

# ELLIPTISKE KURVER

KASPER KJØLBY

*Vejleder: Johan P Hansen.*

## INDHOLD

|                                                               |    |
|---------------------------------------------------------------|----|
| 1. Gruppestrukturen                                           | 2  |
| 1.1. Introduktion                                             | 2  |
| 1.2. Korde-tangent kompositionen                              | 5  |
| 1.3. Additionsformler                                         | 6  |
| 1.4. Associativiteten                                         | 7  |
| 1.5. Gruppestrukturen                                         | 9  |
| 2. Elliptiske kurver over endelige legemer og Hasses sætning  | 10 |
| 2.1. Introduktion                                             | 10 |
| 2.2. Bevis for Hasse's sætning                                | 11 |
| 2.3. Eksempler på elliptiske kurver over endelige legemer.    | 18 |
| 3. Faktorisering                                              | 19 |
| 3.1. Introduktion                                             | 19 |
| 3.2. Pollards algoritme                                       | 19 |
| 3.3. Lenstras algoritme                                       | 20 |
| Bilag A.                                                      | 23 |
| A.1. Specialtilfælde af Bezouts sætning                       | 23 |
| A.2. Kvadratisk rest, Legendre symbolet og Diskret valuation. | 25 |
| Litteratur                                                    | 26 |

## 1. GRUPPESTRUKTUREN

1.1. **Introduktion.** Ideerne til dette kapitel er fra [1] kap.1 og 2. En kubisk kurve er en ligning på formen:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \quad (1.1)$$

som siges, at være over et legeme  $k$ , hvis koefficienterne er fra  $k$ . Det viser sig, at hvis der er en rationel løsning til (1.1) og karakteristikken af  $k$  er forskellig fra 2, kan man ved rationelle manipulationer få den på formen:

$$y^2 = x^3 + ax^2 + bx + c = f(x), \quad (1.2)$$

hvor  $a, b, c \in k$ . Denne form kaldes for Weierstrass normal form. Dette giver anledning til følgende definition.

**Definition 1.1.** Enhver kubisk ligning  $E$ , kaldes for en elliptisk kurve, hvis den er på Weierstrassform og, kurven er glat. D.v.s at hvis  $F = y^2 - f(x)$ , så er  $\frac{\partial F}{\partial x}$  og  $\frac{\partial F}{\partial y}$  ikke 0 samtidigt. Er koefficienter fra legemet  $k$  siges det, at være en elliptisk kurve over  $k$ .

Vi vil i det følgende, med mindre andet er nævnt, kun beskæftige os med kurver på Weierstrassform. Vi skal lige have lidt terminologi op at stå. Hvis et punkt har koordinater i legemet  $k$ , siges punktet at være  $k$ -rationelt. Mængden af  $k$ -rationelle punkter på  $E$  betegnes med  $E(k)$ . Har man givet en elliptisk kurve, findes der en komposition på kurvens punkter kaldet korde-tangent kompositionen. Ideen til kompositionen er følgende: Man vælger sig et  $k$ -rationelt punkt  $\mathcal{O}$  på kurven. Givet to  $k$ -rationelle punkter,  $P$  og  $Q$ , trækker man en linie gennem de to punkter. Linien skærer kurven en gang mere i et nyt punkt  $P * Q$ . Dette er ikke resultatet af kompositionen. Det fås ved at trække en linie gennem  $\mathcal{O}$  og  $P * Q$  og finde skæringen med kurven. Hvis  $P = Q$  tager man i stedet tangenten til  $P$ . Den vil skære kurven i  $P * P$ . Igen trækkes linien igennem  $\mathcal{O}$  og  $P * P$  for at finde resultatet af kompositionen. Se figur 1.

Lad os undersøge kravet om at  $E$  er glat. Det giver anledning til følgende sætning.

**Sætning 1.2.** *Lad  $E$  være en kubisk kurve over  $k$  ( $k$  har karakteristik  $\neq 2$ ), der er på Weierstrassform. Da er følgende ensbetydende.*

- 1)  $E$  er en elliptisk kurve
- 2)  $E$  er glat
- 3) Hvis man ser på polynomiet i  $x$  givet ved  $y^2 = f(x)$ , så er rødderne i  $f(x)$  forskellige. Det kan så være nødvendigt at kigge på en udvidelse af  $k$  således at  $f$  har 3 rødder.
- 4) Diskriminanten  $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$

*Bevis.* At 1)  $\Leftrightarrow$  2) følger af definitionen af elliptiske kurver. Så

2)  $\Leftrightarrow$  3):

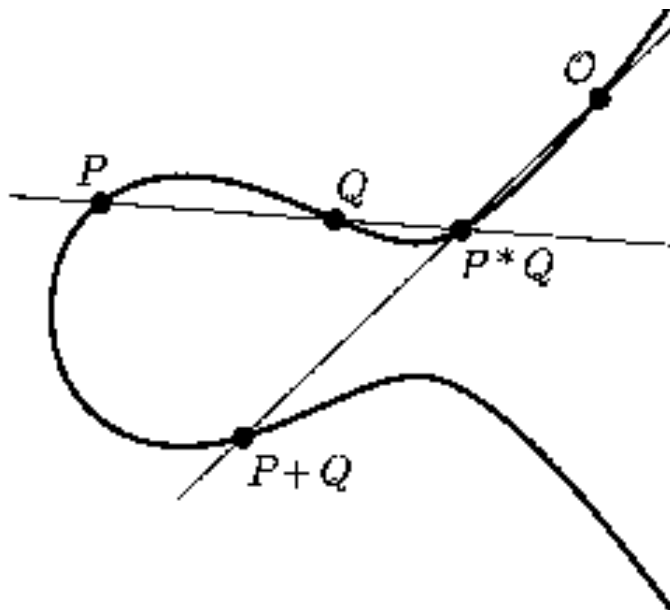
Antag, at kurven ikke er glat. Det betyder per definition, at der eksisterer et  $(x, y)$

$$F(x, y) = y^2 - x^3 - ax^2 - bx - c = y^2 - f(x)$$

$\Downarrow$

$$\frac{\partial F}{\partial x} = -f'(x) = 0 \quad \frac{\partial F}{\partial y} = 2y = 0 \Rightarrow f(x) = 0$$

Det vil sige, at en kurve er glat hvis og kun hvis  $f(x) = 0$  og  $f'(x) = 0$ . Men det er ensbetydende med, at  $x$  er en dobbeltrod, så hvis man forlanger, at rødderne i  $f$



FIGUR 1. Korde-tangent kompositionen

er forskellige, er kurven glat. Det er her vigtigt, at hvis  $f$  ikke har tre rødder i  $k$ , så finder man en udvidelse af  $k$  således at  $f$  har tre rødder, og i det legeme er rødderne forskellige.

3)  $\Leftrightarrow$  4):

Hvis vi kigger på  $f$  i udvidelsen af  $k$ , kan  $f$  faktoriseres til

$$f(x) = (x-x_1)(x-x_2)(x-x_3) = x^3 - (x_1+x_2+x_3)x^2 + (x_1x_2+x_2x_3+x_1x_3)x - x_1x_2x_3,$$

hvor  $x_1, x_2, x_3$  er rødderne i  $f$ . Koefficienterne  $a, b, c$  er så givet ved :

$$a = -(x_1 + x_2 + x_3) \quad b = x_1x_2 + x_2x_3 + x_1x_3 \quad c = -x_1x_2x_3$$

Ved indsættelse af udtrykkene for  $a, b, c$  i ligningen for diskriminanten fås ved hjælp af lidt algebra, at

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

Det ses af det sidste udtryk, at diskriminanten er forskellig fra 0 hvis og kun hvis rødderne i  $f$  er forskellige. □

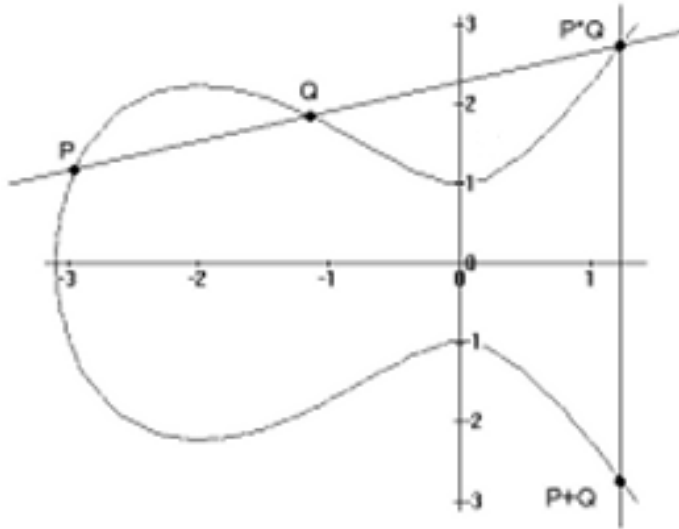
Læg mærke til at det er nødvendigt at vide, at karakteristikken af  $k$  er forskellig fra 2, da man ellers ikke kan konkludere, at  $2y = 0 \Rightarrow y = 0$ .

Når vi ser efter  $k$ -rationelle løsninger til elliptiske kurver er det vigtigt, at man kigger efter løsninger i det projektive plan. Der står lidt om det projektive plan i bilag A. Lad os homogenisere (1.2):

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3 \quad (1.3)$$

Som forklaret i bilag A er de punkter man får ekstra med ved at kigge projektiv dem, der skæres i linien  $Z = 0$ . Ved indsættelse af  $Z = 0$  i (1.3) fås:

$$0 = X^3$$



FIGUR 2. Elliptisk kurve med  $\mathcal{O}$  som neutralelement

Det vil sige, at punktet  $(0:1:0)$  er den eneste løsning til (1.3) (det har multiplicitet 3), der ikke ligger i det affine plan. Dette punkt skal være  $\mathcal{O}$ . Det er klart, at  $\mathcal{O}$  er  $k$ -rationelt.

Det sidste der skal på plads inden kapitlets hovedformål formuleres er begrebet en gruppe.

**Definition 1.3.** En gruppe er en mængde  $G$  med en komposition  $\circ : G \times G \mapsto G$ , hvor kompositionen opfylder:

1) Der er et neutralelement  $e \in G$ , så

$$e \circ s = s \circ e = s$$

for alle  $s \in G$ .

2)  $\forall s \in G \exists s^{-1} \in G$  så

$$s \circ s^{-1} = s^{-1} \circ s = e$$

3) Kompositionen er associativ. D.v.s

$$(s_1 s_2) s_3 = s_1 (s_2 s_3)$$

Formålet med dette kapitel er at bevise følgende sætning:

**Sætning 1.4.** *Lad  $k$  være et dellegeme af  $k'$  med karakteristisk forskellig fra 2 og  $E$  være en elliptisk kurve over  $k$ . Da udgår  $E(k')$  en gruppe med hensyn til kordetangent kompositionen.*

Det er vigtigt her at understrege, at løsningerne skal findes i det projektive plan. Det er vigtigt af to grunde. For det første gælder sætningen ikke, hvis man ikke regner i det projektive rum. For det andet sikrer det, at hvis man har en løsning til den generelle kubiske ligning, er det også en løsning til Weierstrassligningen. Et par spørgsmål hører der til. For det første, kan man være sikker på, at en linie skærer den elliptiske kurve præcis 3 gange? Er man sikker på, at resultatet af kompositionen er et  $k$ -rationelt punkt? Og endelig er der spørgsmålet om gruppestrukturen på  $E$ . Det vil være dette kapitels formål at besvare disse spørgsmål.

**1.2. Korde-tangent kompositionen.** Det første man bør kigge på er, om kompositionen overhovedet er veldefineret. Der er Bezouts sætning utrolig værdifuld. Vi skal blot bruge et specialtilfælde af den, der siger,

**Sætning 1.5** (specialtilfælde af Bezouts sætning). *Givet en kurve  $C$  på formen  $y^2 = x^3 + ax^2 + bx + c$  og en vilkårlig linie  $L$   $\alpha y = \beta x + \gamma$ , hvor koefficienterne til  $C$  og  $L$  er taget fra et algebraisk lukket legeme  $k$ , da skærer  $L$   $C$  præcis 3 gange (talt med multiplicitet) i det projektive plan.*

Der er givet et bevis for sætningen i bilag A.

Vi er nu i stand til at bevise følgende:

**Sætning 1.6.** *Lad  $E$  være en elliptisk kurve over et legeme  $k$ , og  $P_1$  og  $P_2$  være to  $k$ -rationelle punkter på  $E$ . Da vil korde-tangent kompositionen give et  $k$ -rationelt punkt som resultat.*

*Bevis.* For det første bemærkes, at Bezouts sætning giver, at ligegyldigt om  $P_1 = P_2$ , så har linien gennem  $P_1$  og  $P_2$  (evt. tangenten til  $P_1$ ) præcis en ekstra skæring med  $E$ . Det kan selvfølgelig være, at skæringen ligger i  $k' \times k'$ , hvor  $k'$  er en udvidelse af  $k$ . Lad nu  $P_1 = (x_1, y_1)$  og  $P_2 = (x_2, y_2)$ , og antag i første omgang, at  $P_1 \neq \pm P_2$ , hvor  $-P_2 = (x_2, -y_2)$  (det er også et punkt på  $E$ , da  $E$  er symmetrisk i  $x$ -aksen. Det vil snart kunne ses, at  $-P_2$  er  $P_2$ 's inverse element. Linien gennem  $P_1$  og  $P_2$  er nu givet ved udtrykket:

$$y = \alpha x + \beta,$$

hvor

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1}, \quad \beta = y_1 - \alpha x_1 \quad \alpha, \beta \in k.$$

Dette kan indsættes i (1.2).

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

↓

$$f(x) = x^3 + (a - \alpha^2)x^2 + (b - 2\alpha\beta)x + c - \beta^2$$

$f(x)$  kan betragtes som et element i  $k[X]$ , der er mængden af polynomier med koefficienter fra  $k$ . Da legemet  $k$  ikke nødvendigvis er algebraisk lukket, behøver  $f$  umiddelbart ikke at kunne skrives som et produkt af 1.grads polynomier, men siden  $f$  har to rødder nemlig  $x_1$  og  $x_2$ , må  $f$  kunne faktoriseres ud til:

$$f = (x - x_1)(x - x_2)(x - x_3)$$

$f$  har altså en 3. rod  $x_3 \in k$  og punktet  $P_1 * P_2 = (x_3, y_3)$ , hvor  $y_3 = \alpha x_3 + \beta \in k$  ligger på kurven. Læg mærke til, man ikke behøver, at  $k$  er algebraisk lukket, fordi man kender to løsninger, nemlig  $x_1$  og  $x_2$ . Hvis  $P_1 = P_2$  skal man ifølge korde-tangent kompositionen sætte  $\alpha$  lig med hældningen i punktet  $P_1$ . Da kurven per definition er glat, kan det altid lade sig gøre. Ligesom før ender man med en 3.grads ligning, hvor man kender to løsninger ( $x_1$  er dobbeltrod). Den sidste er så  $x$ -koordinaten til den 3. skæring. Er  $P_1 = -P_2$  er  $P_1 * P_2 = \mathcal{O}$ . Når man har fundet den 3. skæring, skal man finde resultatet af kompositionen ved at tage linien gennem  $\mathcal{O}$  og  $P_1 * P_2$ . At dette resultat bliver et  $k$ -rationelt punkt følger af ovenstående. Læg mærke til, hvis man vil fordoble et punkt på formen  $2(x, 0) = (x, 0) + (x, 0)$  er hældningen ikke defineret. Men da er punktet sit eget invers element ( $-(x, 0) = (x, -0) = (x, 0)$ ), og problemet er behandlet.

□

1.3. **Additionsformler.** Det første vi vil vise, er at  $\mathcal{O}$  er neutralelement.

**Sætning 1.7.** Hvis  $G$  er gruppen af  $k$ -rationelle punkter på en elliptisk kurve  $E$ , er  $\mathcal{O}$  gruppens neutralelement, og hvis  $P = (x, y)$  er  $(x, -y)$   $P$ 's inverse element.

*Bevis.* Lad  $P = (x, y) = (x : y : 1)$ . Hvis man skal addere  $P$  med  $\mathcal{O}$  skal man ifølge korde-tangent kompositionen finde linien gennem de to punkter. Den er givet ved den homogene ligning:

$$X = xZ$$

Indsættes den i (1.3) fås:

$$Y^2 Z = x^3 Z^3 + ax^2 Z^3 + bxZ^3 + cZ^3$$

Man kan tjekke, at de tre punkter  $(x : \pm y : 1)$  og  $(0 : 1 : 0)$  er løsninger. Bezout fortæller så, at de er de eneste løsninger. Det giver, at  $P * \mathcal{O} = (x : -y : 1)$ . Nu skal man tage linien gennem  $P * \mathcal{O}$  og  $\mathcal{O}$ , men det giver jo en ligning som den ovenstående, og resultatet er  $P + \mathcal{O} = P$ . Et lignende argument giver, at  $-P = (x, -y)$ .  $\square$

Vi vil nu udregne additionsformlerne for korde-tangent kompositionen. Lad  $P = (x_1, y_1)$  og  $Q = (x_2, y_2)$  være givet, og lad  $P \neq \pm Q$ . Linien gennem  $P$  og  $Q$  vil da være givet ved ligningen:

$$y = \alpha x + \beta, \quad \text{hvor} \quad \alpha = \frac{y_2 - y_1}{x_2 - x_1} \quad \text{og} \quad \beta = y_1 - \alpha x_1$$

Liniens ligning indsættes i (1.2)

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

$\Downarrow$

$$x^3 + (a - \alpha^2)x^2 + (b - 2\alpha\beta)x + c - \beta^2$$

Men det er også lig med

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

,hvor  $x_1, x_2, x_3$  er de tre rødder. Men hvis de to polynomier skal være ens, må koefficienterne være ens. Specielt må koefficienten foran andengradsleddet være det, og det giver den ukendte  $x_3$ .

$$a - \alpha^2 = -(x_1 + x_2 + x_3)$$

$\Downarrow$

$$x_3 = \alpha^2 - a - x_1 - x_2 \tag{1.4}$$

Og ved indsættelse i liniens ligningen fås

$$y_3 = -(\alpha x_3 + \beta) \tag{1.5}$$

Er  $P = -Q$  er resultatet åbenlyst  $\mathcal{O}$ , så det er kun  $P + P$ , der skal beregnes. Som nævnt ovenfor skal man så have fat i den afledede i punktet  $P$ . Implicit differentiation giver, at hældningen er givet ved

$$\alpha = \frac{f'(x_1)}{2y_1}$$

Det kan tjekkes, at det er hældningen på sædvanligvis ved at kigge på de to funktioner  $g_1(x) = \sqrt{f(x)}$  og  $g_2(x) = -\sqrt{f(x)}$  og deres afledede.

$$g_1'(x) = \frac{3x^2 + 2ax + b}{2\sqrt{x^3 + ax^2 + bx + c}} = \frac{f'(x)}{2g_1}$$

$$g_2'(x) = \frac{3x^2 + 2ax + b}{-2\sqrt{x^3 + ax^2 + bx + c}} = \frac{f'(x)}{2g_2}$$

Der er så en formel for tangentlinien, med  $\alpha = \frac{f'(x)}{2y}$  og  $\beta = y - \alpha x$ , der kan indsættes i de ovenstående formler. Det er vigtigt her, at  $k$  ikke har karakteristisk 2, da  $2y$  vil give 0 selvom  $y \neq 0$ . Er  $y = 0$  er hældningen ikke defineret, men da  $(x, 0) = (x, -0)$  er punktet sit eget inverse element, og resultatet af  $P + P$  er  $\mathcal{O}$ . For denne fordobling af  $P$  kan det være nyttigt, at udregne  $x_3$  som funktion af  $x_1$ . Dette gøres nemt ved brug af (1.4) og (1.2).

$$\begin{aligned} x_3 &= \alpha^2 - a - 2x_1 \\ &= \left(\frac{f'(x_1)}{2y_1}\right)^2 - a - 2x_1 \\ &= \frac{(3x_1^2 + 2ax_1 + b)^2 - (a + 2x_1)4(x_1^3 + ax_1^2 + bx_1 + c)}{4(x_1^3 + ax_1^2 + bx_1 + c)} \\ &= \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4(x_1^3 + ax_1^2 + bx_1 + c)} \end{aligned} \quad (1.6)$$

1.4. **Associativiteten.** 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

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

Notationen er

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

Benytter vi resultaterne fra (1.4) og (1.5), finder vi

$$\begin{aligned} (P_1 + P_2)_x &= m^2 - a - x_1 - x_2 \\ (P_1 + P_2)_y &= -m(m^2 - a - x_1 - x_2) - y_2 + mx_2 \end{aligned}$$

samt

$$\begin{aligned} \{(P_1 + P_2) + P_3\}_x &= n^2 - a - x_3 - (P_1 + P_2)_x \\ &= n^2 - a - x_3 - (m^2 - a - x_1 - x_2) \\ &= n^2 - m^2 + x_1 + x_2 - x_3 \end{aligned} \quad (1.7)$$

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

$$\begin{aligned} (P_2 + P_3)_x &= q^2 - a - x_2 - x_3 \\ (P_2 + P_3)_y &= -q(q^2 - a - x_2 - x_3) - y_2 + qx_2 \\ \{P_1 + (P_2 + P_3)\}_x &= u^2 - a - x_1 - (P_2 + P_3)_x \\ &= u^2 - a - x_1 - (q^2 - a - x_2 - x_3) \\ &= u^2 - q^2 + x_2 + x_3 - x_1 \end{aligned} \quad (1.8)$$

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

Vi skal nu undersøge om (1.7) stemmer overens med (1.8). Da  $m, n, u, q$  alle afhænger af valget af punkter, er der flere tilfælde at tjekke. Vi vil se på det mest generelle tilfælde, hvor

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

↓

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

$$q = \frac{y_3 - y_2}{x_3 - x_2}$$

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

og tilsvarende

$$u = \frac{y_1 + q(q^2 - a - x_2 - x_3) + y_2 - qx_2}{a - q^2 + x_1 + x_2 + x_3}$$

Vi skal tjekke, at (1.7), (1.8) stemmer overens - dvs.

$$n^2 - m^2 + x_1 + x_2 - x_3 = u^2 - q^2 + x_2 + x_3 - x_1$$

⇔

$$n^2 - m^2 + q^2 - u^2 + 2(x_1 - x_3) = 0 \quad (1.9)$$

For  $y$ -koordinaten får vi

$$\{P_1 + (P_2 + P_3)\}_y = -(u\{P_1 + (P_2 + P_3)\}_x + y_1 - ux_1) \quad (1.10)$$

$$\{(P_1 + P_2) + P_3\}_y = -(n\{(P_1 + P_2) + P_3\}_x + y_3 - nx_3) \quad (1.11)$$

Vi lader nu MAPLE regne på venstre side af (1.9) givet udtrykkene for  $m, n, u, q$ . Endvidere benytter vi, at  $P_1, P_2, P_3 \in E$  - dvs.  $y_i^2 = x_i^3 + ax_i^2 + bx_i + c$  for  $i=1,2,3$ . Vi ser, at (1.7), (1.8) stemmer overens. Dette benyttes til sammenligning af de to  $y$ -koordinater. Vi lader MAPLE regne 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, hvilket betyder (1.10), (1.11) er ens.

Man kan på tilsvarende måde vise associativiteten i de andre tilfælde - det vil dog ikke blive gjort.

```

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

```

FIGUR 3. Maples udregninger

1.5. **Gruppestrukturen.** Der er i dette kapitel gjort rede for, at de  $k$ -rationelle punkter ( $G$ ) på den elliptiske kurve over legemet  $k'$ , hvor  $k'$  sidder inde i  $k$ , udgør en gruppe m.h.t korde-tangent kompositionen D.v.s følgende er opfyldt:

- 1) Korde-tangent kompositionen fører  $G \times G \mapsto G$
- 2)  $\mathcal{O}$  er et neutral element.
- 3) Der eksisterer et inverst element.
- 4) Kompositionen er associativ.

Det betyder altså, at sætning 1.4 er bevist.

## 2. ELLIPTISKE KURVER OVER ENDELIGE LEGEMER OG HASSES SÆTNING

**2.1. Introduktion.** Det vil være dette kapitels formål, at undersøge, hvad der kan siges om antallet af punkter på en elliptisk kurve over legemet  $\mathbb{Z}/p\mathbb{Z}$ . Hvis vi har en elliptisk kurve  $E$ , med heltallige koefficienter, vil vi i det følgende snakke om  $E$ 's reducering modulo  $p$ . Det vil være kurven beskrevet ved ligningen, hvor man tager  $E$ 's koefficienter, og reducerer dem modulo  $p$ .

**Sætning 2.1.** *Lad  $E$  være en elliptisk kurve med heltallige koefficienter, og lad  $p \neq 2$  være et primtal. Da er reduceringen af  $E$  modulo  $p$  en elliptisk kurve over  $\mathbb{Z}/p\mathbb{Z}$ , hvis og kun hvis  $p \nmid D$ . Reduceringen af  $E$  betegnes med  $E_p$*

*Bevis.* Da  $D \neq 0$  fås af regnereglerne for restklasser, at  $E_p$ 's determinant  $D_p$  er lig med  $D$  mod  $p$ , men det medfører, at  $D_p \neq 0$  hvis og kun hvis  $p \nmid D$ , eller  $E_p$  er en elliptisk kurve over  $\mathbb{Z}/p\mathbb{Z}$  hvis og kun hvis  $p \nmid D$   $\square$

Spørgsmålet er nu, hvad man kan sige om antallet af punkter på  $E_p$ . For at give et kvalitativt svar på det, lønner det sig, at se på ligningen

$$y^2 = x \quad x, y \in \mathbb{Z}/p\mathbb{Z} \quad (2.1)$$

Lader man  $y$  løbe igennem  $\mathbb{Z}/p\mathbb{Z}$  fås, at der er  $p$  affine løsninger til (2.1). Udover dem er der også en projektiv; d.v.s ialt  $p + 1$  løsninger. Man har også, at hvis  $(x, y)$  er en løsning, så er  $(x, -y)$  også en løsning. Det betyder, at kun halvdelen af elementerne fra  $x \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$  har en kvadratrod, eller sagt på en anden måde:  $x$  har 50% chance for at have en kvadratrod, og hvis den har en, så har den også to. Forestiller man sig, at  $x$  løber igennem  $\mathbb{Z}/p\mathbb{Z}$ , og værdierne til  $f(x)$  fra (1.2) er tilfældige, vil  $f(x)$  ca. halvdelen af gangene ramme et  $x$ , der har en kvadratrod. Det svarer til 2 løsninger til (2.1), og der vil være ca.  $p + 1$  løsninger til  $E_p$  (husk den projektive). Det er selvfølgelig et meget flyvsk argument, og man må selvfølgelig regne med et slør. Men det viser sig, at resultatet ikke er helt forkert, da der gælder følgende sætning.

**Sætning 2.2** (Hasses sætning). *Lad  $E$  være en elliptisk kurve over  $\mathbb{Q}$  med heltallige koefficienter, og lad  $p \neq 2$  være et primtal, der ikke deler determinanten  $D$ . Da er  $E_p$  en elliptiske kurve, og*

$$|p + 1 - \sharp E_p(\mathbb{Z}/p\mathbb{Z})| \leq 2\sqrt{p},$$

hvor  $\sharp E_p(\mathbb{Z}/p\mathbb{Z})$  betegner antallet af  $\mathbb{Z}/p\mathbb{Z}$ -rationelle punkter på  $E_p$ .

I beviset for Hasses sætning, vil vi i stedet for at arbejde med den normale Weierstrassligning, arbejde med ligninger af typen:

$$y^2 = x^3 + ax + b \quad (2.2)$$

Så inden vi går i gang med beviset vil vi vise, at en ligning på Weierstrassform kan komme på formen (2.2) ved koordinatskift.

**Sætning 2.3.** *En elliptisk kurve  $E_p$  over legemet  $\mathbb{Z}/p\mathbb{Z}$  kan ved hjælp af rationelle manipulationer komme på formen (2.2), hvis  $p \neq 3$ . Den nye kurve,  $E'_p$  vil også være en elliptisk kurve over  $\mathbb{Z}/p\mathbb{Z}$ , og  $\sharp E_p(\mathbb{Z}/p\mathbb{Z}) = \sharp E'_p(\mathbb{Z}/p\mathbb{Z})$ .*

*Bevis.* Lad  $E_p$  være en elliptisk kurve over  $\mathbb{Z}/p\mathbb{Z}$ . Vi vil bruge koordinatskiftet  $x = x' - \frac{a}{3}$ .

$$y^2 = x^3 + ax^2 + bx + c = (x' - \frac{a}{3})^3 + a(x' - \frac{a}{3})^2 + b(x' - \frac{a}{3}) + c$$

$$\begin{aligned}
&= x'^3 - ax'^2 + \frac{a^2}{3}x' - \frac{a^3}{3^3} + ax'^2 - 2\frac{a^2}{3}x' + \frac{a^3}{3^2} + bx' - b\frac{a}{3} + c \\
&= x'^3 + (b - \frac{a^2}{3})x' + (\frac{a^3}{3^2} - \frac{a^3}{3^3} - b\frac{a}{3} + c),
\end{aligned}$$

som er på formen (2.2). Endvidere ses det, at har man en løsning til  $E_p$  kan man blot løse ligningen  $x = x' - \frac{a}{3}$ , og så har man en løsning til  $E'_p$ , og omvendt. Det betyder, at der er lige mange løsninger til de to kurver. Endvidere er diskriminanten af  $E'_p$

$$\begin{aligned}
D_{E'_p} &= -4(b - \frac{a^2}{3})^3 - 27(\frac{a^3}{3^2} - \frac{a^3}{3^3} - b\frac{a}{3} + c) \\
&= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = D_{E_p} \neq 0,
\end{aligned}$$

og det fortæller, at  $E'_p$  er en elliptisk kurve.  $\square$

**2.2. Bevis for Hasse's sætning.** Vi er nu parate til at kunne give et bevis for Hasses sætning. Dette bevis blev først givet af Manin i 1956 (se [7]), men dette afsnit bygger på [4] s.297-301. Dog beviser Knapp ikke ligning (2.13), men det er bevist i [5] s.230-231.

*Bevis, Hasses sætning.* Først ses på tilfældet  $p = 3$ . For hver  $x$ -værdi er der maksimalt 2 løsninger til  $E_p$ , da  $\mathbb{Z}/p\mathbb{Z}$  er et legeme, og i et legeme har et element maksimalt 2 kvadratrødder. D.v.s, at der ikke er mere end  $2 \cdot 3 + 1 = 7$  punkter på  $E_p$  og minimalt 1 (husk  $\mathcal{O}$ ). Endvidere er  $2\sqrt{3} = 3, 46\dots$ , hvilket beviser sætningen i tilfældet  $p = 3$ . Er  $p > 3$  kan man ifølge sætning 2.3 lave et koordinatskift, der bringer  $E_p$  på formen:

$$y^2 = x^3 + ax + b \quad (2.3)$$

Dette koordinatskift ændrer ikke på antallet af punkter på  $E_p$  eller på det faktum, at  $E_p$  er en elliptisk kurve. Det er derfor nok, at vise Hasses sætning for elliptiske kurver på formen (2.3). Vi skal i dette bevis arbejde med en elliptisk kurve defineret over legemet af polynomiumsbrøker. D.v.s legemet bestående af elementer  $\frac{f}{g}$ , hvor  $f, g \in \mathbb{Z}/p\mathbb{Z}[X]$ . Legemet bestående af polynomiumsbrøker betegnes med  $\mathbb{Z}/p\mathbb{Z}(X)$ . Kurven vil have formen:

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b}, \quad (2.4)$$

hvor  $X, Y, x^3 + ax + b \in \mathbb{Z}/p\mathbb{Z}(X)$ . Notationen vil være, at polynomiumsbrøker betegnes med store bogstaver. Dette er imidlertid ikke en kurve på Weierstrassform, men beregninger lignende dem fra kap.1 viser, at der også er en gruppestruktur på elliptiske kurver på formen

$$\gamma y^2 = x^3 + ax^2 + bx + c = f(x) \quad (2.5)$$

Det eneste resultat vi skal bruge, er at nu ser additionsformlen for  $x$ -koordinaten således ud:

$$x_3 = \gamma\alpha^2 - a - x_2 - x_1, \quad \alpha = \frac{y_2 - y_1}{x_2 - x_1} \quad (2.6)$$

og fordoblingsformlen ser således ud.

$$x_3 = \gamma\alpha^2 - a - 2x_1, \quad \alpha = \frac{f'(x_1)}{\gamma 2y_1} \quad (2.7)$$

Det ses, at de 2 punkter,  $(x, 1)$  og  $(x^p, (x^3 + ax + b)^{\frac{1}{2}(p-1)})$ , ligger på (2.4) da:

$$1^2 = \frac{x^3 + ax + b}{x^3 + ax + b}$$

og

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

hvor der blev brugt at i ringe med karakteristisk  $p$  gælder  $(x + y)^p = x^p + y^p$  se [3] s.107. Ud fra disse punkter kan man nu danne en mængde af punkter:

$$Z_n = (X_n, Y_n) = (x^p, (x^3 + ax + b)^{\frac{1}{2}(p-1)} + n(x, 1)), \quad -\infty < n < \infty \quad (2.8)$$

Hvor det selvfølgelig er korde-tangent kompositionen, der bruges som addition. Endvidere vil vi med  $f_n$  og  $g_n$  benævne de to polynomier, der opfylder at  $X_n = \frac{f_n}{g_n}$  og at  $X_n$  er reduceret mest muligt. D.v.s, at  $\text{sfd}(f_n, g_n) = 1$ . For hvert punkt defineres desuden en talfølge  $d_n$ . Hvis  $Z_n = \mathcal{O}$  er  $d_n = 0$ , ellers er  $d_n = \max(\text{grad}(f_n, g_n))$ . Vi vil udføre beviset ved hjælp af en række lemmaer, der tilsammen beviser Hasses sætning.

**Lemma 2.4.**

$$d_{-1} - d_0 - 1 = \sharp E_p(\mathbb{Z}/p\mathbb{Z}) - p - 1,$$

hvor  $\sharp E_p(\mathbb{Z}/p\mathbb{Z})$  betegner antallet af punkter på  $E_p$

*Bevis.* Det er klart, at  $d_0 = p$ . D.v.s, at lemmaet er opfyldt hvis  $d_{-1} = \sharp E_p(\mathbb{Z}/p\mathbb{Z})$ .  $X_{-1}$  kan beregnes ud fra (2.6):

$$X_{-1} = -x - x^p + \frac{[1 + (x^3 + ax + b)^{\frac{1}{2}(p-1)}]^2 [x^3 + ax + b]}{(x - x^p)^2} \quad (2.9)$$

Sætter man på fælles brøkstreg og ganger  $(x^3 + ax + b)$ -leddet ind får man:

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

Hvor der igen er brugt, at  $(x + y)^p = x^p + y^p$ . Det ses, at de to  $x^{3p}$ -led går ud med hinanden, og det næsthøjeste led bliver  $x^{2p+1}$ , der ikke går ud med noget. Tælleren er altså en grad højere end nævneren, også efter evt. reduceringer af  $X_{-1}$ . Spørgsmålet er så hvilken grad nævneren har, når  $X_{-1}$  er reduceret mest muligt. Til det skal man bruge nogle resultater fra talteori om kvadratiske rester. Man kan læse lidt om kvadratiske rester i bilaget. Hvis man reducerer brøkdudtrykket i (2.9), da vil udtrykket der fremkommer ved at sætte på fælles brøkstreg også være reduceret. Det følger af, at hvis  $\frac{a}{b}$  er uforkortelig, da er  $\frac{a+bc}{b}$  også uforkortelig. Derfor er det nok at reducere i brøkdudtrykket. Da  $(x - x^p) = \prod_{j \in \mathbb{Z}/p\mathbb{Z}} (x - j)$  (se [3] s.94) får man, at nævneren i (2.9) faktoriseres til  $\prod_{j \in \mathbb{Z}/p\mathbb{Z}} (x - j)^2$ . Spørgsmålet er nu hvor meget nævneren kan forkortes?  $(x - j)$  er faktor i tælleren i (2.9) hvis og kun hvis tælleren giver 0 ved indsættelse af  $j$ . Men det at tælleren giver 0 kan beskrives ved kvadratisk rest på følgende måde. Ifølge (A.2) giver  $[1 + (j^3 x a j + b)^{\frac{1}{2}(p-1)}]^2$  leddet nul hvis og kun hvis  $(\frac{j^3 + a j + b}{p})_L = -1$ , og  $(x - j)$  vil være faktor i  $1 + (j^3 x a j + b)^{\frac{1}{2}(p-1)}$ . Men det må betyde, at  $(x - j)$  er faktor 2 gange i tælleren, da leddet jo indgår i anden.  $(j^3 + a j + b)$ -leddet giver nul hvis og kun hvis  $(\frac{j^3 + a j + b}{p})_L = 0$ , og  $(x - j)$  er faktor i tælleren præcis en gang. Hvis den var faktor mere en en gang, ville  $f(x) = x^3 + ax + b$  have en dobbeltrod i modstrid med, at  $y = f(x)$  er en elliptisk kurve. D.v.s, at de

faktorer der er tilbage i nævneren er  $(x - j)^2$  hvis  $(\frac{j^3+aj+b}{p})_L = 1$  og  $(x - j)$  hvis  $(\frac{j^3+aj+b}{p})_L = 0$ . Men det er jo præcis antallet af affine løsninger til (2.3). Husker man at tælleren er en grad større end nævneren fås, at  $d_{-1} = \sharp E_p(\mathbb{Z}/p\mathbb{Z})$ , og lemmaet er bevist.  $\square$

Det næste lemma giver en rekursionsfølge for  $d_n$ . Det siger:

**Lemma 2.5.** *For alle  $n$  gælder at  $d_{n-1} + d_{n+1} = 2d_n + 2$*

*Bevis.* Antag i første omgang, at en af  $Z_{n-1}, Z_n, Z_{n+1}$  er  $\mathcal{O}$ . Da kan de to andre ikke være  $\mathcal{O}$ . Er f. eks  $Z_{n+1} = \mathcal{O}$ , er  $Z_n = -(x, 1) \neq \mathcal{O}$  og  $Z_{n-1} = -2(x, 1) \neq \mathcal{O}$ . Hvis ikke  $Z_{n-1} \neq \mathcal{O}$  ville  $(x, 1)$  være sit eget inverse. Eller  $(x, 1) = -(x, 1) = (x, -1)$ , hvilket vil være i modstrid med at vi arbejder i et legeme med karakteristisk forskellig fra 2. Lad  $Z_n = \mathcal{O}$ . Da er

$$Z_{n\pm 1} = (x, \pm 1) \Rightarrow d_{n\pm 1} = 1$$

hvilket opfylder (2.5). Er det derimod  $Z_{n+1}$  der er  $\mathcal{O}$ , bliver  $Z_n = (x, -1)$  og (2.7) giver

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

Endvidere er brøken uforkortelig. Antag nemlig det modsatte. Da er der en fælles faktor i tæller og nævner. Det vil sige, at for et element,  $x_1$ , giver både tæller og nævner 0. Da

$$X_{n-1} = \frac{(3x^2 + a)^2 + 8x(x^3 + ax + b)}{4(x^3 + ax + b)}$$

fås at  $x_1$  er rod i både  $f(x) = x^3 + ax + b$  og  $f'(x) = 3x^2 + a$  svarende til, at  $x_1$  er dobbeltrod, hvilket giver en modstrid med, at  $y^2 = f(x)$  er en elliptisk kurve. Resultatet bliver, at

$$d_{n-1} = 4 \quad d_n = 1 \quad d_{n+1} = 0,$$

der også opfylder (2.5). Ligeledes for  $Z_{n-1} = \mathcal{O}$ . Vi kan derfor nu antage, at hverken  $Z_{n-1}, Z_n, Z_{n+1}$  er  $\mathcal{O}$ . Da kan vi skrive:

$$X_{n-1} = \frac{f_{n-1}}{g_{n-1}}, \quad X_n = \frac{f_n}{g_n}, \quad X_{n+1} = \frac{f_{n+1}}{g_{n+1}},$$

hvor  $f, g$  er på lavest form. Men  $X_{n-1}$  og  $X_{n+1}$  kan også udtrykkes ved hjælp af (2.6). Det giver:

$$\begin{aligned} X_{n-1} &= \frac{(x^3 + ax + b)(1 + Y_n)^2}{\left(\frac{f_n}{g_n} - x\right)^2} - x - \frac{f_n}{g_n} \\ &= \frac{g_n^3(x^3 + ax + b)(1 + Y_n)^2 - ((xg_n - f_n)^2(xg_n + f_n))}{g_n(xg_n - f_n)^2} \end{aligned}$$

og

$$\begin{aligned} X_{n+1} &= \frac{(x^3 + ax + b)(1 - Y_n)^2}{\left(\frac{f_n}{g_n} - x\right)^2} - x - \frac{f_n}{g_n} \\ &= \frac{g_n^3(x^3 + ax + b)(1 - Y_n)^2 - ((xg_n - f_n)^2(xg_n + f_n))}{g_n(xg_n - f_n)^2} \end{aligned} \tag{2.10}$$

Lægges de to udtryk fra (2.10) sammen fås:

$$\begin{aligned} \frac{1}{2}(X_{n-1} + X_{n+1}) &= \frac{(x^3 + ax + b)g_n^3 + Y_n g_n^3 - (g_n x + f_n)(g_n x - f_n)^2}{g_n(g_n x - f_n)^2} \\ &= \frac{(x^3 + ax + b)g_n^3 + \left(\left(\frac{f_n}{g_n}\right)^3 + a\frac{f_n}{g_n} + b\right)g_n^3 - (g_n^2 x^2 - f_n^2)(g_n x - f_n)}{g_n(g_n x - f_n)^2}, \end{aligned}$$

hvor der er brugt, at  $Y^2 = f(X)$ .

$$\frac{1}{2}(X_{n-1} + X_{n+1}) = \frac{f_n g_n x^2 + f_n^2 x + a x g_n^2 + 2b g_n^2 + a f_n g_n}{(g_n x - f_n)^2} \quad (2.11)$$

Ganger man de to ligninger fra (2.10) sammen får man efter et par reduceringer.

$$X_{n-1} X_{n+1} = \frac{f_{n-1} f_{n+1}}{g_{n-1} g_{n+1}} = \frac{(f_n x - a g_n)^2 - 4b g_n (g_n x + f_n)}{(g_n x - f_n)^2} \quad (2.12)$$

Lad os nu antage (det vil senere blive bevist), at

$$(x g_n - f_n)^2 \mid g_{n-1} g_{n+1} \quad (2.13)$$

Da må der eksistere et polynomium  $S$  således at

$$f_{n-1} f_{n+1} = S((f_n x - a g_n)^2 - 4b g_n (g_n x + f_n))$$

og

$$g_{n-1} g_{n+1} = S(g_n x - f_n)^2 \quad (2.14)$$

Endvidere fås af (2.11) og (2.14).

$$\begin{aligned} f_{n-1} g_{n+1} + g_{n-1} f_{n+1} &= g_{n-1} g_{n+1} (X_{n-1} + X_{n+1}) \\ &= 2S(f_n g_n x^2 + f_n^2 x + a x g_n^2 + 2b g_n^2 + a f_n g_n) \end{aligned} \quad (2.15)$$

Lad nu  $F$  være et primelement i  $S$ . Da fås af (2.14) at  $F \mid g_{n-1} g_{n+1}$ . Da  $F$  er et primelement deler  $F$  enten  $g_{n-1}$  eller  $g_{n+1}$ . Vi antager at  $F \mid g_{n-1}$  ( $F \mid g_{n+1}$  forløber tilsvarende). Da  $\text{sfd}(f_{n-1}, g_{n-1}) = 1$  kan  $F$  ikke gå op i  $f_{n-1}$ . Det må så betyde at  $F \mid f_{n+1}$  da  $F \mid f_{n-1} f_{n+1}$ . Men ifølge (2.15)

$$F \mid f_{n-1} g_{n+1} + g_{n-1} f_{n+1} \Rightarrow F \mid g_{n+1}$$

Det giver en modstrid, da  $\text{sfd}(f_{n+1}, g_{n+1}) = 1$ . Det betyder, at  $S$  er en skalar og (2.14) giver at

$$\text{grad}(f_{n-1} f_{n+1}) = \text{grad}((f_n x - a g_n)^2 - 4b g_n (g_n x + f_n))$$

og

$$\text{grad}(g_{n-1} g_{n+1}) = \text{grad}((g_n x - f_n)^2). \quad (2.16)$$

Ifølge definitionen af  $d_n$  får vi følgende værdier:

$$d_{n-1} = \max\{\text{grad}(f_{n-1}), \text{grad}(g_{n-1})\}$$

$$d_n = \max\{\text{grad}(f_n), \text{grad}(g_n)\}$$

$$d_{n+1} = \max\{\text{grad}(f_{n+1}), \text{grad}(g_{n+1})\}$$

Man kan nu forestille sig 4 situationer:

(a)  $d_{n-1} = \text{grad}(f_{n-1})$  og  $d_{n+1} = \text{grad}(f_{n+1})$

(b)  $d_{n-1} = \text{grad}(g_{n-1})$  og  $d_{n+1} = \text{grad}(g_{n+1})$

(c)  $d_{n-1} = \text{grad}(f_{n-1}) > \text{grad}(g_{n-1})$  og  $d_{n+1} = \text{grad}(g_{n+1}) > \text{grad}(f_{n+1})$

(d)  $d_{n-1} = \text{grad}(g_{n-1}) > \text{grad}(f_{n-1})$  og  $d_{n+1} = \text{grad}(f_{n+1}) > \text{grad}(g_{n+1})$

Vi beviser lemma 2.5 i de 4 tilfælde:

Tilfælde (a):

Vi har fra (2.16) at

$$d_{n-1} + d_{n+1} = \text{grad}(f_{n-1}f_{n+1}) = \text{grad}((f_n x - ag_n)^2 - 4bg_n(g_n x + f_n)).$$

Hvis  $\text{grad}(f_n) \geq \text{grad}(g_n)$  så er

$$\text{grad}((f_n x - ag_n)^2 - 4bg_n(g_n x + f_n)) = \text{grad}(f_n^2 x^2) = 2\text{grad}(f_n) + \text{grad}(x^2) = 2d_n + 2,$$

der opfylder lemma 2.5. Er  $\text{grad}(f_n) < \text{grad}(g_n)$  får vi fra (2.16), at  $\text{grad}(g_{n-1}g_{n+1}) = 2\text{grad}(g_n) + 2$ . Men helt generelt giver (2.16) at :

$$\text{grad}(f_{n-1}f_{n+1}) \leq \max\{2\text{grad}(f_n) + 2, 2\text{grad}(g_n) + 1, \text{grad}(f_n) + \text{grad}(g_n)\}$$

Ifølge antagelsen om at  $\text{grad}(f_n) < \text{grad}(g_n)$  fås, at

$$\text{grad}(f_{n-1}f_{n+1}) \leq 2\text{grad}(g_n) + 1 < 2\text{grad}(g_n) + 2 = \text{grad}(g_{n-1}g_{n+1})$$

Det giver en modstrid, da (a) skal være opfyldt.

Tilfælde (b):

Vi har igen fra (2.16), at

$$d_{n-1} + d_{n+1} = \text{grad}((g_n x - f_n)^2)$$

Hvis  $\text{grad}(g_n) \geq \text{grad}(f_n)$  fås, at lemma 2.5 er opfyldt da

$$d_{n-1} + d_{n+1} = 2\text{grad}(g_n) + 2 = 2d_n + 2$$

Omvendt er  $\text{grad}(g_n) < \text{grad}(f_n)$  får vi fra (2.16), at

$$\text{grad}(f_{n-1}f_{n+1}) = \text{grad}(f_n^2 x^2) > \text{grad}(f_n^2) \geq \text{grad}(g_{n-1}g_{n+1}),$$

hvilket er i modstrid med (b).

Tilfælde (c)

Vi har nu, at :

$$\text{grad}(f_{n-1}g_{n+1}) > \text{grad}(f_{n-1}f_{n+1}) \quad (2.17)$$

$$\text{grad}(f_{n-1}g_{n+1}) > \text{grad}(g_{n-1}g_{n+1}) \quad (2.18)$$

$$\text{grad}(f_{n-1}g_{n+1}) > \text{grad}(g_{n-1}f_{n+1}) \quad (2.19)$$

(2.19) giver nu, at

$$\text{grad}(f_{n-1}g_{n+1}) = \text{grad}(f_{n-1}g_{n+1} + g_{n-1}f_{n+1})$$

og sammen med (2.15) giver:

$$\text{grad}(f_{n-1}g_{n+1}) = \text{grad}(f_n g_n x^2 + f_n^2 x + axg_n^2 + 2bg_n^2 + af_n g_n) \quad (2.20)$$

Hvis  $\text{grad}(f_n) \geq \text{grad}(g_n)$  får vi fra (2.14) og (2.20) at

$$\text{grad}(f_{n-1}g_{n+1}) \leq \text{grad}(f_n^2 x^2) = \text{grad}(f_{n-1}f_{n+1})$$

Det giver en modstrid med (2.17). Har vi derimod, at  $\text{grad}(f_n) < \text{grad}(g_n)$  får vi igen fra en modstrid da vi fra (2.14) og (2.20) har:

$$\text{grad}(f_{n-1}g_{n+1}) \leq \text{grad}(g_n^2 x^2) = \text{grad}(g_{n-1}g_{n+1}),$$

hvilket er i modstrid med (2.18). Tilfældet (d) vil blive udeladt, da det er magen til (c).

Vi mangler stadig at bevise (2.13). først vil vi skrive lidt om på ligningerne (2.10) og (2.12).

$$X_{n-1} = \frac{(xg_n + f_n)(xf_n + ag_n) + 2bg_n^2 + 2Y_n(x^3 + ax + b)g_n^2}{(xg_n - f_n)^2} = \frac{R}{(xg_n - f_n)^2} \quad (2.21)$$

$$X_{n+1} = \frac{(xg_n + f_n)(xf_n + ag_n) + 2bg_n^2 - 2Y_n(x^3 + ax + b)g_n^2}{(xg_n - f_n)^2} = \frac{S}{(xg_n - f_n)^2} \quad (2.22)$$

$$X_{n-1}X_{n+1} = \frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{(f_nx - ag_n)^2 - 4bg_n(g_nx + f_n)}{(g_nx - f_n)^2} = \frac{T}{(xg_n - f_n)^2} \quad (2.23)$$

Læg mærke til, at  $R, S, T$  alle er polynomier.  $T$  er klart et polynomium. Problemet med  $S$  og  $R$  er  $Y_n(x^3 + ax + b)g_n^2$ -leddet. Men da

$$\begin{aligned} Y_n^2(x^3 + ax + b)^2g_n^4 &= (X^3 + aX + b)(x^3 + ax + b)g_n^4 \\ &= \left(\left(\frac{f_n}{g_n}\right)^3 + a\left(\frac{f_n}{g_n}\right) + b\right)(x^3 + ax + b)g_n^4 \end{aligned}$$

er et polynomium, må  $Y_n(x^3 + ax + b)g_n^2$  også være det. Det følger af, at hvis  $(\frac{a}{b})^2$  er et helt tal, så er  $\frac{a}{b}$  det også. Endvidere bliver diskret valuationsfunktionen fra bilaget brugt. Nu kan vi gå igang med beviset for (2.13). Antag, at (2.13) ikke er opfyldt. D.v.s at

$$(xg_n - f_n)^2 \nmid g_{n-1}g_{n+1}$$

Da må der eksistere et irreducibelt polynomie  $f$ , hvor

$$\nu_f((xg_n - f_n)^2) > \nu_f(g_{n-1}g_{n+1}) \quad (2.24)$$

Hvis ikke ville  $(xg_n - f_n)^2 \mid g_{n-1}g_{n+1}$ . Det betyder, at  $f$  går flere gange op i nævneren til højre end nævneren til venstre i (2.23). Men hvis de to brøker skal være lig hinanden kan det kun lade sig gøre hvis

$$f \mid T = (f_nx - ag_n)^2 - 4bg_n(g_nx + f_n)$$

*Bemærkning 2.6.* Læg mærke til, at  $f$  ikke kan dele  $g_n$ . I så fald ville  $f$  også dele  $f_n$ , da den deler  $(xg_n - f_n)$ , og det giver en modstrid da  $f_n$  og  $g_n$  er primiske.

**Lemma 2.7.**  $f$  deler både  $S$  og  $R$ .

*Bevis.* Da  $T = X_{n-1}X_{n+1}(xg_n - f_n)^2 = \frac{RS}{(xg_n - f_n)^2}$  må  $f$  dele mindst en af  $R$  eller  $S$ . Antag at  $f \mid R$ , men  $f \nmid S$ . Da fås af (2.22) :

$$g_{n+1} = \frac{f_{n+1}}{X_{n+1}} = \frac{f_{n+1}(xg_n - f_n)^2}{S},$$

som viser, at

$$\nu_f(g_{n+1}) = \nu_f(f_{n+1}(xg_n - f_n)^2) = \nu_f((xg_n - f_n)^2),$$

da  $\nu_f(f_{n+1}) = 0$  (var  $\nu_f(f_{n+1}) > 0$  ville  $f$  dele både  $f_{n+1}$  og  $g_{n+1}$ ). Endvidere siger (2.23) :

$$f_{n-1}f_{n+1}(xg_n - f_n)^2 = g_{n-1}g_{n+1}T$$

⇓

$$\nu_f(f_{n-1}f_{n+1}(xg_n - f_n)^2) = \nu_f(g_{n-1}g_{n+1}T)$$

Af regneregler (A.8) samt  $\nu_f(f_{n+1}) = 0$  og  $\nu_f(g_{n+1}) = \nu_f(xg_n - f_n)^2$  fås:

$$\nu_f(f_{n-1}) - \nu_f(g_{n-1}) = \nu_f(T) > 0$$

Men det må betyde, at  $f \mid f_{n-1}$  og dermed at  $f \nmid g_{n-1}$ , da  $\text{sfd}(f_{n-1}, g_{n-1}) = 1$ . Det giver så, at

$$\nu_f(g_{n-1}g_{n+1}) = \nu_f(g_{n+1}) = \nu_f((xg_n - f_n)^2).$$

Men det er jo i modstrid med (2.24). Ligeledes med situationen hvor  $f \mid S$ , men  $f \nmid R$ , og det beviser lemma 2.7.  $\square$

Vi har altså at  $f \mid R$  og  $f \mid S$ . Men så går  $f$  specielt op i de to tællere fra (2.10):

$$f \mid g_n^3(x^3 + ax + b)(1 + Y_n)^2 - ((xg_n - f_n)^2(xg_n + f_n))$$

$$f \mid g_n^3(x^3 + ax + b)(1 - Y_n)^2 - ((xg_n - f_n)^2(xg_n + f_n))$$

og da  $f \mid (xg_n - f_n)$  fås

$$f \mid g_n^3(x^3 + ax + b)(1 + Y_n)$$

$$f \mid g_n^3(x^3 + ax + b)(1 - Y_n)$$

Der blev også brugt, at hvis  $f \mid (1 + Y_n)^2 \Rightarrow f \mid (1 + Y_n)$ . Nu må  $f$  også dele summen af de to sidste ligninger:

$$f \mid 2(x^3 + ax + b)g_n^2$$

$f$  kan ikke dele 2, da  $f$  ikke er en enhed. Den kan heller ikke dele  $g_n$  ifølge bemærkningen ovenfor. Altså må  $f \mid (x^3 + ax + b)$ . Man kan ved udregning se, at

$$T = -(xg_n - f_n)(xf_n^2 + (x^3 - 2ax - 4b)g_n) + (x^4 - 2ax^2 - 8bx + a^2)g_n^2$$

Da  $f$  deler  $T$  og første led ligningen ovenfor, må  $f$  også dele sidste led, hvilket fører til at  $f \mid x^4 - 2ax^2 - 8bx + a^2$ . Endvidere kan man skrive diskriminanten som

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

Men det betyder, at  $f$  deler diskriminanten, der er forskellig fra nul. Det er i modstrid med, at  $f$  ikke er en enhed. Det beviser (2.13), og derved lemma 2.5.  $\square$

Det sidste lemma giver en anden formel for følgen  $d_n$ .

**Lemma 2.8.**

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

hvor  $\alpha = -(d_{-1} - d_0 - 1) = p + 1 - \sharp E_p(\mathbb{Z}/p\mathbb{Z})$

*Bevis.* Lemmaet bevises v.h.a induktion frem og tilbage. Induktionsbasis  $n = 0$  og  $n = -1$  opfylder klart lemma 2.8. Så lad os antage, at lemmaet er opfyldt for  $d_n$  og  $d_{n-1}$ . Vi får fra lemma 2.5 at

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

Det samme kan gøres for  $d_{n-2}$ .  $\square$

Vi har altså nu, at  $d_n$  er skrevet som et polynomielt udtryk af  $n$ . Da  $d_n$  er graden af et polynomium, er  $d_n \geq 0$ . Endvidere kan to på hinanden følgende  $d_n$ 'er ikke være 0. Det skyldes, at så vil alle  $d_n$ 'er ifølge lemma 2.5 være lige. Det betyder specielt, at  $d_0 = p$  er lige, men det er i modstrid med, at  $p$  er et primtal forskellig fra 2. Hvis man kan vise, at 2.gradspolynomiet  $x^2 + \alpha x + p \geq 0$  for alle  $x$ , ikke bare heltallige, så har man bevist Hasses sætning, da diskriminanten  $d$  for 2.gradspolynomiet så må være mindre end eller lig 0 (svarende til 1 eller ingen løsninger).

$$d = \alpha^2 - 4p \leq 0 \Rightarrow |\alpha| = |p + 1 - \sharp E_p(\mathbb{Z}/p\mathbb{Z})| \leq 2\sqrt{p}.$$

Læg mærke til, at  $d$  er et helt tal og at kvadratroden af diskriminanten er lig med afstanden mellem rødderne:

$$|x_2 - x_1| = \left| \frac{-b + \sqrt{d} - (-b - \sqrt{d})}{2a} \right| = \sqrt{d}$$

$d$  kan ikke være større end 1, da det vil betyde at der er afstand større end 1 mellem rødderne. Så vil der nemlig også eksisterer et  $d_n$  mellem rødderne, og det vil være negativt i modstrid med at  $d_n$ 'er er positive. Så det lader kun en mulighed tilbage hvis  $d$  er et helt tal, der ikke opfylder, at  $d \leq 0$ ; nemlig  $d = 1$ . Men er  $d = 1$  er vi tilbage i situationen, hvor der er to på hinanden følgende  $d_n$ 'er, der er 0, eller et  $d_n$  mellem to rødder. Så  $d$  er altid mindre end eller lig 0, og Hasses sætning er bevist.  $\square$

**2.3. Eksempler på elliptiske kurver over endelige legemer.** I dette afsnit vil der komme to eksempler, der viser, at antallet af punkter for det første holder sig inden for det slør Hasse giver os, men også, at antallet i nogle tilfælde når til grænserne.

**Eksempel 2.9.** Vi kigger på den elliptiske kurve  $E : y^2 = x^3 - x + 1 = f(x)$  defineret over legemet  $\mathbb{Z}/7\mathbb{Z}$ .  $E$  er klart elliptisk, da diskriminanten er  $D = -4(-1)^3 - 27 = 5 \neq 0$ . Vi kan opstille følgende tabel:

| $x$ | $f(x)$ | $y$ | $y^2$ |
|-----|--------|-----|-------|
| 0   | 1      | 0   | 0     |
| 1   | 1      | 1   | 1     |
| 2   | 0      | 2   | 4     |
| 3   | 4      | 3   | 2     |
| 4   | 5      | 4   | 2     |
| 5   | 2      | 5   | 4     |
| 6   | 1      | 6   | 1     |

Af den kan man se, at de elementer i  $\mathbb{Z}/7\mathbb{Z}$ , der har kvadratrødder er  $\{0, 1, 2, 4\}$  og man kan se, at følgende punkter ligger på  $E$ :  $(0, 1)$ ,  $(0, 6)$ ,  $(1, 1)$ ,  $(1, 6)$ ,  $(2, 0)$ ,  $(3, 2)$ ,  $(3, 5)$ ,  $(5, 3)$ ,  $(5, 4)$ ,  $(6, 1)$ ,  $(6, 6)$ ,  $\mathcal{O}$ . Vi får altså, at  $\sharp E(\mathbb{Z}/7\mathbb{Z}) = 12$ , og det er lige i den ene ydergrænse af Hasse, da  $\sharp E(\mathbb{Z}/7\mathbb{Z}) = (7 + 1) \pm 4$ .

Vi kan også nå den anden ydergrænse. F.eks. ved at se på dette eksempel.

**Eksempel 2.10.** Lad  $E$  være den elliptiske kurve over  $\mathbb{Z}/7\mathbb{Z}$  defineret ud fra ligningen  $y^2 = x^3 - x - 1 = f(x)$ . Igen skal man tjekke, at diskriminanten er forskellig fra 0.  $D = -4(-1) - 27(-1) = 3 \neq 0$ . Vi opstiller igen en tabel:

| $x$ | $f(x)$ | $y$ | $y^2$ |
|-----|--------|-----|-------|
| 0   | 6      | 0   | 0     |
| 1   | 6      | 1   | 1     |
| 2   | 5      | 2   | 4     |
| 3   | 2      | 3   | 2     |
| 4   | 3      | 4   | 2     |
| 5   | 0      | 5   | 4     |
| 6   | 6      | 6   | 1     |

Det giver følgende punkter på  $E$ :  $(3, 3)$ ,  $(3, 4)$ ,  $(5, 0)$ ,  $\mathcal{O}$ . Her har vi så, at  $\sharp E(\mathbb{Z}/7\mathbb{Z}) = 4$ .

## 3. FAKTORISERING

**3.1. Introduktion.** I dette kapitel vil vi se på en af anvendelserne af elliptiske kurver. Ideerne er taget fra [1] kap.4. Det er velkendt, at et helt tal entydigt kan skrives som et produkt af primtal. Men givet et helt tal  $n$ , hvordan finder man en primtalsdivisor i  $n$ . Man kunne selvfølgelig give sig til at dividere med alle ulige tal mindre end  $n$ , for at se om divisionen gik op. Dette kaldes den trivielle metode. Er  $n$  imidlertid et stort tal, vil den trivielle metode, selv med hjælp fra computere være uoverkommelig. Det viser sig, at der findes nogle bedre metoder. To af dem, Pollards algoritme og Lenstras algoritme, vil blive behandlet her. Pollards algoritme bygger godt nok ikke på elliptiske kurver, men ideen bag Pollards minder meget om ideen bag Lenstras.

**3.2. Pollards algoritme.** Vi vil i dette afsnit beskrive Pollards algoritme til faktorisering af hele tal. Givet et tal  $n$ , vil vi altså prøve, at finde en primfaktor i  $n$ . Antag, at  $p$  er en primfaktor i  $n$ . Ideen bag algoritmen er som følger. Da ved vi, ifølge Fermats lille sætning, at  $a^{p-1} \equiv 1 \pmod p$ , hvis  $p$  ikke deler  $a$ . Forestiller man sig nu et tal  $k$ , således, at  $p-1 \mid k$  fås, at

$$a^k = a^{b(p-1)} = a^{p-1} \dots a^{p-1} \equiv 1 \cdot 1 \cdot \dots \cdot 1 \equiv 1 \pmod p,$$

og det betyder igen, at  $p$  deler både  $a^k - 1$  og, pr antagelse,  $n$ . Tricket er nu at tjekke  $\text{sfd}(a^k - 1, n)$  for forskellige  $a, k$ . Får man et tal mellem 1 og  $n$ , har man afsløret en divisor i  $n$ . Typisk vælger man  $k$ , så det er sammensat af "små" primtal. Det betyder, at hvis  $p-1$  er sammensat af "små" primtal er der en god chance for at afsløre en divisor i  $n$ . Skriver man det ud i skridt kommer det til at se således ud:

- 1) Vælg et  $k$ , der er et produkt af små primtal. Sæt f.eks  $k = \text{mfm}(1, 2, \dots, K)$
- 2) Vælg et  $a$  så  $1 < a < n$ . Er  $\text{sfd}(a, n) \neq 1$ , er  $\text{sfd}(a, n)$  en divisor, og algoritmen er færdig.
- 3) Udregn  $\text{sfd}(a^k - 1, n)$ . Er den forskellig fra 1 eller  $n$ , har man fundet en divisor og algoritmen er færdig. Er den 1 kan man vælge et andet  $a$  eller et større  $k$ , og er den lig  $n$ , kan man vælge et mindre  $k$ .

**Eksempel 3.1.** Lad os faktorisere  $n = 10403$ . Vi vælger  $a = 3$ , og  $k = 2^2 \cdot 3^2 \cdot 5^2 = 900$ . Først laves en tabel over hvad  $3^{2^i}$  mod  $n$  er. Grunden til at vi regner mod  $n$  er, at  $\text{sfd}(m, n) = \text{sfd}(m + ln, n)$ .

| $3^{2^i}$ | mod $n$ |
|-----------|---------|
| 3         | 3       |
| $3^2$     | 9       |
| $3^4$     | 81      |
| $3^8$     | 6561    |
| $3^{16}$  | 9510    |
| $3^{32}$  | 6821    |
| $3^{64}$  | 3825    |
| $3^{128}$ | 4007    |
| $3^{256}$ | 4220    |
| $3^{512}$ | 8867    |

Ved hjælp af tabellen kan man nu beregne  $3^{900}$  mod  $n$ .

$$3^{900} = 3^{512+256+128+4} = 3^{512} \cdot 3^{256} \cdot 3^{128} \cdot 3^4 = 8867 \cdot 4220 \cdot 4007 \cdot 81 = 9552 \cdot 4007 \cdot 81$$

$$= 2227 \cdot 81 = 3536$$

Læg mærke til, at alle beregninger er udført mod  $n$ . Spørgsmålet er nu, hvad  $\text{sfd}(3536 - 1, 10403)$ . Til det bruges, igen, at  $\text{sfd}(m + ln, n) = \text{sfd}(m, n)$ .

$$\text{sfd}(3535, 10403) = \text{sfd}(3535, 3333) = \text{sfd}(202, 3333) = \text{sfd}(202, 101) = 101$$

101 skulle altså gerne være divisor i 10403, og det viser sig da også, at  $101 \cdot 103 = 10403$ .

**3.3. Lenstras algoritme.** I dette afsnit vil vi, inspireret af Pollards algoritme, prøve at lave en faktoreringsalgoritme v.h.a elliptiske kurver. Inden da skal vi dog have et par småting op at stå. Givet en elliptisk kurve,  $E$ , over  $\mathbb{Q}$  har vi snakket om  $E$ 's reducering modulo  $p$ . Givet et rationelt punkt,  $P$ , på  $E$ , vil vi også gerne kunne snakke om  $P$ 's reducering modulo  $p$ . Hvis  $P = (A : B : C)$ , hvor  $A, B, C$  er reduceret mest muligt er  $P_p = (A_p : B_p : C_p)$ . Læg mærke til, at man ikke får  $P_p = (0 : 0 : 0)$  da  $A, B, C$  er reduceret mest muligt. Der gælder nu følgende sætning:

**Sætning 3.2.** *Lad  $E$  være en elliptisk kurve over  $\mathbb{Q}$ , og  $P$  et punkt på  $E$ , da er  $P_p$  et punkt på  $E_p$ . Faktisk gælder der, at hvis  $r_p$  betegner funktionen, der tager et element  $P$  fra  $E(\mathbb{Q})$  og fører det over i  $P_p$  så er  $r_p$  en gruppehomomorfi. Det hele forudsat, at  $p$  ikke deler diskriminanten  $D$ .*

*Bevis.* Det følger fra regnereglerne for restklasser, at reduktion modulo  $p$  er en ringhomomorfi. Lad  $P = (A : B : C)$  og  $P_p = (A_p : B_p : C_p)$ . Da fås:

$$B_p^2 C_p = (A^3 + aA^2 C + bAC^2 + cC^3)_p = A_p^3 + a_p A_p^2 C_p + b_p A_p C_p^2 + c_p C_p^3$$

og  $P_p$  ligger på  $E_p$ . Ligeledes, da additionsformlerne kun indbefatter rationelle regneoperationer, og igen at reduktion modulo  $p$  er en ringhomomorfi fås, at  $r_p$  er en gruppehomomorfi.  $\square$

*Bemærkning 3.3.* Læg mærke til, at  $r_p$  er en gruppehomomorfi betyder, at  $(kP)_p = kP_p$ .

Vi skal også bruge følgende sætning:

**Sætning 3.4.** *Lad  $E$  være en elliptisk kurve på formen (2.3) over  $\mathbb{Q}$ , og  $P$  et punkt på  $E$  forskellig fra  $\mathcal{O}$ . Da er  $P$  på formen  $P = (\frac{c}{e^2}, \frac{d}{e^3})$ , hvor de to brøker er skrevet på lavest form.*

*Bevis.* Lad  $P$  være skrevet uforkorteligt, så  $P = (\frac{m}{M}, \frac{n}{M})$ , og begge nævnere er positive. Da  $P$  ligger på  $E$ , fås

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

$\Downarrow$

$$n^2 M^3 = m^3 N^2 + amM^2 N^2 + bM^3 N^2 \quad (3.1)$$

Da  $\text{sfd}(n, N) = 1$ , må  $N^2 \mid M^3$ . Endvidere må  $M^2 \mid N^2 m^3$ , da  $M^2$  indgår i alle de andre led, og igen da  $\text{sfd}(m, M) = 1$  må  $M^2 \mid N^2$  hvilket medfører, at  $N^2 = cM^2$ . Sættes det ind i (3.1) fås:

$$n^2 M^3 = m^3 N^2 + amcM^4 + bM^3 N^2.$$

Nu indgår der et  $M^3$  i alle ledene, og ligesom ovenfor fås, at  $M^3 \mid N^2$ . Da begge er positive, må det betyde, at  $M^3 = N^2$ . Sættes  $e = \frac{N}{M}$  (læg mærke til, at  $e$  er et helt tal, da  $M^2 \mid N^2$ ) fås, at

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M \quad \text{og} \quad e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N,$$

og det betyder, at  $P = (\frac{m}{e^2}, \frac{n}{e^3})$  □

Det sidste vi vil bemærke inden vi går igang med Lenstra er følgende.

**Sætning 3.5.** *Lad  $n \in \mathbb{Z}$ . Da er  $e$ ,  $1 \leq e \leq n - 1$ , en enhed i  $\mathbb{Z}/n\mathbb{Z}$  hvis og kun hvis  $\text{sfd}(e, n) = 1$ .*

*Bevis.* Lad  $\text{sfd}(e, n) = 1$ . Da siger euklid, at  $1 = ae + bn$ . Men det betyder jo, at  $e$  er en enhed, da  $ea_n = 1$  i  $\mathbb{Z}/n\mathbb{Z}$ . Antag omvendt, at  $e$  er en enhed. Da eksisterer der et inverst element  $a$ , og derfor også et  $b$ , så  $ea + bn = 1$ . En fælles divisor for  $e$  og  $n$ , vil derfor også dele 1, og det giver, at  $\text{sfd}(e, n) = 1$ . □

*Bemærkning 3.6.* Der er i beviset skiftet frem og tilbage mellem talsystemerne  $\mathbb{Z}$  og  $\mathbb{Z}/n\mathbb{Z}$

Vi er nu klar til at beskrive ideen bag Lenstras algoritme. Så givet et  $n$  skal vi prøve, at finde en primfaktor  $p$ . Vi vælger en elliptisk kurve,  $E$  på formen (2.3) over  $\mathbb{Q}$ . På denne kurve finder vi et punkt  $P$ . Vi vælger nu et helt tal  $k$ . Hvis antallet af punkter på  $E$ 's reducering modulo  $p$  deler  $k$ , så er  $kP_p = \mathcal{O}$  (se [2] s.57). Eller sagt på en anden måde: Hvis  $\#E_p(\mathbb{Z}/p\mathbb{Z}) \mid k$ , så er  $kP_p = (kP)_p = (ce : d : e^3)_p = (0 : 1 : 0)$ , hvor sætning 3.4 samt at  $r_p$  er en gruppehomomorfi er blevet brugt. Men det betyder, at  $e \equiv 0 \pmod{p}$ , og igen, at  $\text{sfd}(e, n) \geq p$ ; altså en god mulighed for at finde en faktor. Hvis man vælger  $k$  som et produkt af små primtal, skal man altså "bare" ramme ind i en elliptisk kurve, hvor antallet af punkter på  $E$ 's reducering er et produkt af små primtal. Vi har altså i denne algoritme i forhold til Pollards udskiftet gruppen  $(\mathbb{Z}/p\mathbb{Z})^*$  med gruppen  $E_p(\mathbb{Z}/p\mathbb{Z})$  og  $a$  med punktet  $P$ . Men lad os få Lenstras algoritme på opskriftsform.

- 1) Vælg en elliptisk kurve  $E$  og et punkt  $P$  på  $E$ .
- 2) Tjek om  $\text{sfd}(D, n) = 1$ . Hvis den er forskellig fra 1, har vi enten at  $1 < \text{sfd}(D, n) < n$ , og vi har en divisor, eller  $\text{sfd}(D, n) = n$ , og vi må starte forfra.
- 2) Vælg et  $k$ , der er et produkt af små primtal, f.eks.  $k = mfm(1, 2, \dots, K)$
- 3) Udregn  $kP = (\frac{c}{e^2}, \frac{d}{e^3})$
- 4) Er  $\text{sfd}(e, n)$  forskellig fra 1,  $n$  er vi færdige. Er den 1 kan man vælge en ny elliptisk kurve, eller et større  $k$ . Er den  $n$ , kan man vælge et mindre  $k$ . Man bør her nævne, at mange af de fordele der er ved Lenstras er for vanskelige at komme ind på i dette projekt. Dog er der en indlysende grund til at vælge Lenstras: I Pollards er der kun en gruppe, nemlig  $(\mathbb{Z}/p\mathbb{Z})^*$ , mens der er mange flere ved Lenstras (man kan jo bare vælge en ny elliptisk kurve). Lad os prøve at regne et eksempel på Lenstras algoritme. Eksemplet stammer fra [1] s. 144, hvor det er stillet som en opgave.

**Eksempel 3.7.** Vi har givet  $n = 199843247$ . Lad os prøve, at finde en faktor. Først tjekkes, at 2,3 ikke deler  $n$ . det er for at undgå, en situation, hvor  $p = 2, 3$ . Dette er ikke tilfældet. Så vælger vi en kurve  $E$ :

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

Det ses, at  $E$  er elliptisk, da  $D = -4 \cdot (-59) - 27 \cdot (-59)^3 = 5545469$  og man kan beregne, at  $\text{sfd}(5545469, 199843247) = 1$  Endvidere ses det, at  $(1, 1)$  ligger på  $E$ . Vi

vælger nu

$$k = 16296 = 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^9 + 2^8 + 2^7 + 2^5 + 2^3$$

Læg mærke til den smarte opskrivning af  $k$ , ligesom i 3.1. Vi udregner nu en tabel af  $2^i P$  v.h.a fordoblingsformlerne fra kap 1 . Vi regner mod 199843247 for at lette udregningerne.

| i  | $2^i P$ 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 udregne  $kP$  modulo  $n$ , ved hjælp af additionsformlerne, og den smarte opskrivning af  $k$ .

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

Men så kommer problemet. Når vi skal til at addere  $(2^3 + \dots + 2^{12})P$  med  $2^{13}P$  og skal reducere modulo  $n$ , kan vi ikke finde det inverse element til differensen af de to  $x$ -koordinater, der er i formel (1.4). Det må skyldes, at den ikke er en enhed i  $\mathbb{Z}/n\mathbb{Z}$ . Eller, ifølge sætning 3.5, at  $\text{sfd}(x_2 - x_1, n) \neq 1$  Vi ser også, at

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

og

$$199843247 = 10289 \cdot 19423$$

Læg mærke til, at dette eksempel viser, at grunden til Lenstras algoritme virker er, at der ikke er en gruppestruktur på  $E(\mathbb{Z}/n\mathbb{Z})$ , da dette ikke er et legeme. Og når det går galt, er det fordi vi ikke kan finde et invers til et element.

## BILAG A

**A.1. Specialtilfælde af Bezouts sætning.** Da Bezouts sætning kun er sand i det projektive plan, fortælles her ultrakort om det projektive plan. Det består af 3 tupler  $(x : y : z)$ , hvor to punkter,  $(x : y : z), (u : v : w)$  regnes for ens hvis der eksisterer et  $t$  så  $(x : y : z) = (tu : tv : tw)$ . Dog eksisterer  $(0 : 0 : 0)$  ikke i det projektive plan. Eller lidt mere formelt:

**Definition A.1.** Givet et legeme  $k$  defineres det projektive plan  $\mathbb{P}^2(k)$  som de ækvivalensklasser  $(a : b : c)$  (hvor  $a, b, c \in k$  og ikke alle må være lig 0), der opstår under ækvivalensrelationen

$$(a : b : c) \sim (a', b', c') \Leftrightarrow \exists t \neq 0 : a = ta', b = tb', c = tc'$$

eller

$$\mathbb{P}^2(k) = \{(a : b : c) \in k^3 \setminus (0 : 0 : 0)\} / \sim$$

Man kan nu associasere et punkt i det affine plan (det normale  $k^2$  plan) med et punkt i det projektive v.h.a afbildningen:

$$\pi : k^2 \mapsto \mathbb{P}^2(k) : \pi(x, y) = (x : y : 1)$$

Dette kaldes en dehomogenisering med hensyn til  $Z = 1$ . Man kan selvfølgelig også dehomogenisere med hensyn til  $X$  og  $Y$ . Ved dehomogenisering med hensyn til  $Z = 1$  ses det, at de punkter, der ikke kan associeres med et punkt i det affine plan er dem med  $z$ -koordinat 0. Linien  $Z = 0$  kaldes linien i uendelig. Koordinaterne i det projektive plan kaldes for homogene, og man homogeniserer en ligning i det affine plan ved at gange et passende antal  $Z$ 'er på, så monomierne i ligningen er af samme grad. F.eks er ligningen  $y^2 = x^3 + ax^2 + bx + c$  skrevet på homogen form  $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$ . Vi er nu i stand til at bevise følgende.

**Sætning A.2.** *Er  $k$  et algebraisk lukket legeme,  $L$  en linie og  $C$  en kubisk kurve på Weierstraß form i  $\mathbb{P}^2$  begge med koefficienter i  $k$ , da skærer  $L$  og  $C$  hinanden præcis 3 gange talt med multiplicitet.*

*Bevis.* Da det projektive plan består af det affine plus linien i uendelig, kigges først på det affine plan.  $L$  og  $C$  er på formen.

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

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

Antag, at  $\beta \neq 0$   $L$  kan da parametriseres ved:

$$\varphi(t) = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha t - \frac{\gamma}{\beta} \\ \beta t \end{pmatrix}, t \in k$$

Antag  $\alpha \neq 0$ :

Man kan indsætte linien i  $C$ . Da  $x^3$  er det eneste monomie af orden 3 fås en 3.grads ligning i  $t$ . Den har præcis 3 løsninger talt med multiplicitet, eftersom  $k$  er algebraisk lukket. Man bør nu tjekke, at  $L$  og  $C$  ikke skærer hinanden i uendelig ( $Z = 0$ ). I afsnit 1.2 så vi, at  $C$  skar  $Z = 0$  i punktet  $(0:1:0)$ . På homogen form hedder  $L$ .

$$\alpha Y = \beta X + \gamma Z \quad \Rightarrow \quad L \text{ skærer } Z = 0 \text{ i } \left(\frac{\alpha}{\beta} : 1 : 0\right) \neq (0 : 1 : 0), \text{ da } \alpha \neq 0$$

Antag  $\alpha = 0$ :

Da  $\alpha = 0$  er parametriseringen af  $L$  nu:

$$\varphi(t) = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -\frac{\gamma}{\beta} \\ \beta t \end{pmatrix}, t \in k$$

Ved indsættelse af linien i  $C$  giver alle  $x$ -leddene nu konstanter, mens  $y$ -leddet giver anledning til en 2.grads ligning i  $t$ . Den har præcis 2 løsninger talt med multiplicitet. På homogen form ser  $L$  således ud:

$$L: \quad 0 = \beta X + \gamma Z \quad \Rightarrow \quad L \text{ skærer } Z = 0 \text{ i } (0 : 1 : 0)$$

Så  $L$  og  $C$  skærer hinanden i  $(0 : 1 : 0)$  (Det er netop punktet  $\mathcal{O}$ ). Man bør nu tjekke, at multipliciteten er 1. Homogeniseringen af  $L$  og  $C$  giver:

$$Y^2 Z = X^3 + aX^2 Z + bX Z^2 + cZ^3$$

$$0 = \beta X + \gamma Z \quad \Rightarrow \quad \gamma Z = -\beta X$$

Dehomogeniseres ligningerne med hensyn til  $Y = 1$  fås:

$$z = x^3 + ax^2 z + bxz^2 + cz^3$$

Ligningen for  $L$  forbliver den samme. Koordinaterne for skæringspunktet bliver  $(x, z) = (0, 0)$ . Indsættes Linien i  $C$  fås:

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

↓

$$0 = x(x^2 - a\frac{\beta}{\gamma}x^2 + b\left(\frac{\beta}{\gamma}\right)^2 x^2 - c\left(\frac{\beta}{\gamma}\right)^3 x^2 + \frac{\beta}{\gamma})$$

Som betyder, at  $C$  og  $L$  skærer hinanden i  $(0:1:0)$  med multiplicitet 1; nøjagtig som de skulle.

Er  $\beta = 0$  fås, at  $\varphi(t) = \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} t \\ \frac{\gamma}{\alpha} \end{pmatrix}, t \in k$ . Men det giver igen en 3.grads ligning i  $x$ , der har tre løsninger, da  $k$  er algebraisk lukket. □

Det er her på sin plads at nævne, at multipliciteten nævnt i Bezouts sætning er den såkaldte snitmultiplicitet som er defineret således.

**Definition A.3.** Lad  $L$  være en linie og  $C$  en kurve i  $\mathbb{P}^2$  med et fælles punkt  $P$ . Lav lokale affine koordinater så  $P = (0, 0)$ .  $L$  kan da parametriseres som  $\varphi(t) = \begin{pmatrix} \alpha t \\ \beta t \end{pmatrix}$ .  $f(\varphi(t))$  bliver da et polynomium i  $t$  og  $f(\varphi(0)) = 0$ . Ordenen af nulpunktet er snitmultipliciteten i  $P$ .

Man bør lige checke, at snitmultiplicitet og multiplicitet fra algebra er ens. Så lad  $L$  skære  $C$  i  $P$ . Indsæt parametriseringen af  $L$   $\varphi(t) = \begin{pmatrix} \alpha t \\ \beta t \end{pmatrix}$  i  $C$ . Det giver et polynomium  $f(t)$  i  $t$ . Lad  $t_0$  være det  $t$ , der svarer til  $P$ . Det giver, at

$$(t - t_0)^n \mid f, \text{ men } (t - t_0)^{n+1} \nmid f$$

eller

$$f = g(t)(t - t_0)^n, \text{ hvor } g(t_0) \neq 0$$

Her er  $n$  den algebraiske multiplicitet, men for at få snitmultipliciteten skal man jo skifte koordinater svarende til substitutionen  $t' = t - t_0$ , og se hvad orden nulpunktet

i 0 har. Men det er præcis  $n$ , og derved er den algebraiske multiplicitet i overensstemmelse med snitmultipliciteten.

**A.2. Kvadratisk rest, Legendre symbolet og Diskret valuation.** Først defineres kvadratisk rest og Legendre symbolet. Ideerne er taget fra [6] s. 63.

**Definition A.4.** Lad  $a \neq 0 \in \mathbb{Z}/p\mathbb{Z}$ , da kaldes  $a$  for en kvadratisk rest modulo  $p$  hvis der eksisterer en løsning til ligningen  $x^2 = a$ . Ellers kaldes  $a$  for en kvadratisk ikke-rest modulo  $p$

**Definition A.5.** Lad  $a \in \mathbb{Z}/p\mathbb{Z}$ . Da er Legendresymbolet  $\left(\frac{a}{p}\right)_L$  defineret således:

$$\left(\frac{a}{p}\right)_L = \begin{cases} 1 & \text{hvis } a \text{ er en kvadratisk rest modulo } p, \\ 0 & \text{hvis } a = 0, \\ -1 & \text{hvis } a \text{ er en kvadratisk ikke-rest modulo } p, \end{cases} \quad (\text{A.1})$$

Der gælder nu følgende regneregler for Legendre symbolet.

**Sætning A.6.**

$$\left(\frac{a}{p}\right)_L = a^{\frac{1}{2}(p-1)} \quad (\text{A.2})$$

*Bevis.* Er  $\left(\frac{a}{p}\right)_L = 0$  er sætningen klart opfyldt. Er  $\left(\frac{a}{p}\right)_L = 1$  så eksisterer der pr definition et  $x \in \mathbb{Z}/p\mathbb{Z}$  så

$$x^2 = a \quad \Rightarrow \quad a^{\frac{1}{2}(p-1)} = x^{p-1} = 1$$

Det sidste lighedstegn kommer af, at  $(\mathbb{Z}/p\mathbb{Z})^*$  er en cyklisk gruppe af orden  $p-1$ , og i en sådan er et elemen opløftet i  $p-1$  altid lig med 1. Til sidst lad  $\left(\frac{a}{p}\right)_L = -1$  det betyder, at der ingen løsninger er til ligningen  $x^2 = a$ . Men eftersom  $(\mathbb{Z}/p\mathbb{Z})^*$  er en gruppe har vi, at for alle  $j \in (\mathbb{Z}/p\mathbb{Z})^*$  eksisterer der et entydigt  $i$  så  $ij = a$ . Men det parrer tallene i  $(\mathbb{Z}/p\mathbb{Z})^*$   $\frac{1}{2}(p-1)$  par, der hver især giver  $a$ . Ganges disse par sammen fås

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

Det er here vigtigt, at  $(\mathbb{Z}/p\mathbb{Z})^*$  er kommutativ m.h.t. gange. At  $1 \cdot \dots \cdot (p-1) = -1$  ses, af, at alle elementer i  $(\mathbb{Z}/p\mathbb{Z})^*$  har et inverst element. De eneste elementer, der er sit eget inverse er 1 og  $p-1$ . D.v.s, at de andre elementer parres til 1-taller:

$$(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1) = 1 \cdot 1 \cdot \dots \cdot 1 \cdot (p-1) = -1$$

□

Det sidste der omhandles er diskret valuationsfunktionen.

**Definition A.7.** Lad  $f \in k[X]$ , hvor  $f$  er irreducibel og  $k$  er et legeme. Da defineres den diskrete valuation af et polynomie til at være funktionen  $\nu_f : k[X] \mapsto \mathbb{N}$  således at hvis  $g \in k[X]$  er  $\nu_f(g) = n$ , hvor  $n$  opfylder at  $g = f^n h$  og  $(f, h) = 1$ .

Der gælder følgende regneregler for  $\nu_f$ :

**Sætning A.8.**  $\nu_f(g_1 g_2) = \nu_f(g_1) + \nu_f(g_2)$

*Bevis.* Lad  $g_i = f^{n_i} h_i$  så  $(f, h_i) = 1$  for  $i = 1, 2$ . Da er

$$\nu_f(g_1 g_2) = \nu_f(f^{n_1+n_2} h_1 h_2) = n_1 + n_2 = \nu_f(g_1) + \nu_f(g_2)$$

□

## LITTERATUR

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

*E-mail address:* [kjolby@hotmail.com](mailto:kjolby@hotmail.com)

KASPER KJØLBY, RISDALSVEJ 40 VÆR. 222, 8260 VIBY J, DANMARK