

# ELLIPTISKE KURVER

PETER JOHANNES STEFFENSEN

## INDHOLD

1. Gruppestrukturen på elliptiske kurver	2
1.1. Introduktion	2
1.2. Bestemmelse af $\mathcal{O}$	2
1.3. Ikke-singularitet	3
1.4. Korde-tangent komposition	4
1.5. Additionsformler	5
1.6. Redegørelse for gruppestrukturen	7
2. Elliptiske kurver over endelige legemer	10
2.1. Motivation	10
2.2. Reduktion modulo $p$	11
2.3. Variabelskift på elliptisk kurve	11
2.4. Kvadratiske rester og Legendre symbol	12
2.5. Rationale funktioner over $\mathbb{F}_p$	13
2.6. Bevis for Hasse's sætning	13
2.7. Eksempler	22
3. Anvendelser af elliptiske kurver	23
3.1. Indledning	23
3.2. Faktoreringsalgoritmer	23
3.3. Ideén i Lenstra's Algoritme	25
3.4. Lenstra's faktoreringsalgoritme	28
4. Kryptosystemer	33
4.1. Public key kryptosystemer	33
4.2. RSA kryptosystemet	33
4.3. Sikkerhed ved RSA	35
4.4. Alternativt kryptosystem	35
4.5. Afslutningsvis	37
5. Appendiks	38
5.1. Projektiv geometri	38
5.2. Bezout's Sætning	38
5.3. Sætning om Legendre symbol	40
Litteratur	41

---

Version: 29. Juni.

1991 *Mathematics Subject Classification*. 14C10, 93D20.

*Key words and phrases*. TeX, Mathematics.

# 1. GRUPPESTRUKTUREN PÅ ELLIPTISKE KURVER

1.1. **Introduktion.** I dette kapitel skal vi se, at de  $k$ -rationale punkter på en elliptisk kurve over et vilkårligt legeme  $k$  udgør en gruppe. Vi skal herunder definere en elliptisk kurve samt udlede additionsformler for sammensætningen af to punkter på en elliptisk kurve. Behandlingen heraf knytter sig til [1] s.9-32.

Vi vil studere mængden af løsninger til Weierstrass-ligningen

$$y^2 = t(x^3 + ax^2 + bx + c) \quad (1.1)$$

hvor  $t, a, b, c \in k$  og  $t \neq 0$ -elementet i  $k$ . Løsningsmængden til 1.1 beskriver en kurve  $E$ . Vi vil se, at løsningerne til 1.1 består af løsninger i det sædvanlige affine  $xy$ -plan samt, ved at betragte kurven  $E$  i det projektive plan  $\mathbb{P}^2$ , et ekstra "punkt"  $\mathcal{O}$  (se Appendiks afsnit 1 om det projektive plan). De  $k$ -rationale punkter på  $E$  - dvs. de talpar i  $k \times k$ , der løser 1.1  $\cup \mathcal{O}$  - har den vidunderlige egenskab, at de med  $\mathcal{O}$  som neutralelement udgør en gruppe. Inden vi går videre, kræver det, at vi har kendskab til det algebraiske objekt - en gruppe.

**Definition 1.1.** En komposition på en mængde  $G$  er en afbildning  $\pi : G \times G \rightarrow G$ . Man skriver ofte  $\pi(g, h) = gh$  for  $g, h \in G$ .  $(G, \pi)$  kaldes en gruppe, hvis

- 1)  $\exists e \in G$  således at  $es = se = s \forall s \in G$
- 2)  $\forall s \in G \exists s^{-1} \in G$  så  $ss^{-1} = s^{-1}s = e$
- 3) Kompositionen  $\pi$  er associativ - dvs.  $s_1(s_2s_3) = (s_1s_2)s_3$

Vores mål er at konstruere en komposition  $\pi : E(k) \times E(k) \rightarrow E(k)$ , som på  $E(k)$  opfylder betingelserne i ovenstående definition, hvor  $E(k)$  beskriver mængden af de  $k$ -rationale punkter på  $E$ .

Først bestemmelse af punktet  $\mathcal{O}$  samt endelig definition af en elliptisk kurve. Dernæst beskrivelse af vores komposition, der skal gøre  $E(k)$  til en gruppe. Sidst verificeres gruppestrukturen. Vi vil i det følgende antage, at  $\text{char}(k) \neq 2$ .

1.2. **Bestemmelse af  $\mathcal{O}$ .** Vi skal et øjeblik arbejde i det projektive plan  $\mathbb{P}^2$ . I  $\mathbb{P}^2$  beskrives en projektiv kurve  $E$  som dens affine del samt dens punkter i uendelig. Hvis vi homogenerer 1.1 - dvs. finder den projektive kurve til 1.1 - får vi

$$E : Y^2Z = t(X^3 + aX^2Z + bXZ^2 + cZ^3) \quad (1.2)$$

Hvornår skærer  $E$  linien i uendelig? Linien i uendelig beskrives ved  $Z = 0$ , og skæringspunktet findes ved substitution af  $Z = 0$  i 1.2. Man finder

$$tX^3 = 0 \implies X^3 = 0 \implies X = 0$$

Derfor skærer kurven  $E$  linien  $Z = 0$  i "punktet"  $\mathcal{O} = (0 : 1 : 0)$  og, som vist i Appendiks afsn.2, med snitmultiplicitet  $i(\mathcal{O}, E, Z = 0) = 3$ . Vi bemærker, at punktet  $\mathcal{O} = (0 : 1 : 0) \in E(k)$ , da  $0, 1, 0 \in k$ . ( se Appendiks afsn.1 om notationen  $(x : y : z)$  ). Vi har nu følgende

**Definition 1.2.** En elliptisk kurve  $E$  over et legeme  $k$  er en ikke-singulær kubisk kurve på Weierstrass normal form

$$y^2 = tf(x) = t(x^3 + ax^2 + bx + c) \quad (1.3)$$

hvor  $t, a, b, c \in k$  og  $t$  forskellig fra 0-elementet i  $k$ . Punkterne på den elliptiske kurve er alle talpar, der løser 1.3 samt, ved at betragte  $E$  i  $\mathbb{P}^2$ , et punkt  $\mathcal{O}$ .

- eller på projektiv form

**Definition 1.3.** En elliptisk kurve  $E$  i det projektive plan  $\mathbb{P}^2$  over et legeme  $k$  er en ikke-singulær kubisk kurve på Weierstrass normal form

$$Y^2 Z = t(X^3 + aX^2 Z + bX Z^2 + cZ^3) \quad (1.4)$$

hvor  $t, a, b, c \in k$  og  $t$  forskellig fra 0-elementet i  $k$ . Punkterne på  $E$  er mængden af  $(x : y : z) \in \mathbb{P}^2$ , der løser 1.4.

**1.3. Ikke-singularitet.** Grunden til, at vi kræver ikke-singularitet, er, at vi i ethvert punkt på  $E$  ønsker at kunne tegne en tangentlinie - nærmere forklaring under afsnit 1.4 og 1.5. Vi har følgende

**Definition 1.4.** En kurve  $E : F(x, y) = 0$  over et legeme  $k$  er ikke-singulær (glat), hvis  $E$  er ikke-singulær i ethvert punkt i  $E(\bar{k})$ , hvor  $\bar{k}$  er den algebraisk lukkede udvidelse af  $k$ . Derfor er  $E$  ikke-singulær, hvis der ikke findes punkter i  $E(\bar{k})$ , hvor de partielt afledede af  $F$  er 0 samtidig; dvs  $\forall (r, s) \in E(\bar{k})$ :

$$\frac{\partial F}{\partial x}(r, s) \neq 0 \quad \vee \quad \frac{\partial F}{\partial y}(r, s) \neq 0$$

**Bemærkning** Vi siger i analogi med ovenstående, at  $E$  er singulær, hvis der findes et singulært punkt  $(p, q) \in E(\bar{k})$  - dvs. et punkt, der opfylder

$$\frac{\partial F}{\partial x}(p, q) = 0 \quad \wedge \quad \frac{\partial F}{\partial y}(p, q) = 0$$

Men der er en endnu bedre metode til at afgøre, om en given kurve  $E$  er ikke-singulær. Vi har følgende

**Sætning 1.5.** En kurve  $E : F(x, y) = y^2 - tf(x) = y^2 - t(x^3 + ax^2 + bx + c) = 0$  over et legeme  $k$  med algebraisk lukket udvidelse  $\bar{k}$  er ikke-singulær hvis og kun hvis  $\text{sfd}(f, f') = 1$ .

*Bevis.* Ækvivalent med at vise:  $E$  singulær  $\iff \text{sfd}(f, f') > 1$

Antag  $E$  singulær  $\implies \exists (x_0, y_0) \in E(\bar{k})$  :

$$\frac{\partial F}{\partial y}(x_0, y_0) = 2y_0 = 0 \quad \wedge \quad \frac{\partial F}{\partial x}(x_0, y_0) = -tf'(x_0) = 0 \quad (1.5)$$

Da  $\text{char}(k) \neq 2$  og  $t \neq 0$  har vi iflg. 1.5, at  $2y_0 = 0 \implies y_0 = 0 \implies f(x_0) = 0$  samt  $f'(x_0) = 0$ . Altså har  $f, f'$  en fælles rod  $x_0 \implies X - x_0 \mid f$  og  $X - x_0 \mid f'$  - dvs.  $\text{sfd}(f, f') > 1$ .

Omvendt hvis  $\text{sfd}(f, f') > 1$  findes polynomium af  $\text{grad} \geq 1$ , der dividerer  $f, f'$ . Vi skriver nu

$$\begin{aligned} f(X) &= q_1(X)h(X) \\ f'(X) &= q_2(X)h(X) \end{aligned}$$

hvor  $\text{grad}(h) \geq 1$ . Betragtes  $h$  som polynomium i  $\bar{k}[X]$ , faktoriserer vi i lineære faktorer

$$h(X) = \alpha \prod_i (X - \beta_i)$$

Heraf ser vi, at også et polynomium af grad 1 dividerer  $f, f'$ . Hvis

$$\begin{aligned} f(X) &= (X - \beta)p_1(X) \\ f'(X) &= (X - \beta)p_2(X) \end{aligned}$$

har vi så, at  $(\beta, 0) \in E(\bar{k})$  er et singulært punkt. □

**Bemærkning** For at afgøre om en given kurve  $E : F(x, y) = y^2 - tf(x) = 0$ , hvor  $f(x) = x^3 + ax^2 + bx + c$  med  $t, a, b, c \in k$ , er en elliptisk kurve over et legeme  $k$ , skal vi blot udregne  $\text{sfd}(f, f')$ . Dette kan gøres v.h.a Euklids algoritme beskrevet i [3] s.12-14. Vi observerer også, at  $\text{sfd}(f, f') > 1 \iff f, f'$  som polynomier i  $\bar{k}[X]$  har en fælles rod. At  $f, f'$  har en fælles rod er ækvivalent med, at  $f$  har en multipel rod som vist i [3] s.104

**Bemærkning** Betragter vi  $f$  som polynomium i udvidelsen af  $k$ , faktoriserer vi  $f$  og får

$$f(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3) \in \bar{k}[X] \quad (1.6)$$

hvor  $\beta_1, \beta_2, \beta_3$  er rødderne i  $f$ . Man kan nu ved at sammenligne koefficienter på højre og venstre side efterwise

$$a = -(\beta_1 + \beta_2 + \beta_3) \quad (1.7)$$

$$b = (\beta_1\beta_2 + \beta_2\beta_3 + \beta_1\beta_3) \quad (1.8)$$

$$c = -(\beta_1\beta_2\beta_3) \quad (1.9)$$

Definer nu

$$D \equiv (\beta_1 - \beta_2)^2(\beta_1 - \beta_3)^2(\beta_2 - \beta_3)^2 = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Det sidste lighedstegn følger ved at bruge 1.6,1.7,1.8,1.9 - se [2] s. 58-59. Denne størrelse  $D$  afslører automatisk, om  $f$  har en multipel rod, og dermed om  $E$  er en elliptisk kurve. Dermed har vi følgende resultat: En kubisk kurve  $E$  på Weierstrass normal form over et vilkårligt legeme  $k$  med karakteristik  $\neq 2$  er en elliptisk kurve hvis og kun hvis den tilhørende diskriminant  $D \neq 0$  som element i  $k$ .

Faktisk kan vi eksplicit vise, at  $\mathcal{O} \in E(k)$  er et ikke-singulært punkt. Vi homogeniserer den affine ligning 1.3 og beskriver den projektive kurve i  $Y = 1$ -planet

$$E : F(X, Z) = t(X^3 + aX^2Z + bXZ^2 + cZ^3) - Z = 0$$

Heraf ser vi

$$\begin{aligned} \frac{\partial F}{\partial X} \Big|_{\mathcal{O}=(0,0)} &= 0 \\ \frac{\partial F}{\partial Z} \Big|_{\mathcal{O}=(0,0)} &= -1 \end{aligned}$$

hvilket viser, at punktet  $\mathcal{O}$  er ikke-singulært. Så punkterne på vores elliptiske kurve  $E$  består altså af de sædvanlige affine punkter samt et punkt  $\mathcal{O}$ , der er defineret som skæringen mellem kurven  $E$  betragtet i  $\mathbb{P}^2$  og linien i uendelig beskrevet ved  $Z = 0$ . Bemærk, at alle vertikale linier ( $x = \text{konst.}$ ) skærer  $E$  i punktet  $\mathcal{O}$ .

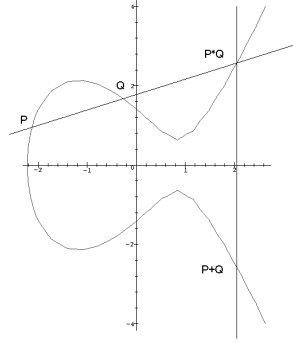
**1.4. Korde-tangent komposition.** For at vise gruppestrukturen på en elliptisk kurve, behøver vi en komposition  $\pi : E(k) \times E(k) \longrightarrow E(k)$ , så  $(E(k), \pi)$  er en gruppe. Lad  $E$  være en elliptisk kurve over et legeme  $k$  og antag, at vi kender et punkt  $\mathcal{O} \in E(k)$ . Dette punkt bliver vores neutralelement, når vi skal beskrive gruppestrukturen. Proceduren er følgende:

Givet to punkter  $P, Q \in E(k)$ . Linien gennem  $P, Q$  tegnes - denne skærer  $E$  i et tredje punkt  $P * Q \in E(k)$ . Linien gennem  $\mathcal{O}$  og  $P * Q$  skærer nu  $E$  i punktet  $P + Q = \mathcal{O} * (P * Q)$ . For  $P = Q$  tegnes tangentlinjen i  $P$  - dvs.  $2P = \mathcal{O} * (P * P)$ .

Derfor defineres for  $P, Q \in E(k)$  korde-tangent kompositionen ved relationen

$$P + Q = \mathcal{O} * (P * Q)$$

og det givne punkt  $\mathcal{O}$  bliver neutralelement.



FIGUR 1. Elliptisk kurve med komposition

Men der er tydeligvis nogle mangler. I min procedure benytter jeg, at enhver linie  $L$  skærer kurven  $E$  i præcis tre punkter. Dette er et specialtilfælde af Bezout's sætning og gælder kun, hvis vi tæller med snitmultiplicitet, accepterer løsninger i  $\bar{k}$  samt betragter  $E, L$  i det projektive plan  $\mathbb{P}^2$  ( se Appendiks afsn.2 om Bezout's sætning ). Det er heller ikke oplagt, at linien gennem  $P, Q \in E(k)$  vil skære  $E$  i et tredje punkt, der også tilhører  $E(k)$ . Vi vil dog se, at dette er tilfældet, når vi udleder eksplicitte formler for addition af punkter - altså er vores komposition veldefineret.

Valget af neutralelementet  $\mathcal{O} = (0 : 1 : 0)$  har nogle umiddelbare konsekvenser.

$$\mathcal{O} = \mathcal{O} * \mathcal{O} \quad (1.10)$$

da  $\mathcal{O}$  er flexpunkt ( $Z = 0$  skærer  $E$  tre gange i  $\mathcal{O}$ ). Givet et punkt  $P \in E(k)$  - da er den additivt inverse til  $P$  ved brug af 1.10 givet ved

$$-P = (\mathcal{O} * \mathcal{O}) * P = \mathcal{O} * P \quad (1.11)$$

For en elliptisk kurve givet ved 1.3, betyder det, at

$$P = (x_0, y_0) \implies -P = (x_0, -y_0)$$

idet linien gennem  $\mathcal{O}$  og  $P$  er  $x = x_0$  i affin form, og  $E$  er symmetrisk om  $x$ -aksen.

**1.5. Additionsformler.** Lad os udlede eksplicitte formler for addition af punkter på en elliptisk kurve beskrevet ved 1.3. Antag  $P_1, P_2 \in E(k) \setminus \mathcal{O}$  samt  $P_1 \neq -P_2$ . Vi skal så udregne  $P_1 * P_2$  og  $P_3 = P_1 + P_2$ . Notationen er

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

Linien gennem  $P_1 * P_2 = (x_3, y_3)$  og  $\mathcal{O}$  er i projektive koordinater givet ved  $X = x_3 Z$ , hvilket i affine koordinater betyder, at der er to skæringer med  $E$  - nemlig  $y_3, -y_3$ . Derfor har vi  $P_3 = (x_3, -y_3)$ . Det er nødvendigt at behandle flere tilfælde.

**1.Kordetilfældet** ( dvs.  $P_1 \neq P_2$  ).

Linien gennem  $P_1$  og  $P_2$  er på formen  $L : y = mx + d$ , hvor

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

og  $d$  bestemmes af

$$y_1 = mx_1 + d \implies d = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

Linien  $L$  skærer  $E$  i  $P_1$  og  $P_2$ . Idet Bezout's sætning giver, at antallet af skæringspunkter mellem  $E, L$  netop er lig 3 - hvis vi tæller korrekt - finder vi det tredje skæringspunkt ved substitution af  $y = mx + d$  i 1.3. Vi får

$$\begin{aligned} y^2 &= (mx + d)^2 = t(x^3 + ax^2 + bx + c) \implies \\ m^2x^2 + d^2 + 2mdx &= t(x^3 + ax^2 + bx + c) \implies \\ tx^3 + (ta - m^2)x^2 + (tb - 2md)x + tc - d^2 &= 0 \end{aligned} \quad (1.12)$$

Vi ved, at  $x_1, x_2$  løser 1.12, så  $(P_1 * P_2)_x = x_3$  bestemmes af

$$tx^3 + (ta - m^2)x^2 + (tb - 2md)x + tc - d^2 = t(x - x_1)(x - x_2)(x - x_3)$$

Ved at sammenligne koefficienter fås

$$ta - m^2 = -t(x_3 + x_2 + x_1) \implies x_3 = \frac{m^2}{t} - a - x_2 - x_1 \quad (1.13)$$

og dermed

$$(P_1 * P_2)_y = y_3 = mx_3 + d \quad (1.14)$$

med  $m, d$  som ovenfor.

**Bemærkning** Så givet  $P_1, P_2 \in E(k)$  - da ser vi, at  $P_3 = P_1 + P_2 \in E(k)$  ifølge ovenstående formler for  $(P_3)_x = x_3$  og  $(P_3)_y = -y_3$ .

**2. Tangent – tilfældet** ( dvs.  $P_1 = P_2$  ).

Linien gennem  $P_1$  og  $P_1$  er netop tangentlinien til  $E$  i punktet  $(x_1, y_1)$ . Da

$$y = \pm \sqrt{t(x^3 + ax^2 + bx + c)}$$

har vi for  $y > 0$

$$\frac{dy}{dx} = \frac{1}{2\sqrt{t(x^3 + ax^2 + bx + c)}} t f'(x) = \frac{t f'(x)}{2y}$$

og for  $y < 0$  ligeledes

$$\frac{dy}{dx} = \frac{t f'(x)}{2y}$$

Så når  $y \neq 0$  er tangentlinien gennem  $P_1$  på formen  $T : y = lx + r$ , hvor

$$\begin{aligned} l &= \frac{t f'(x_1)}{2y_1} \\ r &= y_1 - lx_1 \end{aligned}$$

Vi kan nu bruge formler for  $x_3, y_3$  gennemgået under det forrige tilfælde til at finde det tredje skæringspunkt med  $E$  - erstat blot  $m, d$  med  $l, r$  henholdsvis i 1.13, 1.14 og få

$$\begin{aligned} x_3 &= \frac{l^2}{t} - a - 2x_1 = \frac{1}{t} \left( \frac{t f'(x_1)}{2y_1} \right)^2 - a - 2x_1 \\ &= \frac{1}{t} \left( \frac{t(3x_1^2 + 2ax_1 + b)}{2y_1} \right)^2 - a - 2x_1 \\ &= \frac{t^2(3x_1^2 + 2ax_1 + b)^2}{4t^2(x_1^3 + ax_1^2 + bx_1 + c)} - a - 2x_1 \\ &= \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c} \end{aligned} \quad (1.15)$$

samt

$$y_3 = lx_3 + r \quad (1.16)$$

med  $l, r$  givet ovenfor.

**Bemærkning** Det, vi har fundet, er en formel for, hvordan vi fordobler et punkt - altså givet  $P \in E(k)$ , så beskriver  $x_3, -y_3$  punktet  $P + P = 2P$ . Bemærk igen, at

$$P \in E(k) \implies P + P \in E(k)$$

**3. Tilfældet  $\mathbf{P}_1 = -\mathbf{P}_2$**  (dvs.  $P_1 = (x_2, -y_2)$  og  $-P_1 = (x_2, y_2)$ ).

Da følger, at

$$P_1 + P_2 = \mathcal{O} * (P_1 * P_2) = \mathcal{O} * (P_1 * (-P_1)) = \mathcal{O} * \mathcal{O} = \mathcal{O}$$

per konstruktion af  $\mathcal{O}$ .

**4. Tangent – tilfældet  $y = 0$**

Vi kan betragte tangentlinien i  $P_1 = (x_1, 0)$  som linien gennem  $P_1$  og  $P_2$ , hvor  $P_1 = -P_2$ . Af tilfælde 3 følger

$$P_1 + P_2 = P_1 + (-P_1) = \mathcal{O}$$

Så ovenstående 1.13, 1.14, 1.15, 1.16 giver os formler for addition af  $k$ -rationale punkter på en elliptiske kurve  $E$ .

**1.6. Redegørelse for gruppestrukturen.** Vi har nu fundet en veldefineret komposition  $+: E(k) \times E(k) \rightarrow E(k)$  og vil nu verificere, at de  $k$ -rationale punkter på  $E$  danner en gruppe m.h.t korde-tangent kompositionen.  $E$  er her en elliptisk kurve som beskrevet i DEF 1.2, 1.3.

1) Der findes et neutralt element  $\mathcal{O} \in E(k)$ . Givet  $P = (r, s) \in E(k)$  - da er linien  $L$  gennem  $P, \mathcal{O}$  i affine koordinater på formen  $x = r$ . Sætter vi  $L \cap E(k) = \{\mathcal{O}, P, Q\}$ , finder vi punktet  $Q$  ved at benytte

$$y^2 = t(r^3 + ar^2 + br + c)$$

som har løsningerne  $\pm s$ . Altså  $Q = (r, -s) = \mathcal{O} * P$ . Samme argument giver nu

$$P + \mathcal{O} = \mathcal{O} * (\mathcal{O} * P) = P$$

NB: I tilfældet  $P = \mathcal{O}$  har vi  $\mathcal{O} + \mathcal{O} = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O}$  per konstruktion af  $\mathcal{O}$ .

2) Den additivt inverse til  $P = (r, s) \in E(k)$  er  $Q = (r, -s)$ . Vi bemærker her, at  $Q \in E(k)$ . At  $Q$  er additivt invers ses ved at addere  $P$  og  $Q$ . Linien gennem  $P, Q$  har i det projektive plan formen  $X = rZ$ . Denne skærer  $Z = 0$  i  $\mathcal{O} \in E(k)$ . Vi har altså

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * \mathcal{O} = \mathcal{O}$$

hvilket viser  $Q = -P$ . NB: I tilfældet  $P = \mathcal{O}$  er den additivt inverse til  $P$  lig  $\mathcal{O}$ , idet

$$\mathcal{O} + \mathcal{O} = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O}$$

3) Associativitet. Givet tre vilkårlige punkter  $P_1, P_2, P_3 \in E(k)$ , skal vi vise

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

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 afsnit 1.5, finder vi

$$\begin{aligned}
(P_1 + P_2)_x &= \frac{m^2}{t} - a - x_1 - x_2 \\
(P_1 + P_2)_y &= -m\left(\frac{m^2}{t} - a - x_1 - x_2\right) - y_2 + mx_2 \\
\{(P_1 + P_2) + P_3\}_x &= \frac{n^2}{t} - a - x_3 - (P_1 + P_2)_x = \frac{n^2}{t} - a - x_3 - \left(\frac{m^2}{t} - a - x_1 - x_2\right) \\
&= \frac{n^2 - m^2}{t} + x_1 + x_2 - x_3
\end{aligned} \tag{1.17}$$

hvor  $m, n$  er hældningstallet for linien gennem  $P_1, P_2$  og  $P_1 + P_2, P_3$  henholdsvis.

Omvendt finder vi nu ved symmetri

$$\begin{aligned}
(P_2 + P_3)_x &= \frac{l^2}{t} - a - x_2 - x_3 \\
(P_2 + P_3)_y &= -l\left(\frac{l^2}{t} - a - x_2 - x_3\right) - y_2 + lx_2 \\
\{P_1 + (P_2 + P_3)\}_x &= \frac{u^2 - l^2}{t} + x_2 + x_3 - x_1
\end{aligned} \tag{1.18}$$

hvor  $l, u$  er hældningstallet for linien gennem  $P_2, P_3$  og  $P_1, P_2 + P_3$  henholdsvis.

Vi skal nu undersøge, om 1.17 stemmer overens med 1.18. Da  $m, n, u, l$  alle afhænger af valget af punkter, er der flere tilfælde at tjekke. Vi vil se på det mest generelle tilfælde, hvor

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

$$\begin{aligned}
m &= \frac{y_2 - y_1}{x_2 - x_1} & l &= \frac{y_3 - y_2}{x_3 - x_2} \\
n &= \frac{y_3 - (P_1 + P_2)_y}{x_3 - (P_1 + P_2)_x} = \frac{y_3 - (-m(\frac{m^2}{t} - a - x_1 - x_2) - y_2 + mx_2)}{x_3 - (\frac{m^2}{t} - a - x_1 - x_2)} \\
&= \frac{y_3 + m(\frac{m^2}{t} - a - x_1 - x_2) + y_2 - mx_2}{a - \frac{m^2}{t} + x_1 + x_2 + x_3}
\end{aligned}$$

og tilsvarende

$$u = \frac{y_1 + l(\frac{l^2}{t} - a - x_2 - x_3) + y_2 - lx_2}{a - \frac{l^2}{t} + x_1 + x_2 + x_3}$$

Vi skal tjekke, at 1.17, 1.18 stemmer overens - dvs.

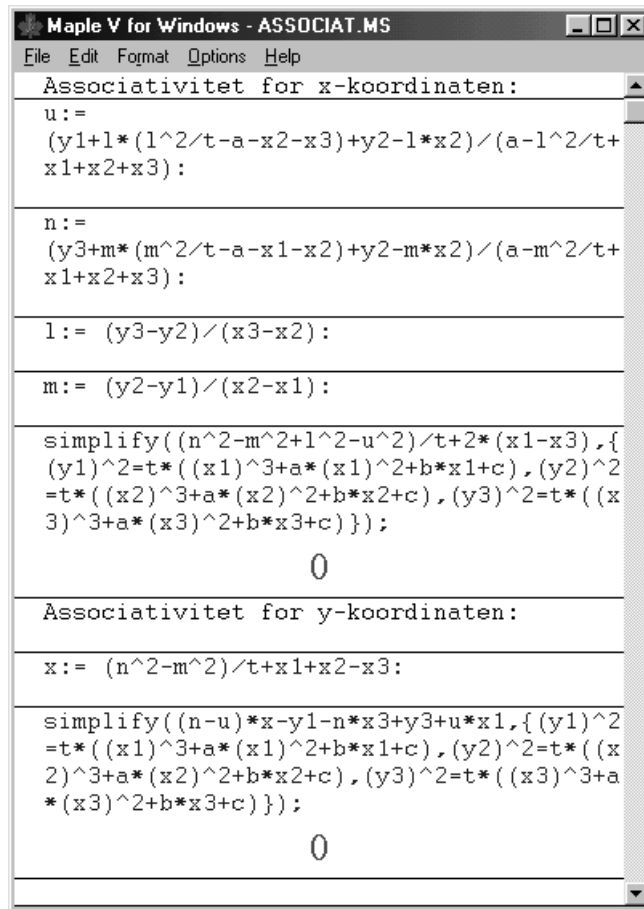
$$\begin{aligned}
\frac{n^2 - m^2}{t} + x_1 + x_2 - x_3 &= \frac{u^2 - l^2}{t} + x_2 + x_3 - x_1 \iff \\
\frac{n^2 - m^2 + l^2 - u^2}{t} + 2(x_1 - x_3) &= 0
\end{aligned} \tag{1.19}$$

For  $y$ -koordinaten får vi

$$\{P_1 + (P_2 + P_3)\}_y = -(u\{P_1 + (P_2 + P_3)\}_x + y_1 - ux_1) \tag{1.20}$$

$$\{(P_1 + P_2) + P_3\}_y = -(n\{(P_1 + P_2) + P_3\}_x + y_3 - nx_3) \tag{1.21}$$

Vi lader nu MAPLE V regne på venstre side af 1.19 givet udtrykkene for  $m, n, u, l$ . Endvidere benytter vi, at  $P_1, P_2, P_3 \in E$  - dvs.  $y_i^2 = t(x_i^3 + ax_i^2 + bx_i + c)$  for  $i = 1, 2, 3$ .



FIGUR 2. Skærbillede af MAPLE V

Vi ser, at 1.17,1.18 stemmer overens. Dette benyttes til sammenligning af de to  $y$ -koordinater. MAPLE V regner nu på

$$(n - u)\{P_1 + (P_2 + P_3)\}_x - y_1 - nx_3 + y_3 + ux_1$$

og får, at dette er lig 0. Det vil sige, at venstre side af 1.20,1.21 stemmer overens. Man kan på tilsvarende måde vise associativiteten i de andre tilfælde - det vil dog ikke blive gjort.

**Bemærkning** Gruppen af de  $k$ -rationale punkter med korde-tangent kompositionen  $+$  er en kommutativ gruppe - dvs.  $P + Q = Q + P \forall P, Q \in E(k)$  - idet linien gennem  $P, Q$  er den samme som linien gennem  $Q, P$  og derfor  $P * Q = Q * P$ . Vi observerer ligeledes, at givet et legeme  $\tilde{k} \supseteq k$ , da udgør de  $\tilde{k}$ -rationale punkter på en elliptisk kurve over et legeme  $k$  også en gruppe m.h.t korde-tangent kompositionen.

Vi har derfor gjort rede for følgende

**Sætning 1.6.** *Lad  $k$  være et vilkårligt legeme med  $\text{char}(k) \neq 2$  og  $E$  en elliptisk kurve på Weierstrass normal form*

$$y^2 = t(x^3 + ax^2 + bx + c)$$

hvor  $t, a, b, c \in k$  og  $t \neq 0$ -elementet i  $k$ . Da er  $E(\tilde{k}) = \{(x, y) \in \tilde{k} \times \tilde{k} \mid (x, y) \in E\} \cup \mathcal{O}$ , hvor  $\tilde{k} \supseteq k$  er et legeme, en kommutativ gruppe m.h.t korde-tangent kompositionen.

## 2. ELLIPTISKE KURVER OVER ENDELIGE LEGEMER

**2.1. Motivation.** Hvor vi i kapitel 1 udarbejdede den grundlæggende teori for elliptiske kurver over et vilkårligt legeme  $k$ , skal vi i dette afsnit specificere  $k$  nærmere. Vi vil i det følgende lade  $k = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ , hvor  $\mathbb{F}_p$  består af restklasser modulo  $p$ . Bemærk, at det her er vigtigt, at  $p$  er et primtal, idet  $\mathbb{Z}/p\mathbb{Z}$  er et legeme hvis og kun hvis  $p$  er et primtal. Som i kapitel 1 lader vi  $\text{char}(k) = \text{char}(\mathbb{F}_p) = p \neq 2$ . Vi vil igen studere elliptiske kurver  $E_p$  på formen

$$y^2 = tf(x) = t(x^3 + ax^2 + bx + c) \quad (2.1)$$

hvor  $t, a, b, c \in \mathbb{F}_p$  og  $t \neq 0$ -elementet i  $\mathbb{F}_p$ . De  $\mathbb{F}_p$ -rationale punkter på  $E_p$  er  $\{(x, y) \in E_p \mid x \in \mathbb{F}_p, y \in \mathbb{F}_p\} \cup \mathcal{O}_p$ . Hovedsætningen i dette kapitel fortæller noget om antallet af  $\mathbb{F}_p$ -rationale punkter på en elliptisk kurve - skrevet  $|E_p(\mathbb{F}_p)|$ . Faktisk kan vi give et kvalificeret gæt. Strategien er succesivt at indsætte værdier  $x \in \mathbb{F}_p$  i 2.1 og så løse om muligt for  $y$ . Vi kan for et  $x \in \mathbb{F}_p$  løse for  $y$ , hvis vi kan uddrage kvadratroden af  $tf(x)$ . Det er i den forbindelse nyttigt at se på afbildningen

$$\varphi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$$

givet ved  $\varphi(g) = g^2$ . Her er  $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$  enhederne/invertible elementer i  $\mathbb{F}_p$ . I [3] s.94-95 vises, at  $\mathbb{F}_p^*$  er en kommutativ, cyklisk gruppe m.h.t multiplikation. Kapitel 3 i [3] bruger resultater fra gruppeteorien, som i det følgende antages kendt.

Afbildningen  $\varphi : \mathbb{F}_p^* \longrightarrow \mathbb{F}_p^*$  er en gruppehomomorfi, idet  $\varphi(xy) = \varphi(x)\varphi(y) \forall x, y \in \mathbb{F}_p^*$ . Den klassiske Isomorfi-sætning giver da en isomorfi

$$\tilde{\varphi} : \mathbb{F}_p^*/\text{Ker}(\varphi) \simeq \varphi(\mathbb{F}_p^*) \quad (2.2)$$

Billedet af  $\mathbb{F}_p^*$  under afbildningen  $\varphi$  er netop de elementer i  $\mathbb{F}_p^*$ , hvoraf man kan uddrage kvadratroden. Ifølge isomorfien i 2.2 ser vi så, at

$$|\mathbb{F}_p^*/\text{Ker}(\varphi)| = \frac{|\mathbb{F}_p^*|}{|\text{Ker}(\varphi)|} = |\varphi(\mathbb{F}_p^*)|$$

Lagrange's index sætning samt det faktum, at  $\text{Ker}(\varphi) \subseteq \mathbb{F}_p^*$  er en undergruppe, er benyttet til at vise den første lighed. Neutralelementet i  $\mathbb{F}_p^*$  er 1  $\implies$

$$\text{Ker}(\varphi) = \{g \in \mathbb{F}_p^* \mid \varphi(g) = 1\} = \{g \in \mathbb{F}_p^* \mid g^2 = 1\} = \{1, p-1\}$$

idet  $1^2 = 1$  og  $(p-1)^2 = p^2 - 2p + 1 = 1$  over  $\mathbb{F}_p$ . Da  $\mathbb{F}_p$  er et legeme, ved vi, at  $|\text{Ker}(\varphi)| \leq 2$  - der findes derfor ikke flere elementer i  $\text{Ker}(\varphi)$ . Dette giver så, at antallet af elementer i  $\mathbb{F}_p^*$ , hvoraf man kan uddrage kvadratroden, er givet ved

$$|\varphi(\mathbb{F}_p^*)| = \frac{p-1}{2}$$

Antager vi nu, at  $tf(\mathbb{F}_p) = \mathbb{F}_p$  gælder faktisk ifølge ovenstående, at

$$|E_p(\mathbb{F}_p)| = 2 \frac{p-1}{2} + 1 + 1 = p + 1$$

idet for  $tf(x) = 0$  tælles én løsning  $y = 0$ . De  $p-1$   $x$ -værdier, hvor  $tf(x) \neq 0$  kan man i præcis  $\frac{p-1}{2}$  tilfælde uddrage kvadratroden, hvilket giver to løsninger  $\pm y$  for hvert tilfælde. Til sidst skal vi tælle vores neutralelement  $\mathcal{O} \in E_p(\mathbb{F}_p)$  med. Lidt løst kan vi sige, at hvis  $tf(x) \neq 0$  er tilfældigt fordelt mellem kvadrater og ikke-kvadrater, når  $x$  gennemløber  $\mathbb{F}_p$  - da får vi følgende

$$|E_p(\mathbb{F}_p)| \approx |\{x \in \mathbb{F}_p \mid tf(x) = 0\}| + |\{x \in \mathbb{F}_p \mid tf(x) \neq 0\}| + 1 \approx p + 1$$

Første led angiver de  $m$  elementer i  $\mathbb{F}_p$  hvor  $tf(x) = 0$ . Andet led de  $p - m$  elementer hvor  $tf(x) \neq 0$ . I ca. halvdelen af disse tilfælde kan vi løse for  $y$ , og derfor er størrelsen af andet led omtrent lig  $p - m$ . Det sidste led følger af, at vi skal tælle i det projektive plan og dermed mangler neutralelementet  $\mathcal{O}$ . Så længe vores kurve  $E_p$  er ikke-singulær - dvs. rødderne i  $f$  er forskellige - er der intet, der peger i retning af, at værdierne af  $tf(x)$  er kvadrater frem for ikke-kvadrater eller omvendt. Derfor skal antallet af løsninger se ud på følgende måde

$$|E_p(\mathbb{F}_p)| = (p + 1) + (\text{korrektionsled})$$

hvor dette korrektionsled skal være lille sammenlignet med  $p$ . Bestemmelse af dette korrektionsled er præcis indholdet af Hasse's sætning, der vises senere. Vi skal se, at korrektionsleddet numerisk er begrænset af  $2\sqrt{p}$ .

Inden beviset for Hasse's sætning, er der nogle begreber at få styr på. Det første knytter sig til [1] s.121-123.

**2.2. Reduktion modulo  $p$ .** Lad  $E$  være en elliptisk kurve over  $\mathbb{Q}$  med heltalskoefficienter givet ved den sædvanlige Weierstrass-ligning

$$y^2 = tf(x) = t(x^3 + ax^2 + bx + c)$$

hvor  $t, a, b, c \in \mathbb{Z}$ . Se nu på afbildningen - den kanoniske ring homomorfi -

$$\gamma_p : \mathbb{Z} \longrightarrow \mathbb{F}_p$$

givet ved  $\gamma_p(r) = [r]_p$ , hvor  $[r]_p$  er restklassen modulo  $p$ , der indeholder  $r$ . Egenskaber ved afbildningen  $\gamma_p$  kan studeres i [1] s.121-123. Givet en elliptisk kurve  $E$  over  $\mathbb{Q}$  med heltalskoefficienter og  $p \nmid t$ , kan vi så reducere koefficienterne modulo  $p$  v.h.a afbildningen  $\gamma_p$ . Dette giver en ny kubisk kurve  $E_p : y^2 - [f]_p(x) = 0$  med koefficienter i  $\mathbb{F}_p$ . Vil denne kurve være ikke-singulær - dvs. forbliver kurven elliptisk? I kapitel 1 så vi, at ikke-singularitet kunne udtrykkes ved, at den tilhørende diskriminant for

$$[f]_p(x) = [t]_p(x^3 + [a]_p x^2 + [b]_p x + [c]_p)$$

hvor  $[t]_p, [a]_p, [b]_p, [c]_p \in \mathbb{F}_p$  er forskellig fra nulelementet i  $\mathbb{F}_p$ . Idet  $\gamma_p$  er en homomorfi ser vi, at diskriminanten  $D_p$  for  $[f]_p(x)$  er givet ved

$$D_p = [-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2]_p = [D]_p$$

hvor  $D$  er diskriminanten for vores oprindelige  $f(x)$  med koefficienter i  $\mathbb{Z}$ . Altså har vi

$$D_p \neq 0 \iff p \nmid D$$

hvor 0 betegner 0-elementet i  $\mathbb{F}_p$ .

**Bemærkning** Der er gode chancer for, at en elliptisk kurve  $E$  under reduktion modulo et tilfældigt primtal  $p$  forbliver en elliptisk kurve  $E_p$ , idet  $D$  kun har endelig mange primtalsdivisorer.

Fremover dropper vi subscriptet  $[ ]_p$  for elementer i  $\mathbb{F}_p$ .

**2.3. Variabelskift på elliptisk kurve.** I beviset for Hasse's sætning får vi brug for et variabelskift. Vores elliptiske kurve  $E_p$  er på Weierstrass normal form

$$y^2 = tf(x) = t(x^3 + ax^2 + bx + c)$$

hvor  $t, a, b, c \in \mathbb{F}_p$  og  $t \neq 0$ -elementet i  $\mathbb{F}_p$ . Variabelskiftet

$$x = tx' \quad y = t^2y'$$

og efterfølgende division med  $t^4$  ( $(t^4)^{-1}$  findes da  $t \in \mathbb{F}_p$  forskellig fra 0) giver en ligning af formen:

$$y'^2 = x'^3 + \frac{a}{t}x'^2 + \frac{b}{t^2}x' + \frac{c}{t^3}$$

Bemærk, at kurven forbliver ikke-singulær under dette variabelskift, idet  $D' = \frac{D}{t^6}$ . Her er  $D'$  diskriminanten for kurven efter variabelskiftet og  $D$  diskriminanten for den oprindelige elliptiske kurve. Da  $D \neq 0 \implies D' \neq 0$ . Valget af variabelskift giver, at antallet af  $\mathbb{F}_p$ -rationale punkter på  $E_p$  er lig antallet af  $\mathbb{F}_p$ -rationale punkter på kurven efter variabelskiftet. Antager vi, at  $\text{char}(\mathbb{F}_p) = p > 3$  sætter vi nu

$$x' = \tilde{x} - \frac{a}{3t} \quad y' = \tilde{y}$$

og får vi en ligning på formen

$$\begin{aligned} \tilde{y}^2 &= \left(\tilde{x} - \frac{a}{3t}\right)^3 + \frac{a}{t}\left(\tilde{x} - \frac{a}{3t}\right)^2 + \frac{b}{t^2}\left(\tilde{x} - \frac{a}{3t}\right) + \frac{c}{t^3} \\ &= \tilde{x}^3 + \left(\frac{3b - a^2}{3t^2}\right)\tilde{x} + \frac{2a^3 - 9ab + 27c}{27t^3} \end{aligned}$$

Også dette variabelskift bevarer antallet af  $\mathbb{F}_p$ -rationale punkter. Under antagelse af, at

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0 \quad (2.3)$$

ser vi, at kurven forbliver ikke-singulær, idet

$$\tilde{D} = \frac{D}{t^6} \quad (2.4)$$

Udledning af 2.4 følger blot ved at bruge diskriminantformlen 2.3 på kurven efter det sidste variabelskift. Altså givet elliptisk kurve over  $\mathbb{F}_p$

$$y^2 = tf(x) = t(x^3 + ax^2 + bx + c)$$

samt  $p > 3$ , kan vi ved passende variabelskift få en ny elliptisk kurve på Weierstrass normal form, hvor koefficienten til  $x^2$ -leddet er lig 0. Antallet af  $\mathbb{F}_p$ -rationale punkter på de to elliptiske kurver er ens. Dette trick vil blive benyttet i beviset for Hasse's sætning.

**2.4. Kvadratiske rester og Legendre symbol.** Et par definitioner inspireret af [4] s.63-64:

**Definition 2.1.** For alle  $a$  så  $\text{sfd}(a, m) = 1$ , kaldes  $a$  en kvadratisk rest modulo  $m$  hvis kongruensligningen

$$x^2 \equiv a \pmod{m} \quad (2.5)$$

har en løsning. Hvis 2.5 ikke har en løsning kaldes  $a$  en ikke-kvadratisk rest.

**Bemærkning** Heraf følger, at  $a$  er en kvadratisk/ikke-kvadratisk rest hvis og kun hvis  $a + nm$  for  $n \in \mathbb{Z}$  er en kvadratisk/ikke-kvadratisk rest. Derfor regnes kvadratiske/ikke-kvadratiske rester forskellige, hvis de er forskellige modulo  $m$ .

**Definition 2.2.** Lad  $p > 2$  være et primtal og  $\text{sfd}(a, p) = 1$ . Legendre symbolet  $\left(\frac{a}{p}\right)$  defineres til at være  $+1$ , hvis  $a$  er en kvadratisk rest og  $-1$ , hvis  $a$  er en ikke-kvadratisk rest modulo  $p$  samt  $0$  hvis  $p \mid a$ .

I beviset for Hasse's sætning bruger vi, at Legendre symbolet

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

hvor  $p > 2$  er et primtal og  $a \in \mathbb{Z}$  valgt så  $\text{sfd}(a, p) = 1$ . I Appendix afsn.3 er givet et bevis for denne påstand.

**2.5. Rationale funktioner over  $\mathbb{F}_p$ .** Vi definerer legemet af rationale funktioner med koefficienter i  $\mathbb{F}_p$  til at være

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

hvor  $\mathbb{F}_p[X]$  er polynomiumsringen over  $\mathbb{F}_p$ . Bemærk, at ethvert ikke 0-element kan inverteres. Givet  $\frac{f(x)}{g(x)} \neq 0$ -elementet - dvs.  $f$  ikke 0-polynomiet - da fås den inverse som  $\frac{g(x)}{f(x)} \in \mathbb{F}_p(x)$ , idet

$$\frac{f(x)}{g(x)} \frac{g(x)}{f(x)} = 1$$

Bemærk endvidere, at  $\text{char}(\mathbb{F}_p(x)) = p$  samt at  $\mathbb{F}_p \subseteq \mathbb{F}_p(x)$ , da  $a \in \mathbb{F}_p$  svarer til  $\frac{a}{1} \in \mathbb{F}_p(x)$ . Det er også værd at nævne, at overgangen  $\mathbb{F}_p[X] \longrightarrow \mathbb{F}_p(x)$  præcis svarer til overgangen  $\mathbb{Z} \longrightarrow \mathbb{Q}$  - dermed menes, at regnereglerne  $(+, \cdot)$  og andre egenskaber fra  $\mathbb{Q}$  også gælder i legemet  $\mathbb{F}_p(x)$ .

**2.6. Bevis for Hasse's sætning.** Nu til hovedresultatet i dette kapitel - Hasse's sætning. Ideen i beviset er fra [2] s.296-301 med reference til [6]. Fordelen ved dette bevis er, at den netop udnytter gruppestrukturen på en elliptisk kurve - dvs. vi kan benytte de resultater, vi opnåede i kapitel 1.

**Sætning 2.3.** *Lad  $E$  være en elliptisk kurve over  $\mathbb{Q}$  med koefficienter i  $\mathbb{Z}$*

$$y^2 = tf(x) = t(x^3 + ax^2 + bx + c) \tag{2.6}$$

med tilhørende diskriminant  $D$ . For ethvert ulige primtal  $p \nmid D$ ,  $t$  lader vi  $E_p$  være reduktion af  $E$  modulo  $p$ . Da gælder

$$|p + 1 - |E_p(\mathbb{F}_p)|| \leq 2\sqrt{p}$$

*Bevis.* Først observerer vi, at for  $p = 3$  gælder  $p < 2\sqrt{p}$ . For ethvert  $x \in \mathbb{F}_p$  får vi maksimalt to  $y$ -værdier, der løser 2.6. Da vi skal tælle i det projektive plan og dermed inkludere punktet  $\mathcal{O}$ , ser vi, at der for  $p = 3$  gælder

$$1 \leq |E_p(\mathbb{F}_p)| \leq 2p+1 \implies -p \leq p+1 - |E_p(\mathbb{F}_p)| \leq p \implies |p+1 - |E_p(\mathbb{F}_p)|| \leq p < 2\sqrt{p}$$

Så i tilfældet  $p = 3$  gælder Hasse's sætning.

For  $p > 3$  kan vi ved passende variabelskift få vores kurve  $E_p$  på formen

$$y^2 = x^3 + ax + b \tag{2.7}$$

hvor  $a, b \in \mathbb{F}_p$  -  $a, b$  skal ikke forveksles med  $a, b$  i Hasse's sætning 2.6. Som vi viste i afsnit 2.3, forbliver kurven elliptisk under variabelskiftet (dvs.  $D_p = -4a^3 - 27b^2 \neq 0$ ) og antallet af  $\mathbb{F}_p$ -rationale punkter ændres ikke. Så vi antager, at  $E_p$  er på formen 2.7.

Vi introducerer nu en ny kubisk kurve  $\mathcal{C}$  over legemet  $\mathbb{F}_p(x)$

$$\mathcal{C} : Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b} \tag{2.8}$$

Vi noterer os, at  $\mathcal{C}$  er en ikke-singulær kubiske kurve, idet den tilhørende diskriminant  $\tilde{D} = -4a^3 - 27b^2 \neq 0$ . Vi adderer punkter på  $\mathcal{C}$  på sædvanlig måde ved korde-tangent kompositionen defineret i kap.1. Endvidere har vi, at de projektive løsninger til 2.8 over  $\mathbb{F}_p(x)$  danner en kommutativ gruppe med  $\mathcal{O}$  som neutralelement. Vi finder hurtigt to  $\mathbb{F}_p(x)$ -rationale punkter på  $\mathcal{C}$

$$(X, Y) = (x, 1) \quad (X, Y) = (x^p, (x^3 + ax + b)^{\frac{p-1}{2}})$$

Det første punkt er oplagt et punkt på  $\mathcal{C}$ . Idet  $\text{char}(\mathbb{F}_p(x)) = p$  gælder, at

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

Denne påstand følger ved at notere sig, at i enhver ring  $R$  med primtalskarakteristik  $p > 0$  gælder, at  $(x+y)^p = x^p + y^p \quad \forall x, y \in R$ . Dette ses ved at bruge binomialformlen samt at  $p \mid \binom{p}{i} \quad \forall 1 \leq i \leq p-1$ . Benytter vi Fermat's sætning fra [3] s.20-21 på  $a, b \in \mathbb{F}_p$  - dvs.  $a^p = a$  og  $b^p = b$  - får vi nu, at også det andet punkt passer i 2.8.

Definér nu det  $n$ 'te gruppeelementet ved

$$P_n = (x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) + n(x, 1) \quad (2.9)$$

for  $n \in \mathbb{Z}$ . For  $P_n \neq \mathcal{O}$  skriver vi  $P_n = (X_n, Y_n)$ , hvor  $X_n, Y_n \in \mathbb{F}_p(x)$ . Ved at skrive  $X_n$  som en uforkortelig brøk  $X_n = \frac{f}{g}$  - dvs.  $\text{sfd}(f, g) = 1$  - defineres en følge af tal  $d_n : \mathbb{Z} \rightarrow \{0, 1, 2, 3, \dots\}$  ved

$$d_n = \begin{cases} 0 & \text{hvis } P_n = \mathcal{O} \\ \max\{\text{grad}(f), \text{grad}(g)\} & \text{ellers} \end{cases} \quad (2.10)$$

Det vil vise sig, at studiet af følgen  $\{d_n\}_{n \in \mathbb{Z}}$  præcis er nøglen til at vise Hasse's sætning. Vi har dog nu brug for et par hjælpesætninger. Den ene vil give en sammenhæng mellem  $|E_p(\mathbb{F}_p)|$  og  $d_0, d_{-1}$ . Den anden er en rekursionsformel, der gør os i stand til ud fra to på hinanden følgende  $d_n$ 'er ( $d_n, d_{n+1}$ ) at udregne ( $d_{n+2}$ ).

**Lemma 2.4.**

$$d_{-1} - d_0 - 1 = |E_p(\mathbb{F}_p)| - p - 1$$

*Bevis.* Ved at sætte  $n = 0$  i 2.9 og benytte definitionen af  $d_n$ , får vi straks  $d_0 = p$ . Lader vi nu  $N_p = |E_p(\mathbb{F}_p)| - 1$  være antallet af affine punkter på vores elliptiske kurve givet ved 2.7, skal vi vise

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

Med additionsformlerne fra kapitel 1, hvor vi nu arbejder med elliptisk kurve givet ved 2.8, får vi med  $t = \frac{1}{x^3 + ax + b}$

$$\begin{aligned} X_{-1} &= \{P_{-1}\}_x = \{(x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) - (x, 1)\}_x \\ &= \{(x^p, (x^3 + ax + b)^{\frac{p-1}{2}}) + (x, -1)\}_x \\ &= \frac{[1 + (x^3 + ax + b)^{\frac{p-1}{2}}]^2}{(x^p - x)^2} \frac{1}{\frac{1}{x^3 + ax + b}} - x - x^p \\ &= -x - x^p + \frac{[1 + (x^3 + ax + b)^{\frac{p-1}{2}}]^2 (x^3 + ax + b)}{(x^p - x)^2} \end{aligned} \quad (2.11)$$

$$= \frac{-x(x^p - x)^2 - x^p(x^p - x)^2 + [1 + (x^3 + ax + b)^{\frac{p-1}{2}}]^2(x^3 + ax + b)}{(x^p - x)^2}$$

Lad os analysere tællerens led i udtrykket for  $X_{-1}$ .

$$\begin{aligned} T_1(x) &= -x(x^p - x)^2 - x^p(x^p - x)^2 \\ &= -x(x^{2p} - 2x^{p+1} + x^2) - x^p(x^{2p} - 2x^{p+1} + x^2) \\ &= -x^{3p} + x^{2p+1} + x^{p+2} - x^3 \end{aligned}$$

$$\begin{aligned} T_2(x) &= (x^3 + ax + b)[1 + (x^3 + ax + b)^{\frac{p-1}{2}}]^2 \\ &= (x^3 + ax + b)[1 + 2(x^3 + ax + b)^{\frac{p-1}{2}} + (x^3 + ax + b)^{p-1}] \\ &= (x^3 + ax + b) + 2(x^3 + ax + b)^{\frac{p+1}{2}} + (x^3 + ax + b)^p \\ &= (x^3 + ax + b) + 2(x^3 + ax + b)^{\frac{p+1}{2}} + (x^{3p} + ax^p + b) \end{aligned}$$

↓

$$\begin{aligned} T_1(x) + T_2(x) &= x^{2p+1} + x^{p+2} + ax^p + 2(x^3 + ax + b)^{\frac{p+1}{2}} + ax + 2b \\ &= x^{2p+1} + R(x) \end{aligned}$$

hvor  $\text{grad}(R) < 2p + 1$ , idet  $\text{grad}((x^3 + ax + b)^{\frac{p+1}{2}}) = 3\frac{p+1}{2} < 2p + 1$  for  $p > 3$ .  
Dermed kan vi altså skrive

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

hvor  $\text{grad}(R) < 2p + 1$ . Idet  $\text{grad}((x^p - x)^2) = 2p$ , er graden af nævneren i  $X_{-1}$ , når  $X_{-1}$  er reduceret mest muligt, stadig èn mindre end graden af tælleren - dvs. lig  $d_{-1} - 1$ . Målet er at få reduceret  $X_{-1}$  mest muligt - at skrive  $X_{-1}$  som uforkortelig brøk. Men at reducere  $X_{-1}$  mest muligt svarer præcis til at reducere brøken i 2.11 mest muligt ifølge afsluttende bemærkning sidst i afsn.2.5. Vi vil se nærmere på denne brøk.

Først noterer vi os, at  $x^p - x$  har  $p$  rødder i  $\mathbb{F}_p$  ( Fermats sætning, [3] s.20-21 ). Heraf følger, at

$$(x^p - x)^2 = (x(x-1)(x-2)\dots(x-(p-1)))^2 = \prod_{j \in \mathbb{F}_p} (x-j)^2$$

For et element  $j \in \mathbb{F}_p$  benytter vi sætning om Legendre symbol ( se afsn.2.4 samt Appendiks afsn.3 ) til at få

$$(j^3 + aj + b)^{\frac{p-1}{2}} = \left( \frac{j^3 + aj + b}{p} \right) \quad (2.12)$$

I termer af afsn.2.4 samt Appendiks afsn.3, skal vi identificere  $j^3 + aj + b$  med  $\{\dots, \alpha - p, \alpha, \alpha + p, \alpha + 2p, \dots\}$  hvor  $\alpha \in \{0, 1, 2, \dots, p-1\}$ . For  $\alpha$  gælder nu

$$\left( \frac{\alpha}{p} \right) \equiv \alpha^{\frac{p-1}{2}} \pmod{p}$$

hvilket forklarer notationen i 2.12. Ifølge 2.12 ser vi endvidere, at

$$[1 + (j^3 + aj + b)^{\frac{p-1}{2}}] = 0 \iff \left( \frac{j^3 + aj + b}{p} \right) = -1$$

Dette giver, at  $j$  er rod i polynomiet  $[1 + (x^3 + ax + b)^{\frac{p-1}{2}}] \implies x - j$  optræder i tælleren præcis to gange iflg. 2.11. På samme måde får vi

$$[j^3 + aj + b] = 0 \iff \left(\frac{j^3 + aj + b}{p}\right) = 0$$

I dette tilfælde er  $j$  rod i polynomiet  $x^3 + ax + b$  og dermed  $x - j \mid (x^3 + ax + b)$ . Da 2.7 beskriver en ikke-singulær kubisk kurve, ser vi samtidig, at  $j$  er rod med multiplicitet 1, da rødderne i  $x^3 + ax + b$  er forskellige. Dermed får vi en faktor  $x - j$  i tælleren præcis én gang. Lad os opsummere - de led, der forekommer i nævneren i 2.11 efter reduktionen, er  $(x - j)^2$  når  $\left(\frac{j^3 + aj + b}{p}\right) = +1$  samt  $(x - j)$  når  $\left(\frac{j^3 + aj + b}{p}\right) = 0$ . Men pr. definition af kvadratiske rester får vi da  $(x - j)^2$  i nævneren, når der er to løsninger til ligningen  $y^2 = j^3 + aj + b$  og  $x - j$  i nævneren, når der er én løsning  $y = 0$  til denne. Men dette svarer præcis til de affine løsninger over  $\mathbb{F}_p$  til 2.7, og dermed er graden af nævneren efter reduktionen netop lig  $N_p$  - dvs.

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

hvilket viser lemmaet. □

**Lemma 2.5.** For  $n \in \mathbb{Z}$  gælder

$$d_{n-1} + d_{n+1} = 2d_n + 2 \tag{2.13}$$

*Bevis.* Der er først et par specialtilfælde at behandle. Antag først  $P_n = \mathcal{O}$ . Da har vi  $d_n = 0$  samt

$$P_{n+1} = P_n + (x, 1) = \mathcal{O} + (x, 1) = (x, 1)$$

$$P_{n-1} = P_n - (x, 1) = \mathcal{O} - (x, 1) = (x, -1)$$

hvilket straks giver  $d_{n+1} = d_{n-1} = 1$ . Med  $d_n = 0$  passer 2.13 i dette tilfælde. Bemærk, at vi her bruger resultat fra kapitel 1 - til et givet  $P = (x_0, y_0)$  er den additivt inverse  $-P = (x_0, -y_0)$ , når vores kurve er på formen 2.8. Antag herefter  $P_{n-1} = \mathcal{O}$ . Dette giver straks  $d_{n-1} = 0$  samt

$$P_n = P_{n-1} + (x, 1) = (x, 1) \implies d_n = 1$$

$$P_{n+1} = P_n + (x, 1) = 2(x, 1) = \left(\frac{(x^2 - a)^2 - 8bx}{4(x^3 + ax + b)}, Y_{n+1}\right)$$

Den sidste lighed følger ved at bruge fordblingsformlen 1.15 i kapitel 1 på punktet  $(x, 1)$  samt kurven  $\mathcal{C}$ . Bemærk, at vi faktisk kan skrive  $\{P_{n+1}\}_x$  som funktion af  $f, f'$ , hvor  $f(x) = x^3 + ax + b$

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

Men vi så jo tidligere, at 2.7 beskriver en ikke-singulær kubisk kurve, hvilket ifølge sætning 1.5 kapitel 1 giver, at  $\text{sfd}(f, f') = 1$ . Heraf ser vi, at  $\{P_{n+1}\}_x$  er uforkortelig  $\implies d_{n+1} = 4$ . Indsætter vi  $d_{n-1} = 0, d_n = 1, d_{n+1} = 4$  passer 2.13. Tilfældet  $P_{n+1} = \mathcal{O}$  foregår på præcis samme måde som tilfældet  $P_{n-1} = \mathcal{O}$ .

Vi vil derfor i det følgende antage  $P_{n-1}, P_n, P_{n+1} \neq \mathcal{O}$ . Endvidere skriver vi  $X_{n-1}, X_n, X_{n+1}$  som uforkortelige brøker

$$X_{n-1} = \frac{A}{B} \quad X_n = \frac{U}{V} \quad X_{n+1} = \frac{C}{D}$$

Idet

$$P_{n-1} = P_n - (x, 1) = \left(\frac{U}{V}, Y_n\right) + (x, -1)$$

$$P_{n+1} = P_n + (x, 1) = \left(\frac{U}{V}, Y_n\right) + (x, 1)$$

kan vi ved brug af additionsformler fra kapitel 1 og vores kurve på formen 2.8 nu udtrykke  $X_{n-1}, X_{n+1}$  ved  $X_n$

$$\begin{aligned} X_{n-1} &= \left(\frac{1+Y_n}{x-\frac{U}{V}}\right)^2 \frac{1}{\frac{1}{x^3+ax+b}} - x - \frac{U}{V} \\ &= \frac{V^3(1+Y_n)^2(x^3+ax+b)}{V(Vx-U)^2} - \left(\frac{Vx+U}{V}\right) \\ &= \frac{V^3(1+Y_n)^2(x^3+ax+b) - (Vx-U)^2(Vx+U)}{V(Vx-U)^2} \\ &= \frac{(Vx+U)(Ux+aV) + 2bV^2 + 2Y_n(x^3+ax+b)V^2}{(Vx-U)^2} \\ &= \frac{T}{(Vx-U)^2} \end{aligned} \tag{2.14}$$

Udtrykket 2.14 fås ved at benytte  $Y_n^2(x^3+ax+b) = (X_n^3+aX_n+b) = \left(\frac{U^3}{V^3} + a\frac{U}{V} + b\right)$ .

Ved symmetri ser vi, at udtrykket for  $X_{n+1}$  blot består i at erstatte  $(1+Y_n)$  med  $(1-Y_n)$ . For at få et udtryk svarende til 2.14 indsættes i dette  $-2Y_n$  i stedet for  $2Y_n$ . Vi får

$$\begin{aligned} X_{n+1} &= \frac{(Vx+U)(Ux+aV) + 2bV^2 - 2Y_n(x^3+ax+b)V^2}{(Vx-U)^2} \\ &= \frac{W}{(Vx-U)^2} \end{aligned} \tag{2.15}$$

Bemærk, at de indførte størrelser  $T, W \in \mathbb{F}_p[X]$ , idet  $Y_n(x^3+ax+b)V^2 \in \mathbb{F}_p[X]$ . Dette kan ses ved at benytte 2.8 på  $P_n = (X_n, Y_n) \in \mathcal{C}$  og få

$$Y_n^2V^4(x^3+ax+b)^2 = (x^3+ax+b)(U^3V+aUV^3+bV^4) \in \mathbb{F}_p[X]$$

Heraf følger, at nævneren i  $Y_n$  dividerer  $V^2$  og/eller  $x^3+ax+b$ , hvilket netop giver  $Y_n(x^3+ax+b)V^2 \in \mathbb{F}_p[X]$  og dermed ifølge 2.14, 2.15 at  $T, W \in \mathbb{F}_p[X]$ .

Lad os for god ordens skyld også nævne, at  $Vx-U$  er forskellig fra 0-polynomiet i  $\mathbb{F}_p(x)$ , da  $X_n \neq x$ . Idet antag omvendt  $X_n = x \iff Y_n = \pm 1$  ifølge 2.8. Dette giver  $P_n = \pm(x, 1)$  og dermed  $P_{n-1} = \mathcal{O}$  eller  $P_{n+1} = \mathcal{O}$  - men disse tilfælde forekommer pr. antagelse ikke.

Vi danner nu middelværdien af 2.14, 2.15 -  $\frac{X_{n-1}+X_{n+1}}{2}$ . Efter et par udregninger får man

$$\frac{X_{n-1}+X_{n+1}}{2} = \frac{UVx^2 + U^2x + axV^2 + 2bV^2 + aUV}{(Vx-U)^2} \tag{2.16}$$

Ved at multiplicere 2.14, 2.15 får man efter at have reduceret udtrykket samt benyttet  $Y_n^2 = \frac{X_n^3+aX_n+b}{x^3+ax+b}$

$$X_{n-1}X_{n+1} = \frac{TW}{(Vx-U)^4} = \frac{(Ux-aV)^2 - 4bV(Vx+U)}{(Vx-U)^2} \tag{2.17}$$

Vi ved samtidig også, at  $X_{n-1}X_{n+1} = \frac{AC}{BD}$  og  $X_{n-1} + X_{n+1} = \frac{AD+BC}{BD}$ . Antager vi nu ( denne antagelse vises sidst i lemmaet ), at  $BD = S(Vx - U)^2$ , hvor  $S \in \mathbb{F}_p^*$ , får vi fra 2.16,2.17 umiddelbart

$$AC = S[(Ux - aV)^2 - 4bV(Vx + U)] \quad (2.18)$$

$$AD + BC = 2S[UVx^2 + U^2x + axV^2 + 2bV^2 + aUV] \quad (2.19)$$

Heraf følger med ovennævnte antagelse samt 2.18, 2.19, at

$$\text{grad}(BD) = \text{grad}((Vx - U)^2) \quad (2.20)$$

$$\text{grad}(AC) = \text{grad}((Ux - aV)^2 - 4bV(Vx + U)) \quad (2.21)$$

$$\text{grad}(AD + BC) = \text{grad}(UVx^2 + U^2x + axV^2 + 2bV^2 + aUV) \quad (2.22)$$

Vi skal finde sammenhæng mellem  $d_{n-1}, d_n, d_{n+1}$  defineret ved

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

$$d_n = \max\{\text{grad}(U), \text{grad}(V)\}$$

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

Vi deler beviset ind i fire tilfælde.

1) Antag  $d_{n-1} = \text{grad}(A)$  og  $d_{n+1} = \text{grad}(C)$ . Ifølge 2.21 har vi så

$$d_{n-1} + d_{n+1} = \text{grad}(AC) = \text{grad}((Ux - aV)^2 - 4bV(Vx + U))$$

Hvis  $\text{grad}(U) \geq \text{grad}(V) \implies \text{grad}(AC) = \text{grad}(U^2x^2)$ , idet alle andre led i udtrykket for  $AC$  da har grad strengt mindre end  $\text{grad}(U^2x^2)$ . Idet  $\text{grad}(U^2x^2) = 2d_n + 2$  har vi  $d_{n-1} + d_{n+1} = 2d_n + 2$  og dermed vist lemmaet i dette tilfælde.

Omvendt hvis  $\text{grad}(U) < \text{grad}(V) \implies \text{grad}(BD) = \text{grad}(V^2x^2) = 2\text{grad}(V) + 2$  ifølge 2.20. Idet

$$AC = S[(Ux - aV)^2 - 4bV(Vx + U)] = S[U^2x^2 + a^2V^2 - 2aUVx - 4bV^2x - 4bUV]$$

hvor  $S \in \mathbb{F}_p^*$ , får vi

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

hvilket strider mod  $d_{n-1} = \text{grad}(A), d_{n+1} = \text{grad}(C)$ , som pr. definition af  $d_{n-1}, d_{n+1}$  netop giver  $\text{grad}(AC) \geq \text{grad}(BD)$ . Så tilfældet  $\text{grad}(U) < \text{grad}(V)$  ej mulig.

2) Antag  $d_{n-1} = \text{grad}(B)$  og  $d_{n+1} = \text{grad}(D)$ . Her får vi

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

Antager vi først  $\text{grad}(V) \geq \text{grad}(U) \implies \text{grad}(BD) = \text{grad}(V^2x^2)$ , da alle andre led i udtrykket for  $BD$  har grad strengt mindre end  $\text{grad}(V^2x^2)$ . Idet  $\text{grad}(V^2x^2) = 2d_n + 2$  har vi  $d_{n-1} + d_{n+1} = 2d_n + 2$  og dermed vist lemmaet i dette tilfælde.

Hvis vi omvendt har  $\text{grad}(V) < \text{grad}(U) \implies$

$$\text{grad}(BD) = \text{grad}(V^2x^2 + U^2 + UVx) \leq \text{grad}(U^2)$$

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

ved brug af 2.20,2.21. Den sidste ulighed er dog i modstrid med antagelsen om  $d_{n-1} = \text{grad}(B), d_{n+1} = \text{grad}(D)$ .

3) Antag  $d_{n-1} = \text{grad}(A) > \text{grad}(B)$  og  $d_{n+1} = \text{grad}(D) > \text{grad}(C)$ . Antagelserne giver os følgende uligheder

$$\text{grad}(AD) > \text{grad}(AC) \quad \text{grad}(AD) > \text{grad}(BD) \quad \text{grad}(AD) > \text{grad}(BC) \quad (2.23)$$

Den sidste ulighed sammen med 2.22 giver straks

$$\text{grad}(AD) = \text{grad}(AD + BC) = \text{grad}(UVx^2 + U^2x + axV^2 + 2bV^2 + aUV) \quad (2.24)$$

Antag først  $\text{grad}(U) \geq \text{grad}(V) \implies \text{grad}(AC) = \text{grad}(U^2x^2)$ . Ifølge 2.24 får vi da

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

hvilket strider mod den første ulighed i 2.23. Har vi derimod  $\text{grad}(U) < \text{grad}(V)$  giver 2.24 samt 2.20

$$\text{grad}(BD) = \text{grad}((Vx - U)^2) = \text{grad}(V^2x^2)$$

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

hvilket er i modstrid med den anden ulighed i 2.23 - dvs. tilfælde 3 forekommer ikke.

4) Antag  $d_{n-1} = \text{grad}(B) > \text{grad}(A)$  og  $d_{n+1} = \text{grad}(C) > \text{grad}(D)$ . Bemærk, at dette tilfælde er helt symmetrisk med det tredje tilfælde. Vi opstiller her ulighederne

$$\text{grad}(BC) > \text{grad}(AC) \quad \text{grad}(BC) > \text{grad}(BD) \quad \text{grad}(BC) > \text{grad}(AD) \quad (2.25)$$

Antag  $\text{grad}(U) \geq \text{grad}(V)$ . Heraf følger ved brug af 2.22 samt første ulighed i 2.25 at

$$\text{grad}(BC) \leq \text{grad}(U^2x^2) = \text{grad}(AC)$$

hvilket er en modstrid med 2.25. Har vi derimod  $\text{grad}(U) < \text{grad}(V)$  og bruger samme fremgangsmåde som før, får vi  $\text{grad}(BC) \leq \text{grad}(BD)$ , som strider mod den anden ulighed i 2.25 - dvs. tilfælde 4 forekommer ikke.

Dermed har vi gennemgået alle muligheder for  $d_{n-1}, d_n, d_{n+1}$ . For de tilladte tilfælde fik vi  $d_{n-1} + d_{n+1} = 2d_n + 2$ . Vi har nu vist lemmaet, hvis vi kan vise vores tidligere antagelse. Behandlingen heraf knytter sig til [5] s.229-231.

**Bevis for tidligere antagelse :**  $BD = (Vx - U)^2$  op til en konstant  $S \in \mathbb{F}_p^*$

Af 2.17 følger at  $(Vx - U)^2 \mid TW$ . Da kan vi skrive  $(Vx - U)^2 = T_1W_1$ , hvor  $T_1, W_1 \in \mathbb{F}_p[X]$  og  $T_1 \mid T$  samt  $W_1 \mid W$ . Idet

$$X_{n-1} = \frac{A}{B} = \frac{T}{(Vx - U)^2} = \frac{T}{T_1W_1}$$

følger, at  $B \mid W_1$ , da  $X_{n-1} = \frac{A}{B}$  er uforkortelig. Tilsvarende har vi

$$X_{n+1} = \frac{C}{D} = \frac{W}{(Vx - U)^2} = \frac{W}{T_1W_1}$$

hvilket giver  $D \mid T_1$ . Sammenholder vi dette, får vi  $BD \mid T_1W_1$  og dermed at  $BD \mid (Vx - U)^2$ . Kan vi vise

$$(Vx - U)^2 \mid BD \quad (2.26)$$

har vi netop vist  $BD = (Vx - U)^2$  op til en konstant.

Vi kan entydigt faktorisere  $(Vx - U) \in \mathbb{F}_p[X]$  i irreducible polynomier ([3] s.96). Vi kan altså skrive

$$(Vx - U) = ug_1g_2 \dots g_r$$

hvor  $u \in \mathbb{F}_p^*$  og  $g_1, g_2, \dots, g_r$  irreducible polynomier i  $\mathbb{F}_p[X]$ . Bemærk, at ethvert irreducibelt element i  $\mathbb{F}_p[X]$  er et primelement, idet  $\mathbb{F}_p[X]$  er et entydigt faktoriseringsdomæne (UFD).

Antager vi, at 2.26 ikke er sand, kan vi finde en irreducibel faktor  $h$  i udtrykket  $(Vx - U)$ , således at graden af  $h$  i faktoriseringen  $(Vx - U)^2$  er større end graden af  $h$  i faktoriseringen af  $BD$ . Kunne vi ikke finde et  $h$  med denne egenskab, ville vi jo netop have  $(Vx - U)^2 \mid BD$ . For at lette notationen indfører vi den diskrete valuation  $\nu_h$  defineret som følger. Lad  $h \in \mathbb{F}_p[X]$  være et irreducibelt polynomium.

Da er den diskrete valuation

$$\nu_h : \mathbb{F}_p[X] \longrightarrow \{0, 1, 2, \dots\}$$

givet ved  $\nu_h(g) = n$ , hvor  $g \in \mathbb{F}_p[X]$  og  $g = h^n r$  med  $\text{sfd}(h, r) = 1$ . Denne måler, hvor mange gange  $h$  går op i et polynomium. Vi vil i det følgende benytte  $\nu_h(g_1g_2) = \nu_h(g_1) + \nu_h(g_2)$ , hvilket nemt kan verificeres.

Med denne notation fås nu

$$\nu_h((Vx - U)^2) > \nu_h(BD)$$

Heraf følger, idet  $\frac{AC}{BD} = \frac{(Ux - aV)^2 - 4bV(Vx + U)}{(Vx - U)^2}$ , at

$$h \mid (Ux - aV)^2 - 4bV(Vx + U) = H$$

Dette giver sammen med 2.17, at  $h \mid TW \implies h \mid T \vee h \mid W$ , da  $h$  er et primelement.

Antager vi, at  $h$  dividerer både  $T, W$ , får vi

$$h \mid -\frac{(Vx + U)(Vx - U)^2}{V} + (1 - Y_n)^2(x^3 + ax + b)V^2$$

$$h \mid -\frac{(Vx + U)(Vx - U)^2}{V} + (1 + Y_n)^2(x^3 + ax + b)V^2$$

og dermed

$$h \mid -(Vx + U)(Vx - U)^2 + (1 - Y_n)^2(x^3 + ax + b)V^3$$

$$h \mid -(Vx + U)(Vx - U)^2 + (1 + Y_n)^2(x^3 + ax + b)V^3$$

Idet  $h \mid (Vx - U)$  giver ovenstående straks  $h \mid (1 - Y_n)^2(x^3 + ax + b)V^3$  samt  $h \mid (1 + Y_n)^2(x^3 + ax + b)V^3$ . Da  $h \mid (Vx - U)$  er muligheden  $h \mid V$  udelukket, da vi ellers har  $\text{sfd}(U, V) > 1$  i modstrid med at  $X_n$  er uforkortelig. Antager vi  $h \nmid (x^3 + ax + b)$ , får vi, idet  $h$  er et primelement

$$h \mid (1 - Y_n)^2 \implies h \mid (1 - Y_n)$$

$$h \mid (1 + Y_n)^2 \implies h \mid (1 + Y_n)$$

og dermed  $h \mid (1 + Y_n) + (1 - Y_n) = 2$ , hvilket er en modstrid. Altså konkluderer vi, at  $h \mid (x^3 + ax + b)$ .

Men gælder vores antagelse om, at  $h$  dividerer både  $T, W$ . Antag modsat at  $h$  dividerer  $T$  men ikke  $W$ . Da  $X_{n+1} = \frac{C}{D}$  er uforkortelig samt

$$X_{n+1} = \frac{W}{(Vx - U)^2}$$

observerer vi følgende

$$\nu_h((Vx - U)^2) = \nu_h(D) > 0 \quad (2.27)$$

$$\nu_h(C) = 0 \quad (2.28)$$

Den første observation følger, idet  $h \mid (Vx - U)$  vil optræde med samme grad i nævneren før og efter reduktionen af  $X_{n+1} = \frac{W}{(Vx-U)^2}$  - netop fordi  $h \nmid W$ . Idet  $h \mid D \implies h \nmid C$ , da  $\text{sfd}(C, D) = 1$  - dermed den anden observation.

Tidligere så vi  $h \mid (Ux - aV)^2 - 4bV(Vx + U) = \frac{AC}{BD}(Vx - U)^2 = H$ , hvilket giver

$$0 < \nu_h(H) = \nu_h(A) + \nu_h(C) - \nu_h(B) - \nu_h(D) + \nu_h((Vx - U)^2) = \nu_h(A) - \nu_h(B)$$

ifølge 2.27, 2.28. Dermed har vi  $\nu_h(A) > \nu_h(B)$ . Imidlertid kan vi dog ikke have både  $\nu_h(A) > 0$  og  $\nu_h(B) > 0$ , idet  $\text{sfd}(A, B) = 1$ . Dette giver

$$\nu_h(B) = 0 \quad (2.29)$$

2.27 sammen med 2.29 giver nu  $\nu_h(BD) = \nu_h(B) + \nu_h(D) = \nu_h((Vx - U)^2)$ , hvilket er i modstrid med  $\nu_h(BD) < \nu_h((Vx - U)^2)$ , som var konsekvensen af vores første antagelse  $(Vx - U)^2 \nmid BD$ . Havde vi antaget  $h \mid W$  men  $h \nmid T$ , ville vi få tilsvarende modstrid. Idet  $h \mid T$  eller  $h \mid W$ , konkluderer vi, at  $h$  derfor dividerer både  $T$  og  $W$ . Som vi viste tidligere, har vi så  $h \mid (x^3 + ax + b)$ .

Ved polynomisk division af  $H$  med  $(Vx - U)$  fås nu efter lange udregninger

$$H = -(Vx - U)[Ux^2 + (x^3 - 2ax - 4b)V] + (x^4 - 2ax^2 - 8bx + a^2)V^2$$

Idet  $h \mid (Vx - U)$  samt  $h \nmid V \implies h \mid (x^4 - 2ax^2 - 8bx + a^2)$ .

Ved at skrive diskriminanten  $D_p = -4a^3 - 27b^2$  for vores kurve givet ved 2.7 som linearkombination af  $(x^3 + ax + b)$ ,  $(x^4 - 2ax^2 - 8bx + a^2)$

$$D_p = (3x^3 - 5ax - 27b)(x^3 + ax + b) - (3x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2) \neq 0$$

ser vi, idet  $h \mid (x^3 + ax + b)$  samt  $h \mid (x^4 - 2ax^2 - 8bx + a^2)$ , at  $h \mid D_p$ . Dette er i modstrid med vores antagelse om, at  $h$  var irreducibelt polynomium - altså er 2.26 sand og  $BD = (Vx - U)^2$  op til en konstant  $S \in \mathbb{F}_p^*$  som ønsket. Dette faktum beviser lemmaet.  $\square$

Vi er nu i stand til at bevise Hasse's sætning. Ved induktion ses, at

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0 \quad (2.30)$$

For  $n = 0, -1$  gælder  $d_0 = d_0$  og  $d_{-1} = 1 + d_{-1} - d_0 - 1 + d_0 = d_{-1}$ . Antager vi 2.30 er rigtig for  $n - 1, n$  for et  $n \geq 0$ , skal vi vise 2.30 for  $n + 1$ . Pr. antagelse har vi

$$d_{n-1} = (n-1)^2 - (d_{-1} - d_0 - 1)(n-1) + d_0$$

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

Ved brug af Lemma 2.5 får vi da

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

Pr. induktion er 2.30 dermed rigtig for  $n \geq -1$ . For  $n \leq 0$  følger 2.30 på præcis samme måde. Indfører vi nu størrelsen  $\xi = p + 1 - |E_p(\mathbb{F}_p)| \in \mathbb{Z}$  fra Lemma 2.4 samt benytter  $d_0 = p$ , har vi da

$$d_n = n^2 + \xi n + p \quad (2.31)$$

Idet vi har  $d_n \geq 0$  for alle  $n \in \mathbb{Z}$ , er forskellen mellem de mulige reelle rødder i 2.31 højst lig 1, da vi ellers kan finde et  $n$ , således  $d_n < 0$ . Hvis vi antager 2.31 har reelle rødder, kan vi eksplícit angive den positive forskel mellem rødderne som

$$\delta = \sqrt{\xi^2 - 4p}$$

De mulige værdier for  $\delta$  er 0 eller tal  $\geq 1$ . Idet  $d_n \geq 0$ , er de mulige værdier for  $\delta$  i dette tilfælde præcis 0 eller 1. Spørgsmålet er, om vi kan have  $d_n = 0$  og  $d_{n+1} = 0$  - altså to på hinanden følgende  $d_n$ 'er lig 0. Min påstand er faktisk, at to på hinanden følgende  $d_n$ 'er ej kan være lige. Hvis vi for et  $n \in \mathbb{Z}$  har  $d_{n-1}, d_n$  lige, giver Lemma 2.5 straks  $d_{n+1}, d_{n-2}$  lige. Fortsætter vi på denne måde, ser vi, at  $d_n$  lige for alle  $n \in \mathbb{Z}$ , hvilket er i modstrid med  $d_0 = p$ . Så hvis 2.31 har en reel rod, er denne beskrevet ved, at diskriminanten  $D$  for 2.31 er lig 0 - ellers har vi  $D < 0$ . Konklusionen er derfor, at  $D \leq 0$ , hvilket giver

$$\xi^2 - 4p \leq 0 \implies |\xi| \leq 2\sqrt{p}$$

Indsætter vi  $\xi = p + 1 - |E_p(\mathbb{F}_p)|$ , får vi  $|p + 1 - |E_p(\mathbb{F}_p)|| \leq 2\sqrt{p}$  og dermed færdiggjort beviset for Hasse's sætning.  $\square$

**Bemærkning** Det skal dog nævnes, at for  $p > 3$  kan argumentet i beviset overtages, således at for et vilkårligt legeme  $\mathbb{F}_q$  med  $q = p^m$  elementer gælder

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

idet vi for  $p > 3$  blot benytter  $\text{char}(\mathbb{F}_q) = p$  samt, at  $\mathbb{F}_q$  er et legeme. Her er  $E$  elliptisk kurve på Weierstrass normal form

$$y^2 = t(x^3 + ax^2 + bx + c)$$

hvor  $t, a, b, c \in \mathbb{F}_q$  og  $t \neq 0$ -elementet i  $\mathbb{F}_q$ . For uddybende detaljer - se [5] s.222-231.

**2.7. Eksempler.** Vi vil afslutningsvis se et par eksempler vedrørende Hasse's sætning, hvor vi betragter elliptiske kurver over legemer  $\mathbb{F}_p$ , hvor  $p$  er et primtal. Idet  $2\sqrt{p} \notin \mathbb{Z}$  for primtal  $p$ , kan vi i de tilfælde omformulere Hasse's sætning, således at

$$|p + 1 - |E_p(\mathbb{F}_p)|| \leq \text{int}(2\sqrt{p})$$

hvor  $\text{int}(2\sqrt{p})$  betegner heltalsværdien af  $2\sqrt{p}$ . Vi vil se et par eksempler, hvor vi befinder os i de to ekstremumsværdier for korrektionsleddet - dvs. tilfælde, hvor

$$|E_p(\mathbb{F}_p)| = p + 1 + \text{int}(2\sqrt{p})$$

$$|E_p(\mathbb{F}_p)| = p + 1 - \text{int}(2\sqrt{p})$$

**Eksempel 1** Betragt elliptisk kurve  $E_1$  over  $\mathbb{F}_5$  givet ved Weierstrass-ligningen

$$y^2 = x^3 + 2x \tag{2.32}$$

Ved succesiv indsættelse af elementer fra  $\mathbb{F}_5$  i 2.32 og så løse om muligt for  $y$ , får vi

$$E_1(\mathbb{F}_5) = \{(0, 0), \mathcal{O}\} \implies |E_1(\mathbb{F}_5)| = 2 = (5 + 1) - 4 = (5 + 1) - \text{int}(2\sqrt{5})$$

**Eksempel 2** Betragt elliptisk kurve  $E_2$  over  $\mathbb{F}_3$  givet ved Weierstrass-ligningen

$$y^2 = x^3 + 2x + 1 \tag{2.33}$$

Samme analyse som i eksempel 1 giver nu

$$E_2(\mathbb{F}_3) = \{(0, \pm 1), (1, \pm 1), (2, \pm 1), \mathcal{O}\} \implies |E_2(\mathbb{F}_3)| = 7 = (3+1)+3 = (3+1)+\text{int}(2\sqrt{3})$$

**3.1. Indledning.** Det er velkendt, at ethvert naturligt tal  $n$  på entydig måde kan skrives som produkt af primtal. At finde primtalsfaktoriseringen for et stort tal  $n$ , skrevet som et produkt af to forskellige store primtal, er dog et beregningsmæssigt svært problem. Dette faktum er netop baggrunden for sikkerheden i mange kryptosystemer - heriblandt RSA ( mere herom senere ).

Et beregningsmæssigt svært problem er et problem, der ikke kan løses inden for overskuelig tid. Et eksempel på denne type er problemer med eksponentiel kompleksitet - dvs. problemer hvis beregningshastighed vokser eksponentielt med problemstørrelsen. Hvis det til gengæld ( med en bedre algoritme ) kan lade sig gøre at bringe problemet ned på polynomiel kompleksitet - f.eks  $n^2$  - betegnes problemet ikke længere som et beregningsmæssigt svært problem.

En måde, hvorpå ( f.eks RSA kryptosystemet ) kan brydes er ved at finde en hurtig faktoreringsalgoritme - en algoritme med polynomiel kompleksitet. Metoderne bliver stadig bedre, og det er dette kapitels formål at belyse et par af disse algoritmer herunder Pollard's faktoreringsalgoritme samt en grundig gennemgang af en endnu stærkere algoritme - Lenstra's faktoreringsalgoritme.

**3.2. Faktoreringsalgoritmer.** Lad  $n > 1$  være et heltal. Antager vi, at  $n$  kan faktorerises som  $n = n_1 n_2 \implies n_1 \leq \sqrt{n}$  eller  $n_2 \leq \sqrt{n}$ . Dette er en metode til at finde en primfaktor i  $n$  eller omvendt til at vise  $n$  er et primtal

1) hvis  $n$  er lige  $\implies 2 \mid n$

2) udfør divisionerne  $3 \mid n, 5 \mid n$  osv.

indtil vi når det største ulige tal  $\leq \sqrt{n}$ . Hvis  $n$  er sammensat vil man finde en faktor på denne måde. Finder man derimod ingen faktor i  $n$ , konkluderer vi, at  $n$  er et primtal. Vil man f.eks faktorisere et tal  $n$  med 200 cifre, som er et produkt af to primtal  $p \neq q$  hver med ca. 100 cifre, skal vi udføre ca.  $10^{100}$  trin med denne metode. Hvis hvert trin tager  $10^{-10}$  sekunder ( med en computer ), finder vi først primfaktoren efter  $10^{90}$  sekunder - omkring  $10^{72}$  år. Til sammenligning kan nævnes, at universets alder er  $5 \cdot 10^9$  år. For store primtal  $p, q$  er denne metode derfor ubrugelig.

En bedre løsning er Pollard's  $(p-1)$  algoritme ( [1] side 129-133 ). Vi skal lade  $n \geq 2$  betegne et sammensat heltal. Ideen er at antage  $p$  en primdivisor i  $n$ . Hvis  $a$  er et heltal så  $\text{sfd}(a, p) = 1$ , giver Fermat's sætning ( [3] side 20-21 ), at

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

Antag nu  $m$  er et heltal så  $(p-1) \mid m \implies a^m \equiv 1 \pmod{p}$  per kongruensregne regler. Den tænkte primfaktor  $p$  dividerer altså  $a^m - 1$ . Tallet  $\text{sfd}(n, a^m - 1)$  vil nu være en seriøs kandidat til en faktor i  $n$ , idet vi kan være heldige, at  $n$  har en primfaktor  $p$  således  $p-1 \mid m$  og dermed vil  $\text{sfd}(n, a^m - 1) \geq p > 1$ . Hvis  $\text{sfd}(n, a^m - 1) < n$  har vi altså en faktor. Strategien er at skrive  $m$  som produkt af de første små primtal -  $m = 2^{k_1} 3^{k_2} 5^{k_3} \dots q^{k_r}$  - i håb om, at  $p-1$  er et produkt af små primtal og dermed  $(p-1) \mid m$ . Bemærk - den underliggende teori er at benytte gruppestrukturen for  $\mathbb{Z}/p\mathbb{Z}$ . Vi vælger et  $a$  i  $(\mathbb{Z}/p\mathbb{Z})^*$  og vælger  $m$  i håb om, at  $|(\mathbb{Z}/p\mathbb{Z})^*| \mid m$ . Ved brug af Lagrange's index sætning får vi da

$$a \in (\mathbb{Z}/p\mathbb{Z})^* \implies a^{p-1} \equiv 1 \pmod{p}$$

$$|(\mathbb{Z}/p\mathbb{Z})^*| \mid m \implies a^m \equiv 1 \pmod{p} \iff p \mid a^m - 1$$

### Pollard's (p - 1) - algoritme

- 1) Vælg  $K > 1$  og udregn  $m = \text{lcm}(1, 2, \dots, K)$  - det mindste tal  $1, 2, \dots, K$  deler.
- 2) Vælg  $1 < a < n$  og beregn  $D = \text{sfd}(a, n)$ .
  - a.  $D > 1$  vi har en faktor
  - b.  $D = 1$  fortsæt
- 3) Udregn  $a^m - 1$  modulo  $n$  og beregn  $D = \text{sfd}(a^m - 1, n)$ .
  - a.  $D = n$  vælg nyt  $a$  i **2**
  - b.  $1 < D < n$  vi har en faktor
  - c.  $D = 1$  vælg større  $K$  i **1**

Ifølge Lemma sidst i dette afsnit er det kun nødvendigt at udregne  $a^k - 1$  modulo  $n$  i punkt **3**) ( dette sparer computerkraft ). For at illustrere pollard's algoritme kan det være nyttigt med et par eksempler.

**Eksempel 1** Vi ønsker at faktorisere  $n = 10403$ . Ved brug af Fermat's sætning, ser vi, at 10403 ej primtal, idet

$$2^{10403-1} \equiv 9296 \pmod{10403}$$

Jeg følger nu proceduren beskrevet i pollard's algoritme.

- Vælg  $K = 17 \implies k = 12252240$ .
- Vælg  $a = 2$  og beregn  $\text{sfd}(2, 10403) = 1$ .
- Udregn  $2^{12252240} - 1 \equiv 7004 \pmod{10403}$ .
- $\text{sfd}(7004, 10403) = 103$ .

Heraf findes faktoriseringen som  $10403 = 101 \cdot 103$ . Følgende tabel viser, at  $K = 17$  er det mindste  $K$ , hvor vi får gevinst med  $a = 2$ .

K	k	$2^k - 1 \pmod{10403}$	$\text{sfd}(2^k - 1, 10403)$
2	3	3	1
3	6	63	1
4	12	4095	1
5	60	4631	1
7	420	902	1
8	840	3974	1
9	2520	6457	1
11	27720	6255	1
13	360360	6348	1
16	720720	8578	1
17	12252240	7004	103

**Eksempel 2** Faktoriser  $n = 7591548931$ . Idet

$$2^{7591548931-1} \equiv 886944787 \pmod{7591548931}$$

får vi straks, at  $n$  ej primtal.

- Vælg  $K = 26 \implies k = 26771144400$ .
- Vælg  $a = 2$  og beregn  $\text{sfd}(2, 7591548931) = 1$ .
- Udregn  $2^{26771144400} - 1 \equiv 6878606797 \pmod{7591548931}$ .
- $\text{sfd}(6878606797, 7591548931) = 79801$ .

Heraf findes faktoriseringen  $7591548931 = 79801 \cdot 95131$ . Man kan nu bruge pollard's algoritme på disse faktorer, indtil den endelige primfaktoriserings er fundet. I dette tilfælde viser det sig, at vi har fundet primfaktoriseringsen. Man kan som i eksempel 1 igen vise, at  $K = 26$  er det mindste  $K$ , hvor vi får en faktor med  $a = 2$ .

**Bemærkning** Disse udregninger kan udføres med papir og blyant - ved udregning af  $a^k - 1$  modulo  $n$ , er det en fordel at skrive  $k$  i det binære talsystem og da benytte kongruensregneregler ( Modular exponentiation, beskrevet i [3] side 9-10 ). Udregning af  $\text{sfd}(a^k - 1, n)$  foregår med euclid's algoritme ( [3] side 12-14 ) . For store tal  $n, a, k$  foretrækker de fleste nok at benytte en computer til udregningerne - evt. lave et program, der gennemkører pollard's algoritme, indtil en faktor er fundet. Ovenstående eksempler er lavet ved brug af MAPLE V.

Nu til lemma, der gør udregning i pollard's algoritme nemmere.

**Lemma 3.1.** *Lad  $a, b, n$  være heltal. Antag  $b \equiv a \pmod{n}$ . Da er*

$$\text{sfd}(a, n) = \text{sfd}(b, n)$$

*Bevis.* Definer  $\alpha = \text{sfd}(a, n)$  og  $\beta = \text{sfd}(b, n)$ . Idet  $\beta \mid n, b$  samt  $b = a + qn$  for passende  $q$  ( $b \equiv a \pmod{n}$ ) ser vi straks, at  $\beta \mid a$  og dermed  $\beta \mid \alpha$ . På fuldstændig tilsvarende måde vises  $\alpha \mid \beta$ . Idet største fælles divisor af to heltal er det største positive tal, der deler disse, er  $\alpha, \beta > 0$  og dermed  $\alpha = \beta$  - dette viser lemmaet.  $\square$

Formålet i dette kapitel er, at beskrive anvendelsen af elliptiske kurver i Lenstra's faktoreringsalgoritme, der benytter gruppestrukturen på elliptiske kurver. Ideén i Lenstra's algoritme minder meget om ideén i Pollard's  $(p - 1)$  algoritme. Gennemgangen knytter sig til [1] side 68-69, 133-138 samt side 251-252.

**3.3. Ideén i Lenstra's Algoritme.** Lad  $n \in \mathbb{N}$  være et sammensat tal. Da har  $n$  en primfaktor  $p$ . Fremgangsmåden er følgende

- 1) Vælg elliptisk kurve  $E$  over  $\mathbb{Q}$  med koefficienter i  $\mathbb{Z}$  på formen

$$y^2 = x^3 + ax + b \quad \text{eller projektivt} \quad Y^2Z = X^3 + aXZ^2 + bZ^3 \quad (3.1)$$

således at  $p \nmid (-4a^3 - 27b^2)$  samt  $P = (r : s : t) \in E(\mathbb{Q}) \setminus \mathcal{O}$ . Reducerer vi nu koefficienterne  $a, b$  modulo  $p$  v.h.a afbildningen  $\gamma_p$  introduceret i kapitel 2.2, får vi

nu en ny elliptisk kurve  $E_p$  over  $\mathbb{F}_p$  ( præcis fordi  $p \nmid (-4a^3 - 27b^2)$ , se kap.2.2 ).

2) I det følgende arbejder vi i det projektive plan  $\mathbb{P}^2$  ( se Appendiks afsnit 1 ). Pr. valg af elliptisk kurve har vi  $P = (r : s : t) \in E(\mathbb{Q}) \setminus \mathcal{O}$ . Vi kan uden videre antage  $r, s, t \in \mathbb{Z}$  samt  $r, s, t$  indbyrdes primiske, idet vi ellers passende skalerer koordinaterne, indtil dette er tilfældet. I Lemma 3.2 nedenfor er vist, at  $P$  er på formen  $P = (\lambda d : \mu : d^3)$ . Reducerer vi nu punktet  $P$  modulo  $p$  med afbildningen

$$\gamma_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$$

får vi  $\gamma_p(P) = \gamma_p(r : s : t) = ([r]_p : [s]_p : [t]_p) = P_p$ . Idet

$$[r]_p = [s]_p = [t]_p = 0 \iff p \mid x \quad \wedge \quad p \mid y \quad \wedge \quad p \mid z$$

er  $P_p$  et gyldigt projektivt punkt, da  $r, s, t$  var valgt indbyrdes primiske. Endvidere har vi  $P_p \in E_p(\mathbb{F}_p)$ , idet  $P \in E(\mathbb{Q}) = E(\mathbb{Z})$  ( se Lemma 3.3 ).

3) Antag nu  $k$  vælges så  $|E_p(\mathbb{F}_p)| \mid k$ . Idet  $E_p(\mathbb{F}_p)$  er en endelig gruppe med neutralelement  $\gamma_p(\mathcal{O}) = \mathcal{O}_p$ , får vi da

$$kP_p = \mathcal{O}_p$$

Dette er en konsekvens af Lagrange's index sætning vist i [3] s.57.

Vi beregner nu  $kP = (\lambda_k d_k : \mu_k : d_k^3)$ . Idet  $\gamma_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$  er en gruppehomomorfi ( vises i Lemma 3.3 ), ser vi, at

$$\gamma_p(kP) = kP_p = \mathcal{O}_p \implies kP \in \ker(\gamma_p) \iff p \mid d_k^3 \iff p \mid d_k$$

Heraf følger, at  $\text{sfd}(d_k, n) \geq p$ . Hvis  $\text{sfd}(d_k, n) < n$  har vi hermed fundet en faktor. Er vi altså i den heldige situation, at  $k$  er valgt så  $|E_p(\mathbb{F}_p)| \mid k$  for en tænkt primtalsdivisor  $p \mid n$ , har vi  $\text{sfd}(d_k, n) \geq p$  - altså  $\text{sfd}(d_k, n)$  seriøs kandidat til en faktor i  $n$ .

Som lovet en uddybning af et par påstande nævnt ovenfor.

**Lemma 3.2.** *Givet elliptisk kurve  $E$  over  $\mathbb{Q}$  med koefficienter i  $\mathbb{Z}$  på formen*

$$y^2 = x^3 + ax + b \tag{3.2}$$

*Antag  $P \in E(\mathbb{Q}) \setminus \mathcal{O}$ . Da er  $P$  på formen  $P = (\frac{\lambda}{d^2}, \frac{\mu}{d^3})$ , hvor  $\text{sfd}(\lambda, d) = 1 = \text{sfd}(\mu, d)$ .*

*Bevis.* Vi skriver  $P = (\frac{\lambda}{M}, \frac{\mu}{N})$ , hvor  $\frac{\lambda}{M}, \frac{\mu}{N}$  er uforkortelige samt  $M, N > 0$ . Ved indsættelse af  $P$  i 3.2 fås nu

$$\begin{aligned} \left(\frac{\mu}{N}\right)^2 &= \left(\frac{\lambda}{M}\right)^3 + a\left(\frac{\lambda}{M}\right) + b \implies \\ \mu^2 M^3 &= \lambda^3 N^2 + a\lambda M^2 N^2 + bM^3 N^2 \end{aligned} \tag{3.3}$$

Heraf følger straks, idet  $\frac{\lambda}{M}, \frac{\mu}{N}$  er valgt uforkortelige

$$\begin{aligned} N^2 \mid M^3 \quad \text{samt} \quad M^2 \mid N^2 &\implies \\ N^2 \mid M^3 \quad \text{samt} \quad M^3 \mid N^2 &\implies M^3 = N^2 \end{aligned}$$

At  $M^3 \mid N^2$  følger ved at benytte  $M^3 \mid M^2 N^2$  i 3.3.

Idet  $M^2 \mid N^2$  samt  $M^3 = N^2$  konkluderer vi derfor, at  $M$  er et kvadrattal - dvs. der findes  $d = p_1 p_2 \dots p_r$  ( primtalsfaktorisering af  $d$  ) så  $M = d^2$ . Skrives  $M^3$  nu som produkt af primtal

$$M^3 = p_1^6 p_2^6 \dots p_r^6$$

får vi, idet  $M^3 = N^2$ , at  $N = p_1^3 p_2^3 \dots p_r^3$  (entydig faktorisering). Med  $d = p_1 p_2 \dots p_r$  betyder dette, at  $M = d^2$  samt  $N = d^3$ . Altså vi kan skrive  $P$  på formen

$$P = \left( \frac{\lambda}{d^2}, \frac{\mu}{d^3} \right) \quad \text{eller projektivt} \quad P = (\lambda d : \mu : d^3)$$

Valget af  $P$  giver automatisk, at  $\text{sfd}(\lambda, d) = 1 = \text{sfd}(\mu, d)$ . □

**Lemma 3.3.** *Lad  $E$  være elliptisk kurve som i 3.1. Da er reduktionsafbildningen modulo  $p$*

$$\gamma_p : E(\mathbb{Q}) \longrightarrow E_p(\mathbb{F}_p)$$

defineret ved  $\gamma_p(r : s : t) = ([r]_p : [s]_p : [t]_p)$  for  $P = (r : s : t) \in E(\mathbb{Q})$  en gruppehomomorfi. Hermed menes, at  $\gamma_p(P + Q) = \gamma_p(P) + \gamma_p(Q) = P_p + Q_p \forall P, Q \in E(\mathbb{Q})$ , hvor  $+$  er korde-tangent kompositionen.

*Bevis.* Lad først  $C$  være en vilkårlig projektiv kurve over  $\mathbb{Q}$  givet ved

$$C : F(X, Y, Z) = \sum_{i,j,k} a_{ijk} X^i Y^j Z^k = 0$$

hvor  $a_{ijk} \in \mathbb{Z}$ . Antag  $(x : y : z) \in C(\mathbb{Q}) \implies F(x, y, z) = \sum_{i,j,k} a_{ijk} x^i y^j z^k = 0$ . Vi kan jvf. tidligere bemærkninger antage  $x, y, z \in \mathbb{Z}$  indbyrdes primiske. Udfører vi nu reduktion modulo  $p$  samt benytter, at  $\gamma_p : \mathbb{Z} \longrightarrow \mathbb{F}_p$  er en ringhomomorfi, får vi

$$(F(x, y, z))_p = \left( \sum_{i,j,k} a_{ijk} x^i y^j z^k \right)_p = 0_p \implies$$

$$\sum_{i,j,k} a_{ijk} x_p^i y_p^j z_p^k = 0_p$$

og dermed  $(x_p : y_p : z_p) \in C_p : F_p(X, Y, Z) = 0_p$ . Så for et punkt  $P \in C(\mathbb{Q})$ , reducerer vi  $P$  modulo  $p$  og får et punkt  $P_p \in C_p(\mathbb{F}_p)$ .

Lader vi nu  $E$  være en elliptisk kurve over  $\mathbb{Q}$  med koefficienter i  $\mathbb{Z}$ . Vi skal da undersøge om  $\gamma_p(P + Q) = \gamma_p(P) + \gamma_p(Q)$ . Lad derfor  $P, Q \in E(\mathbb{Q})$  og antag blot både  $P, Q$  forskellig fra  $\mathcal{O}$ , idet sætningen i disse tilfælde trivielt er sand (husk at neutralelementet  $\mathcal{O}$  i  $E(\mathbb{Q})$  under afbildningen  $\gamma_p$  afbildes til neutralelementet  $\mathcal{O}_p$  i  $E_p(\mathbb{F}_p)$ ). Idet den projektive kurve  $C$  var valgt vilkårlig (dvs. også gyldig for linie i  $\mathbb{P}^2$ ) får vi, at linien gennem  $P, Q$  afbildes til linien gennem  $\gamma_p(P), \gamma_p(Q)$  under reduktionsafbildningen  $\gamma_p$ . Heraf fås straks, at  $\gamma_p(P * Q) = \gamma_p(P) * \gamma_p(Q)$  (se om notationen  $*$  i kap.1.4). Samme argument giver nu  $\gamma_p(P + Q) = \gamma_p(P) + \gamma_p(Q)$ , hvor  $+$  her er korde-tangent kompositionen. □

**Bemærkning** Givet en elliptisk kurve  $E$  over  $\mathbb{Q}$  ved

$$y^2 = x^3 + ax + b$$

hvor  $a, b \in \mathbb{Z}$ . Lad  $P \in E(\mathbb{Q})$ . For  $p \nmid -4a^3 - 27b^2$  gælder så

$$\gamma_p(kP) = k\gamma_p(P) = kP_p$$

**3.4. Lenstra's faktoreringsalgoritme.** Vi opskriver først Lenstra's algoritme for derefter at forklare de forskellige trin. Der afsluttes med et simpelt eksempel, hvor vi bruger Lenstra's algoritme til at faktorisere et heltal.

**Lenstra's Algoritme** Lad  $n \geq 2$  være et sammensat tal, som vi ønsker at faktorisere.

1) Undersøg om  $n$  kan skrives på formen  $N^r$ .

2) Beregn  $D = \text{sfd}(6, n)$ .

a.  $D > 1$  vi har en faktor og er færdig

b.  $D = 1$  fortsæt

3) Vælg heltal  $a, \alpha, \beta$ .

4) Sæt  $b = \beta^2 - \alpha^3 - a\alpha$  og lad  $E$  være kubisk kurve på formen

$$y^2 = x^3 + ax + b$$

med  $a, b$  som ovenfor. Bemærk  $P = (\alpha, \beta) \in E$ .

5) Udregn  $D = \text{sfd}(4a^3 + 27b^2, n)$

a.  $D = n$  vælg nyt  $a$  i **3**

b.  $1 < D < n$  vi har en faktor og er færdig

c.  $D = 1$  fortsæt

6) Vælg  $K > 1$  og sæt  $k = \text{mfm}(1, 2, \dots, K)$  - det mindste tal som  $1, 2, \dots, K$  deler.

7) Beregn  $kP = (\lambda_k d_k : \mu_k : d_k^3)$  og udregn  $D = \text{sfd}(d_k, n)$

a.  $D = n$  vælg mindre  $k$  i **6**

b.  $1 < D < n$  vi har en faktor og er færdig

c.  $D = 1$  vælg større  $k$  i **6** eller vælg nyt  $a$  i **3**

Der er en del uddybende argumenter at tilføje til nogle af punkterne i algoritmen.

1) Man bør undersøge, om  $n$  er på formen  $N^r$  - ved at udregne

$$\sqrt{n}, \sqrt[3]{n}, \dots, \sqrt[s]{n}$$

indtil  $1 < \sqrt[s]{n} < 2$ . Er ingen af disse heltal, konkluderer vi, at  $n$  ej kan skrives som  $N^r$  for passende  $N, r$ . Denne metode afslører hurtigt, om  $n$  er på denne form og i så fald en faktor i  $n$ .

2) Hvis  $\text{sfd}(6, n) > 1$  har vi fundet en faktor - selvfølgelig kan vi opnå  $\text{sfd}(6, n) = n$ , men da er  $n$  lig 2, 3 eller 6. Ellers har vi  $\text{sfd}(6, n) = 1$ , hvilket fortæller os, at  $2, 3 \nmid n$ .

4) Efter at have valgt tilfældige heltal  $a, \alpha, \beta$  danner vi kubisk kurve  $E$  på formen

$$y^2 = x^3 + ax + b \tag{3.4}$$

Kurven er valgt så  $P = (\alpha, \beta) \in E$  - dvs.  $b = \beta^2 - \alpha^3 - a\alpha$ .

5) Vi udregner her  $D = \text{sfd}(4a^3 + 27b^2, n)$ , hvor  $a, b$  er de tilfældigt valgte heltal i punkt **3**. Denne udregning afslører, om  $E$  og  $E_p$  er elliptiske kurver for enhver mulig primdivisor  $p \mid n$ . Reducér evt.  $4a^3 + 27b^2$  modulo  $n$  ( se Lemma 3.1 ).

Hvis  $D = n$  vil  $E_p$  ( $E$  reduceret modulo  $p$ ) for en mulig primdivisor  $p \mid n$  ikke være en elliptisk kurve, idet  $p \mid 4a^3 + 27b^2$ . Vi vælger derfor et nyt  $a$ . Vi kan også have  $1 < D < n$ , hvilket straks giver os en faktor i  $n$ . Sidst kan vi have  $D = 1$  - dette har ikke givet os en faktor, men den vigtige information at  $E, E_p$  begge er elliptiske kurver.

6) Vi vælger et  $k$  i håb om, at  $|E_p(\mathbb{F}_p)| \mid k$  for en tænkt primtalsdivisor  $p \mid n$ .

7) Herefter udregnes  $kP = (\lambda_k d_k : \mu_k : d_k^3)$ . Det er her nyttigt at opskrive  $k$  i det binære talsystem som

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

hvor  $k_i \in \{0, 1\}$  for alle  $i = 0, 1, 2, \dots, r$ . Udregn nu

$$P_0 = P$$

$$P_1 = 2P_0 = 2P$$

$$P_2 = 2P_1 = 2^2 P$$

$$\vdots$$

$$P_r = 2P_{r-1} = 2^r P$$

ved brug af fordoblingsformlerne 1.15, 1.16 i kapitel 1 samt kurven 3.4. Vi har nu

$$kP = k_0 P + k_1 2^1 P + k_2 2^2 P + \dots + k_r 2^r P = \sum_{i, \text{ hvor } k_i \neq 0} P_i$$

Af tidligere Lemma er  $kP$  neutralelementet  $\mathcal{O}$  eller på formen  $kP = (\frac{\lambda_k}{d_k^2}, \frac{\mu_k}{d_k^3})$ . Hvis  $kP = \mathcal{O}$  vælges et mindre  $k$  - der findes jo et  $k$  så  $kP \neq \mathcal{O}$  (dvs.  $d_k \neq 0$ ). Antag derfor nu

$$kP = (\frac{\lambda_k}{d_k^2}, \frac{\mu_k}{d_k^3})$$

Strategien er nu om muligt at reducere  $kP$  modulo  $n$  - man ville få

$$(kP)_n = ((\lambda_k)_n (d_k)_n^{-2}, (\mu_k)_n (d_k)_n^{-3})$$

Denne reduktion forudsætter dog, at det inverse element til  $d_k$  i  $\mathbb{Z}/n\mathbb{Z}$  findes. Derfor kan  $kP$  reduceres modulo  $n$  hvis og kun hvis  $\text{sfd}(d_k, n) = 1$ . Befinder vi os altså i en situation, hvor  $kP$  ej kan reduceres modulo  $n$  (dvs.  $\text{sfd}(d_k, n) > 1$ ), vil  $\text{sfd}(d_k, n)$  være seriøs kandidat til en faktor i  $n$ . Dette giver os følgende situationer

a.  $D = \text{sfd}(d_k, n) = 1$  vælg større  $k$  i **6** eller vælg nyt  $a$  i **3**

b.  $1 < D < n$  vi har en faktor og er færdig

a.  $D = n$  vælg mindre  $k$  i **6**

For store  $k$  bliver disse udregninger dog svære at gennemføre. Det er derfor en fordel at lave udregningerne modulo  $n$ . Proceduren er at reducere  $E$  givet i 3.4 modulo  $n$  og få ny kurve  $E_n$  på formen

$$y^2 = x^3 + ax + b \tag{3.5}$$

hvor nu  $a, b \in \mathbb{Z}/n\mathbb{Z}$  er de oprindelige koefficienter  $a, b$  reduceret modulo  $n$ . At reducere  $kP$  modulo  $n$  (hvis denne reduktion er mulig) svarer til at udregne  $kP_n$  ifølge tidligere Lemma. Punktet  $P_n = (\alpha, \beta) \in E_n$ , hvor  $\alpha, \beta \in \mathbb{Z}/n\mathbb{Z}$  er opnået ved at reducere det oprindelige punkt  $P$  modulo  $n$ .

Men som vi så tidligere, er det ikke altid muligt at lave disse regninger modulo  $n$ . Lad os analysere problemet omkring addition af punkter på kurven  $E_n$  givet ved 3.5. Lad i det følgende  $Q_1 = (x_1, y_1), Q_2 = (x_2, y_2)$ , hvor  $x_1, y_1, x_2, y_2 \in \mathbb{Z}/n\mathbb{Z}$ , være punkter på  $E_n$  og + korde-tangent kompositionen.

- For  $Q_1 \neq Q_2$  giver udregninger fra kapitel 1

$$(Q_1 + Q_2)_x = m^2 - x_1 - x_2$$

hvor  $m = \frac{y_2 - y_1}{x_2 - x_1}$ . Men udregning af  $m$  i  $\mathbb{Z}/n\mathbb{Z}$  er kun mulig hvis  $x_2 - x_1$  har invers element i  $\mathbb{Z}/n\mathbb{Z}$ . Idet  $\text{sfd}(x_2 - x_1, n) = 1 \iff x_2 - x_1$  er en enhed i  $\mathbb{Z}/n\mathbb{Z}$ , ser vi, at betingelsen for at kunne addere  $Q_1, Q_2$  er at  $\text{sfd}(x_2 - x_1, n) = 1$ .

Hvis derimod  $1 < \text{sfd}(x_2 - x_1, n) < n$  kan vi ikke addere  $Q_1, Q_2$  men har fundet en faktor i  $n$ .

I tilfældet  $\text{sfd}(x_2 - x_1, n) = n$  er vi uheldige. Vi kan gå til punkt **6** og reducere værdien af  $k$  eller vælge anden kurve.

- For  $Q_1 = Q_2$  giver vores additionsformler

$$(Q_1 + Q_2)_x = l^2 - x_1 - x_2$$

hvor  $l = \frac{3x_1^2 + a}{2y_1}$ . Så udregning af  $2Q_1$  modulo  $n$  lader sig kun gøre hvis  $\text{sfd}(y_1, n) = 1$ . Fejler additionen, kan vi få en ikke-triviel faktor eller vi er uheldige og må vælge et mindre  $k$  eller ny kurve.

Dette er netop essensen i Lenstra's algoritme - vi kan være heldige at finde faktor, når addition af punkter på  $E_n(\mathbb{Z}/n\mathbb{Z})$  ikke lader sig gøre. Følgende bemærkning viser, at vi med denne algoritme også kan afsløre om et tal er sammensat - det kræver blot, at additionen af punkter bryder sammen.

**Bemærkning** Hvis  $n$  er et primtal, vil alle vore udregninger kunne lade sig gøre, idet  $\mathbb{Z}/n\mathbb{Z}$  er et legeme  $\implies E_n(\mathbb{Z}/n\mathbb{Z}) = \{(x, y) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \mid (x, y) \in E\} \cup \mathcal{O}_n$  vil danne en kommutativ gruppe m.h.t korde-tangent kompositionen. Hvis vi derfor på et tidspunkt ikke kan addere to punkter på  $E_n(\mathbb{Z}/n\mathbb{Z})$  ( et element vi ikke kan invertere ), slutter vi logisk, at  $n$  ikke kan være et primtal.

Hvad er fordelene ved Lenstra's faktoriseringsalgoritme i forhold til Pollard's algoritme. Pollard's algoritme går godt, hvis der findes et primtal  $p \mid n$  således  $p - 1 = |(\mathbb{Z}/p\mathbb{Z})^*|$  er et produkt af små primtal. Hvis der omvendt ikke findes en sådan primdivisor  $p \mid n$  så  $p - 1$  er et produkt af små primtal, vil denne metode ikke være brugbar. Præcis her viser Lenstra's algoritme sig at have en ekstra facilitet. Som beskrevet tidligere går Lenstra's algoritme godt, hvis der findes primdivisor  $p \mid n$ , så  $|E_p(\mathbb{F}_p)|$  er et produkt af små primtal ( bemærk samspillet: I Pollard's algoritme udnyttes gruppestrukturen på  $\mathbb{Z}/p\mathbb{Z}$  mens man i Lenstra's algoritme arbejder i gruppen  $E_p(\mathbb{F}_p)$  ). Hvis der omvendt ikke findes en sådan primdivisor  $p \mid n$ , kan man blot vælge en ny kurve og gentage algoritmen. Idet  $|E_p(\mathbb{F}_p)|$  er spredt ud over et interval svarende til de i kapitel 2 udregnede værdier ( Hasse's sætning )

$$|E_p(\mathbb{F}_p)| = p + 1 - \epsilon_p \quad \text{hvor} \quad |\epsilon_p| \leq 2\sqrt{p}$$

vil chancerne for hurtigt at vælge en kurve med de nævnte egenskaber være relativt gode.

For god ordens skyld viser jeg et lemma, der flittigt har været brugt.

**Lemma 3.4.**  $[m]_n$  er enhed i  $\mathbb{Z}/n\mathbb{Z} \iff \text{sfd}(m, n) = 1$ .

*Bevis.* Antag først  $\text{sfd}(m, n) = 1 \implies \exists a, b \in \mathbb{Z} : am + bn = 1$  ( Euklids algoritme [3] side 12-14 ). Heraf følger

$$[am + bn]_n = [am]_n + [bn]_n = [a]_n[m]_n + [b]_n[n]_n = [a]_n[m]_n = [1]_n$$

hvilket viser, at  $[m]_n$  er en enhed i  $\mathbb{Z}/n\mathbb{Z}$ .

Hvis omvendt  $[m]_n$  er enhed i  $\mathbb{Z}/n\mathbb{Z}$  findes  $[\lambda]_n$  så  $[\lambda]_n[m]_n = [\lambda m]_n = [1]_n$ , hvilket giver eksistens af et  $l \in \mathbb{Z}$  så  $\lambda m + ln = 1$ . Vi vil vise, at det eneste positive heltal, der dividerer både  $m, n$  er 1 - altså

$$d \mid n \wedge d \mid m \implies d = 1$$

Antag der findes  $d \in \mathbb{N}$  så  $d \mid m, n$ . Idet  $1 = \lambda m + ln$  fås da præcis  $d = 1$ . □

Lad os afslutningsvis se et eksempel på brugen af Lenstra's algoritme til faktorisering af heltal. I det følgende bruger vi fordoblings- og additionsformlerne fra kapitel 1. Disse er implementeret i MAPLE V og vi vil bruge udregninger herfra.

**Eksempel 3** Følgende eksempel er taget fra [1] side 144, hvor det er stillet som en opgave. Lad  $n = 199843247$ . Brug Lenstra's algoritme på punktet  $P = (1, 1) \in E(\mathbb{Q})$  samt  $k = 16296$  til at faktorisere  $n$ .

- Idet  $2^{199843247-1} \equiv 101742834 \pmod{199843247}$  konkluderer vi at 199843247 ej et primtal.
- Idet ingen af tallene

$$\sqrt{n}, \sqrt[3]{n}, \dots, \sqrt[31]{n} \approx 1,8525$$

er heltal konkluderer vi, at  $n$  ej er på formen  $N^r$  for passende  $N, r$ .

- $\text{sfd}(199843247, 6) = 1$ .
- Jeg vælger elliptisk kurve over  $\mathbb{Q}$  med koefficienter i  $\mathbb{Z}$  på formen

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

således  $P = (1, 1) \in E(\mathbb{Q})$ .

- $D = \text{sfd}(4 \cdot 59^3 + 27 \cdot (-59)^2, 199843247) = 1$ .
- Vælg nu  $k = 16296 = 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3$
- Udregning af  $2^i P$  mod 199843247 for  $i = 0, 1..13$  er indholdet i følgende tabel.

$i$	$2^i P \text{ mod } 199843247$
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 kan nu begynde at addere disse punkter modulo  $n$  ved brug af formler beregnet i kapitel 1. Vi får

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

Vi får nu punktet  $kP \pmod{n}$  ved at addere  $2^{13}P$  og  $(2^3 + \dots + 2^{12})P$  modulo  $n$

$$(116509380, 17886653) + (3834541, 80821724) \pmod{n}$$

Addition af disse punkter kræver dog, at vi til differensen af  $x$ -koordinaterne kan udregne den inverse modulo  $n$ . Man opdager dog, at den inverse ikke findes, idet

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

Her ser vi netop pointen i Lenstra's algoritme. Vi forsøger at udregne  $16296(1,1)$  modulo  $199843247$  på den valgte elliptiske kurve. Denne addition kan dog ikke lade sig gøre, men giver istedet en faktor. Dette leder faktisk til den endelige primtalsfaktorisering

$$199843247 = 10289 \cdot 19423$$

## 4. KRYPTOSYSTEMER

**4.1. Public key kryptosystemer.** Et public key system er et kryptosystem, der bl.a. har den egenskab at enkryptering (kodning) og dekryptering (afkodning) af en meddelelse foregår med to forskellige nøgler. Afsenderen krypterer sin meddelelse med modtagerens offentlige nøgle. Herefter kan kun modtageren foretage dekrypteringen, hvilket gøres med modtagerens hemmelige nøgle. Ethvert menneske på jorden kan altså faktisk have et eksemplar af ethvert andet menneskes offentlige nøgle, mens kun modtageren af en besked er i besiddelse af sin egen hemmelige nøgle.

Public key kryptosystemet blev i 1976 defineret af Whitfield Diffie og Martin Hellman. En mere tilbundsående beskrivelse af systemet kan læses i [7] side 56-58.

**4.2. RSA kryptosystemet.** RSA kryptosystemet blev udviklet i 1977 af Rivest, Shamir og Adleman, og sikkerheden i dette kryptosystem er netop baseret på faktoreringsproblemet. Det vil være dette kapitels formål i tilknytning til [7] side 101-105 at beskrive metoden samt vise, at RSA kryptosystemet fungerer. Endvidere diskuteres enkryptering/dekryptering i henhold til et eksempel. Sidst lidt om sikkerheden ved RSA kryptosystemet samt alternative kryptosystemer.

Først introduceres Eulers  $\varphi$ -funktion  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ , der til et givet naturligt tal  $n$  tæller antal naturlige tal mindre end samt relativt primisk med  $n$ . Vi har altså følgende

**Definition 4.1.** Lad  $n \in \mathbb{N}$  være naturligt tal. Da er

$$\varphi(n) = |\{a \in \mathbb{N} | 0 \leq a \leq n, \text{sfd}(a, n) = 1\}|$$

**Bemærkning** For  $m, n$  relativt primiske gælder  $\varphi(mn) = \varphi(m)\varphi(n)$  som vist i [3] side 21-22. For to primtal  $p \neq q$  gælder da

$$\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$$

ved brug af definition af Eulers  $\varphi$ -funktion.

I RSA kryptosystemet beregnes nøglerne som følger

- Vælg to tilfældigt store primtal  $p \neq q$  - typisk hver på ca. 100 cifre. Sæt  $n = pq$ .
- Beregn  $\varphi(n) = (p-1)(q-1)$ .
- Vælg  $e \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$  - dvs. naturligt tal  $0 < e < \varphi(n)$  så  $\text{sfd}(e, \varphi(n)) = 1$ .
- Beregn det inverse element  $d$  til  $e$  - man skal altså vælge et positivt tal  $d$  så  $(p-1)(q-1) \mid ed - 1$ .

Der er et par bemærkninger at tilføje. Antag  $e$  er valgt relativt primisk med  $\varphi(n)$ . Når  $p, q, e$  er valgt, kan  $d$  da udregnes ved brug af Euklids algoritme. Idet  $\text{sfd}(e, (p-1)(q-1)) = 1$  findes heltal  $x, y$  så

$$x(p-1)(q-1) + ye = 1$$

Opskrivningen  $x(p-1)(q-1) + ye = (x-e)(p-1)(q-1) + (y+(p-1)(q-1))e$  gør, at vi kan antage  $x < 0$  og  $y > 0$ . Dette giver eksistens af naturlige tal  $d, k$  så

$$k(p-1)(q-1) = ed - 1$$

Den offentlige nøgle består af  $(n, e)$ . Den hemmelige nøgle består af  $d$ . En meddelelse konverteres til tal og inddeles i blokke. Vælger vi at kode alfabetet ved  $A = 21, B = 22, C = 23, \dots$  konverteres meddelelsen FERMAT eksempelvis til 262538332140 - som deles op i blokkene 2625, 3833, 2140. Her er det vigtigt, at ingen af disse tal er større end eller lig det valgte  $n$ . Lad os prøve at beskrive enkryptering/dekryptering af et tal.

Lad  $1 \leq B < n$  være et heltal. Enkryptering af  $B$  er beskrevet ved enkrypteringsfunktionen  $E$  defineret ved

$$E(B) = [B^e]_n \quad (4.1)$$

Tilsvarende er dekrypteringsfunktionen  $D$  defineret ved

$$D(B) = [B^d]_n \quad (4.2)$$

hvor  $[x]_n$  betegner rest af  $x$  ved division med  $n$ .

Følgende sætning, inspireret af [3] side 28-29, viser, at RSA kryptosystemet fungerer - altså dekryptering af en enkrypteret tekst genskaber teksten.

**Sætning 4.2.** *Antag  $n = pq$  er produkt af to forskellige primtal. Lad  $E, D$  være enkrypterings/dekrypterings-funktionerne defineret i 4.1, 4.2 og lad  $1 \leq B < n$  være et heltal. Da er*

$$D(E(B)) = B$$

*Bevis.* Idet  $D(E(B)) = [[B^e]_n^d]_n = [B^{ed}]_n$ , vil vi vise  $[B^{ed}]_n = B$  eller ækvivalent  $B^{k(p-1)(q-1)+1} \equiv B \pmod{n}$  for et vilkårligt naturligt tal  $k$  ( der findes jo ifølge tidligere bemærkning naturligt tal  $k$  så  $k(p-1)(q-1) + 1 = ed$  ).

Antag først  $\text{sfd}(B, n) = 1 \implies \text{sfd}(B^k, n) = 1$ . Ved brug af Eulers sætning ( [3] side 20 ) fås nu

$$(B^k)^{\varphi(n)} \equiv 1 \pmod{n} \implies B^{k(p-1)(q-1)} \equiv 1 \pmod{n}$$

og dermed  $B^{k(p-1)(q-1)+1} \equiv B \pmod{n}$ .

Antag herefter  $\text{sfd}(B, n) > 1$ . Hvis  $n$  dividerer  $B$  - dvs.  $\text{sfd}(B, n) = n$  - følger straks  $B^{k(p-1)(q-1)+1} \equiv B \pmod{n}$ . Lad derfor nu  $\text{sfd}(B, n) < n$ . Dette giver, at kun en af primfaktorerne  $p, q$  dividerer  $B$ . Antager vi  $q \mid B$  og  $p \nmid B$  har vi  $\text{sfd}(B^{k(q-1)}, p) = 1$  og dermed

$$(B^{k(q-1)})^{p-1} \equiv 1 \pmod{p}$$

ifølge Fermat's sætning. Heraf ser vi

$$p \mid B^{k(q-1)(p-1)+1} - B \quad \wedge \quad q \mid B^{k(q-1)(p-1)+1} - B \implies pq \mid B^{k(q-1)(p-1)+1} - B$$

Den sidste konklusion fås idet  $\text{sfd}(p, q) = 1$ . Men her står jo at læse

$$B^{k(q-1)(p-1)+1} \equiv B \pmod{n}$$

hvoraf sætningen følger. □

Lad os se et eksempel på hvordan man enkrypterer og dekrypterer en tekst.

**Eksempel** Som vi så tidligere konverteres klarteksten FERMAT, når vi vælger at kode vores alfabet som tidligere beskrevet, til tallet 262538332140 - som vi deler op i blokkene 2625, 3833, 2140. Nu skal et RSA datasæt genereres.

Jeg vælger først  $p = 101, q = 103$  og får  $n = 10403$  samt  $\varphi(n) = 10200$ . Der skal nu vælges  $e \in (\mathbb{Z}/\varphi(n)\mathbb{Z})^*$  - jeg vælger  $e = 53$  som opfylder  $\text{sfd}(53, 10200) = 1$ . Herefter

beregnes  $d = 2117$ . Den offentlige nøgle består nu af talparret  $(10403, 53)$  mens den hemmelige nøgle er beskrevet ved tallet 2117. Vi foretager nu enkrypteringen blokvis og får

$$E(2625) = [2625^{53}]_{10403} = 3736$$

$$E(3833) = [3833^{53}]_{10403} = 2400$$

$$E(2140) = [2140^{53}]_{10403} = 5445$$

Kryptoteksten bliver altså 3736, 2400, 5445. Modtageren dekrypterer kryptoteksten ved

$$D(3736) = [3736^{2117}]_{10403} = 2625$$

$$D(2400) = [2400^{2117}]_{10403} = 3833$$

$$D(5445) = [5445^{2117}]_{10403} = 2140$$

Dekrypteringen fungerede altså, og vi kommer let tilbage til klarteksten FERMAT. De nødvendige udregninger er lavet i MAPLE V, men kunne i princippet være lavet med papir og blyant blot man mestrer Euklids algoritme samt Modulær exponentiation ( [3] side 12-14 samt side 9-10 ). Det skal dog bemærkes, at man i den virkelige kryptoverden vælger  $p, q$  ( og dermed  $n$  ) meget større for at højne sikkerheden. I dette eksempel ville man hurtigt kunne faktorisere  $n$  - bl.a ved pollard's algoritme beskrevet i kapitel 3 eksempel 1.

**4.3. Sikkerhed ved RSA.** Grunden til sikkerheden i RSA kryptosystemet er, at  $p, q$  ikke er kendt. Derfor er det meget vanskeligt at beregne  $\varphi(n)$  og dermed den hemmelige nøgle  $d$ . Tallet  $n$  er dog kendt, så kunne man blot faktorisere  $n$ , var man færdig. For store  $n$  - dvs.  $p, q$  af størrelsesordenen  $10^{100}$  - viser dette sig ( i dag ) at være umuligt inden for overskuelig tid. Én af matematikkens store opgaver er at faktorisere store tal og som beskrevet i kapitel 3, er der udviklet mange hurtige faktoreringsalgoritmer til dette formål. Der er dog stadig ikke fundet en polynomieltidsløsning på problemet. Ergo - vælges  $p, q$  store nok ( og dermed  $n$  stor ) vil RSA ikke ad denne vej kunne brydes inden for overskuelig tid.

**4.4. Alternativt kryptosystem.** Selvom RSA kryptosystemet på nuværende tidspunkt må anses for ubrydeligt, blot  $p, q$  vælges store nok, er der i de senere år forsket meget i nye kryptosystemer, hvor sikkerheden er større. Hermed menes systemer, for hvilke det anses for mindre sandsynligt, at der nogensinde findes en polynomieltidsløsning til at løse problemet og dermed bryde systemet. Desuden ønsker man, at nøglerne skal være små og enkle således, at en- og dekryptering kan foretages hurtigere. Et ret nyt kryptosystem, der netop opfylder ovenstående gør brug af elliptiske kurver. Det pågældende system kaldes ECDSA ( elliptic curve digital signature algorithm ) som nedenfor kort vil blive omtalt. Idéen er i grove træk følgende:

Der vælges en elliptisk kurve  $E$  over  $\mathbb{F}_p$  (  $p > 3$  et primtal ) og et punkt  $P$  på kurven. Herefter vælges et tilfældigt tal  $d$ , og punktet  $Q = dP$  udregnes. Den offentlige nøgle består nu af bl.a  $E, P, Q$  mens den hemmelige nøgle består af tallet  $d$ . Det viser sig at være et endnu sværere problem at beregne  $d$  - givet  $E, P, Q$  - end det tilsvarende problem i RSA - at faktorisere  $n$ . Lad os se, hvordan nøglerne præcis beregnes.

## ECDSA nøgle – beregning.

- Vælg elliptisk kurve  $E$  over  $\mathbb{F}_p$  på formen

$$y^2 = x^3 + ax + b$$

således der findes stort primtal  $\eta$  som deler  $|E(\mathbb{F}_p)|$ .

- Vælg et punkt  $P \in E(\mathbb{F}_p)$  af orden  $\eta$ .
- Vælg tilfældigt heltal  $d \in \{1, 2, \dots, \eta - 1\}$ .
- Udregn  $Q = dP$ .

Først vælges en elliptisk kurve  $E$  over  $\mathbb{F}_p$  på den velkendte form og antag denne valgt således et stort primtal  $\eta$  dividerer  $|E(\mathbb{F}_p)|$ . Man vælger sig herefter et punkt  $P \in E(\mathbb{F}_p)$  af orden  $\eta$ . Lad os prøve at analysere, hvordan  $P$  bestemmes. Da argumentet ikke er specielt for gruppen af punkter på en elliptisk kurve, gennemføres argumentet for en vilkårlig endelig kommutativ gruppe  $G$ .

Lad  $G$  med  $|G| = n$  være endelig kommutativ gruppe med neutralelement  $e$  og antag  $n = p^i m$  hvor  $\text{sfd}(p, m) = 1$  og  $i > 0$ . Altså er  $p$  et primtal, der dividerer  $|G|$ , hvilket straks giver eksistens af et element  $g \in G$  af orden  $p$  ( Cauchy's sætning, [8] side 53-54 ). For et tilfældigt element  $g \in G$  lader vi  $|\langle g \rangle|$  betegne ordenen af  $g$ .

Idet ordenen af  $g$  dividerer  $|G|$  kan vi have følgende situationer

$$\mathbf{1)} \quad |\langle g \rangle| = p^r s \text{ hvor } r = 0 \text{ og } s \mid m.$$

$$\mathbf{2)} \quad |\langle g \rangle| = p^j l \text{ hvor } j > 0 \text{ og } l \mid m.$$

Er vi i tilfælde 1, vælger vi andet  $g$ . Er vi derimod i tilfælde 2, danner vi elementet  $h = g^{p^{j-1}l} \in G$  som har orden  $p$ , da  $h^p = e$  og  $h \neq e$ .

Vi har altså nu valgt et punkt  $P \in E(\mathbb{F}_p)$  af orden  $\eta$ , hvor  $\eta \mid |E(\mathbb{F}_p)|$ . At finde ordenen af en vilkårlig elliptisk kurve er dog svært og involverer Schoofs algoritme. Antager vi  $E, P$  valgt på den ønskede måde, vælges  $d \in \{1, 2, \dots, \eta - 1\}$  og punktet  $Q = dP$  beregnes.

Den offentlige nøgle er nu  $(E, P, \eta, Q)$ , mens den hemmelige nøgle er beskrevet ved tallet  $d$ . Sikkerheden ved ECDSA, som beskrevet ovenfor, består i problemet med at løse det Diskrete Logaritme Problem for Elliptiske Kurver ( ECDLP ): Givet elliptisk kurve  $E$  over  $\mathbb{F}_p$  samt  $P \in E(\mathbb{F}_p)$  af orden  $\eta$  og  $Q \in E(\mathbb{F}_p)$ . Bestem da - om muligt - heltallet  $d$ ,  $0 \leq d \leq \eta - 1$ , således  $Q = dP$ . I de senere år har matematikere rundt om i verden forsøgt at angribe dette problem, men der er endnu ikke ( hvad jeg ved af ) meldt om svaghedstegn ved ECDLP. Yderligere information om ECDSA - bl.a om en- og dekryptering af meddelelse - kan hentes på ”<http://www.certicom.com/research/wecdsa.html>”, hvorfra jeg har fået inspiration.

4.5. **Afslutningsvis.** Elliptiske kurver - matematisk objekt med mange smukke egenskaber. Specielt har vi etableret en gruppestruktur på de  $k$ -rationale punkter på en elliptisk kurve. Endvidere studerede vi elliptiske kurver over endelige legemer, fik bevist Hasse's utrolige sætning samt så på nogle nyttige praktiske anvendelser af elliptiske kurver. Sidst vil jeg dog tilføje et ekstra punkt. Studiet af elliptiske kurver var faktisk krumtappen i beviset for tidens sværeste matematiske problem - Fermat's sidste sætning. Pierre de Fermat ( Fransk matematiker, 1601-65 ) nedskrev i et gyldent øjeblik, at ligningen  $x^n + y^n = z^n$  ikke har nogen heltallige løsninger  $x, y, z$  for heltal  $n > 2$ . Forbløffende resultat - når man ved at studere  $n = 1, 2$  finder uendelig mange løsninger. Beviset for Fermat's sidste sætning er indeholdt i følgende sætninger hentet fra <http://www.mbay.net/cgd/ft/ft01.htm>

**Sætning 4.3.** *Antag  $(x, y, z, n)$  en løsning til Fermat's ligning. Da vil den elliptiske kurve defineret ved ligningen*

$$Y^2 = X(X - x^n)(X + x^n)$$

*ikke være modulær.*

**Sætning 4.4.** *Alle elliptiske kurver med rationale koefficienter er modulære.*

Så med en løsning til Fermat's ligning vil man kunne konstruere en elliptisk kurve med for mange egenskaber. Store matematikere som Gauss, Kummer, Euler, Lamè og Dirichlet har forsøgt at bevise Fermat's sidste sætning men uden held. Først i 1994 - en tidlig september morgen - lykkedes det den engelske matematiker, Andrew Wiles, efter 7 år's intens arbejde at bevise Fermat's sidste sætning.

## 5. APPENDIKS

**5.1. Projektiv geometri.** Vi vil her kort give en algebraisk definition af det projektive plan i tilknytning til [1] s.220-232. For et legeme  $k$  defineres det projektive plan  $\mathbb{P}^2(k)$  over  $k$  til mængden af ækvivalensklasser  $(x : y : z)$ , hvor  $x, y, z \in k$  ikke alle er lig 0 ) under ækvivalensrelationen defineret ved

$$(x : y : z) \sim (x' : y' : z') \iff \exists \lambda \neq 0 : x = \lambda x', y = \lambda y', z = \lambda z'$$

- altså

$$\mathbb{P}^2(k) = \{(x, y, z) \in k^3 \setminus (0, 0, 0)\} / \sim \quad (5.1)$$

En linie i  $\mathbb{P}^2(k)$  er mængden af "punkter" i  $\mathbb{P}^2(k)$ , hvis koordinater løser en ligning på formen  $\alpha X + \beta Y + \gamma Z = 0$  for  $\alpha, \beta, \gamma$  konstante og ikke alle lig 0.

Det sædvanlige affine plan  $k^2 = \{(x, y) \mid x \in k, y \in k\}$  afbildes injektivt ind i  $\mathbb{P}^2(k)$  under  $\phi : k^2 \rightarrow \mathbb{P}^2(k)$  givet ved  $\phi(x, y) = (x : y : 1)$ . Vi har her associeret ethvert punkt i  $k^2$  med et punkt i det projektive plan ved hjælp af afbildningen  $\phi$ . Punkter i  $\mathbb{P}^2(k)$ , der ikke kan associeres med et punkt i  $k^2$ , er præcis dem, hvor  $z$ -koordinaten er 0. Linien beskrevet ved  $Z = 0$  kaldes linien i uendelig. Man skriver ofte

$$\mathbb{P}^2(k) = k^2 \cup \text{linie i } \infty$$

En kurve i  $\mathbb{P}^2(k)$  - en projektiv kurve - beskrives som dens affine del samt dens punkter i uendelig. Starter vi med en kurve  $C_0 : f(x, y) = 0$  i  $k^2$ , kan vi finde dens projektive kurve beskrevet ved  $F(X, Y, Z) = 0$ . Dette gøres ved at homogenisere  $C_0$ . Lad  $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$ . Da er  $F(X, Y, Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$ , hvor  $d = \text{grad}(f)$ . Tilsvarende siger vi at dehomogenisere en kurve  $F(X, Y, Z) = 0$  med hensyn til  $z$ -variablen  $Z$  - ved at sætte  $Z = 1$  og få affin kurve  $F(x, y, 1) = 0$  i  $xy$ -planet.

**5.2. Bezout's Sætning.** Vi vil her vise et specialtilfælde af en Bezout's sætning - nemlig

**Sætning 5.1.** *Lad  $L$  være en linie og  $E$  en elliptisk kurve i det projektive plan begge defineret over et legeme  $k$ . Lad  $\bar{k}$  være en algebraisk lukket udvidelse af  $k$ . Da har vi*

$$\sum_{P \in E(\bar{k}) \cap L(\bar{k})} i(P, E, L) = 3$$

hvor  $i(P, E, L)$  er snitmultipliciteten af linien  $L$  med kurven  $E$  i punktet  $P$ .

**Bemærkning** Antag  $P \in E \cap L$ . Vi kan antage  $P = (0, 0)$  ved koordinattransformation. Linien  $L$  kan da parametriseres ved  $\phi(s) = \begin{pmatrix} as \\ bs \end{pmatrix}$ . Givet  $E : F(x, y) = 0$  - findes skæringspunkter med  $L$  ved substitution, dvs. find de  $s : F(as, bs) = 0$ . Bemærk  $s = 0$  er en løsning, der giver punktet  $P$ . Da  $s = 0$  er rod i  $F$ , har vi  $s \mid F(as, bs)$ . Antag nu, at vi kan skrive

$$F(as, bs) = s^d g(s) \quad \wedge \quad g(0) \neq 0$$

Da er snitmultipliciteten i punktet  $P$  defineret til at være  $i(P, E, L) = d$ .

Nu til beviset.

*Bevis.* Punkterne på en elliptisk kurve  $E$  i det projektive plan består af punkter i det affine plan samt dets punkter i uendelig. Vores projektive kurve er på formen

$$E : Y^2 Z = t(X^3 + aX^2 Z + bX Z^2 + cZ^3)$$

$Z = 0$ : Som vi før har set, skærer  $E$  linien  $Z = 0$  i præcis et punkt  $\mathcal{O} = (0 : 1 : 0)$ . Hvordan opfører vores kurve sig nær  $\mathcal{O}$ . Vi laver lokale affine koordinater og beskriver kurven i  $xz$ -planet, hvor koordinatsættet for  $\mathcal{O}$  er  $(0, 0)$ .

$$Z = t(X^3 + aX^2Z + bXZ^2 + cZ^3) \quad (5.2)$$

Linien  $Z = 0$  i  $xz$ -planet parametriseres ved  $\psi(s) = \begin{pmatrix} s \\ 0 \end{pmatrix}$ . Snitmultiplicitet findes ved substitution af parametriseringen for  $Z = 0$  i 5.2. Man finder

$$ts^3 = 0 \implies s^3 = 0 \implies s^3 \cdot 1 = 0$$

hvor  $1(0, 0) \neq 0$  Altså  $i(\mathcal{O}, E, Z = 0) = 3$ .

Den affine del af  $E$  kan beskrives som løsninger til

$$y^2 = t(x^3 + ax^2 + bx + c)$$

Enhver linie i det affine plan kan parametriseres ved  $\varphi(s) = \begin{pmatrix} \alpha s + \beta \\ \gamma s + \xi \end{pmatrix}$

$\alpha \neq 0$ : Skæringspunkter i det affine plan findes ved i udtrykket for  $E$  at substituere  $x = \beta, y = \gamma s + \xi$ . Dette giver andengradslikning i  $s$ , som vi ved har præcis to løsninger talt med multiplicitet, eftersom  $\bar{k}$  er en algebraisk lukket udvidelse af  $k$  (Algebraens fundamentalsætning).

Linien i det affine plan  $x = \beta$  homogeniseres ved at sætte  $x = \frac{X}{Z} \implies X = \beta Z$ . Denne linie skærer  $Z = 0$  i  $\mathcal{O} \in E(k)$ , da  $Z = 0 \implies X = 0$ . Vi parametriserer nu linien i  $xz$ -planen og får  $\psi(s) = \begin{pmatrix} \beta s \\ s \end{pmatrix}$  Substitueres nu i 5.2 fås

$$t(\beta^3 s^3 + a\beta^2 s^3 + b\beta s^3 + cs^3) - s = 0 \implies$$

$$t\beta^3 s^3 + at\beta^2 s^3 + bt\beta s^3 + cts^3 - s = 0 \implies$$

$$s(t\beta^3 s^2 + at\beta^2 s^2 + bt\beta s^2 + cts^2 - 1) = 0$$

Heraf aflæses  $i(\mathcal{O}, L, E) = 1$ .

$\alpha \neq 0$ : Vi substituerer nu  $x = \alpha s + \beta, y = \gamma s + \xi$  i  $E$  og finder nu en tredjegradslikning i  $s$ , som vi ved har præcis tre løsninger talt med multiplicitet. Hvornår skærer denne linie  $Z = 0$ . Linien i affin form  $y - \frac{\gamma}{\alpha}x + (\xi - \frac{\gamma\beta}{\alpha}) = 0$  homogeniseres

$$Y - \frac{\gamma}{\alpha}X + (\xi - \frac{\gamma\beta}{\alpha})Z = 0$$

Heraf aflæses skæringspunktet med  $Z = 0$  til  $(\frac{\alpha}{\gamma} : 1 : 0) \neq \mathcal{O}$ . □

**Bemærkning** Vi har benyttet, at definitionen af snitmultiplicitet og multiplicitet er ens. At funktionen  $f$  har en rod  $\beta$  med multiplicitet  $m$ , betyder jo netop, at

$$m = \max\{n \in \mathbb{N} \mid (s - \beta)^n \mid f\}$$

Dvs.  $f(s) = (s - \beta)^m h(s)$ , hvor  $h(\beta) \neq 0$ . Ved koordinattransformation fås så

$$f(s) = s^m h(s), \quad h(0) \neq 0$$

hvilket betyder, at  $\beta$  har snitmultiplicitet  $m$ .

5.3. **Sætning om Legendre symbol.** I kapitel 2 definerede vi kvadratiske rester og Legendre symbol i tilknytning til [4] s.63-64 og brugte i beviset for Hasse's sætning følgende

**Sætning 5.2.** *Lad  $p > 2$  være et primtal og  $a \in \mathbb{Z}$  være relativt primisk med  $p$  - dvs.  $\text{sfd}(a, p) = 1$ . Da gælder*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

*Bevis.* Antag først  $\left(\frac{a}{p}\right) = 1$ . Da har  $x^2 \equiv a \pmod{p}$  en løsning  $x_0$ . Bemærk, at  $x_0 \neq 0$  og multiplum af  $p$ , da  $a$  og  $p$  er relativt primiske. Fermat's sætning beskrevet i [3] s.20-21 giver nu, idet  $\text{sfd}(x_0, p) = 1$ , at

$$x_0^{p-1} \equiv 1 \pmod{p}$$

Men  $x_0^2 \equiv a \pmod{p} \implies x_0^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}$ , hvilket viser

$$a^{\frac{p-1}{2}} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$$

Hvis  $\left(\frac{a}{p}\right) = -1$  har kongruensligningen  $x^2 \equiv a \pmod{p}$  ingen løsning. Men for alle  $1 \leq j \leq p-1$  findes præcis et  $i$  modulo  $p$  således at  $ij \equiv 1 \pmod{p}$ , idet ethvert ikke 0-element i  $\mathbb{F}_p$  har præcis et inverst element. Vælges  $l = ai$  ser vi, at

$$\forall 1 \leq j \leq p-1 \exists! 1 \leq l \leq p-1 : lj \equiv a \pmod{p}$$

Bemærk, at givet  $j$  - da har vi automatisk  $l \neq 0$ , idet  $\text{sfd}(a, p) = 1$  samt  $l \neq j$ , da kongruensen  $x^2 \equiv a \pmod{p}$  ikke har nogen løsning. Heltallene  $1, 2, \dots, p-1$  deles nu op i forskellige par  $(l_n, j_n)$  i henhold til ovenstående, således at vi får

$$\begin{aligned} l_1 j_1 &\equiv a \pmod{p} \\ l_2 j_2 &\equiv a \pmod{p} \\ &\vdots \\ l_{\frac{p-1}{2}} j_{\frac{p-1}{2}} &\equiv a \pmod{p} \end{aligned}$$

Benytter vi nu kongruensregnerregler samt, at de  $\frac{p-1}{2}$  par  $(l_n, j_n)$  præcis svarer til tallene  $1, 2, \dots, p-1$ , får vi

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

I [3] s.94 er vist, at  $(p-1)! \equiv -1 \pmod{p}$  og dermed

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}$$

□

**Bemærkning** Hvis  $\left(\frac{a}{p}\right) = 0$  har vi, at  $p \mid a$  og dermed  $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$  for  $p > 2$ . Dette giver  $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ .

LITTERATUR

- [1] J.H.Silverman&J.Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.
- [2] A.W.Knapp, *Elliptic Curves*, Princeton University Press, Princeton NJ, 1992.
- [3] N. Lauritzen, *Algebra I & II*, Matematisk Institut, Aarhus Universitet, 1999
- [4] I.Niven & H.S.Zuckerman *An Introduction to the Theory of Numbers* , Third Edition, John Wiley & Sons Inc. New York-London-Sydney-Toronto, 1972
- [5] Jasbir S.Chahal, *Manin's proof of the Hasse Inequality Revisited*, Brigham Young University, Utah, Nieuw Arch. Wisk. (4) Vol 13, 1995
- [6] Manin, Yu.I., On Cubic Congruences to a Prime Modulus Amer. Math. Soc. Transl. (2) Vol 13, 1960
- [7] Knud Nissen & Peter Landrock, *Kryptologi - fra viden til videnskab*, 1.udgave Forlaget ABACUS, 1997
- [8] Johan P. Hansen, *Algebra* , Bind 1, Matematisk Institut, Aarhus Universitet, 1992

*E-mail address:* hoegh49@mail.tele.dk

DEPARTMENT OF MATHEMATICS, NY MUNKEGADE, 8000 AARHUS C, DENMARK  
PRIVAT: HØEGH GULDBERGSGADE 49,3-7, 8000 AARHUS C, DENMARK