Matematyka Dyskretna

Ćwiczenia – Lista 3

Zadanie 4.

- Algorytm (zapisany w SML'u):

```
(* expmod - podnosi x do potęgi k modulo n *)
fun expmod x 1 n = x mod n
  | expmod x k n =
        let
            val xl = expmod x (k div 2) n
        in
            if k mod 2 = 0
                then (xl * xl) mod n
                else (x * xl * xl) mod n
        end
```

- Ilość mnożeń wykonywanych przez powyższy algorytm:

$$T(k) = c + T\left(\left\lfloor \frac{k}{2} \right\rfloor\right) = c + c + T\left(\left\lfloor \frac{k}{4} \right\rfloor\right) = c + c + c + T\left(\left\lfloor \frac{k}{2^3} \right\rfloor\right) =$$
$$= \underbrace{c + c + c + \cdots + c}_{m} + T\left(\left\lfloor \frac{k}{2^m} \right\rfloor\right) = \underbrace{c + c + c + \cdots + c}_{\log_2 k} + T\left(\left\lfloor \frac{k}{2^{\log_2 k}} \right\rfloor\right) =$$
$$= \log_2 k \cdot c + 0 = O(\log_2 k)$$

Zadanie 11.

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

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

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

Zatem:

$$x = 23 \qquad y = -37 \qquad \gcd(448, 721) = 7$$

(b) $333x + 1234y = 1$, $x, y \in \mathbb{Z}$,

1234	333		
333	$1234 - 3 \cdot 333$	$=$	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

$$\begin{aligned} 21 - 19 = 20 - (39 - 20) = 2 \cdot 20 - 39 = 2 \cdot (98 - 2 \cdot 39) - 39 = 2 \cdot 98 - 5 \cdot 39 = \\ = 2 \cdot 98 - 5 \cdot (235 - 2 \cdot 98) = 12 \cdot 98 - 5 \cdot 235 = 12 \cdot (333 - 235) - 5 \cdot 235 = \\ = 12 \cdot 333 - 17 \cdot 235 = 12 \cdot 333 - 17 \cdot (1234 - 3 \cdot 333) = 63 \cdot 333 - 17 \cdot 1234 \end{aligned}$$

Zatem:

$$x = 63 \qquad y = -17 \qquad \Longrightarrow \qquad 333^{-1} \text{ w pierścieniu } \mathbb{Z}_{1234} \text{ wynosi } 63$$

(c) $-69^{-1} \mod 1313 \equiv x$,

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

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

$$\begin{aligned} 69 - 34 \cdot 2 = 69 - 34 \cdot (1244 - 18 \cdot 69) = 613 \cdot 69 - 34 \cdot 1244 = \\ = 613 \cdot (1313 - 1244) - 34 \cdot 1244 = 613 \cdot 1313 - 647 \cdot 1244 \end{aligned}$$

Zatem:

$$x = -647 \equiv \underline{666} \mod 1313$$

Zadanie 12.

Aby udowodnić tezę postawioną w zadaniu najpierw pokażę trzy lematy:

(a) $\gcd(F_{n-1}, F_n) = 1$,

Dowód.
Indukcja po n:

- $\gcd(F_1, F_2) = \gcd(1, 1) = 1 \qquad \surd$
- Załóżmy, że dla $n' < n$ równość zachodzi, zatem:

$$\gcd(F_{n-1}, F_n) = \gcd(F_{n-1}, F_{n-1} + F_{n-2}) = \gcd(F_{n-1}, F_{n-2}) \overset{\text{z zał. ind.}}{=} 1$$

□

(b) $F_{m+n} = F_{m+1}F_n + F_mF_{n-1}$,

Dowód.
Indukcja po n:

- $F_{m+1} = F_{m+1}F_1 + F_mF_0 = F_{m+1} \cdot 1 + F_m \cdot 0 = F_{m+1} \qquad \surd$
- Załóżmy, że dla $n' < n$ równość zachodzi, zatem:

$$\begin{aligned} F_{m+n} = F_{m+n-2} + F_{m+n-1} \overset{\text{z zał. ind.}}{=} F_{m+1}F_{n-2} + F_mF_{n-3} + F_{m+1}F_{n-1} + F_mF_{n-2} = \\ = F_{m+1}(F_{n-2} + F_{n-1}) + F_m(F_{n-3} + F_{n-2}) = F_{m+1}F_n + F_mF_{n-1} \end{aligned}$$

□

(c) jeśli $m|n$ to $F_m|F_n$,

Dowód.
Skoro zachodzi $m|n$ to $\exists_{q\in\mathbb{N}}\ n = qm$, zatem $F_n = F_{qm}$.
Oczywistym jest, że $F_m|(q' \cdot F_m)$ (dla $q' \in \mathbb{N}$).
Aby dowieść, że $F_m|F_{qm}$ pokażę, że $\exists_{q'\in\mathbb{N}}\ F_{qm} = q' \cdot F_m$.
Indukcja po q:

- $F_{1\cdot m} = 1 \cdot F_m \qquad \surd$
- Załóżmy dla pewnego $k \in \mathbb{N}$, że jeśli $q \le k$ to $\exists_{q'\in\mathbb{N}}\ F_{qm} = q' \cdot F_m$, zatem (dla $q = k$):

$$F_{(q+1)m} = F_{qm+m} \overset{\text{(b)}}{=} F_{qm+1}F_m + F_{qm}F_{m-1} \overset{\text{z zał. ind.}}{=} F_{qm+1}F_m + q'F_mF_{m-1} =$$
$$= F_m \overbrace{(F_{qm+1} + q'F_{m-1})}^{q''}$$

□

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

Dowód.

$$\gcd(F_m, F_n) = \gcd(F_m, F_{qm+r}) \overset{\text{(b)}}{=} \gcd(F_m, F_{qm+1}F_r + F_{qm}F_{r-1}) \overset{\text{(c)}}{=} \gcd(F_m, F_{qm+1}F_r) \overset{\star}{=} \gcd(F_m, F_r)$$

$\star$ z (c) wiadomo, że $F_m|F_{qm}$, natomiast z (a) wiemy, że $F_{qm} \perp F_{qm+1}$, zatem $F_m \perp F_{qm+1}$,

Otrzymaliśmy, że dla $n = qm + r$, zachodzi $\gcd(F_n, F_m) = \gcd(F_m, F_r)$, czyli algorytm Euklidesa działający dla <u>indeksów</u> liczb Fibonacciego. □

Zadanie 13.

Jeśli $a \perp b$ i $a > b$ to $\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(m,n)} - b^{\gcd(m,n)}$ $(\star)$, $0 < m < n$.

Dowód.
Indukcja po n.

1. <u>$n = 0$</u>: $\gcd(a^m - b^m, 0) = a^{\gcd(m,0)} - b^{\gcd(m,0)} \qquad \surd$
2. Załóżmy, że dla $n' < n$ równanie $(\star)$ jest prawdziwe, pokażę zatem, że dla $n' = n$ równość $(\star)$ też zachodzi.

$$\gcd(a^m - b^m, a^n - b^n) = \gcd(a^m - b^m, a^{m+k} - b^{m+k}) =$$
$$= \gcd(a^m - b^m, (a^{m+k} - a^m b^k) + (a^m b^k - b^{m+k})) =$$
$$= \gcd(a^m - b^m, a^m(a^k - b^k) + b^k(a^m - b^m)) \overset{\text{(a)}}{=} \gcd(a^m - b^m, a^m(a^k - b^k)) \overset{\text{(b)}}{=}$$
$$\overset{\text{(b)}}{=} \gcd(a^m - b^m, a^k - b^k) \overset{\text{z założenia indukcyjnego}}{=} a^{\gcd(m,k)} - b^{\gcd(m,k)} =$$
$$= a^{\gcd(m,n-m)} - b^{\gcd(m,n-m)} \overset{\text{(a)}}{=} \underline{a^{\gcd(m,n)} - b^{\gcd(m,n)}}$$

(a) $\gcd(m, qm + r) = \gcd(m, r)$,
(b) jeśli $b \perp c$ to $\gcd(ab, c) = \gcd(a, c)$,

□