

$$\left(\sum_{k=1}^{\lceil \frac{n}{2} \rceil} \lceil \log_2 k \rceil = \sum_{k=2}^{\lceil \frac{n-1}{2} \rceil} \lceil \log \left(k - \frac{1}{2}\right) \right)$$

$$\lceil \log_2 1 \rceil + \lceil \log_2 2 \rceil + \lceil \log_2 3 \rceil + \lceil \log_2 4 \rceil + \ldots + \lceil \log_2 \lceil \tfrac{n}{2} \rceil \rceil$$

$$\lceil \log_2 1{,}5 \rceil + \lceil \log_2 2{,}5 \rceil + \lceil \log_2 3{,}5 \rceil + \ldots + \lceil \log_2 \lceil \tfrac{n}{2} \rceil - \tfrac{1}{2} \rceil$$

~~Zad. $f(1) = 0$~~

2) $f(1) = 2 \Rightarrow f$ to jedyna funkcja spełniająca podaną zależność (jest jednoznaczna)

~~Dowód~~

$f(1) = 0$

$f(2) = 2 - 1 + f(1) + f(1)$

$f(3) = 3 - 1 + f(1) + f(2)$

$f(4) = 4 - 1 + f(2) + f(2)$

$\vdots$

Każda kolejna wartość odwołuje się rekurencyjnie do $f(1)$. Czyli znając wartość $f(1)$ wiemy że f jest jednoznaczna. Prosta indukcja.