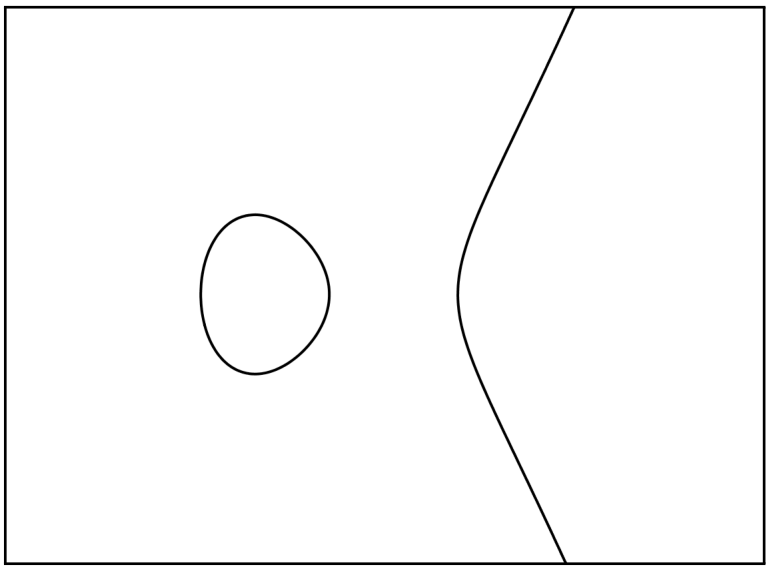
Elliptiske Kurver
&
Primtalsfaktorisering

(Elliptic curves and prime factorization)



Bachelorprojekt i matematik

Jakob Krejberg Ørhøj — 20104919

Vejleder: Johan P. Hansen

28. juli 2013

Institut for Matematik
Aarhus Universitet

Abstract

We present the group structure that arises on elliptic curves over fields. We study endomorphisms on elliptic curves, specifically the Frobenius endomorphism over finite fields $\mathbb{F}_q$ is of our interest. We use these endomorphisms to prove Hasse's theorem that gives a bound on the order of the group $E(\mathbb{F}_q)$, and a theorem that makes it possible to determine the order of $E(\mathbb{F}_{q^n})$ when the order of $E(\mathbb{F}_q)$ is known. Lastly we present two factoring algorithms, Pollards $p-1$ algorithm and Lenstras elliptic curve method, where the latter exploits the group structure on elliptic curves to factor integers.

Indholdsfortegnelse

1 Indledning

Denne opgave omhandler elliptiske kurver, en specifik form for algebraiske kurver, som har nogle interessante egenskaber. Vi viser at gruppen af punkter på en elliptisk kurve, sammen med et såkaldt punkt i uendelig, under en geometrisk defineret addition giver os en abelsk gruppe. Dette resultat åbner for en rig teori, hvor vi først undersøger endomorfier for elliptiske kurver. Specielt ser vi på Frobenius endomorfien, som vi benytter til at bevise Hasses sætning, der begrænser antallet af punkter på en elliptisk kurve over et endeligt legeme $\mathbb{F}_q$. Vi viser desuden en sætning, som gør det muligt for os, at bestemme ordenen af $E(\mathbb{F}_{q^n})$ hvis blot vi kender ordenen af $E(\mathbb{F}_q)$.

Vi ser på en praktisk anvendelse af elliptiske kurver over endelige legemer idet, at man kan udnytte dem til primtalsfaktorisering. Vi beskriver først Pollards $p-1$ algoritme da den var inspirationen til den anden algoritme vi ser, nemlig Lenstras elliptiske kurve algoritme. Der er blevet udviklet et program, som demonstrerer disse algoritmer som kan findes på:

`http://orhoj.com/bachelor/factorization.zip`

I filen er vedlagt kildekoden og en eksekverbar fil `factorization.jar`, som skulle kunne afvikles direkte, hvis den nyeste version af Java er installeret. Man kan passende bruge programmet sideløbende med eksemplerne i kapitel 5. I tilfælde af at ovenstående link ikke virker findes en kopi også på

`http://daimi.au.dk/~jakkrej/bachelor/factorization.zip`

Ellers kan man ved henvendelse til `jakobii@msn.com` få tilsendt en kopi.

Inden vi for alvor går i gang vil jeg gerne takke Johan P. Hansen for både god vejledning og hyggelige samtaler under hele forløbet.

2 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.

2.1 Definition af elliptiske kurver

Det er muligt at definere elliptiske kurver på flere måder. For et legeme K vil følgende definition være tilstrækkelig til vores formål:

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

$$y^2 = x^3 + Ax + B, \tag{2.1}$$

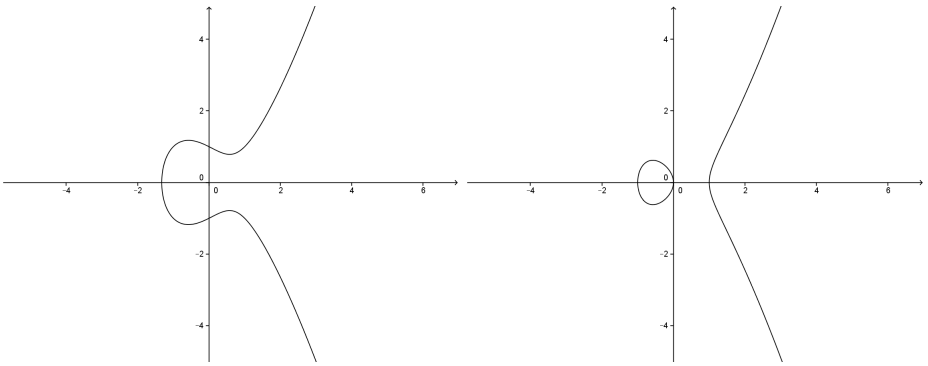
hvor $A, B \in K$ er konstanter og $4A^3 + 27B^2 \neq 0$.

Vi siger, at den elliptiske kurve E er på Weierstrass normalform, når den kan beskrives som i (2.1). Hvis $\text{char}(K) \neq 2, 3$ er det altid muligt, at omskrive en elliptisk kurve til Weierstrass normalform (se [8, kapitel 2]). Det kan vises, at diskriminanten for (2.1) er

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

så en elliptisk kurve kan ikke have multiple rødder pr. kravet i definitionen. I figur 2.1 ses to eksempler på elliptiske kurver over de reelle tal. Definitionen siger, at A og B skal tilhøre et legeme K. Det kunne f.eks. være $\mathbb{R}, \mathbb{C}$ eller $\mathbb{Q}$. Vi vil dog dog fokusere på de endelige legemer $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ hvor p er et primtal, og de endelige legemer med q elementer $\mathbb{F}_q$, hvor $q = p^r$ for $r \geq 1$ (se appendiks A.1). Hvis $A, B \in K$ for en elliptisk kurve E siger vi, at E er givet over K. Fremover menes en elliptisk kurve på Weierstrass normalform, når vi snakker om en elliptisk kurve E. Punkterne på en elliptisk kurve med koordinater i et legeme $L \supseteq K$ skriver vi som $E(L)$, hvor

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}. \tag{2.2}$$



Figur 2.1: Eksempler på elliptiske kurver over $\mathbb{R}$. Venstre: $y^2 = x^3 - x$, Højre: $y^2 = x^3 - x + 1$

Punktet ∞ kaldes punktet i uendelig og viser sig nødvendigt for at $E(L)$ bliver en gruppe under additionen vi introducerer 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, hvilket betyder at to lodrette linjer skærer 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 punktet ∞ i toppen og i bunden er et og samme punkt.

2.2 Den projektive plan

Vi vil i dette afsnit formalisere punktet ∞, som vi kort diskuterede ovenfor. For atk unne gøre dette får vi brug for den projektive plan $\mathbb{P}^2$. Rent intuitivt kan man se den 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. Den projektive plan er da givet ved

$$\mathbb{P}^2(K) = \{(x, y, z) \in K^3 \mid (x, y, z) \neq (0, 0, 0)\}/\sim .$$

I de tilfælde hvor $z \neq 0$ har vi, at

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

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 inklusion $\mathbb{A}^2(K) \hookrightarrow \mathbb{P}^2(K)$ givet ved

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

Dette kan vi selvfølgelig ikke gøre, når $z = 0$ og når dette er tilfældet ser vi det som, at enten x eller y-koordinaten er ∞. Vi kalder dermed punkterne $(x, y, 0)$ for punkterne i uendelig og punktet ∞ på en elliptisk kurve vil vi identificere med netop ét af disse.

Et polynomium siges at være homogent af grad n, hvis det er summen af led på formen $ax^i y^j z^k$, hvor $a \in K$ og $i + j + k = n$. Eksempelvis er

$$F(x, y, z) = 5x^4 - 2x^2yz + 7yz^3$$

et homogent polynomium af grad 4. For et homogent polynomium F af grad n er

$$F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z), \quad \lambda \in K.$$

Vi har altså, at når $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ er $F(x_1, y_1, z_1) = 0$ hvis og kun hvis $F(x_2, y_2, z_2) = 0$. Et nulpunkt for F i $\mathbb{P}^2(K)$ er altså ikke afhængig af repræsentanten for en given ækvivalensklasse, hvilket betyder at nulpunkterne for F er veldefineret i $\mathbb{P}^2(K)$.

For et arbitrært polynomium $F(x, y, z)$ giver det ikke mening, at snakke om et punkt i $\mathbb{P}^2(K)$ hvor $F(x, y, z) = 0$, da det nemlig afhænger af repræsentanten (x, y, z) for ækvivalensklassen. Vi har f.eks., at for $F(x, y, z) = 2x^2 - y - z$ at $F(1, 1, 1) = 0$, men $F(2, 2, 2) = 4$. Men da $(1 : 1 : 1) = (2 : 2 : 2)$ har vi et problem, som vi undgår ved at arbejde med homogene polynomier i stedet. For et polynomium $f(x, y)$ kan vi homogenisere det ved, at indsætte de korrekte potenser af z. F.eks. for $f(x, y) = y^2 - x^3 - Ax - B$ har vi, at $F(x, y) = y^2z - x^3 - Axz^2 - Bz^3$. Generelt for et polynomium $f(x, y)$ har vi at, hvis

$$f(x, y) = \sum_i a_i x^{p_i} y^{q_i},$$

hvor $\max\{p_i + q_i\} = n$, er dets homogene form

$$F(x, y, z) = \sum_i a_i x^{p_i} y^{q_i} z^{n - p_i - q_i}.$$

Dermed har vi, at

$$\begin{aligned} F(x, y, z) &= z^n \sum_i a_i x^{p_i} z^{-p_i} y^{q_i} z^{-q_i} = z^n \sum_i a_i \left(\frac{x}{z}\right)^{p_i} \left(\frac{y}{z}\right)^{q_i} \\ &= z^n f\left(\frac{x}{z}, \frac{y}{z}\right). \end{aligned}$$

Da er det klart, at

$$f(x, y) = F(x, y, 1).$$

Vi er nu i stand til at undersøge, hvad det vil sige for to parallelle linjer at mødes i uendelig. Lad først

$$y = mx + b_1, \quad y = mx + b_2,$$

være to linjer, som ikke er lodrette og hvor $b_1 \neq b_2$. Homogeniserer vi dem, som forklaret ovenfor, får vi

$$y = mx + b_1 z, \quad y = mx + b_2 z.$$

Trækker vi ligningerne fra hinanden får vi, at

$$0 = (b_1 - b_2)z \Rightarrow z = 0,$$

hvilket så betyder, at $y = mx$. Da vi ikke kan have, at både x, y og z er 0 samtidigt må vi have $x \neq 0$. Vi kan da dele med x og vi får, at skæringen er

$$(x : mx : 0) = (1 : m : 0).$$

Dette er et af punkterne i uendelig fra $\mathbb{P}^2(K)$. På samme måde har vi, at hvis $x = c_1$ og $x = c_2$ er lodrette linjer, at de skærer hinanden i punktet $(0 : 1 : 0)$. Dette er også ét af de punkter, som vi identificerede som værende et punkt i uendelig i $\mathbb{P}^2(K)$.

Hvis vi nu homogeniserer ligningen for en elliptisk kurve E med variablen z får vi, at

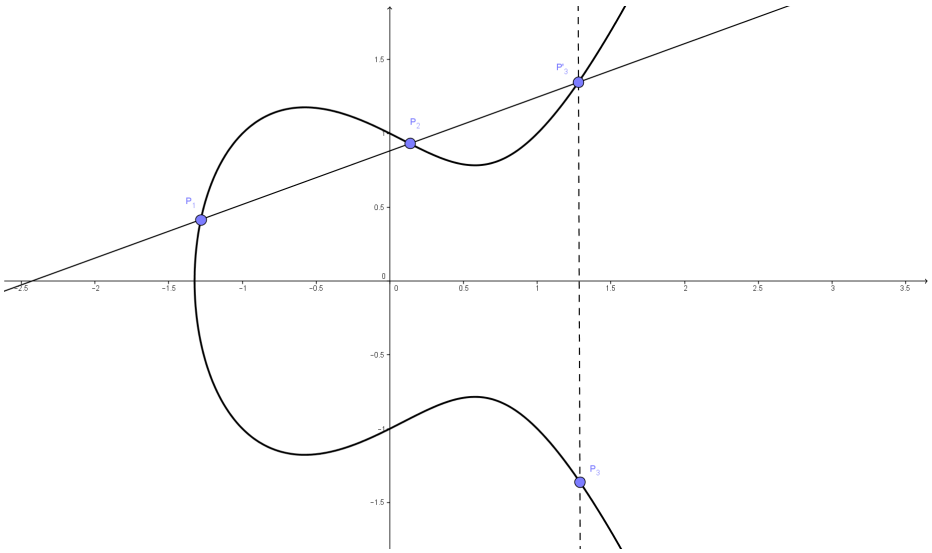
$$y^2 z = x^3 + Axz^2 + Bz^3.$$

For at se hvilke punkter i uendelig, som er på E sætter vi $z = 0$. Dette giver os, at $0 = x^3$ hvilket har en tredobbelt rod i $x = 0$ og y kan være et hvilket som helst tal som ikke er 0, da vi ikke kan have $(0 : 0 : 0)$. Efter en skalering med y har vi $(0 : y : 0) = (0 : 1 : 0)$ så $(0 : 1 : 0)$ er det eneste punkt i uendelig på E. Da $(0 : 1 : 0)$ er et punkt på enhver lodret linje skærer enhver lodret linje E i dette punkt i uendelig. Vi har desuden, da $(0 : 1 : 0) = (0 : -1 : 0)$, at punkterne i uendelig i toppen og bunden af y-aksen er de samme.

Vi vil dog her foretrække, at arbejde med affine koordinater, hvor punktet ∞ behandles som et specialtilfælde, men vi har nu givet konkret mening til punktet ∞.

2.3 Gruppeloven

Lad E være en elliptisk kurve over et legeme 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



Figur 2.2: Addition af to punkter på en elliptisk kurve

dette afsnit vise, hvordan dette gøres og til slut konkludere, at defineres dette som en additions 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 $x_1 \neq x_2$, vi har da

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

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

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

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 $P_1 + P_2 = P_3 = (x, y)$. 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 $P_1 = P_2 = (x_1, y_1)$ kræver lidt flere overvejelser. For to punkter som ligger tæt på hinanden vil linjen igennem punkterne nærme sig tangenten til et af punkterne. Når vi har to ens punkter lader vi da linjen igennem dem være tangenten til punktet. Ved implicit differentiation finder vi, at

$$2y\frac{dy}{dx} = 3x^2 + A, \quad \text{så} \quad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

Hvis $y_1 = 0$ er linjen lodret og i det tilfælde lader vi $P_1 + P_2 = \infty$. Antag altså, at $y_1 \neq 0$. Ligningen for L er

$$y = m(x - x_1) + y_1,$$

som før. Vi får den kubiske ligning

$$0 = x^3 - m^2x^2 + \dots$$

Vi kender dog kun én rod, x_1, men den er en dobbelt rod idet at L er tangent til E i P_1. Så på samme måde som før får vi, at

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

Antag nu, at $P_2 = \infty$. Linjen som går igennem P_1 og ∞ er en lodret linje, som skærer E i reflektionen af P_1 over x-aksen. Når vi reflekterer dette punkt igen over x-aksen får vi igen P_1. Altså har vi, at

$$P_1 + \infty = P_1.$$

Denne definition udvides sådan, at $\infty + \infty = \infty$.

Det er nu mere klart, hvorfor elliptiske kurver og denne definition for en addition passer sammen. Højresiden i en ligning på Weierstrass normalform er kubisk så en linje igennem to punkter skærer den i et tredje punkt. At venstresiden er y^2 sikrer os, at kurven er symmetrisk om x-aksen, som benyttes når vi reflekterer et punkt. Vi opsummerer denne diskussion og kan opstille gruppeloven:

Definition 2 (Gruppeloven) *Lad E være en elliptisk kurve. Givet to punkter, $P_1, P_2 \in E(K)$, $P_i = (x_i, y_i)$, findes et tredje punkt $P_3 = P_1 + P_2 = (x_3, y_3)$ da som følger*

1. *Hvis $x_1 \neq x_2$ 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 $P_1 + P_2 = \infty$.*

3. *Hvis $P_1 = P_2$ og $y_1 \neq 0$ 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 $P_1 + P_2 = \infty$.*

Vi definerer desuden, at

$$P + \infty = \infty,$$

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

Det måske overraskende hovedresultatet i dette kapitel er, at denne addition resulterer i en abelsk gruppe:

Sætning 1 *Punkterne på E, altså $E(K)$, udgør en additiv abelsk gruppe hvor ∞ er identiteten og additionen er som defineret i gruppeloven.*

Bevis. For at være en gruppe skal additionen af punkter være kommutativ, der skal eksistere en identitet, hvert element skal have en invers og additionen af punkter skal være associativ.

Kommutativiteten kan enten ses direkte fra formlerne eller fra det faktum, at linjen igennem P_1 og P_2 er den samme som linjen igennem P_2 og P_1. At ∞ er identiteten følger pr. definitionen af denne. For de inverse elementer lader vi P' være reflektionen af P, da er $P + P' = \infty$. Associativiteten kan vises direkte ud fra formlerne, men der er mange tilfælde der skal behandles, hvilket gør det besværligt. Et bevis for associativiteten kan findes i [8, afsnit 2.4] eller i [7]. □

3 Endomorfier

Vi vil i dette kapitel etablere nogle vigtige resultater vedrørende endomorfier på elliptiske kurver, som vi bl.a. vil benytte i beviset for Hasses sætning.

3.1 Endomorfier på elliptiske kurver

Lad K være et legeme og $\overline{K}$ en tilhørende algebraisk aflukning. I det følgende vil vi med en elliptisk kurve E mene en kurve på formen $y^2 = x^3 + Ax + B$. 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 specialt 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 $(x, y) \in E(\overline{K})$ 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 2 *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 $y^2 = x^3 + Ax + B$. Dette medfører, 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

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}. \tag{3.1}$$

Vi kan endda gøre det endnu simplere ved at gange udtrykket i (3.1) med $p_3(x) - p_4(x)$, hvilket gør at vi i nævneren får

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

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

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{3.2}$$

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 (3.2) 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 og vi har det ønskede. □

Vi viser da lemmaet, som blev benyttet i beviset ovenfor. Bemærk, at hvis to polynomier har en fælles rod må de nødvendigvis have en fælles faktor.

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

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

så $p(x_0) = 0$. 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

$$(x^3 + Ax + B)s(x)^2 q(x)^3 = u(x)t(x)^2. \tag{3.3}$$

Hvis $q(x_0) = 0$ følger det direkte fra (3.3), 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 (3.3), at

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

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 $(x - x_0)$ deler $(x^3 + Ax + B)$. 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 (3.3) kan da skrives, som

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

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

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

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

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

men da $Q(x_0) \neq 0$ og $s(x_0) \neq 0$ må $q(x_0)^3 = 0$, hvilket i sidste ende giver os, at $q(x_0) = 0$. □

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 $r_1'(x) \neq 0$.

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 $p'q - pq'$ (tælleren af r_1') ikke nulpolynomiet. Lad nu

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

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. $(a, b) \in \alpha(E(\overline{K}))$.

Vi skal da argumentere for, at sådan et punkt findes. Da $\overline{K}$ er algebraisk lukket er $E(\overline{K})$ en uendelig mængde og vi kan derfor undgå de punkter, hvor $a = 0, b = 0$ eller $(a, b) = \infty$. Lad

$$p(x) = cx^n + (\text{led af lavere orden}), \quad q(x) = dx^m + (\text{led af lavere orden}).$$

Hvis $\deg p > \deg q$ er $n > m$ og dermed er $\deg(p - aq) = n$ som påkrævet. På samme måde gælder det hvis $\deg q > \deg p$. Hvis $n = m$ er (ii) ikke opfyldt når $c - ad = 0$, men i dette tilfælde kan vi gange a med et heltal større end 1 og finde et punkt hvor (ii) er opfyldt. Da $p'q - pq'$ 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 vil vise, at der findes netop $\deg \alpha$ punkter $(x_1, y_1) \in E(\overline{K})$ sådan at

$$\alpha(x_1, y_1) = (a, b).$$

Det er velkendt fra gruppeteorien, at $\alpha^{-1}(\alpha(x_1, y_1)) = (x_1, y_1) \ker \alpha$, så dette vil medføre at $\ker \alpha$ har $\deg \alpha$ elementer. 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

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

da hvis x_0 er en multipel rod er den også rod i den afledte. 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 $p'q - pq'$ 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.

Hvis α ikke er separabel kan det samme bevis anvendes, hvor $p' - aq'$ dog altid er nulpolynomiet så $p - aq(x) = 0$ har altid multiple rødder, så den har færre end $\deg \alpha$ løsninger. □

Sætning 3 *Lad E være en elliptisk kurve over et legeme K. Lad $\alpha \neq 0$ være en endomorfi for E. Da er $\alpha : E(\overline{K}) \to E(\overline{K})$ surjektiv.*

Bevis. Lad $(a, b) \in E(\overline{K})$. Vi vil vise, at der findes et punkt $(x, y) \in E(\overline{K})$ sådan, at $\alpha(x, y) = (a, b)$. Da $\alpha(\infty) = \infty$ kan vi antage, at $(a, b) \neq \infty$. Lad $r_1(x) = p(x)/q(x)$. Vi skal betragte to tilfælde:

Hvis $p(x) - aq(x)$ ikke er et konstant polynomium har det en rod x_0. Hvis vi nu har, at $q(x_0) = 0$ må $p(x_0) = 0$, hvilket er i modstrid med at p og q ikke har nogen fælles rødder. Derfor har vi $q(x_0) \neq 0$ og det følger, at

$$p(x_0) - aq(x_0) = 0 \Rightarrow a = \frac{p(x_0)}{q(x_0)}.$$

Vælg nu $y_0 \in E(\overline{K})$ som en af kvadratrødderne af $x_0^3 + Ax_0 + B$. Da er $\alpha(x_0, y_0)$ defineret og $\alpha(x_0, y_0) = (a, b')$ for et b'. Da

$$(b')^2 = a^3 + Aa + B = b^2,$$

er $b = \pm b'$. Hvis $b' = b$ er vi færdige. Hvis $b' = -b$ har vi, at

$$\alpha(x_0, -y_0) = (a, -b') = (a, b).$$

Vi mangler nu, at betragte tilfældet hvor $p(x) - aq(x)$ er konstant. Da $E(\overline{K})$ er uendelig og $\ker \alpha$ er endelig afbilledes kun endeligt mange punkter fra $E(\overline{K})$ til en given x-koordinat. Derfor må enten $p(x)$ eller $q(x)$ være ikke-konstant, da hvis de begge var konstante ville der være uendeligt mange punter fra $E(\overline{K})$ der afbilledes til en x-koordinat. Hvis p og q er to ikke-konstante polynomier er der højest én konstant a sådan at $p - aq$ er konstant, da vi ellers for en anden sådan konstant a' har, at

$$(a' - a)q = (p - aq) - (p - a'q), \quad (a' - a)p = a'(p - aq) - a(p - a'q),$$

hvor begge ligninger er konstante, som medfører at p og q er konstante. Så der er højest to punkter (a, b) og $(a, -b)$ som ikke er i billedet af α. Lad (a_1, b_1) være et andet punkt end disse. Da er $\alpha(P_1) = (a_1, b_1)$ for et punkt P_1. Vi kan vælge (a_1, b_1) sådan, at $(a_1, b_1) + (a, b) \neq (a, \pm b)$, så der findes et punkt P_2 sådan, at $\alpha(P_2) = (a_1, b_1) + (a, b)$. Dermed har vi, at

$$\alpha(P_2 - P_1) = (a, b) \quad \text{og} \quad \alpha(P_1 - P_2) = (a, -b).$$

Vi har da ramt alle punkter, så α er surjektiv. □

Dette bevis konkluderer vores undersøgelse af endomorfier på generelle legemer K. Vi vil i kapitel 4 fortsat behandle endomorfier, men der vil det være for endelige legemer.

4 Elliptiske kurver over endelige legemer

Vi skal i dette kapitel betragte elliptiske kurver over endelige legemer. Lad $\mathbb{F}$ være et endeligt legeme og lad E være en elliptisk kurve over $\mathbb{F}$. Da er gruppen $E(\mathbb{F})$ endelig, da der kun findes endeligt mange talpar (x, y) hvor $x, y \in \mathbb{F}$. Et endeligt legeme har p^n elementer for et primtal p, hvor $n \geq 1$ (se bilag A.1). Derfor lader vi $\mathbb{F}_q$ være det endelige legeme med $q = p^n$ elementer.

Vi vil vise Hasses sætning, som giver os en vurdering på antallet af punkter i gruppen $E(\mathbb{F}_q)$. Denne vurdering viser sig, at have en anvendelse indenfor heltalsfaktorisering, som vi ser på i kapitel 5. Vi ser også på en måde, hvorpå vi kan bestemme den eksakte orden af en gruppe $E(\mathbb{F}_{q^n})$, hvis vi kender ordenen af $E(\mathbb{F}_q)$, som er let at bestemme for legemer med få elementer.

4.1 Eksempler

Lad E være en elliptisk kurve på formen

$$E : y^2 = x^3 - x,$$

defineret over $\mathbb{F}_5$. Da er gruppen $E(\mathbb{F}_5)$ endelig, som nævnt ovenfor. For at bestemme den eksakte orden af $E(\mathbb{F}_5)$ laver vi en tabel over alle mulige værdier for x, $x^3 - x \pmod 5$ og for kvadratrødderne y af $x^3 - x \pmod 5$. 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	–	–
∞		∞	∞

Vi kan da tælle punkterne og vi ser, at $E(\mathbb{F}_5)$ har orden 7, hvilket vi skriver som $\#E(\mathbb{F}_5) = 7$. Bemærk at $\sqrt{2} \notin \mathbb{Z}_5$, hvilket er hvorfor der ikke er en tilhørende værdi for y til $x = 4$.

Additionen af punkterne på en sådan kurve over et endeligt legeme foretages på samme måde, som i formlerne i gruppeloven, men de foretages modulo p. Eksempelvis hvis vi ville bestemme $(1,0)+(3,3)$ får vi, at

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3-0}{3-1} = \frac{3}{2} \equiv 4 \pmod 5.$$

Dermed har vi, at

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 = 4^2 - 1 - 3 = 12 \equiv 2 \pmod 5, \\ y_3 &= m(x_1 - x_3) - y_1 = 4(1-2) - 0 = -4 \equiv 1 \pmod 5. \end{aligned}$$

Vi får altså punktet

$$(1,0) + (3,3) = (2,1),$$

som netop er ét af punkterne vi har opgivet i tabellen.

4.2 Frobenius endomorfien

I det forrige kapitel så vi på endomorfier for generelle legemer. Nu vil vi se på en endomorfi som er defineret over endelige legemer, som viser sig at have en kritisk rolle i vores bevis for Hasses sætning. Denne endomorfi er Frobenius endomorfien ϕ_q. For en elliptisk kurve E over et endeligt legeme $\mathbb{F}_q$ er denne givet ved

$$\phi_q(x,y) = (x^q, y^q), \quad \phi_q(\infty) = \infty. \tag{4.1}$$

Vi skal nu vise nogle af de egenskaber, som denne endomorfi besidder:

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

Vi skal bruge, at $(a+b)^q = a^q + b^q$ når $q = p^n$ hvor p er et primtal (se appendiks A.1).

Bevis. Vi vil først 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 $x_1 \neq x_2$. Det følger da fra gruppeloven, at summen af de to punkter $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ er givet ved

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2, \\ y_3 &= m(x_1 - x_3) - y_1, \end{aligned}$$

hvor $m = (y_2 - y_1)/(x_2 - x_1)$. Opløfter vi til q'ende potens får vi videre, at

$$\begin{aligned} x_3^q &= m'^2 - x_1^q - x_2^q, \\ y_3^q &= m'(x_1^q - x_3^q) - y_1^q, \end{aligned}$$

hvor $m' = (y_2^q - y_1^q)/(x_2^q - x_1^q)$. Sammensætter vi de resultater har vi netop, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$, hvilket er hvad ϕ_q skal opfylde for at være en homomorfi (for alle punkter).

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 $\infty^q = \infty$ 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 vi har endnu engang, at $\phi_q(x_3, y_3) = \phi_q(x_1, y_1) + \phi_q(x_2, y_2)$.

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

$$\begin{aligned} x_3 &= m^2 - 2x_1, \\ y_3 &= m(x_1 - x_3) - y_1, \end{aligned}$$

hvor $m = (3x_1^2 + A)/2y_1$. På samme måde som før opløfter vi dette til den q'ende potens og får, at

$$\begin{aligned} x_3^q &= {m'}^2 - 2x_1^q, \\ y_3^q &= m'(x_1^q - x_3^q) - y_1^q, \end{aligned}$$

hvor $m' = (3^q(x_1^q)^2 + A^q)/2^q y_1^q$. Idet, at $2, 3, A \in \mathbb{F}_q$ følger det, at $2^q = 2, 3^q = 3$ og $A^q = A$. Dette er altså netop formlen for fordoblingen af punktet (x_1^q, y_1^q) på den elliptiske kurve E. Hvis $A^q \neq A$ ville vi have været på en anden elliptisk kurve. Vi har dermed 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. □

Bemærkning 1. 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 $\mathbb{F}_q$, da gælder der*

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

for alle $(x, y) \in E(\overline{\mathbb{F}}_q)$.

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

$$\begin{aligned}(y^q)^2 &= (x^q)^3 + A^q(x^q) + B^q \\ &= (x^q)^3 + A(x^q) + B.\end{aligned}$$

hvor vi har brugt, at $(a+b)^q = a^q + b^q$ når q er en potens af legemets karakteristik og at $a^q = a$ for alle $a \in \mathbb{F}_q$ (se proposition 3 i A.1). 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). □

Følgende proposition er vigtig, da den skaber en sammenhæng mellem kernen for $\phi_q^n - 1$ og antallet af punkter på en elliptisk kurve E over et endeligt legeme $\mathbb{F}_q$.

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. Betragter vi $(\phi_q^n - 1)$ som en endomorfi har vi, at

$$(\phi_q^n - 1)(x, y) = 0 \Leftrightarrow (x^{q^n}, y^{q^n}) - (x, y) = 0 \Leftrightarrow (x^{q^n}, y^{q^n}) = (x, y).$$

Da ϕ_q^n er Frobenius afbildningen for $\mathbb{F}_{q^n}$ følger det at

$$\ker(\phi_q^n - 1) = E(\mathbb{F}_{q^n})$$

fra lemma 3. At $\phi_q^n - 1$ er separabel vil vi ikke vise, men et bevis kan findes i [8, s. 58]. Da $\phi_q^n - 1$ er separabel følger det fra proposition 1, at

$$\#E(E_{q^n}) = \deg(\phi_q^n - 1).$$

Vi har dermed vist det ønskede. □

4.3 Hasses sætning

Vi skal i dette afsnit vise Hasses sætning nu, da vi har fået etableret de nødvendige resultater vedrørende endomorfier på elliptiske kurver over endelige legemer.

Sætning 4 (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 skal i kapitel 5 hvordan elliptiske kurver over endelige legemer kan benyttes til heltalsfaktorisering, hvilket bl.a. hviler på Hasses sætning. Det skal nævnes, at der også findes et elementært bevis for Hasses sætning af oprindeligt af Manin (se [1]) men vi vil benytte teorien om endomorfier til at bevise sætningen. Lad i det følgende

$$a = q + 1 - \#E(\mathbb{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{4.2}$$

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*

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

Bevis. Vi vil ikke give beviset her, da det bygger på en række af tekniske resultater. For et bevis se [8, s. 100]. □

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

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

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

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 $\mathbb{R}$ følger det, at $qx^2 - ax + 1 \geq 0$, for alle $x \in \mathbb{R}$ (se proposition 4 i A.3). 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. □

Det viser sig, at proposition 2 også har andre interessante konsekvenser, som vi vil se på her.

Ordenen af et element P fra en gruppe over en elliptisk kurve er det mindste positive heltal k sådan at

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

Hvis der ikke findes et sådan k siges ordenen af P at være uendelig. Torsionspunkterne er netop de punkter, som har endelig orden. For en elliptisk kurve E og et legeme K definerer vi n-torsionspunkterne til at være

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

Vi bemærker at alle punkter fra en elliptisk kurve over et endeligt legeme er et torsionspunkt. Følgende sætning karakteriserer disse torsionspunkter:

Sætning 5 *Lad E være en elliptisk kurve over et legeme K og lad n være et positivt heltal. Hvis karakteristikken for K ikke deler n, eller er 0, da er*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n.$$

Hvis karakteristikken for K er $p > 0$ og $p \mid n$, lader vi $n = p^r n'$ sådan at $p \nmid n'$. Da er

$$E[n] \simeq \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \quad \textit{eller} \quad \mathbb{Z}_n \oplus \mathbb{Z}_{n'}.$$

Bevis. Et bevis for denne sætning kan findes i [8, s. 79]. □

En konsekvens af sætning 5 er, at vi snakke om en basis for $E[n]$, da vi nu ved hvordan den ser ud. 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 $a, b, c, d \in \mathbb{Z}_n$ 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

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

Med disse detaljer på plads er vi i stand til at vise følgende sætning:

Sætning 6 *Lad E være en elliptisk kurve over $\mathbb{F}_q$. Lad a være som i (4.2). 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 $\gcd(m, q) = 1$.

Bevis. Det følger direkte fra lemma 1 at hvis $\phi_q^2 - a\phi_q + q \neq 0$ (hvis den ikke er nul-endomorfien) 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 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 (se proposition 2) følger det fra proposition 1 og fra det faktum, at $\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$ (se [8, proposition 3.15]), at

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

Videre har vi, at $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. Da vi fra (4.2) har, at $\#\ker(\phi_q - 1) = q + 1 - a$, så

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

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

$$(\phi_q)_m^2 - a(\phi_q)_m + qI \equiv 0 \pmod{m},$$

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.

For at vise entydigheden af a lader vi nu $a_1 \neq a$ være sådan, at

$$\phi_q^2 - a_1\phi_q + q = 0,$$

er opfyldt. Da har vi også, at (ved at lægge 0 til)

$$(a - a_1)\phi_q = (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0$$

Vi har fra sætning 3, at $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ er surjektiv så $(a - a_1)$ annihilerer $E(\overline{\mathbb{F}}_q)$ (dvs. for hvert element $x \in E(\overline{\mathbb{F}}_q)$ er $(a - a_1)x = 0$). Specielt har vi, at $(a - a_1)$ annihilerer $E[m]$ for hvert $m \geq 1$. Men da der er punkter i $E[m]$ med orden m når $\gcd(m, q) = 1$ har vi, at $a - a_1 \equiv 0 \pmod{m}$ for sådan et m. Dermed er $a - a_1 = 0$ og vi har vist, at a er entydig. □

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 7 *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 7. Lad først

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

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 sætning 10 i appendikset). Derfor er

$$f(\phi_q) = (\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0, \tag{4.3}$$

som endomorfier for E pr. sætning 6. Idet vi husker, at $\phi_q^n = \phi_{q^n}$ giver sætning 6 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 (4.3) 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 2. Vi vender tilbage til eksemplet vi så på i afsnit 4.1, hvor E er givet ved $y^2 = x^3 - x$. Vi har da, at

$$\#E(\mathbb{F}_5) = q + 1 - a = 5 + 1 - a = 7 \Rightarrow a = -1.$$

Vi får dermed polynomiet

$$X^2 + X + 5 = \left(X + \frac{1 - i\sqrt{19}}{2}\right)\left(X + \frac{1 + i\sqrt{19}}{2}\right).$$

Sætning 7 siger da, at

$$\#E(\mathbb{F}_{25}) = 25 + 1 - \left(\frac{1 - i\sqrt{19}}{2}\right)^2 - \left(\frac{1 + i\sqrt{19}}{2}\right)^2. \tag{4.4}$$

Den sidste del af udtrykket i (4.4) kan udregnes direkte, men vi kan også bruge rekurrensen fra 5:

$$s_2 = as_1 - qs_0 = -(-1) - 5 \cdot 2 = 1 - 10 = -9.$$

Vi har da, at $\#E(\mathbb{F}_{25}) = 25 + 1 - (-9) = 35$.

5 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, hvordan man bestemmer en faktor for et tal n, er et interssant problem, da alle heltal kan faktoriseres:

Sætning 8 (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. [4]. 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. Vi vil dog ikke berøre kørselstiderne direkte.

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 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.

5.1 Pollards $p - 1$ algoritme

Da Lenstras algoritme er stærkt inspireret af Pollards $p - 1$ algoritme og til dels kan ses som værende en analog til denne, vælger vi at behandle den først. Pollards

$p-1$ algoritme blev først præsenteret i [6] 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 formaliserer begrebet *små* primfaktorer med følgende definition:

Definition 5 *Lad n være et positivt heltal med primtalsfaktorisering $n = \prod p_i^{e_i}$, da siges n at være B-glat hvis $p_i^{e_i} \leq B$ for alle i.*

Vi skal se, at Pollards $p-1$ algoritme giver os en faktor netop, når tallet vi ønsker at faktorisere har en primtalsfaktor p sådan at $p-1$ er B-glat.

Eksempel 3. $30 = 2 \cdot 3 \cdot 5$ så 30 er 5-glat, 6-glat osv. Men $50 = 2 \cdot 5^2$ er ikke 5-glat, den er derimod 25-glat, 26-glat osv.

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 $a \in \mathbb{Z}$ valgt sådan at $\gcd(a, n) = 1$, har vi fra Fermats lille sætning, at

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

Lad nu $k = \operatorname{lcm}[1, 2, \ldots, K]$ for et $K \in \mathbb{Z}^+$, hvor lcm angiver det mindste fælles multiplum. Antag at $p-1 \mid k$, da har vi videre, 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 udregningerne ovenfor ikke gar haft brug for at kende p. Vi vil i grunden beregne $\gcd(x \pmod{n}, n)$ da x kan blive et meget stort tal, men dette 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

$$p - 1 \mid \operatorname{lcm}[1, 2, \ldots, K],$$

hvilket er tilfældet når n har en primtalsfaktor p sådan, at $p-1$ er K-glat. Det er altså nødvendigt, at $p-1$ har mange små primfaktorer hvis algoritmen skal have en chance. Vi kan da opskrive algoritmen (inspireret af gennemgangen i [7]):

Algoritme 1 (Pollards $p-1$ algoritme) *Lad $n \geq 2$ være et sammensat tal.*

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*

$$k = \operatorname{lcm}[1, 2, \ldots, K],$$

   for et $K \in \mathbb{Z}^+$, 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.

Algoritmen vil på et tidspunkt stoppe, da vi før eller siden vil ende i tilfældet, hvor $K = \frac{1}{2}(p-1)$ 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

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

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

$$k = \operatorname{lcm}[1, 2, \ldots, 11] = 27720.$$

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

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

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

$$30042491 = 3251 \cdot 9241.$$

Det tjekkes at 3251 og 9241 rent faktisk er primtal og vi har fundet den fulde faktorisering.

Bemærkning 2. Vi fandt en faktor netop når $K = 11$ fordi, at

$$9241 - 1 = 9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11,$$

hvilket betyder at 9240 er 11-glat.

5.2 Lenstras elliptiske kurve algoritme

I [5] præsenterede H. W. Lenstra en algoritme til faktorisering af heltal, som anvender elliptiske kurver. Vi skal benytte koncepterne vi udviklede til gruppeloven, men vi skal anvende dem på $E(\mathbb{Z}_n)$, hvor n er et sammensat tal. Når n er et sammensat tal er $\mathbb{Z}_n$ ikke er legeme og derfor kan vi ikke være sikre på at $E(\mathbb{Z}_n)$ er en gruppe. Derfor er det teknisk set ikke elliptiske kurver vi arbejder med, men derimod hvad man kunne kalde for elliptiske pseudokurver. Der vil altså være tidspunkter, hvor en addition fra gruppeloven ikke vil give mening, men det er netop det der kan give os en faktor.

Antag, at n er et sammensat tal og $\gcd(6, n) = 1$ (det udelukker faktorer af 2 og 3) og lad p være en primfaktor i n. Vi ser nu på, hvordan vi kan finde en faktor, når additionen af to punkter ikke er defineret. Vi husker fra gruppeloven, at vi ved additionen af to punkter $P = (x_1, y_1)$ og $P = (x_2, y_2)$ (forskellige fra ∞) skal bruge værdien af inverserne til $x_2 - x_1$ og y_1 alt efter, hvilket tilfælde vi er i. Disse inverser eksisterer kun modulo n, hvis (se proposition 5 i appendikset)

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

Når dette ikke er tilfældet giver de i stedet en faktor i n, som vi håber på er ikke-triviel. Hvornår kan vi støde på en situation, hvor denne addition ikke er defineret? Antag, at $x_1 \neq x_2$ og $y_1 \neq y_2$. Hvis vi støder på en udregning der ikke kan lade sig gøre er det fordi, at $(x_1 - x_2)^{-1}$ ikke eksisterer modulo n. Antag derudover, at $x_1 - x_2$ er et multiplum af p. Vi har da, at $x_1 - x_2 \equiv 0 \pmod{p}$. Gruppeloven giver os, at når $x_1 \equiv x_2 \pmod{p}$ er $P_1 + P_2 = \infty$ på kurven modulo p. Fordoblingen af punktet P_1 fejler, når y_1 er et multiplum af p. Dette sker når $y_1 \equiv 0 \pmod{p}$, men da er $2P_1 = \infty$ på kurven modulo p.

Generelt har vi altså, at en addition slår fejl på en kurve modulo n, når additionen giver $P_1 + P_2 = \infty$ på kurven modulo p. Måden hvorpå vi kan finde en faktor er altså ved at foretage disse additioner og fordoblinger på en kurve modulo n, hvor vi håber på at en addition giver os ∞ på kurven modulo en primfaktor p. Vi præsenterer da en algoritme, inspireret af [7] og [8], som forsøger at generere elementet ∞ fra $E(\mathbb{F}_p)$.

Vælg først tilfældige heltal x, y, A mellem 1 og n, og sæt

$$B = y^2 - x^3 - Ax \pmod{n}.$$

Vi har da en elliptisk pseudokurve $y^2 = x^3 + Ax + B$, hvor vi ved at punktet $P = (x, y)$ er placeret. Vi tjekker da, at

$$d = \gcd(4A^3 + 27B^2, n) = 1.$$

Hvis det 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 B lader vi $k = \operatorname{lcm}[1, 2, \ldots, B]$ og vi forsøger da, at bestemme

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

Det er ikke praktisk 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 meget langsommelige 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 ved fra Hasses sætning, at $\#E(\mathbb{F}_p)$ er endelig. Lagranges sætning giver os da, at ordenen af punktet P på kurven modulo p deler $\#E(\mathbb{F}_p)$. Hvis k er et multiplum af $\#E(\mathbb{F}_p)$ er $kP = \infty$ på kurven modulo p. For at algoritmen kan finde en faktor er det nødvendigt, at for en eller anden primfaktor p i n, at $\#E(\mathbb{F}_p)$ er K-glat. Fordelen ved Lenstras algoritme over Pollards $p-1$ algoritme viser sig her, da vi i Pollards algoritme kun kan vælge én gruppe, som har orden $p-1$, kan vi her skifte vores elliptiske kurve hvis $\#E(\mathbb{F}_p)$ ikke er K-glat.

Vi kan også være uheldige, at løbe ind i den trivielle faktor n. Antag, at $n = pq$ for primtal p og q. Hvis både $\#E(\mathbb{F}_p)$ og $\#E(\mathbb{F}_q)$ er K-glatte da vil k være et multiplum af både $\#E(\mathbb{F}_p)$ og $\#E(\mathbb{F}_q)$. Så $kP = \infty$ på kurven både modulo p og q. Dermed er $x_1 - x_2$ og y_1 multipla af både p og q, så vi får

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

Vi opsummerer diskussionen af algoritmen nedenfor:

Algoritme 2 (Lenstras algoritme) *Lad $n \geq 2$ være et sammensat tal.*

1. *Vælg heltal x, y og A mellem 1 og n. Lad da $B = y^2 - x^3 - Ax \pmod{n}$, så vi har den elliptiske kurve*

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

   hvor 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*

$$k = \text{lcm}[1, 2, 3, ..., K],$$

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. Ellers har vi fundet en faktor som enten $d = \gcd(x_1 - x_2, n)$ eller $d = \gcd(y_1, n)$. Hvis $d = 1$ gå da til (1) og vælg en ny kurve eller gå til (3) og vælg større k. Hvis $d = n$ gå til (3) og vælg mindre k. Ellers er d en ikke-triviel faktor.*

For at se hvorfor der er en chance for, at vi støder på et valg af x, y, A sådan at vi finder en faktor, lader vi p være en primfaktor i n. Til den elliptiske kurve E har vi den abelske gruppe $E(\mathbb{F}_p)$ og pr. sætning 4 ved vi, at

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

En sætning af Deuring [3] siger, at for ethvert heltal $m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$ findes der talpar (A, B) i mængden

$$\{(A, B) \mid A, B \in \mathbb{F}_p, 4A^3 + 27B^2 \neq 0\},$$

sådan at $\#E(\mathbb{F}_p) = m$ (se også [2, afsnit 7.3]). For hvert tal i intervallet findes der altså en elliptisk kurve, som har denne orden. Der er altså en positiv sandsynlighed for, at vi kan finde sådan en kurve. Hvor stor denne sandsynlighed er vil vi ikke komme ind på her, men nogle af disse overvejelser kan findes i både [5] og [2].

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

$$k = \text{lcm}[1, 2, \ldots, 10] = 2520.$$

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

$$753161713 = 19259 \cdot 39107.$$

Det kan umiddelbart se ud til, at det var spild da vi lavede hele tabellen, men i beregningerne af $2^iP \pmod{753161713}$ ville vi også kunne have stødt på et element, som ikke havde en invers og som dermed kunne give os en faktor.

Bemærkning 3. Da $19258 = 2 \cdot 9629$ og $39106 = 2 \cdot 19553$ er de hhv. 9629-glat og 19553-glat så Pollards $p-1$ algoritme skulle vente på, at $k = \text{lcm}[1, 2, \ldots, 9629]$ for at finde en faktor, hvilket ville være meget ineffektivt i forhold til Lenstras algoritme.

A Udeladte resultater

Her samler vi nogle af de resterende resultater, som benyttes igennem kapitlerne. I opgaven henvises der til resultaterne her, når de anvendes i beviserne.

A.1 Legemer

Lad p være et primtal. Heltallene modulo p giver os et legeme $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der indeholder p elementer. Antallet af elementer i ethvert endeligt legeme er på formen p^n. For at se dette lader vi K være et endeligt legeme. Dets karakteristik må være p for et eller andet primtal, da et legeme med karakteristik 0 er uendeligt. Derfor må K være endeligt frembragt som et vektorrum over $\mathbb{Z}/p\mathbb{Z}$. Så lad $x_1, \ldots, x_n$ være en basis for K. Elementerne i K kan da skrives entydigt som

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n, \quad \text{hvor} \quad \alpha_i \in \mathbb{Z}/p\mathbb{Z}.$$

Da hvert $\alpha_i \in K$ har vi altså p forskellige valg for hver af $\alpha_1, \alpha_2, \ldots, \alpha_n$. Dette betyder, at vi har p^n valg for x, som også giver os hele legemet K. Antallet af elementer i K er altså p^n.

Vi benytter notationen $\mathbb{F}_q = \mathbb{F}_{p^n}$ for det endelige legeme med $q = p^n$ elementer. Bemærk, at $\mathbb{Z}/p^n\mathbb{Z}$ ikke er et legeme for $n \geq 2$, da p ikke har nogen multiplikativ invers.

Sætning 9 *Lad $\overline{\mathbb{F}}_p$ være den algebraiske aflukning af $\mathbb{F}_p$ og lad $q = p^n$, da er*

$$\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\}. \tag{A.1}$$

Bevis. Vi vil først vise, at $\mathbb{F}_q \subseteq \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\}$. Ikke-nul elementerne fra $\mathbb{F}_q$ danner en gruppe af orden $q-1$ så $\alpha^{q-1} = 1$ når $0 \neq \alpha \in \mathbb{F}_q$. Da $0^q = 0$ har vi, at $\alpha^q = \alpha$ for alle $\alpha \in \mathbb{F}_q$ og vi har den ønskede inklusion.

Idet vi husker, at et polynomium $g(X)$ kun har multiple rødder, hvis den har en fælles rod med dens afledede $g'(X)$ ser vi, at

$$\frac{d}{dX}(X^q - X) = qX^{q-1} - 1 = -1,$$

da $q = p^n = 0$ i $\mathbb{F}_p$. Dermed har $g(X)$ altså ikke nogen multipel rod, så der findes q forskellige elementer $\alpha \in \overline{\mathbb{F}}_p$ sådan at $\alpha^q = \alpha$.

Da begge mængder i (A.1) har samme antal elementer og den ene er indeholdt i den anden, må de nødvendigvis være ens. □

Lad $\phi_q(x) = x^q$ for alle $x \in \overline{\mathbb{F}}_q$. Vi kalder da ϕ_q for Frobenius automorfien (analogt til Frobenius endomorfien). Følgende proposition fastsætter nogle af dens egenskaber:

Proposition 3 *Lad $q = p^n$ hvor p er et primtal.*

1. *Lad $\alpha \in \overline{\mathbb{F}}_q$. Da er $\alpha \in \mathbb{F}_{q^n}$ hvis og kun hvis $\phi_q^n(\alpha) = \alpha$.*
2. *ϕ_q er en automorfi for $\overline{\mathbb{F}}_q$. Specielt gælder der, at*

$$\phi_q(x+y) = \phi_q(x) + \phi_q(y) \quad og \quad \phi_q(xy) = \phi_q(x)\phi_q(y).$$

En automorfi er en bijektiv homomorfi (isomorfi), som afbilleder til sig selv.

Bevis. (1) følger fra sætning 9 med q^n i stedet for q. Vi kan derfor fokusere på (2). Lad $1 \leq j \leq p-1$, da vi vil binomial koefficienten $\binom{p}{j}$ have en faktor p i dens tæller som ikke går ud med nævneren. Derfor har vi, at

$$\binom{p}{j} \equiv 0 \pmod{p}.$$

Det følger heraf, at

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \ldots + y^p = x^p + y^p,$$

da vi er i karakteristik p. Vi vil lave et induktionsbevis og dette viser basistilfældet. Antag nu, at der gælder at $(x+y)^{p^n} = x^{p^n} + y^{p^n}$. Da har vi, at

$$\begin{aligned}(x+y)^{p^{n+1}} &= (x+y)^{p^n p} = ((x+y)^{p^n})^p = (x^{p^n} + y^{p^n})^p \\ &= x^{p^{n+1}} + y^{p^{n+1}}.\end{aligned}$$

Dette giver os, at $\phi_q(x+y) = \phi_q(x) + \phi_q(y)$. Det er klart, at $\phi_q(xy) = \phi_q(x)\phi_q(y)$, da $(xy)^q = x^q y^q$. Vi har da, at ϕ_q er en homomorfi for legemer. Vi mangler at vise, at ϕ_q er en bijektion. En homomorfi for legemer er injektiv (kernen af en homomorfi er et ideal, så over et legeme er kernen tom eller hele legemet). Hvis $\alpha \in \overline{\mathbb{F}}_p$ da er $\alpha \in \mathbb{F}_{q^n}$ for et eller andet n, så $\phi_q^n(\alpha) = \alpha$. Dermed er α i billedet af ϕ_q så ϕ_q er surjektiv. Dermed er ϕ_q en automorfi. □

A.2 Tæthedsargumentet i Hasses sætning

Følgende propositon benyttes i Hasses sætning:

Proposition 4 *Mængden*

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

er tæt i $\mathbb{R}$ *og* $qx^2 - ax + 1 \geq 0$ *for alle* $x \in \mathbb{R}$.

Bevis. En delmængde $X \subseteq \mathbb{R}$ siges at være tæt, hvis der for alle heltal $a \in \mathbb{R}$ findes et interval med centrum i a, som også indeholder punkter fra X.

Lad X være mængden i propositionen og lad s være en potens af 2 eller 3. Ét af de to må nødvendigvis være primisk med q, da q er en potens af ét enkelt primtal p. Vi ser, at rationalerne på formen $r/2^n$ er tæt i $\mathbb{R}$ på følgende måde. Lad $a, b \in \mathbb{R}$ være sådan at $a < b$. Der findes da $n \in \mathbb{N}$ sådan, at

$$0 < \frac{1}{n} < b - a \Rightarrow 0 < \frac{1}{2^n} < \frac{1}{n} < b - a.$$

Vi har altså at $1 < 2^n b - 2^n a$. Når afstanden mellem $2^n b$ og $2^n a$ er større end 1 findes der $r \in \mathbb{Z}$ sådan, at

$$2^n a < r < 2^n b \Rightarrow a < \frac{r}{2^n} < b.$$

Dette viser netop, at $r/2^n$ er tæt i $\mathbb{R}$. Det samme kan gøres for $r/3^n$. Vi har da, at X indeholder en delmængde som er tæt i $\mathbb{R}$, hvilket giver os at X selv er tæt i $\mathbb{R}$.

Vi vi vil nu vise, at $qx^2 - ax + 1 \geq 0$ for alle $x \in \mathbb{R}$. Antag for modstrid, at der findes $r \in \mathbb{R}$ sådan at $ar^2 - ar + 1 < 0$. Vi ser på en følge af intervaller omkring r:

$$(r - \varepsilon, r + \varepsilon), \quad \text{hvor } \varepsilon = \frac{1}{n}, \quad n = 1, 2, \ldots$$

I hvert af disse intervaller findes $x_n \in X$, da vi netop har vist at X er en tæt mængde i $\mathbb{R}$. Vi får en følge $x_1, x_2, \ldots$ af tal som nærmer sig r. For et stort nok i har vi, at $qx_i^2 - ax_i + 1$ er arbitrært tæt på $qr^2 - ar + 1$. Men da $x_i \in X$ må den første af disse to være ≥ 0 mens den anden er < 0. Dette er en modstrid og vi har, at $qx^2 - ax + 1 \geq 0$ for alle $x \in \mathbb{R}$. □

A.3 Andre resultater

Sætning 10 *Lad* K *være et legeme. Hvis* $f, g \in K[X]$*, da findes der polynomier* $q, r \in K[X]$ *sådan at* $\deg r < \deg g$ *og*

$$f = qg + r.$$

Hvis $f, g \in \mathbb{Z}[X]$ *og* g *er monisk, da findes der* $q, r \in \mathbb{Z}$ *sådan at* $\deg r < \deg g$ *og*

$$f = qg + r.$$

Bevis. Det følger direkte af divisionsalgoritmen for polynomier. Hvis f har ledende term ax^n og g har ledende term bx^m hvor $n \geq m$, da har $f - \frac{a}{b}x^{n-m}$ grad mindre end f. Vi kan dermed blive ved med at trække multipla af g fra f indtil resultatet har grad mindre end $\deg g$. Hvis g er monisk er $b = 1$ så hver gang trækker vi et polynomium med heltalskoefficienter fra, så både kvotienten q og resten r vil dermed have heltalskoefficienter. □

Proposition 5 *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 $ae \equiv 0 \pmod{n}$. Vi har altså, at

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

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

Litteratur

[1] J. S. Chahal. "Manin's Proof of the Hasse Inequality Revisited". I: *Nieuw Arch. Wiskd., IV.* 13. ser. (2 1995), s. 219–232.

[2] R. Crandall og C. B. Pomerance. *Prime Numbers: A Computational Perspective.* Springer, 2005.

[3] M. Deuring. "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper". I: *Abhandlungen Aus Dem Mathematischen Seminar Der Universitat Hamburg* 14 (1 1941), s. 197–272.

[4] J. P. Hansen. *Algebra Og Talteori.* Aspekt serien. Gyldendal Uddannelse, 2002.

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

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

[7] J. H. Silverman og J. Tate. *Rational Points on Elliptic Curves.* Springer Undergraduate Texts in Mathematics and Technology. Springer, 1992.

[8] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography, Second Edition.* Discrete Mathematics and Its Applications. Taylor & Francis, 2008.