1. DBD. Tarpusavyje pirminiai skaičiai. Pirminiai skaičiai. Skaičių faktorizacija.

Euklido algoritmas ir tiesinė DBD išraiška.Matrica Euklido algoritmui:

$$\begin{bmatrix} 1 & 0 & 7605 \\ 0 & 1 & 5733 \end{bmatrix} (-1)\uparrow \rightsquigarrow \begin{bmatrix} 1 & -1 & 1872 \\ 0 & 1 & 5733 \end{bmatrix} (-3)\downarrow \rightsquigarrow$$

$$\begin{bmatrix} 1 & -1 & 1873 \\ -3 & 4 & 177 \end{bmatrix} (-16)\uparrow \rightsquigarrow \begin{bmatrix} 49 & -65 & 0 \\ -3 & 4 & 117 \end{bmatrix} \Longrightarrow$$

$(7605, 5733) = 117$ ir $117 = (-3)\cdot 7605 + 4 \cdot 5733$.

1. Apskaičiuokite:
1) $(1776, 1492) =$
2) $(1274, 1089) =$
3) $(7605, 5733) =$
4) $(3553, 527) =$

FIBONACCI skaičių apibrėžimas matricomis:

$f_0 = 0$, $\begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}$.

2. Įrodyti, kad $\forall n \in \mathbf{N}_0$ $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1} = \begin{pmatrix} f_{n+2} & f_{n+1} \\ f_{n+1} & f_n \end{pmatrix}$.

3. Įrodyti, kad $\forall n, m \in \mathbf{N}, m > 1$ $f_{m+n} = f_{m-1}f_n + f_m f_{n+1}$.

4. Įrodyti, kad $f_{mn} \mid f_m$.
5. Įrodyti, kad $\mathrm{DBD}(f_n, f_{n+1}) = 1$.
6. Įrodyti, kad $\mathrm{DBD}(f_m, f_n) = f_{\mathrm{DBD}(m,n)}$.

FERMAT faktorizacijos procesas:

Babilono laikų formulė $n = a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$ *sako, kad faktorizuojamą skaičių reikia rašyti dviejų kvadratų skirtumu:* $n = r^2 - s^2$ *. Todėl:*

(i) Apibrėžiame $r_0 = [\sqrt{n}]$;

(ii) Tikriname, ar $(r_0 + i)^2 - n$ *yra pilnas kurio nors skaičiaus kvadratas , kai* $i = 0, 1, 2, 3, ...$

Jei $n + s^2$ *nėra sveikojo skaičiaus kvadratas, kai* $s = 1, 2, ..., \frac{n-3}{2}$ *, tai n - pirminis .*

7. Faktorizuokite:

1) 2881;
2) 135337;
3) 2027651281;
4) 236273;
5) 438359;
6) 2091589.