MONTGOMERY'S ZEROS

$n = 98 \quad (98,99) \to (49,50) \to (24,25) \to (12,13)$

$\to (6,7) \to (3,4) \to (1,2)$

$\leftarrow \quad \rightleftarrows \quad \rightleftarrows$

$$(n_{i+1}, n'_{i+1}) = \begin{cases} (2n_i,\ n_i + n'_i) \\ (n_i + n'_i,\ 2n'_i) \end{cases}$$

$$n = \sum_{i=0}^{k-1} a_i 2^i$$

$$2^{k-1} \le n < 2^k$$

$a_{k-1} \neq 0$

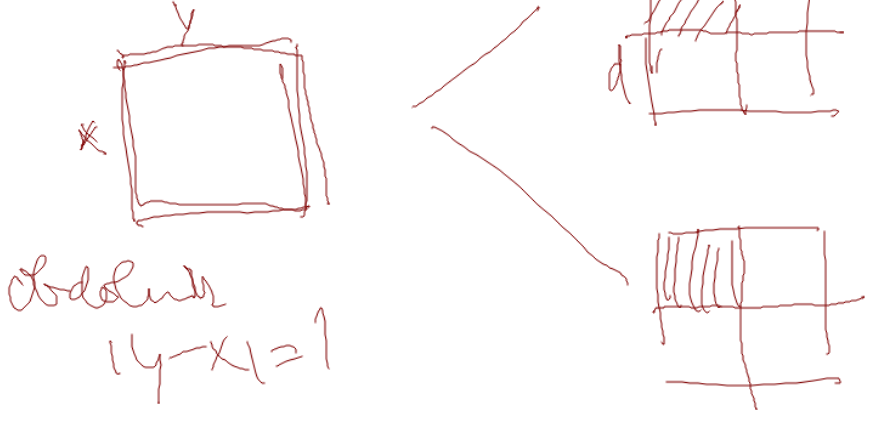
$$n_j = \sum_{1 \le i \le j} a_{k-i} 2^{j-i} \qquad n_1 = a_{k-1}$$

$$n'_j = n_j + 1$$

$$n_k = \sum_{1 \le i \le k} a_{k-i} 2^{k-i} = \sum_{i=0}^{k-1} a_i 2^i = n$$

$j < i \quad a_{k-j-1} = 0, \quad n_{j+1} = \sum_{1 \le i \le j+1} a_{k-i} 2^{j+1-i} = \sum_{1 \le i \le j} a_{k-i} 2^{j+1-i} = 2n_j$

$j < i \quad a_{k-j-1} = 1, \quad n_{j+1} = 1 + \sum_{1 \le i \le j} a_{k-i} 2^{j+1-i} = 2n_j + 1 = 2n'_j$



Ordinate
$|y - x| = 1$

2 dvojas

$$[2](x,y) = (-2x + B\tilde{\lambda}^2 - A,\ \tilde{\lambda}(x - \tilde{x}) - y)$$

$$(\tilde{x}, \tilde{y}) \qquad \tilde{\lambda} = \frac{3x^2 + 2Ax + 1}{2By} \qquad \tilde{\lambda}^2 = \frac{(3x^2 + 2Ax + 1)^2}{4(x^3 + Ax^2 + x)}$$

$B^2 y^2$

$$(-2x + B\tilde{\lambda}^2 - A)(4x^3 + Ax^2 + x) = -(2x + A)\,4(x^3 + Ax^2 + x)$$

$$+ (3x^2 + 2Ax + 1)^2 =$$

$$9x^4 + 4A^2x^2 + 1 + 12Ax^3 + 6x^2 + 4Ax$$

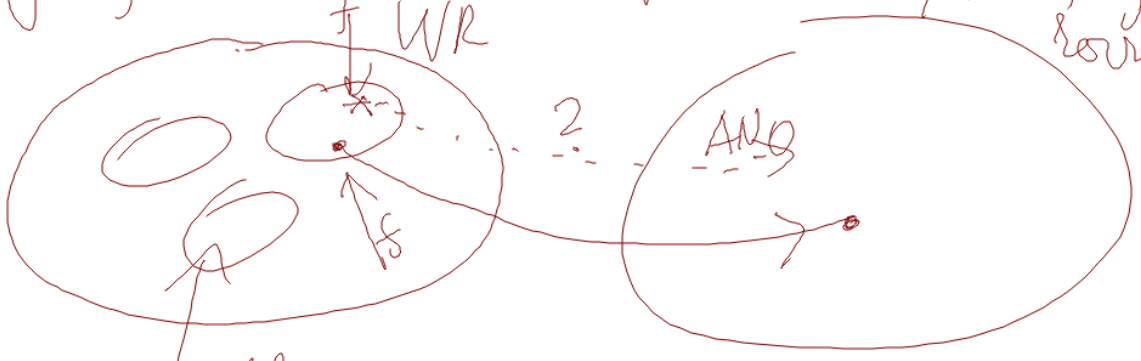
$$-8x^4 - 4Ax^2 \quad -12Ax^3 \quad -8x^2 \quad -4Ax \quad -A^2x^2$$

$$= x^4 - 2x^2 + 1 = (x^2 - 1)^2$$

$$\tilde{x} = \frac{(x^2 - 1)^2}{4(x^3 + Ax^2 + x)}$$

WK

$y^2 = f(x)$ ⟶ WK pokud $\exists \xi$, že $f(\xi) = 0$ $f'(\xi) \neq 0$ (jednoduchý kořen WK)



skupiny dle K-ekvivalence

$\tilde{f}(x) = f(x+\mu)$

$\xi - \mu$ je kořen f

Dle při K-ekvivalenci zůstal posloupnost

posunutím $X \longmapsto X + \mu$ a při zachování

TO DEPRIMOVAT, KDY ODE STUPEŇ V VYNÁSOBENÍ

$y^2 = f(x)$

$y^2 = x^3 + a_2 x^2 + a_4 x + a_6$

$y^2 = x^3 + a_2 \lambda^2 x^2 + a_4 \lambda^4 x + \lambda^6$

$\xi \to \lambda^2 \xi$

$\tilde{f}(\lambda^2 \xi) = \lambda^6 f(\xi) = 0$

$f'(\xi) = 3\xi^2 + 2a_2\xi + a_4$

$(\tilde{f}'(\lambda^2\xi)) =$

$3\lambda^4\xi^2 + 2a_2\lambda^2\xi + \lambda^4 a_4$

JACOBIHO SOUŘADNICE

$[a:b:c] = [u:v:w]$ $\quad aw = cu \quad bw = vc \quad av = bu$

$[a|b|c] = [u|v|w]$ $\quad aw^2 = c^2u \quad bw^3 = vc^3 \quad a^3v^2 = b^2u^3$

afinní bod

$[a:b:1] = [ac:bc:c]$

$[a|b|1] = [ac^2|bc^3|c]$

$[a|b|0] = [u|v|0]$

$\Longleftrightarrow a^3v^2 = b^2u^3$

v bodech afinních 1-1 korespondence

v bodech v ∞ bez záruk

$a = \sum a_{ij} x^i y^j \xrightarrow{\text{hom}} \sum a_{ij} X^i Y^j Z^k \quad i+j+k = d = \max\{i+j;\ a_{ij} \neq 0\}$

JACOBI

$\sum a_{ij} X^i Y^j Z^k \quad 2i+3j+k = d = \max\{2i+3j;\ a_{ij} \neq 0\}$

Homogenizace

znamená je

nula polynomu nezávisí na volbě

zástupce bodu

$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$

$Y^2 + a_1 XYZ + a_3 YZ^3 = X^3 + a_2 X^2 Z^2 + a_4 X Z^6 + a_6 Z^6$

který bod v nekonečnu $Z = 0$

$[\alpha|\beta|0] \quad \beta^2 = \alpha^3$

$[\alpha|\beta|0] = [1|1|0] \Longleftrightarrow \alpha^3 = \beta^2$

JEDINÝ BOD V NEKONEČNU

Ptejme se, jak vypadá sčítání na křivce $y^2 = x^3 + ax + b$ v Jacobiho souřadnicích [v projektivních]

$$\lambda = \frac{\alpha_2 - \beta_2}{\alpha_1 - \beta_1} = \frac{\alpha_2/\alpha_3^3 - \beta_2/\beta_3^2}{\alpha_1/\alpha_3^2 - \beta_1/\beta_3^2} \qquad \lambda \alpha_3 \beta_3 = \frac{\alpha_2 \beta_3^3 - \beta_2 \alpha_3^3}{\alpha_1 \beta_3^2 - \alpha_2 \beta_3^2}$$

Odvodí se vzorce v Jacobiho souřadnicích pro sčítání a zdvojení. Ukáže se nakonec, že v Jacobiho souřadnicích

	ZDVOJENÍ	PROJEKTIVNÍ
	4M+6S	5S+7M
	12M+4S	12M+2S
	11M+4S	

(X, Y, Z, Z^2, Z^3) CHUDNOVSKÉHO SOUŘADNICE

5M+6S 11M+3S