1 Faktorizace

Problém faktorizace spočívá v tom, že je výpočetně složité nalézt řešení pro rovnici $a^x = b \bmod n$, kde známe b, a a snažíme se nalézt x. Tomuto principu se říká princip diskrétního logaritmu. Na tomto principu je postaveno mnoho kryptosystémů jako např.: RSA, DSA, Diffie-Hellman apod..

2 Eliptické křivky

Eliptické křivky jsou v klasické definici definovány jako hladké spojité křivky definované rovnicí $y^2 + 2xy = ax^3 + bx^2 + cx + d$, tato obecná definice je ale jak pro potřeby kryptografických protokolů zkrácena na tzv. Weierstrassův tvar $y^2 = x^3 + ax + b$. Nad těmito křivkami je definována operace sčítání.

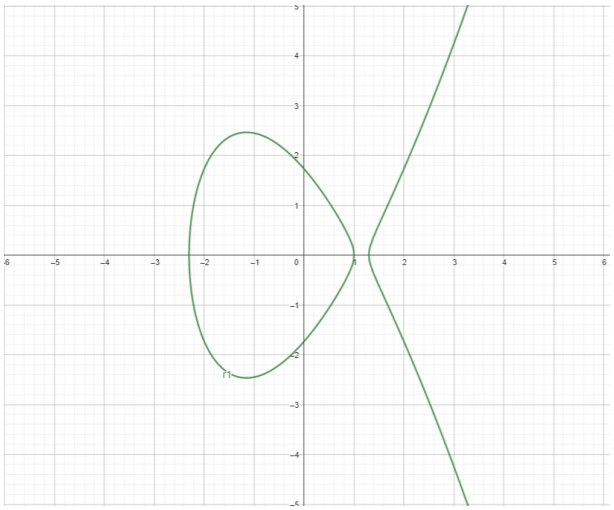

Figure 1: Eliptická křivka ve Weierstrassově tvaru: $y^2 = x^3 - 4x + 3$

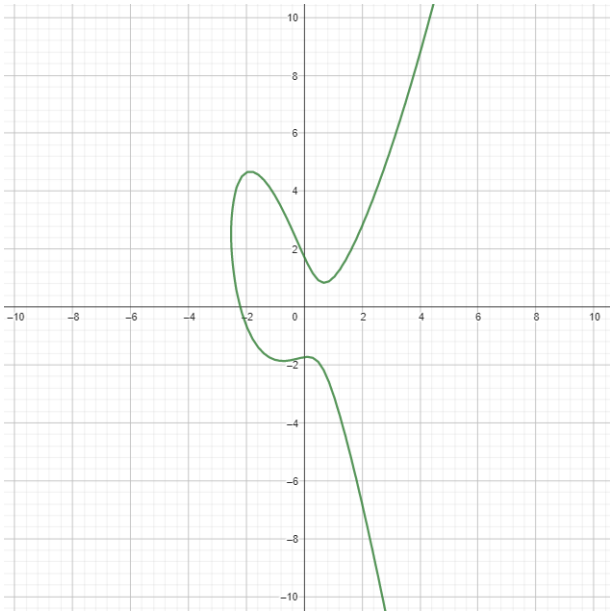

Figure 2: Eliptická křivka v obecném tvaru: $y^2 + 2xy = 2x^3 + 2x^2 - 4x + 3$

2.1 Eliptické křivky nad tělesem F_p

Pro potřeby kryptografie bylo rozhodnuto že se budou používat eliptické křivky nad tělesem F_p. Tělesem F_p se rozumí zbytková třída modulo p. Tedy eliptické křivky v kryptografii mají nejčastěji Weierstrassovu formu, tedy: $y^2 \equiv x^3 + ax + b \mod p$, kde $4a^3 + 27b^2 \mod p \neq 0$.

2.1.1 Sčítání nad bodů nad tělesem

Mějme dva body $P = [x_1, y_1]$ a $Q = [x_2, y_2]$ a libovolnou křivku E modulo p. Pak lze definovat sčítání takto:

$$\begin{aligned} R &= P + Q, \text{kde} - P \neq Q && \mod p; \\ \lambda &\equiv \frac{y_1 - y_2}{x_1 - x_2} && \mod p; \\ x_r &\equiv \lambda^2 - x_1 - x_2 && \mod p; \\ y_r &\equiv \lambda(x_1 - x_2) - y_1 && \mod p. \end{aligned}$$

Nebo jako:

$$\begin{aligned} R &= P + P; \\ \lambda &\equiv \frac{3x_1^2 + a}{2x_1} && \mod p; \\ x_r &\equiv \lambda^2 - 2x_1 && \mod p; \\ y_r &\equiv \lambda(x_1 - x_r) - y_1 && \mod p. \end{aligned}$$

3 Lenstrova faktorizace pomocí eliptických křivek

Lenstrova faktorizace je algoritmus používající eliptické křivky pro nalezení faktorů.
Samotný algoritmus vypadá následovně:

1. Zvolí se náhodná eliptická křivka nad tělesem Z_n ve tvaru $y^2 = x^3 + ax + b \mod n$ společně s bodem $P[x, y]$.

2. Definuje se sčítání pro operaci $R = P + P$ například:

$$\begin{aligned} \lambda &= (3x^2 + a) \cdot (2y^{n-2}) && \mod n; \\ x_r &\equiv \lambda^2 - 2x && \mod n; \\ y_r &\equiv \lambda \cdot 2x - \lambda^2 && \mod n. \end{aligned}$$

3. Spočítá se $k \cdot P$, kde $k = \lfloor \sqrt{n} \rfloor$. V průběhu počítání je nutné spočítat pro každý bod $d = \text{GCD}(f, y_i)$, kde y_i je současná y souřadnice současného bodu a f je číslo jež je faktorizováno. Pokud je $d \neq 1$ a zároveň je různé od n tak byl nalezen dělitel.

4. Pokud byla zvolena vhodná definice sčítání a při spočítání $k \cdot P$ nebyl nalezen dělitel tak lze s nějakou pravděpodobností uvažovat že je f prvočíslo.