A Lang-Trotter primitív pont sejtésről véges karakterisztikájú függvénytestek felett

Erdélyi Márton

merdelyi@renyi.hu
Rényi Alfréd Matematikai Kutatóintézet,
1053 Budapest, Reáltanoda utca 13-15.

1. Bevezetés

A Lang-Trotter primitív pont sejtés az Artin-féle primitív gyök sejtés elliptikus görbés megfelelője. A klasszikus esetben ($\mathbb{Q}$ felett) egyelőre elérhetetlennek tűnik az igazolása, viszont bizonyos más testek fölött könnyebb a helyzet, és vannak részeredmények. A továbbiakban egy ehhez használt bizonyítási módszert vizsgálunk, és egy kriptográfiai szempontból érdekes következményt is látni fogunk.

1.1. Az Artin-féle primitív gyök sejtés

Legyen $a \in \mathbb{Z}$ rögzített egész szám, továbbá X_a a prímszámok $\mathcal{P}$ halmazának azon részhalmaza, ami azokat p prímeket tartalmazza, amire a (mod p) primitív gyök (tehát, $a, a^2, a^3, \ldots, a^{p-1} \equiv 1$ redukált maradékrendszer modulo p). Az Artin-féle primitív gyök sejtés az $X_a \subset \mathcal{P}$ halmaz „sűrűségére" vonatkozik.

Ha a négyzetszám, akkor nyilván $p > 2$-re nézve nem lehet primitív gyök, hiszen $a^{(p-1)/2} \equiv 1$ modulo p. Hasonlóan $a = -1$ sem lehet primitív gyök, mert ekkor $a^2 = 1$. Artin sejtése szerint minden más esetben X_a végtelen halmaz, sőt a Dirichlet-sűrűsége pozitív, és $q_a \cdot c_A$, ahol q_a egy a-tól függő pozitív racionális szám és c_A az Artin-konstans:

$$c_A = \prod_{\ell \text{ prím}} \left(1 - \frac{1}{\ell(\ell-1)}\right) = \sum_{m \geq 1} \frac{\mu(m)}{m \cdot \varphi(m)} \simeq 0,37396.$$

A konstans a következő módon kapható meg: Ahhoz, hogy a primitív gyök legyen, az kell, hogy minden ℓ prímre az alábbi két feltétel legalább egyike ne teljesüljön: (1) $\ell | p-1$ azaz $p \equiv 1 \pmod{\ell}$, (2) $a^{(p-1)/\ell} \equiv 1 \pmod{p}$.

Artin észrevette, hogy ebben a bizonyos számtestek algebrai egészeinek számelmélete játszik szerepet: adott ℓ prímre legyen $L_\ell = \mathbb{Q}(\zeta_\ell, a^{1/\ell})|\mathbb{Q}$ testbővítés, ahol ζ_ℓ egy primitív ℓ-edik egységgyök. Ekkor $L_\ell|\mathbb{Q}$ Galois-bővítés. L_ℓ algebrai egészeinek gyűrűje egy Dedekind-gyűrű és fenti feltételek pontosan akkor teljesülnek ℓ-re, ha p teljesen szétesik az $L_\ell|\mathbb{Q}$ bővítésben. Ha a négyzetmentes, akkor $|L_\ell : \mathbb{Q}| = \ell(\ell-1)$ így a Csebotarev sűrűségi tétel szerint az ilyen ℓ prímek sűrűsége $1/\ell(\ell-1)$.

Tehát a számunkra kérdéses sűrűség várhatóan éppen c_A. A q_a számok azért kellenek, mert az L_ℓ bővítések csak a négyzetmentes esetben épp ekkorák és általában nem mindig függetlenek, ami viszont befolyásolja a várt sűrűséget.

Az általánosított Riemann-hipotézis mellett Hooley bizonyította az Artin primitív gyök sejtést ([Ho]). Enélkül azt lehet tudni, hogy a sejtés körülbelül igaz: ha csak olyan a-kra vizsgáljuk amik prímek (ebből könnyen levezethető az általános állítás), akkor Heath-Brown tétele szerint legfeljebb 2 prímszámra nem igaz a sejtés – de nem tudni melyikre ([HB]). Tehát egyelőre egyetlen a számot sem tudunk mondani, amire X_a sűrűsége biztosan pozitív. ([GuMu])

1.2. A Lang-Trotter primitív pont sejtés

A fenti kérdés átfogalmazható elliptikus görbékre, ez a Lang-Trotter primitív pont sejtés ([LaTr]). Az elliptikus görbék olyan görbék, amelyek pontjain természetes módon van egy kommutatív csoportstruktúra.

Legyen most E egy elliptikus görbe és A egy rögzített pont E-n. Az Artin-sejtéshez analóg kérdés, hogy mely p prímszámokra lesz a modulo p vett görbe csoportjában (ez véges sok esettől

eltekintve egy elliptikus görbe a véges test felett) generátorelem A képe. Erre akkor lehet esély, amikor a redukált görbe csoportja ciklikus, ami a klasszikus Artin-sejtésben szereplő $(\mathbb{Z}/p\mathbb{Z})^*$-al ellentétben nem mindig igaz. Ha A torzió-pont, akkor nyilván nem lehet végtelen sokszor generátor a képe: elég nagy prímekre a redukált görbének több pontja van, mint A rendje, így a többszörösei nem adják ki az egész görbét.

A fenti heurisztika erre az esetre is működik, de a helyzet jóval bonyolultabbnak tűnik az Artin-sejtésnél – még az általánosított Riemann-hipotézis felhasználásával sem jutunk eredményre, mert túl nagy hibatagot kapunk. Jelenleg abban az esetben tudunk valamit mondani, ha E CM görbe (azaz az endomorfizmus-gyűrűje nagy). Illetve az általános esetben, ha a görbe legalább 18 rangú (tehát $\mathbb{Z}^{18}$ részcsoportja E-nek), akkor egy hasonló állítás igaz: ha veszünk 18 lineárisan független pontot, akkor ezek képe generálja a redukált görbék egy pozitív sűrűségű részét. ([GuMu])

1.3. A továbbiak összefoglalása

A következőkben olyan felállásban vizsgáljuk a kérdést, ahol sokkal többet tudunk: a Dedekind-gyűrűk egy másik, jelentős csoportja a véges test feletti algebrai görbék koordinátagyűrűi. A prímek véges testbővítésbeli elágazási tulajdonságai hasonlóan vizsgálhatók, mint a klasszikus esetben. A véges karakterisztikájú függvénytestekre Weil bebizonyította az általánosított Riemann-hipotézist ([We]), és sok klasszikus számelméleti tétel sokkal erősebb változata igaz – a Csebotarev sűrűségi tételé is. Ennek következtében meg tudtak válaszolni néhány olyan kérdést, ami a klasszikus esetben egyelőre elérhetetlennek tűnik.

Legyen K egy véges karakterisztikájú függvénytest (pl $K = \mathbb{F}_q(T)$ – egy véges test feletti egyváltozós racionális függvények testje), o_K az egészek gyűrűje ($\mathbb{F}_q[T]$) és E/K egy elliptikus görbe. Ekkor ha ν egy prímideál o_K-ban (egy irreducibils polinom $\mathbb{F}_q[T]$-ben), akkor az E-t megadó egyenletet modulo ν tekintve egy véges k_ν test feletti E_ν elliptikus görbét kapunk (ami nem elfajuló, ha ν nem osztja E diszkriminánsát).

A cikkben vizsgált kérdések rögzített E-re a redukált görbék bizonyos tulajdonságait járják körül: milyen „valószínűséggel" lesz E_ν csoportja ciklikus ([CT]), vagy az elemszáma négyzetmentes ([CTV]), illetve az eredeti kérdést: ha rögzítünk egy pontot (rácsot) E-n, akkor ennek a pontnak (rácsnak) a képe mikor generálja a redukált görbét ([HaVo]).

A valószínűség alatt a következőket értjük:

- rögzített n-re a véges sok n fokú értékelési hely (irreducibilis polinom) közül véletlenszerűen választva mekkora valószínűséggel igaz a vizsgált tulajdonság,
- az összes értékelési hely között mekorra a Dirichlet-sűrűsége azoknak, amikre teljesül a vizsgált tulajdonság,
- mikor lesz ez a valószínűség/sűrűség 0.

A megoldások elég hasonló sémával működnek: szita formulát alkalmazunk, és utána a alapkérdést át tudjuk fogalmazni bizonyos Frobenius konjugált osztályokra (eddig a klasszikus esetben is megy), amire egy erős, effektív Csebotarev sűrűségi tételt lehet alkalmazni.

A következő fejezetben összeszedjük azokat a tudnivalókat, amik a megoldásokhoz kellenek. Az ezt követő részekben egy-egy kérdést vizsgálunk meg és a ma ismert eredményeket foglaljuk össze: az elsőnél a megoldási séma egyszerűen és gyorsan működik, a továbbiakban egyre nehezebb dolgunk lesz. Az utolsó fejezetben az eredményeinknek az elliptikus görbés nyilvános kulcsú kódolásokkal való összefüggéséről lesz szó.

2. Előzetes tudnivalók, jelölések

2.1. Függvénytestek és értékelések

Legyen K egy $p < \infty$ karakterisztikájú függvénytest, melyben az alaptest lezártja $k = \mathbb{F}_q$, valamely $q = p^f$-re. Jelöljük K érékeléseinek halmazát V_K-val, és $\nu \in V_K$-ra ν foka legyen $\deg(\nu) = [k_\nu : \mathbb{F}_q]$.

A legismertebb példa egy véges test feletti racionális törtfüggvények teste: $K = \mathbb{F}_q(T)$, ekkor $k = \mathbb{F}_q$, és a következők az értékelések:

- Ha $\nu \in \mathbb{F}_q[T]$ egy irreducibilis polinom, akkor ez természetes módon megad egy $\mathbb{F}_q(T) \to \mathbb{Z} \cup \{\infty\}$ értékelést, amit szintén ν-vel jelölünk: tetszőleges $f \in \mathbb{F}_q[T] \setminus \{0\}$ polinomra legyen $\nu(f) = \max(n \in \mathbb{N} : \nu^n | f)$, $f/g \in \mathbb{F}_q(T)$-re $\nu(f/g) = \nu(f) - \nu(g)$, és $\nu(0) = \infty$. Ekkor $\deg(\nu)$ a hagyományos fokszám.

- A végtelen értékelés $\nu_\infty : \mathbb{F}_q(T) \to \mathbb{Z} \cup \{\infty\}$, amire $\nu_\infty(f/g) = \deg(g) - \deg(f)$, és $\nu_\infty(0) = \infty$. Ekkor $\deg(\nu_\infty) = 1$.

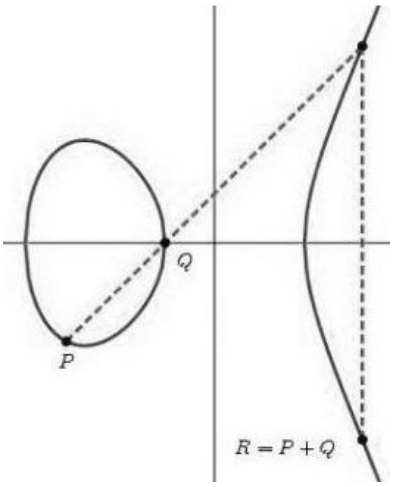
Egy $n \in \mathbb{N}$-re legyen $V_K(n) = \{\nu \in V_K | \deg(\nu) = n\}$ – ez egy véges halmaz, elemszáma $q^n/n + o(q^{n/2})$ és $S \subset V_K$ részhalmazra legyen $S(n) = S \cap V_K(n)$. Az S részhalmaz sűrűségét a következő módon értelmezhetjük: legyen $\delta(S, n) = |S(n)|/|V_K(n)|$, továbbá

$$\delta(S) = \lim_{s \to 1+0} \frac{\sum_{\nu \in S} q^{-s \deg(\nu)}}{\sum_{\nu \in V_K} q^{-s \deg(\nu)}},$$

a Dirichlet-sűrűség. Ekkor $0 \leq \delta(S) \leq 1$, és ha $|S|$ véges, akkor $\delta(S) = 0$.

2.2. Elliptikus görbék

Legyen $E/K : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ ($a_i \in K$) projektív algebrai görbe. A görbe $\Delta(E)$ diszkriminánsa az a_i-k egy polinomja, a görbe pontosan akkor sima, ha $\Delta(E) \neq 0$. A görbe j-invariánsa az a_i-k egy racionális törtfüggvénye – $j(E) \in K$. Ha két görbére $j(E) = j(E')$, akkor E és E' izomorf K egy legfeljebb másodfokú bővítése felett – tehát a j-invariáns többé-kevésbé az elliptikus görbék izomrfizmus osztályait adja meg. Mostantól feltesszük, hogy $j(E) \notin k$, mert a konstans j-invariánsú görbék a mi kérdéseinkben a többitől eltérő, általában egyszerűbb esetet adnak – ami többé-kevésbé a klasszikus CM esetnek felel meg. Az egy génuszú projektív algebrai görbék pontosan a sima elliptikus görbék, és ha az egyetlen végtelen távoli pontjuk az $O[0, 1, 0]$, akkor olyan alakúak, mint a fenti E.



Ekkor a $\overline{K}$ algebrai lezártban a görbe pontjain természetes módon definiálható a következő művelet ($+$): Ha $P \neq Q \in E$, akkor a két pontot összekötő egyenes metszi E-t egy harmadik pontban (multiplicitással számolva) – ez $-(P + Q)$. Ezt összekötve O-val, a harmadik metszéspont $R = P + Q$. (Ha $P = Q$, akkor a két pontot összekötő egyenes az érintő). Ez a művelet egy kommutatív csoportstruktúrát ad E pontjain, az egységelem O.

Ha $L|K$ testbővítés, akkor $E(L)$-lel jelöljük a görbe L-pontjait, ekkor $E(L) \leq E(\overline{K})$.

Ismert, hogy $E(K)$ végesen generált, és ha $E[m] = \{P \in E(\overline{K}) | m \cdot P = 0\}$ az m-torzió, akkor $E[m] = (\mathbb{Z}/m\mathbb{Z})^e$, $(m, p) = 1$ esetén $e = 2$, és a feltételeink mellett ha $m = p^k$, akkor $e = 1$.

Legyen $K_m = K(E[m])|K$ az a testbővítés, ahol az m-torzió pontok koordinátáival ($x = X/Z$ és $y = Y/Z$) bővítjük K-t. Ekkor $K_m|K$ Galois-bővítés, és ha rögzítünk két független torziópontot, akkor a $G_m = \mathrm{Gal}(K_m/K) \leq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ természetes módon: hiszen egy $\sigma \in G_m$ automorfizmus $E[m]$-t önmagába képzi, ráadásul a csoportműveletre lineárisan.

Legyen $(m, p) = 1$. $K_m|K$ felbontható két részre: Legyen $\mathbb{F}_{q^{c_m}}$ az alaptest bővítése, tehát $\overline{\mathbb{F}}_q^{K_m}$. Ekkor a skalár bővítés $G_m^{(\text{skalár})} = \mathrm{Gal}(K\mathbb{F}_{q^{c_m}}/K)$, a geometriai $G_m^{(\text{geom})} = \mathrm{Gal}(K_m/K\mathbb{F}_{q^{c_m}})$. Így a következő egzakt sorozatot kapjuk:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_m^{(\text{geom})} & \longrightarrow & G_m & \longrightarrow & G_m^{(\text{skalár})} = \langle q \rangle & \longrightarrow & 1 \\ & & \wedge| & & \wedge| & & \wedge| & & \\ 1 & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) & \longrightarrow & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) & \xrightarrow{\det} & (\mathbb{Z}/m\mathbb{Z})^* & \longrightarrow & 1 \end{array}$$

Az algebrai bővítésre mindig igaz, hogy $c_m = \mathrm{ord}_m(q)$, tehát q multiplikatív rendje modulo m. Mivel feltettük, hogy $j(E) \notin k$, a geometriai bővítés majdnem mindig maximális – tehát $G_m^{(\mathrm{geom})} = \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.

Ha ν nem osztja $\Delta(E)$-t, akkor az egyenletet modulo ν nézve kapunk egy sima E_ν elliptikus görbét k_ν felett. Legyen az ilyen értékelési helyek halmaza $V_{E/K}$, és $V_{E/K}(n) = V_{E/K} \cap V_K(n)$. Az ilyen ν-kre $E_\nu(k_\nu)$ véges, tehát $E_\nu(k_\nu)$ csoportja izomorf $\mathbb{Z}_{d_\nu} \times \mathbb{Z}_{d_\nu e_\nu}$-vel alkalmas $d_\nu, e_\nu \in \mathbb{N}$-re. Legyen $a_\nu = q^{\deg(\nu)} + 1 - |E_\nu(k_\nu)|$. Ekkor Hasse tétele szerint $|a_\nu| \leq 2q^{\deg(\nu)/2}$. Egy $A \in E(K)$ pont képe a redukciónál legyen $A_\nu \in E_\nu(k_\nu)$.

2.3. Frobenius konjugált osztályok és Csebotarev sűrűségi tétel

Legyen $L|K$ egy Galois-bővítés, $\nu \lhd o_K$ egy nem elágazó prím (tehát L-ben minden prím ami osztja ν-t legfeljebb egy multiplicitással szerepel), $V \lhd O_L$ egy ν feletti prím. A klasszikus esetben a Gauss egészeknél (a $L = \mathbb{Q}(i)|K = \mathbb{Q}$ testbővítésre, ahol az egészek gyűrűje $O_L = \mathbb{Z}[i] \geq O_K\mathbb{Z}$) egyetlen prím elágazó: $(2) = (1+i)^2$ – tehát elágazik. Ha a ν egy $4k+1$ alakú prímszám által generált ideál, akkor $\nu \cdot O_L$ két különböző $\mathbb{Z}[i]$-beli prímideál szorzatára bomlik, ha pedig $4k+3$ alakú akkor $\nu \cdot O_L \leq \mathbb{Z}[i]$ prímideál így ha ν páratlan prím által generált ideál, akkor nem elágazó.

Ekkor $\mathrm{Gal}(L/K) \geq \{\sigma | \sigma V = V\} \simeq \mathrm{Gal}(k_V/k_\nu)$, és az utóbbi véges testek bővítésének Galois-csoportja – tehát ciklikus, és van egy kitüntetett generátor-eleme, a Frobenius-automorfizmus, ami minden x elemet $x^{q^{\deg(\nu)}}$-be küld. Ennek az elemnek az előbbi izomorfizmusnál vett ősképét (ami $\mathrm{Gal}(L/K)$ egy eleme) nevezzük ν V-hez tartozó Frobenius-elemének, és $\Phi_{\nu,V}$-vel jelöljük. Ha V helyett egy másik ν feletti prímet választunk, akkor a Frobenius-elem konjugálódik. Az egész konjugált osztály a ν Frobenius konjugált osztálya, és a jele $\Phi_\nu = \Phi_{\nu,L/K}$.

A Frobenius konjugált osztály a prím elágazási tulajdonságaitól függ: a klasszikus példánkban a $4k+1$ alakú prímek szétesnek, tehát $k_V \simeq k_\nu$, így $\Phi_\nu = \{\mathrm{id}\}$. A $4k+3$ alakú prímek nem esnek szét, tehát a $k_V|k_\nu$ bővítés másodfokú és Φ_ν a $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ generátor elemét tartalmazó konjugált osztály.

Nekünk a $\nu \in V_{E/K}$ prímek K_m-beli elágazási tulajdonságaira lesz szükségünk. Legyen V egy ν feletti prím. Ekkor $g = \Phi_{\nu,V} \in G_m$ természetes módon $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ egy eleme. g hatása az m-torzió pontokon a definíció szerint a véges test q-Frobeniusa, tehát pontosan akkor van m-torziópont $E_\nu(k_\nu)$-ben, ha g-nek sajátértéke 1. Másrészt g hat E_ν-n is, és hasonló módon $E_\nu(k_\nu) = \mathrm{Ker}(g-1)$. Egész pontosan le lehet írni, hogy melyik elem $\Phi_{\nu,V}$, nekünk azonban elég lesz a következő két tulajdonsága. A determinánsa kongruens $q^{\deg(\nu)}$-vel modulo m, és a nyoma összefüggésben van a görbe pontjainak számával: $\mathrm{tr}(g) \equiv a_\nu = q^{\deg(\nu)} + 1 - |E_\nu(k_\nu)| \pmod m$.

Legyen most $L|K$ véges Galois-bővítés, amelyik k véges test felett definiált sima projektív görbék Galois-fedéséből jön (nálunk mindig ilyen lesz, legtöbbször $L = K_m$ valamely m-re) és $G = \mathrm{Gal}(L/K)$. Ekkor a prímek véges S halmazán kívül a többi nem elágazó, legyen $|S| = \sum_{\nu \in S} \deg(\nu)$. Legyen c az a szám, hogy az alaptest algebrai lezártja L-ben k c fokú bővítése és legyen tetszőleges $n \in \mathbb{N}$-re és $C \subset G$ konjugált osztályra $\pi(n, L/K, C) = \#(\nu \in V_K(n) \setminus S | \Phi_\nu = C)$.

A klasszikus esettől eltérően, adott n-re nem feltétlen fordulhat elő minden konjugált osztály Frobenius osztályként, hiszen ha $c \nmid n$, akkor az $x \mapsto x^n$ nincs is benne $\mathrm{Gal}(k_V/k_\nu)$-ben.

1. Tétel. *(Csebotarev sűrűségi tétel, [MuSc] Theorem 2.) Ha $c \nmid n$, akkor $\pi(n, L/K, C) = 0$, különben*

$$\left| \pi(n, L/K, C) - \frac{c \cdot |C|}{|[L:K]|} |V_K(n)| \right| \leq 2|C|^{1/2} \left((3g_K + (\rho+1)|S|) \frac{q^{n/2}}{n} + \frac{|S|}{2n} \right) + |S|,$$

ahol g_K a K test (és a megfelelő projektív görbe) génusza – $K = \mathbb{F}_q(T)$ esetén 0 – és ρ bizonyos K-tól függő konstans. (ρ L-től való függetlensége a $p < 5$ esetben az [Er] Section 2-ben van bizonyítva)

Ez pont azt állítja, hogy a lehetséges konjugált osztályok nagyjából a konjugált osztály méreteivel arányos sűrűséggel fordulnak elő. A hibatag sokkal jobb, mint a klasszikus esetben, ott csak $o(q^n)$-t tudunk mondani.

A $K_m|K$ bővítésekre $|S|$ becsülhető a nem sima redukciójú $\nu \in V_K \setminus V_{E/K}$ értékelési helyek fokszámösszegével, ekkor a hibatag $O_E(|C|^{1/2} q^{n/2}/n)$.

3. Ciklikusság

Először azt nézzük meg, hogy a redukált görbék pozitív sűrűséggel ciklikusak-e – ez nyilván szükséges feltétele annak, hogy A_ν generátor legyen.

Jelöljük $\delta_{\text{cikl}}(E/K)$-vel a $\{\nu \in V_{E/K} | E_\nu(k_\nu) \text{ ciklikus}\} \subset V_{E/K}$ halmaz sűrűségét (meg fogjuk mutatni, hogy ez létezik).

$E_\nu(k_\nu)$ csoportja pontosan akkor ciklikus, ha semelyik $\ell \neq p$ prímre $E_\nu[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ nem részcsoportja. Továbbá $E_\nu[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$ pontosan akkor van benne $E_\nu(k_\nu)$-ben, ha a $\Phi_{\nu,K_m/K}$ Frobenius konjugált osztály az identitás.

Így egy egyszerű szitával a következőt kapjuk:

$$\#(\nu \in V_{E/K}(n) | E_\nu(k_\nu) \text{ ciklikus}) = \sum_{p \nmid m} \mu(m) \# \left(\nu \in V_{E/K}(n) | E_\nu[m] \leq E_\nu(k_\nu)\right).$$

A szitának nagyon kevés tagja nem 0, mert Hasse tétele szerint $m^2 \leq q^n + 2q^{n/2} + 1$ kell legyen, azaz $m \leq q^{n/2} + 1$, és ráadásul a Csebotarev-tételben csak akkor nem 0 a kapott sűrűség, ha $c = c_m | n$, azaz ha $m | q^n - 1$ (ez lényegében a Weil-párosítás). A maradék tagok pedig

$$\#(\nu \in V(E/K, n) | E_\nu(k_\nu) \text{ ciklikus}) = \sum_{\substack{m \leq q^{n/2}+1 \\ m | q^n - 1}} \mu(m) \# \left(\nu \in V(E/K, n) | E_\nu[m] \leq E_\nu(k_\nu)\right)$$

$$= \sum_{\substack{m \leq q^{n/2}+1 \\ m | q^n - 1}} \left(\frac{\mu(m) c_m q^n}{|G_m| \cdot n} + O_E\left(\frac{q^{n/2}}{n}\right)\right) = \sum_{\substack{m \leq q^{n/2}+1 \\ m | q^n - 1}} \frac{\mu(m) \text{ord}_m(q) q^n}{|G_m| \cdot n} + O_{E,\varepsilon}\left(\frac{q^{(1/2+\varepsilon)n}}{n}\right).$$

Például, ha $q = 2$ és $2^n - 1$ Mersenne prím, akkor csak az $m = 1$-nek megfelelő tag marad, tehát az összes redukált görbe ciklikus. Ezek alapján

2. Tétel. *([CT] Theorem 1, $p < 5$-re [Er] Theorem 1)*

$$\left| \#(\nu \in V_{E/K}(n) | E_\nu(k_\nu) \text{ ciklikus}) - \delta_{\text{cikl}}(E/K, n) \frac{q^n}{n} \right| < O_{E,\varepsilon}\left(\frac{q^{(1/2+\varepsilon)n}}{n}\right),$$

ahol $\delta_{\text{cikl}}(E/K, n) = \sum_{m | q^n - 1} \frac{\mu(m) \text{ord}_m(q)}{|G_m|}$. *Ezek segítségével standard módon kiszámolható a Dirichlet-sűrűség:*

$$\delta_{\text{cikl}}(E/K) = \sum_{(m,p)=1} \frac{\mu(m)}{|G_m|}.$$

Itt nem kapunk szorzat alakot, mert a G_m-ek rendje nem multiplikatív: véges sok ℓ-től eltekintve ugyan $G_\ell \simeq \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, de a skalárbővítések a véges test $\text{ord}_\ell(q)$ rendű bővítései, amik nem függetlenek. (a geometriai bővítések véges sok prímtől eltekintve viszont függetlenek)

Ha az E görbe csoportja nem ciklikus – tehát, ha tartalmaz torziópontot, akkor a redukció csak akkor lehet ciklikus, ha a pont képe az új görbe egységeleme, ami viszont csak véges sokszor fordulhat elő. Tehát ilyenkor $\delta_{\text{cikl}}(E/K) = 0$. Meglepő módon máskor is lehet a Dirichlet-sűrűség 0:

3. Állítás. *([Er] Theorem 2)* $\delta_{\text{cikl}}(E/K) = 0 \iff \delta_{\text{cikl}}(E/K, 1) = 0$. *Legyen K rögzített, ebben az esetben pontosan akkor létezik olyan E elliptikus görbe, aminek a csoportja ciklikus és* $\delta_{\text{cikl}}(E/K) = 0$, *ha $q - 1$-nek legalább 3 prímosztója van.*

4. Négyzetmentes elemszám

Ebben a részben azt vizsgáljuk meg, hogy mikor lesz $|E_\nu(k_\nu)|$ négyzetmentes – pontosabban $|E_\nu(k_\nu)|$ p-hez relatív prím része (amit $|E_\nu(k_\nu)|'$-vel jelölünk) négyzetmentes. Jelöljük a megfelelő Dirichlet-sűrűséget $\delta_{\mathrm{nm}}(E/K)$-val.

Ha azt akarjuk leírni, hogy p^2 mikor osztja $|E_\nu(k_\nu)|$-t, akkor egy másik (nem $K_m|K$ alakú) testbővítést kell vizsgálnunk. Ettől az egyszerűség kedvéért most eltekintünk, $(\mathbb{Z}/p\mathbb{Z})^2$ úgysem lehet részcsoportja a redukált görbének – tehát az előbbinél erősebb feltételünk van, amit szintén le lehet írni bizonyos Frobenius konjugált osztályokkal:

Ha $(m,p)=1$ és $g=\Phi_{\nu,K_{m^2}/K}$, akkor $m^2||E_\nu(k_\nu)| \iff m^2|\det(g)-\mathrm{tr}(g)+1\equiv 0 \pmod{m^2}$. Az ilyen konjugált osztályokat könnyű megtalálni: legyen

$$C_{m^2}^{(n)}=\{g\in \mathrm{GL}_2(\mathbb{Z}/m^2\mathbb{Z})|\det(g)\equiv q^n \pmod{m^2}, \det(g)-\mathrm{tr}(g)+1\equiv 0 \pmod{m^2}\}.$$

Ekkor $\ell\neq p$ prímre

$$\left|C_{\ell^2}^{(n)}\right|=\begin{cases}\ell^4+\ell^3, & \text{ha } q^n\not\equiv 1 \pmod{\ell},\\ \ell^4+\ell^3-\ell^2, & \text{ha } q^n\equiv 1 \pmod{\ell}.\end{cases}$$

Összességében $\left|C_{m^2}^{(n)}\right|\le m^4\prod_{\ell|m}(1+1/\ell)=O(m^4\log\log m)$ és $\left|C_{m^2}^{(n)}\right|/\left|G_{m^2}^{(n)}\right|=O(m^{-2}\log\log m)$, ahol $G_{m^2}^{(n)}=\{g\in G_{m^2}|\det(g)\equiv q^n \pmod{m^2}\}$.

Fontos különbség a ciklikus esethez képest, hogy itt nincs oszthatósági feltétel m-re, tehát a szitában jóval több tagot kapunk, ezért a nagy m-ekre más becslést kell alkalmazni. Ezért osszuk ketté a szita tagjait egy később, optimálisan megválasztott y-nál:

$$\#\left(\nu\in V_{E/K}(n)||E_\nu(k_\nu)|' \text{ négyzetmentes}\right)=\sum_{\substack{m\le q^{n/2}+1\\(m,p)=1}}\mu(m)\cdot\#\left(\nu\in V_{E/K}(n)|m^2||E_\nu(k_\nu)|\right)$$

$$=\sum_{\substack{m\le y\\(m,p)=1}}\mu(m)\cdot\#\left(\nu\in V_{E/K}(n)|m^2||E_\nu(k_\nu)|\right)+O\left(\sum_{\substack{y<m\le q^{n/2}+1\\(m,p)=1}}\#\left(\nu\in V_{E/K}(n)|m^2||E_\nu(k_\nu)|\right)\right)$$

$$=: S_{\mathrm{fo}}+S_{\mathrm{hiba}}.$$

Az első részre a Csebotarev-tételt alkalmazva:

$$S_{\mathrm{fo}}=\sum_{\substack{m\le y\\(m,p)=1}}\mu(m)\cdot\#\left(\nu\in V_{E/K}(n)|\Phi_{\nu,K_{m^2}/K}\subset C_{m^2}^{(n)}\right)$$

$$=\left(\sum_{\substack{m\le y\\(m,p)=1}}\mu(m)\frac{\mathrm{ord}_{m^2}(q)\left|C_{m^2}^{(n)}\right|}{|G_{m^2}|}\right)\frac{q^n}{n}+O\left(\sum_{x\equiv 1 \pmod{\mathrm{ord}_{m^2}(q)}}\sum_{m\le y}\left|C_{m^2}^{(n)}\right|^{1/2}\frac{q^{n/2}}{n}\right)$$

$$=\left(\sum_{\substack{m\ge 1\\(m,p)=1}}\mu(m)\frac{\left|\mathrm{ord}_{m^2}(q)\cdot C_{m^2}^{(n)}\right|}{|G_{m^2}|}+O_E\left(\frac{\log\log y}{y}\right)\right)\frac{q^n}{n}+O_E\left(\frac{q^{n/2}y^3(\log\log y)^{1/2}}{n}\right)$$

A nagy m-ekhez tartozó tagok becsléséhez azt használjuk, hogy a redukált görbék elemszáma nem csak véges sok féle lehet (a Hasse-tétel szerint $q^n-2q^{n/2}+1\le|E_\nu(k_\nu)|\le q^n+2q^{n/2}+1)$), hanem ez a véges sok lehetőség többé-kevésbé egyenletesen oszlik el (az igazság az, hogy van néhány érték, ami nagyon kevésszer szerepel, és a $q+1$-hez közeliek gyakrabban fordulnak elő az átlagosnál), és van egy használható becslésünk az adott elemszámú görbék számára:

4. Tétel. *([Pa] Theorem 2.8, [CTV])*

$$\#(\nu\in V_{E/K}(n)|a_\nu=a)=O_E(q^{n/2}n^2).$$

Itt a konstans igazából csak $j(E)$ fokszámától függ.

Így ν-ket az $a = a_\nu$ szerint szétválasztva

$$S_{\text{hiba}} = O\left(\sum_{|a|<2q^{n/2}} \sum_{\substack{y<m\le q^{n/2}+1 \\ m^2 | q^n - a + 1}} \#\left(\nu \in V_{E/K}(n) | a_\nu = a\right)\right) = O_E\left(\sum_{|a|<2q^{n/2}} \sum_{\substack{y<m\le q^{n/2}+1 \\ m^2 | q^n - a + 1}} q^{n/2} n^2\right)$$
$$= O_E\left(q^{n/2} n^2 \sum_{y<m} \frac{q^{n/2}}{m^2}\right) = O_E\left(\frac{q^n n^2}{y}\right).$$

Ezek alapján az $y \simeq q^{n/8} \cdot n^{3/4}$ választással azt kapjuk, hogy

5. Tétel. *([CTV])*

$$\#\left(\nu \in V_{E/K}(n) | |E_\nu(k_\nu)|' \text{ négyzetmentes}\right) = \delta_{\text{nm}}(E/K, n)\frac{q^n}{n} + O_E\left(q^{\frac{7}{8}n} \cdot n^{\frac{5}{4}}\right),$$

ahol $\delta_{\text{nm}}(E/K, n) = \left(\sum_{\substack{m\ge 1 \\ (m,p)=1}} \mu(m) \frac{\text{ord}_{m^2}(q) \cdot \left|C^{(n)}_{m^2}\right|}{\left|G_{m^2}\right|}\right)$. *Továbbá ha* $\overline{C}_{m^2} = \sum_{1\le n\le \text{ord}_{m^2}(q)} \left|C^{(n)}_{m^2}\right|$, *akkor*

$$\delta_{\text{nm}}(E/K) = \sum_{\substack{m\ge 1 \\ (m,p)=1}} \mu(m) \frac{\overline{C}_{m^2}}{|G_{m^2}|}.$$

5. A Lang-Trotter sejtés

Most már az eredeti kérdést vizsgáljuk: hogy milyen sűrűséggel lesz egy pont képe generátor.

Legyen $A \in E(K)$ rögzített, $m \in \mathbb{N}$-re $E[m^{-1}A] = \{B \in E | m \cdot B = A\} \subset E$ és $A_m \in E[m^{-1}A]$ egy kiválasztott pont. Tekintsük az alábbi testbővítést: $L_{A,m} = K(E[m], E[m^{-1}A])|K$, ahol megint a megfelelő pontok koordinátáival bővítjük K-t.

Ha A nem torziópont, akkor majdnem minden ℓ prímre $H_{A,\ell} = \text{Gal}(L_{A,\ell}/K) \le \text{Aff}_2(\mathbb{Z}/\ell\mathbb{Z})$, ami $E[\ell^{-1}] \simeq (\mathbb{Z}/\ell\mathbb{Z})^2$ eltolásainak $T_{A,\ell}$ csoportjának bővítése G_ℓ-lel. $H_{A,\ell}$ természetes módon hat $E[\ell^{-1}A]$-n az affin csoport részcsoportjaként: minden eleme reprezentálható egy (γ, τ) párral valamely $\gamma \in G_\ell$-re és $\tau \in T_{A,\ell}$-re, ekkor egy $B \in E[\ell^{-1}]$ pontra $(\gamma, \tau)B = B_0 + \gamma(B - B_0) + \tau$.

Ha ℓ olyan, mint az előbbi bekezdésben, akkor $\nu \in V_{E/K}(n)$-ra pontosan akkor lesz $\langle A_\nu \rangle \le E_\nu(k_\nu)$ indexe osztható az ℓ-lel, ha $(\gamma, \tau) \in \Phi_{\nu, L_{A,\ell}/K} \subseteq H_{A,\ell}$-ra γ féligegyszerű, saját értéke 1 és ha $\gamma \ne \text{id}$, akkor $\tau \in \text{Im}(\gamma - 1)$. Jelöljük ezen elemek halmazát $D_{A,\ell}$-el, továbbá $D^{(n)}_{A,\ell} = \{(\gamma, \tau) \in D_{A,\ell} | \det(\gamma) \equiv q^n \pmod{\ell}\}$. Ekkor

$$\left|D^{(n)}_{A,\ell}\right| = \begin{cases} \ell^3 + \ell^2, & \text{ha } q^n \not\equiv 1 \pmod{\ell}, \\ \ell^3 + \ell^2 - \ell, & \text{ha } q^n \equiv 1 \pmod{\ell}. \end{cases}$$

Az előbbihez hasonlóan $\left|D^{(n)}_{A,m}\right| = O(m^3 \log\log m)$ és $|D^{(n)}_{A,m}|/|H^{(n)}_{A,m}| = O(m^{-2} \log\log m)$, ha $H^{(n)}_{A,m} = \{(\gamma, \tau) \in H_{A,m} | \det(\gamma) \equiv q^n \pmod{m}\}$.

A gond az, hogy itt még sokkal több tag van a szitában, mint az előbb, hiszen most m elvileg akár $q^n + 2q^{n/2} + 1$ is lehet. Viszont ha m nagy, akkor A_ν rendje (amit most k-val jelöljünk) kicsi, hiszen legfeljebb $|E_\nu(k_\nu)|/m$, ami nem sokszor fordulhat elő: az kell, hogy $\nu(x(k \cdot A)) < 0$ legyen, ez pedig egy nyilvánvaló becsléssel $O(k^2)$ esetben fordulhat elő, tehát $O(x^3)$ esetben lesz A_ν rendje legfeljebb x. Így tehát az $m \gg q^{2/3 \cdot n}$ tagok elintézhetők. Sajnos egy pontra nincs jobb becslés, és a maradék tagok is túl sokan vannak, mert a Csebotarev-tételben a hiba $\Omega(q^{n/2})$ nagyságrendű, tehát így nem juthatunk eredményre.

Amit lehet csinálni, hogy A helyett több, független pontot veszünk, mondjuk r darabot, és az általuk generált Σ rácsot nézzük. Ekkor a Néron-Tate párosítás szerint Σ-ban nem lehet túl sok kis magasságú pont és ennek következményeként

6. Állítás. *([GuMu] Lemma 14)*

$$\sum_{\substack{\nu\in V_{E/K}\\ |\Sigma_\nu|\le x}} \deg(\nu) = O_\Sigma\left(x^{(r+2)/r}\right).$$

Itt a jobb oldal Σ regulátorától függ.

Tehát minél nagyobb Σ rácsunk van $E(K)$-n, a képéről annál erősebbet tudunk mondani: ha r rangú, akkor az $m \gg q^{2n/(r+2)}$-nél nagyobb tagokból legfeljebb $o(q^n/n)$ van.

Legyen S azon prímek (véges) halmaza, ahol valamelyik $A \in \Sigma$ genrátorra $\mathrm{Gal}(K(E[\ell], E[\ell^{-1}A])$ nem olyan, mint a fenti, általános esetben (igazából ezek közül néhányra nem is feltétlenül van szükség). És keressük azokat a $\nu \in V_{E/K}(n)$ prímeket, amikre Σ_ν már tartalmazza az $E_\nu(k_\nu)$ S-beliekhez relatív prím részét, és az ilyenek halmazát jelöljük $V_{LT}(E/K, \Sigma, n)$-nel.

Ha m-nek nincs S-beli prímosztója, akkor $H_{\Sigma,m} = \mathrm{Gal}(K(E[m], E[m^{-1}\Sigma]/K) \simeq (\mathbb{Z}/\ell\mathbb{Z})^{2r} \rtimes G_m$. Az előbbiekhez hasonlóan a megfelelő konjugált osztályok azok, amik minden generátor elemre megfelelők. Az értelemszerű jelöléssel $|D^{(n)}_{\Sigma,\ell}| = \ell^{r+2} + \ell^{r+1} - \ell^r$, ha $q^n \equiv 1 \pmod{\ell}$ és $\ell^{r+2} + \ell^{r+1}$ különben.

Ahhoz, hogy a módszerünk működjön, tovább kell finomítani a becsléseket:

- Ha m kicsi, akkor a szokásos érvelést használjuk. Mivel itt a testbővítés nem $K_m|K$ alakú a Csebotarev-tételben sokkal rosszabb hibát kapunk, úgyhogy ez csak az $m \le Cn$ esetre használható.
- Ha m közepes ($Cn < m < Dq^{n/5}/n$), akkor egy olyan becslést használunk, ami $r+1$ különböző teljesen szétesési feltételre bontja szét az eredeti konjugált osztályos feltételt, és erre használjuk a Csebotarev-tételt – a kis m-ekre ez elrontaná a főtagot.
- Az $Dq^{n/5}/n < m < Dq^{n/5} \cdot \log n$ esetet kezelhető a prímszámtétel megfelelő alkalmazásával.

Így, ha $r \ge 10$ akkor a eddigi bizonyítási séma működik.

Az érvelést még lehet erősíteni: ehhez azt az L testet érdemes nézni, ami egy egyenes stabilizátorának felel meg G_m-ben, továbbá az $L_{\Sigma,m} = L(E[m], E[m^{-1}\Sigma])|L$ bővítést. Ez nem normális bővítés, úgyhogy ebben sokkal bonyolultabbak a prímek elágazási tulajdonságai. De ha $\nu \in V_{E/K}$ és $\Phi_{\nu, L_{\Sigma,m}/K} \in C_{\Sigma,m}$, akkor ν felett van egy megkülönböztetett $\overline{\nu} \le L$ prím, ami segítségével hasonló módon $q^{n/4}\log n$-ig fel lehet vinni a becslést, így az $r \ge 6$ eset kezelhető. Egyelőre ez a legtöbb, amit tudunk:

7. Tétel. *([HaVo] Theorem 1) Ha E/K elliptikus görbe, $j(E) \notin k$, és $\Sigma \le E(K)$ rács aminek a rangja legalább 6, akkor létezik a prímszámok egy véges S halmaza, amire a $\nu \in V_{E/K}(n)$ prímek pozitív részére Σ_ν tartalmazza $E_\nu(k_\nu)$ S-beli prímekhez relatív prím részét. A fenti jelölésekkel*

$$|V_{LT}(E/K, \Sigma, n)| = \delta_{LT}(E/K, n)\frac{q^n}{n} + o\left(\frac{q^n}{n}\right),$$

ahol $\delta_{LT}(E/K, n) = \sum_{m\ge 1} \mu(m)\dfrac{\left|D^{(n)}_{\sigma,m}\right|}{\left|H^{(n)}_{\sigma,m}\right|}$. *És* $\inf_n (\delta_{LT}(E/K, \Sigma, n)) > 0$.

6. Egy kriptográfiai alkalmazás

Véges test feletti elliptikus görbéket használnak bizonyos nyilvános kulcsú titkosítási eljárásokban (pl ECDH, ECIES, [Br] Section 3.3 és 5.1). Ez az elliptikus görbés diszkrét logaritmus problémán alapszik: Ha $E_0/\mathbb{F}_{q^n}$ egy elliptikus görbe, akkor egy pont m-szeresét gyorsan és hatékonyan lehet számolni (még ha n és m nagyok is), viszont egy pont m-ed részét úgy tűnik, hogy általában elég nehéz. Ez meglehetősen hasonlít a klasszikus diszkrét logaritmus problémára, amin

az RSA alapszik. Az elliptikus görbés kódolások előnye az RSA-val szemben, hogy ha nyilvános kulcsú kódot csinálunk, ugyanakkora biztonsághoz elég jóval kisebb kulcsokat használni.

Röviden mutatunk egy példát egy kódolási sémára:

Ha Alíz szeretne Bobtól titkos üzeneteket kapni, meg kell adnia egy véges test feletti E_0 elliptikus görbét (vigyázni kell, mert nem minden görbe „biztonságos"), és azon egy A_0 pontot, aminek a rendje n. Alíz titkos kulcsa egy $1 \leq d \leq n$ természetes szám, a nyilvános kulcs $Q = d \cdot A_0$.

Bob üzenete egy $M \in E_0$ pont (vannak olyan algoritmusok, amik természes számokhoz a görbe pontjait rendelik hozzá), aminek továbbításához választ egy $1 \leq k \leq n$ véletlen számot és az $(M_1 = M + k \cdot Q, M_2 = k \cdot A_0)$ pontpárt küldi tovább Alíznak.

Ekkor az $S = d \cdot M_2 = d \cdot (k \cdot A_0) = k \cdot (d \cdot A_0) = k \cdot Q$ pontot csak Alíz és Bob ismeri, ennek segítségével Alíz könnyen megfejtheti az üzenetet: $M = M_1 - S = M_1 - d \cdot M_2$.

Látható, hogy olyan A_0 pontot érdemes választani, ahol az $\langle A_0 \rangle \leq E_0$ részcsoport indexe kicsi (a gyakorlatban legfeljebb 4). Viszont ahogy láttuk, az RSA-val ellentétben, adott E_0-ra nem biztos, hogy van ilyen pont – mivel E_0 csoportja nem feltétlen ciklikus (mint a modulo p redukált maradékosztályoké). De az eddigi eredményeink alapján

8. Állítás. *Ha n elég nagy, akkor a $\mathbb{F}_q$ feletti elliptikus görbék legalább negyedének a csoportja ciklikus.*

Bizonyítás. Tekintsük most egy olyan $K = \mathbb{F}_q(T)$ felett egy olyan E elliptikus görbét, amire $j(E) = T$. Ilyen például az

$$E/K : y^2 + xy = x^3 + \frac{36}{1728 - T}x + \frac{1}{1728 - T}$$

affin egyenlet által definiált elliptikus görbe. Ekkor az E_ν redukált görbék $\nu \in V_{E/K}(n)$-re azok a görbék, ahol T helyére $\mathbb{F}_{q^n}$ elemeit helyettesítjük be, és ahogy láttuk, ez lényegében a $\mathbb{F}_{q^n}$ feletti elliptikus görbéket (illetve azok felét) adják meg.

Tehát ha $\delta_{\text{cikl}}(E/K, n)$ pozitív, akkor a $\mathbb{F}_{q^n}$ feletti elliptikus görbék egy pozitív hányadára a görbe csoport ciklikus. Igusa tétele szerint erre görbére a geometriai bővítés mindig maximális ([Ig], Theorem 4), így a 2. tétel szerint

$$\delta_{\text{cikl}}(E/K, n) = \sum_{m | q^n - 1} \mu(m) \frac{\text{ord}_m(q)}{|G_m|} = \sum_{m | q^n - 1} \mu(m) \frac{1}{|G_m^{(\text{geom})}|} = \prod_{\ell | q^n - 1} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right)$$
$$\geq \prod_{\ell \neq p} \left(1 - \frac{1}{\ell(\ell^2 - 1)}\right) \simeq 0.788 \cdot \frac{p^3 - p}{p^3 - p - 1} > 0.5.$$

Ez elég az állításunkhoz. □

Ha a Lang-Trotter sejtés igaz lenne, akkor arról is tudnánk valamit mondani, hogy egy adott $A \in E$ pont képe mekkora valószínűséggel lenne jó Alíz A_0 pontjának.

Hivatkozások

[Br] D. Brown. *Standards for Efficient Cryptography, Elliptic Curve Cryptography*, volume SEC 1, version 2.0. 2009.

[CT] A. C. Cojocaru and Á. Tóth. The distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field. *Journal of Number Theory*, 132:953–965, 2012.

[CTV] A. C. Cojocaru, Á. Tóth, and J. F. Voloch. Squarefree orders for the reductions of an elliptic curve over a function field. Preprint.

[Er] M. Erdélyi. The distribution and density of cyclic groups of the reductions of an elliptic curve over a function field. *J. Number Theory*, 175:87–99, 2017.

[GuMu] R. Gupta and M. R. Murty. Cyclicity and generation of points mod p on elliptic curves. *Invent. Math.*, 101 (1):225–235, 1990.

[HB] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford*, 37:27–38, 1987.

[Ho] C. Hooley. Artin's conjecture for primitive roots. *J. Reine Angew. Math.*, 225:209–220, 1967.

[HaVo] C. Hall and J. F. Voloch. Towards Lang-Trotter for elliptic curves over function fields (part 1). *Pure Appl. Math. Q.*, 2 (1):163–178, 2006.

[Ig] J.-I. Igusa. Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves. *Amer. J. Math.*, 81:453–476, 1959.

[LaTr] S. Lang and H. Trotter. Primitive points on elliptic curves. *Bull. Amer. Math. Soc.*, 83 (2):289–292, 1977.

[MuSc] V. K. Murty and J. Scherk. Effective versions of the Chebotarev density theorem for function fields. *C. R. Acad. Sci. Paris*, 319, Série I:523–528, 1994.

[Pa] A. Pacheco. Distribution of the traces of Frobenius on elliptic curves over function fields. *Acta Arithmetica*, 106.3:255–263, 2003.

[We] A. Weil. On the Riemann hypothesis in function-fields. *Proc. Nat. Acad. Sci. U.S.A.*, 27:345–347, 1941.