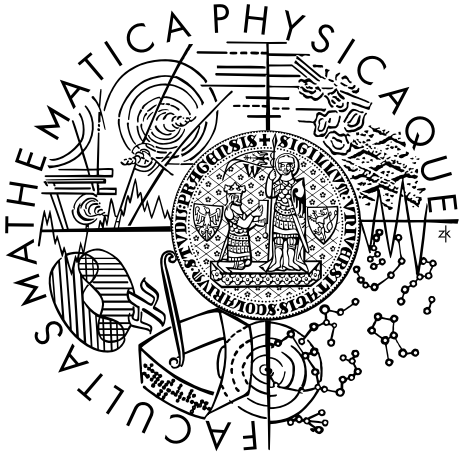
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Vilém Štěpánek

Složitost některých faktorizačních algoritmů

Katedra algebry

Vedoucí bakalářské práce:	doc. Mgr. Pavel Příhoda, Ph.D.
Studijní program:	Matematika
Studijní obor:	Matematické metody informační bezpečnosti (MMIB)

Praha 2016

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Složitost některých faktorizačních algoritmů

Autor: Vilém Štěpánek

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Práce se věnuje odhadu složitosti běhu algoritmu pro faktorizaci celého čísla použitím metody ECM.

Klíčová slova: ECM Faktorizace Eliptické křivky

Title: Complexity of some factoring algorithms

Author: Vilém Štěpánek

Department: Department of algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of algebra

Abstract: Thesis is devoted to estimate complexity of algorithms running time for factorization of integer using ECM.

Keywords: ECM Factorization Elliptic curves

Rád bych poděkoval panu doc. Mgr. Pavlu Příhodovi, Ph.D., vedoucímu mé bakalářské práce, za jeho odborné rady, vedení a věnovaný čas. Také bych chtěl poděkovat rodině a mým blízkých za jejich podporu.

Obsah

Úvod

Faktorizační algoritmus na principu eliptických křivek (ECM, z anglického Elliptic curve method) byl sestaven H. W. Lenstrou ml. roku 1985. O rok později Goldwasser a Kilian upravili Lenstrovu metodu a získali prvočíselný test na principu eliptických křivek. Obě zmíněné metody využívají vlastnosti eliptických křivek nad konečnými tělesy.

Algoritmus ECM je sestaven tak, aby byl efektivní pro hledání malých (řádu 10 až 40ti cifer) prvočíselných dělitelů velkých čísel. Oproti ostatním faktorizačním algoritmům ECM metoda vyčnívá tím, že její složitost záleží především na velikosti nalezeného dělitele p zadaného čísla n. Na metodu ECM lze nahlížet jako na zobecnění Pollardovy $p-1$ metody.

Metoda ECM je postavena na Hasseho Větě 10, která nám říká, že pokud p je prvočíslo, pak eliptická křivka E nad tělesem $\mathbf{F}_p$ má řád $p+1-t$, kde $|t| \leq 2\sqrt{p}$ a kde t záleží na zvolené křivce. Pokud $p+1-t$ je hladké číslo pro nějakou mez B, pak ECM s velkou pravděpodobností uspěje a vrátí netriviálního dělitele p čísla n.

Od jejího objevení, metoda ECM byla mnohokrát zlepšována a byly k jejímu běhu přidávány další fáze, které umožňují zrychlení běhu algoritmu na hledání netriviálního dělitele čísla n. Přesto v této práci budeme vycházet především z původní verze algoritmu, jak s ní přišel roku 1985 Lenstra. Proto také ve většině práce budu vycházet z jeho článku (Lenstra Jr, 1987) z roku 1987 a v implementační části budu z důvodu celistvého obsahu látky vycházet z Crandall a Pomerance (2005).

Metoda ECM se jako další faktorizační algoritmy řadí do tzv. subexponenciálních algoritmů a o ECM se říká, že je typu $L[\frac{1}{2},\sqrt{2}]$.

V práci se zaměřím především na analýzu složitosti algoritmu, jak ji provádí autor metody ECM H. W. Lenstra ml. v článku Lenstra Jr (1987). Látku kolem této problematiky více rozvedu, doplním chybějící kroky v důkazech a názorně ukáži, jak fungují operace na eliptických křivkách. Dále nastíním souvislost Lenstrovy metody ECM s několika důležitými větami, o které se autor opírá (Hasseho Věta 10 a Deuringova Věta 12). Dále rozvedu, kde autor přichází na věci, které explicitně neuvádí a v neposlední řadě implementuji program, který provádí ECM faktorizaci celého čísla a program, který umožňuje alespoň částečně testovat hypotézu, o kterou se opírá Hypotéza 1, která uvádí odhadovaný čas běhu této faktorizační metody. Poslední zmíněný program bude testovat pravděpodobnost, že náhodné číslo z intervalu $(p-\sqrt{p}+1, p+\sqrt{p}+1)$ je hladké pro danou mez.

1. Složitost Metody eliptických křivek pro faktorizaci celého čísla

Vzhledem k rozsahu práce nebudu probírat veškerou teorii kolem eliptických křivek, proto pro více informací ohledně „fungování“ eliptických křivek doporučuji nahlédnout literaturu: EllipticCurves Jedlicka, Kapitola 2 a video Riverninj4. Přestože nebudu teorii kolem eliptických křivek zcela probírat, snažím se v práci o přiblížení této problematiky a doplnění nejasných, nebo chybějících kroků z materiálů, ze kterých čerpám a případně přiblížit látku srozumitelněji a zřetelněji.

1.1 Definice a zavedení pojmů

Značení 1 (Přirozený logaritmus)**.** *V celé práci budeme* log *označovat přirozený logaritmus. Logaritmus při jiném základu explicitně vyjádříme.*

Nejprve začneme s tělesem $\mathbf{K}$, později nás bude zajímat především případ $\mathbf{K} = \mathbf{F}_p$ pro nějaké prvočíslo p. Pro zjednodušení výkladu budeme předpokládat, že charakteristika $\mathbf{K}$ je různá od 2 a od 3.

Definice 1 (Projektivní rovina)**.** *Projektivní rovinu* $\mathbf{P}^2(\mathbf{K})$ *definujeme jako množinu ekvivalentních tříd trojic* $(x, y, z) \in \mathbf{K} \times \mathbf{K} \times \mathbf{K}, (x, y, z) \neq (0, 0, 0)$*. Dva body* (x, y, z) *a* (x', y', z') *jsou ekvivalentní, pokud existuje* $c \in \mathbf{K}^*$ *takové, že* $cx = x', cy = y'$ *a* $cz = z'$*. Třída ekvivalence obsahující* (x, y, z) *se značí* $(x : y : z)$*.*

Pro dobrou práci s eliptickými křivkami je nutné, abychom byli schopni vést každým bodem $P = (x_0 : y_0 : z_0) \in \mathbf{P}^2(\mathbf{K})$ eliptické křivky $\mathrm{E}(\mathbf{K}) = \{(x : y : z) \in \mathbf{P}^2(\mathbf{K}) : y^2z = x^3 + axz^2 + bz^3\}$ tečnu (viz Definice 3 níže). Označme $f(x, y, z) = y^2z - x^3 - axz^2 - bz^3$, poté tato tečna odpovídá projektivní přímce s rovnicí

$$\frac{\delta f}{\delta x}\big(P\big) \cdot x + \frac{\delta f}{\delta y}\big(P\big) \cdot y + \frac{\delta f}{\delta z}\big(P\big) \cdot z = 0,$$

kde alespoň jedna z parciálních derivací $\frac{\delta f}{\delta x}\big(P\big), \frac{\delta f}{\delta y}\big(P\big), \frac{\delta f}{\delta z}\big(P\big)$ je nenulová. To vede k definici:

Definice 2 (Singulární křivka)**.** *Nechť* $\mathbf{K}$ *je těleso a* F *je křivka daná množinou bodů*

$$\mathrm{F}(\mathbf{K}) = \{(x : y : z) \in \mathbf{P}^2(\mathbf{K}) : y^2z - x^3 - axz^2 - bz^3 = 0\}.$$

Označme $f(x, y, z) = y^2z - x^3 - axz^2 - bz^3$.
Řekneme, že křivka F *je singulární, pokud existuje bod* $P = (x_0 : y_0 : z_0) \in \mathbf{P}^2(\overline{\mathbf{K}})$:

$$\frac{\delta f}{\delta x}\big(P\big) = \frac{\delta f}{\delta y}\big(P\big) = \frac{\delta f}{\delta z}\big(P\big) = 0, \qquad f(P) = 0 \tag{1.1}$$

Řekneme, že křivka je nesingulární, pokud není singulární.

V následující definici budeme využívat nerovnosti $4a^3+27b^2 \neq 0$, kde $a, b \in \mathbf{K}$, důvod této nerovnosti plyne z nutnosti nesingularity eliptické křivky. Odvození této nerovnosti je vysvětleno v Poznámce 2, která je uvedena až po definici eliptické křivky.

Definice 3 (Eliptická křivka)**.** *Nechť* $\mathbf{K}$ *je těleso. Eliptickou křivku nad tělesem* $\mathbf{K}$ *rozumíme dvojici prvků* $a, b \in \mathbf{K}$*, která určuje Weierstrassovu rovnost*

$$y^2 = x^3 + ax + b, \tag{1.2}$$

a která splňuje $4a^3 + 27b^2 \neq 0$.
Eliptickou křivku danou dvojicí (a, b) *označme* $\mathrm{E}_{a,b}$*, nebo zjednodušeně* E.
Poté množinu bodů eliptické křivky definujeme jako množinu bodů

$$\mathrm{E}(\mathbf{K}) = \{(x : y : z) \in \mathbf{P}^2(\mathbf{K}) : y^2z = x^3 + axz^2 + bz^3\},$$

kde $\mathbf{P}^2(\mathbf{K})$ *značí projektivní rovinu nad tělesem* $\mathbf{K}$*.*

Poznámka 1. *Pro zjednodušení zápisu budeme množinu bodů eliptické křivky často zjednodušeně nazývat eliptickou křivkou.*

Mějme E eliptickou křivku nad tělesem $\mathbf{K}$. Poté $\mathrm{E}(\mathbf{K})$ obsahuje právě jeden bod $(x : y : z)$, pro který $z = 0$. Jedná se o bod $(0 : 1 : 0)$. Tento bod budeme nazývat „nulovým bodem“ křivky a budeme ho značit O. Ostatní body $\mathrm{E}(\mathbf{K})$ jsou body $(x : y : 1)$, kde $x, y \in \mathbf{K}$ a splňují (1.2). Množina $\mathrm{E}(\mathbf{K})$ má strukturu Abelovské grupy, grupový zákon je definován následovně:

- $O + P = P + O = P$ pro všechna $P \in \mathrm{E}(\mathbf{K})$, graficky viz Obrázek 3.4.
- Nechť $P = (x_1 : y_1 : 1), Q = (x_2 : y_2 : 1)$ jsou nenulové body. Poté $P + Q = O \iff x_1 = x_2$ a $y_1 = -y_2$, graficky viz Obrázek 3.4.
- V ostatních případech položme $\lambda \in \mathbf{K}$:

  $\lambda = (y_1 - y_2)/(x_1 - x_2)$ pokud $P \neq Q$, graficky viz Obrázek 3.2,
  $\lambda = (3x_1^2 + a)/(2y_1)$ pokud $P = Q$, graficky viz Obrázek 3.1.

  Poté $P + Q = R$, kde $R = (x_3 : y_3 : 1)$, kde

  $$x_3 = \lambda^2 - x_1 - x_2,$$
  $$y_3 = \lambda(x_1 - x_3) - y_1.$$

  Graficky lze nahlédnout také na obrázcích 3.5 a 3.6.
  Navíc $P + Q = Q + P$ viz 3.7.
- $(P + Q) + R = P + (Q + R)$ viz 3.8.
- O je nulový prvek grupy (viz 3.4).
- $-(x : y : z) = (x : -y : z)$ (viz 3.4).

Poznámka 2. *Mějme* $\mathrm{E}_{a,b}$ *eliptickou křivku nad tělesem* $\mathbf{K}$. *Pak* $\mathrm{E}_{a,b}$ *je nesingulární právě tehdy, když* $4a^3 + 27b^2 \neq 0$

Důkaz. Z Definice 2 máme, že kdyby $\mathrm{E}_{a,b}$ byla singulární, pak by existoval bod $P = (x_0 : y_0 : z_0) \in \mathbf{P}^2(\overline{\mathbf{K}})$:

$$\frac{\delta f}{\delta x}\big(P\big) = \frac{\delta f}{\delta y}\big(P\big) = \frac{\delta f}{\delta z}\big(P\big) = 0 \qquad f(P) = 0 \text{ (viz 1.1)}$$

Derivací snadno vidíme, že

$$\begin{aligned}
\frac{\delta f}{\delta x}\big(P\big) &= -3x^2 - az^2 &&= 0\\
\frac{\delta f}{\delta y}\big(P\big) &= 2yz &&= 0\\
\frac{\delta f}{\delta z}\big(P\big) &= y^2 - 2axz - 3bz^2 &&= 0
\end{aligned}$$

Z úvahy výše vidíme, že body $\mathrm{E}_{a,b}(\mathbf{K})$ jsou buď body tvaru $(x : y : 1)$, kde $x, y \in \mathbf{K}$, nebo bod $(0 : 1 : 0)$.
Pro $(0 : 1 : 0)$ dostáváme $\frac{\delta f}{\delta z}\big((0 : 1 : 0)\big) \neq 0$, tedy $\mathrm{E}_{a,b}$ je v tomto bodě nesingulární pro všechna $a, b \in \mathbf{K}$
Pro $(x : y : 1)$ dostáváme

$$\begin{aligned}
\frac{\delta f}{\delta x}\big(P\big) &= -3x^2 - a &&= 0\\
\frac{\delta f}{\delta y}\big(P\big) &= 2y &&= 0\\
\frac{\delta f}{\delta z}\big(P\big) &= y^2 - 2ax - 3b &&= 0
\end{aligned}$$

Tedy dosazením $y = 0$, které získáme z $\frac{\delta f}{\delta y}$, a $x = \sqrt{\frac{-a}{3}} \in \overline{\mathbf{K}}$, získaného z $\frac{\delta f}{\delta x}$, do $\frac{\delta f}{\delta z}$ dostáváme:

$$-2a\sqrt{\frac{-a}{3}} = 3b \implies -4a^3 = 27b^2$$

Tedy v bodech tvaru $(x : y : 1)$, kde $x, y \in \mathbf{K}$ je $\mathrm{E}_{a,b}$ nesingulární pro $a, b \in \mathbf{K}$ taková, že $4a^3 + 27b^2 \neq 0$.

Naopak předpokládejme $27b^2 + 4a^3 = 0$. Položme $y = 0$ a

$$\begin{aligned}
x &= 0 && \text{pokud } a = b = 0,\\
x &= \frac{-3b}{2a} && \text{pokud } a \neq 0 \neq b.
\end{aligned}$$

Ukážeme, že $P = (x : y : 1)$ splňuje:

$$\begin{aligned}
y^2z &= x^3 + axz^2 + bz^3,\\
\frac{\delta f}{\delta x}\big(P\big) = \frac{\delta f}{\delta y}\big(P\big) &= \frac{\delta f}{\delta z}\big(P\big) = 0.
\end{aligned}$$

Z derivace v důkazu opačné implikace vidíme, že $\frac{\delta f}{\delta x}(P) = \frac{\delta f}{\delta y}(P) = \frac{\delta f}{\delta z}(P) = 0$ je splněno, zbývá tedy ukázat, že $(x : 0 : 1)$ pro oba případy splňuje

$$y^2 z = x^3 + axz^2 + bz^3.$$

Tedy po dosazení:

$$\begin{aligned} 0 &= 0 + 0 + 0 && \text{pokud } a = b = 0, \\ 0 &= \frac{-27b^3}{8a^3} + \frac{-3b}{2} + b = \frac{-27b^3 - 4a^3 b}{8a^3} && \text{pokud } a \neq 0 \neq b. \end{aligned}$$

Tedy, pokud $\mathrm{E}_{a,b}$ je nesingulární, pak $a, b \in \mathbf{K}$ jsou taková, že $4a^3 + 27b^2 \neq 0$. ❑

Definice 4 (Izomorfismus eliptických křivek)**.** *Nechť* $\mathrm{E} = \mathrm{E}_{a,b}$ *a* $\mathrm{E}' = \mathrm{E}_{a',b'}$ *jsou eliptické křivky nad tělesem* $\mathbf{K}$*. Izomorfismus* $\mathrm{E} \to \mathrm{E}'$ *(nad tělesem* $\mathbf{K}$*) je definován jako prvek* $u \in \mathbf{K}^*$*, pro který* $a' = u^4 a$ *a* $b' = u^6 b$*. Pokud izomorfismus* $\mathrm{E} \to \mathrm{E}'$ *existuje, říkáme, že* E *a* E' *jsou izomorfní.*

Z toho již lze snadno nahlédnout následující:

Poznámka 3. *Z libovolného izomorfismu* $u : \mathrm{E} \to \mathrm{E}'$ *plyne izomorfismus* $\mathrm{E}(\mathbf{K}) \to \mathrm{E}'(\mathbf{K})$ *abelovských grup, který zobrazí* $(x : y : z)$ *na* $(u^2 x : u^3 y : z)$*.*

Definice 5 (Automorfismus eliptické křivky)**.** *Nechť* E *je eliptická křivka nad tělesem* $\mathbf{K}$*. Automorfismus* E *je definován jako izomorfismus* $\mathrm{E} \to \mathrm{E}$*.*
Množina automorfismů E *je podgrupou* $\mathbf{K}^*$*, která se označuje* AutE*.*

V následující sekci budeme uvažovat případ, kdy $\mathbf{K} = \mathbf{F}_p$ pro prvočíslo $p > 3$.

Z důvodu propojení souvislosti vážené mohutnosti (viz Definice 7) a velikosti (mohutnosti) množiny je potřeba ujasnit značení velikosti množiny:

Značení 2. *Velikost (mohutnost) množiny* S *budeme značit* $\#S$

Definice 6 (Počet eliptických křivek)**.** *Počet eliptických křivek nad tělesem* $\mathbf{F}_p$ *definujeme jako počet dvojic* $(a, b) \in \mathbf{F}_p \times \mathbf{F}_p$ *splňující* $4a^3 + 27b^2 \neq 0$*.*

Poznámka 4. *Počet eliptických křivek nad tělesem* $\mathbf{F}_p$ *se rovná* $p^2 - p$*.*

Důkaz. Hodnota $p^2 - p$ se získá následovně:

- Počet všech dvojic $(a, b) \in \mathbf{F}_p \times \mathbf{F}_p$ je roven p^2.
- $4a^3 + 27b^2 = 0 \iff a = -3c^2, b = 2c^3$ pro nějaké $c \in \mathbf{F}_p$. Prvek c je jednoznačně určen prvky a, b jako $c = -3b/(2a)$, pokud $a \neq 0$. Tedy $4a^3 + 27b^2 = 0$ právě pro p dvojic (a, b).

Tedy počet dvojic $(a, b) \in \mathbf{F}_p \times \mathbf{F}_p$ takových, že $4a^3 + 27b^2 \neq 0$ je roven $p^2 - p$. ❑

Předešlé definice využijeme pro spočítání počtu množin

$$\{\mathrm{E} : \mathrm{E} \text{ eliptická křivka nad } \mathbf{F}_p\} / \cong_{\mathbf{F}_p}$$

tříd izomorfismů eliptických křivek nad $\mathbf{F}_p$. Počet eliptických křivek izomorfních dané eliptické křivce E je $\#\mathbf{F}_p^*/\#\mathrm{AutE} = (p-1)/\#\mathrm{AutE}$. Sečtením přes množinu reprezentantů tříd izomorfismů a vydělením $(p-1)$ získáváme

$$\sum_{[\mathrm{E}]\in\mathcal{E}} \frac{1}{\#\mathrm{AutE}} = p,$$

kde $\mathcal{E} = \{\mathrm{E} : \mathrm{E}$ eliptická křivka nad $\mathbf{F}_p\}/\cong_{\mathbf{F}_p}$.

Definice 7 (Vážená mohutnost)**.** *Váženou mohutnost podmnožiny $\mathcal{M}$ množiny tříd izomorfismů eliptických křivek nad $\mathbf{F}_p$, kde*

$$\mathcal{M} \subseteq \{\mathrm{E} : \mathrm{E} \textit{ eliptická křivka nad } \mathbf{F}_p\}/\cong_{\mathbf{F}_p}$$

definujeme jako

$$\#'\mathcal{M} = \sum_{[\mathrm{E}]\in\mathcal{M}} \frac{1}{\#\mathrm{AutE}},$$

kde třída křivek izomorfních s danou eliptickou křivkou E *je počítána s vahou* $(\#\mathrm{AutE})^{-1}$.

Poznámka 5. *Nechť $\mathcal{M} = \{\mathrm{E} : \mathrm{E}$ eliptická křivka nad $\mathbf{F}_p\}/\cong_{\mathbf{F}_p}$, pak*

$$\#'\mathcal{M} = \#'\{\mathrm{E} : \mathrm{E} \textit{ eliptická křivka nad } \mathbf{F}_p\}/\cong_{\mathbf{F}_p} = \sum_{[\mathrm{E}]\in\mathcal{M}} \frac{1}{\#\mathrm{AutE}} = p.$$

Definice 8 (Forma)**.** *Nechť $\Delta \in \mathbb{Z}, \Delta < 0, \Delta \equiv 0{,}1 \bmod 4$. Pozitivně definitní celočíselnou binární kvadratickou formou s diskriminantem Δ, zkráceně budeme označovat formou, rozumíme polynom $F = aX^2 + bXY + cY^2$ s koeficienty $a, b, c \in \mathbb{Z}, a > 0, b^2 - 4ac = \Delta$.*

Definice 9 (Ekvivalence forem)**.** *Izomorfismem mezi formami $F = aX^2+bXY+cY^2$ a $F' = a'X^2 + b'XY + c'Y^2$ rozumíme matici $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$, kde $\alpha, \beta, \gamma, \delta \in \mathbb{Z}, \alpha\delta - \beta\gamma = 1$, pro které $aX^2+bXY+cY^2 = a'X'^2+b'X'Y'+c'Y'^2$, kde $X' = \alpha X + \beta Y$ a $Y' = \gamma X + \delta Y$. Pokud takovýto izomorfismus existuje, pak řekneme, že F a F' jsou ekvivalentní. Automorfismem F rozumíme izomorfismus mezi F a F.*

Poznámka 6. *Množina automorfismů F je podgrupa $\mathrm{SL}_2\mathbb{Z}$ grupy matic 2×2 s celočíselnými členy a determinantem 1, tato podgrupa se označuje* Aut$F$.
Tyto grupy lze explicitně určit a jsou konečné (Viz Lenstra Jr (1987, sekce (1.6)))

Poznámka 7. *Pro pevné Δ je množina tříd ekvivalence forem s diskriminantem Δ konečná (Viz Lenstra Jr (1987, sekce (1.6))).*

Definice 10 (Kroneckerova třída čísel)**.** *Kroneckerovu třídu čísel $H(\Delta)$ s diskriminantem Δ definujeme jako váženou mohutnost množin tříd ekvivalence forem s diskriminantem Δ, třída ekvivalence obsahující F je počítána s vahou $(\#\mathrm{Aut}F)^{-1}$, tj.:*

$$H(\Delta) = \#'\{F : F \textit{ forma s diskriminantem } \Delta\}/\sim,$$

kde $\sim$ značí ekvivalenci a význam $\#'$ je jako v Definici 7.

Poznámka 8. *Existence formy* $X^2 + bXY - ((\Delta - b^2)/4)Y^2$*, kde* $\Delta \equiv b^2 \bmod 4$ *ukazuje, že* $H(\Delta) > 0$.

Definice 11 (Primitivní forma)**.** *Nechť* $F = aX^2 + bXY + cY^2$ *je forma a nechť prvky* a, b, c *splňují* $NSD(a, b, c) = 1$*, poté říkáme, že forma* F *je primitivní.*

Poznámka 9. *Označme* $h(\Delta)$ *váženou mohutnost množiny tříd ekvivalence primitivních forem s diskriminantem* Δ *počítanou se stejnou vahou jako výše. Poté*

$$H(\Delta) = \sum_d h(\Delta/d^2),$$

kde suma prochází přes $d \in \mathbb{N}$*, pro která* $\Delta/d^2 \equiv 0{,}1 \bmod 4$.

Věta 10 (Hasseho)**.** *Řád* $\#\mathrm{E}(\mathbf{F}_p)$ *eliptické křivky* $\mathrm{E}(\mathbf{F}_p)$ *splňuje*

$$|\#\mathrm{E}(\mathbf{F}_p) - (p+1)| \leq 2\sqrt{p}. \tag{1.3}$$

Pro více informací lze nahlédnout v Crandall a Pomerance (2005) Věta 7.3.1.

Poznámka 11. *Hasseho věta je důležitý důsledek pro teorii eliptických křivek, jelikož nám přímo ukazuje, kolik prvků může eliptická křivka mít, tedy:*

$$\#\mathrm{E}(\mathbf{F}_p) = p + 1 - t, \text{ kde } t \in \mathbb{Z}, |t| \leq 2\sqrt{p} \tag{1.4}$$

jelikož platí

$$p + 1 - 2\sqrt{p} \leq \#\mathrm{E}(\mathbf{F}_p) \leq p + 1 + 2\sqrt{p}.$$

Věta 12 (Deuringova)**.** *Nechť* $p > 3$ *je prvočíslo,* $|t| \leq 2\sqrt{p}$*. Poté počet eliptických křivek* E *nad tělesem* $\mathbf{F}_p$*, pro které* $\#\mathrm{E}(\mathbf{F}_p) = p+1-t$*, je* $(p-1) \cdot H(t^2-4p)$*. Tedy*

$$\#\{\mathrm{E} : \mathrm{E} \text{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) = p+1-t\} = \frac{p-1}{2} \cdot H(t^2-4p), \tag{1.5}$$

kde $H(t^2 - 4p)$ *je Kroneckerova třída čísel s diskriminantem* $t^2 - 4p$*. Viz Cox (2011, kapitola C., Věta 14.18), dále lze také nahlédnout Schoof (1987).*

Nyní jsme již schopni přijít na vážený počet (až na izomorfismus) eliptických křivek E nad tělesem $\mathbf{F}_p$ splňující 1.4. Z Věty 12 víme, že pro dané t máme počet eliptických křivek s $p + 1 - t$ body roven $\frac{p-1}{2} \cdot H(t^2 - 4p)$. Dále víme, že $\mathrm{E}_{a,b}$ je izomorfní s $\mathrm{E}_{a',b'}$ znamená, že existuje $u \in \mathbf{F}_p^* : a = u^4a', b = u^6b'$. Tedy takových u máme $p - 1$. Navíc platí $u^2 = (-u)^2$, tedy zřejmě $a = u^4a' = (-u)^4a'$ a $b = u^6b! = (-u)^6b'$. Z toho již zřejmě počet různých eliptických křivek izomorfních $\mathrm{E}_{a,b}$ je $(p - 1)/2$.

Důsledek 13. *Nechť* $p > 3$ *je prvočíslo,* $|t| \leq 2\sqrt{p}$*. Poté vážený počet eliptických křivek (až na izomorfismus)* E *nad tělesem* $\mathbf{F}_p$ *splňující 1.4 je:*

$$\#'\{\mathrm{E} : \mathrm{E} \text{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) = p + 1 - t\}/\cong_{\mathbf{F}_p} = H(t^2 - 4p), \tag{1.6}$$

kde $H(t^2 - 4p)$ *je Kroneckerova třída čísel s diskriminantem* $t^2 - 4p$*.*

Teorie kolem předchozích dvou vět je mnoho, přestože se o tyto dvě věty bude práce hodně opírat, nebudu ji zde uvádět. Pro více informací lze nahlédnout Cox (2011, §14. Kapitola C. a §2. Kapitola A.), Crandall a Pomerance (2005, kapitola 7.3), Lenstra Jr (1987), Ughi (1983).

1.2 Odhady různými konstantami

Pro určení složitosti a efektivity algoritmu je nejdříve potřebné provést několik odhadů konstantami. Konstanty postupně čísluji, abych se na ně později snadno odkázal, přesto konstanty nečísluji od c_1, jelikož 7546 z prvního tvrzení, které zde uvedu, lze odhadnout sdola. K tomu odhadu se využijí právě konstanty c_1 a c_2, dolní odhad nepoužiji, proto ho zde neuvedu. Z tohoto důvodu, aby čtenář mohl snadno nahlédnout do odkazované literatury, využívám číslování konstant tak, aby se nepřekrývalo s odkazovanou literaturou a tím nevznikaly nejasnosti.

Tvrzení 14 (Konstanta c_3)**.** *Existuje efektivně spočitatelná konstanta $c_3 > 0$ taková, že*

$$H(\Delta) \leq c_3 \cdot \sqrt{-\Delta} \cdot \log|\Delta| \cdot (\log\log|\Delta|)^2$$

pro každé $\Delta \in \mathbb{Z}, \Delta < 0, \Delta \equiv 0{,}1 \bmod 4$.

Důkaz. Důkaz využívá odhadů v Lenstra Jr (1987, sekce (1.6)), zde nebude uveden, jelikož používá pojmy mimo možnosti této práce. ❑

Tvrzení 15 (Konstanty c_4, c_5)**.** *Existují efektivně spočitatelné konstanty c_4,$c_5 > 0$ takové, že pro každé prvočíslo $p > 3$, platí:*
(a) Nechť $\mathcal{S}$ je množina celých čísel taková, že $\forall s \in \mathcal{S}$ platí: $|s - (p+1)| \leq 2\sqrt{p}$, pak

$$\#'\{\mathrm{E} : \mathrm{E} \text{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) \in \mathcal{S}\}/\cong_{\mathbf{F}_p}$$

$$\leq c_4 \cdot \#\mathcal{S} \cdot \sqrt{p} \cdot (\log p) \cdot (\log\log p)^2.$$

(b) Nechť $\mathcal{S}$ je množina celých čísel taková, že $\forall s \in \mathcal{S}$ platí: $|s - (p+1)| \leq \sqrt{p}$, pak

$$\#'\{\mathrm{E} : \mathrm{E} \text{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) \in \mathcal{S}\}/\cong_{\mathbf{F}_p}$$

$$\geq c_5 \cdot (\#\mathcal{S} - 2) \cdot \sqrt{p}/(\log p).$$

Důkaz. V obou případech (a) i (b) se z 1.6 levá strana nerovnosti rovná

$$\sum_{t, p+1-t \in \mathcal{S}} H(t^2 - 4p)$$

(a) aplikací Tvrzení 14 na každý prvek sumy:

$$\sum_{t, p+1-t \in \mathcal{S}} H(t^2 - 4p) \leq \sum_{t, p+1-t \in \mathcal{S}} c_3 \cdot \sqrt{-t^2 + 4p} \cdot \log\left|t^2 - 4p\right| \cdot (\log\log\left|t^2 - 4p\right|)^2$$

$$\leq c_3 \cdot \#\mathcal{S} \cdot \sqrt{4p} \cdot \log 4p \cdot (\log\log 4p)^2$$

$\log 4p = \log p + \log 4 < 2\log p$, protože $p > 5$, poté $\log\log 4p < \log 2\log p < 3\log\log p$ (lze snadno nahlédnout, že $2\log p < (\log p)^3 \iff e^{\sqrt{2}} < 5 \leq p$). Poté

$$c_3 \cdot \#\mathcal{S} \cdot \sqrt{4p} \cdot \log 4p \cdot (\log\log 4p)^2 \leq 36 \cdot c_3 \cdot \#\mathcal{S} \cdot \sqrt{p} \cdot \log p \cdot (\log\log p)^2$$

Z toho okamžitě získáváme konstantu c_4.
(b) Důkaz využívá odhadu $|t^2 - 4p| \geq 3p$ pro $p + 1 - t \in \mathcal{S}$ a pojmů z kapitoly Lenstra Jr (1987, sekce (1.6)), které jsou mimo možnosti této práce.

❑

Poznámka 16. *Nechť* E *je eliptická křivka nad tělesem* $\mathbf{F}_p$, l *je prvočíslo takové, že* $l < \#\mathrm{E}(\mathbf{F}_p)$, *pak* $\#\mathrm{E}(\mathbf{F}_p) \equiv 0 \bmod l \iff$ *grupa* $\mathrm{E}(\mathbf{F}_p)$ *obsahuje prvek řádu* l. *(Viz Rotman (1995, Věta 4.2))*

Tvrzení 17 (O - Konstanty)**.** *Nechť* p, l *jsou prvočísla,* $p > 3$, $l \neq p$. *Pak se číslo*

$$\#'\{\mathrm{E} : \mathrm{E} \textit{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) \equiv 0 \bmod l\}/\cong_{\mathbf{F}_p}$$

rovná

$$\begin{aligned} &\frac{1}{l-1}p + \mathcal{O}(l\sqrt{p}) \qquad \textit{pokud } p \not\equiv 1 \bmod l, \\ &\frac{l}{l^2-1}p + \mathcal{O}(l\sqrt{p}) \qquad \textit{pokud } p \equiv 1 \bmod l. \end{aligned}$$

$\mathcal{O}$ *- konstanty jsou absolutně a efektivně spočitatelné.*
Význam $\mathcal{O}(l\sqrt{p})$ *je následující:* $\exists c \in \mathbb{R}, c > 0 : \left|\mathcal{O}(l\sqrt{p})\right| \leq c \cdot (l\sqrt{p})$.

Důkaz. Důkaz tvrzení využívá modulární křivky a pojmy s nimi spojené, důkaz je mimo možnosti práce. Více informací lze nalézt v Lenstra Jr (1987, kapitola (1.10)).

❑

Tvrzení 18 (Konstanta c_6)**.** *Existuje efektivně spočitatelná konstanta* $c_6 > 0$ *taková, že pro každou dvojici prvočísel* p, l, *kde* $p > 3, p \neq l$ *platí*

$$\#'\{\mathrm{E} : \mathrm{E} \textit{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) \not\equiv 0 \bmod l\}/\cong_{\mathbf{F}_p} \geq \; c_6 \cdot p.$$

Důkaz. Z Tvrzení 17 a Definice 7 dostáváme, že levá strana je rovna

$$\begin{aligned} p - \frac{1}{l-1}p + \mathcal{O}(l\sqrt{p}) &= \frac{(l-2)}{(l-1)}p + \mathcal{O}(l\sqrt{p}) \qquad \text{pokud } p \not\equiv 0, 1 \bmod l, \\ p - \frac{l}{l^2-1}p + \mathcal{O}(l\sqrt{p}) &= \frac{(l^2-l-1)}{(l^2-1)}p + \mathcal{O}(l\sqrt{p}) \qquad \text{pokud } p \equiv 1 \bmod l. \end{aligned}$$

V prvním případě je $l \geq 3$ a v druhém případě $l \geq 2$, tedy koeficient u p je alespoň $1/3$, tedy pokud $l \leq c_7\sqrt{p}$ pro vhodnou konstantu $c_7 > 0$, poté tvrzení platí.
Aplikací Tvrzení 15 (a) na množinu $\mathcal{S} = \{s \in \mathbb{Z} : |s - (p+1)| \leq 2\sqrt{p}, s \equiv 0 \bmod l\}$, která má mohutnost $\mathcal{O}(1 + \sqrt{p} \cdot l^{-1})$ (velikost intervalu $(-2\sqrt{p} + p + 1, 2\sqrt{p} + p + 1)$ je $4\sqrt{p}$, tedy hodnot $s \equiv 0 \bmod l$ je v tomto intervalu $\lfloor 4\sqrt{p}/l \rfloor$ a zároveň 0 vždy splňuje požadovanou kongruenci), dostáváme

$$\#'\{\mathrm{E} : \mathrm{E} \text{ eliptická křivka nad } \mathbf{F}_p, \#\mathrm{E}(\mathbf{F}_p) \not\equiv 0 \bmod l\}/\cong_{\mathbf{F}_p}$$

$$\geq p - c_4 \cdot \mathcal{O}(1 + \sqrt{p} \cdot l^{-1}) \cdot \sqrt{p} \cdot (\log p) \cdot (\log\log p)^2.$$

Tedy získáváme platnost Tvrzení, pokud $p \geq c_8$ a $l \geq c_9 \cdot (\log p) \cdot (\log \log p)^2$ pro vhodné konstanty $c_8, c_9 > 0$.
Ve zbylých případech máme $p < c_8$ nebo $c_9 \cdot (\log p) \cdot (\log \log p)^2 > c_7\sqrt{p}$, tedy p je omezené. Pro pevné p Tvrzení také platí, protože díky 1.6 a pomocí Kroneckerových tříd čísel máme eliptické křivky E_1, E_2 nad tělesem $\mathbf{F}_p$ takové, že

$$\#\mathrm{E}_1(\mathbf{F}_p) = p, \#\mathrm{E}_2(\mathbf{F}_p) = p + 1,$$

a zároveň l nedělí alespoň jeden z prvků $p, p + 1$

❑

Tvrzení 19 (Konstanta c_{10})**.** *Existuje efektivně spočitatelná konstanta $c_{10} > 0$ taková, že pro každé prvočíslo $p > 3$ platí:*
(a) Nechť $\mathcal{S}$ je množina čísel taková, že $\forall s \in \mathcal{S}$ platí: $|s - (p + 1)| \leq \sqrt{p}$, pak počet trojic $(a, x, y) \in \mathbf{F}_p^3$, pro které

$$4a^3 + 27b^2 \neq 0, \#\mathrm{E}_{a,b}(\mathbf{F}_p) \in \mathcal{S},$$

kde $b = y^2 - x^3 - ax$, je alespoň $c_{10}(\#\mathcal{S} - 2) \cdot p^{5/2}/\log p$.
(b) Nechť $l \neq p$ je libovolné prvočíslo, pak počet trojic $(a, x, y) \in \mathbf{F}_p^3$, pro které

$$4a^3 + 27b^2 \neq 0, \#\mathrm{E}_{a,b}(\mathbf{F}_p) \not\equiv 0 \bmod l,$$

kde $b = y^2 - x^3 - ax$, je alespoň $c_{10} \cdot p^3$.

Důkaz. (a) Počet trojic $(\mathbf{F}_p)$, který chceme odhadnout, je rovný počtu čtveřic $(a, b, x, y) \in \mathbf{F}_p^4$, pro které $\mathrm{E}_{a,b}$ je eliptická křivka nad $\mathbf{F}_p$, $(x : y : 1) \in \mathrm{E}_{a,b}(\mathbf{F}_p)$ a $\#\mathrm{E}_{a,b}(\mathbf{F}_p) \in \mathcal{S}$.
Každá eliptická křivka E nad $\mathbf{F}_p$ je izomorfní $\mathrm{E}_{a,b}$ právě pro $(p - 1)/\#\mathrm{AutE}$ dvojic $(a, b) \in \mathbf{F}_p^2$ (viz úvaha po Definici 6) a každá $\mathrm{E}_{a,b}$ dává základ právě pro $\#\mathrm{E}_{a,b}(\mathbf{F}_p) - 1$ bodů $(x : y : 1)$. Z toho získáváme, že počet trojic $(\mathbf{F}_p)$, který chceme odhadnout, je roven

$$\sum \frac{(p-1)(\#\mathrm{E}(\mathbf{F}_p) - 1)}{\#\mathrm{AutE}},$$

suma prochází až na izomorfismus přes všechny eliptické křivky E nad $\mathbf{F}_p$, pro které $\#\mathrm{E}(\mathbf{F}_p) \in \mathcal{S}$. Použitím Hasseho Věty 10 a Tvrzení 15 (b) dostáváme, že

$$\sum \frac{(p-1)(\#\mathrm{E}(\mathbf{F}_p) - 1)}{\#\mathrm{AutE}} \geq (p-1) \cdot (p - 2\sqrt{p}) \cdot c_5 \cdot (\#\mathcal{S} - 2) \cdot \sqrt{p}/(\log p)$$

(b) Důkaz se provede obdobně jako v (a), jen se nahradí použití Tvrzení 15 (b) za Tvrzení 18 Dostáváme tedy

$$\sum \frac{(p-1)(\#\mathrm{E}(\mathbf{F}_p) - 1)}{\#\mathrm{AutE}} \geq (p-1) \cdot (p - 2\sqrt{p}) \cdot c_6 \cdot p$$

❑

1.3 Faktorizační algoritmus na principu eliptických křivek

Zásadní význam eliptických křivek pro faktorizaci je fakt, že pokud máme složené číslo n, které chceme faktorizovat, můžeme zkusit pracovat na eliptické křivce E nad $\mathbb{Z}/n\mathbb{Z}$, přestože nebudeme mít definovaný grupový zákon Abelovské grupy vždy. Pokud bychom takovouto „nelegální“ operaci prováděli, pak bychom toho využili a nalezli bychom dělitele n. Tato myšlenka je základem pro faktorizační metodu ECM.

Definice 12 (Netriviální dělitel)**.** *Nechť $d, n \in \mathbb{N}, d|n$, řekneme, že d je netriviální dělitel n, pokud $1 < d < n$*

Definice 13 (Projektivní rovina nad $\mathbb{Z}/n\mathbb{Z}$)**.** *Projektivní rovinu nad $\mathbb{Z}/n\mathbb{Z}$ definujeme následovně: Nechť $\mathcal{M} = \{(x, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3 : NSD(x, y, z, n) = 1\}$. Nechť $\mathcal{R}$ je relace na $\mathcal{M}$ definovaná násobením invertibilním prvkem z $\mathbb{Z}/n\mathbb{Z}$. Poté $\mathcal{R}$ je ekvivalence a projektivní rovinu $\mathbf{P}^2(\mathbb{Z}/n\mathbb{Z})$ definujeme jako*

$$\mathbf{P}^2(\mathbb{Z}/n\mathbb{Z}) = \mathcal{M}/\mathcal{R},$$

tedy jako množinu tříd ekvivalence množiny $\mathcal{M}$ podle relace $\mathcal{R}$. Více viz (Cohen (1993, Kapitola 7))

Značení 3. *Třídu ekvivalence bodů (x, y, z) v $\mathbf{P}^2(\mathbb{Z}/n\mathbb{Z})$ budeme značit $(x : y : z)$.*

Definice 14 ($\mathrm{E}(\mathbb{Z}/n\mathbb{Z})$)**.** *Nechť $a, b \in \mathbb{Z}/n\mathbb{Z}$. Symbolem $\mathrm{E} = \mathrm{E}_{a,b}$ definujeme množinu bodů*

$$\begin{aligned}\mathrm{E}(\mathbb{Z}/n\mathbb{Z}) = \{&(x : y : z) \in \mathbf{P}^2(\mathbb{Z}/n\mathbb{Z}) : NSD(x, y, z, n) = 1,\\ &y^2z \equiv x^3 + axz^2 + bz^3 (\mathrm{mod} p) \text{ pro každé prvočíslo } p|n\}.\end{aligned}$$

Nejvhodnější cesta k formulaci faktorizačního algoritmu by byla využít právě formulovanou množinu s grupovou strukturu. Ve skutečnosti však potřebujeme tuto strukturu jen v případě, že n je prvočíslo. Pro naše účely budeme pracovat s číslem n a částečně definovanou grupovou strukturou na podmnožině $\mathrm{E}(\mathbb{Z}/n\mathbb{Z})$.

Značení 4 (Množina V_n)**.** *Označme bod $(0 : 1 : 0) \in \mathbf{P}^2(\mathbb{Z}/n\mathbb{Z})$ jako O a označme podmnožinu $V_n \in \mathbf{P}^2(\mathbb{Z}/n\mathbb{Z})$ jako*

$$V_n = \{(x : y : 1) : x, y \in (\mathbb{Z}/n\mathbb{Z})\} \cup \{O\}. \tag{1.7}$$

Pro $P \in V_n$ a pro prvočíslo $p|n$ označme $P_p \in \mathbf{P}^2(\mathbf{F}_p)$ získaný z P upravením souřadnic modulo p.

1.3.1 Sčítací algoritmus

Popíšeme sčítací algoritmus, který pro dané $n \in \mathbb{Z}, n > 1, a \in \mathbb{Z}/n\mathbb{Z}$ a $P, Q \in V_n$ buď spočte netriviálního dělitele d čísla n nebo vrátí bod $R \in V_n$ s následujícími vlastnostmi:

Nechť p je prvočíslo, $p|n$, pro které existuje $b \in \mathbf{F}_p$ takové, že

$$\begin{aligned}&6(4\bar{a}^3 + 27b^2) \neq 0 && \text{pro } \bar{a} = (a \bmod p)\\ &P_p, Q_p \in \mathrm{E}_{\bar{a},b}(\mathbf{F}_p) && \text{poté } P_p + Q_p = R_p \text{ v grupě } \mathrm{E}_{\bar{a},b}(\mathbf{F}_p).\end{aligned}$$

1. Pokud $P = O$ polož $R = Q$ a zastav krok.

2. Pokud $P \neq O, Q = O$ položme $R = P$ a zastav krok.

3. Ve zbývajících případech $P \neq O, Q \neq O$.
   Nechť $P = (x_1 : y_1 : 1), Q = (x_2 : y_2 : 1)$. Použij Eukleidův algoritmus na spočítání $NSD(x_1 - x_2, n)$.

   - Pokud $NSD(x_1 - x_2, n)$ je netriviální (různé od $1, n$), pak polož $d = NSD(x_1 - x_2, n)$ a zastav krok.
   - V případě, že $NSD(x_1 - x_2, n) = 1$, nám Eukleidův algoritmus také vrátí $(x_1 - x_2)^{-1}$. V tomto případě polož

     $$\begin{aligned} \lambda &= (y_1 - y_2) \cdot (x_1 - x_2)^{-1}, \\ x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ R &= (x_3 : y_3 : 1) \end{aligned}$$

     a zastav krok.
   - Pokud $NSD(x_1 - x_2, n) = n$ pak $x_1 = x_2$. Spočti $NSD(y_1 + y_2, n)$.
     - Pokud $NSD(y_1 + y_2, n)$ je netriviální (různé od $1, n$), pak polož $d = NSD(y_1 + y_2, n)$ a zastav krok.
     - V případě, že $NSD(y_1 + y_2, n) = 1$, nám Eukleidův algoritmus také vrátí $(y_1 + y_2)^{-1}$. V tomto případě polož

       $$\begin{aligned} \lambda &= (3x_1^2 + a) \cdot (y_1 + y_2)^{-1}, \\ x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda(x_1 - x_3) - y_1, \\ R &= (x_3 : y_3 : 1) \end{aligned}$$

       a zastav krok.
     - Pokud $NSD(y_1 + y_2, n) = n$, pak $y_1 = -y_2$ a polož $R = O$ a zastav krok.

Pokud algoritmus vrátí bod R, nazveme ho bodem $P + Q$ a částečná binární operace na V_n se bude nazývat sčítáním. Pokud zde existuje $b \in \mathbb{Z}/n\mathbb{Z}$ takové, že

$$6(4a^3 + 27b^2) \in (\mathbb{Z}/n\mathbb{Z})^*$$

$P, Q \in \mathrm{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$, tedy pokud výraz $P + Q$ je definován, pak platí $P + Q \in \mathrm{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$.

Více algoritmický zápis poskytnu v části Implementace 2 v Algoritmech 3 a 4, ty jsou však již připraveny pro specifickou implementaci a tedy nejsou tak obecné.

1.3.2 Násobící algoritmus

Opakovaným sčítáním získáme algoritmus, který pro zadané $k, n \in \mathbb{Z}, k > 0, n > 1, a \in \mathbb{Z}/n\mathbb{Z}, P \in V_n$, buď spočte netriviálního dělitele d čísla n nebo vrátí bod $R \in V_n$ s následujícími vlastnostmi:

Nechť p je prvočíslo, $p|n$, pro které existuje $b \in \mathbf{F}_p$ takové, že

$$\begin{aligned} 6(4\bar{a}^3 + 27b^2) &\neq 0 \qquad \text{pro } \bar{a} = (a \bmod p) \\ P_p &\in \mathrm{E}_{\bar{a},b}(\mathbf{F}_p) \qquad \text{poté } k \cdot P_p = R_p \text{ v grupě } \mathrm{E}_{\bar{a},b}(\mathbf{F}_p). \end{aligned}$$

Pokud algoritmus vrátí bod R, nazveme ho bodem $k \cdot P$ a takto definovaná částečná operace se bude nazývat násobením. Počet sčítání, které algoritmus provede, záleží na „sčítacím řetězci“, který se použije. Například v případě použití „sčítacího řetězce“ vzniklého z binární reprezentace k je počet sčítání roven $O(\log_2(k))$. To, zda $k \cdot P$ je definováno nebo ne, záleží na použitém „sčítacím řetězci“ (v případě, že n je složené číslo). Pokud dostaneme k zadáno, jako $k = k_1 \cdot k_2$ pro $k_1, k_2 \in \mathbb{N}$, můžeme $k \cdot P$ spočítat jako $k \cdot P = k_1 \cdot (k_2 \cdot P)$. Předpokládejme nyní že

$$k = \prod r^{e(r)}$$

kde r prochází přes danou konečnou množinu celých, kladných čísel a každý prvek $e(r) \in \mathbb{N}$. Opakovanou aplikací předešlého můžeme přijít na to, že k vynásobení k a P stačí pro každé r provést $e(r)$ násobení číslem r. V následujícím textu budeme předpokládat, že násobení r se vykonává ve vzestupném pořadí podle r.

Pozorování. *Pro $k = \#\mathrm{E}(\mathbf{F}_p)$ a bod $P \in V_n$ takový že $P \in \mathrm{E}(\mathbf{F}_p)$, pak platí $k \cdot P_p = O_p$.*

Značení 5 (Množina prvočísel)**.** *Symbolem $\mathbb{P}$ rozumíme množinu všech prvočísel.*

1.3.3 Faktorizační algoritmus s použitím jedné křivky

Nechť $n, v, w > 1, n, v, w \in \mathbb{N}$, $a, x, y \in \mathbb{Z}/n\mathbb{Z}$ a nechť $P = (x : y : 1) \in V_n$. Pro každé prvočíslo $r \geq 2$ označme $e(r)$ největšího číslo m takové, že $r^m \leq v + 2\sqrt{v} + 1$ a položme

$$k = \prod_{r=2, r \in \mathbb{P}}^{w} r^{e(r)}$$

Nyní můžeme popsat algoritmus, který se pokouší najít netriviálního dělitele d čísla n.

Algoritmus 1 (Faktorizace s použitím jedné křivky)**.** *Faktorizace jednou křivkou.*

- *Pokus se spočítat $k \cdot P$.*
- *Algoritmus selhal - našli jsme netriviálního dělitele čísla $n \Longrightarrow$ vrať d - tohoto dělitele.*
- *Algoritmus úspěšně spočetl $k \cdot P \Longrightarrow$ vrať zprávu, že selhalo hledání netriviálního dělitele čísla n.*

Poznámka 20. *Je dobré si uvědomit, co které prvky použité v Algoritmu 1 znamenají:*

- *Volba a, x, y určuje eliptickou křivku, která se používá.*

- *Číslo v je horní mez pro dělitele d čísla n, kterého se snažíme najít, ale není žádná jistota, že skutečně $d \leq v$.*
- *Parametr w v podstatě měří čas, po který algoritmus běží.*
- *Pravděpodobnost úspěchu roste s rostoucím w.*

1.3.4 Faktorizační algoritmus s použitím více křivek

Nechť $n, v, w, h > 1, n, v, w, h \in \mathbb{N}$. Nyní popíšeme pravděpodobnostní algoritmus, který se pokouší najít netriviálního dělitele d čísla n.

Algoritmus 2 (Faktorizace s použitím více křivek)**.** *Faktorizace více křivkami.*

- *Pokud počet volání Algoritmu 1 je větší než $h \Longrightarrow$ vrať zprávu, že selhalo hledání netriviálního dělitele čísla n.*
- *Zvol náhodně tři prvky $a, x, y \in \mathbb{Z}/n\mathbb{Z}$.*
- *Aplikuj Algoritmus 1 na n, v, w, a, x, y.*
- *Pokud je výsledkem Algoritmu 1 netriviální dělitel čísla $n \Longrightarrow$ vrať d - tohoto dělitele.*
- *Jinak jdi zpět na první krok.*

Poznámka 21. *Je dobré si opět uvědomit, co které prvky použité v Algoritmu 2 znamenají:*

- *Číslo v opět je horní mez pro dělitele d čísla n, kterého se snažíme najít, ale stále není žádná jistota, že skutečně $d \leq v$.*
- *Parametr w v podstatě měří čas, po který algoritmus běží pro jednu křivku.*
- *Parametr h značí počet křivek, který se maximálně použije pro hledání dělitele čísla n. (Níže uvedu pravděpodobnost úspěchu algoritmu v závislosti na w a h a jejich optimální volbu)*

Věta 22 (Úspěšnost Algoritmu 1)**.** *Nechť $n, v, w > 1, n, v, w \in \mathbb{N}$ a $a, x, y \in \mathbb{Z}/n\mathbb{Z}$ jako z (1). Nechť $b = y^2 - x^3 - ax \in \mathbb{Z}/n\mathbb{Z}$ (viz 1.2) a $P = (x : y : 1) \in V_n$. Uvažujme, že n má prvočíselného dělitele p a q splňuje následující podmínky*
(i) $p \leq v$,
(ii) $6(4\bar{a}^3 + 27\bar{b}^2) \neq 0$ pro $\bar{a} = (a \bmod p), \bar{b} = (b \bmod p)$,
(iii) každé prvočíslo $r | \#\mathrm{E}_{\bar{a},\bar{b}}(\mathbf{F}_p)$ platí $r \leq w$,
(iv) $6(4\hat{a}^3 + 27\hat{b}^2) \neq 0$ pro $\hat{a} = (a \bmod q), \hat{b} = (b \bmod q)$,
(v) $\#\mathrm{E}_{\hat{a},\hat{b}}(\mathbf{F}_q)$ není dělitelné největším prvočíslem dělícím řád P_p,
Pak Algoritmus 1 je úspěšný v hledání netriviálního dělitele n.

Důkaz. Z $p \leq v$ a Věty 10 plyne

$$\#\mathrm{E}_{\bar{a},\bar{b}}(\mathbf{F}_p) \leq v + 2\sqrt{v} + 1,$$

to znamená, že pro každé prvočíslo r je exponent čísla r v $\#\mathrm{E}_{\bar{a},\bar{b}}(\mathbf{F}_p)$ nejvýše $e(r)$ definovaný v Algoritmu 1. To samé platí pro exponent r v řádu o bodu P_p.

Označme l největší prvočíslo dělící o a označme m exponent l v o. Tedy máme $1 \leq m \leq e(l)$. Položme

$$k_0 = (\prod_{r=2, r\in\mathbb{P}}^{l-1} r^{e(r)}) \cdot l^{m-1}$$

poté $k_0 \not\equiv 0 \bmod o$ a $k_0 l \equiv 0 \bmod o$, tedy

$$k_0 P_p \neq O_p, k_0 l P_p = O_p \text{ v grupě } \mathrm{E}_{\bar{a},\bar{b}}(\mathbf{F}_p).$$

Z (iii) máme $l \leq w$, tedy k_0 a $k_0 l$ jsou dělitele čísla k z Algoritmu 1. Navíc, pokud kP je algoritmem úspěšně spočteno, poté $k_0 P$ a $k_0 l P$ jsou spočteny v průběhu algoritmu. Z toho již plyne, že k dokázání věty stačí ukázat, že $k_0 P$ a $k_0 l P$ nemohou být definovány současně. K dokázání toho, že nemohou být definovány současně, využijeme toho, že pokud $Q_p = O_p$ pak $Q = O$. Tedy pokud existuje $k_0 l P \in V_n$, poté $(k_0 l P)_p = k_0 l \cdot P_p = O_p$ v grupě $\mathrm{E}_{\bar{a},\bar{b}}(\mathbf{F}_p)$ a proto $k_0 l P = O \in V_n$, ale poté $k_0 l \cdot P_q = (k_0 l P)_q = O_q$ v grupě $\mathrm{E}_{\hat{a},\hat{b}}(\mathbf{F}_q)$. Tedy podle (v) máme $k_0 P_q = O_q$. Proto, když $k_0 P \in V_n$ je také definováno, musíme mít $k_0 P = O$ z toho plyne, že $k_0 P_p = O_p$, čímž jsme došli ke sporu.

❑

Tvrzení 23 (Konstanta c_{11})**.** *Existuje efektivně spočitatelná konstanta $c_{11} > 0$ s následujícími vlastnostmi: Nechť $n, v, w, h > 1, n, v, w, h \in \mathbb{N}$ takové, že n má alespoň dva různé prvočíselné dělitele. Zároveň prvočíselní dělitelé n jsou větší než 3. Dále nechť nejmenší prvočíselný dělitel p čísla n, splňuje $p \leq v$. Položme*

$$u = \#\{s \in \mathbb{Z} : |s - (p+1)| < \sqrt{p} \text{ a každé prvočíslo } q | s \text{ splňuje } q \leq w\}.$$

Poté N počet trojic $(a, x, y) \in (\mathbb{Z}/n\mathbb{Z})^3$, pro které Algoritmus 1 uspěje v hledání netriviálního dělitele čísla n splňuje

$$\frac{N}{n^3} > \frac{c_{11}}{\log p} \cdot \frac{u-2}{2\lfloor\sqrt{p}\rfloor + 1}.$$

Důkaz. Nechť $q > 3$ je prvočíselný dělitel čísla n, $q \neq p$. Pro každé $s \in \mathbb{N}$ označme T_s množinu trojic $(\alpha, \xi, \upsilon) \in \mathbf{F}_p^3$ splňující:

$$4\alpha^3 + 27\beta^2 \neq 0, \qquad \#\mathrm{E}_{\alpha,\beta}(\mathbf{F}_p) = s,$$

kde $\beta = \upsilon^2 - \xi^3 - \alpha\xi$. Pro $(\alpha, \xi, \upsilon) \in T_s$, $l_{\alpha\xi\upsilon}$ označme největšího prvočíselného dělitele řádu bodu $(\xi : \upsilon : 1)$ v grupě $\mathrm{E}_{\alpha,\beta}(\mathbf{F}_p)$ a $U_{\alpha\xi\upsilon}$ označme množinu trojic $(\alpha', \xi', \upsilon') \in \mathbf{F}_q^3$, pro které

$$4\alpha'^3 + 27\beta'^2 \neq 0, \qquad \#\mathrm{E}_{\alpha',\beta'}(\mathbf{F}_q) \text{ není dělitelné } l_{\alpha\xi\upsilon},$$

kde $\beta' = \upsilon'^2 - \xi'^3 - \alpha'\xi'$. Poté takto označené prvky s použitím Věty 22 dávají:

$$N \geq \sum_s \sum_{(\alpha,\xi,\upsilon)\in T_s} \sum_{(\alpha',\xi',\upsilon')\in U_{\alpha\xi\upsilon}} \#V_{\alpha\xi\upsilon\alpha'\xi'\upsilon'},$$

kde s prochází přes množinu kladných čísel takových, že s má všechny prvočíselné dělitele $\leq w$ a

$$V_{\alpha\xi\upsilon\alpha'\xi'\upsilon'} = \{(a,x,y) \in (\mathbb{Z}/n\mathbb{Z})^3 : \quad (a \bmod p, x \bmod p, y \bmod p) = (\alpha,\xi,\upsilon), \\ (a \bmod q, x \bmod q, y \bmod q) = (\alpha',\xi',\upsilon')\}.$$

Tedy dostáváme, že každá množina $V_{\alpha\xi\upsilon\alpha'\xi'\upsilon'}$ má mohutnost $n^3/(pq)^3$. Aplikací Tvrzení 19 (b) dostáváme $\#U_{\alpha\xi\upsilon} \geq c_{10}q^3$. Z toho plyne

$$\frac{N}{n^3} \geq c_{10} \sum_s \frac{\#T_s}{p^3},$$

kde s prochází přes množinu kladných čísel takových, že s má všechny prvočíselné dělitele $\leq w$. Restrikcí sumy na čísla s, která splňují $|s-(p+1)| \leq \sqrt{p}$ a aplikací Tvrzení 19 (a) dostáváme

$$\frac{N}{n^3} \geq \frac{c_{10}^2 \cdot (u-2)}{\sqrt{p} \cdot \log p} > \frac{2 \cdot c_{10}^2 \cdot (u-2)}{(2\lfloor\sqrt{p}\rfloor+1) \cdot \log p}.$$

❑

Nyní uvažujme, že náhodný generátor, používaný v Algoritmu 2 pro generování $(a,x,y) \in (\mathbb{Z}/n\mathbb{Z})^3$, generuje každou trojici se stejnou pravděpodobností a že všechna volání náhodného generátoru jsou nezávislá

Věta 24 (Konstanta c_{12})**.** *Existuje efektivně spočitatelná konstanta $c_{12} > 1$ s následujícími vlastnostmi: Nechť $n, v > 1, n, v \in \mathbb{N}$ takové, že n má alespoň dva různé prvočíselné dělitele. Zároveň prvočíselní dělitelé čísla n jsou větší než 3. Dále nechť nejmenší prvočíselný dělitel p čísla n splňuje $p \leq v$. Nechť dále $w > 1, w \in \mathbb{N}$ je takové, že číslo u definované jako*

$$u = \#\{s \in \mathbb{Z} : |s-(p+1)| < \sqrt{p} \text{ a každé prvočíslo } q|s \text{ splňuje } q \leq w\}$$

splňuje $u \geq 3$ a nechť $f(w) = \frac{u}{2\lfloor\sqrt{p}\rfloor+1}$ značí pravděpodobnost, že náhodné číslo z intervalu $(p+1-\sqrt{p}, p+1+\sqrt{p})$ má všechny prvočíselné dělitele $d \leq w$. Pak pro libovolné $h > 1, h \in \mathbb{N}$ je pravděpodobnost úspěchu Algoritmu 2 na vstup n, v, w, h alespoň $1 - c_{12}^{-h \cdot f(w)/\log v}$.

Důkaz. Podle Tvrzení 23 a předpokladů uvedených před tímto Tvrzením máme, že pravděpodobnost neúspěchu Algoritmu 2 se rovná $(1-N/n^3)^h$, kde

$$\frac{N}{n^3} > \frac{c_{11}}{\log p} \cdot \frac{u-2}{2\lfloor\sqrt{p}\rfloor+1} \geq \frac{c_{11} \cdot f(w)}{3 \log v}.$$

Z rozvoje Taylorova polynomu pro $\log(1+y) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{y^i}{i}$, kde $y \in (-1,1\rangle$ použitého na $y = -\frac{N}{n^3}$ dostáváme:

$$\log\left(1 - \frac{N}{n^3}\right) < -\frac{N}{n^3} \leq -\frac{c_{11} \cdot f(w)}{3 \log v}$$

Tedy

$$\log\left(1-\frac{N}{n^3}\right) \leq -\frac{c_{11}\cdot f(w)}{3\log v}$$

Tedy po úpravě dostáváme

$$\left(1-\frac{N}{n^3}\right)^h \leq e^{-h\cdot c_{11}\cdot f(w)/3\log v} = (e^{c_{11}/3})^{-h\cdot f(w)/\log v}$$

❑

1.3.5 Efektivita algoritmu

Dostáváme se k fázi, kdy můžeme rozebrat složitost algoritmu pro faktorizaci celého čísla za použití eliptických křivek. Označme $M(n)$ horní mez pro čas, měřený v bitových operacích, který je potřeba k provedení jednoho sčítání v kapitole 1.3.1. Existuje několik možností, čemu se může rovnat $M(n)$, kde Eukleidův algoritmus je prováděn na čísla ze $\mathbb{Z}/n\mathbb{Z}$ délky $\log n$. Pokud použijeme obyčejný Eukleidův algoritmus, pak $M(n) = O((\log n)^2)$, také však lze použít modifikovanou verzi, která vede k $M(n) = O((\log n)(\log\log n)^2(\log\log\log n))$. Pro více informací ohledně složitosti Eukleidova algoritmu doporučuji Knuth (1997, Kapitola 4.5.2) a Stehlé a Zimmermann (2004).

Dále pro k z Algoritmu 1 zřejmě platí, že $\log k = O(w\log v)$. S notací $M(n)$ pro horní mez pro čas potřebný pro provedení jednoho sčítání dostáváme, že čas potřebný Algoritmem 1 je $O(w(\log v)M(n))$.

Čas potřebný pro Algoritmus 2 je nejvýše h krát větší, kde h je jako v Algoritmu 2. Tedy čas potřebný pro Algoritmus 2 je $O(hw(\log v)M(n))$. Věta 24 ukazuje, že abychom měli rozumnou šanci uspět při hledání netriviálního dělitele čísla n, je potřeba zvolit číslo h stejného řádu jako $(\log v)/f(w)$. Z toho vyplývá, že pro minimalizaci času potřebného pro Algoritmus 2 je potřeba zvolit číslo w tak, aby $w/f(w)$ bylo minimální. V tento okamžik potřebujeme vyjít z odhadu Ψ, jemuž se věnuje Canfield a kol. (1983). Pro pochopení uvedu definici Ψ a následně používaný odhad Canfield a kol. (1983, Corollary to Theorem 3.1).

Definice 15 (De Bruijnova funkce Ψ)**.** *Nechť $y, z \in \mathbb{N}, y \leq z$. De Bruijnovu funkci Ψ definujme jako:*

$$\Psi(z,y) = \#\{n \in \mathbb{N} : 1 \leq n \leq z, \textit{pro každé prvočíslo } p, p|n : p \leq y\}. \tag{1.8}$$

Poté $\Psi(z,y)$ značí počet čísel $n \leq z$ takových, že jejich prvočíselné dělitele nepřevyšují y.

Věta 25 (Vyjádření Ψ (Viz Canfield a kol. (1983) Corollary to Theorem 3.1))**.** *Nechť $1 > \epsilon > 0$ je libovolné a u splňuje $3 \leq u \leq \frac{(1-\epsilon)\log z}{\log\log z}$, pak*

$$\Psi(z,z^{1/u}) = z\cdot\exp\{-u\cdot(\log u + \log\log u + o(1))\}. \tag{1.9}$$

Důkaz. Horní odhad funkce Ψ vychází z De Bruijn (1966, sekce 2) a dolní odhad vychází z Canfield a kol. (1983, Theorem 3.1). Důkazy jednotlivých nerovností

jsou mimo možnosti práce a jejich platnosti se věnují autoři v De Bruijn (1966, sekce 2) a v Canfield a kol. (1983, Theorem 3.1).
Více informací v Canfield a kol. (1983, Corollary to Theorem 3.1).

❑

Chování funkce Ψ se věnuje autor i v Hildebrand (1986).
Mějme nyní číslo $x > e$ definujme

$$L(x) = \exp\{\sqrt{\log x \cdot \log\log x}\}.$$

Dále mějme $\alpha \in \mathbb{R}, \alpha > 0$. Chtěli bychom aplikovat Větu 25 pro $z = x, x^{1/u} = L(x)^{\alpha}$. Nejprve si potřebujeme vyjádřit u. Lze snadno nahlédnout, že

$$u = \frac{\log(x)}{\alpha \cdot \sqrt{\log x \cdot \log\log x}}. \tag{1.10}$$

Nyní si označme $EXP = -u \cdot (\log u + \log\log u + o(1))$ exponent funkce exp z 1.9. Dale potřebujeme určit hodnoty $\log u$ a $\log\log u$ po dosazení 1.10:

$$\begin{aligned}\log u = \log\left(\frac{\log(x)}{\alpha \cdot \sqrt{\log x \cdot \log\log x}}\right) &= \log\log x - \log\alpha - 1/2\log(\log x \cdot \log\log x) \\ &= 1/2\log\log x - \log\alpha - 1/2\log\log\log x\end{aligned}$$

Z výše určeného $\log u$ máme:

$$\begin{aligned}\log\log u &= \log(1/2\log\log x - \log\alpha - 1/2\log\log\log x) \\ &= \log(1/2\log\log x \cdot (1 - \frac{\log\log\log x}{\log\log x} - \frac{2\log\alpha}{\log\log x})) \\ &= \log(1/2\log\log x \cdot (1 - o(1))) = \log 1/2 + \log\log\log x + \log(1 - o(1))\end{aligned}$$

Celkem tedy dostáváme:

$$\begin{aligned}EXP = &- \frac{\log(x)}{\alpha \cdot \sqrt{\log x \cdot \log\log x}} \cdot \Big(1/2\log\log x - \log\alpha - 1/2\log\log\log x \\ &+ \log 1/2 + \log\log\log x + \log(1 - o(1)) + o(1)\Big) \\ = &- \frac{\log(x)}{\alpha \cdot \sqrt{\log x \cdot \log\log x}} \cdot \Big(1/2\log\log x + 1/2\log\log\log x + c + o(1)\Big)\end{aligned}$$

pro $c = -\log\alpha + \log 1/2 + \log(1 - o(1))$.
Tedy po roznásobení a vytknutí $-\frac{\sqrt{\log x \cdot \log\log x}}{2\alpha}$ máme:

$$\begin{aligned}EXP &= -\frac{\sqrt{\log x \cdot \log\log x}}{2\alpha} \cdot \left(1 + \frac{\log\log\log x}{\log\log x} + \frac{2 \cdot (c + o(1))}{\log\log x}\right) \\ &= \sqrt{\log x \cdot \log\log x} \cdot \left(\frac{-1}{2\alpha} + o(1)\right)\end{aligned}$$

Nyní tedy aplikací Věty 25 pro $z = x, x^{1/u} = L(x)^{\alpha}$ dostáváme:

$$\Psi(x, L(x)^{\alpha}) = x \cdot \exp\{\sqrt{\log x \cdot \log\log x} \cdot \left(\frac{-1}{2\alpha} + o(1)\right)\} = x \cdot L(x)^{(\frac{-1}{2\alpha} + o(1))}.$$

Z toho dostáváme: Nechť $x > e, \alpha \in \mathbb{R}, \alpha > 0$, poté pravděpodobnost, že náhodné číslo $s \leq x$ má všechny prvočíselné dělitele $p \leq L(x)^\alpha$, je rovna

$$L(x)^{(\frac{-1}{2\alpha}+o(1))}, \qquad \text{pro } x \to \infty.$$

Pro naše účely však potřebujeme, aby stejný výsledek platil i pro náhodné číslo $s \in (x+1-\sqrt{x}, x+1+\sqrt{x})$. Předpokládejme tedy, že tato hypotéza platí. Poté položíme-li $x = p$ dostaneme

$$f(L(p)^\alpha) = L(p)^{(\frac{-1}{2\alpha}+o(1))}, \qquad \text{pro } p \to \infty$$

pro pevné α a f jako ve Větě 24.

Položme $w = L(p)^\alpha$, naše hypotéza nám dává

$$w/f(w) = L(p)^{(\frac{1}{2\alpha}+\alpha+o(1))}, \qquad \text{pro } p \to \infty.$$

Derivací funkce $g(\alpha) = L(p)^{(\frac{1}{2\alpha}+\alpha+o(1))}$ podle α zjistíme, že má minimum pro $\alpha = \sqrt{2}$. Z toho získáváme optimální volbu pro $w, w/f(w)$:

$$w = L(p)^{1/\sqrt{2}+o(1)}, \qquad w/f(w) = L(p)^{\sqrt{2}+o(1)}, \qquad \text{pro } p \to \infty.$$

Ověření platnosti této hypotézy - ověření optimálnosti volby α pro rostoucí p a ověření pravděpodobnosti viz příloha - Tabulka 3.1.

Předchozí úvaha vede k následující hypotéze ohledně času běhu algoritmu pro faktorizaci celého čísla pomocí metody eliptických křivek.

Značení 6 (Kladná reálná čísla)**.** *Symbolem $\mathbb{R}^+$ budeme rozumět kladná reálná čísla.*

Hypotéza 1 (Doba běhu Algoritmu 2)**.** *Existuje funkce $K : \mathbb{R}^+ \to \mathbb{R}^+$, pro kterou*

$$K(x) = \exp\{\sqrt{(2+o(1)) \cdot \log x \cdot \log\log x}\} \qquad \textit{pro } x \to \infty,$$

taková, že platí následující: Nechť $n \in \mathbb{N}, n > 1$ je číslo, které není mocninou prvočísla a 2,3 nedělí n. Nechť $g \in \mathbb{N}$. Poté Algoritmus 2 aplikovaný na vhodné hodnoty v, w, h může být použit na nalezení netriviálního dělitele čísla n s pravděpodobností alespoň $1 - e^{-g}$ v čase

$$gK(p)M(n),$$

kde p značí nejmenšího prvočíselného dělitele čísla n a $M(n)$ je definována jako na začátku kapitoly 1.3.5.

Je nutné si uvědomit, že není nijak zaručeno, že dělitel, kterého najde Algoritmus 2 je nejmenším dělitelem čísla n. Dále je nutné zmínit, že Algoritmus 2 najde dělitele, ale neprovede kompletní faktorizaci. Proto, pokud bychom chtěli provést kompletní faktorizaci čísla n, pak by čas běhu algoritmu také obsahoval $gK(p')M(n)$ odpovídající jinému prvočíselnému děliteli p' čísla n, kromě největšího prvočíselného dělitele n. Ve všech případech se dá celkem očekávat čas běhu faktorizačního algoritmu jako $L(n)^{1+o(1)}$ pro $n \to \infty$. K nejhoršímu času běhu algoritmu dojde v případě, že druhý největší prvočíselný dělitel n je velký téměř jako $\sqrt{n}$, tedy, že n je součin malých prvočísel a dvou velkých prvočísel stejného řádu. Možnosti zrychlení algoritmu lze nahlédnout v Montgomery (1987).

2. Implementace faktorizační metody ECM

V následující sekci budu, oproti předchozímu textu, algoritmy uvádět v pseudokódu, jelikož se jedná o algoritmy, které se už dají prakticky implementovat jen s drobnými úpravami v závislosti na daném programovacím jazyku.

V aplikacích na faktorizaci případně při prvočíselném testování nás zajímá zvolení náhodné křivky. Existují dva přístupy jak se k tomuto problému postavit. První je, že zvolíme a, b náhodně a to nám již určí křivku. V jiném případě potřebujeme mimo křivky také získat náhodný bod na této křivce, pokud bychom pracovali se skutečnou eliptickou křivkou nad konečným tělesem, pak body na této křivce můžeme snadno najít (lze nahlédnout pomocí Algoritmu 7.2.1 v Crandall a Pomerance (2005)). Pokud však pracujeme nad $(\mathbb{Z}/n\mathbb{Z})$, kde n je složené, pak druhá odmocnina, která k nalezení náhodného bodu je potřebná (opět viz Algoritmus 7.2.1 v Crandall a Pomerance (2005)), nemůže být použita. Přesto tento problém můžeme kompletně obejít: Zvolme a náhodně a poté určeme bod (x_0, y_0) náhodně, poté zvolme b tak, aby (x_0,y_0) byl na křivce dané 1.2, to znamená, že $b = y_0^2 - x_0^3 - ax_0$.

Při implementaci dochází k dalšímu problému: Pro zadanou množinu bodů na dané eliptické křivce chceme provést sčítání a ještě důležitější je jak provést $k \cdot P$?

Je zde několik možností, jak k tomu přistupovat:

1. Afinní souřadnice: Použít základní grupové operace a přistupovat k problému přímočaře - budeme potřebovat inverzi pro operace na křivce.

2. Projektivní souřadnice: Použít grupové operace, ale pro projektivní souřadnice (x, y, z) - vyhneme se potřebě inverzu. Pro $z \neq 0$ odpovídá (x, y, z) afinnímu bodu $(x/z,y/z)$.

3. Modifikované projektivní souřadnice: Použít trojice (x, y, z), kde pro $z \neq 0$ odpovídá (x, y, z) afinnímu bodu $(x/z^2,y/z^3)$. Tento přístup se také vyhne inverznímu prvku.

Který z těchto přístupu je nejvhodnější závisí na daném případě. Pokud bychom například dokázali rychle provádět hledání inverzního prvku mod$p$, pak bychom zvolili první možnost. Pokud bychom již měli implementovanou první variantu a chtěli bychom ušetřit drahý čas pro provádění (pomalého) hledání inverzního prvku, pak bychom se přesunuli k druhému nebo třetímu přístupu.

Pokud bychom používali druhý přístup, pak bychom uvažovali křivku danou rovností $y^2z = x^3 + axz^2 + bz^3$. Poté pro dva body $P = (x_1, y_1, z_1)$, $Q = (x_2, y_2, z_2)$ takové, že $P, Q \neq O, P \neq \pm Q$ z této křivky platí:

$$R = P + Q = (x_3, y_3, z_3),$$

kde

$$\begin{aligned} x_3 &= \alpha \cdot (\gamma^2 \upsilon - \alpha^2 \beta), \\ y_3 &= \frac{1}{2} \cdot (\gamma(3\alpha^2 \beta - \gamma^2 \upsilon) - \alpha^3 \delta), \\ z_3 &= \alpha^3 \upsilon, \end{aligned}$$

a $\alpha, \beta, \gamma, \delta, \upsilon$ se rovnají

$$\alpha = x_2 z_1 - x_1 z_2, \qquad \beta = x_2 z_1 + x_1 z_2,$$

$$\gamma = y_2 z_1 - y_1 z_2, \qquad \delta = y_2 z_1 + y_1 z_2,$$

$$\upsilon = z_1 z_2.$$

Pokud bychom si pamatovali $\gamma^2 \upsilon, \alpha^2, \alpha^2 \beta, \alpha^3$, pak mohou být souřadnice R spočteny použitím 14 násobení a 8 sčítání (násobení $\frac{1}{2}$ lze vyřešit jako posun, nebo jako součet a posun čísla).

V případě přičítání bodu P k sobě samému dostáváme v případě $2 \cdot P \neq O$:

$$2 \cdot P = 2 \cdot (x_1, y_1, z_1) = (x_1', y_1', z_1'),$$

kde

$$\begin{aligned} x_1' &= \alpha \cdot (\gamma^2 - 2\alpha\beta), \\ y_1' &= \gamma(3\alpha\beta - \gamma^2) - 2y_1^2 \alpha^2, \\ z_1' &= \alpha^3, \end{aligned}$$

a α, β, γ se rovnají

$$\alpha = 2y_1 z_1, \qquad \beta = 2x_1 y_1, \qquad \gamma = 3x_1^2 + a z_1^2.$$

To znamená, že přičítání bodu P k sobě samému jsme schopni provést použitím 13 násobení a 4 sčítání.

V případě třetího přístupu se opět vyhneme hledání inverzního prvku, získáme náročnější sčítání dvou rozdílných bodů, ale získáme snazší přičítání bodu k sobě samému. Lze nahlédnout, že násobení $n \cdot P$ většinou obsahuje téměř dvojnásobně přičítání bodu k sobě samému, než sčítání dvou rozdílných bodů, proto je preferovanější třetí přístup než druhý.

V druhém a třetím přístupu začneme s afinním bodem (u,v), snadno z něj vytvoříme bod $(u, v, 1)$. Pokud naopak na konci dlouhého výpočtu chceme vrátit afinní bod, pak pokud nemáme nulový bod, tj. bod tvaru $(0, 1, 0)$, pak ho upravíme dle $(x/z,y/z)$ respektive $(x/z^2,y/z^3)$ na bod s afinními souřadnicemi.

Následující algoritmy, nám poskytují potřebné operace přímo odvozené z operace + pro běh faktorizačního algoritmu s afinními nebo modifikovanými projektivními souřadnicemi:

Algoritmus 3 (Sčítání: Afinní souřadnice (Viz Crandall a Pomerance (2005) Algoritmus 7.2.2))**.**

Data: Uvažujeme eliptickou křivku E nad tělesem $\mathbf{F}_p$ charakteristiky různé od 2,3 (viz 3), body $P = (x_1, y_1, z_1)$, $Q = (x_2, y_2, z_2)$, kde $z_1 = z_2 = 1$ a $(x_1, y_1), (x_2, y_2)$ jsou body s afinními souřadnicemi na dané (afinní) křivce E, nulový bod $O = (0, 1, 0)$.

Result: Operace pro negaci, sčítání (i dvou totožných bodů) a odčítání.

[**Negace**] $neg(P)$ **return** $(x_1, -y_1, z_1)$;

[**Sčítání dvou totožných bodů**] $double(P)$ **return** $add(P, P)$;

[**Sčítání dvou bodů**] $add(P, Q)$

if $(z_1 == 0)$ **then**
| **return** Q;
end
if $(z_2 == 0)$ **then**
| **return** P;
end
if $(x_1 == x_2)$ **then**
| **if** $(y_1 + y_2 == 0)$ **then**
| | **return** $(0, 1, 0)$;
| **end**
| $\lambda = (3x_1^2 + a) \cdot (2y_1)^{-1}$;
end
else
| $\lambda = (y_2 - y_1) \cdot (x_2 - x_1)^{-1}$;
end
$x_3 = (\lambda^2 - x_2 - x_1)$;
return $(x_3, \lambda \cdot (x_1 - x_3) - y_1, 1)$;

[**Odčítání**] $sub(P, Q)$ **return** $add(P, neg(Q))$;

Je důležité si uvědomit, že algoritmus ve skutečnosti provádíme pro $x_i, y_i, z_i \in \mathbb{Z}/n\mathbb{Z}$, kde $i = 1, 2$ tedy hledání inverzního prvku by nám mohlo selhat, v tom případě nám hledání inverzního prvku vrátí dělitele n. Pokud hledání inverzního prvku neselže, jsme schopni spočítat inverzní prvek a tedy dopočteme funkci $add(P, Q)$.

Algoritmus 4 (Sčítání: Modifikované projektivní souřadnice (Viz Crandall a Pomerance (2005) Algoritmus 7.2.3))**.**

Data: Uvažujeme eliptickou křivku E nad tělesem $\mathbf{F}_p$ charakteristiky různé od 2,3 (viz 3), body $P = (x_1, y_1, z_1)$, $Q = (x_2, y_2, z_2)$ s modifikovanými projektivními souřadnicemi.
Result: Operace pro negaci, sčítání (i dvou totožných bodů) a odčítání.
[**Negace**] $neg(P)$ **return** $(x_1, -y_1, z_1)$;
[**Sčítání dvou totožných bodů**] $double(P)$
if $(y_1 == 0$ *nebo* $z_1 == 0)$ **then**
  return $(0, 1, 0)$;
end
$\lambda = (3x_1^2 + az_1^4)$; $\nu = 4x_1y_1^2$;
$x' = (\lambda^2 - 2\nu)$; $y' = \lambda \cdot (\nu - x') - 8y_1^4$; $z' = 2y_1z_1$;
return (x', y', z');
[**Sčítání dvou rozdílných bodů**] $add(P, Q)$
if $(z_1 == 0)$ **then**
  return Q;
end
if $(z_2 == 0)$ **then**
  return P;
end
$\alpha_1 = (x_2z_1^2)$; $\alpha_2 = (x_1z_2^2)$;
$\beta_1 = (y_2z_1^3)$; $\beta_2 = (y_1z_2^3)$;
$\lambda = \alpha_1 - \alpha_2$; $\nu = \beta_1 - \beta_2$;
if $(\lambda == 0)$ **then**
  if $(\nu == 0)$ **then**
    return $double(Q)$;
  end
  return $(0 : 1 : 0)$;
end
$\gamma = \alpha_1 + \alpha_2$; $\delta = \beta_1 + \beta_2$;
$x_3 = (\nu^2 - \gamma\lambda^2)$; $y_3 = \frac{1}{2} \cdot ((\gamma\lambda^2 - 2x_3) \cdot \nu - \delta\lambda^3)$; $z_3 = z_1z_2\lambda$;
return (x_3, y_3, z_3);
[**Odčítání**] $sub(P, Q)$ **return** $add(P, neg(Q))$;

Následující algoritmus nám poskytuje operaci násobení kP.

Algoritmus 5 (Násobení: Na principu řetězu sčítání a odčítání (Viz Crandall a Pomerance (2005) Algoritmus 7.2.4))**.**

Data: Uvažujeme B-bitovou reprezentaci čísla $m = 3n$ jako posloupnost bitů $(m_{B-1}, \ldots, m_0)$ a odpovídající B-bitovou reprezentaci čísla n jako $(0, \ldots, 0, n_k, \ldots, n_0)$. Pro $n = 0$ uvažujeme $B = 0$.
Result: Operace pro násobení nP.
[**Inicializace**]
if *(*$n == 0$*)* **then**
| **return** O;
end
$Q = P$
[**Porovnání bitů čísel** $3n$ **a** n]
forall *(*$B - 2 \geq j \geq 1$*)* **do**
| $Q = double(Q)$; **if** *(*$(m_j, n_j) == (1, 0)$*)* **then**
| | $Q = add(Q, P)$;
| **end**
| **if** *(*$(m_j, n_j) == (0, 1)$*)* **then**
| | $Q = sub(Q, P)$;
| **end**
end
return Q;

Nyní máme operace pro sčítání i násobení pro všechny tři zmíněné přístupy. Existuje ještě další, využívající Zobecněné Montgomeryho identity, ten je však mimo možnosti této práce, proto pro více informací doporučuji Crandall a Pomerance (2005, Věta 7.2.6, Algoritmy 7.2.7, 7.2.8 a kapitola 7.4.2), protože ve výsledku je tento přístup ještě efektivnější než předchozí tři, jelikož díky němu lze sestrojit algoritmus, který se kompletně vyhne inverzním prvkům.

Nyní konečně máme vše potřebné a můžeme přistoupit k skutečnému algoritmu, který implementuji (samozřejmě dochází k implementaci operací na eliptické křivce) a který je přílohou práce:

Algoritmus 6 (ECM (Viz Crandall a Pomerance (2005) Algoritmus 7.4.2))**.**

Data: Uvažujeme složené číslo n, které chceme faktorizovat, $NSD(n,6) = 1$ a n není mocninou nějakého prvočísla. Algoritmus se pokouší najít netriviálního dělitele n. Algoritmus má volitelný parametr B, který značí mez pro prvočísla, která budeme testovat.
Result: Prvočíselný dělitel d čísla n
[**Nalezení křivky** $\mathrm{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ **a bodu** (x,y) **na ní**]
Náhodně zvol $x, y, a \in [0, n-1]$; $b = (y^2 - x^3 - ax) \bmod n$;
$g = NSD(4a^3 + 27b^2, n)$; **if** *(*$g == n$*)* **then**
  jdi na [**Nalezení křivky** $\mathrm{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ **a bodu** (x,y) **na ní**];
end
if *(*$g > 1$*)* **then**
  return g;
end
$P = (x, y)$
[**Násobení prvočísly**]
forall *(*$1 \leq i \leq \pi(B)$*)* **do**
  Najdi největší $a_i \in \mathbb{N} : p_i^{a_i} \leq B$;
  forall *(*$1 \leq j \leq a_i$*)* **do**
    $P = p_i \cdot P$;
    if *Operace selže: hledání* d^{-1} *(není definována)* **then**
      Značí to netriviálního dělitele $g = NSD(n, d)$;
      return g
    end
  end
end
[**Selhalo hledání**]
Je možné navýšit hodnotu B;
Jdi na [**Nalezení křivky** $\mathrm{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ **a bodu** (x,y) **na ní**];

3. Přílohy

3.1 Programy

Přílohou práce jsou dva programy:

1. Program, který umožňuje ověření platnosti Hypotézy z kapitoly 1.3.5 Výstup z programu viz Tabulka 3.1.
   - Ověření umožňuje na základě vstupu pro dané α a poté podle volby buď pro nějaký interval $\langle 3, x \rangle$ pro uživatelem zadané číslo x,
   - nebo jen pro zadané číslo x.
   - Program při testování hypotézy vrací seznam čtveřic:
     - počet prvočísel, pro která hypotéza platí s hodnotou α na výstupu v této čtveřici,
     - nejmenší prvočíslo, pro které byla tato hodnota α použita,
     - největší prvočíslo, pro které byla tato hodnota α použita,
     - nejmenší parametr α, pro který prvočísla příslušná tomuto parametru splňují hypotézu.
2. Druhý program je implementací faktorizační metody s použitím eliptických křivek. Implementovaný je výše zmíněný přístup k reprezentaci bodu v podobě Afinních souřadnic. Výstup z programu viz Tabulky 3.2 a 3.3. Výstup odpovídá spuštění Algoritmu ECM na stejná data dvakrát po sobě.

U druhého algoritmu je potřeba si uvědomit, že algoritmus při hledání dělitele volí křivky náhodně, z tohoto důvodu může dojít k tomu, že algoritmus dvakrát puštěný na stejná data nevrátí stejný výsledek. Tedy jednou se podaří najít více dělitelů, tj více faktorizovat zadané číslo a po druhé provede rozklad na méně dělitelů.

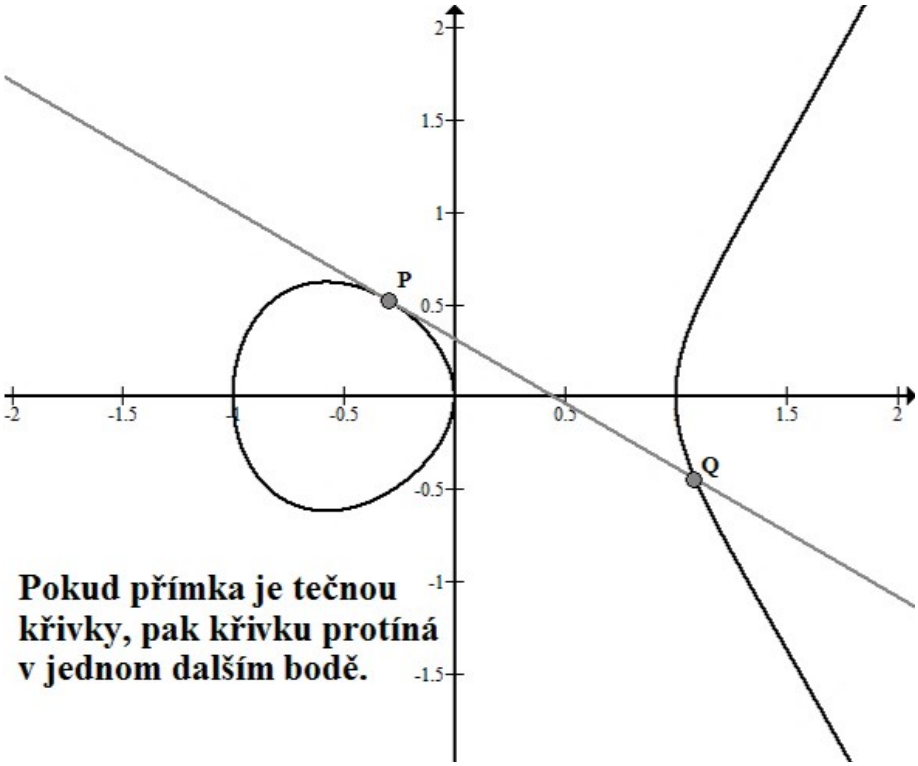
Znamená to tedy, že algoritmus nemusí nutně najít všechny dělitele zadaného čísla.

3.2 Tabulky a výstupy z programů

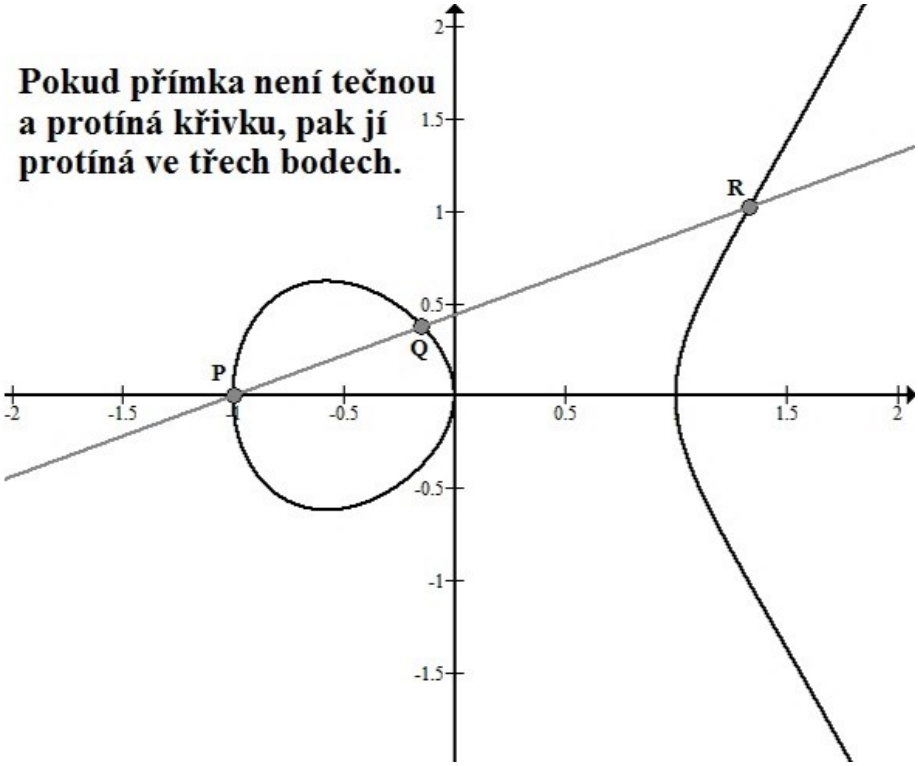
Přílohou práce jsou tabulky s výstupy z programů.

3.3 Obrázky

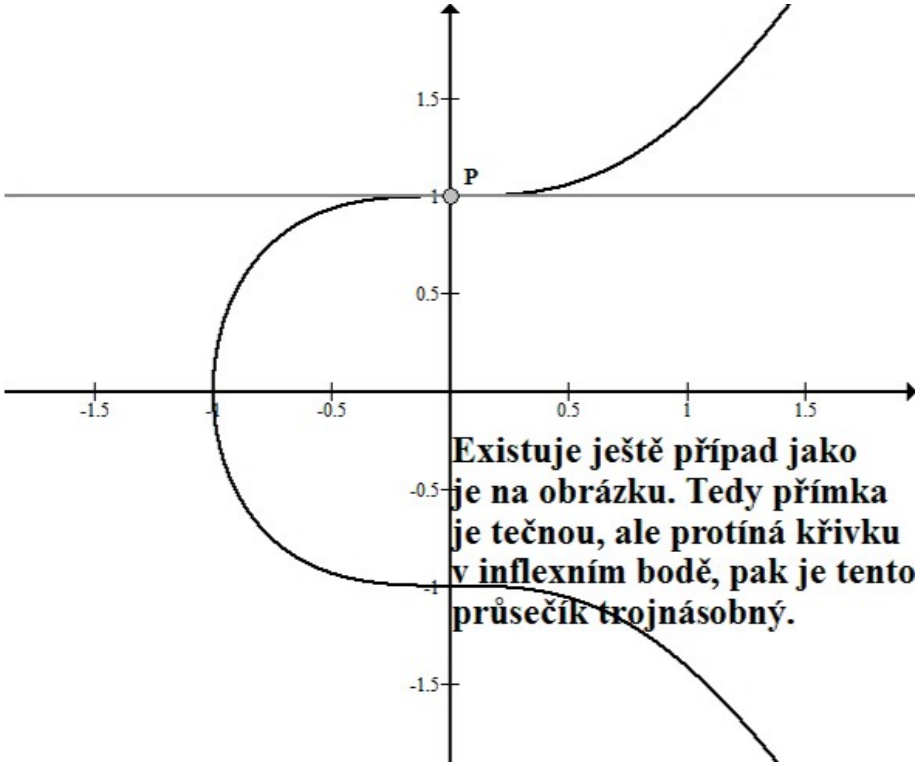
Následují obrázky názorně ukazující operace na eliptické křivce. Pro jednoduchost a čitelnost názorné ukázky jsem použil eliptickou křivku danou rovnicí $y^2 = x^3 - x$ nad reálnými čísly.



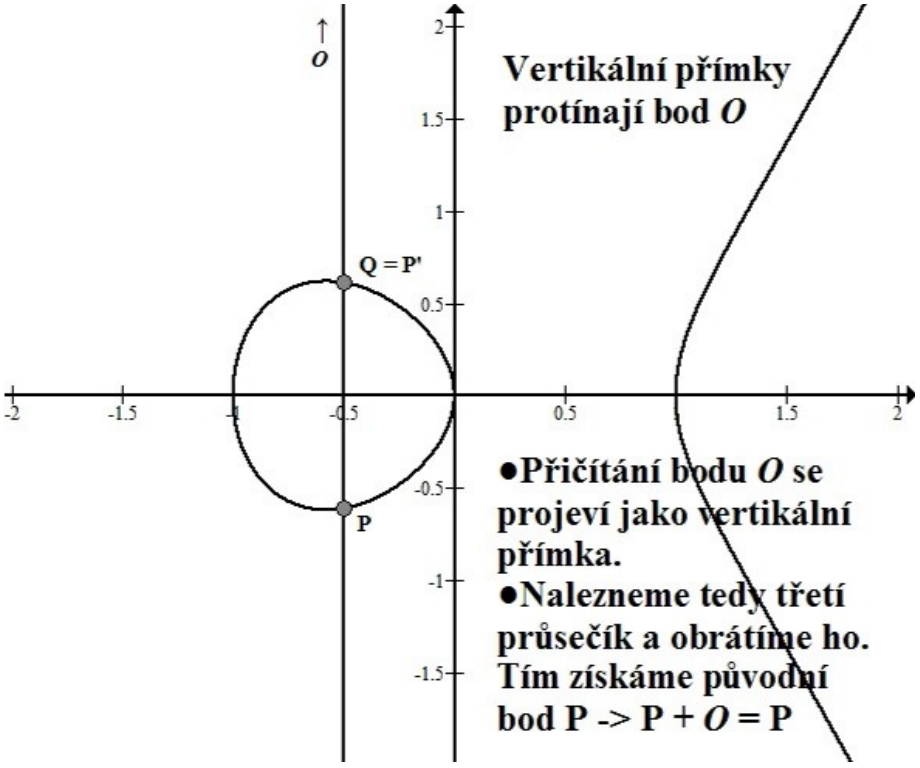
Obrázek 3.1: Přímka, která je tečnou k eliptické křivce.



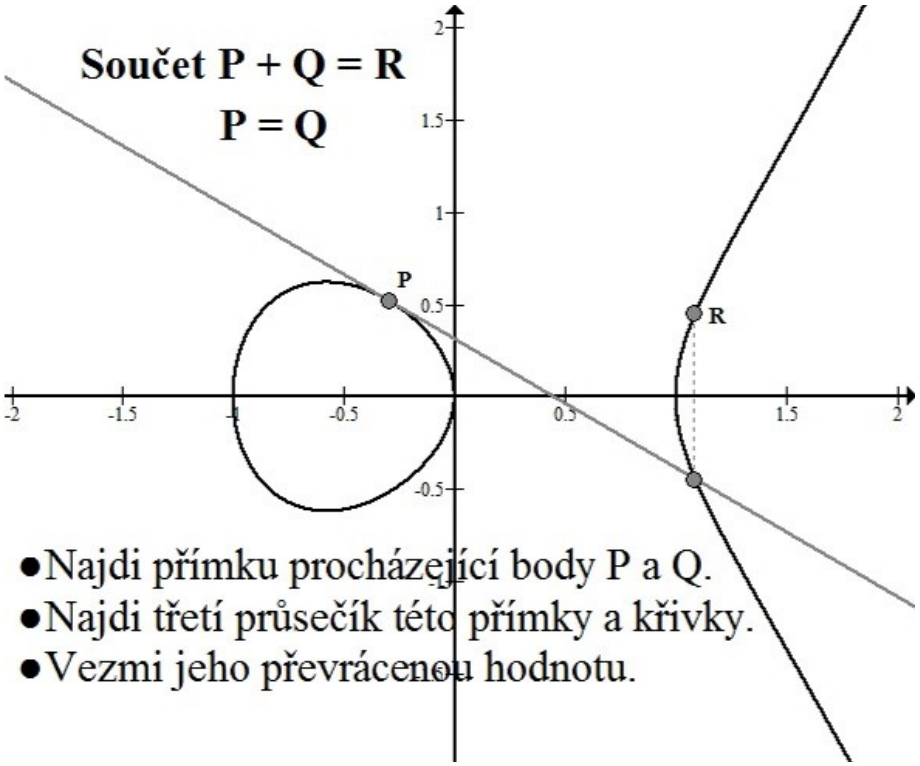
Obrázek 3.2: Přímka, která je sečnou k eliptické křivce.



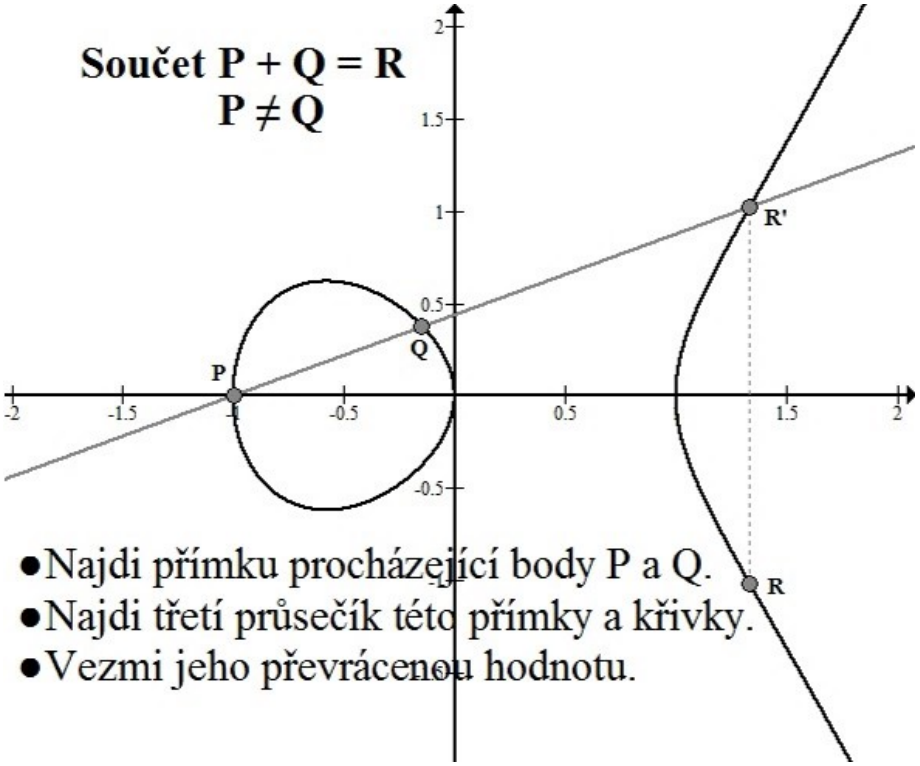
Obrázek 3.3: Inflexní bod eliptické křivky.



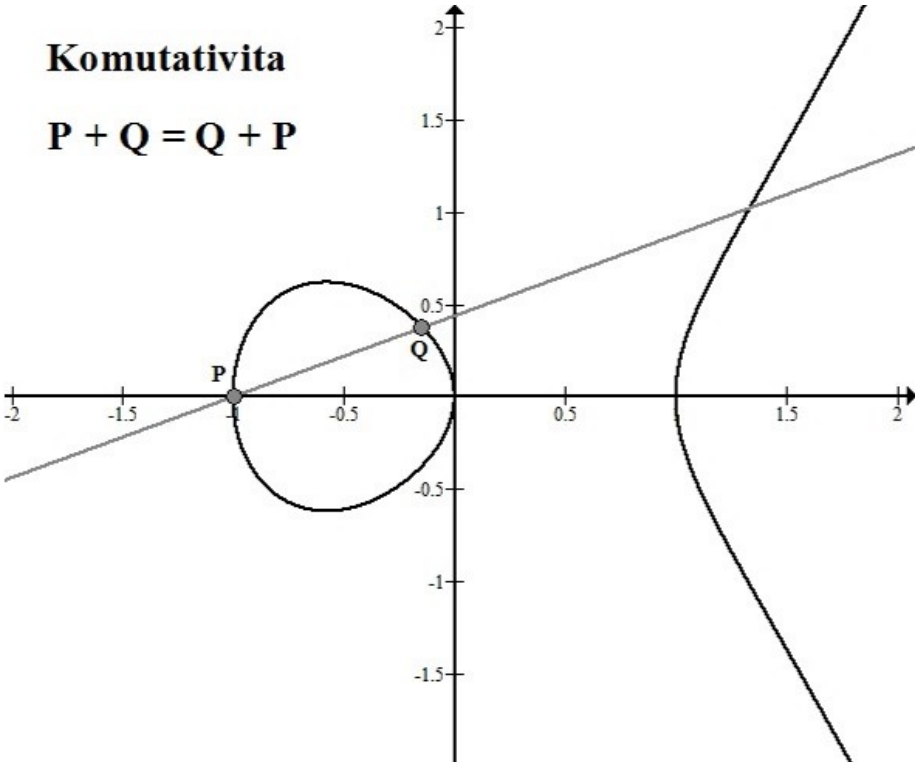
Obrázek 3.4: Nulový bod eliptické křivky, přímky procházející tímto bodem a jejich geometrický význam.



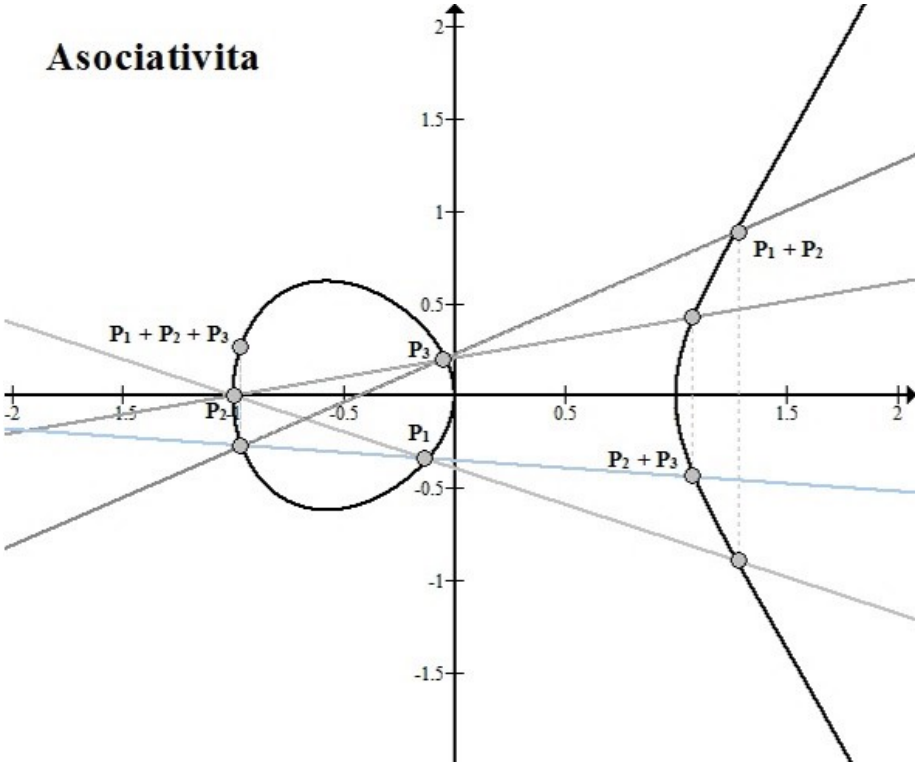
Obrázek 3.5: Princip sčítání dvou rozdílných bodů na eliptické křivce.



Obrázek 3.6: Princip sčítání dvou totožných bodů na eliptické křivce.



Obrázek 3.7: Komutativita operace + na eliptické křivce.



Obrázek 3.8: Asociativita operace + na eliptické křivce.

Koeficient α	**Počet prvočísel**	**Nejmenší prvočíslo**	**Největší prvočíslo**
5,00700029545846	1	3	3
1,25532544808878	1	5	5
0,96523721675247	1	7	7
0,758624300018952	1	11	11
0,70710678	38309473	13	839999981

Tabulka 3.1: Výstup programu pro testování Hypotézy z kapitoly 1.3.5 pro interval $\langle 3, 839999981 \rangle$

Vstupní číslo a jeho rozklad	**Doba běhu**
46218836464814872252727	
$= 6661 \cdot 1144081 \cdot 530897 \cdot 11423851$	524
61497430744759922867	
$= 331 \cdot 241489 \cdot 672473 \cdot 1144081$	689
24278215013642666753	
$= 1381 \cdot 6661 \cdot 672473 \cdot 3924721$	111
37725186539107977991	
$= 547 \cdot 61423 \cdot 2114963 \cdot 530897$	203
17042895011356928377	
$= 331 \cdot 11467 \cdot 1144081 \cdot 3924721$	172
8300680200098577140129 59	
$= 103171 \cdot 114487 \cdot 61424707 \cdot 1144081$	2190
655771330477303264001	
$= 11467 \cdot 141233 \cdot 103171 \cdot 3924721$	87
41156716733975732768333 53	
$= 331 \cdot 3924721 \cdot 11467 \cdot 241489 \cdot 1144081$	297
97935649749788509298853457	
$= 331 \cdot 141233^2 \cdot 241489 \cdot 61424707$	256
5628062270846107	
$= 181080457 \cdot 31080451$	100
74632711416723699688718599728372640277 04	
$= 2^3 \cdot 3^4 \cdot 19 \cdot 143 \cdot 12157 \cdot 5209$	
$\cdot 31080451 \cdot 34763 \cdot 181080457 \cdot 342143$	37713
23409544845606048682818257	
$= 12157 \cdot 1925602109534099587301$	4650
907309872693110017115752016897826187847975 28	
$= 2^3 \cdot 3^4 \cdot 11 \cdot 34763 \cdot 5209 \cdot 13$	
$\cdot 19 \cdot 12157^2 \cdot 342143 \cdot 5628062270846107$	44644

Pozn: Doba běhu je měřena v milisekundách.

Tabulka 3.2: Výstup programu na faktorizaci celého čísla s použitím metody ECM - první spuštění

Vstupní číslo a jeho rozklad	Doba běhu
46218836464814872252727 $= 6661 \cdot 530897 \cdot 1144081 \cdot 11423851$	964
61497430744759922867 $= 331 \cdot 672473 \cdot 241489 \cdot 1144081$	536
24278215013642666753 $= 1381 \cdot 6661 \cdot 3924721 \cdot 672473$	152
37725186539107977991 $= 257 \cdot 547 \cdot 239 \cdot 2114963 \cdot 530897$	5178
17042895011356928377 $= 331 \cdot 11467 \cdot 4490198726401$	1717
830068020009857714012959 $= 114487 \cdot 103171 \cdot 70274840209267$	3805
6557713304773032640001 $= 11467 \cdot 103171 \cdot 141233 \cdot 3924721$	52
41156716733975732768333353 $= 331 \cdot 11467 \cdot 241489 \cdot 1144081 \cdot 3924721$	162
97935649749788509298853457 $= 331 \cdot 241489 \cdot 141233^2 \cdot 61424707$	1039
5628062270846107 $= 5628062270846107$	8578
7463271141672369968871859972837264027704 $= 2^3 \cdot 3^4 \cdot 12157 \cdot 19 \cdot 11 \cdot 13$ $\cdot 34763 \cdot 5209 \cdot 342143 \cdot 181080457 \cdot 31080451$	45766
23409544845606048682818257 $= 12157 \cdot 342143 \cdot 5628062270846107$	2262
907309872693110017115752016897826184784797528 $= 2^3 \cdot 3^4 \cdot 19 \cdot 11 \cdot 13 \cdot 34763 \cdot 5209$ $\cdot 12157^2 \cdot 342143 \cdot 5628062270846107$	50255

Pozn: Doba běhu je měřena v milisekundách.

Tabulka 3.3: Výstup programu na faktorizaci celého čísla s použitím metody ECM - druhé spuštění

Závěr

V práci jsem se věnoval odhadu složitosti algoritmu ECM pro faktorizaci celého čísla. Látku jsem uvedl, aby bylo srozumitelné, o jaké pojmy se opírám. Tedy nejprve jsem rozebral teorii, o kterou jsem se později opíral, a také princip operací na eliptických křivkách, které jsem doplnil o obrázky, které názorně ukazují operace na eliptických křivkách nad reálnými čísly. Následně jsem uvedl dvě nejdůležitější věty, o které se teorie potřebná k odhadu složitosti běhu faktorizačního algoritmu opírá.

Než jsem se mohl věnovat odhadu složitosti algoritmu, musel jsem nejprve provést několik odhadů konstant, které vyústily ve Větu 24, která nám poskytla odhad pravděpodobnosti, že Algoritmus 2 na daný vstup skončí úspěchem. Důkazy jednotlivých odhadů konstant, které vedly k již zmiňované Větě 24, jsem dokázal nebo se explicitně odkázal na Lenstra Jr (1987). Tyto důkazy jsem doplnil o vynechané kroky v původním článku, aby bylo patrné, odkud se každý krok daného důkazu bere a z čeho platí.

Po odhadu konstant jsem se dostal k potřebné Hypotéze 1, u které jsem ukázal, jak dochází ke konstrukci této hypotézy na základě funkce Ψ. K této hypotéze jsem naimplementoval program, který testuje platnost hypotézy, ze které tato hypotéza vychází. Tedy jedinou část, která se předpokládá, že platí, a to, že pro náhodné číslo $s \in (x+1-\sqrt{x}, x+1+\sqrt{x})$ platí, že s má všechny prvočíselné dělitele $p \leq L(x)^{\alpha}$ s pravděpodobností alespoň:

$$L(x)^{(\frac{-1}{2\alpha}+o(1))}, \qquad \text{pro } x \to \infty.$$

A nakonec jsem rozvedl, jak dochází k implementaci faktorizačního algoritmu ECM, jak se dá modifikovat reprezentace bodů na eliptické křivce při implementaci. Na závěr jsem poskytnul algoritmus, který je implementován ve druhém programu, který je součástí příloh a který umožňuje provést faktorizaci složeného čísla n ze vstupu programu.

Seznam použité literatury

Canfield, E., Erdös, P. a Pomerance, C. (1983). On a problem of oppenheim concerning "factorisatio numerorum". *Journal of Number Theory*, **17** (1), 1 – 28.

Cohen, H. (1993). *A Course in Computational Algebraic Number Theory*, volume 138. Springer-Verlag Berlin Heidelberg.

Cox, D. A. (2011). *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons.

Crandall, R. a Pomerance, C. (2005). *Prime numbers: A Computational Perspective*, volume 182. Springer-Verlag New York. ISBN 978-0-387-25282-7.

De Bruijn, N. (1966). On the number of positive integers $\leq$ x and free of prime factors $>$ y. *Nederl. Akad. Wetensch. Proc. Ser. A*, **II**, 239 – 247.

EllipticCurves. URL `http://www.maths.tcd.ie/pub/Maths/Courseware/EllipticCurves/EllipticCurves.pdf`.

Hildebrand, A. (1986). On the number of positive integers $\leq$ x and free of prime factors $>$ y. *Journal of Number Theory*, **22**(3), 289 – 307.

Jedlicka, P. Faktorizace velkých čísel. URL `https://artax.karlin.mff.cuni.cz/~ppri7485/nmib014/faktorizace.pdf`.

Knuth, D. E. (1997). *The Art of Computer Programming, Volume 2: Seminumerical Algorithms (3rd Edition)*, volume 2. Addison-Wesley Professional. ISBN 978-0-201-89684-8.

Lenstra Jr, H. W. (1987). Factoring integers with elliptic curves. *Annals of mathematics*, **126**, 649 – 673.

Montgomery, P. L. (1987). Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, **48**(177), 243 – 264.

Riverninj4. Elliptic curve point addition. URL `https://www.youtube.com/watch?v=XmygBPb7DPM`.

Rotman, J. (1995). *An Introduction to the Theory of Groups*, volume 148. Springer-Verlag New York.

Schoof, R. (1987). Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory, Series A*, **46**(2), 183 – 211.

Stehlé, D. a Zimmermann, P. (2004). *A Binary Recursive Gcd Algorithm*, pages 411–425. Springer Berlin Heidelberg, Berlin, Heidelberg.

Ughi, E. (1983). On the number of points of elliptic curves over a finite field and a problem of b. segre. *European Journal of Combinatorics*, **4**(3), 263 – 270.

Seznam obrázků

Seznam tabulek