Indhold

Kapitel 1

Elliptiske kurver

I dette kapitel vil vi introducere elliptiske kurver. Det viser sig, at være muligt at påføre de elliptiske kurver en gruppestruktur ved en geometrisk addition af punkter fra en sådan kurve. Vi vil indføre denne additionslov og vise, at det resulterer i en abelsk gruppe. For at kunne gøre dette skal vi desuden anvende projektiv geometri, som også vil blive introduceret.

1.1 Elliptiske kurver

Det er muligt at definere elliptiske kurver på flere måder. Lad K være et legeme, da er følgende defintion tilstrækkelig til vores formål:

Definition 1. En elliptisk kurve E er grafen for en ligning

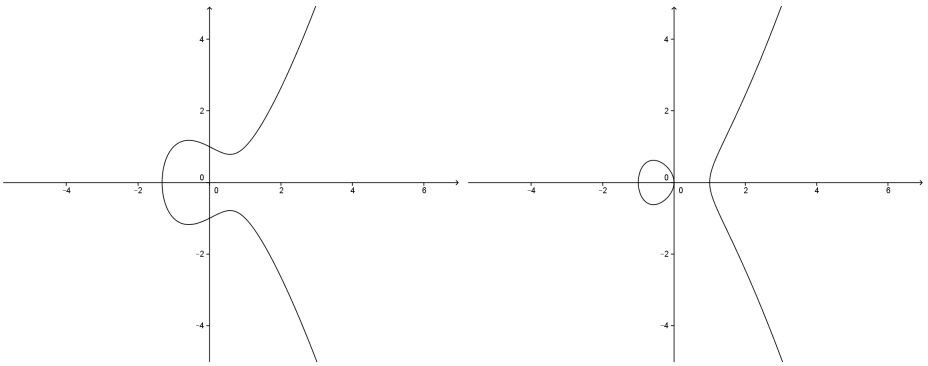
$$y^2 = x^3 + Ax + B, \tag{1.1}$$

hvor $A, B \in K$ er konstanter og $4A^3 + 27B^2 \neq 0$.

Vi siger, at den elliptiske kurve E er på Weierstrass normalform, når den kan beskrives som i (1.1). Hvis $\text{char}(K) \neq 2, 3$ er det faktisk altid muligt, at omskrive en elliptisk kurve til Weierstrass normalform (se eksempelvis kapitel 2 i [5]). Det kan vises, at diskriminanten for (1.1) er

$$\Delta = 4A^3 + 27B^2,$$

så en elliptisk kurve kan ikke have multiple rødder pr. kravet i definitionen. I figur 1.1 ses to eksempler på elliptiske kurver over de reelle tal. Definitionen siger, at A, B skal tilhøre et legeme K. Det kunne være $\mathbb{R}, \mathbb{C}$ eller $\mathbb{Q}$. I denne opgave vil vi dog fokusere på de endelige legemer $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ hvor p er et primtal, eller de endelige legemer $\mathbb{F}_q$ hvor $q = p^r$ for $r \geq 1$. Hvis $A, B \in K$ for en elliptisk kurve E siger vi, at E er givet over K. Vi vil fra nu af med E mene en elliptisk kurve på Weierstrass normalform og med K mene et legeme



Figur 1.1: Eksempler på elliptiske kurver over $\mathbb{R}$. Venstre: $y^2 = x^3 - x$, Højre: $y^2 = x^3 - x + 1$

medmindre andet er nævnt. Punkterne på en elliptisk kurve med koordinater i et legeme $L \supseteq K$ skriver vi som $E(L)$, hvor

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}. \tag{1.2}$$

Punktet ∞ kaldes punktet i uendelig og viser sig nødvendigt for at $E(L)$ bliver en gruppe under additionen vi vi introducere i næste afsnit. Intuitivt kan vi se ∞ som værende punktet (∞, ∞) som er placeret i toppen af y-aksen. En linje siges at gå igennem ∞ præcist, når den er lodret. To lodrette linjer skærer derfor hinanden i ∞. ∞ kan også tænkes som værende i bunden af y-aksen, men så vil to lodrette linjer skære hinanden to steder, hvilket er hvorfor vi kræver at ∞ i toppen og i bunden er et og samme punkt.

1.2 Det projektive plan

Som tidligere nævnt vil vi etablere en gruppestruktur på de elliptiske kurver. For at kunne gøre dette får vi brug for det projektive plan $\mathbb{P}^2$. Rent intuitivt kan man se det projektive plan, som værende den affine plan

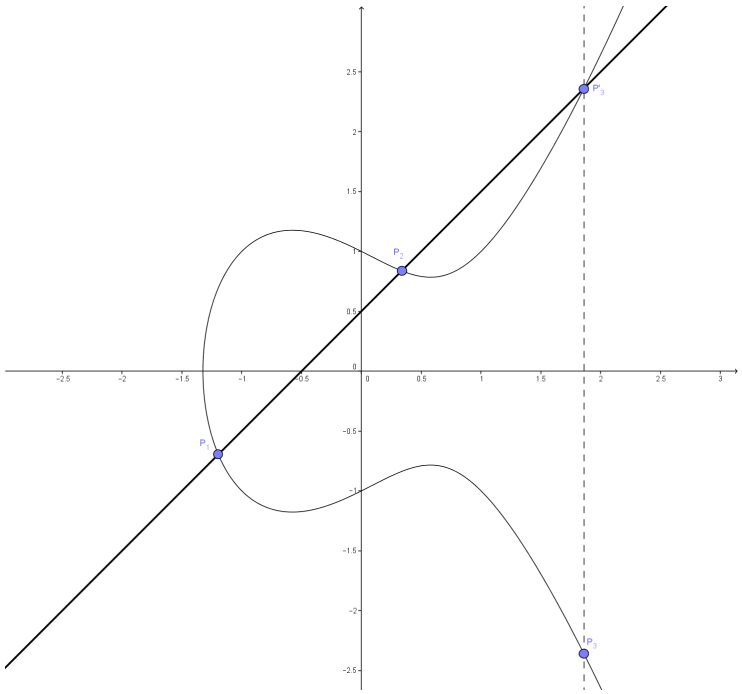
$$\mathbb{A}^2(K) = \{(x, y) \in K \times K\},$$

hvor K et et legeme, med en ekstra linje "i uendelig". Vi ønsker at formalisere dette begreb. For $x, y, z \in K$ ikke alle nul og $\lambda \in K$, $\lambda \neq 0$, definerer vi en ækvivalensrelation. To tripler (x_1, y_1, z_1) og (x_2, y_2, z_2) siges at være ækvivalente hvis

$$(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2),$$

og vi skriver $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. Vi vil fremover skrive $(x : y : z)$ for en sådan ækvivalensklasse. I de tilfælde hvor $z \neq 0$ har vi, at

$$(x, y, z) = (x/z, y/z, 1),$$



Figur 1.2: Addition af to punkter på en elliptisk kurve

hvilket er de punkter vi kalder for de "endelige"punkter i $\mathbb{P}^2(K)$. Vi er nemlig i stand til at associere et punkt fra $\mathbb{A}^2(K)$ med et sådan punkt. Vi har en afbildning (en inklusion for at være mere præcis) $\mathbb{A}^2(K) \to \mathbb{P}^2(K)$ givet ved

$$(x, y) \mapsto (x, y, 1).$$

Dette kan vi selvfølgelig ikke gøre, når $z = 0$ og vi ser det som at vi har ∞ i enten x- eller y-koordinaten. Vi kalder dermed punkterne $(x, y, 0)$ for punkterne i "uendelig".

1.3 Gruppeloven

Lad E være en elliptisk kurve over K. Det viser sig, at vi kan tage to punkter (eller blot ét) på E og producere et tredje punkt som også er på E. Vi vil i dette afsnit vise, hvordan dette gøres og til slut konkludere, at defineres dette som en addition operator bliver $E(K)$ en additiv abelsk gruppe. Vælg to punkter

$$P_1 = (x_1, y_1) \quad \text{og} \quad P_2 = (x_2, y_2)$$

på E. Vi kan da trække en ret linje L igennem punkterne P_1 og P_2, som så vil skære kurven for E i et tredje punkt $P_3{}'$ (se appendiks for bevis om skæring

i 3 punkter). Vi definerer $P_1 + P_2 = P_3$ til at være reflektionen i x-aksen af dette punkt.

Vi vil nu udlede formlerne for denne addition af punkter på E. Antag først, at $P_1 \neq P_2$ og lad P_1 og P_2 være forskellige fra ∞. Vi har da, at hældningen for linjen der går igennem P_1 og P_2 er

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Hvis $x_1 = x_2$ er linjen lodret, hvilket er et tilfælde som vi behandler senere. Antag altså at $x_1 \neq x_2$, da har vi at

$$y_2 = m(x_2 - x_1) + y_1.$$

Vi indsætter dette i ligningen for E og får, at

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

Skrives dette ud får vi, at

$$\begin{aligned} 0 &= x^3 + Ax + B - 2y_1 m(x - x_1) - m^2(x - x_1)^2 - y_1^2 \\ &= x^3 + Ax + B - 2y_1 mx - 2y_1 mx_1 - m^2(x^2 - 2xx_1 + x_1^2) - y_1^2 \\ &= x^3 - m^2 x^2 + (A - 2my_1 + 2m^2 x_1)x - 2my_1 x_1 - m^2 x_1^2 - y_1^2 + B. \end{aligned}$$

Denne har tre rødder, som netop er de tre punkter, hvor L skærer E. Pr. vores konstruktion kender vi allerede de to rødder x_1 og x_2, og vi ønsker at finde den tredje. Generelt for et kubisk polynomium $x^3 + ax^2 + bx + c$, med rødder r, s, t, har vi at

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \ldots,$$

hvilket giver os, at $-a = r + s + t$. Hvis de to rødder vi kender er r og s kan vi finde den sidste som

$$t = -a - r - s.$$

I vores tilfælde er $a = -m^2$ så vi har, at

$$x = m^2 - x_1 - x_2.$$

Vi mangler da blot at reflektere dette punkt for at have fundet punktet punktet $P_1 + P_2 = (x, y)$. Vi reflekterer over x-aksen og finder, at

$$x = m^2 - x_1 - x_2, \quad y = m(x_1 - x) - y_1.$$

Vi vender nu tilbage til tilfældet, hvor $x_1 = x_2$. Da vil linjen igennem P_1 og P_2 være lodret, så den skærer E i ∞. Vi husker, at når ∞ reflekteres over x-aksen får vi igen ∞. Vi får altså, at $P_1 + P_2 = \infty$.

Tilfældet hvor $P = Q = (x, y)$ kræver lidt flere overvejelser, da ikke ligeså let kan udvælge en linje. For to punkter der ligger tæt på hinanden vil linjen igennem punkterne nærme sig tangenten til et af punkterne. Derfor vælger vi i dette tilfælde, at lade linjen der går igennem punkterne være deres tangentlinje.

Blah blah blah.

Hvis $P = \mathcal{O}$ er linjen igennem P og Q en lodret linje der skærer E i refleksionen af Q. Derfor får vi, at

$$\mathcal{O} + Q = Q.$$

Der gælder derfor også, at $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Vi har nu dækket de mulige tilfælde og kan opstille gruppeloven som følger.

Definition 2 (Gruppeloven for elliptiske kurver)**.** Givet to punkter $P_1, P_2 \in E(K)$, $P_i = (x_i, y_i)$. Et tredje punkt $R = P_1 + P_2 = (x_3, y_3)$ findes da som følger

1. Hvis $x_1 \neq x_2$ da er

   $$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1,$$

   hvor $m = (y_2 - y_1)/(x_2 - x_1)$.

2. Hvis $x_1 = x_2$, men $y_1 \neq y_2$ da er $R = P_1 + P_2 = \mathcal{O}$.

3. Hvis $P_1 = P_2$ og $y_1 \neq 0$ da er

   $$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1,$$

   hvor $m = (3{x_1}^2 + A)/2y_1$.

4. Hvis $P_1 = P_2$ og $y_1 = 0$ da er $R = P_1 + P_2 = \mathcal{O}$.

Vi definerer desuden, at

$$P + \mathcal{O} = \mathcal{O},$$

for alle $P \in E(K)$.

Kapitel 2

Endomorfier og torsionpunkter

Ordenen af et element P fra en gruppe over en elliptisk kurve er det mindste heltal n sådan at $nP = \infty$. Hvis der ikke findes et sådan n siges ordenen af P at være uendelig. Torsionspunkterne er netop de punkter, som har endelig orden og de viser sig at have relevans for elliptiske kurver over endelig legemer, som vi vil undersøge i næste kapitel 3.

Vi skal desuden etablere nogle vigtige resultater vedrørende endomorfier på elliptiske kurver, som viser sig nødvendige i beviset for Hasses sætning.

2.1 Endomorfier

Lad K være et legeme og $\overline{K}$ dens tilhørende algebraiske aflukning. I det følgende vil vi med en elliptisk kurve E mene en kurve på formen Når vi skriver om en elliptisk kurve E menes den at være på Weierstrass normalform, altså $y^2 = x^3 + Ax + B$.

Vi begynder da med følgende definition:

Definition 3. En endomorfi på E er en homomorfi $\alpha : E(\overline{K}) \to E(\overline{K})$ givet ved rationale funktioner.

Med en rational funktion forstår vi en kvotient af polynomier. Det vil altså sige, at en endomorfi α skal opfylde, at $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ og der skal findes rationale funktioner $R_1(x, y)$ og $R_2(x, y)$, begge med koefficienter i $\overline{K}$, så

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

for alle $(x, y) \in E(\overline{K})$. da α er en homomorfi gælder der, at $\alpha(\infty) = \infty$. Den trivielle endomorfi angives med 0 og er den endomorfi, som sender ethvert punkt til ∞. Vi vil fremover antage, at α ikke er den trivielle endomorfi, hvilket betyder at der findes (x, y) sådan at $\alpha(x, y) \neq \infty$.

Eksempel 1. Lad E være en elliptisk kurve og lad α være givet ved, at $\alpha(P) = 2P$. Da er α en homomorfi og $\alpha(x,y) = (R_1(x,y), R_2(x,y))$, hvor

$$\begin{aligned} R_1(x,y) &= \left(\frac{3x^2+A}{2y}\right)^2 - 2x, \\ R_2(x,y) &= \left(\frac{3x^2+A}{2y}\right)\left(x - \left(\left(\frac{3x^2+A}{2y}\right)^2 - 2x\right)\right) - y \\ &= \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y. \end{aligned}$$

Da både R_1 og R_2 er rationale funktioner er α en endomorfi for E.

Vi ønsker nu, at finde en standard repræsentation for de rationale funktioner, som en endomorfi er givet ved. Følgende sætning gør dette muligt for os:

Sætning 1. *Lad E være en elliptisk kurve over et legeme K. En endomorfi α kan da skrives som*

$$\alpha(x,y) = (r_1(x), r_2(x)y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

hvor p, q henholdsvis s, t ikke har nogen fælles faktor.

Bevis. For et punkt $(x,y) \in E(\overline{K})$ gælder der, at $y^2 = x^3 + Ax + B$ så vi har også, at

$$y^{2k} = (x^3 + Ax + B)^k \quad \text{og} \quad y^{2k+1} = y^{2k}y = (x^3 + Ax + B)^k y, \quad k \in \mathbb{N}.$$

Vi kan altså erstatte en lige potens af y med et polynomium der kun afhænger af x, og en ulige potens med y ganget med et polynomium der kun afhænger af x. For en rational funktion $R(x,y)$ kan vi da beskrive en anden rational funktion, som stemmer overens med denne på punkter fra $E(\overline{K})$. Vi kan altså antage, at

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{2.1}$$

Vi kan endda gøre det endnu simplere ved at gange udtrykket i (2.1) med $p_3(x) - p_4(x)$, hvilket giver

$$(p_3(x) - p_4(x)y)(p_3(x) + p_4(x)y) = p_3(x)^2 - p_4(x)^2y^2,$$

hvorefter vi kan erstatte y^2 med $x^3 + Ax + B$. Dette giver os altså, at

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{2.2}$$

Da α er en endomorfi er den givet ved

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)),$$

hvor R_1 og R_2 er rationale funktioner. Da α specielt er en homomorfi bevarer den strukturen for en elliptisk kurve så vi har, at

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

Dette medfører, at

$$R_1(x,-y) = R_1(x,y) \quad \text{og} \quad R_2(x,-y) = -R_2(x,y).$$

Skriver vi R_1 på samme form som i (2.2) må $q_2(x) = 0$, og ligeledes må vi for R_2 have at $q_1(x) = 0$. Vi kan altså antage, at

$$\alpha(x,y) = (r_1(x), r_2(x)y),$$

hvor $r_1(x)$ og $r_2(x)$ er rationale funktioner. Skriv da

$$r_1(x) = \frac{p(x)}{q(x)} \quad \text{og} \quad r_2(x) = \frac{s(x)}{t(x)}y,$$

hvor p, q henholdsvis s, t ikke har nogen fælles faktorer. Hvis $q(x) = 0$ for et punkt (x,y) lader vi $\alpha(x,y) = \infty$. Hvis $q(x) \neq 0$ giver (ii) i lemma 1, at $r_2(x)$ da også vil være defineret. □

Lemma 1. *Lad α være en endomorfi givet ved*

$$\alpha(x,y) = \left(\frac{p(x)}{q(x)}, \frac{s(x)}{t(x)}y\right),$$

for en elliptisk kurve E. Lad p, q henholdsvis s, t være sådan, at de ikke har nogen fælles rødder. Da har vi, at

(i) For et polynomium $u(x)$, som ikke har en fælles rod med $q(x)$ har vi, at

$$\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3}.$$

(ii) $t(x_0) = 0$ hvis og kun hvis $q(x_0) = 0$.

Bevis. (i) For et punkt $(x,y) \in E(K)$ har vi også, at $\alpha(x,y) \in E(K)$, da α er en endomorfi. Derfor har vi, at

$$\begin{aligned}\frac{(x^3 + Ax + B)s(x)^2}{t(x)^2} &= \frac{y^2 s(x)^2}{t(x)^2} = \left(\frac{s(x)}{t(x)}y\right)^2 \\ &= \left(\frac{p(x)}{q(x)}\right)^3 + A\left(\frac{p(x)}{q(x)}\right) + B \\ &= \frac{p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3}{q(x)^3} = \frac{u(x)}{q(x)^3},\end{aligned}$$

hvor $u(x) = p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3$. Antag nu, at $q(x_0) = 0$. Hvis nu også $u(x_0) = 0$ følger det, at

$$u(x_0) = p(x_0)^3 + Ap(x_0)q(x_0)^2 + Bq(x_0)^3 = 0 \Rightarrow p(x_0)^3 = 0 \\ \Rightarrow p(x_0) = 0,$$

men p og q havde pr. antagelse ingen fælles rødder. Så hvis $q(x_0) = 0$ må $u(x_0) \neq 0$ og de har dermed ingen fælles rødder.

(ii) Vi ved fra (i), at

$$(x^3 + Ax + B)s(x)^2q(x)^3 = u(x)t(x)^2. \tag{2.3}$$

Hvis $q(x_0) = 0$ følger det direkte fra (2.3), at

$$u(x_0)t(x_0)^2 = 0.$$

Da q og u ikke har nogen fælles rødder følger det, at $t(x_0) = 0$. Antag nu, at $t(x_0) = 0$, da har vi fra (2.3), at

$$({x_0}^3 + Ax_0 + B)s(x_0)^2q(x_0)^3 = 0.$$

Da s og t pr. antagelse ikke har nogen fælles rødder giver det yderligere, at

$$({x_0}^3 + Ax_0 + B)q(x_0)^3 = 0.$$

Hvis ${x_0}^3 + Ax_0 + B \neq 0$ er $q(x_0)^3 = 0$ og dermed må $q(x_0) = 0$. Hvis vi derimod har, at ${x_0}^3 + Ax_0 + B = 0$ er det klart, at $(x - x_0) \mid (x^3 + Ax + B)$. Med andre ord findes et polynomium $Q(x)$ sådan, at

$$(x^3 + Ax + B) = (x - x_0)Q(x),$$

hvor $Q(x_0) \neq 0$, da $x^3 + Ax + B$ ikke har nogen dobbeltrødder. Da $t(x_0) = 0$ findes der også et polynomium $T(x)$ sådan, at

$$t(x) = (x - x_0)T(x).$$

Udtrykket fra (2.3) kan da skrives, som

$$(x - x_0)Q(x)s(x)^2q(x)^3 = u(x)((x - x_0)T(x))^2,$$

hvilket med division med $(x - x_0)$ giver os, at

$$Q(x)s(x)^2q(x)^3 = u(x)(x - x_0)T(x)^2.$$

I tilfældet, hvor $x = x_0$ har vi så, at

$$Q(x_0)s(x_0)^2q(x_0)^3 = 0,$$

men da $Q(x_0) \neq 0$ og $s(x_0) \neq 0$ må $q(x_0)^3 = 0$ så $q(x_0) = 0$. □

Med den nu etablerede standard repræsentation for endomorfier, er vi i stand til at give en definition for graden af en endomorfi:

Definition 4. Graden af en endomorfi α er givet ved

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\},$$

når α ikke er den trivielle endomorfi, altså for $\alpha \neq 0$. For $\alpha = 0$ lader vi $\deg(\alpha) = 0$.

En endomorfi siges at være separabel hvis den afledede $r_1'(x) \neq 0$.

Eksempel 2. Eksempel på en separabel endomorfi. Bogen ser på $2P$ som også er oplagt, men måske skulle man vælge en mere interessant.

Den følgende proposition er essentiel idet, at det tilknytter graden af en endomorfi til antallet af elementer i kernen for selvsamme endomorfi. Dette faktum benyttes direkte i beviset for Hasses sætning.

Proposition 1. *Lad E være en elliptisk kurve. Lad $\alpha \neq 0$ være en separabel endomorfi for E. Da er*

$$\deg \alpha = \#\ker(\alpha),$$

hvor $\ker(\alpha) =$ *angiver kernen for homomorfien $\alpha : E(\overline{K}) \to E(\overline{K})$. I tilfældet hvor $\alpha \neq 0$ ikke er separabel gælder der, at*

$$\deg \alpha > \#\ker(\alpha).$$

Bevis. Vi skriver α på standardformen, som vi introducerede tidligere, altså sættes

$$\alpha(x, y) = (r_1(x), r_2(x)y)),$$

hvor $r_1(x) = p(x)/q(x)$. Da α er antaget til at være separabel er $r_1' \neq 0$ og dermed er $pq' - p'q$ ikke nulpolynomiet. Lad nu

$$S = \{x \in \overline{K} \mid (pq' - p'q)(x)q(x) = 0\}.$$

Lad da $(a, b) \in E(\overline{K})$ være valgt sådan, at følgende er opfyldt

1. $a \neq 0$, $b \neq 0$ og $(a, b) \neq \infty$,
2. $\deg(p(x) - aq(x)) = \max\{\deg p(x), \deg q(x)\} = \deg \alpha$,
3. $a \notin r_1(S)$,
4. $(a, b) \in \alpha(E(\overline{K}))$.

Da $pq'-p'q$ ikke er nulpolynomiet er S en endelig mængde, hvilket dermed også betyder, at $\alpha(S)$ er en endelig mængde. Funktionen $r_1(x)$ antager uendeligt mange forskellige værdier når x gennemløber $\overline{K}$, da en algebraisk aflukning indeholder uendeligt mange elementer. Da der for hvert x er et punkt $(x, y) \in E(\overline{K})$ følger det, at $\alpha(E(\overline{K}))$ er en uendelig mængde. Det er altså muligt, at vælge et punkt $(a, b) \in E(\overline{K})$ med egenskaberne ovenfor.

Vi ønsker at vise, at der netop er $\deg \alpha$ punkter $(x_1, y_1) \in E(\overline{K})$ sådan, at $\alpha(x_1, y_1) = (a, b)$. For et sådan punkt gælder der, at

$$\frac{p(x_1)}{q(x_1)} = a, \quad r_2(x_1)y_1 = b.$$

Da $(a, b) \neq \infty$ er $q(x_1) \neq 0$. Da $b \neq 0$ har vi også, at $y_1 = b/r_2(x_1)$. Dette betyder, at y_1 er bestemt ved x_1, så vi behøver kun at tælle værdier for x_1. Fra antagelse (2) har vi, at $p(x)-aq(x) = 0$ har $\deg \alpha$ rødder talt med multiplicitet. Vi skal altså vise, at $p-aq$ ikke har nogen multiple rødder. Antag for modstrid, at x_0 er en multipel rod. Da har vi, at

$$p(x_0) - aq(x_0) = 0 \quad \text{og} \quad p'(x_0) - aq'(x_0) = 0.$$

Dette kan omskrives til ligningerne $p(x_0) = aq(x_0)$ og $aq'(x_0) = p'(x_0)$, som vi ganger med hinanden og får, at

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0).$$

Da $a \neq 0$ pr. (1) giver det os, at x_0 er en rod i $pq' - p'q$ så $x_0 \in S$. Altså er $a = r_1(x_0) \in r_1(S)$, hvilket er i modstrid med (3). Dermed har $p - aq$ netop $\deg \alpha$ forskellige rødder. Da der er præcist $\deg \alpha$ punkter (x_1, y_1) så $\alpha(x_1, y_1) = (a, b)$ har kernen for α netop $\deg \alpha$ elementer. □

Kapitel 3

Elliptiske kurver over endelige legemer

Vi skal i dette kapitel undersøge elliptiske kurver over endelige legemer. Lad $\mathbb{F}$ være et endeligt legeme og lad E være en elliptisk kurve på formen

$$y^2 = x^3 + Ax + B,$$

som er defineret over $\mathbb{F}$. Da er gruppen $E(\mathbb{F})$ endelig, da der kun findes endeligt mange talpar (x, y) så $x, y \in \mathbb{F}$. Lad E være den elliptiske kurve $y^2 = x^3 - x$ over $\mathbb{F}_5$. For at bestemme ordenen af $E(\mathbb{F})$ laver vi en tabel over mulige værdier for x, $x^3 - x \pmod 5$ og for y som er kvadratrødderne af $x^3 - x$. Dette giver os samtlige punkter på kurven:

x	$x^3 - x$	y	Punkter
0	0	0	$(0, 0)$
1	0	0	$(1, 0)$
2	1	± 1	$(2, 1), (2, 4)$
3	4	± 2	$(3, 2), (3, 3)$
4	2	$-$	$-$
∞		∞	∞

Bemærk, at $\sqrt{2} \notin \mathbb{Z}$ og derfor har 2 ikke en kvadratrod i $\mathbb{F}_5$. Dette giver os, at $E(\mathbb{F}_5)$ har orden 7 og vi skriver $\#E(\mathbb{F}_5) = 7$. Vi skal i dette kapitel vise Hasses sætning, som giver en vurdering for antallet af punkter på en elliptisk kurve over et endeligt legeme:

Sætning 2 (Hasse)**.** *Lad E være en elliptisk kurve over et endeligt legeme $\mathbb{F}_q$. Da gælder der, at*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Vi vil i kapitel 3 se på en af anvendelserne, som disse elliptiske kurver over endelige legemer har, nemlig indenfor faktorisering af heltal.

3.1 Frobenius endomorfien

En endomorfi med en absolut kritisk rolle for teorien om elliptiske kurver over endelige legemer er Frobenius endomorfien ϕ_q. For en elliptisk kurve E over et endeligt legeme $\mathbb{F}_q$ er denne givet ved

$$\phi_q(x, y) = (x^q, y^q), \tag{3.1}$$

og $\phi_q(\infty) = \infty$. Denne endomorfi spiller en vigtig rolle i beviset for Hasses sætning, men vi skal først vise nogle af dens egenskaber.

Lemma 2. *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Da er ϕ_q en endomorfi for E af grad q, desuden er ϕ_q ikke seperabel.*

Bevis. Vi skal vise, at $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er en homomorfi. Lad da $(x_1, y_1), (x_2, y_2) \in E(\overline{\mathbb{F}}_q)$, hvor $x_1 \neq x_2$. Da følger det fra gruppeloven, at summen af de to punkter $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ er givet ved

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{hvor } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Opløftes dette i q'ende potens får vi, at

$$x_3{}^q = m'^2 - x_1{}^q - x_2{}^q, \quad y_3{}^q = m'(x_1{}^q - x_3{}^q) - y_1{}^q, \quad \text{hvor } m' = \frac{y_2{}^q - y_1{}^q}{x_2{}^q - x_1{}^q}.$$

Dette giver os, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$, hvilket netop er hvad ϕ_q skal opfylde for at være en homomorfi. I tilfældet hvor $x_1 = x_2$ har vi fra gruppeloven, at $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \infty$. Men hvis $x_1 = x_2$ må $x_1{}^q = x_2{}^q$ hvilket betyder, at $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \infty$. Så da $\infty^q = \infty$ (lægges ∞ sammen q gange er det stadigvæk ∞) får vi, at

$$\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2).$$

Hvis ét af punkterne er ∞, eksempelvis $(x_1, y_1) = \infty$, har vi fra gruppeloven, at $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = (x_2, y_2)$. Bruger vi igen, at $\infty^q = \infty$ følger det direkte, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$.

Når $(x_1, y_1) = (x_2, y_2)$ hvor $y_1 = 0$ er $(x_3, y_3) = (x_1, y_1) + (x_2, y_2) = \infty$. Når $y_1 = 0$ er $y_1{}^q = 0$ så $\phi_q(x_1, y_1) + \phi_q(x_2, y_2) = \infty$ og dermed er $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$.

Det resterende tilfælde er når $(x_1, y_1) = (x_2, y_2)$ og $y_1 \neq 0$. Fra gruppeloven har vi, at $(x_3, y_3) = 2(x_1, y_1)$, hvor

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{hvor } m = \frac{3{x_1}^2 + A}{2y_1}.$$

Som tidligere opløftes dette til den q'ende potens

$$x_3{}^q = m'^2 - 2{x_1}^q, \quad y_3{}^q = m'(x_1{}^q - x_3{}^q) - y_1{}^q, \quad \text{hvor } m' = \frac{3^q(x_1{}^q)^2 + A^q}{2^q {y_1}^q}.$$

Idet, at $2, 3, A \in \mathbb{F}_q$ følger det, at $2^q = 2, 3^q = 3$ og $A^q = A$. Vi står altså tilbage med formlen for fordoblingen af punktet $({x_1}^q, {y_1}^q)$ på den elliptiske kurve E.

Dermed har vi vist, at ϕ_q er en homomorfi for E. Da $\phi_q(x, y) = (x^q, y^q)$ er givet ved polynomier, som specielt er rationale funktioner, er ϕ_q en endomorfi. Den har tydeligvis grad q. Da $q = 0$ i $\mathbb{F}_q$ er den afledte af x^q lig nul, hvilket betyder at ϕ_q ikke er separabel. □

Bemærk, at da ϕ_q er en endomorfi for E er ${\phi_q}^2 = \phi_q \circ \phi_q$ det også og dermed også ${\phi_q}^n = \phi_q \circ \phi_q \circ \ldots \circ \phi_q$ for $n \geq 1$. Da multiplikation med -1 også er en endomorfi er ${\phi_q}^n - 1$ også en endomorfi for E.

Lemma 3. *Lad E være en elliptisk kurve over $\mathbb{F}_q$, og lad $(x, y) \in E(\overline{\mathbb{F}}_q)$. Da gælder der, at*

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$,
2. $(x, y) \in E(\mathbb{F}_q) \Leftrightarrow \phi_q(x, y) = (x, y)$.

Bevis. Vi har, at $y^2 = x^3 + ax + b$, hvor $a, b \in \mathbb{F}_q$. Vi opløfter denne ligning til den q'ende potens og får, at

$$(y^q)^2 = (x^q)^3 + (a^q x^q) + b^q,$$

hvor vi har brugt, at $(a+b)^q = a^q + b^q$ når q er en potens af legemets karakteristik (detaljer placeres i appendiks?). Men dette betyder netop, at $(x^q, y^q) \in E(\overline{\mathbb{F}}_q)$, hvilket viser (1). For at vise (2) husker vi, at $\phi_q(x) = x \Leftrightarrow x \in \mathbb{F}_q$. Det følger da, at

$$\begin{aligned}(x, y) \in E(\mathbb{F}_q) &\Leftrightarrow x, y \in \mathbb{F}_q \\ &\Leftrightarrow \phi_q(x) = x \text{ og } \phi_q(y) = y \\ &\Leftrightarrow \phi_q(x, y) = (x, y),\end{aligned}$$

hvilket fuldfører beviset for (2). □

Proposition 2. *Lad E være en elliptisk kurve over $\mathbb{F}_q$ og lad $n \geq 1$. Da gælder der, at*

1. $\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$.
2. *$\phi_q^n - 1$ er separabel, så $\#E(\mathbb{F}_{q^n}) = \deg(\phi_q^n - 1)$.*

Bevis. Da $(\phi_q^n - 1)(x, y) = 0 \Leftrightarrow (x^q, y^q) = (x, y)$ følger det fra lemma 3, at $\ker(\phi_q^n - 1) = E(\mathbb{F}_q)$. Da ϕ_q^n er Frobenius afbildningen for $\mathbb{F}_{q^n}$ følger (1) fra lemma 3. At $\phi_q^n - 1$ er separabel vil vi ikke vise, men et bevis kan findes i [LW]. Da følger det fra proposition 1, at $\#E(E_{q^n}) = \deg(\phi_q^n - 1)$. □

3.2 Hasses sætning

Med de foregående resultater er vi nu næsten klar til at vise Hasses sætning (sætning 2). Lad i det følgende afsnit

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{3.2}$$

Da skal vi vise, at $|a| \leq 2\sqrt{q}$ for at vise Hasses sætning. Først har vi dog følgende lemma

Lemma 4. *Lad $r, s \in \mathbb{Z}$ så $\gcd(s, q) = 1$. Da er*

$$\deg(r\phi_q - s) = r^2 q + s^2 - rsa.$$

Bevis. Vi vil ikke give beviset her, da det bygger på en række af tekniske resultater. Et bevis kan findes i [LW]. □

Nu er vi da i stand til, at gives beviset for Hasses sætning:

Bevis for Hasses sætning. Da graden af en endomorfi altid er ≥ 0 følger det fra lemma 4, at

$$r^2 q + s^2 - rsa = q\left(\frac{r^2}{s^2}\right) - \frac{rsa}{s^2} + 1 \geq 0,$$

for alle $r, s \in \mathbb{Z}$ med $\gcd(s, q) = 1$. Da mængden

$$\left\{\frac{r}{s} \mid \gcd(s, q) = 1\right\} \subseteq \mathbb{Q},$$

er tæt i $\mathbb{R}$ (se appendiks?) følger det, at $qx^2 - ax + 1 \geq 0$, for alle $x \in \mathbb{R}$. Dette medfører at diskrimanten må være negativ eller lig 0. Altså har vi, at

$$a^2 - 4q \leq 0 \Rightarrow |a| \leq 2\sqrt{q},$$

hvilket viser Hasses sætning. □

Eventuelt afsnit for torsionspunkter?

Følgende sætning følger også fra proposition 2, som vil vise sig at være nyttigt til at udvide resultatet fra Hasses sætning.

Sætning 3. *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Lad a være som i* (3.2)*. Da er a det entydige heltal så*

$$\phi_q{}^2 - a\phi_q + q = 0,$$

set som endomorfier. Med andre ord er a det entydige heltal sådan, at

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = \infty,$$

for alle $(x, y) \in E(\overline{\mathbb{F}}_q)$. Desuden er a det entydige heltal der opfylder, at

$$a \equiv \mathit{Trace}((\phi_q)_m) \pmod{m},$$

for alle m, hvor $\gcd(m, q) = 1$.

Før vi starter på beviset for sætning 3 skal vi først se på torsions punkterne for en elliptisk kurve. For en elliptisk kurve E givet over et legeme K lader vi

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}.$$

Det er altså de punkter, hvis orden er endelig (alle punkter over et endeligt legeme er torsions punkter).

Opskriv eventuelt sætning 3.2?

Lad da $\{\beta_1, \beta_2\}$ være en basis for $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$. Ethvert element fra $E[n]$ kan altså skrives som $\beta_1 m_1 + \beta_2 m_2$, hvor $m_1, m_2 \in \mathbb{Z}$ er entydige mod n. For en homomorfi $\alpha : E(\overline{K}) \to E(\overline{K})$ afbilleder α torsionspunkterne $E[n]$ til $E[n]$, derfor findes $a, b, c, d \in \mathbb{Z}$ sådan, at

$$\alpha(\beta_1) = a\beta_1 + b\beta_2, \quad \alpha(\beta_2) = c\beta_1 + d\beta_2.$$

Vi kan altså repræsentere en sådan homomorfi med matricen

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Bevis for sætning 3. Det følger direkte fra lemma 1, at hvis ${\phi_q}^2 - a\phi_q + q \neq 0$, altså hvis den ikke er nul-endomorfien, da er dens kerne endelig. Så hvis vi kan vise, at kernen er uendelig, da må endomorfien være lig 0.

Lad nu $m \geq 1$ være valgt sådan, at $\gcd(m, q) = 1$. Lad da $(\phi_q)_m$ være den matricen, som beskriver virkningen af ϕ_q på $E[m]$, som vi beskrev ovenfor. Lad da

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}.$$

Da $\phi_q - 1$ er separabel følger det fra proposition 1 og 3.15 (nævn resultat og henvis?, at

$$\begin{aligned} \#\ker(\phi_q - 1) &= \deg(\phi_q - 1) \equiv \det((\phi_q)_m - I) \\ &= \begin{vmatrix} s-1 & t \\ u & v-1 \end{vmatrix} \\ &= sv - tu - (s+v) + 1 \pmod{m}. \end{aligned}$$

Fra 3.15 (henvis, opskriv?) har vi, at $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. Fra (3.2) har vi, at $\#\ker(\phi_q - 1) = q + 1 - a$ så det følger, at

$$\mathrm{Trace}((\phi_q)_m) = s + v \equiv a \pmod{m}.$$

Idet vi husker, at $X^2 - aX + q$ er det karakteristiske polynomium for $(\phi_q)_m$ følger det fra Cayley-Hamiltons sætning fra lineær algebra, at

$${(\phi_q)_m}^2 - a(\phi_q)_m + qI \equiv I \pmod{m},$$

hvor I er 2×2 identitetsmatricen. Vi har da, at endomorfien ${\phi_q}^2 - a\phi_q + q$ er nul på $E[m]$. Da der er uendeligt mange muligheder for valget af m er kernen for $\phi^2 - a\phi_q + q$ uendelig. Dermed er endomorfien lig 0.

Mangler beviset for entydigheden af a. □

Endeligt vil vi vise en sætning, som gør det muligt at bestemme ordenen af en gruppe af punkter for en elliptisk kurve. Hvis vi kender ordenen af $E(\mathbb{F}_q)$ for et lille endeligt legeme gør følgende sætning det muligt, at bestemme ordenen af $E(\mathbb{F}_{q^n})$.

Sætning 4. *Lad $\#E(\mathbb{F}_q) = q + 1 - a$. Skriv $X^2 - aX + q = (X - \alpha)(X - \beta)$. Da er*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

for alle $n \geq 1$.

Vi har brug for, at $\alpha^n + \beta^n$ er et heltal, hvilket følgende lemma giver os:

Lemma 5. *Lad $s_n = \alpha^n + \beta^n$. Da er $s_0 = 2$, $s_1 = a$ og $s_{n+1} = as_n - qs_{n-1}$ for alle $n \geq 1$.*

Bevis. Bemærk først, at $s_0 = \alpha^0 + \beta^0 = 2$ og $s_1 = a$. Vi ser, at

$$(\alpha^2 - a\alpha + q)\alpha^{n-1} = \alpha^{n+1} - a\alpha^n + q\alpha^{n-1} = 0,$$

da α er en rod i $X^2 - aX + q$. Altså har vi, at $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. På samme måde har vi, at $\beta^{n+1} = a\beta^n - q\beta^{n-1}$, da β også er en rod. Lægges disse udtryk sammen får vi, at

$$\begin{aligned} s_{n+1} = \alpha^{n+1} + \beta^{n+1} &= a\alpha^n - q\alpha^{n-1} + a\beta^n - q\beta^{n-1} \\ &= a(\beta^n + \beta^n) - q(\alpha^{n-1} + \beta^{n-1}) \\ &= as_n - qs_{n-1}. \end{aligned}$$

Dermed er s_n et heltal for alle $n \geq 0$. □

Bevis for sætning 4. Lad nu

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Da deler $X^2 - aX + q = (X - \alpha)(X - \beta)$ polynomiet $f(X)$. Kvotienten er et polynomium $Q(X)$ med heltallige koefficienter, da $X^2 - aX + q$ er monisk og $f(X)$ har heltallige koefficienter (se appendiks). Derfor er

$$f(\phi_q) = (\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0, \tag{3.3}$$

som endomorfier for E pr. sætning 3. Idet vi husker, at $\phi_q^n = \phi_{q^n}$ giver sætning 3 også, at der findes entydigt $k \in \mathbb{Z}$ sådan at $\phi_{q^n}^2 - k\phi_q^n + q^n = 0$. Sådan et k

er givet ved $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$, og dette sammen med (3.3) giver os netop, at

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}),$$

hvilket netop var hvad vi ønskede at vise. □

Eksempel 3. Eksempel på 4.12 i aktion.

Kapitel 4

Faktoriseringsalgoritmer

I dette kapitel ønsker vi at se på faktoriseringsalgoritmer. Det viser sig nemlig, at en af de anvendelser som elliptiske kurver besidder, er indenfor faktoriseringen af heltal. Faktoriseringsproblemet, altså hvordan man bestemmer en faktor for et tal n er yderst relevant, da alle heltal kan faktoriseres:

Sætning 5 (Aritmetikkens fundamentalsætning)**.** *Et heltal $n > 1$ kan faktoriseres entydigt som et produkt af primtal, så hvis*

$$p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q,$$

hvor p_i og q_j er primtal for $1 \leq i \leq k$ og $1 \leq j \leq l$ er $k = l$ og $p_i = q_i$ for alle $i = 1, 2, \ldots, k$ (efter eventuelle ombytninger). Desuden er faktorerne $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ entydigt bestemte.

For et bevis af sætningen se f.eks. [1]. Det vigtige at bemærke er, at beviset ikke er konstruktivt og dermed ikke giver os en måde, hvorpå vi kan finde disse faktorer. Men hvordan kan vi så finde disse faktorer, som vi nu ved findes? Hvis vi har et sammensat tal n, som vi ønsker at faktorisere kunne vi angribe problemet med en naiv tilgang. Vi antager for nemhedens skyld at $n = pq$, hvilket gør det klart at $\min\{p, q\} \leq \sqrt{n}$. Vi kan altså finde en faktor ved at undersøge om først $2 \mid n$, dernæst om $3 \mid n$ osv. indtil at vi finder en faktor, hvilket vil ske senest når vi når til $\sqrt{n}$. Denne løsning er fin for tilstrækkeligt små tal, men det bliver hurtigt uoverkommeligt for store tal (eksempler på hvor lang tid det tager?).

Sikkerheden i moderne kryptosystemer hviler på det faktum, at det tager lang tid at faktorisere et heltal. Derfor er det interessant at undersøge om man gøre det hurtigere end den med den naive tilgang. Vi skal se på to af sådanne algoritmer, nemlig Pollards $p-1$ algoritme og Lenstras algoritme, som benytter elliptiske kurver til at finde en faktor. Idéen med begge algoritmer er at finde et $x \in \mathbb{Z}$ sådan, at $x \not\equiv 0 \pmod{n}$ og $x \equiv 0 \pmod{p}$ for en eller anden primfaktor p i n. Da har vi nemlig, at $\gcd(x, n)$ er en ikke-triviel divisor i n.

4.1 Pollards $p-1$ algoritme

Da Lenstras algoritme er stærkt inspireret af Pollards $p-1$ algoritme og devlist kan ses som værende en analog til denne, vælger vi at behandle den først. Pollards $p-1$ algoritme blev først præsenteret i [3] i 1970'erne af J. M. Pollard. Algoritmen er en måde hvorpå vi kan finde primfaktorer p for et heltal n når $p-1$ kun har *små* primfaktorer.

Vi ser nu på, hvordan Pollards $p-1$ algoritme prøver at finde en faktor. Lad n være et sammensat tal og lad p være en primfaktor i n. For $a \in \mathbb{Z}$ sådan at $\gcd(a,n) = 1$ har vi fra Fermats lille sætning, at

$$a^{p-1} \equiv 1 \pmod{p}.$$

Antag nu, at $p-1 \mid \mathrm{LCM}[1,2,\ldots,K] = k$ for et alle andet $K \in \mathbb{Z}^+$, hvor LCM er mindste fælles multiplum. Da har vi, at

$$a^k = a^{m(p-1)} = (a^{p-1})^m \equiv 1 \pmod{p}.$$

Lader vi $x = a^k - 1$ har vi nu, at $p \mid d = \gcd(x,n)$. Hvis nu $x \not\equiv 0 \pmod{n}$ er d en ikke-triviel divisor i n. Bemærk, at vi i de udregninger ikke har haft brug for at kende p. I praksis vil vi dog udregne $\gcd(x \pmod{n}, n)$ da vi ellers kan risikere at x bliver meget stort og besværligt at regne med, men det ændrer ikke på resultatet. Med den nu fundne faktor har vi en faktorisering $n = d \cdot \frac{n}{d}$ og vi kan gentage processen på disse to faktorer, hvis de ikke allerede er primtal.

Det hele hviler altså på, at n skal have en primfaktor p sådan, at

$$p-1 \mid \mathrm{LCM}[1,2,\ldots,K].$$

Dette vil der være stor sandsynlighed for, hvis $p-1$ har mange små primfaktorer. Vi er da klar til, at præsentere algoritmen, som er inspireret af gennemgangen af algoritmen i [4]:

Algoritme 1 (Pollards $p-1$ algoritme)**.** Lad $n \geq 2$ være et sammensat tal, som er tallet vi ønsker at finde en faktor for.

1. Vælg $k \in \mathbb{Z}^+$ sådan, at k er et produkt af mange små primtal opløftet i små potenser. Eksempelvis kan k vælges til at være

   $$k = \mathrm{LCM}[1,2,\ldots,K],$$

   for et $K \in \mathbb{Z}^+$ og hvor LCM er det mindste fælles multiplum.

2. Vælg et heltal a sådan, at $1 < a < n$.

3. Udregn $\gcd(a,n)$. Hvis $\gcd(a,n) > 1$ har vi fundet en ikke-triviel faktor for n og vi er færdige. Ellers fortsæt til næste trin.

4. Udregn $D = \gcd(a^k - 1 \pmod{n}, n)$. Hvis $1 < D < n$ er D en ikke-triviel faktor for n og vi er færdige. Hvis $D = 1$ gå da tilbage til trin 1 og vælg et større k. Hvis $D = n$ gå da til trin 2 og vælg et nyt a.

Denne version af algoritmen vil på et tidspunkt stoppe, da vi på et tidspunkt vil have at $K = \frac{1}{2}(p-1)$ i trin 1 for et eller andet $p \mid n$, hvilket betyder at $p - 1 \mid k$. Hvis der ikke bliver fundet en faktor før dette sker er algoritmen dog yderst ineffektiv og man vil i praksis kun teste til en fastsat grænse for K.

Følgende er et eksempel på anvendelsen af Pollards algoritme, hvor det går godt, altså hvor $p - 1$ har små primfaktorer:

Eksempel 4. Vi vil forsøge at faktorisere

$$n = 30042491.$$

Vi ser at $2^{n-1} = 2^{30042490} \equiv 25171326 \pmod{30042491}$, så N er ikke et primtal. Vi vælger som beskrevet i algoritmen

$$a = 2 \quad \text{og} \quad k = \text{LCM}[1, 2, \ldots, 7] = 420.$$

Da $420 = 2^2 + 2^5 + 2^7 + 2^8$ skal vi udregne 2^{2^i} for $0 \leq i \leq 8$. Dette resulterer i følgende tabel:

i	$2^{2^i} \pmod{n}$	i	$2^{2^i} \pmod{n}$
1	4	5	28933574
2	16	6	27713768
3	256	7	10802810
4	65536	8	16714289
5	28933574		

Denne tabel gør det forholdsvist let for os, at bestemme

$$\begin{aligned} 2^{420} &= 2^{2^2+2^5+2^7+2^8} \\ &\equiv 16 \cdot 28933574 \cdot 10802810 \cdot 16714289 \pmod{30042491} \\ &\equiv 27976515 \pmod{30042491}. \end{aligned}$$

Ved anvendelse af den euklidiske algoritme finder vi dernæst, at

$$\gcd(2^{420} - 1 \pmod{n}, n) = \gcd(27976514, 30042491) = 1.$$

Her fejler testen altså og vi er nået frem til, at n ikke har nogle primtalsfaktorer p sådan, at $p - 1$ deler 420. Algoritmen foreskriver da, at vi skal vælge et nyt k. Vi lader

$$k = \text{LCM}[1, 2, \ldots, 11] = 27720.$$

Da $27720 = 2^{14}+2^{13}+2^{11}+2^{10}+2^6+2^3$ skal vi udvide tabellen til at indeholde værdierne for 2^{2^i} for $0 \leq i \leq 14$:

i	$2^{2^i} \pmod n$	i	$2^{2^i} \pmod n$
9	19694714	12	26818902
10	3779241	13	8658967
11	11677316	14	3783587

Vi fortsætter på samme måde, som vi gjorde før og bestemmer

$$\begin{aligned} 2^{27720} &= 2^{2^3+2^{2^6}+2^{2^{10}}+2^{2^{11}}+2^{2^{13}}+2^{2^{14}}} \\ &= 256 \cdot 27713768 \cdot 3779241 \cdot 11677316 \cdot 8658967 \cdot 3783587 \\ &= 16458222 \pmod{30042491}. \end{aligned}$$

Vi finder dernæst, at

$$\gcd(2^{27720} - 1 \pmod n, n) = \gcd(16458221, 30042491) = 9241,$$

hvilket betyder at vi har fundet en ikke-triviel faktor for n. Mere præcist har vi fundet faktoriseringen

$$30042491 = 3251 \cdot 9241.$$

4.2 Lenstras elliptiske kurve algoritme

I [2] Lenstra præsenterede H. W. Lenstra en algoritme til faktorisering af heltal, som anvender elliptiske kurver. Vi skal arbejde med elliptiske kurver over $\mathbb{Z}/n\mathbb{Z}$, hvor n er et sammensat tal. Dette er dog ikke et legeme og derfor er $E(\mathbb{Z}/n\mathbb{Z})$ ikke en gruppe, da additionen ikke er defineret for alle punkter.

Lad n være et sammensat tal. Vi har, at inverserne til $x_1 - x_2$ og y_1 (se gruppeloven) kun findes modulo n, hvis (se bevis i appendiks)

$$\gcd(x_1 - x_2, n) = 1 \quad \text{og} \quad \gcd(y_1, n) = 1.$$

Men hvis vi er i stand til at finde punkter $P = (x_1, y_1)$ og $Q = (x_2, y_2)$ sådan, at summen $P + Q$ ikke er defineret, da er $\gcd(x, n) > 1$ hvor $x = x_1 - x_2$ eller $x = y_1$ og dermed har vi muligvis fundet en ikke-triviel faktor i n. Vores behandling af algoritmen her er inspireret af [4] og [5].

Vælg først tilfældige heltal $x, y, A \in [1, n]$ og lad da $B = y^2 - x^3 - Ax \pmod{n}$. Vi har da den elliptiske kurve (pseudo-kurve, da n er et sammensat tal)

$$E : y^2 = x^3 + Ax + B,$$

hvorpå vi har punktet $P = (x, y)$. Vi tjekker da, at $d = \gcd(4A^3+27B^2, n) = 1$. Hvis dette ikke er tilfældet og $1 < d < n$ har vi fundet en faktor i n. Hvis $d = n$ vælger vi et nyt A. For et heltal K lader vi $k = \text{LCM}[1, 2, \ldots, K]$ og vi forsøger da, at udregene

$$kP = \underbrace{P + P + \ldots + P}_{k \text{ led}}.$$

Det er ineffektivt at udregne $P + P + \ldots + P$ så vi gør ligesom i Pollards $p-1$ algoritme og skriver k som den binære udvidelse

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + k_3 \cdot 2^3 + \ldots + k_r \cdot 2^r,$$

hvor alle k_i er 0 eller 1. Vi kan da udregne

$$\begin{aligned} P_0 &= P \\ P_1 &= 2P_0 = 2P \\ P_2 &= 2P_1 = 2^2 P \\ &\vdots \\ P_r &= 2P_{r-1} = 2^r P. \end{aligned}$$

Da kan vi bestemme $kP =$ (summen af P_i'erne hvor $k_i = 1$). I hver udregning regner vi modulo n, da tallene ellers bliver alt for store og umulige at arbejde med. Vi håber på, at der i løbet af de udregninger er en addition, som ikke kan lade sig gøre og at dette giver os vores faktor. Vi opsummerer diskussionen i algoritmen nedenfor:

Algoritme 2 (Lenstras algoritme)**.** Lad $n \geq 2$ være et sammensat tal, som vi ønsker at finde en faktor for.

1. Vælg $x, y, A \in [1, n]$. Lad da $B = y^2 - x^3 - Ax \pmod{n}$ for da har vi den elliptiske kurve

$$E : y^2 = x^3 + Ax + B,$$

hvorpå punktet $P = (x, y)$ er placeret.

2. Tjek at $D = \gcd(4A^3 + 27B^2, n) = 1$. Hvis $D = n$ går vi tilbage til (1) og vælger et nyt b. Hvis $1 < D < n$ har vi fundet en faktor af n og vi er færdige.

3. Vælg et positivt heltal k som et produkt af mange små primtal, lad eksempelvis

$$k = \mathrm{LCM}[1, 2, 3, ..., K],$$

hvor $K \in \mathbb{Z}^+$.

4. Forsøg at bestemme $kP = P + P + \ldots + P$. Hvis udregningen kan lade sig gøre går vi tilbage til (1) og vælger en ny kurve, eller går til (3) og vælger et større k.

For at se hvorfor der er en god chance for, at vi støder på et valg af x, y, A sådan, at additionsloven bryder sammen lader vi p være en primfaktor i n. Beregningerne i diskussion af algoritmen blev alle lavet modulo n, men så gælder de også modulo p. Til den elliptiske kurve E har vi den abelske gruppe $E(\mathbb{F}_p)$ og pr. sætning 2 ved vi, at

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}.$$

En sætning af Deuring [DEURING] giver os endda, at for hvert heltal i intervallet findes $A, B \in \mathbb{F}_p$ sådan at $4A^3 + 27B^2 \neq 0$ og sådan at E har denne orden. Lad igen $k = \mathrm{LCM}[1, 2, \ldots, K]$ og antag, at $m \mid k$ for $m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$. Vi vil da vælge A, x og y indtil vi støder på en kurve E så $\#E(\mathbb{F}_p) = m$. Pr. Deurings sætning er der en positiv sandsynlighed for, at vi finder en kurve sådan at dette er tilfældet. Pr. Waterhouse og andre er der specielt god chance hvis $p - \sqrt{p} < m < p + \sqrt{p}$. Vi kan her bemærke, at i Pollards $p - 1$ algoritme var det nødvendigt, at $m \mid k$, men der kunne vi kun vælge m sådan at $m = p - 1$.

Antag da, at $\#E(\mathbb{F}_p) \mid k$ og at vi var i stand til at udregne kP, samt at $kP \neq \mathcal{O}$ på $E(\mathbb{Z}/n\mathbb{Z})$. Lad $P + Q = kP$ være den sidste addition, hvor $P = (x_1, y_1)$ og $Q = (x_2, y_2)$ begge er forskellige fra $\mathcal{O}$. Da er $P+Q = kP = \mathcal{O}$ på $E(\mathbb{F}_p)$ og vi har, at

$$x_1 \equiv x_2 \pmod{p}, \quad y_1 \equiv -y_2 \pmod{p},$$

hvilket videre giver os, at

$$p \mid \gcd(x_1 - x_2, n), \quad p \mid \gcd(y_1 + y_2, n).$$

Men så er $P+Q$ ikke defineret på $E(\mathbb{Z}/n\mathbb{Z})$, men dette er i modstrid med vores antagelse. Vi har altså enten, at $kP = \mathcal{O}$ på $E(\mathbb{Z}/n\mathbb{Z})$ eller at vi i forsøget på at udregne kP i $E(\mathbb{Z}/n\mathbb{Z})$ vil støde på to punkter, hvis sum ikke er defineret, hvilket med lidt held så resulterer i en ikke-triviel faktor i n.

Med algoritmen på plads kan vi nu se på et eksempler:

Eksempel 5. Lad nu

$$n = 753161713$$

være det tal, som vi ønsker at faktorisere. Da $2^{n-1} = 437782651 \pmod{n}$ er n ikke et primtal. Vi vælger da $x = 0$, $y = 1$ og $A = 164$. Vi har dermed, at $B = 1^2 - 0^3 - 164 \cdot 0 = 1$ og den elliptiske kurve vi vil arbejde over bliver

$$E : y^2 = x^3 + 164x + 1,$$

hvorpå punktet $P = (0, 1)$ er placeret. Vi ser, at

$$\begin{aligned} D &= \gcd(4 \cdot 164^3 + 27 \pmod{753161713}, 753161713) \\ &= \gcd(17643803, 753161713) = 1, \end{aligned}$$

så vi fortsætter derfor med algoritmen. Vi lader

$$k = \mathrm{LCM}[1, 2, \ldots, 10] = 2520.$$

Da $2520 = 2^{11} + 2^8 + 2^7 + 2^6 + 2^4 + 2^3$ skal vi beregne $2^i P \pmod{753161713}$ for $0 \leq i \leq 11$. Dette gøres med additionsformlen og vi opsummerer vores resultater i tabellen nedenfor:

i	$2^iP \pmod{753161713}$	i	$2^iP \pmod{753161713}$
0	$(0, 1)$	6	$(743238772, 703386057)$
1	$(6724, 752610344)$	7	$(309161840, 219780637)$
2	$(293427237, 450490340)$	8	$(116974611, 722899047)$
3	$(468952095, 385687511)$	9	$(329743899, 182819134)$
4	$(288125200, 446796094)$	10	$(163952469, 456288424)$
5	$(106753239, 115973502)$	11	$(15710788, 301760412)$

Vi kan nu addere disse punkter igen vha. additionsformlerne, hvor vi stadigvæk regner modulo n:

$$(2^3 + 2^4)P = (606730980, 447512524).$$

Algoritmen giver os en faktor netop når additionen bryder sammen, hvilket kan ske da $\mathbb{Z}/n\mathbb{Z}$ ikke er et legeme. Dette problem viser sig i dette eksempel allerede ved den næste addition, hvor vi forsøger at udregne

$$\begin{aligned}(2^3 + 2^4 + 2^6)P = &(743238772, 703386057)\\ &+(606730980, 447512524) \pmod{n}.\end{aligned}$$

For at denne addition skal kunne lade sig gøre, skal differensen af deres x-koordinater have en invers modulo n. Dette er kun tilfældet, hvis $\gcd(x_2 - x_1, n) = 1$ (se appendiks, sætning k). Men vi ser, at

$$\gcd(606730980 - 743238772, 753161713) = 19259,$$

så der findes altså ikke en invers, men vi har i stedet fundet en faktor i n. Dermed har vi faktoriseringen

$$753161713 = 19259 \cdot 39107.$$

Nu kan det virke til, at det var spild da vi lavede hele tabellen, men i beregningerne af $2^i P \pmod{753161713}$ ville vi også kunne have løbet ind i et element, som ikke havde en invers og som dermed kunne give os en faktor.

Bilag A

Appendiks

Her samler vi nogle af de (hovedsagligt) mindre resultater, som benyttes igennem kapitlerne. De præsenteres her kort og henvises til i opgaven, når de er blevet anvendt.

Proposition 3. *Et element $a \in \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ har ikke en invers i $\mathbb{Z}_n$ hvis* $\gcd(a, n) > 1$.

Bevis. Antag for modstrid, at $d = \gcd(a, n) > 1$, men at der samtidigt eksisterer en invers c til a modulo n. Da $d = \gcd(a, n)$ findes et heltal e, som ikke er nul, sådan at $de = n$. Da $d > 1$ har vi også, at $|e| < |n|$ så e er ikke nul modulo n. Da d deler a har vi, at $n = de$ deler ae så $ae = 0 \pmod{n}$. Vi har altså, at

$$e = e \cdot 1 = eac = 0 \cdot c = 0 \pmod{n},$$

hvilket er i modstrid med at e ikke kunne være 0 modulo n. Altså har a ikke en invers når $\gcd(a, n) > 1$. □

Vi giver nu beviset for sætning **??**:

Bevis for Fermats lille sætning. Vi ser først på de $p-1$ positive multipla af a

$$a, 2a, \ldots, (p-1)a. \tag{A.1}$$

Hvis $ra = sa \pmod{p}$ har vi, at $r = s \pmod{p}$, så elementerne listet i (A.1) er forskellige og ikke-nul. De må altså være kongruente til $1, 2, \ldots, p-1$ men ikke nødvendigvis i den opskrevne rækkefølge. Ganger vi elementerne sammen må de to kongruenser være de samme, altså er

$$a \cdot 2a \cdots (p-1)a = 1 \cdot 2 \cdots (p-1) \pmod{p},$$

hvilket giver os, at

$$a^{p-1}(p-1)! = (p-1)! \pmod{p} \Rightarrow a^{p-1} = 1 \pmod{p}.$$

□

Bibliografi

[1] Johan P. Hansen. *Algebra og talteori*.

[2] H. W. Lenstra Jr. „Factoring Integers with Elliptic Curves". I: *The Annals of Mathematics, Second Series,* 126 (03 nov. 1987), s. 649–673.

[3] J. M. Pollard. „Theorems on factorization and primality testing". I: *Mathematical Proceedings of the Cambridge Philosophical Society* 76 (03 okt. 1974), s. 521–528.

[4] Joseph H. Silverman. *Rational Points on Elliptic Curves*.

[5] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*.