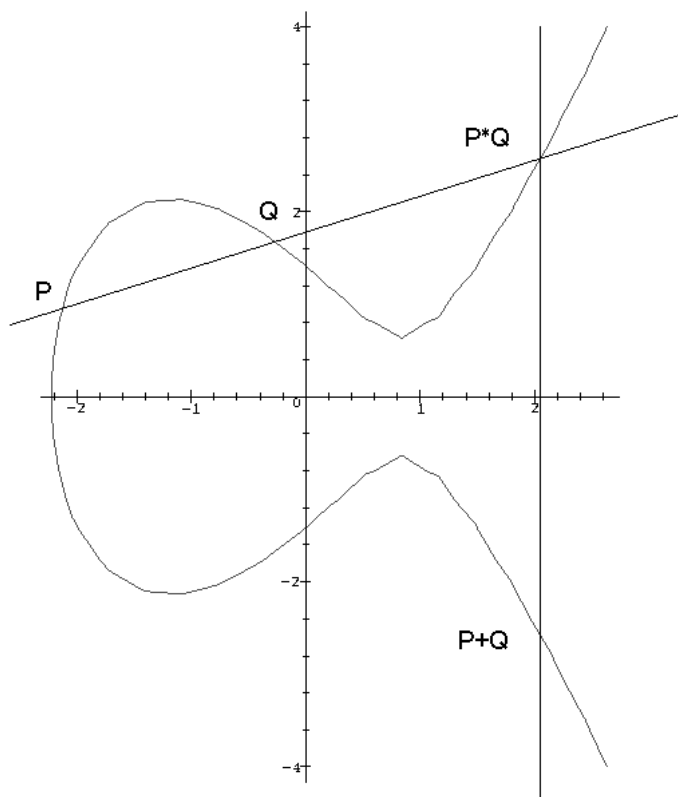


# ELLIPTISKE KURVER

STEFFEN BACH HANSEN

*Vejleder: Johan P. Hansen*

Bachelorprojekt i matematik  
Århus Universitet  
Forår 2000



---

28. juni 2000.  
Årskortnr.: 970613.

## INDHOLD

1. Gruppestrukturen på elliptiske kurver	2
1.1. Elliptiske kurver	2
1.2. Det projektive plan $\mathbb{P}^2$	3
1.3. Kompositionen og gruppestrukturen	3
2. Elliptiske kurver over endelige legemer	8
2.1. Endelige legemer	8
2.2. Legendre symbolet	8
2.3. Hasses Sætning	9
3. Lenstras faktoreringsalgoritme	16
3.1. Lenstras ide	18
3.2. Lenstras algoritme	18
3.3. Hvorfor er Lenstras algoritme smart?	20
Bilag A.	22
A.1. Bezout	22
A.2. MAPLE	23
A.3. Legendre	23
A.4. Diskret valuation funktionen	24
Litteratur	25

## 1. GRUPPESTRUKTUREN PÅ ELLIPTISKE KURVER

Vi vil i dette kapitel se på gruppestrukturen på elliptiske kurver, herunder definere hvad en elliptisk kurve er, og udlede additionsformler for sammensætningen af to punkter på en elliptisk kurve. Inspirationen til dette kapitel er hentet i [1] kapitel 1 og 2.

1.1. **Elliptiske kurver.** En generel kubisk kurve

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

siges at være rational over et legeme  $k$ , hvis koefficienterne tilhører  $k$ . Hvis denne kubiske kurve har et  $k$ -rationalt punkt, og  $\text{char}(k) \neq 2$ , kan den ved passende valg af koordinatskift skrives på Weierstrass normalform

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in k \quad (1.1)$$

Denne kurve betegnes  $C$ , og vi vil i denne opgave antage, at  $\text{char}(k) \neq 2$ . Vi vil nu undersøge, hvornår kurven er glat, altså hvornår tangentliniens ligning eksisterer for alle punkter  $(x_0, y_0)$  på kurven. Hvis vi skriver ligning 1.1 som  $F(x, y) = y^2 - f(x) = 0$ , skal vi altså kræve at de partielt afledede af  $F$  ikke er nul samtidigt, dvs.  $\forall (x_0, y_0) \in C$ :

$$\left(\frac{\partial F}{\partial x}\right)_{(x_0, y_0)}(x - x_0) \neq 0 \vee \left(\frac{\partial F}{\partial y}\right)_{(x_0, y_0)}(y - y_0) \neq 0$$

Differentierer vi nu  $F(x, y)$  partielt får vi

$$\frac{\partial F}{\partial y} = 2y = 0 \Rightarrow y = 0$$

Hvilket viser, at de 3 punkter hvor tangenten kan forsvinde er  $(\alpha_1, 0); (\alpha_2, 0); (\alpha_3, 0)$ . Differentierer vi med hensyn til  $x$ , får vi

$$\frac{\partial F}{\partial x} = -f'(x) = 0 \Rightarrow f'(x) = 0.$$

Men hvis  $f(\alpha_i) = f'(\alpha_i) = 0$  så er  $\alpha_i$  dobbeltrod i  $f$ , se [5] lemma 5.3.3. Men det vil sige at  $(\alpha_i - x)|f(x)$  og  $(\alpha_i - x)|f'(x)$  så største fælles divisor mellem  $f$  og  $f'$ ,  $\text{sfd}(f(x), f'(x)) \neq 1$ . Vi er nu klar med en definition.

**Definition 1.1.** En kubisk kurve, som er skrevet på Weierstrass normal-form,

$$y^2 = x^3 + ax^2 + bx + c \quad a, b, c \in k$$

kaldes en elliptisk kurve, hvis  $f(x) = x^3 + ax^2 + bx + c$  har 3 forskellige rødder (evt. i en algebraisk lukket udvidelse  $\bar{k}$  af  $k$ ) eller ækvivalent, hvis  $\text{sfd}(f(x), f'(x)) = 1$ .

*Bemærkning 1.2.* Diskriminanten af  $f(x)$  er givet ved

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \quad (1.2)$$

Men faktorerer vi  $f(x)$ , evt. over en udvidelse  $\bar{k}$  af  $k$  får vi

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \quad (1.3)$$

Man kan deraf hurtigt få, at

$$\Delta = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 \quad (1.4)$$

ved at sammenligne koefficienter, men dette viser, at diskriminanten  $\Delta \neq 0$  hvis og kun hvis  $f(x)$  har 3 forskellige rødder.

**1.2. Det projektive plan  $\mathbb{P}^2$ .** For at vi er i stand til at etablere en gruppestruktur på de elliptiske kurver, definerer vi det projektive plan  $\mathbb{P}^2$ . Lidt løst sagt er det det affine plan  $k^2$ , hvor  $k$  er et legeme, plus en ekstra linie i uendelig. Mere præcist kan vi se på  $k^3$  og definerer en ækvivalensrelation  $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ ,  $\lambda \neq 0$ . Det vil sige, at en linie i rummet, gennem origo, svarer til et punkt i  $\mathbb{P}^2$ . Dvs. at

$$\mathbb{P}^2(k) = (k^3 \setminus \{0, 0, 0\}) / \sim$$

Man associerer nogle punkter

$$k^2 \rightarrow \mathbb{P}^2$$

vha. afbildningen

$$(x, y) \mapsto (X : Y : 1)$$

Kolon imellem koordinaterne betyder, at vi kan skalere indgangene. Hvis vi homogeniserer  $y^2 = x^3 + ax^2 + bx + c$  med den 3. variabel  $Z$  får vi

$$Y^2 Z = X^3 + aX^2 Z + bX Z^2 + cZ^3 \quad (1.5)$$

$Z = 0$  er en linie i  $\mathbb{P}^2$ , som er i uendelig i forhold til  $(x, y)$  planet, men sætter vi  $Z = 0$  i ligning 1.5, får vi  $0 = X^3$ , som har en tredobbelt rod i  $X = 0$ , dvs. linien i uendelig skærer den elliptiske kurve 3 gange i samme punkt. Punktet der opfylder denne betingelse er  $(0 : 1 : 0)$ . Det definerer en ny afbildning:  $(x, z) \mapsto (X : 1 : Z)$  i hvilken  $(0, 0) \mapsto (0 : 1 : 0)$ . Dette punkt er oplagt  $k$ -rationalt og vi kalder det for  $\mathcal{O}$ , og vi skal senere se, at dette bliver neutralelementet i gruppen af punkter i  $k^2$  på den elliptiske kurve. Indsættes  $Y = 1$  i ligning 1.5 får vi

$$F(X, Z) = X^3 + aX^2 Z + bX Z^2 + cZ^3 - Z$$

For at undersøge om  $\mathcal{O}$  er et singulært punkt udregnes:

$$\frac{\partial F}{\partial X} \Big|_{(0,0)} = 0$$

og

$$\frac{\partial F}{\partial Z} \Big|_{(0,0)} = -1$$

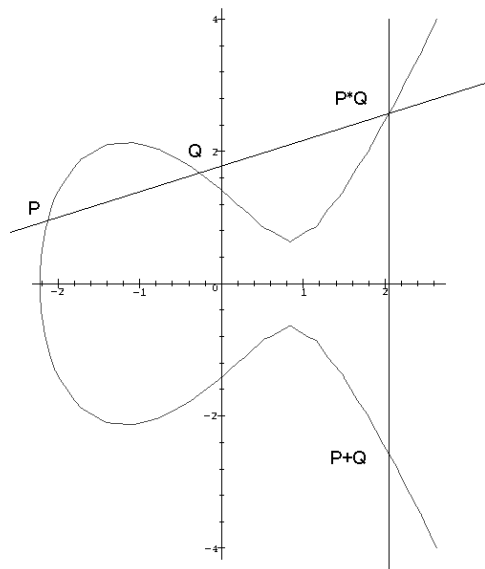
Hvilket viser, at  $\mathcal{O}$  ikke er singulært.

*Bemærkning 1.3.* Man siger, at et punkt  $P \in \mathbb{P}^2$  er  $k$ -rationalt, hvis det kan skrives på formen  $P = (a : b : c)$ , hvor  $a, b, c \in k$ .

### 1.3. Kompositionen og gruppestrukturen.

**Definition 1.4.** En gruppe  $G$  er defineret som en mængde med en komposition, som opfylder følgende 3 punkter.

- 1:** Der eksisterer et neutralt element  $\mathcal{O} \in G$  så,  $\mathcal{O} + P = P + \mathcal{O} = P$ , For alle  $P \in G$
- 2:** For alle  $P \in G$  findes der et inverst element  $-P \in G$  så,  $P - P = -P + P = \mathcal{O}$
- 3:** Kompositionen er associativ,  $(P + Q) + R = P + (Q + R)$



FIGUR 1. Elliptisk kurve

Kompositionen på punkter på en elliptisk kurve er givet som følger.

**Kompositionen.** Lad  $P, Q \in k^2$  være 2 punkter på den elliptiske kurve  $C$ , for at finde  $P + Q$  forbindes  $P$  og  $Q$  med en ret linie. Da en linie skærer en elliptisk kurve præcis 3 gange (se sætning A.1 i bilag A), vil linien skære  $C$  i et tredje punkt, kald dette punkt  $P * Q$ . Forbind nu  $P * Q$  med  $\mathcal{O}$  og tag igen tredje skæringspunkt, dette punkt kaldes  $P + Q$ , se figur. 1.

*Bemærkning 1.5.* Punktet  $\mathcal{O}$  bliver som tidligere nævnt neutralelementet, og en linie gennem  $P * Q$  og  $\mathcal{O}$  vil være lodret, så det tredje punkt  $P + Q$  findes ved en spejling i  $x$ -aksen (da en elliptisk kurve på Weierstrass normalform er symmetrisk omkring  $x$ -aksen).

*Bemærkning 1.6.* Det ses at gruppen er kommutativ, da linien gennem  $P$  og  $Q$  er den samme som linien gennem  $Q$  og  $P$ .

*Bemærkning 1.7.* Hvis vi vil udregne  $P + P = 2P$ , gør vi på samme måde som før, men linien gennem  $P$  og  $P$  er nu tangenten i  $P$  (som findes i alle punkter i følge definition 1.1), og vi tæller 2 skæringer med  $C$  i  $P$ , se bemærkning A.2 i bilag A.

**Sætning 1.8.** *Lad  $k$  være et vilkårligt legeme og  $C$  en elliptisk kurve på Weierstrass normalform,*

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in k$$

*så er  $G = \{\text{Punkter } P \in C \mid P \in k^2\} \cup \mathcal{O}$ , mængden af alle punkter på kurven som tilhører  $k^2$  forenet med  $\mathcal{O}$ , en gruppe.*

*Bevis.* Vi går gennem punkterne 1 til 3 i definition 1.4 en ad gangen.

- 1:** At  $\mathcal{O} + P = P + \mathcal{O} = P$  ses ved at tegne en lodret linie gennem  $P$  (og dermed også  $\mathcal{O}$ ). Tredje skæringspunkt vil da være  $-P$  (se pkt. 2) Forbinder man så  $-P$  med  $\mathcal{O}$  vil tredje skæring med  $C$  naturligvis være  $P$  igen.
- 2:** Da  $C$  er symmetrisk omkring  $x$ -aksen, får vi, at hvis  $Q = (x, y)$  så vil  $-Q = (x, -y)$ . Dette kontrolleres på følgende måde. Tag linien gennem  $Q$  og  $-Q$  og tag tredje skæring med  $C$ , dette giver neutralelementet  $\mathcal{O}$ , tag så  $\mathcal{O}$  og forbind det med sig selv og tag tredje skæring med  $C$ , dette giver igen  $\mathcal{O}$ . Så der findes et inverst element til  $Q = (x, y)$ , nemlig  $-Q = (x, -y)$ .
- 3:** Associativiteten er en smule vanskeligere, og vises separat i sætning 1.12

□

Vi ønsker nu at vise, at kompositionen overhovedet er veldefineret.

**Lemma 1.9.** *Hvis vi har 2  $k$ -rationale punkter  $\alpha_1, \alpha_2$  på den elliptiske kurve  $C$ , og forbinder dem med en ret linie, så vil det 3. skæringspunkt  $\alpha_3$  mellem linie og kurve også være  $k$ -rationalt.*

*Bevis.* Lad linien  $l$  være givet ved

$$l : y = \alpha x + \beta, \quad \alpha, \beta \in k$$

og den elliptiske kurve givet ved

$$y^2 = x^3 + ax^2 + bx + c, \quad a, b, c \in k.$$

Indsættes ligningen for  $l$  i  $C$  får man

$$\alpha^2 x^2 + \beta^2 + 2\alpha\beta x = x^3 + ax^2 + bx + c$$

↓

$$\begin{aligned} 0 &= x^3 + (a - \alpha^2)x^2 + (b - 2\alpha\beta)x + (c - \beta^2) \\ &= x^3 + Ax^2 + Bx + C, \quad A, B, C \in k \end{aligned}$$

Men denne ligning har pr. konstruktion 2  $k$ -rationale rødder  $\alpha_1, \alpha_2$ , så da summen af rødderne er lig minus koefficienten til  $x^2$ -leddet, får man

$$-(\alpha_1 + \alpha_2 + \alpha_3) = A$$

↓

$$\alpha_3 = -(\alpha_1 + \alpha_2 + A) \in k$$

Men når højre side af ligningen tilhører  $k$ , gør venstresiden det også, dvs.  $\alpha_3 \in k$ , ved indsættelse af  $\alpha_3$  i ligningen for linien  $l$  ses, at også  $y$  tilhører  $k$ . □

Før vi går over til at vise associativiteten, vil vi vise nogle eksplicitte udtryk for addition af to punkter.

**Eksempel 1.10** (Addition af 2 forskellige punkter  $P_1$  og  $P_2$ ). Lad  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$ , begge forskellig fra  $\mathcal{O}$ ,  $P_1 * P_2 = (x_3, y_3)$ , og  $P_1 + P_2 = (x_3, -y_3)$ . Antag at  $(x_1, y_1)$  og  $(x_2, y_2)$  er givet, og at  $P_1 \neq -P_2$ , da er ligningen for linien gennem dem givet ved

$$y = \lambda x + \nu, \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$$

Så for at få det tredje skæringspunkt substituerer vi ligningen for linien ind i ligningen for den elliptiske kurve.

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$$

↓

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

Da  $-(x_1 + x_2 + x_3) = a - \lambda^2$  ved udregning af  $x^2$ -leddet får vi

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda(x_3 - x_2) + y_2$$

For at finde  $P_1 + P_2$  skiftes bare fortegn på  $y$ -koordinaten, dvs.

$$P_1 + P_2 = [\lambda^2 - a - x_1 - x_2, \lambda(x_2 - x_3) - y_2] \quad (1.6)$$

**Eksempel 1.11** (Addition af 2 ens punkter  $P_0 + P_0$ ). Lad  $P_0 = (x_0, y_0)$  hvor  $y_0 \neq 0$  og  $2P = (x_1, y_1)$ . Da vi nu ikke kan finde hældningen  $\lambda$  som før, bliver vi nødt til at bruge tangentens hældning  $\gamma$  i punktet  $P_0$ . Dette gøres ved implicit differentiation af  $y^2 = x^3 + ax^2 + bx + c$

$$2ydy = (3x^2 + 2ax + b)dx$$

↓

$$\frac{dy}{dx} = \frac{3x^2 + 2ax + b}{2y} = \gamma$$

Som er hældningen af tangenten gennem  $P_0 = (x_0, y_0)$ , dvs.  $y = \gamma x + b \Rightarrow b = y_0 - \gamma x_0$  ved indsættelse af punktet  $(x_0, y_0)$  i ligningen for linien. Vi har altså at

$$y = \gamma(x - x_0) + y_0$$

Dette indsætter vi nu i ligningen for den elliptiske kurve, og man får

$$y^2 = (\gamma(x - x_0) + y_0)^2 = x^3 + ax^2 + bx + c$$

Men ved samme trick som i eksempel 1.10 fås nu at  $-(x_0 + x_0 + x_1) = (a - \gamma^2)$ , så

$$x_1 = \gamma^2 - a - 2x_0, \quad y_1 = \gamma(x_1 - x_0) + y_0$$

Igen, for at finde  $P_0 + P_0 = 2P_0$  skiftes fortegn på  $y$ -koordinaten, dvs. duplikationsformlen er

$$2P_0 = [\gamma^2 - a - 2x_0, \gamma(x_0 - x_1) - y_0] \quad (1.7)$$

**Sætning 1.12** (Associativitet). *Givet tre vilkårlige punkter  $P_1, P_2, P_3 \in k^2$ , på den elliptiske kurve, da er*

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$$

*Bevis.* Vi vil i det følgende antage

$$P_1 \neq -P_2, \quad P_2 \neq -P_3, \quad P_1 + P_2 \neq -P_3, \quad P_2 + P_3 \neq -P_1$$

Notationen er

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad P_3 = (x_3, y_3)$$

Benytter vi resultaterne fra eksempel 1.10, finder vi

$$\begin{aligned} (P_1 + P_2)_x &= \lambda^2 - a - x_1 - x_2 \\ (P_1 + P_2)_y &= -\lambda(\lambda^2 - a - x_1 - x_2) - y_2 + \lambda x_2 \end{aligned}$$

hvor  $(P_1 + P_2)_x$  betegner  $x$ -koordinaten af  $P_1 + P_2$ , samt

$$\begin{aligned} \{(P_1 + P_2) + P_3\}_x &= \kappa^2 - a - x_3 - (P_1 + P_2)_x \\ &= \kappa^2 - a - x_3 - (\lambda^2 - a - x_1 - x_2) \\ &= \kappa^2 - \lambda^2 + x_1 + x_2 - x_3 \end{aligned} \quad (1.8)$$

hvor  $\lambda, \kappa$  er hældningstallet for linien gennem  $P_1, P_2$  og  $P_1 + P_2, P_3$  henholdsvis. Omvendt finder vi nu ved symmetri

$$\begin{aligned} (P_2 + P_3)_x &= \mu^2 - a - x_2 - x_3 \\ (P_2 + P_3)_y &= -\mu(\mu^2 - a - x_2 - x_3) - y_2 + \mu x_2 \\ \{P_1 + (P_2 + P_3)\}_x &= \tau^2 - a - x_1 - (P_2 + P_3)_x \\ &= \tau^2 - a - x_1 - (\mu^2 - a - x_2 - x_3) \\ &= \tau^2 - \mu^2 + x_2 + x_3 - x_1 \end{aligned} \quad (1.9)$$

hvor  $\mu, \tau$  er hældningstallet for linien gennem  $P_2, P_3$  og  $P_1, P_2 + P_3$  henholdsvis. Vi skal nu undersøge om ligning 1.8 stemmer overens med ligning 1.9. Da  $\lambda, \kappa, \tau, \mu$  alle afhænger af valget af punkter, er der flere tilfælde at undersøge. Vi vil se på det mest generelle tilfælde, hvor

$$P_1 \neq P_2, P_2 \neq P_3, P_1 + P_2 \neq P_3, P_2 + P_3 \neq P_1$$

↓

$$\begin{aligned} \lambda &= \frac{y_2 - y_1}{x_2 - x_1} \\ \mu &= \frac{y_3 - y_2}{x_3 - x_2} \\ \kappa &= \frac{y_3 - (P_1 + P_2)_y}{x_3 - (P_1 + P_2)_x} = \frac{y_3 - (-\lambda(\lambda^2 - a - x_1 - x_2) - y_2 + \lambda x_2)}{x_3 - (\lambda^2 - a - x_1 - x_2)} \\ &= \frac{y_3 + \lambda(\lambda^2 - a - x_1 - x_2) + y_2 - \lambda x_2}{a - \lambda^2 + x_1 + x_2 + x_3} \end{aligned}$$

og tilsvarende

$$\tau = \frac{y_1 + \mu(\mu^2 - a - x_2 - x_3) + y_2 - \mu x_2}{a - \mu^2 + x_1 + x_2 + x_3}$$

Vi skal nu kontrollere, at ligning 1.8 og ligning 1.9 stemmer overens, dvs.

$$\kappa^2 - \lambda^2 + x_1 + x_2 - x_3 = \tau^2 - \mu^2 + x_2 + x_3 - x_1$$

⇕

$$\kappa^2 - \lambda^2 + \mu^2 - \tau^2 + 2(x_1 - x_3) = 0 \quad (1.10)$$

For  $y$ -koordinaten får vi

$$\{P_1 + (P_2 + P_3)\}_y = -(\tau\{P_1 + (P_2 + P_3)\}_x + y_1 - \tau x_1) \quad (1.11)$$

$$\{(P_1 + P_2) + P_3\}_y = -(\kappa\{(P_1 + P_2) + P_3\}_x + y_3 - \kappa x_3) \quad (1.12)$$

Vi lader nu MAPLE regne på venstre side af ligning 1.10 givet udtrykkene for  $\lambda, \kappa, \tau, \mu$ . Endvidere benytter vi, at  $P_1, P_2, P_3 \in C$  - dvs.  $y_i^2 = x_i^3 + ax_i^2 + bx_i + c$  for  $i = 1, 2, 3$ . Vi ser, at ligning 1.8 og ligning 1.9 stemmer overens. Dette benyttes til sammenligning af de to  $y$ -koordinater. Vi lader MAPLE regne på

$$(\kappa - \tau)\{(P_1 + P_2) + P_3\}_x - y_1 - \kappa x_3 + y_3 + \tau x_1$$

og får at dette er lig 0, hvilket betyder ligning 1.11 og ligning 1.12 er ens. MAPLE udregningerne kan ses på figur 2 i bilag A. Man kan på tilsvarende måde vise associativiteten i de andre tilfælde, dette vil dog ikke blive gjort.  $\square$

## 2. ELLIPTISKE KURVER OVER ENDELIGE LEGEMER

**2.1. Endelige legemer.** Vi skal i dette kapitel se på elliptiske kurver over endelige legemer, dvs. elliptiske kurver med koefficienter i  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$  på formen

$$C_p(\mathbb{F}_p) : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_p \quad (2.1)$$

hvor  $p > 3$  er et primtal. Netop pga. at  $p > 3$ , kan man ved hjælp af simple koordinatskift komme fra den elliptiske kurve fra kapitel 1 til en på formen 2.1. Hvis  $C$  er en elliptisk kurve over  $\mathbb{Q}$  med heltallige koefficienter, skriver vi  $C_p$  når vi har reduceret den elliptiske kurve  $C$ 's koefficienter modulo  $p$ .

*Bemærkning 2.1.* Da  $\Delta \neq 0$  iflg. bemærkning 1.2 vil reduktionen modulo  $p$ ,  $\Delta_p$ , da det er ringhomomorfi, være forskellig fra nul hvis og kun hvis  $p \nmid \Delta$ . Altså vil en kurve forblive en elliptisk kurve under reduktion modulo  $p$  hvis og kun hvis  $p \nmid \Delta$ .

Notationsmæssigt skriver vi i dette kapitel  $a = b$  hvis  $a \equiv b \pmod{p}$ . Målet med dette kapitel er at vise Hasses sætning, der siger, at antallet af punkter på den elliptiske kurve  $C_p$  med koordinater i  $\mathbb{F}_p$  (skrives  $\sharp C_p(\mathbb{F}_p)$ ) er  $p + 1 + \epsilon$ , hvor  $\epsilon$  er en fejlmargen, som skal bestemmes. For at bevise Hasses sætning har vi brug for to lemmaer og lidt om Legendre symbolet, derudover vil vi i beviset arbejde med en elliptisk kurve på formen

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b} \quad (2.2)$$

der er defineret over legemet af rationale funktioner

$$\mathbb{F}_p(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{F}_p[X], g \neq 0 \right\}$$

hvor de variable  $X$  og  $Y$  altså er rationale funktioner med koefficienter i  $\mathbb{F}_p$ . Punkterne på denne elliptiske kurve definerer også en gruppe, selvom den ikke er på Weierstrass-form, dette kan vises ved samme fremgangsmåde som i kapitel 1. Vi får brug for at revidere additionsformlerne 1.6 og 1.7 fra kapitel 1 en smule. Men dette klares ved at bemærke, at de eneste forskelle er, at koefficienten til 2. gradsleddet nu er nul, og at 3. gradsleddet har en konstant foran sig, som man skal gange igennem med, dvs.

$$(P_1 + P_2)_x = [\lambda^2(x^3 + ax + b) - X_1 - X_2] \quad (2.3)$$

$$(2P_0)_x = [\gamma^2(x^3 + ax + b) - 2X_0] \quad (2.4)$$

**2.2. Legendre symbolet.** Vi begynder med at definere en kvadratisk rest. Se [4] for uddybning af dette afsnit.

**Definition 2.2.** For alle  $a$  hvorom det gælder, at  $\text{sfd}(a, m) = 1$  kaldes  $a$  en kvadratisk rest modulo  $m$  hvis  $x^2 \equiv a \pmod{m}$  har en løsning. Altså med vores notation skriver vi bare, at  $a$  er en kvadratisk rest hvis  $x^2 = a$  har en løsning.

Det vil sige, at hvis  $a$  er en kvadratisk rest, kan man finde kvadratroden af  $a$ , nemlig  $x$ . Vi definerer nu Legendre symbolet.

**Definition 2.3.** Hvis  $p > 2$  er et primtal og  $\text{sfd}(a, p) = 1$  så er Legendre symbolet  $\left(\frac{a}{p}\right)_l$  defineret til at være 1 hvis  $a$  er en kvadratisk rest, og  $-1$  hvis  $a$  ikke er en kvadratisk rest, og 0 hvis  $p \mid a$ .

Vi er nu klar til at præsentere sætningen, vi skal bruge. Beviset står i bilag A sætning A.3

**Sætning 2.4.** *Lad  $p > 2$  være et primtal, og  $\text{sfd}(a, p) = 1$ , og lad  $\left(\frac{a}{p}\right)_l$  betegne Legendre symbolet, da gælder*

$$\left(\frac{a}{p}\right)_l = a^{\frac{p-1}{2}}$$

**2.3. Hasses Sætning.** Dette afsnit bygger på [2] s.296-301, men beviset for Hasses sætning blev først vist af Manin [6]. Inden vi viser de to lemmaer, har vi brug for følgende bemærkninger.

$$P_1 = (x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) \text{ og } P_2 = (x, 1)$$

er punkter på vores elliptiske kurve ligning 2.2. Dette ses ved at  $P_2$  giver  $1 = 1$  og  $P_1$  giver

$$(x^3 + ax + b)^{p-1}(x^3 + ax + b) = x^{3p} + ax^p + b$$

⇓

$$x^{3p} + ax^p + b = x^{3p} + ax^p + b$$

Da  $(x + y)^p = x^p + y^p$  og  $b^p = b^{p-1}b = b$  i  $\mathbb{F}_p$ . Vi ved fra kapitel 1, at de projektive løsninger over  $\mathbb{F}_p(x)$  til den elliptiske kurve danner en gruppe, så vi kan lave elementet

$$Z_n = (X_n, Y_n) = P_1 + nP_2 = (x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) + n(x, 1) \quad (2.5)$$

for alle  $n \in \mathbb{Z}$ . Vi vil nu definere en følge  $d_n \in \mathbb{N}$  på følgende måde: Hvis  $Z_n = \mathcal{O}$  er  $d_n = 0$ , ellers er  $Z_n$  på formen  $(X_n, Y_n)$  og vi kan reducere  $X_n$  mest muligt. Skrives tælleren af  $X_n$  som  $T_n$  og nævneren af  $X_n$  som  $N_n$ , så er

$$d_n = \max\{\text{grad}(T_n), \text{grad}(N_n)\}$$

Vi er nu klar med første lemma.

**Lemma 2.5.** *Lad  $d_n$  være defineret som ovenfor, og lad  $\sharp C_p(\mathbb{F}_p)$  betegne antallet af projektive løsninger til den elliptiske kurve, ligning 2.1. Da er*

$$d_{-1} - d_0 - 1 = \sharp C_p(\mathbb{F}_p) - p - 1$$

*Bevis.* Hvis vi sætter  $n = 0$  i ligning 2.5, får vi at  $d_0 = \text{grad}(x^p) = p$ . Lad  $N_p = \sharp C_p(\mathbb{F}_p) - 1$  være antallet af affine løsninger. Hvis vi nu kan vise, at

$$d_{-1} = N_p + 1$$

er vi færdige. Vi prøver at udregne  $X_{-1}$  med de nye additionsformler, og vi får

$$\begin{aligned} X_{-1} &= (Z_{-1})_x \\ &= (P_1 - P_2)_x \\ &= -x - x^p + \left(\frac{1 + (x^3 + ax + b)^{\frac{p-1}{2}}}{x - x^p}\right)^2 (x^3 + ax + b) \\ &= \frac{-(x + x^p)(x - x^p)^2 + (x^3 + ax + b)^p + (x^3 + ax + b) + 2(x^3 + ax + b)^{\frac{p+1}{2}}}{(x - x^p)^2} \end{aligned} \quad (2.6)$$

Reduceres dette yderligere, får vi at  $x^{3p}$  leddene går ud, og tilbage får vi

$$X_{-1} = \frac{x^{2p+1} + R(x)}{(x - x^p)^2} \quad (2.7)$$

hvor  $\text{grad}(R(x)) \leq 2p$ , altså er graden af tælleren 1 større end graden af nævneren, så  $d_{-1} = \text{grad}(T_{-1})$ , og  $d_{-1} - 1 = \text{grad}(N_{-1})$ . Vi vil nu reducere  $X_{-1}$  så meget som muligt, til det formål, er det nok at reducere brøken i ligning 2.6. Nævneren i denne brøk kan skrives som

$$(x - x^p)^2 = (x(1 - x^{p-1}))^2$$

Men da  $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, (p-1)\}$  er cyklisk gælder der, at  $x^{(p-1)} = 1 \forall x \in (\mathbb{Z}/p\mathbb{Z})^*$  så vi kan nu skrive

$$(x - x^p)^2 = [x(x-1)(x-2) \cdots (x-(p-1))]^2 = \prod_{j \in \mathbb{Z}/p\mathbb{Z}} (x-j)^2$$

Vi vil nu se på tælleren af brøken i ligning 2.6 som ifølge sætning 2.4 kan skrives

$$\left(1 + \left(\frac{x^3 + ax + b}{p}\right)_l\right)^2 (x^3 + ax + b)$$

Denne brøk forsvinder for de  $j$  hvorom det gælder, at  $\left(\frac{j^3 + aj + b}{p}\right)_l = -1$ , men hvis

$$\left(1 + \left(\frac{x^3 + ax + b}{p}\right)_l\right)^2 = 0$$

må det altså betyde, at  $(x-j)$  er en faktor to gange, og de bliver forkortet ud af nævneren. Tælleren giver også nul hvis  $(x-j)$  er en faktor i  $(j^3 + aj + b)$ , men den forekommer kun én gang, da der er tre forskellige rødder i en elliptisk kurve. De faktorer, der nu er tilbage i nævneren, er de  $(x-j)^2$  hvorom der gælder, at  $\left(\frac{j^3 + aj + b}{p}\right)_l = 1$  og de  $(x-j)$  hvorom der gælder, at  $\left(\frac{j^3 + aj + b}{p}\right)_l = 0$ . Men at  $\left(\frac{j^3 + aj + b}{p}\right)_l = 1$  betyder jo iflg. definition 2.2, at

$$\exists y : y^2 = j^3 + aj + b,$$

så vi har altså (da det er  $(x-j)^2$ ) to løsninger til vores elliptiske kurve og for  $\left(\frac{j^3 + aj + b}{p}\right)_l = 0$  har vi én løsning, nemlig  $y = 0$ . Dette giver præcis  $N_p$ , de affine løsninger til  $C_p(\mathbb{F}_p)$ . Altså  $d_{-1} - 1 = N_p$  og lemmaet er vist.  $\square$

**Lemma 2.6.** *Der gælder, at*

$$d_{n-1} + d_{n+1} = 2d_n + 2 \tag{2.8}$$

for alle  $n \in \mathbb{Z}$

*Bevis.* Antag først, at en af  $Z_{n-1}, Z_n, Z_{n+1}$  er lig  $\mathcal{O}$ , så er de to andre iflg. ligning 2.5 forskellig fra  $\mathcal{O}$ . Lad nu  $Z_n = \mathcal{O}$ , så er  $d_n = 0$  og

$$Z_{n+1} = (x, 1), \quad Z_{n-1} = -(x, 1) = (x, -1)$$

men så er  $d_{n-1} = d_{n+1} = 1$  og ligning 2.8 er opfyldt. Lad nu  $Z_{n-1} = \mathcal{O}$  så er  $d_{n-1} = 0$  og  $Z_n = (x, 1) = P_2$  og

$$Z_{n+1} = P_1 + (n+1)P_2 = (P_1 + nP_2) + P_2 = Z_n + Z_n$$

$x$ -koordinaten af  $Z_{n+1}$  fås fra formel 2.4.

$$\begin{aligned}
 (2Z_n)_x &= [\gamma^2(x^3 + ax + b) - 2X] \\
 &= \left(\frac{3X^2 + a}{(x^3 + ax + b)2y}\right)^2(x^3 + ax + b) - 2X \\
 &= \frac{X^4 - 2aX^2 + 8bX}{4(X^3 + aX + b)} \\
 &= \frac{(X^2 - a)^2 - 8bX}{4(X^3 + aX + b)}
 \end{aligned}$$

Indsættes nu  $X = x$  får vi, at vi kan skrive

$$Z_{n+1} = \frac{f'(x)^2 - 8xf(x)}{4f(x)}$$

og da  $\text{sfd}(f, f') = 1$  er brøken uforkortelig og  $d_{n+1} = 4$  og  $d_n = 1$  og ligning 2.8 er igen opfyldt. Sidste tilfælde, med  $Z_{n+1} = \mathcal{O}$  vises på tilsvarende måde som  $Z_{n-1} = \mathcal{O}$ .

Antag nu, at ingen af  $Z_{n-1}, Z_n, Z_{n+1}$  er lig  $\mathcal{O}$ , og skriv  $X_{n-1}, X_n, X_{n+1}$  som uforkortede brøker

$$X_{n-1} = \frac{A}{B}, \quad X_n = \frac{P}{Q}, \quad X_{n+1} = \frac{C}{D}$$

Da  $Z_{n+1} = Z_n + (x, 1) = (X_n, Y_n) + (x, 1)$  medfører det, at

$$\begin{aligned}
 X_{n+1} &= -\frac{P}{Q} - x + \frac{(1 - Y_n)^2(x^3 + ax + b)}{(x - \frac{P}{Q})^2} \\
 &= -\frac{P + Qx}{Q} + \frac{(1 - Y_n)^2(x^3 + ax + b)Q^2}{(Qx - P)^2} \\
 &= \frac{-(Qx + P)(Qx - P)^2 + (1 - Y_n)^2(x^3 + ax + b)Q^3}{Q(Qx - P)^2} \tag{2.9}
 \end{aligned}$$

på lignende vis får vi

$$X_{n-1} = \frac{-(Qx + P)(Qx - P)^2 + (1 + Y_n)^2(x^3 + ax + b)Q^3}{Q(Qx - P)^2} \tag{2.10}$$

Med disse formler kan vi nu udregne

$$\frac{1}{2}(X_{n-1} + X_{n+1}) = \frac{PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ}{(Qx - P)^2} \tag{2.11}$$

$$X_{n-1}X_{n+1} = \frac{(Px - aQ)^2 - 4bQ(Qx + P)}{(Qx - P)^2} \tag{2.12}$$

Men  $X_{n-1}X_{n+1} = \frac{AC}{BD}$  og vi påstår, at

$$(Qx - P)^2 \mid BD. \tag{2.13}$$

At det gælder er ikke trivielt og det vises til sidst i lemmaet. Hvis  $S$  er den største fælles divisor af  $AC$  og  $BD$  giver ligning 2.12

$$AC = S[(Px - aQ)^2 - 4bQ(Qx + P)] \tag{2.14}$$

$$BD = S(Qx - P)^2 \quad (2.15)$$

og tælleren i ligning 2.11 giver

$$AD + BC = 2S[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ] \quad (2.16)$$

Lad  $F$  være en primfaktor i  $S$ , altså et irreducibelt polynomium. Iflg. ligning 2.15 har vi så at  $F|BD$ , antag at  $F|B$ , det betyder, da  $\text{sfd}(A, B) = 1$ , at  $F \nmid A$ . Og iflg. ligning 2.14 ser vi at  $F|AC$ , men det vil sige, at  $F|C$ , så  $F|BC$ . Til slut har vi iflg. ligning 2.16 der fortæller os, at  $F|(AD + BC)$ . Men så må  $F|AD$  hvilket vil sige at  $F|D$ , da  $F$  ikke gik op i  $A$ . Så har vi både  $F|C$  og  $F|D$ , men det er en modstrid af  $\text{sfd}(C, D) = 1$ . Altså må  $S \in \mathbb{F}_p$  og vi har vist, at

$$BD = (Qx - P)^2. \quad (2.17)$$

Op til en  $\mathbb{F}_p$  faktor, altså er  $\text{grad}(BD) = \text{grad}[(Qx - P)^2]$ . Det var de indledende manøvre, nu går vi over til at se på  $d_{n-1}$ ,  $d_n$  og  $d_{n+1}$ .

$$d_{n-1} = \max(\text{grad}(A), \text{grad}(B))$$

$$d_n = \max(\text{grad}(P), \text{grad}(Q))$$

$$d_{n+1} = \max(\text{grad}(C), \text{grad}(D))$$

Vi deler nu beviset for lemmaet op i følgende tilfælde:

**a:**  $d_{n-1} = \text{grad}(A)$  og  $d_{n+1} = \text{grad}(C)$

**b:**  $d_{n-1} = \text{grad}(B)$  og  $d_{n+1} = \text{grad}(D)$

**c:**  $d_{n-1} = \text{grad}(A)$  og  $d_{n+1} = \text{grad}(D)$ ,  
hvor  $\text{grad}(A) > \text{grad}(B)$  og  $\text{grad}(D) > \text{grad}(C)$

**d:**  $d_{n-1} = \text{grad}(B)$  og  $d_{n+1} = \text{grad}(C)$ ,  
hvor  $\text{grad}(B) > \text{grad}(A)$  og  $\text{grad}(C) > \text{grad}(D)$

Tilfælde a: Fra ligning 2.14 har vi, at

$$d_{n-1} + d_{n+1} = \text{grad}(A) + \text{grad}(C) = \text{grad}(AC) = \text{grad}[(Px - aQ)^2 - 4bQ(Qx + P)]$$

Hvis  $\text{grad}(P) \geq \text{grad}(Q)$ , så er leddet af højeste grad ( $P^2x^2$ ) og da  $\text{grad}(P) = d_n$  og  $\text{grad}(x^2) = 2$ , er højre side lig  $2d_n + 2$  og ligning 2.8 er vist. Hvis  $\text{grad}(P) < \text{grad}(Q)$  giver ligning 2.17

$$\text{grad}(BD) = \text{grad}(Q^2x^2) = 2\text{grad}(Q) + 2$$

på den anden side ved vi fra ligning 2.14 at der gælder

$$\begin{aligned} \text{grad}(AC) &\leq \max(2\text{grad}(P) + 2, 2\text{grad}(Q), 2\text{grad}(Q) + 1, \text{grad}(P) + \text{grad}(Q)) \\ &\leq 2\text{grad}(Q) + 1 < \text{grad}(BD) \end{aligned}$$

Men dette er i modstrid med antagelsen i tilfælde a, så  $\text{grad}(P) < \text{grad}(Q)$  er umulig.

Tilfælde b: Fra ligning 2.17 har vi at

$$d_{n-1} + d_{n+1} = \text{grad}(BD) = \text{grad}[(Qx - P)^2]$$

Så hvis  $\text{grad}(Q) \geq \text{grad}(P)$ , så er højeste grads leddet ( $Q^2x^2$ ), og højresiden giver  $2d_n + 2$  og ligning 2.8 er opfyldt. På den anden side, hvis  $\text{grad}(Q) < \text{grad}(P)$  har vi iflg. ligning 2.14 at

$$\text{grad}(AC) = \text{grad}(P^2x^2) > \text{grad}(P) \geq \text{grad}(BD)$$

men dette er en modstrid af antagelsen i tilfælde b, så  $\text{grad}(Q) < \text{grad}(P)$  er ikke muligt.

Tilfælde c: Da  $\text{grad}(A) > \text{grad}(B)$  og  $\text{grad}(D) > \text{grad}(C)$  følger, at  
 $\text{grad}(AD) > \text{grad}(AC)$ ,  $\text{grad}(AD) > \text{grad}(BD)$ ,  $\text{grad}(AD) > \text{grad}(BC)$  (2.18)

Så fra ligning 2.16 ses nu, at

$$\begin{aligned} \text{grad}(AD) &= \text{grad}(AD + BC) \\ &= \text{grad}(PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ) \end{aligned} \quad (2.19)$$

Hvis  $\text{grad}(P) \geq \text{grad}(Q)$  så er ligning 2.19

$$\text{grad}(AD) \leq \text{grad}(P^2x^2) = \text{grad}(AC)$$

hvilket er i strid mod den første ulighed i 2.18. Hvis  $\text{grad}(P) < \text{grad}(Q)$  er ligning 2.19

$$\text{grad}(AD) \leq \text{grad}(Q^2x^2) = \text{grad}(BD)$$

hvilket er i strid mod den anden ulighed i 2.18, så tilfælde c er umulig.

Tilfælde d: Er symmetrisk med tilfælde c, og er altså heller ikke mulig.

Vi har nu vist at ligning 2.8 er opfyldt for alle tilfælde. Kan vi nu vise ligning 2.13, er vi færdige. Denne mangel i [2] er vist i [3].

Vi kan skrive ligning 2.9 som

$$\begin{aligned} X_{n+1} &= \frac{-(Qx + P)(Qx - P)^2 + (1 - Y_n)^2(x^3 + ax + b)Q^3}{Q(Qx - P)^2} \\ &= \frac{(Qx + P)(Px + aQ) + 2bQ^2 - 2Y_n(x^3 + ax + b)Q^2}{(Qx - P)^2} \end{aligned} \quad (2.20)$$

$$= \frac{S}{(Qx - P)^2} \quad (2.21)$$

og ligning 2.10 som

$$X_{n-1} = \frac{R}{(Qx - P)^2}. \quad (2.22)$$

så får vi, at ligning 2.12 kan skrives som

$$X_{n-1}X_{n+1} = \frac{(Px - aQ)^2 - 4bQ(Qx + P)}{(Qx - P)^2} = \frac{RS}{(Qx - P)^4} = \frac{AC}{BD} \quad (2.23)$$

Vi skal altså at vise at

$$(Qx - P)^2 | BD. \quad (2.24)$$

Antag at det ikke gælder: Så findes et irreducibelt polynomium  $f$  som er faktor i  $(Qx - P)$ , således at  $f$  går op i  $(Qx - P)^2$  i en højere potens end i  $BD$ , eller udtrykt ved diskret valuation funktionen  $\nu_f$  (se bilag A afsnit A.4.)

$$\nu_f((Qx - P)^2) > \nu_f(BD)$$

Så iflg. 2.23 har vi, at

$$f(x) | (Px - aQ)^2 - 4bQ(Qx + P) = T \quad (2.25)$$

da  $f$  går op i  $(Qx - P)^2$  flere gange end i  $BD$ , så må  $f$  også gå op i  $T$ . Antag nu, at  $f|R$  og  $f|S$  (dette vises senere). Pr. konstruktion af  $f$  gælder nu at

$$f | (1 - Y_n)^2(x^3 + ax + b)Q^3.$$

og

$$f | (1 + Y_n)^2(x^3 + ax + b)Q^3.$$

Vi ved at  $\text{sfd}(Q, f) = 1$ , da  $f$  ellers ville være en fælles faktor af  $P$  og  $Q$ . Antag at

$$f|(1 - Y_n)^2 \Rightarrow f|(1 - Y_n)$$

$$f|(1 + Y_n)^2 \Rightarrow f|(1 + Y_n)$$

men det betyder, at

$$f|(1 - Y_n) + (1 + Y_n) = 2$$

Men dette er en modstrid af at  $f$  er et irreducibelt polynomium, så alt i alt giver det os at

$$f|(x^3 + ax + b).$$

Ved division med rest af  $T$  med  $(Qx - P)$  får vi udtrykket

$$T = -(Qx - P)[P^2x + (x^3 + 2ax - 4b)P] + (x^4 - 2ax^2 - 8bx + a^2)Q^2$$

Altså har vi også, at

$$f|(x^4 - 2ax^2 - 8bx + a^2)$$

da  $f|T$  iflg. ligning 2.25. Udregnes diskriminanten  $\Delta$  giver det os

$$\Delta = (3x^3 - 5ax - 27b)(x^3 + ax + b) - (3x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2)$$

så  $f|\Delta \neq 0$ , men så går  $f$  op i en konstant, hvilket er en modstrid af konstruktionen af  $f$  og så er ligning 2.24 vist, hvis vi kan vise, at  $f|R$  og  $f|S$ .

Antag at  $f|R$  men at  $f \nmid S$ . Ligning 2.21 siger, at

$$\frac{S}{(Qx - P)^2} = \frac{C}{D}$$

men da  $f \nmid S$ , må der gælde, at

$$\nu_f(D) = \nu_f(Qx - P)^2 > 0. \quad (2.26)$$

Den er større end nul pr. konstruktion. Men så gælder jo også, at  $\nu_f(C) = 0$ , altså at  $f \nmid C$ . Hvilket giver os fra ligning 2.23, da  $\nu_f(T) > 0$ , at

$$(AC)(Qx - P)^2 = (BD)T$$

Udtrykt ved valuationsfunktionen og ligning 2.26 giver det

$$\nu_f(A) - \nu_f(B) = \nu_f(T)$$

Da  $\text{sfd}(A, B) = 1$  medfører det, at  $\nu_f(B) = 0$ , så

$$\nu_f(BD) = \nu_f(Qx - P)^2$$

iflg. ligning 2.26. Men dette er en modstrid af den oprindelige antagelse om  $f$ , så  $f|S$ . På samme måde vises at  $f|R$ . Vi har nu vist ligning 2.13, og lemmaet er vist.  $\square$

**Korollar 2.7.** *Det gælder, at*

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0 \quad (2.27)$$

for alle  $n \in \mathbb{Z}$

*Bevis.* Induktion: For  $n = 0$  bliver ligning 2.27:  $d_0 = 0 - (d_{-1} - d_0 - 1)0 + d_0 = d_0$  og for  $n = -1$  får vi  $d_{-1} = 1 + d_{-1} - d_0 - 1 + d_0 = d_{-1}$ . Antag nu at 2.27 gælder for  $n = k$ , vis at den gælder for  $n = k + 1$ . Iflg. ligning 2.8 gælder, at

$$\begin{aligned} d_{k+1} &= 2d_k + 2 - d_{k-1} \\ &= 2[k^2 - (d_{-1} - d_0 - 1)k + d_0] + 2 - [(k-1)^2 - (d_{-1} - d_0 - 1)(k-1) + d_0] \\ &= 2k^2 - k^2 - 1 + 2k - (d_{-1} - d_0 - 1)k - (d_{-1} - d_0 - 1) + 2d_0 - d_0 + 2 \\ &= k^2 + 2k + 1 - (d_{-1} - d_0 - 1)k - (d_{-1} - d_0 - 1) + d_0 \\ &= (k+1)^2 - (d_{-1} - d_0 - 1)(k+1) + d_0 \end{aligned}$$

Ligning 2.27 gælder nu for  $n \in \mathbb{N}$ , men ligningen gælder jo også for  $n = -1$ , så antag nu at 2.27 gælder for  $n = -k$ , vis at den gælder for  $n = -(k+1)$ . Vi kan genbruge beviset fra før og få:

$$\begin{aligned} d_{-k-1} &= 2d_{-k} + 2 - d_{-k+1} \\ &= k^2 + 2k + 1 - (d_{-1} - d_0 - 1)(-k-1) + d_0 \\ &= (-k-1)^2 - (d_{-1} - d_0 - 1)(-k-1) + d_0 \end{aligned}$$

Ligning 2.27 gælder altså for alle  $n \in \mathbb{Z}$  og korollaret er vist.  $\square$

Med de to ovenstående lemmaer og dette korollar til vores rådighed er vi nu klar til at vise Hasses sætning.

**Sætning 2.8** (Hasse). *Lad  $C_p(\mathbb{F}_p)$  være en elliptisk kurve på formen 2.1. Så er*

$$|p + 1 - \sharp C_p(\mathbb{F}_p)| \leq 2\sqrt{p} \quad (2.28)$$

*Bevis.* Substituerer vi resultatet fra lemma 2.5 ind i ligning 2.27 og bruger, at  $d_0 = p$  får vi

$$d_n = n^2 + (p + 1 - \sharp C_p(\mathbb{F}_p))n + p = n^2 + a_p n + p \quad (2.29)$$

hvor  $a_p = p + 1 - \sharp C_p(\mathbb{F}_p)$ . Vi vil nu vise, at 2. gradspolynomiet

$$x^2 + a_p x + p \quad (2.30)$$

er  $\geq 0$  for alle  $x \in \mathbb{R}$ . Da  $d_n$ 'erne  $\geq 0$ , da de jo er graden af polynomier, kan 2.30 ikke være negativ i et interval af længde  $> 1$  indeholdende  $n$  og  $n + 1$ . Hvis  $D$  er diskriminanten, vil  $\sqrt{D}$ , være et mål for afstanden mellem de to nulpunkter af 2.30,  $x_1$  og  $x_2$ , da

$$|x_1 - x_2| = \left| \frac{-B + \sqrt{D} - (-B - \sqrt{D})}{2A} \right| = \left| \frac{2\sqrt{D}}{2A} \right| = \sqrt{D}$$

da  $A = 1$  i vores tilfælde. Men så kan 2.30 ikke være negativ i et interval af længde  $< 1$  mellem  $n$  og  $n + 1$ , da  $D = a_p^2 - 4p$  er et heltal og kvadratroden af et heltal er  $\geq 1$ . Den sidste mulighed der er, for at 2.30 er negativ for nogle  $x \in \mathbb{R}$ , er hvis to på hinanden følgende  $d_n$ 'er er nul. Men to på hinanden følgende  $d_n$ 'er kan ikke være lige, for hvis de var det, ville alle  $d_n$ 'er være lige iflg. ligning 2.8, men  $d_0 = p$  er ulige (da vi jo ser på primtal  $p > 3$ ). Så specielt kan to på hinanden følgende  $d_n$ 'er ikke være lig nul. Vi har altså vist at ligning 2.30, og dermed også 2.29, må have diskriminant  $D \leq 0$ , dvs.

$$D = a_p^2 - 4p \leq 0$$

$\Leftrightarrow$ 

$$a_p^2 \leq 4p$$

 $\Leftrightarrow$ 

$$|a_p| \leq 2\sqrt{p}.$$

Hasses sætning er hermed vist.  $\square$

*Bemærkning 2.9.* Hasses sætning gælder også for tilfældet  $p = 3$ , og det ses let på følgende måde. Da der er 3 elementer i  $\mathbb{F}_3$  får vi maksimalt 7 punkter der løser ligning 2.1 når vi tæller  $\mathcal{O}$  med, altså  $\sharp C_p(\mathbb{F}_3) \in [1, \dots, 7]$ . Men det betyder, da  $3 < 2\sqrt{3}$  at

$$|3 + 1 - \sharp C_p(\mathbb{F}_3)| \leq 3 < 2\sqrt{3}$$

og sætningen er vist for  $p = 3$ .

**Eksempel 2.10** (Hasses sætning i praksis). Betragt en elliptiske kurve  $y^2 = x^3 + ax + b$  i  $\mathbb{F}_5$ , der iflg. Hasse skulle have

$$|5 + 1 - \sharp C(\mathbb{F}_5)| \leq 2\sqrt{5} \simeq 4,5$$

altså  $\sharp C(\mathbb{F}_5) \in [2, \dots, 10]$  Vælg nu  $y^2 = x^3 + 2x$ . Først undersøger vi om den er glat vha. ligning 1.2, og får

$$\Delta = -4a^3 - 27b^2 = [-32]_5 = 3 \neq 0.$$

Punkterne på denne elliptiske kurve er da  $\mathcal{O}$  som altid, og det affine punkt  $(0, 0)$ , altså 2 punkter. Vi prøver med  $y^2 = x^3 + 3x$  og får

$$\Delta = -4a^3 - 27b^2 = [-108]_5 = 2 \neq 0$$

de affine punkterne her er

$$(0, 0); (1, 2); (1, 3); (2, 2); (2, 3); (3, 1); (3, 4); (4, 1); (4, 4)$$

plus  $\mathcal{O}$ , alt i alt 10 punkter.

### 3. LENSTRAS FAKTORISERINGSALGORITME

Aritmetikkens fundamentalsætning siger, at de naturlige tal entydigt kan skrives som produktet af deres primtalsfaktorer. Der er (så vidt vides) imidlertid ikke nogen hurtig måde at gøre dette på, og rent praktisk er det alt for tidskrævende bare at dividere med  $2, 3, 4, \dots, \sqrt{n}$  for at finde en primfaktor i  $n$ , hvis  $n$  er stor. Faktisk, hvis man vil benytte denne metode til at faktorisere et 100 ciffer stort tal, der er et produkt af to 50 ciffer store tal, må man udføre ca.  $10^{50}$  divisioner. Antager vi, at vi på en computer kan udføre  $10^{10}$  divisioner i sekundet, vil det tage os  $10^{-40}$  sekunder eller ca.  $10^{32}$  år. Sammenlignet med universets alder på omkring  $5 \cdot 10^9$  år, ser vi tydeligt at denne metode ikke er brugbar. I dette kapitel skal vi se på en hurtigere og snedig metode til at finde en faktor i et sammensat tal  $n$ , nemlig Lenstras faktoreringsalgoritme, der gør brug af gruppestrukturen på elliptiske kurver. En vigtig brik i algoritmen, er følgende afbildning.

**Definition 3.1.** Lad  $P = (X : Y : Z) \in \mathbb{P}^2(\mathbb{Q})$  være et punkt i det projektive plan med  $X, Y, Z \in \mathbb{Q}$ , hvor ikke alle er nul. Vi ved fra kapitel 1 at vi kan skalere indgangene, så vi kan antage, at  $X, Y, Z \in \mathbb{Z}$  og at de ingen fælles faktorer har. Vi kan nu definere afbildningen

$$r_p : \mathbb{P}^2(\mathbb{Q}) \rightarrow \mathbb{P}^2(\mathbb{F}_p)$$

som reduktionen af punktet  $P$  modulo  $p$ , dvs.

$$P = (X : Y : Z) \mapsto P_p = (X_p : Y_p : Z_p)$$

hvor  $P_p = (X_p : Y_p : Z_p) \neq (0 : 0 : 0)$ , da  $p$  ellers ville være en fælles faktor i  $X, Y, Z \in \mathbb{Z}$  og dette ville være i strid mod antagelsen.

Vi vil nu vise, at denne afbildning er en gruppehomomorfi.

**Lemma 3.2.** *Reduktionen modulo  $p$ ,  $r_p : \mathbb{P}^2(\mathbb{Q}) \rightarrow \mathbb{P}^2(\mathbb{F}_p)$  er en gruppehomomorfi. Dvs, at  $r_p(P_1 + P_2) = r_p(P_1) + r_p(P_2)$ , altså om man bruger gruppekompositionen og derefter reducerer modulo  $p$  eller om man først reducerer og så bruger kompositionen, er underordnet.*

*Bevis.* Lad  $f(X, Y, Z) \in \mathbb{Z}[X, Y, Z]$  være et polynomium tilhørende polynomiumsringen  $\mathbb{Z}[X, Y, Z]$ , vi kan da skrive  $f$  som

$$f(X, Y, Z) = \sum a_{ijk} X^i Y^j Z^k = 0, \quad a_{ijk} \in \mathbb{Z}$$

hvor summationsgrænserne er uden betydning til vores formål. Dette udtryk kan vi reducere modulo  $p$  og vi får

$$\left( \sum a_{ijk} X^i Y^j Z^k \right)_p = 0_p.$$

Men er dette det samme som

$$f_p(X_p, Y_p, Z_p) = \sum (a_{ijk})_p X_p^i Y_p^j Z_p^k = 0_p.$$

Svaret er ja, da reduktion modulo  $p$  er en ringhomomorfi, så  $(x^i)_p = (x_p)^i$ .  $f(X, Y, Z)$  er jo bare et polynomium, så specielt kan det være en elliptisk kurve  $C$  over  $\mathbb{Q}$ , og så vil  $r_p(C)$  også være en elliptisk kurve med koefficienter i  $\mathbb{F}_p$  (medmindre  $p|\Delta$ ). Men med kompositionen på elliptiske kurver, vil  $P, Q, P * Q \in C(\mathbb{Q})$  ligge på en ret linie, og da en linie også er et polnomielt udtryk, vil også  $r_p(P), r_p(Q), r_p(P * Q) \in C(\mathbb{F}_p)$  ligge på en ret linie. Altså har vi, at

$$r_p : \mathbb{P}^2(\mathbb{Q}) \rightarrow \mathbb{P}^2(\mathbb{F}_p)$$

og specielt

$$r_p : C(\mathbb{Q}) \rightarrow C(\mathbb{F}_p)$$

er en gruppehomomorfi, og vi har vist lemmaet.  $\square$

Vi får også bruge for følgende lemma, se [1] s.68.

**Lemma 3.3.** *Antag at  $C : y^2 = x^3 + ax + b$ , hvor  $a, b \in \mathbb{Q}$ , er en elliptisk kurve og at  $P$  er et punkt på  $C$ . Da er  $P$  på formen  $P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$  eller i projektive koordinater*

$$P = \left(\frac{a}{d^2} : \frac{b}{d^3} : 1\right) = (ad : b : d^3)$$

hvor  $\text{sfd}(a, d) = \text{sfd}(b, d) = 1$ .

*Bevis.* Antag at  $P = (\frac{m}{M}, \frac{n}{N})$ , hvor  $\frac{m}{M}$  og  $\frac{n}{N}$  er to uforkortelige brøker og at  $M, N > 0$ . Indsætter vi nu  $P$  i  $C$  får vi

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m}{M} + b \quad (3.1)$$

$\Downarrow$

$$n^2 M^3 = m^3 N^2 + amM^2 N^2 + bM^3 N^2 \quad (3.2)$$

Da venstre og højre side af ligning 3.2 er hele tal, må der, når vi dividerer med  $N^2$ , stadig stå et helt tal på højre side og da  $N^2 \nmid n^2$  må  $N^2 | M^3$ . På samme måde fås, at  $M^2 | N^2$ . Men vi kan også skrive ligning 3.1 som

$$n^2 = m^3 \frac{N^2}{M^3} + am \frac{N^2}{M} + bN^2$$

hvilket viser, at  $M^3 | N^2$ , og det giver os, at

$$M^3 = N^2.$$

Sæt nu  $d = \frac{N}{M}$ , der er et helt tal, da  $M^2 | N^2$ . Da får vi:

$$d^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M$$

og

$$d^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N$$

Altså må  $P$  være på formen  $P = (\frac{a}{d^2}, \frac{b}{d^3})$  og lemmaet er vist.  $\square$

**3.1. Lenstras ide.** Ideen bag Lenstras algoritme bygger på Pollards  $(p-1)$ -metode, se [5] s. 25, og er som følger: Lad  $n \in \mathbb{N}$  og lad  $p$  være et primtal hvorom der gælder, at  $p|n$ . Vælg nu en elliptisk kurve  $C$  og et punkt  $P \in C(\mathbb{Q})$ . Så er  $r_p(C(\mathbb{Q})) = C_p(\mathbb{F}_p)$  og  $r_p(P) = P_p$ . Nu vælges  $k \in \mathbb{N}$  således, at  $\#C_p(\mathbb{F}_p) | k$ , så ved vi, at  $kP_p = \mathcal{O}_p$ , se [5] prop.3.5.2. s.57. Vi ved også fra lemma 3.3 at  $P$  er på formen  $P = (ad : b : d^3) \in C(\mathbb{Q})$ , så hvis vi erindrer at  $\mathcal{O} = (0 : 1 : 0)$ , kan vi se at det gælder at

$$r_p(P) = \mathcal{O}_p \Leftrightarrow p|d.$$

Men det vil altså sige, da

$$r_p(kP) = kr_p(P) = kP_p = (a_k d_k : b_k : d_k^3) = \mathcal{O}_p$$

at  $p|d_k$ . Men vi havde også, at  $p|n$ , så  $\text{sfd}(d_k, n) \geq p$ , men hvis  $\text{sfd}(d_k, n) < n$  så har vi fundet en divisor, og vi er færdige.

**3.2. Lenstras algoritme.** Vi er nu klar til at give en beskrivelse af Lenstras faktoreringsalgoritme, [1] s.133. Antag  $n > 2$  ikke er et primtal, som vi ønsker at finde en faktor i.

**1:** Beregn  $D_1 = \text{sfd}(6, n)$ .

**a:** Hvis  $D_1 > 1$  har vi fundet en faktor og vi er færdige.

**b:** Hvis  $D_1 = 1$  fortsætter vi.

**2:** Vælg tilfældigt  $x, y, a \in \mathbb{Z}$  mellem 1 og  $n$  lad så  $b = y^2 - x^3 - ax$ , på denne måde har vi en elliptisk kurve  $C : y^2 = x^3 + ax + b$  og punktet  $P = (x, y)$  som pr. konstruktion ligger på  $C$ . Beregn også  $\Delta = 4a^3 + 27b^2$  som jo skal være forskellig fra nul, ellers gå tilbage til start af **2**.

**3:** Udregn  $D_2 = \text{sfd}(\Delta, n) = \text{sfd}(4a^3 + 27b^2, n)$ .

**a:** Hvis  $D_2 = n$ , gå tilbage til **2** og vælg et nyt  $a$ .

**b:** Hvis  $1 < D_2 < n$  ved vi, at  $D_2|n$  og vi har fundet en faktor i  $n$  og vi er færdige.

**c:** Hvis  $D_2 = 1$  fortsætter vi.

**4:** Vælg et  $K \in \mathbb{N} > 1$ , og lad  $k = \text{mfm}(1, 2, \dots, K)$ .

**5:** Udregn  $kP = (a_k d_k : b_k : d_k^3)$ .

**6:** Udregn  $D_3 = \text{sfd}(d_k, n)$ .

**a:** Hvis  $D_3 = n$ , gå til **4** og vælg et mindre  $k$ .

**b:** Hvis  $D_3 = 1$  kan vi enten gå til **2** og vælge et nyt  $a$  eller vi kan gå til **4** og vælge et mindre  $k$ .

**c:** Hvis  $1 < D_3 < n$  har vi fundet en faktor, og vi er færdige.

Dette er i al sin enkelthed Lenstras algoritme, som altså udnytter egenskaberne ved elliptiske kurver til at belyse nogle tal, som værende kandidater til at faktorisere  $n$ . Vi vil nu knytte et par kommentarer til de enkelte skridt i algoritmen.

**add. 1:** Hvis  $D_1 = \text{sdf}(6, n) = 1$  går hverken 2 eller 3 op i  $n$ .

**add. 3:** Her undersøges, om  $C_p$  er en elliptisk kurve, for hvis  $D_2 = \text{sfd}(\Delta, n) = n$  betyder det, at  $n|\Delta$  og så kan  $C_p$  ikke være en elliptisk kurve iflg. bemærkning 2.1. Hvis  $\Delta = 0$  vil  $D_2 = \text{sfd}(\Delta, n) = n$ , så faktisk undersøges her både om  $C$  og  $C_p$  er elliptiske kurver iflg. bemærkning 1.2.

**add. 4:** Iflg. ideen bag algoritmen vælges  $k$  i håb om, at  $\#C_p(\mathbb{F}_p)|k$  for et  $p|n$ .

**add. 5:** Ved beregningen af  $kP$  er der et par praktiske problemer. For det første vil  $P + P + \dots + P$ ,  $k$  gange tage alt for lang tid at udregne, så i stedet benytter vi os af, at vi kan skrive

$$k = 2^0 k_0 + 2^1 k_1 + 2^2 k_2 + 2^3 k_3 + \dots + 2^r k_r$$

hvor  $k_i$  er enten 0 eller 1, herefter kan vi nu udregne

$$\begin{aligned} P_0 &= P \\ P_1 &= 2P_0 = 2P \\ P_2 &= 2P_1 = 2^2 P \\ &\vdots \\ P_r &= 2P_{r-1} = 2^r P \end{aligned} \tag{3.3}$$

På denne måde får vi, at

$$kP = \sum_{i:k_i=1} P_i$$

Hvilket er meget hurtigere for store  $k$ , faktisk kan man klare beregningerne i mindre end  $2 \log_2(k)$  skridt. Næste problem er, at udregningen af de rationale koordinater af  $kP$ , for store  $k$ , igen bliver alt for regneteknisk krævende. Det ville være meget lettere, at regne modulo  $n$ . Men da  $n$  ikke er et primtal, er  $\mathbb{Z}/n\mathbb{Z}$  ikke et legeme. Problemerne opstår når vi vil bruge formlerne for at addere to punkter. Det er ikke givet at vi kan finde et inverst element til  $(x_2 - x_1)$  i

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

eller til  $2y$  i

$$\gamma = \frac{3x^2 + a}{2y}.$$

Hvis vi alligevel prøver at regne på første tilfælde, er der 3 mulige udfald.

- a:** Hvis  $\text{sfd}(x_2 - x_1, n) = 1$  har  $x_2 - x_1$  et inverst element i  $\mathbb{Z}/n\mathbb{Z}$  (iflg. lemma 3.4), så vi kan bruge additionsformlen.
- b:** Hvis  $1 < \text{sfd}(x_2 - x_1, n) < n$  kan vi ikke bruge formlen, men vi har fundet en faktor i  $n$ , så vi er færdige.
- c:** Hvis  $\text{sfd}(x_2 - x_1, n) = n$  kan vi heller ikke bruge formlen, så vi må gå tilbage til **2** og vælge en ny kurve, eller gå til **4** og vælge et mindre  $k$ .
- På tilsvarende måde fås de samme 3 tilfælde når vi bruger fordoblingsformlen.

**Lemma 3.4.** *Resten ved division med  $n$  af  $m$ ,  $[m]_n$  er en enhed i  $\mathbb{Z}/n\mathbb{Z}$  hvis og kun hvis  $\text{sfd}(m, n) = 1$ .*

*Bevis.* Antag at  $\text{sfd}(m, n) = 1$ , da findes iflg. Euklid  $p, q \in \mathbb{N}$  således, at  $mp + nq = 1$ , men reduceres dette modulo  $n$  får vi

$$[mp + nq]_n = [mp]_n + [nq]_n = [m]_n [p]_n = 1$$

Så  $[m]_n$  er en enhed i  $\mathbb{Z}/n\mathbb{Z}$ .

Antag nu, at  $[m]_n$  er en enhed i  $\mathbb{Z}/n\mathbb{Z}$ . Så findes der et  $k \in \mathbb{Z}$ , således, at  $[m]_n [k]_n = 1$ . Da  $[m]_n [k]_n - [1]_n = [mk - 1]_n = 0$  må der eksistere et  $l \in \mathbb{Z}$  således, at  $mk + nl = 1$ , men da er det eneste tal  $d$ , som både går op i  $m$  og  $n$ ,  $d = 1$ , så  $\text{sfd}(m, n) = 1$ , og lemmaet er vist.  $\square$

**3.3. Hvorfor er Lenstras algoritme smart?** Som tidligere nævnt bygger Lenstras algoritme på Pollards  $(p-1)$ -metode. Fordelen ved Lenstra er, at når algoritmen af den ene eller anden grund ikke giver noget resultat, kan vi bare vælge en helt ny elliptisk kurve og dermed en ny gruppe, hvor vi i Pollards kun har gruppen  $(\mathbb{Z}/n\mathbb{Z})^*$ . Altså, vi har flere forsøg med Lenstra til at finde en gruppe hvorom det gælder, at  $\#C_p(\mathbb{F}_p) | k$ , hvorimod vi med Pollard kun kan finde en primfaktor  $p$  i rimelig tid, hvis den opfylder at  $p - 1$  er et produkt af små primtal opløftet til små potenser. Se [1] s. 132.

Til slut vil vi nu vise et eksempel på, at Lenstras faktoreringsalgoritme rent faktisk giver en ikke-triviel faktor. Eksemplet er stillet som en opgave i [1] s. 144.

**Eksempel 3.5** (Lenstras algoritme). Lad  $n = 199843247$  være tallet vi ønsker at finde en faktor i og lad den elliptiske kurve  $C$  være givet ved

$$C : y^2 = x^3 + 59x - 59$$

Vælg  $P = (1, 1)$  og  $k = 16296$ , vi vil nu udregne  $kP \pmod{n}$  og se om det giver en ikke-triviel faktor. Til udregningerne er MAPLE benyttet.

- Da  $2^{199843247-1} \equiv 101742834 \pmod{199843247}$  er  $199843247$  ikke et primtal iflg. Fermats lille sætning, se kor. 1.9.3 s. 20 i [5]
- $\text{sfd}(6, 199843247) = 1$
- $\Delta = 4 \cdot 59^3 + 27 \cdot (-59)^2 = 915503$  og  $\text{sfd}(915503, 199843247) = 1$
- Vi kan skrive  $k = 16296 = 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3$

- Vi kan nu udregne  $2^i P \pmod{199843247}$  for  $i = 0, 1, \dots, 13$  ved hjælp af duplikationsformlen ved samme fremgangsmåde som i formel 3.3.

$i$	$2^i P \pmod{199843247}$
0	(1,1)
1	(959,199813548)
2	(140976106,178964503)
3	(142634722,33539717)
4	(149383726,113827137)
5	(5784508,152911406)
6	(139894866,196412831)
7	(169802754,196416866)
8	(11812898,62341168)
9	(13592075,60713669)
10	(41756751,77665319)
11	(162046219,1023294)
12	(171948746,183303558)
13	(116509380,17886653)

Vi addere nu disse punkter modulo  $n$  vha. de normale additionsformler.

$$\begin{aligned}
 (2^3 + 2^5)P &= (32573211, 64333866) \\
 (2^3 + 2^5 + 2^7)P &= (122586107, 134071689) \\
 (2^3 + 2^5 + 2^7 + 2^8)P &= (84524000, 69800545) \\
 ([\text{Forrige sum}] + 2^9)P &= (118912774, 18013736) \\
 ([\text{Forrige sum}] + 2^{10})P &= (190955731, 104499251) \\
 ([\text{Forrige sum}] + 2^{11})P &= (132762455, 427350) \\
 ([\text{Forrige sum}] + 2^{12})P &= (3834541, 80821724)
 \end{aligned} \tag{3.4}$$

Vi er nu klar til at beregne  $kP = 2^{13}P + (2^3 + 2^5 + \dots + 2^{12})P \pmod{n}$ . Altså  
 $(116509380, 17886653) + (3834541, 80821724) \pmod{n}$

Om vi kan udregne dette afhænger som tidligere nævnt af, om vi kan finde den inverse til differensen af  $x$ -koordinaterne. Men ved udregning får vi:

$$\text{sfd}(116509380 - 3834541, 199843247) = 10289$$

Vi ser altså nu, at algoritmen bryder sammen, men at dette netop giver os den ønskede faktor i vores tal, og

$$199843247 = 10289 \cdot 19423.$$

## BILAG A

A.1. **Bezout.** Vi beviser nu, at en ret linie snitter en elliptisk kurve præcis 3 gange, hvilket er et specialtilfælde af Bezout's sætning.

**Sætning A.1** (Specialtilfælde af Bezout's sætning). *Lad  $k$  være et algebraisk lukket legeme,  $L$  en linie,  $C$  en elliptisk kurve i  $\mathbb{P}^2$  på Weierstrass normalform, med koordinater i  $k$ , så snitter linien den elliptiske kurve 3 gange (talt med multiplicitet).*

*Bevis.* Linien og den elliptiske kurve er givet ved følgende mængder.

$$L = \{x, y \in k \mid \alpha y = \beta x + \gamma\}$$

$$C = \{x, y \in k \mid y^2 = x^3 + ax^2 + bx + c\}$$

Vi kan nu parametrisere linien  $L$ ,  $\begin{pmatrix} x \\ y \end{pmatrix} = \phi(t) = \begin{pmatrix} \alpha t - \frac{\gamma}{\beta} \\ \beta t \end{pmatrix}$  og ser på 2 tilfælde.

$\alpha = 0$ :

Nu får vi ved indsættelse af parameterfremstillingen:

$$\beta^2 t^2 = \left(-\frac{\gamma}{\beta}\right)^3 + a\left(-\frac{\gamma}{\beta}\right)^2 + b\left(-\frac{\gamma}{\beta}\right) + c = \text{konstant}.$$

Denne 2. grads ligning har 2 nulpunkter iflg. algebraens fundamental sætning. Vi undersøger nu, om linien  $L$  skærer i  $\mathcal{O} = (0, 1, 0)$ . Når  $\alpha = 0$  har linien  $L$  ligningen

$$0 = \beta x + \gamma$$

med afbildningen

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

Sæt nu

$$x = \frac{X}{Z} \text{ og } y = \frac{Y}{Z}$$

$\Downarrow$

$$0 = \beta \frac{X}{Z} + \gamma = \beta X + \gamma Z$$

med afbildningen

$$(x, z) \mapsto (X : 1 : Z).$$

Indsætter vi  $(0, 0) \mapsto (0 : 1 : 0)$  ses, at  $L$  skærer i punktet  $\mathcal{O}$ , så  $L$  har  $2 + 1 = 3$  skæringer med  $C$ .

$\alpha \neq 0$ :

Indsætter vi parameterfremstillingen i ligningen for  $C$  fås:

$$\beta^2 t^2 = \left(\alpha t - \frac{\gamma}{\beta}\right)^3 + a\left(\alpha t - \frac{\gamma}{\beta}\right)^2 + b\left(\alpha t - \frac{\gamma}{\beta}\right) + c$$

$\Downarrow$

$$0 = \alpha^3 t^3 + \dots = f(x)$$

Så  $f$  er et 3. grads polynomium, og da  $k$  er algebraisk lukket, siger algebraens fundamentalsætning, at  $f$  har 3 rødder. Vi undersøger nu, hvornår linien  $L$  skærer linien  $Z = 0$ . På samme måde som før får vi

$$-\alpha Y + \beta X + \gamma Z = 0$$

men den skærer  $Z = 0$  i  $\left(\frac{\alpha}{\beta} : 1 : 0\right) \neq (0 : 1 : 0)$ . Da vi allerede i afsnit 1.2 har set at linien  $Z = 0$  skærer  $\mathcal{O}$  tre gange, er sætningen hermed vist.  $\square$

```

Maple V for Windows - BEREGN.MS
File Edit Format Options Help
Associativitet for x-koordinaten:
> u
> :=(y1+q*(q^2-a-x2-x3)+y2-q*x2)/(a-q^2+x1+
> x2+x3):
> n
> :=(y3+m*(m^2-a-x2-x1)+y2-m*x2)/(a-m^2+x1+
> x2+x3):
> q :=(y3-y2)/(x3-x2):
> m :=(y2-y1)/(x2-x1):
> simplify(u^2-q^2+2*x3-2*x1-n^2+m^2,{(y1)^
> 2=(x1)^3+a*(x1)^2+b*x1+c,(y2)^2=(x2)^3+a*
> (x2)^2+b*x2+c,(y3)^2=(x3)^3+a*(x3)^2+b*x3
> +c});
0
Associativitet for y-koordinaten:
> x :=n^2-m^2-x3+x1+x2:
> simplify((n-u)*x-y1-n*x3+y3+u*x1,{(y1)^2=
> (x1)^3+a*(x1)^2+b*x1+c,(y2)^2=(x2)^3+a*(x
> 2)^2+b*x2+c,(y3)^2=(x3)^3+a*(x3)^2+b*x3+c
> });
0
>

```

FIGUR 2. Skærbillede af MAPLE V

*Bemærkning A.2.* Heraf ses altså, at en lodret linie skærer kurven 2 gange i det affine plan og 1 gang i punktet i uendelig.

A.2. **MAPLE.** Vi har sat MAPLE til at regne på de udledte udtryk, og taget et skærbillede af det, se figur 2.

A.3. **Legendre.**

**Sætning A.3.** Lad  $p > 2$  være et primtal, og  $\text{sfd}(a, p) = 1$ , og lad  $\left(\frac{a}{p}\right)_l$  betegne Legendre symbolet, da gælder

$$\left(\frac{a}{p}\right)_l = a^{\frac{p-1}{2}}$$

*Bevis.* Hvis  $\left(\frac{a}{p}\right)_l = 0$  betyder det, at  $a = 0$  i  $\mathbb{F}_p$ , så  $a^{\frac{p-1}{2}} = 0$ .

Hvis  $\left(\frac{a}{p}\right)_l = 1$  så  $\exists x_0 : x_0^2 = a$ , men

$$x_0^{p-1} = 1$$

da  $x^{p-1} = 1$  for alle  $x \in (\mathbb{Z}/p\mathbb{Z})^*$ , den multiplikative gruppe, så er vi færdige da  $x_0^{p-1} = a^{\frac{p-1}{2}}$ .

Hvis  $\left(\frac{a}{p}\right)_l = -1$ , så har  $x_0^2 = a$  ingen løsning. Dvs,

$$\forall j, (1 \leq j \leq p-1) \exists! i \neq j : ij = a$$

Disse  $(i, j)$ -par er der  $\frac{p-1}{2}$  af, da der er  $p-1$  muligheder for valg af  $j$  og  $(ij) = (ji)$

Der gælder, at

$$1 \cdot \dots \cdot (p-1) = -1$$

da 1 og  $p-1$  er de eneste elementer i gruppen, der er deres egne inverse, så  $2 \cdot 3 \cdot \dots \cdot (p-2) = 1$  men  $p-1 = 1p-1 = -1$ . Sammensætter vi nu  $1 \cdot \dots \cdot (p-1)$  så vi får alle  $ij$ -parrene sat sammen, har vi altså vist følgende

$$a^{\frac{p-1}{2}} = (i_1 j_1)(i_2 j_2) \cdot \dots \cdot (i_{p-1} j_{p-1}) = 1 \cdot \dots \cdot (p-1) = (p-1)! = -1$$

og det ønskede er vist.  $\square$

#### A.4. Diskret valuation funktionen.

**Definition A.4.** Lad  $f \in \mathbb{F}_p[X]$  være et irreducibelt polynomium. Den diskrete valuationsfunktion  $\nu_f : \mathbb{F}_p[X] \rightarrow \mathbb{N}$  er en funktion, der for en given funktion  $g \in \mathbb{F}_p[X]$  fortæller, hvor mange gange  $f$  går op i  $g$ , altså hvis  $\nu_f(g) = n$  har vi at  $g = f^n h$ , hvor  $\text{sfd}(f, h) = 1$ .

*Bemærkning A.5.* En enkelt regneregul for  $\nu_f$  er som følger: Lad  $f|g$   $a$  gange og lad  $f|h$   $b$  gange, da vil  $f|gh$   $a+b$  gange, så  $\nu_f(gh) = \nu_f(g) + \nu_f(h)$

## LITTERATUR

- [1] Joseph H. Silverman & John Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.
- [2] A. W. Knap, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.
- [3] Jasbir S. Chahal, *Manin's Proof of the Hasse Inequality Revisited*, Nieuw Arch. Wisk. (4), vol. 13, 1995.
- [4] Ivan Niven & Herbert S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons inc., New York-London-Sydney 1972.
- [5] Niels Lauritzen, *Algebra I & II*, Århus universitet, 1999.
- [6] Yu. I. Manin, *On Cubic Congruences to a Prime Modulus*, Amer. Math. Soc. Transl. (2) vol 13. s.1-7, 1960.