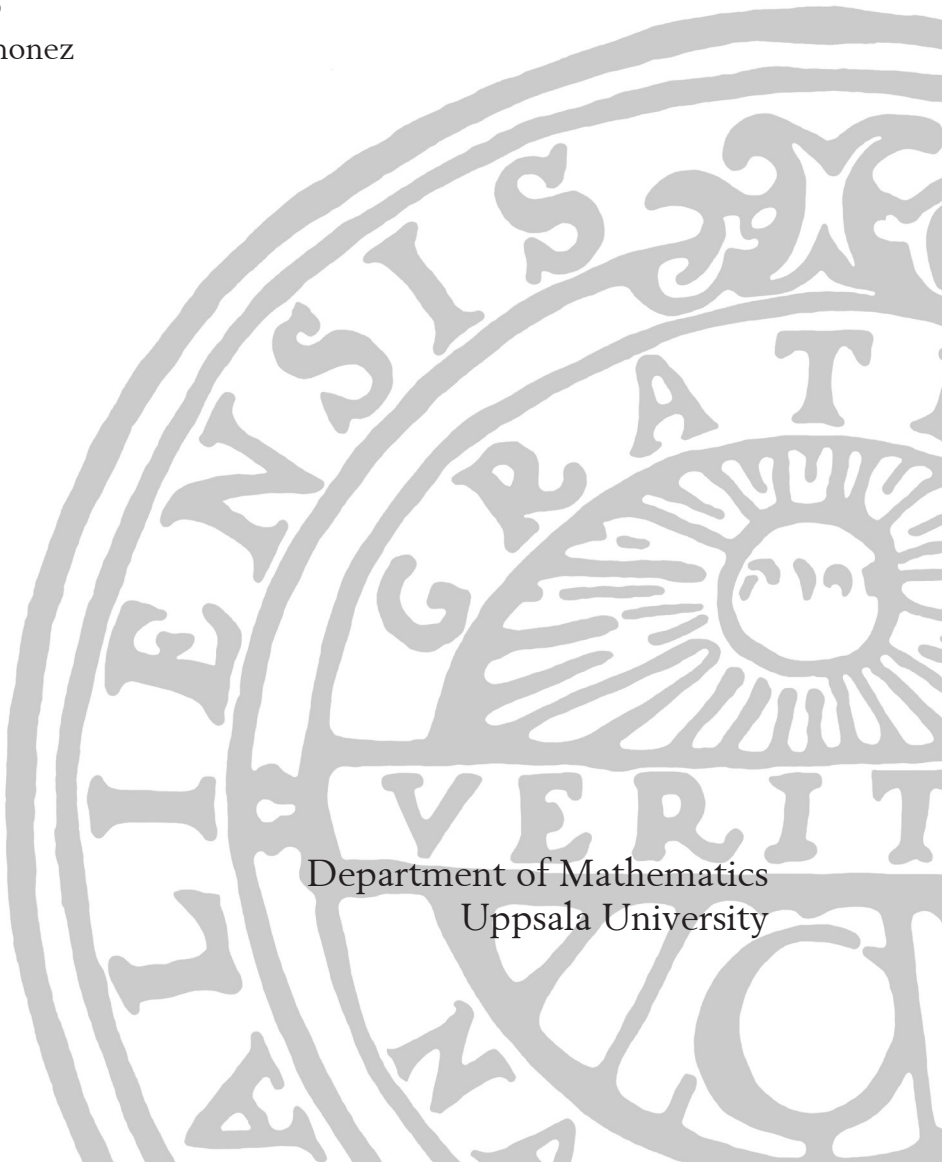
UPPSALA
UNIVERSITET

U.U.D.M. Project Report 2020:3

Elliptiska kurvor och kryptografi

Noraldeen Alyounes

Examensarbete i matematik, 15 hp
Handledare: Veronica Crispin Quinonez
Examinator: Martin Herschend
Februari 2020



Department of Mathematics
Uppsala University

Innehåll

1 Inledning

Denna uppsats handlar om elliptiska kurvor och kryptografi. Först behöver vi veta vad kryptografi betyder, och sedan beskriver vi hur vi kan tillämpa elliptiska kurvor inom detta område.
I sin bok *A Course in Number Theory and Cryptography* [K] beskriver Neal Koblitz kryptografi som studien av metoderna för hur man skickar hemliga meddelanden på ett sådant sätt att endast den tilltänkta mottagaren kan läsa/se meddelandet. Meddelandet som vi vill skicka kallas för klartext och det hemliga meddelandet kallas för krypterad text. Processen som vi använder för att omvandla klartexten till en hemlig/krypterad text kallas för kryptering. Vi kan tänka oss att krypteringen är en ”en-till-en”-funktion som tar vilken klartext som helst och ger en krypterad text. ”En-till-en” betyder att funktionen har endast en krypterad text för varje klartext. Om vi kallar mängden av klartexter för *P* och alla krypterade texter för *C* får vi denna notation

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

Detta betyder att vi får *P* igen genom så kallad dekrypteringsprocess (f^{-1}). Man kan tillämpa elliptiska kurvor, mer noggrant över ändliga kroppar, inom kryptografi.

Vi börjar med att presentera viktiga förkunskaper från abstrakt algebra. Därefter beskriver vi elliptiska kurvor över olika slags kroppar med betoning på ändliga kroppar. I slutet presenteras kryptering som använder elliptiska kurvor, nämligen Diffie-Hellman och Elgamal. Vi kommer också att presentera en algoritm för digitala signaturer.

2 Algebra

I detta avsnitt kommer vi att presentera nödvändiga definitioner och resultat.

Nedanstående del är hämtad från [KW14].

Definition 1. Vi betecknar två tal *a* och *b* som är kongruenta modulo *m* med $a \equiv b \pmod{m}$. Om $a - b$ är multipel av *m* kallas *m* för modulo till kongruensen och den ska vara positiv.

Proposition 1. Kongruens är en ekvivalensrelation.

Proposition 2. Låt a, b, c och m vara heltal med $m > 0$. Om $a \equiv b \pmod{m}$ och $c \equiv d \pmod{m}$ då är:

(i) $a + c \equiv b + d \pmod{m}$;
(ii) $ac \equiv bd \pmod{m}$.

2.1 Grupper

Nedanstående del bygger på kap 3 i [JA] och kap 10 i [BD].
Definition 2. En binär operation på en mängd G är en funktion $G \times G \rightarrow G$ som tilldelar varje par $(a, b) \in G \times G$ ett unikt element $a \cdot b$ eller ab i G, som kallas för komposition av a och b. En grupp $(G, \cdot)$ är en mängd G tillsammans med en kompositionsregel $(a, b) \rightarrow a \cdot b$ som uppfyller följande axiom:

- Kompositionsregeln är associativ, alltså $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ för $a, b, c \in G$.
- Det finns ett enhetselement $e \in G$, sådant att för alla $a \in G$ är $ea = ae = a$.
- För varje element $a \in G$ finns det ett element i G, betecknat a^{-1}, sådant att $aa^{-1} = a^{-1}a = e$.

Definition 3. En grupp G med egenskapen att $ab = ba$ för alla $a, b \in G$, kallas för abelsk eller kommutativ.

Definition 4. H är en delgrupp till $(G, \cdot)$ om $H \subseteq G$ och $(H, \cdot)$ är en grupp.

Om vi i en grupp $(G,\cdot)$ tar ett element $g \in G$ och ”parar ihop” det med sig självt får vi $g \cdot g$. Låt oss med vanlig potensnotation beteckna detta element g^2. På samma sätt låter vi g^{-2} beteckna $g^{-1}g^{-1}$. Slutligen låter vi g^0 vara e. Vi kan nu räkna med den vanliga potenslagen: $g^n g^m = g^{m+n}$ för alla heltal m,n.

Inom elliptiska kurvor och kryptografi kommer vi arbeta med abelska grupper.

2.1.1 Cykliska grupper
För varje element $g \in G$ kan vi definiera mängden av alla dess potenser som $\langle g \rangle = \{g^n | n \in \mathbb{Z}\}$. Det visar sig att $\langle g \rangle$ också är en grupp som därför kallas gruppen som genereras av g. Elementet g kallas för gruppens generator.

Exempel 1. Gruppen $(\mathbb{Z}, +)$ är cyklisk. Eftersom varje heltal kan skrivas som en summa av tillräckligt många ettor eller minusettor, har denna grupp två generatorer: 1 och -1.

Exempel 2. Den multiplikativa gruppen modulo p, $\mathbb{Z}_p^*$ är en cyklisk grupp. Den genereras av ett element $g \neq 1$ och har enhetselementet $e = 1$.

Definition 5. Låt $a \in G$ vara en generator. I detta fall definierar vi ordningen av a som det minsta positiva heltal n sådant att $a^n = e$. Vi skriver $|a| = n$. Om detta n inte existerar säger vi att ordningen av a är oändlig och vi skriver $|a| = \infty$.

Sats 1. Ordningen av en cyklisk grupp är lika med ordningen av dess generator.

Bevis. Det finns två olika typer av cykliska grupper: ändliga och oändliga. Beviset nedan gäller för de ändliga, eftersom vi i denna uppsats endast behandlar ändliga grupper.

Låt G vara en cyklisk grupp som är genererad av a. Då kan vi skriva $|a| = n$, där n är ordningen av a. Gruppen G innehåller alla exponenter av a, det vill säga $a^0, a^1, a^2, \dots, a^{n-1}$. Först vill vi bevisa att alla a^i, $0 \leq i \leq n-1$ är olika. Antag att vi har två element som är lika i G, a^i och a^k där $0 < k < i < n$. Då får vi:

$a^i = a^k \Leftrightarrow a^i a^{-k} = a^k a^{-k} \Leftrightarrow a^{i-k} = a^{k-k} = a^0 = e$.

Vi får att $0 < i - k < n$ och $|a| = i - k$, men detta är motsägelse till att *n* är ordningen av a. Detta betyder att alla potenser av n är olika. Nu bevisar vi att det inte finns andra element i G. Vi vet att G är cyklisk. Om vi väljer ett element $X \in G$ kan vi skriva $X = a^m$. Vi skriver om m som $m = nq + r$ *där* $0 \leq r < n$.

Därmed är $a^m = a^{nq+r} = (a^n)^q a^r$, men $(a^n)^q = e$.

Så $a^m = a^r$ där $0 \leq r < n$. Vi får ett element som ingår i $a^0, a^1, a^2, \ldots, a^{n-1}$. Detta bevisar att *G* har ordning n som också är ordningen av gruppens generator. □

Exempel 3. Hitta ordningen av $a = 5$ i $\mathbb{Z}_7^*$.

Vi måste hitta *n* sådant att $5^n = 1 \pmod 7$.

$5^2 = 4 \pmod 7$

$5^3 = 4 \cdot 5 = 6 \pmod 7$

$5^4 = 4 \cdot 4 = 2 \pmod 7$

$5^5 = 4 \cdot 6 = 3 \pmod 7$

$5^6 = 3 \cdot 5 = 1 \pmod 7$, vilket är enhetselementet.

Ordningen av 5 är därmed 6, det vill säga |5| = 6.

2.1.2 Lagranges sats

Nedanstående resultat utgör Lagranges sats.

Proposition 3. Låt H vara en delgrupp till G och $g \in G$. Låt $\phi: H \to gH$ vara en funktion $\phi(h) = gh$. Funktionen ϕ är en bijektion. Därmed är antalet element i H samma som antalet element i gH.

Bevis. Antag att $\phi(h_1) = \phi(h_2)$ för elementen h_1, h_2. För att bevisa att ϕ är injektiv måste vi bevisa att $h_1 = h_2$. Vi vet att $\phi(h_1) = gh_1$ och $\phi(h_2) = gh_2$, då får vi $gh_1 = gh_2 \Leftrightarrow h_1 = h_2$. Nu bevisar vi att ϕ är surjektiv. Man vet att alla element i gH är på formen gh där $h \in H$, då är $\phi(H) = gh$ för varje $gh \in gH$. Därmed är ϕ en bijektion. □

Definition 6. Låt *H* vara en delgrupp till *G*. Definiera en vänstersidoklass av *H* med avseende på $g \in G$ som $gH = \{gh : h \in H\}$. Definiera en högersidoklass på samma sätt $Hg = \{hg : hH\}$.

Sats 2. Låt G vara en ändlig grupp och låt H vara en delgrupp. Då gäller att $|G|/|H| = [G:H]$ är antalet disjunkta vänstersidoklasser av H i G. Särskilt, ordningen av H dividerar ordningen av G.

Bevis. Gruppen H är uppdelad till $[G:H]$ disjunkta vänster sidoklasser. Varje vänstersidoklass har $|H|$ element, således är $|G| = [G:H]\,|H|$. □

Korollarium 1. Låt G vara en ändlig grupp och g en generator i G. Då dividerar ordningen av g ordningen av G.

2.2 Ringar

Nedanstående delen är hämtad från *Diskret matematik fördjupning* av K. Eriksson och H. Gavel [EG].

En icke-tom mängd R är en ring om den är sluten under två binära operationer som kallas addition och multiplikation. Additionen och multiplikationen uppfyller följande villkor:

- $a + b = b + a$ för all $a, b \in R$
- $(a + b) + c = a + (b + c)$ för alla $a, b, c \in R$.
- Det finns ett element 0 i R sådant att $a + 0 = a$ för alla $a \in R$.
- För varje element $a \in R$, existerar ett element $-a$ i R sådant att $a + (-a) = 0$.
- $(ab)c = a(bc)$ för $a, b, c \in R$.
- För $a, b, c \in R$ gäller
$$a(b + c) = ab + ac.$$
$$(a + b)c = ac + bc.$$

Det sista villkoret, det distributiva axiomet, binder ihop de två binära operationerna. De första fyra axiomen kräver att en ring måste vara en abelsk grupp under addition. Därmed kan vi definiera en ring som en abelsk grupp (R, +) som under en annan binär operation uppfyller de två sista villkoren.

Om det finns ett element $1 \in R$ sådant att $1 \neq 0$ och $1(a) = (a)1 = a$ för alla element $a \in R$, säger vi att R är en ring som innehåller ett enhetselement. En ring R för vilka $ab = ba$ för alla a, b i R kallas kommutativ. En kommutativ ring R som innehåller enhetselement kallas för ett integritetsområde om, för alla $a, b \in R$ sådana att $ab = 0$, är antingen $a = 0$ eller $b = 0$. En skevkropp eller divisionsring är en ring R som innehåller ett enhetselement, där alla element som är skilda från noll i R har en multiplikativ invers, dvs det existerar ett unikt element a^{-1} sådant att $a\,a^{-1} = a^{-1}a = 1$.

Exempel 4. Heltalsringen $\mathbb{Z}$ är ett integritetsområde. Uppenbarligen, om $ab = 0$ för två heltal a och b, är antingen $a = 0$ eller $b = 0$. Dock är $\mathbb{Z}$ inte en kropp. Det finns inget heltal i $\mathbb{Z}$ som har multiplikativ invers av 2, eftersom $\frac{1}{2}$ inte är ett heltal. Det är bara 1 och $= -1$ som har multiplikativ invers i $\mathbb{Z}$.

Exempel 5. Mängden av alla 2×2-matriser med element i en ring R utgör en ring under de vanliga operationerna matrisaddition och multiplikation. Denna ring är däremot icke-kommutativ, eftersom generellt är $AB \neq BA$ där A, B är 2×2-matriser. Man ser att denna ring inte heller är ett integritetsområde, ty det finns nollskilda matriser A och B sådana att $AB = 0$.

2.3 Kroppar

Nedanstående del är hämtad från [K].

Definition 7. En kropp $\mathbb{F}$ är en ring där varje nollskilt element har en multiplikativ invers.

Exempel 6. De rationella talen $\mathbb{Q}$, de reella talen $\mathbb{R}$, de komplexa talen $\mathbb{C}$ och $\mathbb{F}_p$, bestående av heltalen modulo ett primtal p, är de klassiska exemplen på en kropp.

Definition 8. Om man adderar det multiplikativa enhetselementet 1 med sig självt i $\mathbb{F}$ och aldrig får 0 säger vi att $\mathbb{F}$ har karakteristisk noll. I detta fall innehåller $\mathbb{F}$ en kopia av $\mathbb{Q}$. Om

det däremot existerar ett p sådant att 1+1+ ... +1= 0 (p termer), då kallas p för kroppens karakteristik. I detta fall innehåller $\mathbb{F}$ en kopia av kroppen $\mathbb{F}_p$.

$\mathbb{Q}$ och $\mathbb{F}_p$ är exempel på så kallade primkroppar som inte innehåller strikt mindre kroppar.

Låt oss beteckna en kropp som har en ändlig mängd av tal i sig $\mathbb{F}_q$. Uppenbarligen kan en ändlig kropp inte ha karakteristik noll. Så låt p vara karakteristiken av kroppen $\mathbb{F}_q$. Då innehåller den primkroppen $\mathbb{F}_p$. Det finns en ändlig kropp för alla primtal.

Definition 9. En generator g av en ändlig kropp $\mathbb{F}_q$ är ett element med ordning $q-1$. Man säger att g är generator om g's exponenter genererar alla nollskilda element i $\mathbb{F}_q$.

2.4 Eulers φ-funktion

Denna del är hämtad från kap 8 i [KW18] och [K].

Eulers φ-funktion kan berätta för oss om hur många element som är relativt prima med varandra i en ändlig mängd.

Definition 10. Låt *n* vara ett positivt heltal. Då definieras $\varphi(n)$ som antalet positiva heltal *j*, där $1 \leq j \leq n$, sådana att $SGD(j,n) = 1$.

Exempel 7. $\varphi(12)$= 4. Heltalen 1, 5, 7 och 11 är relativt prima med 12.

Om p är ett primtal, då är $\varphi(p) = (p-1)$.

Proposition 4. Låt m, n vara positiva heltal. Om $SGD(m,n) = 1$ då är:

$\varphi(mn) = \varphi(m)\varphi(n)$.

Proposition 5. Om p är ett primtal och $k \geq 1$, då är**:** $\varphi(p^k) = p^k - p^{k-1}$.

Sats 3. Låt $n = p_1^{a_1} \cdot p_2^{a_2} \cdot p_3^{a_3} \cdots p_r^{a_r}$ där p_i är distinkta primtal med exponenterna $a_i \geq 1$. Då är:

$$\varphi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i-1}) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Bevis. Från proposition 4 och 5 får vi:

$\varphi(n) = \prod_i \varphi(p_i^{a_i}) = \prod_i (p_i^{a_i} - p_i^{a_i-1})$.

Eftersom $p^a - p^{a-1} = p^a\,(1 - \frac{1}{p})$, får vi:

$$\varphi(n) = \prod_i p_i^{a_i} \left(1 - \frac{1}{p_i}\right) = \left(\prod_i p_i^{a_i}\right) \prod_i \left(1 - \frac{1}{p_i}\right) = n \prod_i \left(1 - \frac{1}{p}\right).$$

Lemma 1. För alla heltal $N > 1$ är $\sum_{d|N} \varphi(d) = N$, där *N* och $d \in \mathbb{N}$.

Bevis. Låt oss beteckna $f(N) = \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_i)$ där d_i är alla delare till *N*. Vi har från proposition 5 att $\varphi(p^k) = p^k - p^{k-1}$ och vi vet att $\varphi(1) = 1$. Då kan vi skriva:
$f(p^k) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1}) = p^k$ (1)
Då $N = p_1^{k1} \cdot p_2^{k2} \cdots p_n^{kn}$, kan vi skriva $f(N) = f(p_1^{k1}) \cdot f(p_2^{k2}) \cdots f(p_n^{kn})$ eftersom $f(N)$ är en multiplikativ funktion.

Från (1) får vi $f(N) = p_1^{k1} \cdot p_2^{k2} \cdots p_n^{kn} = N$. □

Exempel 8. Beräkna $\varphi(100)$.

Först faktoriserar vi 100 = $2^2 \cdot 5^2$. $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$.

Sats 4. Varje ändlig kropp har en generator. Om g är en generator till $\mathbb{F}_q^*$, då är g^j också en generator om och endast om $SGD(j, q-1) = 1$. Således finns det totalt $\varphi(q-1)$ olika generatorer av $\mathbb{F}_q^*$.

Bevis. Låt oss säga att vi har en ändlig kropp $\mathbb{F}_q^*$, och att $g \in \mathbb{F}_q^*$ har ordning *d*. Då kan vi enligt definition 9 skriva $|g| = d = q - 1$. Vi påstår att $g^m \in \mathbb{F}_q^*$ är en generator av $\mathbb{F}_q^*$ om och endast om $SGD(m, q-1) = 1$. Låt oss säga att vi har en annan generator g^m då kan vi skriva g i termer av g^m så att

$g = (g^m)^k = g^{mk}$ där $k \in \mathbb{Z}$.
$e = g^{mk} g^{-1} = g^{mk-1}$

$\Rightarrow d \mid (mk - 1)$ (enligt Lagranges sats)
$mk - 1 = di$ där $i \in \mathbb{Z} \Leftrightarrow mk - di = 1$.
Enligt den euklidiska algoritmen får vi $SGD(m, d) = 1$, så vi har två heltal x, y där $mx + dy = 1$.
Detta betyder att $g^{mx+dy} = g \Leftrightarrow g^{mx}(g^d)^y = g$ men vi har $g^d = e \Leftrightarrow$
$g^{mx} = (g^m)^x = g$.
Vi ser här att g^m också är en generator för G.□

Exempel 9. Hitta antalet generatorer i $\mathbb{F}_{11}^*$och hitta alla generatorer till denna kropp.

För att veta hur många generatorer vi har använder vi Eulers $\varphi -$ funktion och sats 4:
$\varphi(11-1) = \varphi(10) = 10\left(1 - \frac{1}{2}\right).\left(1 - \frac{1}{5}\right) = 4$ så vi har 4 generatorer i $\mathbb{F}_{11}^*$.

Det är inte enkelt att hitta generatorerna för stora ändliga kroppar, men för $\mathbb{F}_{11}^*$ är det relativt enkelt. Det räcker att hitta en generator för att hitta de andra.

Vi börjar med 2:

$2^2 = 4 \pmod{11}$

$2^3 = 8 \pmod{11}$

$2^4 = 5 \pmod{11}$

$2^5 = 10 \pmod{11}$

$2^6 = 9 \pmod{11}$

$2^7 = 7 \pmod{11}$

$2^8 = 3 \pmod{11}$

$2^9 = 6 \pmod{11}$

$2^{10} = 1 \pmod{11}$

Så 2 är en generator till $\mathbb{F}_{11}^*$, eftersom vi kunde få alla heltal i $\mathbb{F}_{11}^*$. Nu hittar vi alla element i $\mathbb{F}_{11}^*$ som är relativt prima med $q-1=10$: $\{3,7,9\}$.

Enligt sats 4 är våra fyra generatorer: $2, 2^3, 2^7$ och 2^9.

3 Elliptiska kurvor

Denna del är hämtad från [K] och [W].

Elliptiska kurvor över ändliga kroppar har tillämpats för att lösa flera problem, bland annat bildning av kryptosystem. Inledningsvis kommer vi att beskriva dessa kurvor allmänt sett och sedan elliptiska kurvor över ändliga kroppar.

En elliptisk kurva *E* över en kropp $\mathbb{F}$ är en kurva som ges av följande ekvation:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \text{ där } a_i \in \mathbb{F}.$$

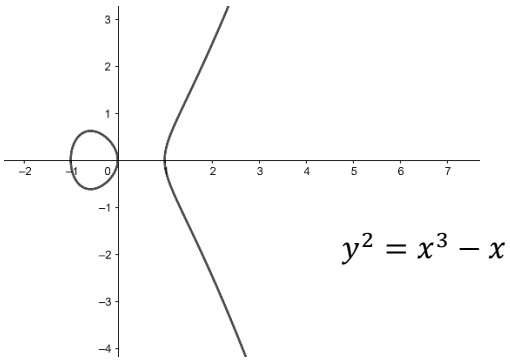
Om vi betecknar $E(\mathbb{F})$ som mängden av alla punkter $(x,y) \in \mathbb{F}^2$ och om vi definierar O som en punkt i oändligheten satisfierar föregående ekvation den så kallade *generella Weierstrass-ekvationen* för elliptiska kurvor. Vi kommer att studera *Weierstrass* ekvation på normalform som är:

$y^2 = x^3 + Ax + B$ där A, B är konstanter och $4A^3 + 27B^2 \neq 0$.

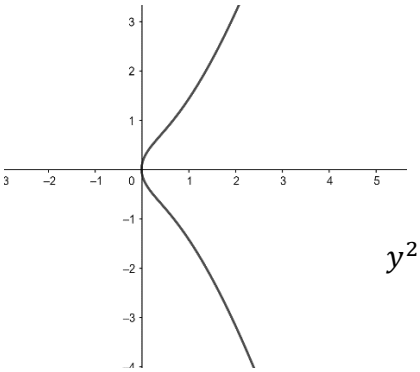
Elliptiska kurvor över till exempel reella tal har två grundformer, se graf 1. Den första formen $y^2 = x^3 - x$ har tre distinkta reella rötter och den andra $y^2 = x^3 + x$ har bara en reell rot och två komplexa rötter. Så vad händer om vi har en dubbel rot eller rötter som tillhör olika talmängder? Man tillåter inte detta genom villkoret $4A^3 + 27B^2 \neq 0$, som kommer från följande. Låt oss säga att vi har tre rötter r_1, r_2 och r_3. Då kan vi räkna ut diskriminanten

$\Delta = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2 = -(4A^3 + 27B^2)$.

Därför kan vi inte ha flera rötter som tillhör andra mängder, utan alla rötter måste vara distinkta.



$y^2 = x^3 - x$



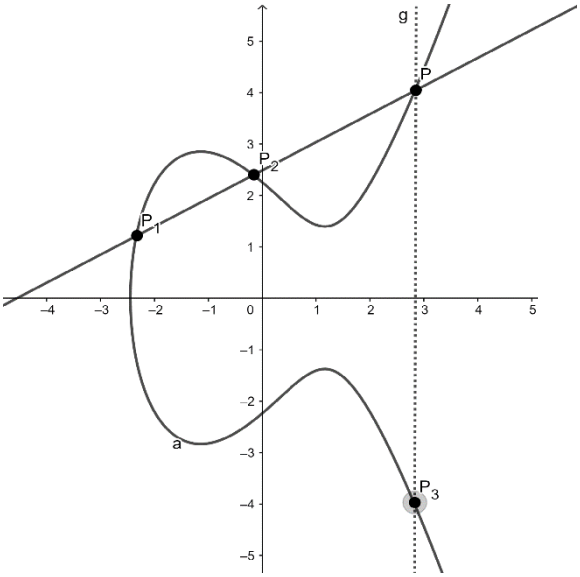
$y^2 = x^3 + x$

Graf (1).

3.1 Addition

Låt *E* vara en elliptisk kurva över de reella talen som uppfyller $y^2 = x^3 + Ax + B$. Låt $P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$ vara två punkter på *E*. Då definieras ytterligare en tredje punkt P_3 enligt följande:

Vi drar en rät linje h mellan P_1 och P_2 . Då skär linjen *E* i en punkt P_3', se graf 2. Vi speglar P_3' med avseende på $x-$ axeln. Spegelbilen av P_3' är den tredje punkten som definieras som $P_1 + P_2 = P_3$. För att kunna hitta P_3 måste vi hitta (x_3, y_3).



Graf 2

$y^2 = x^3 - 4x + 5$

Om vi först säger att $P_1 \neq P_2$ och att ingen är ∞ så vi får lutningen av h: $l = \frac{y_2 - y_1}{x_2 - x_1}$.

Om $x_1 \neq x_2$, då kan ekvationen för h skrivas som:
$y = l(x - x_1) + y_1 \Leftrightarrow y = lx + \beta$ där $\beta = y_1 - lx_1$. (1)

Nu vill vi hitta skärningen mellan *E* och h.

$(l(x - x_1) + y_1)^2 = x^3 + Ax + B \Leftrightarrow\ (lx + \beta)^2 = x^3 + Ax + B \Leftrightarrow$

$x^3 - l^2x^2 - 2lx\beta - \beta^2 + Ax + B = 0.$ (2)

Men vi vet redan att $P_1,\ P_2$ är rötter, alltså är x_1, x_2 kända. Eftersom vi arbetar med en kubisk ekvation vet vi att koefficienten framför x^2 är den negativa summan av rötterna, alltså:

$x_1 + x_2 + x_3 = l^2 \Leftrightarrow x_3 = l^2 - x_1 - x_2$ och $y_3 = l(x - x_1) + y_1$.

Detta är P_3' och vi behöver P_3. Vi speglar med avseende på $x-$ axeln och får

$x_3 = l^2 - x_1 - x_2$ och $y_3 = l(x_1 - x_3) - y_1$.

Om $x_1 = x_2$ men $y_1 \neq y_2$, är linjen mellan P_1och P_2 vertikal. Då skär den kurvan *E* i oändligheten. Om man speglar denna punkt med avseende på $x-$ axeln får man samma punkt. Därmed $P_1 + P_2 = \infty$.

I det tredje fallet har vi $P_1 = P_2 = (x_1, y_1)$. Detta betyder att vi bara har en punkt. Då är linjen som skär *E* en tangentlinje. Men här måste vi förutsätta att $y_1 \neq 0$, eftersom vi i så fall får $P_1 + P_2 = \infty$. För att få lutningen deriverar vi *E* och får:

$2y\frac{dy}{dx} = 3x^2 + A \iff l = \frac{dy}{dx} = \frac{3x_1^2+A}{2y_1}$, som sätts in i (1) och (2).

Det är nästan samma fall förutom att vi bara har en dubbelrot x_1. Då blir punkten $P_3 = (x_3, y_3)$ med $x_3 = l^2 - 2x_1$ och $y_3 = l(x_1 - x_3) - y_1$.

Definition 11. Låt *E* vara en elliptisk kurva definierad som $y^2 = x^3 + Ax + B$. Låt $P_1 = (x_1, y_1)$ och $P_2 = (x_2, y_2)$ vara två punkter på *E* sådana att $P_1, P_2 \neq \infty$. Definiera $P_1 + P_2 = P_3 = (x_3, y_3)$ som följer:

- Om $x_1 \neq x_2$, då är $x_3 = l^2 - x_1 - x_2$ och $y_3 = l(x_1 - x_3) - y_1$, där $l = \frac{y_2-y_1}{x_2-x_1}$.
- Om $x_1 = x_2$, men $y_2 \neq y_1$, då är $P_1 + P_2 = \infty$.
- Om $P_1 = P_2$ och $y_1 \neq 0$ då är:
  $x_3 = l^2 - 2x_1$ och $y_3 = l(x_1 - x_3) - y_1$ där $l = \frac{3x_1^2+A}{2y_1}$.
- Om $P_1 = P_2$ och $y_1 = 0$, då är $P_1 + P_2 = \infty$.
- Slutligen definierar man $P + \infty = P$ för alla $P \in E$.

Sats 5. Addition av punkter på en elliptisk kurva *E* har följande egenskaper:

a) Kommutativ: $P_1 + P_2 = P_2 + P_1$ för alla $P_1, P_2 \in E$.
b) Det finns ett enhetselement ∞ sådant att $P + \infty = P$ för alla $P \in E$.
c) Det finns en invers till varje punkt, det vill säga, det existerar $-P$ på *E* där $P + (-P) = \infty$.
d) Associativitet $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ för alla P_1, P_2 och $P_3 \in E$.

Med andra ord kan man säga att alla punkter på *E* formar en additiv abelsk grupp med ∞ som enhetselementet.

Bevis. a) Den första egenskap är enkel att bevisa. Linjen som går från P_1 till P_2 är samma linje som går från P_2 till P_1.

b) Enhetselmentet finns enligt definition 11.

c) Låt $P' = (x_1, -y_1)$ vara spegelbilden av $P = (x_1, y_1)$ med avseende på $x-$axeln, då gäller enligt definition 11 att $P + P' = \infty$.

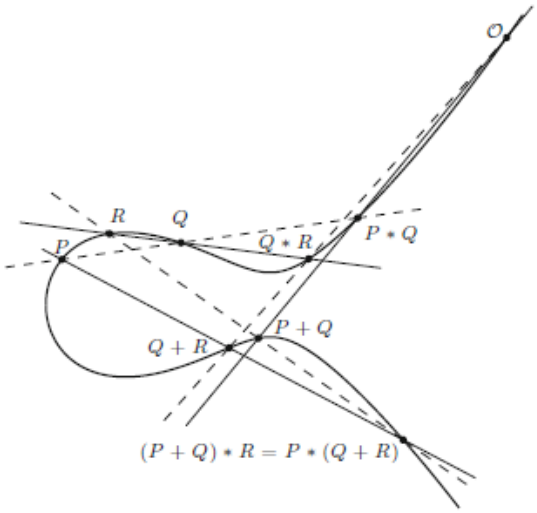
d) Eftersom beviset av associativitet med algebraiska metoder är långt och kräver mycket t förkunskaper än vad vi hittills presenteras kommer vi att presentera ett geometrisket bevis [ST].

Vi tar en elliptisk kurva *E* som uppfyller $y^2 = x^3 + Ax + B$, se graf 3[ST].

Vi börjar först med att konstruera $P + Q$ på följande sätt. Vi drar en linje från P till Q och som skär *E* i $P * Q$. Nu drar vi en linje från $P * Q$ till en punkt i oändligheten O. Nu får vi $P + Q$ som är skärningenspunktev mellan *E* och linjen mellan O och $P * Q$. Vi vill egentligen konstruera $(P + Q) + R$. För att addera $(P + Q)$ till R drar vi en linje från R

till $P + Q$. Skärningenspunkten mellan denna linje och E är $(P + Q) * R$. För att få $(P + Q) + R$ behöver vi dra en linje mellan $(P + Q) * R$ och O. Skärningen av denna linje med E är ju $(P + Q) + R$. För att bevisa att $(P + Q) + R = P + (Q + R)$ räcker det att visa att $(P + Q) * R = P * (Q + R)$.

För att konstruera $P * (Q + R)$ drar vi en linje mellan Q och R. Skärningspunkten mellan denna och E är $Q * R$. Om man drar en linje mellan $Q * R$ och O får man $(Q + R)$ som är på E. För att addera P till $(Q + R)$, drar vi först en linje mellan P och $(Q + R)$ då får man $P * (Q + R)$. Vi kan se att denna punkt har samma koordinater som $(P + Q) * R$. Om vi ”ansluter” denna punkt till O och sedan skär med E kommer vi att få samma punkt också, alltså: $(P + Q) + R = P + (Q + R)$. □



Graf 3

Exempel 10. Låt E: $y^2 = x^3 - 7x + 10$ vara en elliptisk kurva över $\mathbb{Q}$. Givet två punkter $P_1 = (x_1,\ y_1) = (1, 2)$ och $P_2 = (x_2,\ y_2) = (3, 4)$, hitta summan av $P_1 + P_2$.

Lösning:

$P_3 = P_1 + P_2 = (x_3,\ y_3)$.

$l = \frac{y_2 - y_1}{x_2 - x_1} = \frac{-2}{-2} = 1$.

$x_3 = l^2 - x_1 - x_2 = 1 \cdot 1 - 1 - 3 = -3$.

$y_3 = l(x_1 - x_3) + y_1 = 1 \cdot (1 + 3) - 2 = 2$.

$P_1 + P_2 = P_3 = (-3, 2)$.

3.2 Elliptiska kurvor över ändliga kroppar

Låt $\mathbb{F}_q$vara en ändlig kropp och låt E vara en elliptisk kurva som definieras över $\mathbb{F}_q$. Då är gruppen $E(\mathbb{F}_q)$ en ändlig grupp eftersom vi har en ändlig mängd av par (x, y) där $x, y \in \mathbb{F}_q$.

Denna grupp har viktiga egenskaper som är användbara i flera sammanhang, bland annat kryptering.

Exempel 11. Låt *E* vara elliptiska kurvan $y^2 = x^3 + 2x + 2$ över $\mathbb{F}_{17}$ och vi har *P* = (5,1) som en generator, vi vill lista ut alla punkter på *E* över $\mathbb{F}_{17}$.

Lösning:

Vi använder addition som är definierad i delavsnitt 3.1.

$2P = P + P = (5,1) + (5,1) = (x_3, y_3)$.

$l = \frac{3x_1^2 + A}{2y_1} = (2 \cdot 1)^{-1}(3 \cdot 5^2 + 2) = 2^{-1} \cdot 9 \equiv 9 \cdot 9 \equiv 13 \pmod{17}$

$x_3 = l^2 - 2x_1 \quad = 13^2 - 5 - 5 \equiv 6 \pmod{17}$.

$y_3 = l(x_1 - x_3) - y_1 = 13(5 - 6) - 1 = -14 \equiv 3 \pmod{17}$

Så vi har 2*P* = (6,3). Vi kan verifiera att denna punkt ligger på kurvan genom enkel substitution i ekvationen.

Om vi genomför denna process $\#E$ gånger, det vill säga ordning av *E*, får vi alla punkter på *E*. Genom vanliga uträkningar får vi:

2*P* = (5,1) + (5,1) = (6,3)	11*P* = (13,10)
3*P* = *2P* + *P* = (10,6)	12*P* = (0,11)
4*P* = (3,1)	13*P* = (16,4)
5*P* = (9,16)	14*P* = (9,1)
6*P* = (16,13)	15*P* = (3,16)
7*P* = (0,6)	16*P* = (10,11)
8*P* = (13,7)	17*P* = (6,14)
9*P* = (7,6)	18*P* = (5,16)
10*P* = (7,11)	19*P* = ∞
20*P* = 19*P* + *P* = *P*	21*P* = 2*P* ……

Observera att alla uträkningar utförs (mod 17). Detta betyder att $P = (5,1)$ är inversen till punkten 18*P*. Vi ser här att ordningen av $E(\mathbb{F}_{17})$ är 19.

3.2.1 Hasses sats

Låt *E* vara en elliptisk kurva över en ändlig kropp $\mathbb{F}_q$, då satisfierar kurvans ordning $\#E$ följande olikheter:

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

Bevis. Beviset av Hasses sats bygger på bland annat Frobenius endomorfism, Lagranges sats och Cayley-Hamiltons sats för linjär algebra. Därför hänvisas läsaren till kapitel 2 i [W].

Hasses sats konstaterar att antalet punkter på en elliptisk kurva över en ändlig kropp $\mathbb{F}_p$ cirka är *p.* Detta har viktiga implikationer i praktiken. Till exempel, om vi vill ha en elliptisk kurva med 2^{160} element måste vi ha en ändlig kropp över ett primtal av längden 160 bit.

3.2.2 Ordning av punkter på elliptiska kurvor

Låt $P \in E(\mathbb{F}_q)$. Ordningen av P är det minsta heltal k sådant att $kP = \infty$. Vi vet från Lagranges sats att ordningen av en punkt måste dividera ordningen av gruppen. Enligt Hasse sats ligger ordningen av en elliptisk kurva i ett intervall av längd $4\sqrt{q}$. Således om vi kan hitta en punkt av ordning större än $4\sqrt{q}$, då finns bara en multipel av denna ordning i det korrekta intervallet. Därmed måste denna multipel vara $\#E(\mathbb{F}_q)$.

Om ordningen av punkten skulle vara mindre än $4\sqrt{q}$ då får vi en kortare lista av möjligheter för $\#E(\mathbb{F}_q)$. Genom att använda sig av flera punkter kan man minska listan till en unik möjlighet för $\#E(\mathbb{F}_q)$. Vi hittar ordningen av en punkt genom en metod kallad*"baby step, giant step".*

Exempel 12. Låt *E* vara en elliptisk kurva definierad av $y^2 = x^3 + 7x + 1$ över $\mathbb{F}_{101}$. Vi har en punkt $P = (0,1)$ på kurvan som har ordning 116. Ordningen av *E* över $\mathbb{F}_{101} = \#E(\mathbb{F}_q)$ är en multipel av 116. Enligt Hasses sats får vi:

$101 + 1 - 2\sqrt{101} \leq \#E(\mathbb{F}_q) \leq 101 + 1 + 2\sqrt{101}.$

$82 \leq \#E(\mathbb{F}_q) \leq 122.$

I detta intervall har vi bara en multipel av 116, nämligen själva 116. Därmed är $\#E(\mathbb{F}_q) = 116.$

4 Elliptiska kurvor och kryptografi

Nedanstående del är hämtad från [W].

En naturlig fråga är varför vi använder elliptiska kurvor inom kryptering. Anledningen är att elliptiska kurvor tros erbjuda lika hög säkerhet som vanliga kryptosystem såsom *RSA*, men de använder färre bitar. Till exempel tros ge en nyckel av storlek 2096 bitar baserad på *RSA* samma säkerhetsnivå som en nyckel av 313 bitar baserad på en elliptisk kurva. Detta betyder att användning av elliptiska kurvor innebär mindre storlek på datachip, mindre energiförbrukning och är snabbare, för att nämna några fördelar.

4.1 Det diskreta logaritmproblemet

Låt *p* vara ett primtal och låt a, b vara heltal skilda från noll (mod *p*). Då vet vi att det finns ett heltal k sådant att: $a^k \equiv b \pmod{p}$.

Det diskreta logaritmproblemet är att hitta $k = log_p$. Till exempel, låt oss ta en kropp $\mathbb{F}_5^*$ och låt gruppens generator vara 2. Logaritmen av 1 är då 4 eftersom $2^4 \equiv 1 \pmod{5}$. Vi ser att det är enkelt för små primtal, men för stora primtal finns det inget effektivt sätt att hitta k. Då

kommer elliptiska kurvor till hjälp och problemet förmuleras på följande sätt. Givet en elliptisk kurva $E(\mathbb{F}_q)$ och en generator $G = (x, y) \in E(\mathbb{F}_q)$, hitta ett heltal k sådant att $kG = A$, där $1 \leq k \leq \#E(\mathbb{F}_q)$.

De krypteringssystem som vi ska gå genom bygger på det diskreta logaritmproblemet. Vi börjar med att presentera följande scenario. Alice vill skicka ett medelande till en annan person som heter Bob. För att skydda meddelandet från en eventuell hackare krypterar hon meddelandet och skickar det till Bob. Han avkrypterar texten för att läsa meddelandet. För detta använder Alice en krypteringsnyckel. Och Bob använder avkrypteringsnyckel. Båda nycklar måste vara hemliga för andra.

Det finns två sorters krypteringssystem: symmetriska så som *DES* och *AES,* vilka är opraktiska på grund av flera anledningar. Och asymmetriska så som *Diffie-Hellman*s nyckelutbyte och *ElGamal*.

4.2 Diffie-Hellmans nyckelutbyte

För att beskriva hur proceduren för Diffie-Hellmans nyckelutbyte går till, tar vi som vanligt Alice och Bob.

1- Alice och Bob kommer överens om en elliptisk kurva *E* över en ändlig kropp $\mathbb{F}_q$ sådan att det diskreta logaritmproblemet är svårt i $E(\mathbb{F}_q)$. De kommer också överens om en punkt $P \in E(\mathbb{F}_q)$ sådan att delgruppen som genereras av *P* har en stor ordning.
2- Alice väljer ett ”privat” heltal a. Sedan gör hon uträkningen $P_a = aP = A$ och skickar denna uträkning till Bob.
3- Bob väljer ett ”privat” heltal b och gör en uträkning $P_b = bP = B$ och skickar denna till Alice.
4- Alice beräknar $aP_b = abP$.
5- Bob beräknar $bP_a = baP$.
6- Alice och Bob använder en allmänt känd publik nyckel för att finna en nyckel från abP. Till exempel kan de använda 256 sista bitar av *x*-koordinaten av abP som den publika nyckeln. Till slut ser vi att både Bob och Alice har samma nyckel alltså $abP = baP$.

Övriga personer, till exempel en eventuell hackare, kan veta kurvan *E*, den ändliga kroppen $\mathbb{F}_q$, samt punkterna *P, A* och *B*. Om den eventuella hackaren vill se meddelandet måste hackaren ta reda på *abP*, detta betyder att lösa ut det diskreta logaritmproblemet, alltså att lösa *a* från *aP* eller *b* från *bP* men det finns inget effektivt sätt att göra det.

Exempel 13. Låt oss tillämpa proceduren med hjälp av exempel 11 med den elliptiska kurvan $y^2 = x^3 + 2x + 2$ över $\mathbb{F}_{17}$ där punkterna bildar en cyklisk grupp av ordning $\#E = 19$ och med generator *P* = (5,1).

Alice	Bob
$3P = A$	$10P = B$
Publika nyckeln $3P = (10,6)$	Publika nyckeln $10P = (7,11)$
Skickar *A* till Bob	Skickar *B* till Alice

$3B = 3(7,11) = (13,10)$ $10A = 10(10,6) = (13,10)$

Vi ser att båda får (13,10). Ett sätt att knäcka denna kryptering är att lösa det diskreta logaritmproblemet alltså lösa:

$a = log_p A$ (mod 17) eller $b = log_p B$ (mod 17).

4.3 Elgamal-kryptering med elliptiska kurvor.

Elgamal-kryptering är baserad på det diskreta logaritmproblemet. Den presenterades av Taher Elgamal år 1985. Idén ligger i att det hemliga meddelandet *M* betraktas som en punkt $M \in E(\mathbb{F}_q)$ på en elliptisk kurva.

Vi tar samma exempel som ovan med Alice och Bob.

Alice vill skicka ett meddelande till Bob. Först konstruerar Bob sin publika nyckel enligt följande:

- Väljer en elliptisk kurva över en ändlig kropp $E(\mathbb{F}_q)$. Han väljer sedan en punkt *P* (generator) på $E(\mathbb{F}_q)$;
- Väljer ett ”privat” heltal *s* och gör uträkningen $B = sP$.

Den elliptiska kurvan $E(\mathbb{F}_q)$, *P* och *B* är Bobs publika nycklar, medan *s* är Bobs privata nyckel.

När Alice vill skicka ett meddelande till Bob gör hon följande:

- Laddar ner Bobs publika nyckel;
- Väljer ett privat heltal k och gör uträkningen $M_1 = kP$;
- Gör uträkningen $M_2 = M + kB$, och sedan skickar hon M_1, M_2 till Bob; observera att M är Alices meddelande.

Bob kan nu läsa meddelandet genom att göra uträkningen $M = M_2 - sM_1$. Detta fungerar eftersom: $M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M$.

En eventuell hackare kan se Bobs publika nyckel och punkterna M_1, M_2. Om hackaren kan lösa det diskreta logaritmproblemet, då kan *P* och *B* användas för att lösa ut s och därmed M. Det är viktigt för Alice att använda olika k varje gång hon skickar ett meddelande till Bob. Annars kan hackaren observera att $M_1 = M_1'$ och då räknar ut $M_2' - M_2 = M' - M$, och därmed veta M'om *M* blir känt genom $M' = M - M_2 + M_2'$.

Exempel 14. Alice vill skicka ett meddelande till Bob representerat av punkten $P_m = (5, 1743)$. Bob väljer elliptiska kurvan $y^2 = x^3 + x + 19$ (mod 8831) och punkten $G = (3,7) \in E(\mathbb{F}_p)$. Vidare väljer han ett slumpmässigt heltal $s = 5$ och genomför uträkningen $B = 5(3,7) = (7335,7164)$ och gör det till en publik nyckel. Nu laddar Alice ned denna publika nyckel, väljer ett heltal $k = 4$ och gör två uträkningar:

$M_1 = k \cdot P = 4 \cdot (3,7) = (254,2386)$ och

$M_2 = P_m + kB = (5,1742) + 4(7335,7164) = (269,1803)$.

Nu skickar Alice M_1, M_2 till Bob.

Bob gör uträkningen $s \cdot M_1 = 5(254{,}2386) = (4217{,}7788)$

Sedan får han P_m genom att använda ekvationen $M = M_2 - s \cdot M_1 = (269{,}1803) + (4217, -7788) = (5, 1743)$.

4.4 Algoritm för digital signatur

Digitala signaturer är ett av de viktigaste kryptografiska verktygen. Nyttan av digitala signaturer sträcker sig från digitala certifikat för säker e-handel till undertecknanden av juridiska kontrakt. En digital signatur delar viss funktionalitet med en handskriven signatur. Särskilt tillhandahåller den en metod för att säkerställa att ett meddelande är giltigt för en användare.

Den ursprungliga versionen av algoritmen för digtala signatur DSA använder den multiplikativa gruppen i en ändlig kropp. Den senare versionen, som använder elliptiska kurvor, kallas för ECDSA. För att presentera hur man konstruerar ECDSA tar vi samma scenario med Alice och Bob.

Alice vill skriva under ett dokument. Alice väljer en elliptisk kurva $E(\mathbb{F}_q)$, sådan att $\#E(\mathbb{F}_q) = fr$, där r är ett stort primtal och f är ett litet heltal, ofta 1, 2 eller 4. Sedan väljer hon en generator $G \in (\mathbb{F}_q)$. Hon väljer ett ”privat” heltal a och gör uträkningen $Q = aG$. Alice gör $E(F_q)$, r, G, och Q publika.

För att signera meddelandet m gör hon som följer:

- Väljer ett slumpmässigt heltal k där $1 \leq k < r$ och gör uträkningen $R = kG = (x, y)$;
- Gör uträkningen $s = k^{-1}(m + ax) \pmod r$.

Det signerade dokumentet är (m, R, s). För att verifiera signaturen gör Bob följande:

- Räknar ut $u_1 = s^{-1}m \pmod r$, $u_2 = s^{-1}x \pmod r$;
- Räknar ut $V = u_1G + u_2Q$;
- Säkerställer att signaturen är giltig om $V = R$.

Om signaturen är giltig, då stämmer följande ekvation:

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R.$$

Exempel 15. Alice vill skicka ett meddelande som är signerat av ECDSA. Processen går enligt följande (som i exempel 11):

Alice väljer en elliptisk kurva $y^2 = x^3 + 2x + 2$ över $\mathbb{F}_{17}$ och tar G = (5,1) som en generator.

Hon väljer ett heltal $a = 7$ vilket ger $Q = 7(5,1) = (0,6)$.

Den publika informationen är dessa parametrar $E(\mathbb{F}_q)$, r= 19, G=(5,1), Q och f=1.

Nu signerar hon meddelandet m som är representerat av heltalet 13.

Hon väljer ett heltal $k = 10$ som ger $R = 10(5,1) = (7,11)$

Sedan räknar hon ut $s = 10^{-1}(13 + 7 \cdot 7) \equiv 10 \pmod{19}$.

Bob får det signerade dokumentet (m, (7,11), 10) från Alice.

För att verifiera att Alice var den person som skickade meddelandet gör Bob följande:

$u_1 = s^{-1}m = 10^{-1} \cdot 13 \equiv 7 \pmod{19}$

$u_2 = s^{-1}x = 2 \cdot 7 \equiv 14 \pmod{19}$

$V = u_1G + u_2Q = 7(5,1) + 14(0,6) = (0,6) + (10,6) = (7,11) = R$

Signaturen är således giltig.

5 Avslutning

Vi har härmed skrivit en kort introduktion till elliptiska kurvor över ändliga kroppar, samt hur dessa kan användas inom kryptering med några illustrerande exempel.

6 Referenser

[BD] Bisht, R. K. och Dhami, H. S., *Discrete Mathematics*. Oxford University Press, 2015.

[EG] Eriksson, K. och Gavel, H., *Diskret Matematik Fördjupning.* Studentlittratur, Lund, 2003.

[JA] Judson, T. W och Austin, S. F., *Abstract Algebra Theory and Applications.* Austin State University, 2013. http://abstract.ups.edu/download/aata-20130816.pdf . hämtades 2019-06-24.

[K] Koblitz, N., *Algebraic Aspects of Cryptography Algorithms and Computation in Mathematics*, 3. Springer-Verlag, Berlin, 1998.

[KW14] Kraft, J. S. och Washington, L. C., *Elementary number theory*. CRC Press LLC, 2014.

[KW18] Kraft, J. S. och Washington, L. C., *An Introduction to Number Theory with Cryptography*. CRC Press LLC, 2018.

[ST] Silverman, J. H. och Tate, J. T., *Rational Points on Elliptic Curves*. Springer International Publishing Switzerland, 2015.

[W] Washington, L. C., *Elliptic curves. Number theory and cryptography.* Second edition. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008.