Eötvös Loránd Tudományegyetem

Elliptikus görbék

Készítette:
Erdélyi Márton
II. évfolyam, Matematikus MSc

Témavezető:
Tóth Árpád

Budapest, 2011

Köszönetnyilvánítás

Szeretném megköszönni Tóth Árpádnak, hogy bevezetett a matematikának ebbe az érdekes és szép ágába, hogy megismertette velem ezt a konkrét kérdést, és tanácsait, útmutatását a megoldáshoz.

Köszönöm Zábrádi Gergelynek, hogy többször is, amikor elakadtunk, segített továbblépni.

Tartalomjegyzék

1. Bevezetés

Ebben a fejezetben az elliptikus görbék legalapvetőbb tulajdonságait foglalom össze, amik segítségével meg lehet fogalmazni a kérdést, amit a dolgozatban megoldunk. Ezen kívül írok arról, hogy milyen kriptográfiai módszerek adnak motivációt a probléma vizsgálatára.

1.1. Kriptográfiai motiváció

Az elliptikus görbék pontjain lehet definiálni egy Abel-csoport struktúrát ($(E, +)$-al jelöljük), aminek vizsgálata az utóbbi 30 évben kriptográfiai szempontból is hasznos feladat lett. Ugyanis az derül ki, hogy egy pont többszöröseit elég gyorsan ki lehet számolni, viszont "osztani" - adott $P, Q \in E$-re megtalálni a legkisebb n-t melyre $[n]P = P + P + \cdots + P = Q$, már ha van ilyen - úgy tűnik meglehetősen nehéz. Ez eléggé hasonlít arra a helyzetre, mint ami modulo p a hatványozással és diszkrét logaritmussal van. Így az RSA-hoz hasonlóan az elliptikus görbéken is lehet egy nyilvános kulcsú kódolást bevezetni, ezt ECC-vel szokták rövidíteni. ([16])

Hasonlóan a többi nyilvános kulcsú kódoláshoz, az ECC-ről sincs bizonyítva, hogy nem lehet gyorsan feltörni. Ennek ellenére széles körben alkalmazzák, többek között például az amerikai National Security Agency az ECC bizonyos változatait az ajánlott algoritmusok közé sorolta (NSA Suite B Cryptography), és engedélyezi top secret információk titkosításához. Adott erősségű kódoláshoz hasonló méretű testek fölött kell számolni mint a korábbi módszereknél, viszont a kulcsok mérete sokkal kisebb, és az eddigi tapasztalatok és próbálkozások azt mutatják, hogy jóval nehezebb feltörni.

A kód erőssége többek között azon múlik, hogy milyen a görbe csoportjának a szerkezete. Venni kell egy elliptikus görbét, a csoportjában egy torzióelemet és tekinteni az általa generált részcsoportot. Ezen már tényleg értelmes az osztási feladat. A legjobb az az eset, amikor a csoport maga ciklikus. Ha a test véges, meg lehet mutatni, hogy van olyan görbe ami ezt teljesíti, sőt hogy a görbék pozitív hányada ilyen. És így ha véletlenszerűen válogatunk a görbék között, akkor elég gyorsan találhatunk "jó" görbét.

[7]-ben ez be van bizonyítva, ha a karakterisztika legalább 5, ezt a bizonyítást visszük át a 2 karakterisztikájú esetre. Itt a helyzet több ponton is eltér a nagyobb karakterisztikájú esettől, főleg azért mert ekkor vad elágazás (wild ramification) is előfordulhat.

A végeredmény az alkalmazások szempontjából azért előnyösebb, mert

sokkal könnyebb és gyorsabb számítógépekre implementálni a kódolási algoritmust: rögzített N-re $\mathbb{F}_{2^N}$-ben az összeadást nagyon egyszerű, és egy primitív gyök segítségével a szorzás is gyorsan megy.

Tehát a célunk megszámolni hogy egy véges, 2 karakterisztikájú test fölött hány olyan elliptikus görbe van, aminek a csoportja - a nem sokára bevezetésre kerülő jelöléssel $(E_{\mathbb{F}}, +)$ - ciklikus. A fő eredményünk, hogy ha N elég nagy, páratlan szám, akkor a görbék egy pozitív hányada ilyen.

1.2. Elliptikus görbék csoportja

Az itt szereplő definíciók értelmességének és az állításoknak bizonyítása Joseph H. Silverman The Arithmetic of Elliptic Curves című könyvének [1] harmadik fejezetében megtalálható. A jelölések nagy része is ezzel a könyvvel van összhangban.

Legyen $\mathbb{F}$ test, algebrai lezártja $\overline{\mathbb{F}}$. $\mathbb{P}^n(\mathbb{F})$ az $\mathbb{F}$ fölötti n dimenziós projektív tér, H a homogén polinomjainak halmaza, $\overline{H}$ a $\mathbb{P}^n(\overline{\mathbb{F}})$ homogén polinomjai.

1.2.1. Definíció. $X \subset \mathbb{P}^n(\mathbb{F})$ $\mathbb{F}$ fölötti projektív algebrai halmaz $(X/\mathbb{F})$, ha $\exists f_1, f_2, \ldots, f_k \in H$ homogén polinomok, melyekre

$$X = \{x \in \mathbb{P}^n(\overline{\mathbb{F}}) | \forall i : f_i(x) = 0\}$$

Ez értelmes, mert a homogén polinomok nullhalmaza jól definiált $\mathbb{P}^n(\overline{\mathbb{F}})$-en. X $\mathbb{F}$-racionális pontjai $X_{\mathbb{F}} = X \cap \mathbb{P}^n(\mathbb{F})$.

1.2.2. Definíció. $\mathbb{F}$ fölött az elliptikus görbéknek nevezzük az olyan halmazokat, ami felírhatók a következő alakú (Weierstrass) egyenlettel, és még bizonyos értelemben simák (nem elfajulók):

$$E/\mathbb{F}: \quad F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0$$

Ahol F a görbét - mint projektív algebrai halmazt - definiáló homogén polinom. Ezt át lehet írni inhomogén alakra ($A^n = \{Z \neq 0\}$), akkor egy affin harmadrendű görbét kapunk egy extra, végtelen távoli ponttal (amit a homogén egyenlet [0:1:0] megoldásának felel meg). Jelöljük ezt a végtelen távoli pontot O-val.

A görbe pontjai az F megoldásai. Általában a megoldásokat az algebrai lezártban értjük, de van amikor csak $\mathbb{F}$ felettieket érdemes vizsgálni, ezeket $E_{\mathbb{F}}$-fel jelöljük.

Érdemes az alábbi mennyiségeket is bevezetni:

$b_2 = a_1^2 + 4a_2$ $\quad$ $c_4 = b_2^2 - 24b_4$

$b_4 = 2a_4 + a_1a_3$ $\quad$ $c_6 = b_2^3 + 36b_2b_4 - 216b_6$

$b_6 = a_3^2 + 4a_6$ $\quad$ $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$

$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ $\quad$ $j = c_4^3/\Delta$

Δ a görbe diszkriminánsa, és akkor nem elfajuló a görbe, ha $\Delta \neq 0$, j a j-invaránsa. Ha elfajuló, akkor két féle szingularitása lehet:

- ha $c_4 \neq 0$, akkor kettőspontja (node) van,
- ha $c_4 = 0$, akkor csúcsa (cusp).

Két különböző egyenlettel felírt görbét nem érdemes minden esetben megkülönböztetni, hiszen ha változókat lineárisan változtatjuk:

$$X = u^2X' + r, \qquad Y = u^3Y' + su^2X' + t,$$

akkor újra egy Weierstrass-egyenletet kapunk. Ismert, hogy $\overline{\mathbb{F}}$ fölött - tehát ha $r, s, t, u \in \overline{\mathbb{F}}$ lehet - ilyen lineáris izomorfizmus erejéig az elliptikus görbét meghatározza a j-invariánsa ([1], III/1.4,3.1). Másrészt tetszőleges j_0 értékre megadunk egy görbét, aminek a j invariánsa j_0. Tekintsük a következőket:

Ha $j_0 \neq 0, 1728$, akkor

$$E : f(X, Y, Z) = Y^2Z + XYZ - X^3 + \frac{36}{1728 - j_0}XZ^2 + \frac{1}{1728 - j_0}Z^3 = 0$$

Leellenőrizhető, hogy ennek j-invariánsa $j = j_0$, diszkriminánsa $\Delta = \frac{j_0^2}{(1728-j_0)^3}$. Tehát $j_0 \neq 0, 1728$-ra kaptunk egy j_0 j-invariánsú elliptikus görbét.

De a maradék értékekre is van:

Ha $j_0 = 0$, akkor $E' : \quad y^2 + y - x^3 = 0$, erre $j = 0$, $\Delta = -27$.

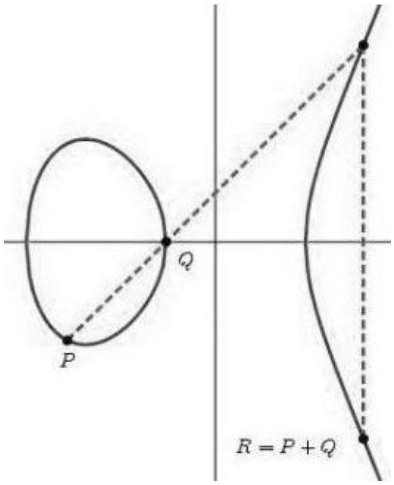
Ha $j_0 = 1728$, akkor $E'' : \quad y^2 - x^3 - x = 0$, erre $j = 1728$, $\Delta = -64$.

Ha $\mathrm{char}(\mathbb{F}) = 2, 3$, akkor $0{=}1728$, viszont az utolsó két görbéből pontosan az egyik nem szinguláris, tehát ebben az esetben is megkaptuk a hiányzó j-invariánsú görbét.

Így ha $\mathbb{F}$ véges, akkor $\overline{\mathbb{F}}$ feletti izomorfizmus erejéig $|\mathbb{F}|$ különböző elliptikus görbe van $\mathbb{F}$ felett.

1.3. Definíció. A görbe pontjain definiáljuk az alábbi kétváltozós műveletet:

Legyen $P, Q \in E$, L az őket összekötő egyenes (projektív értelemben, és ha $P = Q$, akkor az érintő). Legyen S az $E \cap L$ harmadik pontja, L' az S, O-t összekötő egyenes, $R = P + Q$ pedig $E \cap L'$ harmadik pontja. Ez jól definiált és $(E, +)$ Abel csoport. ([1] III/2.5, III/3.4)



Legyen $[m] : E \to E$ az a leképzés, melyre $[m]P = \overbrace{P + P + \cdots + P}^{m \text{ db}}$, $E[m] = \{P \in E | [m]P = O\}$ - azon pontok halmaza, melynek m-szerese O. Jelöljük $\mathbb{F}(E[m])$-el az $\mathbb{F}$-nek az m-torziópontok koordinátáival (az O-tól különböző pontok felírhatók $[x : y : 1]$ alakban) való bővítését.

1.2.4. Állítás. Ezt a műveletet le lehet írni a koordinátákkal is: Ha $P(x_1, y_1) \neq O$, akkor az inverze

$$-P(x_1, -y_1 - a_1 x_1 - a_3).$$

Az hogy az első koordináta ugyanaz, az szemléletesen is látszik a csoportművelet definíciójából: akkor lesz a végeredmény O, ha a tükörképe is, tehát ha a $P, -P$-n át húzott szelő "függőleges". Ebből a második koordináta értéke triviális számolással következik. Kicsit több munkával az is kijön, hogy ha $Q(x_2, y_2) \in E \setminus \{O\}$, $P \neq \pm Q$, akkor $P + Q = R$, $R(x_3, y_3) \in E \setminus \{O\}$-ra:

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1 \frac{y_2 - y_1}{x_2 - x_1} - a_2 - x_1 - x_2$$

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1} + a_1\right) x_3 + \frac{x_1 y_2 - x_2 y_1}{x_2 - x_1} - a_3$$

Ha P, $[2]P \neq O$, akkor $[2]P(x_3, y_3)$-ra:

$$x_3 = \frac{x_1^4 - b_4 x_1^2 - 2 b_6 x_1 - b_8}{4 x_1^3 + b_2 x_1^2 + 2 b_4 x_1 + b_6}$$

$$y_3 = -\left(\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} + a_1\right)x_3 + \frac{x_1^3 - a_4x_1 - 2a_6 + a_3y_1}{2y_1 + a_1x_1 + a_3} - a_3$$

Tehát látjuk hogy egy elliptikus görbén a csoportműveletet le lehet írni racionális törtfüggvényekkel. Így a $[d] : E \to E$ leképzés racionális, sőt a többszörözött pont első (X) koordinátája csak az eredeti első koordinátájától függ. Ezeknek az egyenleteit átalakítva létezik olyan $\psi^{[d]} \in \mathbb{F}[X]$ polinom, melyre

$$\psi^{[d]}(x) = 0 \iff \exists y : [x : y : 1] \in E[d] \setminus \{O\}$$

Ezeket az elliptikus görbe osztási (division) polinomjának nevezzük. Ha d páratlan, $(d, P) = 1$, akkor $\psi^{[d]}$ $(d^2 - 1)/2$ fokú polinom. ([2] VI. rész, 4. feladat)

2. Szita formula

2.1. Egy görbecsalád

Ebben a részben precízen is megfogalmazzuk a kérdésünket. Az összes lehetséges j-invariáns helyett egy szűkebb görbecsaládra tudunk majd jó becslést adni. Megmutatjuk hogy ha erre kihozzuk a kívánt eredményt, akkor az a természetesen feltett kérdésre is választ ad.

Mostantól csak véges, 2 karakterisztikájú testekkel foglalkozunk. Legyen $N \in \mathbb{N}$, $Q = 2^N$, $\mathbb{F} = \mathbb{F}_Q$ a Q elemű test. Jelöljük az egyik primitív harmadik egységgyököt $\omega \in \overline{\mathbb{F}}$-sal!

Az előbb felírtunk paraméteres egyenlettel az elliptikus görbéket, ez 2 karakterisztikájú esetben még egyszerűbb alakú is:

$$F(X,Y,Z) = Y^2Z + XYZ + X^3 + \frac{1}{j_0}Z^3 = 0$$

Ha ezt a paraméterezés használnánk, később kényelmetlen lenne mert projektív értelemben a $j_0 = \infty$-nél nem jól viselkedik. Ezért egy új görbecsaládot vezetünk be és ezt vizsgáljuk.

2.1.1. Definíció.

$$E(t)/\mathbb{F}: \quad F(X,Y,Z) = Y^2Z + tXYZ + YZ^2 + X^3 = 0$$

(Ez a Deuring-féle normál alak, [1] Appendix A/1.3) Ennek a megoldáshalmaza a $t^3 \neq 1$ esettől eltekintve egy elliptikus görbe, melyre kiszámolva a fent definiált paramétereket $b_2 = t^2$, $b_4 = t$, $b_6 = 1$, $b_8 = 0$, $c_4 = t^4$, $c_8 = t^6$, $\Delta = t^3 + 1$ és $j = t^{12}/(t^3+1)$. $\psi_t^{[d]}(x)$-k a hozzá tartozó osztási polinomok. Ezt néha érdemes lesz $\mathbb{F}(T)$ - a projektív egyenes függvényteste - felett nézni:

$$E(T)/\mathbb{F}(T): Y^2 + TXY + Y = X^3$$

Itt minden ugyanúgy megy mint az előbb, csak az osztási polinomjait tekinthetjük mint $\psi^{[d]} \in \mathbb{F}[X,T]$ kétváltozós polinomokat.

Így nem kapunk minden j-invariánsra elliptikus görbét, de egy pozitív hányaduk előáll:

2.1.2. Állítás.

$$\left|\left\{\frac{t^{12}}{t^3+1}\middle| t \in \mathbb{F}\right\}\right| > cQ$$

Az állítás általában $c = 1/12$-vel igaz. Ha N páratlan, akkor $c = 1/4$-del.

2.1.3. Megjegyzés. A továbbiakban fel fogjuk tenni azt, hogy N páratlan - ez pontosan akkor teljesül, ha $\omega \notin \mathbb{F}$. Később ezt több ponton is ki kell majd használjuk. Szerencsére kriptográfiai szempontból is ez az érdekes, ugyanis ha N összetett, akkor van módszer a kódok vártnál gyorsabb feltörésére. ("Weil descent attack", [17])

Bizonyítás. Ha $t^3 = 1$, akkor nem is elliptikus görbét kapunk. Elég tehát megmutatni, hogy $\forall \alpha \in \mathbb{F}$-re a $j(E(t)) = \alpha$-nak legfeljebb $1/c$ megoldása van $t \in \mathbb{F}$-ben, és van egy olyan α, amire kevesebb mint 9 - oda tesszük a rossz t értékeket.

$$\frac{t^{12}}{t^3+1} = \alpha \iff t^{12} + \alpha t^3 + \alpha = 0$$

Ennek minden α-ra legfeljebb 12 megoldása lehet. És az $\alpha = 0$-ra csak a $t = 0$ a megoldás.

Ha N páratlan, akkor $\omega \notin \mathbb{F}$ így csak egy rossz t érték van. Másrészt szintén $\omega \notin \mathbb{F}$ miatt az $x \mapsto x^3$ leképzés automorfizmus. Ezért bevezetve az $u = t^{1/3}$ jelölést, most az $u^4 + \alpha u + \alpha$ egyenlet megoldásait keressük. Az $\alpha = 0$-ra az egyenletnek most is egy megoldása van, ide téve a $t = 1$-t, a szigorú egyenlőtlenség most is kijön.

2.1.4. Definíció.

$$P(\mathbb{F}) = \frac{|\{t \in \mathbb{F} | (E_{\mathbb{F}}(t), +) \text{ ciklikus}\}|}{Q}$$

Ez valami olyasmit mér, amit szeretnénk: ha véletlenszerűen kiválasztunk egy görbét $\mathbb{F}$ felett (az $E(t)$ görbecsaládból, a véges sokból mindet ugyanakkora eséllyel), akkor $P(\mathbb{F})$ valószínűséggel lesz a csoportja ciklikus. Ebből kapunk valamit a véletlenül megválasztott j-invariánsra is:

2.1.5. Állítás. Jelöljük $P'(\mathbb{F})$-vel hogy ha egyenletesen eloszlással választunk egy $j_0 \in \mathbb{F}$-t, akkor mekkora annak a valószínűsége, hogy van olyan j_0 j-invariánsú elliptikus görbe, aminek csoportja ciklikus, c az előző állításban szereplő konstans. Ekkor $P'(\mathbb{F}) > c^2 P(\mathbb{F})$.

Bizonyítás. Ha j_0 olyan, hogy a j_0 j-invariánsú görbe előfordul az $E(t)$-k között, akkor legalább $cP(\mathbb{F})$ valószínűséggel ciklikus a csoportja, hiszen $QP(\mathbb{F})$ t értékre ciklikus, és így minden j_0-t legfeljebb $1/c$-szer számolunk. Legyen

$$A = \{j_0 \in \mathbb{F} | \exists t \in \mathbb{F} : j(E(t)) = j_0\}$$

Ekkor a feltételes valószínűségeket értelemszerűen jelölve, a triviális becslésekkel, a Bayes-tételből megkapjuk a kívánt állítást:

$$P'(\mathbb{F}) = P'(\mathbb{F}|j_0 \in A)P'(j_0 \in A) + P'(\mathbb{F}|j_0 \in \mathbb{F} \setminus A)P'(j_0 \in \mathbb{F} \setminus A) >$$

$$> cP(\mathbb{F}) \cdot c + 0 \cdot (1 - c) = c^2 P(\mathbb{F})$$

2.2. Szita formula

Mint sok más számelméleti kérdésnél, a mienknél is érdemes egy egyszerű szita formulát felírni $P(\mathbb{F})$-re. Ráadásul erről ki fog derülni, hogy a tagok nagy része eltűnik, így ha a maradék tagokra tudnánk egy jó becslést adni, abból egyszerűen kapnánk az egészre is.

2.2.1. Állítás. Legyen $d \in \mathbb{N}$, $N(d) = |\{t \in \mathbb{F} | Z_d \times Z_d \leq E_{\mathbb{F}}(t)\}|$, μ a Möbius-függvény. Ekkor

$$P(\mathbb{F}) = \frac{1}{Q} \sum_d \mu(d) N(d).$$

Bizonyítás. A kívánt állítást beszorozva Q-val:

$$|\{t \in \mathbb{F} | (E_{\mathbb{F}}(t), +) \text{ ciklikus}\}| = \sum_d \mu(d) N(d)$$

Egy $E_{\mathbb{F}}(t)$ csoport pontosan akkor nem ciklikus, ha van benne $Z_d \times Z_d$-vel izomorf részcsoport valamilyen $d > 1$ számra. Mert ha nem ciklikus, akkor van olyan H részcsoportja, ami pontosan 2 elemmel generált. De mivel $E_{\mathbb{F}}(t)$ Abel és véges, ezért ez $Z_a \times Z_b$ alakú ($a, b \in \mathbb{N}$). $(a, b) = 1$ nem lehet, mert akkor H már 1 elemmel is generálható lenne. Különben pedig tartalmaz $Z_{(a,b)} \times Z_{(a,b)}$-t részcsoportként. Ha pedig $E_{\mathbb{F}}(t)$ ciklikus, akkor nyilván nem tartalmaz $d > 1$-re $Z_d \times Z_d$-t.

Ha az $A, B \leq E_{\mathbb{F}}(t)$, $A \simeq Z_a \times Z_a$, $B \simeq Z_b \times Z_b$ és $(a, b) = 1$, akkor $< A, B >= A \times B \simeq Z_{ab} \times Z_{ab}$. Tehát $\{d | Z_d \times Z_d \leq E_{\mathbb{F}}(t)\}$ egy természetes szám osztóinak halmaza, így a Möbius inverziós formula épp a kívánt állítást adja.

Ez egy szokásos szita formula, és itt érdemes megjegyezni, hogy ezután csak a négyzetmentes d értékek érdekesek, különben $\mu(d) = 0$. Egy ilyen egyszerű szitával általában nem lehet pontos becsléseket végezni, mert nagyon sok tag szerepel az összegzésben, és az nem kezelhető jól. De ebben a konkrét helyzetben nem így van.

Ugyanis, ha $d \in \mathbb{N}$, $(\mathrm{char}(\mathbb{F}), d) = 1$, akkor $E_{\mathbb{F}}(t)[d] \simeq Z_d \times Z_d$. ([1] III/6.4) Tehát csak azt kell megvizsgálni, hogy mikor esik a teljes d-torzió $E_{\mathbb{F}}$-be. A Weil-pairing ([1] III/8) következményeként ha $E_{\mathbb{F}}(t)[d] \subset E_{\mathbb{F}}(t)$, akkor $\mathbb{F}$-ben benne vannak a d. egységgyökök, tehát $d | Q - 1$.

$E_{\mathbb{F}}(t)[\mathrm{char}(\mathbb{F})]$ ciklikus, így ha $\mathrm{char}(\mathbb{F}) | d$, akkor $Z_d \times Z_d \nsubseteq E_{\mathbb{F}}(t)[d]$.

Így már lényegesen kevesebb taggal kell foglalkozni, de még meg lehet mutatni néhányról, hogy eltűnik. Ugyanis egy elliptikus görbe pontjainak számát jól lehet becsülni, és ha meg tudjuk mutatni, hogy kevesebb mint d^2 pontja van, akkor $Z_d \times Z_d \nleq E_{\mathbb{F}}(t)$. A BSc-s szakdolgozatom második részében ezt a problémát vizsgáltam, de az ott elért eredmények 2 karakterisztikájú testekre nem adnak olyan korlátot, ami most kell. Viszont Hasse tétele szerint ([1] V/1.1)

$$|Q + 1 - |E_{\mathbb{F}}(t)|| \leq 2Q^{1/2}.$$

Így nem kell figyelembe venni azokat a d értékeket, melyekre $Q + 1 - d^2 < -2Q^{1/2}$, azaz $d > \sqrt{Q} + 1$. Tehát a következőt kaptuk:

2.2.2. Állítás.

$$P(\mathbb{F}) = \frac{1}{Q} \sum_{\substack{d | Q-1 \\ d \leq \sqrt{Q}+1}} \mu(d) N(d) = \frac{1}{Q} \sum_{\substack{d | Q-1 \\ d \leq \sqrt{Q}+1}} \mu(d) |\{t | \mathbb{F}(E(t)[d]) \leq \mathbb{F}\}|.$$

3. Jelölések

Ahhoz, hogy tudjunk mit kezdeni az előbbi eredménnyel, algebrai geometriai eszközöket fogunk használni. Ezért érdemes minden eddigi dolgot egy másik nézőpontból is megvizsgálni, és egyben új jelöléseket és definíciókat bevezetni. Ebbe a fejezetbe gyűjtöttem össze azokat a fogalmakat, amik nem közvetlen az elliptikus görbékkel kapcsolatban vannak definiálva. Ezek a definíciók nem csak $\mathbb{F}_{2^N}$-re értelmesek, legyen ismét $\mathbb{F}$ tetszőleges test.

3.1. Algebrai görbék

3.1.1. Definíció. Legyen $V/\mathbb{F}$ projektív algebrai halmaz, $\overline{A}^n \subset \mathbb{P}^n(\overline{\mathbb{F}})$ egy n dimenziós affin tér, melyre $V' = V \cap A^n \neq \emptyset$, és $A^n = \overline{A}^n \cap \mathbb{P}^n(\mathbb{F})$. $A^n[X] = A^n[X_1, X_2, \ldots, X^n]$ az A^n feletti polinomgyűrű, ugyanígy az algebrai lezárt felett $\overline{A}^n[X]$. V' ideálja

$$I(V') = \{f \in \overline{A}^n[X] | f(V') = 0\} \lhd \overline{A}^n[X], \qquad I(V'/\mathbb{F}) = I(V') \cap A^n[X]$$

V' affin (és V projektív) algebrai varietás, ha $I(V') \lhd A^n[X]$ prímideál.

Ekkor az affin koordinátagyűrűjük $\mathbb{F}[V] = A^n[X]/I(V/\mathbb{F})$ - ez egy integritási tartomány, függvénytestük $\mathbb{F}(V)$ ennek hányadosteste. Ugyanígy definiáljuk $\overline{\mathbb{F}}[V]$-t és $\overline{\mathbb{F}}(V)$-t.

Egy affin varietás koordinátagyűrűje és függvényteste nem függ $\overline{A}^n$ választásától. ([1] I/2)

3.1.2. Definíció. Legyen V algebrai varietás, függvényteste $\mathbb{F}(V)$, $K/\mathbb{F}(V)$ pedig egy Galois testbővítés. Ekkor $A = K \cap \overline{\mathbb{F}}$-et nevezzük a $K/\mathbb{F}(V)$ Galois-bővítés algebrai részének, és K/A-t a geometriainak. Hiszen ha ekkor vessszük $\mathbb{F}$-nek egy $\mathbb{F}'$ skalár (algebrai) bővítését, akkor $K\mathbb{F}'/A\mathbb{F}' \simeq K/A$ - a geometriai rész nem változik. Legyen $m_X = |\overline{\mathbb{F}} \cap \mathbb{F}(V) : \mathbb{F}|$ az algebrai bővítés foka.

3.1.3. Definíció. Ha V projektív algebrai varietás, akkor dimenziója $\overline{\mathbb{F}}(V)/\overline{\mathbb{F}}$ transzcendenciafoka. V projektív görbe, ha 1 dimenziós projektív algebrai sokaság.

$B \in V \cap \overline{A}^n$ $B[x_1 : x_2 : \cdots : x_n : 1]$ pont foka

$$\deg(B) = \left|\mathbb{F}(x_1, x_2, \ldots, x_n) : \mathbb{F}\right|$$

$B \in V \cap \overline{A}^n$ sima, ha az $(\partial f_i/\partial X_j(B))$ mátrix rangja $n - \dim(V)$ - ahol az f_i-k az 1.2. fejezetben a projektív algebrai halmaz definíciójában szereplő polinomok.

Mostantól legyen $C/\mathbb{F}$ sima projektív algebrai görbe.

3.1.4. Definíció. Ekkor ha $A \in C$ a görbe egy pontja, akkor legyen

$$\mathfrak{a} = \{f \in \mathbb{F}[C] | f(A) = 0\} \lhd \mathbb{F}[C]$$

$\mathfrak{a}$ egy prímideál, egy ponthoz az így konstruált prímideált általában is a pontnak megfelelő kis betűvel jelölöm. $\mathbb{F}[C]_A$ a lokalizált gyűrű, maximális ideálja M_A.

Ekkor minden A pontjára $\mathbb{F}(C)_A$ diszkrét értékelési gyűrű - angol rövidítéssel DVR. ([1] II/1.1) Így az

$$\mathrm{ord}_A(f) = \max\{d \in \mathbb{Z} | f/1 \in M_A^d\}, \qquad \mathrm{ord}_A(0) = \infty$$

jól definiált értékelés $\mathbb{F}[C]$-n, kiterjeszthetjük a hányadostestre is. Egy ν értékelésre $\{x \in \mathbb{F}(C) | \nu(x) > 0\}$ ν ideálja.

$t \in \mathbb{F}(C)$ uniformizáló elem A-nál, ha $\mathrm{ord}_A(t) = 1$.

Ha azokat az értékeléseket ekvivalensnek tekintjük, amiknek ugyanaz az ideáljuk, akkor egy ekvivalenciarelációt kapunk, az ekvivalenciaosztályokat placeknek hívjuk. Az algebrai görbe pontjai bijektíven megfeleltethetők $\mathbb{F}(C)$ placeinek: $A \in C \subset \mathbb{A}^n \longleftrightarrow \left[\mathrm{ord}_A\right]$.

3.1.5. Definíció. Legyen C divizor csoportja, $\mathrm{Div}(C)$ a C pontjai által generált szabad Abel csoport. Az $A \in C$-nek megfelelő csoportelemet jelöljük (A)-val. Ekkor

$$\forall D \in \mathrm{Div}(C) - \mathrm{re} \quad \forall P \in C \exists n_P \in \mathbb{Z} : D = \sum_{P \in C} n_P(P),$$

ahol ráadásul az n_P közül csak véges sok nem 0. Legyen

$$\deg(D) = \sum_{P \in C} n_P, \qquad \mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) | \deg(D) = 0\} \leq \mathrm{Div}(C).$$

Ha $f \in \overline{\mathbb{F}}(C)^*$, legyen

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Ez értelmes, $\mathrm{Div}^0(C)$-beli. ([1] II/3.1) Legyen $D_1, D_2 \in \mathrm{Div}(C)$ ekvivalensek ($D_1 \sim D_2$), ha $D_1 - D_2$ előáll $\mathrm{div}(f)$ alakban. Ez egy ekvivalenciareláció.

Vezessük be a következő részben rendezést $\mathrm{Div}(C)$-n:

$$D \geq 0 \iff \forall P \in C : n_P \geq 0, \qquad D_1 \geq D_2 \iff D_1 - D_2 \geq 0$$

Legyen

$$\mathcal{L}(D) = \{f \in \mathbb{F}^* | \mathrm{div}(f) \geq -D\} \cup \{0\}$$

Ez egy véges dimenziós $\overline{\mathbb{F}}$-vektortér, ha $D \leq 0$, akkor $\mathcal{L}(D) = \{0\}$. Ha $D_1 \sim D_2$, akkor $\mathcal{L}(D_1) \simeq \mathcal{L}(D_2)$. ([1] II/5.2)

Ekkor legyen $l(D) = \dim_{\overline{\mathbb{F}}}(\mathcal{L}(D))$.

C görbe g_C génuszát a Riemann-Roch tétel alapján definiálhatjuk:

3.1.6. Állítás. ([1] II/5.4) Ha C sima algebrai görbe, akkor van olyan $K_C \in \mathrm{Div}(C)$ - kanonikus divizor, és $g_C \in \mathbb{N}$ - génusz, melyre

$$\forall D \in \mathrm{Div}(C) : l(D) - l(K_C - D) = \deg(D) - g_C + 1$$

Ennek bizonyítása megtalálható például [3] IV/1-ben. C pontosan akkor elliptikus görbe, ha 1 génuszú sima projektív görbe ([1] III/3.1).

3.2. Görbék közti leképzések

3.2.1. Definíció. A $V, W \subset \mathbb{P}^n(\mathbb{F})$, a $\Psi : V \to W$ algebrai varietások közötti leképzés racionális, ha $\exists f_0, f_1, \ldots f_n \in \overline{\mathbb{F}}(V)$ hogy ahol értelmes ott

$$\Psi : B \mapsto [f_0(B) : f_1(B) : \cdots : f_n(B)].$$

Ψ reguláris $B \in V$-ben, ha $\exists g \in \overline{\mathbb{F}}(V) : \forall i : gf_i$ értelmes B-ben, és $\exists i : gf_i(B) \neq 0$. Ekkor legyen

$$\Psi(B) = [gf_0(B) : gf_1(B) : \cdots : gf_n(B)]$$

Ha X, Y algebrai görbék, Ψ racionális leképzés, akkor Ψ mindenütt reguláris ([1] II/2.1). És Ψ ekkor konstans vagy szürjektív ([3] II/6.8).

3.2.2. Definíció. Ψ sima, ha sima görbék közötti racionális leképzés. Ekkor legyen

$$\Psi^* : \mathbb{F}(Y) \to \mathbb{F}(X), f \mapsto f \circ \Psi$$

Ψ foka $[\mathbb{F}(X) : \Psi^*(\mathbb{F}(Y))]$. Ez véges ([3] II/6.8).

Ilyen helyzetben legyen $\mathbb{F}$ algebrai lezártja $\mathbb{F}(X)$-ben $\overline{\mathbb{F}}^X$. Továbbá $\Psi^*(\mathbb{F}[Y])$ egész lezártja $\mathbb{F}(X)$-ben $\overline{\Psi^*(F[Y])}$.

3.2.3. Definíció. Ha $\Psi : X \to Y$ sima, akkor legyen $A \in X$ elágazási (ramifikációs) indexe

$$e_\Psi(A) = \mathrm{ord}_A(\Psi^*(t_{\Psi(A)})),$$

ahol $t_{\Psi(A)} \in K(Y)$ egy uniformizáló elem $\Psi(A)$-nál. $B \in Y$ nem ágazik el Ψ-nél, ha $\forall A \in X, \Psi(A) = B : e_\Psi(A) = 1$. B szelíden elágazó (tamely ramified), ha $\mathbb{F}$ 0 karakterisztikájú, vagy

$$\forall A \in X, \Psi(A) = B : \mathrm{char}(\mathbb{F}[Y]/\mathfrak{b}) = \mathrm{char}(\mathbb{F}) \nmid e_\Psi(A),$$

különben B vadul elágazó (wildly ramified). Legyen

$$S_\Psi = \{B \in Y | B \text{ elágazó}\}, \text{ ekkor } |S_\Psi| = \sum_{B \in (Y_\mathbb{F} \cap S_\psi)} \deg B.$$

Ha $\Psi(A) = B$, akkor legyen A tehetetlenségi foka (inertial degree)

$$f_\Psi(A) = |\mathbb{F}(X)/\mathfrak{a} : \Psi^*(\mathbb{F}(Y))/\Psi^*(\mathfrak{b})|.$$

3.2.4. Definíció. Legyen Ψ olyan, mint eddig, és $\mathbb{F}(X)/\Psi^*(\mathbb{F}(Y))$ normális bővítés, $\mathfrak{b} \lhd \mathbb{F}[Y]$ olyan prímideál, amire $\Psi^*(B)$ nem ágazik el $\mathbb{F}(X)/\Psi^*(\mathbb{F}(Y))$-ben, $B \geq \Psi^*(A)$ prímideál $\mathbb{F}(X)$-ben.

$$D = \{\sigma \in \mathrm{Gal}(\mathbb{F}(X)/\Psi^*(\mathbb{F}(Y))) | \sigma A = A\}$$

D-t A/B dekompozíciócsoportjának nevezzük.

Ekkor $|D| = e_\Psi(A) f_\Psi(A)$.

3.2.5. Definíció. Ebben a helyzetben keletkezik a következő természetes leképzés:

$$D \to \mathrm{Gal}((\mathbb{F}(X)/\mathfrak{a})/(\Psi^*(\mathbb{F}(Y))/\Psi^*(\mathfrak{b})))$$

Ez izomorfizmus, mert B nem ágazik el ([4] IX.6). A jobb oldalon a véges test Galois csoportja van, ami ciklikus. Egy generátoreleme a $\Phi : x \mapsto x^{|\mathbb{F}(Y)/\mathfrak{b}|}$. Az ennek megfelelő D-beli elemet $\Phi_\Psi(A/B)$-vel jelöljük, és A/B Frobenius-automorfizmusának hívjuk.

Ez A-tól és B-től is függ, azonban triviális számolás mutatja, hogy

$$\forall \sigma \in \mathrm{Gal}(\mathbb{F}(X)/\Psi^*(\mathbb{F}(Y))) : \Phi_\Psi(\sigma A/B) = \sigma \Phi_\Psi(A/B)\sigma^{-1}$$

Tehát a Frobenius-automorfizmus konjugált osztálya nem függ attól, hogy A melyik B fölötti prímideál. $\Phi_\Psi(B)$ legyen ez a konjugált osztály, B Frobenius-konjugált osztálya. ([4] IX)

3.2.6. Definíció. Legyen $\pi(r) = |\{B \in Y | B \text{ nem ágazik el, } \deg(B) = r\}|$.

Ha $C \subset \mathrm{Gal}(\mathbb{F}(X)/\Psi^*(\mathbb{F}(Y)))$ egy konjugált osztály, akkor legyen

$$\pi_C(r) = |\{B \in Y | B \text{ nem ágazik el, } \deg(B) = r, \Phi_\Psi(B) = C\}|.$$

4. Előkészületek

A szita formula egy tagjában azokat a t-ket kellene megszámolni, amikre $Z_d \times Z_d \leq E(t)[d]$, azaz azon t-ket, melyre $\mathbb{F}(E(t))[d] \leq \mathbb{F}$. Ezt fogjuk még inkább átfogalmazni, és mindent előkészíteni az Csebotarev sűrűségi tétel használatára, aminek az általunk használt verzióját az utolsó fejezetben mondjuk és, és amivel majd ott a becslésünket végezzük.

4.1. A Frobenius-automorfizmus

A Csebotarev sűrűségi tétellel egy görbék közti sima leképzésnél egy adott Frobenius-konjugált osztályú pontok számát becsülhetjük meg. A következő részben definiáljuk a görbéket és a leképzést úgy, hogy a nekünk érdekes t értékek megfeleltethetők legyenek azon pontoknak, amiknek a Frobenius-konjugált osztálya az identitás.

4.1.1. Definíció.

$$X_0'(d) = \{(x,y,t) | [x:y:1] \in E(t)[d], \nexists m < d : [x:y:1] \in E(t)[m]\} \subset \overline{\mathbb{F}}^3$$

$X_0'(d)$ az $E(t)$ definiáló polinom és a szigorú d-torziópontokban eltűnő függvény közös affin nullhelyeinek halmaza.

Itt a definícióban racionális törtfüggvények vannak x, y, t-ben, az utóbbi: $\prod_{m|d}(\psi^{[d/m]})^{\mu(m)}$. Tehát $X_0(d)$ affin algebrai halmaz, legyen a projektív lezártja $X'(d)$. Tulajdonképen arra vagyunk kíváncsiak, hogy adott t_0-ra milyen pontjai vannak a $t = t_0$ síkon, ezért érdemes bevezetni a következőket:

4.1.2. Definíció. Legyen $T/\mathbb{F}$ a projektív egyenes, mint algebrai görbe $\mathbb{F}$ felett. És legyen

$$\pi_d' : X'(d) \to T, \qquad [X:Y:T:Z] \mapsto [T:Z]$$

Így majdnem $t \in T$ fölé kerül $E(t)$ d-torziója - attól eltekintve, amikor $E(t)$ elfajuló. Viszont $X'(d)$ nem egy sima görbe, a $T : T^3 = 1$, és a $Z = 0$ hipersíkokon szingularitásai lehetnek, π_d' nem sima leképzés. De az algebrai görbéknek meg lehet szüntetni a szingularitásait a következő értelemben ([6] VII. fejezet):

$\exists X(d)$ sima görbe $\mathbb{F}$ felett, $f : X(d) \to X'(d)$ racionális leképzés, melyre $X'(d)$ szinguláris pontjain kívül f izomorfizmus. Legyen $\pi_d = \pi_d' \circ f$.

4.1.3. Állítás. Ha $(d,P)=1$, akkor $X(d)$ sima projektív algebrai görbe $\mathbb{F}$ felett, $\pi_d : X(d) \to T$ racionális leképzés. Ha ℓ-el prímeket jelölünk, akkor

$$\deg(\pi_d) = |\{g \in Z_d \times Z_d | \nexists m < d : g^m = id\}| = d^2 \prod_{\ell|d} \Big(1 - \frac{1}{\ell^2}\Big).$$

Bizonyítás. Az első állítás nyilvánvaló. A fokszámra vonatkozó azért igaz, mert $Z_d \times Z_d$ d-rendű pontjait kell megszámolni, ez egyszerűen szitával:

$$\sum_{m|d} \mu(m) \Big(\frac{d}{m}\Big)^2 = d^2 \prod_{\ell|d} \Big(1 - \frac{1}{\ell^2}\Big)$$

Tehát véges sok T-beli ponton kivételével ennyi van egy fölött $X(d)$-ben. De ezek nem is elágazóak, így $\deg(\pi_d) = d^2 \prod_{\ell|d}(1 - 1/\ell^2)$. ([1] II/2.6)

4.1.4. Állítás. Ha $(\mathrm{char}(\mathbb{F}), d) = 1$, akkor

$$\mathbb{F}(E(j)[d]) \leq \mathbb{F} \iff \Phi_{\pi_d}((T-j)) = \{id\} \subset \mathrm{Gal}(\mathbb{F}(X(d))/\pi^*(\mathbb{F}(T)))$$

Bizonyítás. Legyen $A \in X(d), B \in T$. Ekkor $\pi_d(A) = B \iff \mathfrak{a} \lhd \mathbb{F}[X(d)]$, $\mathfrak{b} \lhd \mathbb{F}[T] : \pi_d(\mathfrak{a}) \subset \mathfrak{b}$, hiszen az A-ban eltűnő függvények B-ben eltűnőbe mennek. De ez pontosan akkor teljesül, ha $\mathfrak{a} \subset \pi_d^*(\mathfrak{b})$.

Így $\mathbb{F}(E(j)[d]) \leq \mathbb{F}$ pontosan akkor, ha van $\deg(\pi_d)$ különböző prímideál $\mathbb{F}[X(d)]$-ben, melyek részei $\pi_d^*((T-j))$-nek, azaz $\pi_d^*((T-j))$ teljesen szétesik $\mathbb{F}[X(d)]$-ben:

$$\pi_d^*((T-j)) = \mathfrak{a}_1 \mathfrak{a}_2 \dots \mathfrak{a}_k, \qquad k = \deg(\pi_d).$$

(Nem $\overline{\mathbb{F}}[X(d)]$-t nézzük, ott tudjuk hogy mindig van ennyi pont felette)

$\pi_d^*((T-j))$ teljesen szétesik, akkor

$$\forall j : e(\mathfrak{a}_j/\pi_d^*((T-j))) = 1, \qquad f(\mathfrak{a}_j/\pi_d^*((T-j))) = 1,$$

$$|D(\mathfrak{a}_j/\pi_d^*((T-j))| = e(\mathfrak{a}_j) f(\mathfrak{a}_j) = 1.$$

És ez nyilván fordítva is igaz, ha a dekompozíciócsoport triviális, akkor $\pi_d^*((T-j))$ teljesen szétesik. Végül

$$D(\mathfrak{a}_i/\pi_d^*((T-j))) = \{id\} \iff \Phi(\mathfrak{a}_j/\pi_d^*((T-j))) = id,$$

mert $\Phi(\mathfrak{a}_j/\pi_d^*((T-j)))$ generálja a dekompozíciócsoportot, tehát a Frobenius-automorfizmus pontosan akkor az identitás, ha a dekompozíciócsoport triviális.

4.1.5. Megjegyzés. Ha $j \neq 0$, akkor az hogy $\pi_d^*((T-j))$ teljesen szétesik $\mathbb{F}[X(d)]$-ben az ekvivalens azzal, hogy a $(T-j)$ ideál teljesen szétesik $\mathbb{F}[T](E(j)[d])$-ben. Mert legyen R $\mathbb{F}[T]$ algebrai lezártja $\mathbb{F}(T)(E(j)[d])$-ben, és tekintsük az alábbi struktúrát:

$$\begin{array}{ccccc} (T-j)R & \lhd & R & \leq & \mathbb{F}(T)(E(j)[d]) \\ | & & | & & | \\ (T-j)\mathbb{F}[T] & \lhd & \mathbb{F}[T] & \leq & \mathbb{F}(T) \end{array}$$

(Itt az alsó sorban egy gyűrű prímideálja és hányadosteste van, a felső sorban a hányadostest egy bővítése, abban a gyűrű egész lezártja, és ebben a prímideál által generált ideál) Erre π_d^*-t alkalmazva, a következőt kapjuk:

$$\begin{array}{ccccc} \pi_d^*((T-j))S & \lhd & S & \leq & \mathbb{F}(X(d)) \\ | & & | & & | \\ \pi_d^*((T-j)) & \lhd & \pi_d^*(\mathbb{F}[T]) & \leq & \pi_d^*(\mathbb{F}(T)) \end{array}$$

Ahol S $\pi_d^*(\mathbb{F}[T])$ egész lezártja $\mathbb{F}(X(d))$-ben. A jobb felső sarokban azért van így, mert $X_0'(d)$ sima ${\pi_d'}^{-1}(j)$ pontjaiban, tehát $X(d)$ helyett tekinthetjük $X_0'(d)$ j feletti részét, itt pedig az $\mathbb{F}(X(d))/\pi_d^*(\mathbb{F}(T))$ testbővítésnél pont a d-torziópontokat adjungáljuk. Viszont $\mathbb{F}[X(d)] \leq S$, és mivel $\pi_d^*((T-j))$ már $\mathbb{F}[X(d)]$-ben is szétesik, ezért S-ben is. Tehát $\pi_d^*((T-j))$ pontosan akkor esik teljesen szét $\mathbb{F}[X(d)]$-ben, ha a $T-j$ által generált ideál teljesen szétesik a megfelelő gyűrűben.

4.2. A torziópontok

A későbbiekben segítségünkre lesz, ha ismerjük $E_{\mathbb{F}(T)}(T)$ torziópontjait:

4.2.1. Állítás. Ha $2 \nmid N$, akkor az $E(T) : Y^2 + TXY + Y = X^3$ elliptikus görbének két torziópontja van $\mathbb{F}(T)$-ben, ezek a $(0,0), (0,1)$, rendjük 3.

Bizonyítás. Először megmutatjuk, hogy ha van torziópont, akkor az első koordinátája $\mathbb{F}[T]$-ben van. Ez általában is igaz (a Nagell-Lutz tétel egy

általánosított verziója), de char($\mathbb{F}$) = 2-re abban az esetben, amikor nincs 2-torzió, akkor nagyon egyszerűen kijön:

Ugyanis, 2-torzió tényleg nincs, mert akkor lenne, ha $a_1X + a_3 = TX + 1 = 0$, $X = T^{-1}$ lenne valamilyen (X, Y) megoldásra, tehát ekkor $Y^2 = T^{-3}$, ennek nyilván nincs megoldása $\mathbb{F}(T)$-ben. Tegyük fel hogy $P(X_0, Y_0) \in E(T)[d]$. Ekkor $X_0 = f/g$ ahol $f, g \in \mathbb{F}[T]$ relatív prímek. Tegyük fel, hogy $\exists r \in \mathbb{F}[T]$ irreducibilis, melyre $r|g$. Legyen ν_r az (r)-hez tartozó értékelés,

$$\nu_r(g) = \max\{n \in \mathbb{N} | r^n | g\}, \qquad \nu_r(X_0) = \nu_r(f) - \nu_r(g) < 0.$$

Tekintsük $[2]P \neq O$-t! A koordinátái legyenek (X_1, Y_1), ekkor mivel a karakterisztika 2, a pontkétszeresének első koordinátájára a képlet egyszerűbb:

$$X_1 = \frac{X_0^4 + b_4X_0^2 + b_8}{b_2X_0^2 + b_6}, \qquad \nu_r(X_1) = \nu_r(X_0^4 + b_4X_0^2 + b_8) - \nu_r(b_2X_0^2 + b_6) \leq$$

$$\leq 4\nu_r(X_0) - 2\nu_r(X_0) = 2\nu_r(X_0) < \nu_r(X_0).$$

Így azt kaptuk, hogy $[2]P$-nek "nagyobb" a nevezője, mint P-nek. De ez nem lehet, mert ha d páros akkor már egy kisebb d-re is kéne legyen nem $\mathbb{F}[T]$-beli torziópont. Ha d páratlan, akkor pedig mondjuk van olyan $P \in E(T)[d]$-t, amire $\nu_r(X_1)$ minimális, hiszen $E(T)[d]$ véges, ez ellentmondás.

Az $\mathbb{F}[T]$-beli torziót pedig könnyű megvizsgálni, mert ha $P \in E(T)[d]$, akkor az előbbiek szerint $[2P] \neq O$, viszont ugyanígy d-torzió. De erre a konkrét görbére ha $P(X_0, Y_0)$, akkor $[2]P$ első koordinátája:

$$\frac{X_0^4 + TX_0^2 + 0}{T^2X_0^2 + 1} = TX_0^2 + \frac{(T^3 + 1)X_0^4}{(TX_0 + 1)^2} \in \mathbb{F}[T]$$

Itt $(X_0, TX_0 + 1) = 1$, és mivel $\omega \notin \mathbb{F}$, $TX_0 + 1 | T^3 + 1 = (T + 1)(T^2 + T + 1)$. Így csak a következő esetek lehetnek ($\alpha \in \mathbb{F}^*$): Itt $(X_0, TX_0 + 1) = 1$, és mivel $\omega \notin \mathbb{F}$, $TX_0 + 1 | T^3 + 1 = (T + 1)(T^2 + T + 1)$. Ráadásul a konstans tag mindenhol 1, így csak a következő esetek lehetnek:

- $TX_0 + 1 = 1$. Ekkor $X_0 = 0$, tehát $X_0 = 0$, $Y_0 = 0, 1$, ezek a torziók.
- $TX_0 + 1 = T + 1$. Itt $X_0 = 1$, és például ha Y_0 konstansának együtthatója α, akkor $Y_0^2 + TY_0 + Y_0 = 1$, és itt a konstans tag együtthatója $\alpha^2 + \alpha = 1$, ennek viszont nincs megoldása, hiszen $2 \nmid N$.

- $TX_0 + 1 = T^2 + T + 1$. Ekkor $X_0 = T + 1$, és az előbbihez hasonlóan, a konstans tag miatt nincs megoldás.
- $TX_0 + 1 = T^3 + 1$. Most $X_0 = T^2$ és $Y_0^2 + T^3 Y_0 + Y_0 = T^6$. Itt a fokszámok miatt $\deg_T(Y_0) = 3$ kell legyen ha $Y_0 = \alpha T^3 + \beta T^2 + \gamma T + \delta$, de ekkor T^6 együtthatójára $\alpha^2 + \alpha = 1$, ami nem lehet.

4.3. A geometriai Galois-bővítés

Fontos lesz tudnunk, hogy ha az $X(d)$ az előbb definiált algebrai görbe, akkor mekkora az $\mathbb{F}(X(d))/\mathbb{F}$ testbővítés foka - ugyanis a Csebotarev sűrűségi tételben ez adja meg a becslés főtagját. Ebben a részben azt mutatjuk meg, hogy a geometriai Galois-bővítés szinte mindig maximális.

Legyen $E_0(T)/\mathbb{F}(T)$ felett egy elliptikus görbe, $K = \mathbb{F}(T)(E_0(T))$ az $E_0(T)$, mint $\mathbb{F}(T)$ feletti elliptikus görbe függvényteste. Így $\mathbb{F}(X(d)) \simeq K(E_0(T)[d])$. Csak $(\mathrm{char}(\mathbb{F}), d) = 1$-re kell vizsgálnunk, ebben az esetben a torzió $Z_d \times Z_d$. Így ha rögzítünk egy bázist, keletkezik egy természetes

$$\mathrm{Gal}(K(E_0(T)[d])/K) \to \mathrm{GL}_2(Z_d)$$

leképzés: minden automorfizmushoz azt rendeljük, hogy az adott bázisban hogyan permutálja a torziópontokat. Ez nyilván egy beágyazás, $\mathbb{F}(T)(E_0(T)[d])$ definíciója szerint.

Ekkor a Weil-pairing szerint az algebrai Galois-bővítés

$$K(E_0(T)[d]) \cap \overline{\mathbb{F}} = \mathbb{F}(\omega_d),$$

ahol ω_d primitív d. egységgyök és így a geometriai Galois-csoport fixen hagyja a $\mathrm{GL}_2(Z_d)/\mathrm{SL}_2(Z_d)$ mellékosztályokat. ([1] III/8.1.1). Így keletkezik a következő diagram egzakt sorokkal, és lefelé beágyazásokkal:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H(E_0) & \longrightarrow & G(E_0) & \longrightarrow & < q > & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{SL}_2(Z_d) & \longrightarrow & \mathrm{GL}_2(Z_d) & \stackrel{\det}{\longrightarrow} & Z_d^* & \longrightarrow & 1 \end{array}$$

Ahol $G(E_0) = \mathrm{Gal}(K(E_0(T)[d])/K)$, és a geometriai Galois csoport

$$H(E_0) = \mathrm{Gal}(K(E_0(T)[d])/(K(E_0(T)[d]) \cap \overline{\mathbb{F}})).$$

Igusa megmutatta, hogy ha $(\mathrm{char}(\mathbb{F}), d) = 1$, akkor az eredeti paraméterezésű görbecsaládban a geometriai Galois-csoport maximális ([9], 3. tétel):

4.3.1. Állítás. Ha $(d, \mathrm{char}(\mathbb{F})) = 1$, és $E'(J)/\mathbb{F}(J)$ egy J j-invariánsú görbe, akkor $H(E'(J)) \simeq \mathrm{SL}_2(Z_d)$, és így

$$|H(E'(J))| = |\mathrm{SL}_2(Z_d)| = \frac{1}{d^3 \prod_{\ell|d} \left(1 - \frac{1}{\ell^2}\right)}$$

Feltehetjük, hogy $G(E'(J)) = 1$, hiszen $\mathbb{F}$ helyett tekintve egy véges, konstans bővítését ilyet kapunk, és ekkor a geometriai Galois-csoport nem változik.

4.3.2. Következmény. Ha d_1, d_2 olyan, hogy $(d_1, \mathrm{char}(\mathbb{F})) = (d_2, \mathrm{char}(\mathbb{F})) = (d_1, d_2) = 1$, akkor

$$\mathbb{F}(J)(E'(J)[d_1]) \cap \mathbb{F}(J)(E'(J)[d_2]) = \mathbb{F}(J).$$

Mert ekkor nyilván

$$\mathbb{F}(J)(E'(J)[d_1])\mathbb{F}(J)(E'(J)[d_2]) \subset \mathbb{F}(J)(E'(J)[d_1 d_2]),$$

és az előző állítás szerint a fokszámok $\mathbb{F}(J)$ felett $|\mathrm{SL}_2(Z_{d_1 d_2})| = |\mathrm{SL}_2(Z_{d_1})||\mathrm{SL}_2(Z_{d_2})|$, tehát fönt egyenlőség van, és a metszet 1 fokú $\mathbb{F}(J)$ felett.

4.3.3. Állítás. Ha $2 \nmid N$ és $(6, d) = 1$, akkor $H(E(T)) \simeq \mathrm{SL}_2(Z_d)$.

Bizonyítás. Legyen $E'(J)/\mathbb{F}(J)$: $Y^2 + XY = X^3 + J^{-1}$. Ez 2 karakterisztikában az 1.2-beli egyenlet, itt $b_2 = 1$, $b_4 = b_6 = 0$, $b_8 = J^{-1}$.

A mi paraméterezésünkkel az $E(T)$ görbét úgy kapjuk, hogy $J = \frac{T^{12}}{T^3+1}$. Ráadásul ha $2 \nmid N$, akkor bevezetve az $U = T^{1/3}$ változót (ezt lehet mivel ekkor $X \mapsto X^3$ automorfizmus), továbbá α-val jelölve a $0 = U^4 + JU + J$ egy megoldását, $\mathbb{F}(T) = \mathbb{F}(J)(\alpha)$. Ez egy véges bővítése $\mathbb{F}(J)$-nek így az előbbi következmény szerint ha véges sok kivételes prím nem osztja d-t, akkor

$$\mathbb{F}(T) \cap \mathbb{F}(J)(E'(J)[d]) = \mathbb{F}(J).$$

De $\overline{\mathbb{F}}$ felett $E'(J)$ és $E(T)$ izomorfak, így geometriai Galois-csoport majdnem mindig maximális.

Láttuk, $E(T)$-nek konstans 3-torziója van, ezért azt várnánk, hogy az $\ell = 3$ egy kivételes prím. Ennél többet fogunk megmutatni, azt hogy $\mathbb{F}(T) \subset \mathbb{F}(J)(E'(J)[3])$, ebből már következik az állítás.

Számoljuk ki $E'(J)$-re $\psi^{[3]}$-t: Legyen $P(X,Y) \in E'(J) \setminus \{O\}$, ekkor $Q(X',Y') = [2]P$-re

$$X' = \frac{X^4 - b_4X^2 - 2b_6X - b_8}{4X^3 + b_2X^2 + 2b_4X + b_6} = \frac{X^4 + J^{-1}}{X^2}$$

És P akkor 3-torzió, ha $Q = -P$. De mivel $Q \neq P$, és mivel $-P$ első koordinátája ugyanaz mint P-é , ez pontosan akkor igaz ha $X' = X$, tehát

$$X = \frac{X^4 + J^{-1}}{X^2}, \qquad \psi^{[3]}(X) = X^4 + X^3 + J^{-1} = 0$$

Bevezetve az $U = X^{-1}$ jelölést és átrendezve: $U^4 + JU + J = 0$. Még csak a torziópontok első koordinátáit adjungáltuk, és máris kijött hogy

$$\mathbb{F}(T) = \mathbb{F}(\alpha) \subset \mathbb{F}(J)(E'(J)[3]).$$

4.3.4. Következmény. Ha $d|Q-1$, akkor

$$\frac{m_{X(d)}}{|G|} = \frac{1}{|\mathrm{SL}_2(Z_d)|}$$

Mert $(6,d) = 1$, és ez pont a geometriai Galois-bővítés fokának reciproka.

4.4. Az elliptikus fibrálás

Ahhoz hogy jól tudjuk becsülni a hibatagot a Csebotarev sűrűségi tételben, meg kell érteni hogy mi történik $X'(d)$ szinguláris ponjaiban. Ebben a részben azt látjuk be, hogy a mi görbecsaládunkban csak sima vagy multiplikatív redukciójú görbe van, így a π_d-nél csak szelíd elágazás van.

4.4.1. Definíció. Legyen

$$X'_0 = \{(x,y,t) | [x:y:1] \in E(t)\} \subset \overline{\mathbb{F}}^3$$

Ez az $X_0'(d)$-hez hasonlóan egy affin algebrai varietás, a projektív lezártját jelöljük X'-vel, és legyen

$$\pi' : X' \to T, \qquad [X : Y : T : Z] \mapsto [T : Z]$$

Most π'-nél minden lehetséges j-invariáns fölé tesszük az egész elliptikus görbét, ami bizonyos helyeken elfajuló is lehet. Az ilyen a helyzetet nevezik elliptikus fibrálásnak.

4.4.2. Definíció.

$$E(T)/\mathbb{F}(T) : Y^2 + TXY + Y = X^3$$

A szokásos elliptikus görbe, csak most $\mathbb{F}(T)$ - a projektív egyenes függvénytesteste - felett, B egy pontja T-nek, ν_B a hozzá tartozó értékelés, $\mathbb{F}(T)_B$ a lokalizált gyűrű, M_B maximális ideállal, legyen $K_B = \mathbb{F}(T)_B/M_B$ a hányadostest.

Legyen E^B/K_B az $E(T)$ elliptikus görbe ν_B szerinti redukciója, azaz

$$E^B : \quad Y^2 + XY = X^3 + (T + M_B)$$

- Ha E^B nem elfajuló elliptikus görbe ($\Delta(E^B) \neq 0$), akkor ν_B szerint jó a redukciója,
- Ha E^B kettőspontja van ($c_4(E^B) \neq 0$), akkor ν_B szerint multiplikatív a redukciója,
- Ha E^B csúcsa ($c_4(E^B)$ is 0), akkor ν_B szerint additív a redukciója.

Ezeket meg lehet csinálni általában egy $E/\mathbb{F}$ elliptikus görbére $\mathfrak{a} \lhd \mathbb{F}[E]$ prímideállal. Az elnevezések azért természetesek, mert a fenti jelölésekkel az E-től örökölt additív struktúra E^B nem szinguláris pontjain a multiplikatív redukció esetén izomorf $\mathbb{F}[E]_B/M_B$ multiplikatív csoportjával, az additív esetben az additív csoporttal. ([1] VII/5.1)

4.4.3. Állítás. Ekkor E^B pontosan a $\pi' : X' \to T$ elliptikus fibrálás B pontja feletti fibrum. Továbbá

- ha $B \neq [1 : 1], [\omega : 1], [\omega^2 : 1], [1 : 0]$, akkor E^B nem elfajuló elliptikus görbe,

- ha $B = [1:1], [\omega:1], [\omega^2:1]$, vagy $[1:0]$, akkor E^B szinguláris, és multiplikatív a redukció.

Bizonyítás. Ha $B \neq [1:0]$, és a B-nek megfelelő prímideál $\mathfrak{b} = (t_B)$, ahol $t_B \in \mathbb{F}[T]$ irreducibilis, akkor

$$f, g \in \mathbb{F}[T]: \quad \nu_B(f/g) = \max\{m \in \mathbb{N} |\ t_B^m | f\} - \max\{m \in \mathbb{N} |\ t_B^m | g\}$$

Legyen t_B egy gyöke $\beta \in \overline{\mathbb{F}}$. Ekkor

$$K_B \sim \mathbb{F}(\beta),\ T + M_B \sim \beta,\ \ E^B : Y^2 + \beta XY + Y = X^3,$$

ami pont a $\pi'(B)$ feletti fibrum. És ekkor $B = [1:0]$-ban is innét kapható a fibrum.

Ha B nem a fönti 4 kivételes pont egyike, akkor E^B nem elfajuló.

Ha $B = [\omega^\alpha : 1]$, akkor $c_4(E^B) = \omega^{4\alpha} \neq 0$, ez kellett.

Ha $B = [1:0]$, akkor legyen $T' = 1/T$ és szorozzuk be az egyenletet T'^6-nal, ekkor kicsit átalakítva

$$(T'^3 Y)^2 + (T'^3 X)(T'^2 Y) + T'^3 (T'^3 Y) = (T'^2 X)^3$$

Bevezetve az $X' = T'^2 X$, $Y' = T'^3 Y$ jelölést:

$$Y'^2 + X'Y' + T'^3 Y' = X'^3,$$

amire kiszámolva $b_2 = 1$, $b_4 = T'^3$, $b_6 = T'^6$, $b_8 = 0$, $c_4 = c_6 = 1$, $\Delta = T'^{12} + T'^9$, tehát E^B szinguláris, és a redukció csak multiplikatív.

4.4.4. Következmény. Mivel a szinguláris pontokban a redukció multiplikatív, a testbővítés szelíden elágazó. ([2] X/10.2)

4.4.5. Megjegyzés. Általában igaz, hogy egy véges testbővítéssel el lehet érni, hogy mindenhol vagy jó, vagy multiplikatív redukció legyen ([1] VII/5.4)

Az elliptikus fibrálások szinguláris pontjainak (amik fölött elfajuló elliptikus görbe van) szerkezetéről 0 karakterisztikájú esetben Kodaira, ez alapján általánosan Mumford teljes leírást adott ([10],[11]), ami szerint egy szinguláris pont véges sok féle lehet, és ezeket különböző módokon rendszerezve a típusát a szingularitás Kodaira vagy Néron szimbólumának nevezzük. (a típusok összefoglaló leírása megtalálható például [2] IV/9-ben)

Ennek segítségével az additív redukciójú esetben, testbővítések nélkül is lehet valamit mondani a vad elágazásról.

5. Csebotarev sűrűségi tétel

5.1. Csebotarev sűrűségi tétel

Most már csak be kell helyettesíteni a Csebotarev sűrűségi tételbe az eddigi eredményeinket, és azonnal kijön a becslés a szita formulában szereplő tagokra. A Csebotarev sűrűségi tétel következő változatát fogjuk használni (lásd [8]):

5.1.1. Állítás. Legyen $\Psi : X \to Y$ sima leképzés $\mathbb{F}$ feletti görbék között, $r \in \mathbb{N}$. $G = \mathrm{Gal}(\mathbb{F}(X)/\Psi^*(\mathbb{F}(Y)))$, $C \subset G$ egy konjugált osztály, melynek a megszorítása $\overline{\mathbb{F}}^X$-re Φ^r, ahol $\Phi : x \mapsto x^{\mathrm{char}(\mathbb{F})}$, a test Frobenius automorfizmusa. Ekkor

$$\left|\pi_C(r) - m_X \frac{|C|}{|G|}\pi(r)\right| \leq 2|C|^{1/2}\left((3g_Y + (\rho_\Psi + 1)|S_\Psi|)\frac{Q^{r/2}}{r} + \frac{|S_\Psi|}{r}\right) + |S_\Psi|$$

Ahol ρ-t a következő módon definiáljuk: Legyen tetszőleges $B \in S_\Psi$, $A \in X$: $\Psi(A) = B$-re A elágazási indexe e,

$$L = (\mathbb{F}(X)/\mathfrak{a}), \qquad K = \Psi^*(\mathbb{F}(Y))/\Psi^*(\mathfrak{b}).$$

Ha L/K vadul elágazó, akkor $\exists 1 \leq j < e : \nu(\mathcal{D}_{L/K}) \equiv -j - 1 (\mathrm{mod}\ e)$, legyen ekkor $\rho_{B/A} = \rho_A = (\nu_L(\mathcal{D}) - j - 1)/e$, ahol $\mathcal{D}_{L/K}$ az L/K testbővítés diszkriminánsa, ν_L pedig a megfelelő értékelés. Ha L/K szelíden elágazó, akkor pedig legyen $\rho_{B/A} = \rho_A = 0$. Végül

$$\rho_\Psi = \max\{\rho_B | B \in S_\Psi\}.$$

5.1.2. Következmény.

$$\left||\{j|\mathbb{F}(E(j)[d]) \leq \mathbb{F}\}| - \frac{Q}{|\mathrm{SL}_2(Z_d)|}\right| \leq 16Q^{1/2} + 20$$

Bizonyítás. Ehhez nincs más hátra, mint hogy összerakjuk az eddigi eredményeinket. Az előbbi tételt alkalmazzuk $\Psi = \pi_d$, $r = 1$, $C = \{id\}$-re.

Ekkor $g_Y = 0$,

$$\pi_C(1) = |\{j|\mathbb{F}(E(j)[d]) \leq \mathbb{F}\}|, \qquad \pi(1) = Q$$

A geometria Galois-bővítés maximalitása miatt $m_X/|G| = 1/|\mathrm{SL}_2(Z_d)|$.

$|S_{\pi_d}| = 4$, mert csak az $[\omega^n : 0], [0 : 1] \in T$ pontokban volt elágazás. Az $\mathbb{F}(T)(E(T)[d])/\mathbb{F}(T)$ testbővítés mindenhol szelíden elágazó, tehát $\rho_{\pi_d} = 0$. Ezeket beírva a kívánt állítást kapjuk.

5.2. A végeredmény

Végül a szita formula tagjainak becsléséből kapunk egy konstans alsó becslést $P(\mathbb{F})$-re.

Az jött ki, hogy ha $Q = 2^N$ elég nagy (pl N>3), akkor

$$\left| |\{j|\mathbb{F}(E(j)[d]) \leq \mathbb{F}\}| - \frac{Q}{|\mathrm{SL}_2(Z_d)|} \right| \leq 20Q^{1/2}$$

Ezt beírva a 2.2. rész végén kapott szita formulába:

$$\left| P(\mathbb{F}) - \sum_{\substack{d|Q-1 \\ d\leq\sqrt{Q}+1}} \frac{\mu(d)}{|\mathrm{SL}_2(Z_d)|} \right| \leq 20Q^{-1/2} \sum_{\substack{d|Q-1 \\ d\leq\sqrt{Q}+1}} |\mu(d)| \leq 20Q^{-1/2} \sum_{\substack{d|Q-1 \\ |\mu(d)|=1}} 1$$

5.2.1. Állítás.

$$\forall \varepsilon > 0 : \quad \sum_{\substack{d|n \\ |\mu(d)|=1}} 1 = \mathcal{O}(n^{\varepsilon})$$

Bizonyítás. Legyen $P(n)$ az n prímosztóinak halmaza, $p(n) = |P(n)|$. Ekkor

$$\sum_{\substack{d|n \\ |\mu(d)|=1}} 1 = \sum_{H\subset P(n)} 1 = 2^{p(n)}$$

Továbbá legyen $\pi(m) = |\{\ell < m\}|$, az m-nél kisebb prímek száma. Ekkor nyilván

$$\forall m \in \mathbb{N}, m > 1 : \quad p(n) < \pi(m) + \frac{\log n}{\log m},$$

$$\sum_{\substack{d|n\\|\mu(d)|=1}} 1 \le 2^{\pi(m)+\frac{\log n}{\log m}} = k(m)n^{\log 2/\log m} = \mathcal{O}(n^{\log 2/\log m}),$$

ahol $k(m)$ m-től függő konstans. m-et elég nagyra, pl $m > 2^{1/\varepsilon}$-nak választjuk, akkor megkapjuk az állítást.

5.2.2. Következmény. Nekünk ez azt jelenti hogy

$$P(\mathbb{F}) = \sum_{\substack{d|Q-1\\d\le\sqrt{Q}+1}} \frac{\mu(d)}{|\mathrm{SL}_2(Z_d)|} + \mathcal{O}\Big(Q^{-1/2+\varepsilon}\Big)$$

És $(2, N) = 1$ esetén (amikor automatikusan $(6, Q-1) = 1$ igaz)

$$P'(\mathbb{F}) \ge \frac{1}{16} \sum_{\substack{d|Q-1\\d\le\sqrt{Q}+1}} \frac{\mu(d)}{|\mathrm{SL}_2(Z_d)|} + \mathcal{O}\Big(Q^{-1/2+\varepsilon}\Big) \ge$$

$$\ge \frac{1}{16}\left(1 + \sum_{\substack{\ell|Q-1\\\ell\le\sqrt{Q}+1}} \frac{\mu(\ell)}{|\mathrm{SL}_2(Z_\ell)|}\right) + \mathcal{O}\Big(Q^{-1/2+\varepsilon}\Big) \ge$$

$$\ge \frac{1}{16}\left(1 - \sum_{\ell>3} \frac{1}{|\mathrm{SL}_2(Z_\ell)|}\right) + \mathcal{O}\Big(Q^{-1/2+\varepsilon}\Big) =$$

$$= \frac{1}{16}\left(1 - \sum_{\ell>3} \frac{1}{\ell^3-\ell}\right) + \mathcal{O}\Big(Q^{-1/2+\varepsilon}\Big) \simeq 0.0616 + \mathcal{O}\Big(Q^{-1/2+\varepsilon}\Big).$$

Tehát az elliptikus görbék egy pozitív hányadának ciklikus a csoporja.

5.2.3. Megjegyzés. Például ha ε-t $1/4$-nek választjuk, akkor a fönti becslésben $m = 16$, $k(m) = 64$, és ebből kijön az, hogy ha $N > 50$, akkor $P'(\mathbb{F}) > 0.05$. Ez egy használható eredmény, hiszen az ECC-nél a test mérete 2^{120} és 2^{360} között szokott lenni.

Hivatkozások

[1] Joseph H. Silverman: The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[2] Joseph H. Silverman: Advanced Topics in the Arithmetic of Elliptic Curves, Springer-Verlag, 1995.

[3] Robin Hartshorne: Algebraic Geometry, Springer-Verlag, 1977.

[4] Michael Rosen: Number Theory in function fields, Springer-Verlag, 2001.

[5] Daniel A. Marcus: Number Fields, Springer-Verlag, 1977.

[6] William Fulton: Algebraic Curves, 2008.

[7] Alina-Carmen Cojocaru, Árpád Tóth: The distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field, még nem jelent meg.

[8] V. K. Murty, J. Scherk: Effective versions of the Chebotarev density theorem for function fields, C. R. Acad. Sci. Paris, t. 319, Série I, 1994, pp 523-528.

[9] Jun-Ichi Igusa: Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves, Amer. J. Math. 81 (1959), pp 453-476.

[10] Kunihiko Kodaira: On the structure of complex analytic surfaces I-IV, American Journal of Mathematics, 1964-1968.

[11] Enrico Bombieri, David Mumford: Enriques' classification of surfaces in char. p. II, Complex analysis and algebraic geometrz, 1977, Tokyo: Iwanami Shoten, pp. 23-42.

[12] Alina-Carmen Cojocaru, Chris Hall: Uniform results for Serre's theorem for elliptic curves, International Mathematical Research Notices, 2005 No. 50, pp 3065-3080.

[13] Barry Mazur: Modular curves and the Eisenstein ideal, IHES Publ. Math. 47(1977), pp 33-186.

[14] Jean-Pierre Serre: Quelques applications du theoreme de densite de Chebotarev, Hautes Études. Sci. Publ. Math. 54, 1981.

[15] www.wikipedia.org

[16] Neal Koblitz: Elliptic curve cryptosystems, Mathematics of Computation 48, 1987, pp. 203-209.

[17] S.D. Galbraith and N.P. Smart, A cryptographic application of the Weil descent, Cryptography and Coding, 1999.