Rational points on curves over finite fields and their asymptotic

Alp Bassa

Boğaziçi University, Istanbul

Number Fields and Function Fields

$\mathbb{Z}$	$\leftrightarrow$	$\mathbb{F}_q[T]$

Number Fields		**Function Fields/Curves**
primes		places/points
$\log \lvert \mathrm{disc} \rvert$	$\leftrightarrow$	genus
class group		Jacobian
$\ldots$		$\ldots$

Zeta function: RH holds for congruence function fields!

Curves over Finite Fields

Let $\mathcal{C}$ be smooth, projective, absolutely irreducible curve over $\mathbb{F}_q$.

(alternatively $F/\mathbb{F}_q$ an algebraic function field with full constant field $\mathbb{F}_q$)

$\mathcal{C}(\mathbb{F}_q)$ set of rational points of $\mathcal{C}$.

$$\#\mathcal{C}(\mathbb{F}_q) \text{ is finite}$$

$$\#\mathcal{C}(\mathbb{F}_q) = ?$$

Notation: $N = N_1 := \#\mathcal{C}(\mathbb{F}_q)$.

The Hermitian Curve

q_0 a prime power, $\quad q = q_0^2$.

$$X^{q_0+1} + Y^{q_0+1} + Z^{q_0+1} = 0$$

Smooth plane of degree $q_0 + 1$, genus $g = \frac{1}{2} q_0(q_0 - 1)$.

$N = q_0^3 + 1$:
Involution of the quadratic extension $\mathbb{F}_q/\mathbb{F}_{q_0}$ given by

$$x \mapsto \bar{x} = x^{q_0}$$

Count isotropic vectors of the Hermitian form $x\bar{x} + y\bar{y} + z\bar{z}$.

Alternatively, use the (affine) model

$$y^{q_0} + y = x^{q_0+1}$$

Trace and Norm $\mathbb{F}_q/\mathbb{F}_{q_0}$.

- Each of the q_0^2 values for x in $\mathbb{F}_q$ gives q_0 values for y.
  $\rightarrow q_0^3$ points
- One point at infinity

So $N = q_0^3 + 1$.

$g = \frac{1}{2}q_0(q_0 - 1), N = q_0^3 + 1$. So $N \approx 2q_0 \cdot g = 2\sqrt{q} \cdot g$.
(in fact $N = q + 1 + 2\sqrt{q}g$)

Zeta Function

$$\mathcal{C}/\mathbb{F}_q, \qquad N_r := \#\mathcal{C}(\mathbb{F}_{q^r})$$

$$Z_{\mathcal{C}} := \exp\left(\sum_{r=1}^{\infty} N_r \frac{T^r}{r}\right).$$

Weil Conjectures

- **Rationality**

$$Z_{\mathcal{C}}(T) \in \mathbb{Q}(T).$$

In fact

$$Z_{\mathcal{C}}(T) = \frac{L(T)}{(1-T)(1-qT)},$$

where $L(T) \in \mathbb{Z}[T], \deg L(T) = 2g$.
Writing $L(T) = a_0 + a_1 T + \cdots + a_{2g} T^{2g}$, we have

$$a_0 = 1, a_1 = N - (q+1).$$

- **Functional Equation**

$$Z_{\mathcal{C}}(T) = q^{g-1} T^{2g-2} Z_{\mathcal{C}}(\frac{1}{qT})$$

Weil Conjectures

- **Riemann Hypothesis**

$$Z_{\mathcal{C}}(T) = \frac{L(T)}{(1-T)(1-qT)}, \ \deg L(T) = 2g, \ L(0) = 1$$

$$L(T) = \prod_{i=1}^{2g} (1 - \alpha_i T).$$

$$\mathrm{RH}: |\alpha_i| = \sqrt{q} \quad \text{(Hasse–Weil)}.$$

Define $\zeta_{\mathcal{C}}(s) = Z_{\mathcal{C}}(q^{-s})$. Then

$$\zeta_{\mathcal{C}}(s) = 0 \Rightarrow Z_{\mathcal{C}}(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2} \Rightarrow \mathrm{Re}(s) = 1/2.$$

Bounds on the number of points

$$N = q + 1 + a_1 = q + 1 - \sum_{i=1}^{2g} \alpha_i$$

so

$$N \leq q + 1 + 2g\sqrt{q} \quad \text{(Hasse–Weil bound)}.$$

Similarly, considering $\mathcal{C}/\mathbb{F}_{q^r}$

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$$

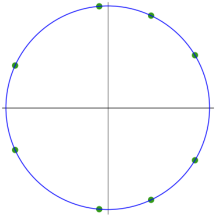
Example

$\mathcal{C}/\mathbb{F}_3$ genus 4 hyperelliptic curve given by the (affine) equation

$$y^2 = x \cdot (x+1) \cdot (x^7 + x^2 - 1).$$

$$Z_{\mathcal{C}} = \frac{81T^8 - 27T^7 + 18T^6 + 6T^5 - 2T^4 + 2T^3 + 2T^2 - T + 1}{(1-T)(1-3T)}.$$

Inverse roots have norm $\sqrt{3}$



How good is the Hasse–Weil bound?

Hermitian Curve

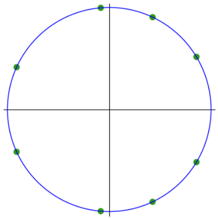
q_0 a prime power, $\quad q = q_0^2$.

$$X^{q_0+1} + Y^{q_0+1} + Z^{q_0+1} = 0$$

$g = \frac{1}{2} q_0(q_0 - 1), N = q_0^3 + 1.$
So $N = q + 1 + 2\sqrt{q}g$.

The Hermitian Curve attains the Hasse–Weil bound. Such curves are called *maximal*.

Ihara Bound



$$N = q + 1 - \sum_{i=1}^{2g} \alpha_i, \ |\alpha_i| = \sqrt{q}$$

$\mathcal{C}$ is maximal (attains HW-bound) $\Leftrightarrow \alpha_i = -\sqrt{q}$ for $i = 1, \ldots, 2g$

We have $N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r$

many $\mathbb{F}_q$-rational points	$\rightarrow \alpha_i$ "negative" $\rightarrow \alpha_i^2$ "positive" $\rightarrow$	few $\mathbb{F}_{q^2}$-rational points

Ihara Bound

Say $\mathcal{C}/\mathbb{F}_q$ is a maximal curve. So $\alpha_i = -\sqrt{q}$.

$$\mathcal{C}(\mathbb{F}_{q^2}) \geq \mathcal{C}(\mathbb{F}_q)$$
$$q^2 + 1 - \sum_{i=1}^{2g} q \geq q + 1 + \sum_{i=1}^{2g} \sqrt{q}$$

or

$$g \leq \frac{1}{2}\left(q - \sqrt{q}\right).$$

Hasse–Weil bound cannot be attained for large g.
"α_i cannot all be to the left"

(note: $\frac{1}{2}\left(q - \sqrt{q}\right)$ is the genus of the Hermitian curve)

Ihara's constant

Ihara:

$$A(q) = \limsup_{g(\mathcal{C})\to\infty} \frac{\#\mathcal{C}(\mathbb{F}_q)}{g(\mathcal{C})}$$

$\mathcal{C}$ runs over all absolutely irreducible, smooth, projective curves over $\mathbb{F}_q$.

Hasse–Weil bound	$\Longrightarrow A(q) \leq 2\sqrt{q}$
Ihara	$\Longrightarrow A(q) \leq \sqrt{2q} - \frac{1}{2}$
Drinfeld–Vladut	$\Longrightarrow A(q) \leq \sqrt{q} - 1$

$\left(\mathcal{C}(\mathbb{F}_{q^r}) \geq \mathcal{C}(\mathbb{F}_q)\right)$

How to obtain lower bounds for $A(q)$?

Find sequences $\mathcal{C}_i/\mathbb{F}_q$ such that $g(\mathcal{C}_i) \to \infty$ and

$$\lim_{i\to\infty} \frac{\#\mathcal{C}_i(F_q)}{g(\mathcal{C}_i)} \text{ is large.}$$

Many ways to construct good sequences:

- Modular curves (Elliptic, Shimura, Drinfeld)
- Class field towers (over prime fields)
- Explicit equations (recursively defined)

Modular curves

Ihara (1981), Tsfasman–Vladut–Zink:
Suppose $q = q_0^2$ is a square. Then

$$A(q) \geq \sqrt{q} - 1 \quad \big(\text{so } A(q) = \sqrt{q} - 1\big).$$

(case $q_0 = p$) Choose prime $\ell \neq p$, with $\ell \equiv 11 \pmod{12}$.

Consider the modular curve $X = X_0(\ell)$ over $\mathbb{F}_p$.

Curve of genus $(\ell + 1)/12$.

Points on $X_0(\ell)$

Points: $\{0, \infty\}$ "cusps", and points corresponding to pairs (E, C), E elliptic curve, C subgroup of E of order ℓ.

Supersingular elliptic curves and their $\ell + 1$ subgroups can be defined over $\mathbb{F}_{p^2}$.
We get many $\mathbb{F}_{p^2}$-rational supersingular points:

$$\frac{p-1}{12}(\ell + 1).$$

So

$$\frac{X(\mathbb{F}_{p^2})}{g(X)} \geq p - 1 = \sqrt{q} - 1.$$

Letting $\ell \to \infty$ we get

$$A(q) \geq \sqrt{q} - 1.$$

Zink Bound

Zink (Degeneration of Shimura surfaces):
If $q = p^3$, p a prime number, then

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}$$

(generalized by Bezerra–Garcia–Stichtenoth to all cubic finite fields)

Class Field Towers

$\mathcal{C}/\mathbb{F}_q$, with function field F.

S non-empty set of rational places of F.

Define sequence (F_n, S_n) inductively:

- $(F_0, S_0) = (F, S)$,
- F_{n+1} is the maximal abelian unramified ℓ-extension of F_n, in which the elements of S_n split completely,
- S_{n+1} is the set of places of F_{n+1} above S_n.

These defines curves over $\mathbb{F}_q$.

(S, ℓ)-class field tower of F.

If the (S,ℓ)-class field tower of F is *infinite*, then

$$A(q) \geq \frac{\#S}{g(\mathcal{C})-1}.$$

Golod-Shafarevich

- Serre: There exists $c > 0$ s.t. $A(q) \geq c \log(q) > 0$ for every q.
- Various results for small q:
  (Serre, Schoof, Niederreiter, Xing, Yeo, Temkine, Kuhnt, Duursma, Mak,...)
  $A(2) \geq 0.3169\ldots, \quad A(3) \geq 0.49287\ldots$, etc.

Recursive towers

Feng, Pellikaan, Garcia, Stichtenoth,...

Fix $F(U, V) \in \mathbb{F}_q[U, V]$. Recursive tower defined by $F(U, V)$:

Recursive towers

Feng, Pellikaan, Garcia, Stichtenoth,...

Fix $F(U, V) \in \mathbb{F}_q[U, V]$. Recursive tower defined by $F(U, V)$:

$$C_2 = \{(a_1, a_2) | F(a_1, a_2) = 0\} \subseteq \bar{\mathbb{F}_q}^2$$

Recursive towers

Feng, Pellikaan, Garcia, Stichtenoth,...

Fix $F(U, V) \in \mathbb{F}_q[U, V]$. Recursive tower defined by $F(U, V)$:

$$C_3 = \{(a_1, a_2, a_3) | F(a_1, a_2) = 0, F(a_2, a_3) = 0\} \subseteq \bar{\mathbb{F}}_q^{\,3}$$

$$\downarrow$$

$$C_2 = \{(a_1, a_2) | F(a_1, a_2) = 0\} \subseteq \bar{\mathbb{F}}_q^{\,2}$$

Recursive towers

Feng, Pellikaan, Garcia, Stichtenoth,...

Fix $F(U,V) \in \mathbb{F}_q[U,V]$. Recursive tower defined by $F(U,V)$:

$$C_4 = \{(a_1,a_2,a_3,a_4) | F(a_1,a_2) = F(a_2,a_3) = F(a_3,a_4) = 0\} \subseteq \bar{\mathbb{F}}_q^{\,4}$$

$$\downarrow$$

$$C_3 = \{(a_1,a_2,a_3) | F(a_1,a_2) = 0, F(a_2,a_3) = 0\} \subseteq \bar{\mathbb{F}}_q^{\,3}$$

$$\downarrow$$

$$C_2 = \{(a_1,a_2) | F(a_1,a_2) = 0\} \subseteq \bar{\mathbb{F}}_q^{\,2}$$

Let $\widetilde{\mathcal{C}}_n$ be a smooth projective model corresponding to $\mathcal{C}_n$.

Find suitable $F(U, V)$ such that

- $\widetilde{\mathcal{C}}_n/\mathbb{F}_q$ are irreducible
- $\#\widetilde{\mathcal{C}}_n(\mathbb{F}_q)$ grows fast
- $g(\widetilde{\mathcal{C}}_n)$ grows slowly.

$$\lambda = \lim_{n\to\infty} \frac{\#\widetilde{\mathcal{C}}_n(\mathbb{F}_q)}{g(\widetilde{\mathcal{C}}_n)} \leq A(q) \leq \sqrt{q} - 1$$

Norm-Trace Tower

Garcia–Stichtenoth, 1996
$q = \ell^2$

$$V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

Attains the Drinfeld–Vladut bound.
Genus computation is difficult (wild ramification)
Why many rational points?

$$q = \ell^2 \qquad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$X_n^\ell + X_n = \frac{X_{n-1}^{\ell+1}}{X_{n-1}^\ell + X_{n-1}}, \ldots, X_3^\ell + X_3 = \frac{X_2^{\ell+1}}{X_2^\ell + X_2},\ X_2^\ell + X_2 = \frac{X_1^{\ell+1}}{X_1^\ell + X_1}$$

$$q = \ell^2 \qquad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$X_n^\ell + X_n = \frac{X_{n-1}^{\ell+1}}{X_{n-1}^\ell + X_{n-1}}, \ldots, X_3^\ell + X_3 = \frac{X_2^{\ell+1}}{X_2^\ell + X_2},\ X_2^\ell + X_2 = \frac{X_1^{\ell+1}}{X_1^\ell + X_1}$$

$$X_1 = a_1 \in \mathbb{F}_q \text{ s.t. } Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_1) \neq 0$$

($\ell^2 - \ell$ choices)

$$q = \ell^2 \qquad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$X_n^\ell + X_n = \frac{X_{n-1}^{\ell+1}}{X_{n-1}^\ell + X_{n-1}}, \dots, X_3^\ell + X_3 = \frac{X_2^{\ell+1}}{X_2^\ell + X_2},\ X_2^\ell + X_2 = \frac{X_1^{\ell+1}}{X_1^\ell + X_1}$$

$$X_1 = a_1 \in \mathbb{F}_q \text{ s.t. } Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_1) \neq 0$$

($\ell^2 - \ell$ choices)

$$X_2 = a_2 \text{ with } a_2^\ell + a_2 = \frac{a_1^{\ell+1}}{a_1^\ell + a_1} \in \mathbb{F}_\ell \backslash \{0\}$$

ℓ choices with $a_2 \in \mathbb{F}_q$, $Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_2) \neq 0$)

$$q = \ell^2 \qquad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$X_n^\ell + X_n = \frac{X_{n-1}^{\ell+1}}{X_{n-1}^\ell + X_{n-1}}, \ldots, X_3^\ell + X_3 = \frac{X_2^{\ell+1}}{X_2^\ell + X_2},\ X_2^\ell + X_2 = \frac{X_1^{\ell+1}}{X_1^\ell + X_1}$$

$$X_1 = a_1 \in \mathbb{F}_q \text{ s.t. } Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_1) \neq 0$$

($\ell^2 - \ell$ choices)

$$X_2 = a_2 \text{ with } a_2^\ell + a_2 = \frac{a_1^{\ell+1}}{a_1^\ell + a_1} \in \mathbb{F}_\ell \backslash \{0\}$$

ℓ choices with $a_2 \in \mathbb{F}_q$, $Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_2) \neq 0$)

$$X_3 = a_3 \text{ with } a_3^\ell + a_3 = \frac{a_2^{\ell+1}}{a_2^\ell + a_2} \in \mathbb{F}_\ell \backslash \{0\}$$

ℓ choices with $a_3 \in \mathbb{F}_q$, $Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_3) \neq 0$)

$$q = \ell^2 \qquad V^\ell + V = \frac{U^{\ell+1}}{U^\ell + U}$$

$$X_n^\ell + X_n = \frac{X_{n-1}^{\ell+1}}{X_{n-1}^\ell + X_{n-1}}, \ldots, X_3^\ell + X_3 = \frac{X_2^{\ell+1}}{X_2^\ell + X_2},\ X_2^\ell + X_2 = \frac{X_1^{\ell+1}}{X_1^\ell + X_1}$$

$$X_1 = a_1 \in \mathbb{F}_q \text{ s.t. } Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_1) \neq 0$$

($\ell^2 - \ell$ choices)

$$X_2 = a_2 \text{ with } a_2^\ell + a_2 = \frac{a_1^{\ell+1}}{a_1^\ell + a_1} \in \mathbb{F}_\ell \setminus \{0\}$$

ℓ choices with $a_2 \in \mathbb{F}_q$, $Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_2) \neq 0$)

$$X_3 = a_3 \text{ with } a_3^\ell + a_3 = \frac{a_2^{\ell+1}}{a_2^\ell + a_2} \in \mathbb{F}_\ell \setminus \{0\}$$

ℓ choices with $a_3 \in \mathbb{F}_q$, $Tr_{\mathbb{F}_q/\mathbb{F}_\ell}(a_3) \neq 0$)

$\cdots \ \cdots$ so $\#\mathcal{C}_n(\mathbb{F}_q) \geq (\ell^2 - \ell)\ell^{n-1}$

Towers over cubic finite fields

- van der Geer–van der Vlugt, $q = 2^3 = 8, \mathcal{F}_2/\mathbb{F}_q$

$$V^2 + V = U + 1 + 1/U$$

  $\lambda = 3/2$. Attains Zink's bound for $p = 2$.

- Bezerra–Garcia–Stichtenoth, $q = \ell^3, \mathcal{F}_3/\mathbb{F}_q$

$$\frac{1-V}{V^\ell} = \frac{U^\ell + U + 1}{U} \quad \lambda(\mathcal{F}_3) \geq \frac{2(\ell^2-1)}{\ell+2}.$$

  Generalizes Zink's bound.

- B.–Garcia–Stichtenoth, $q = \ell^3, \mathcal{F}_4/\mathbb{F}_q$

$$(V^\ell - V)^{\ell-1} + 1 = \frac{-U^{\ell(\ell-1)}}{(U^{\ell-1}-1)^{\ell-1}} \quad \lambda(\mathcal{F}_4) \geq \frac{2(\ell^2-1)}{\ell+2}.$$

Towers over all non-prime fields

B.–Beelen–Garcia–Stichtenoth

$q = \ell^n, n \geq 2, k = \lfloor n/2 \rfloor$:

$$\text{Notation: } Tr_r(t) = t + t^{\ell} + \cdots + t^{\ell^{r-1}}$$

$$\frac{Tr_k(V) - 1}{(Tr_{k+1}(V) - 1)^{\ell^k}} = \frac{(Tr_k(U) - 1)^{\ell^{k+1}}}{(Tr_{k+1}(U) - 1)}$$

Lower bound:

- n even: $\sqrt{q} - 1 \to$ Drinfeld–Vladut bound
- $n = 3$: $\frac{2(\ell^2-1)}{\ell+2} \to$ Zink's bound
- For $n = 2k + 1 \geq 3$

$$\ell^{k+\frac{1}{2}} - 1 \geq A(\ell^{2k+1}) \geq \lambda \geq \frac{2}{\frac{1}{\ell^k-1} + \frac{1}{\ell^{k+1}-1}}.$$

Modular Interpretation

Idea: for classical modular curves many rational points over $\mathbb{F}_{p^2}$ come from the supersingular points.

Why quadratic? Over $\mathbb{C}$, elliptic curves $\leftrightarrow$ rank 2 lattices.
$[\mathbb{C} : \mathbb{R}] = 2$, no higher rank possible.

Drinfeld Modular Varieties

$$\begin{array}{ccc}
 & & C_\infty \\
 & & | \\
\mathbb{C} & & \bar{k_\infty} \\
| & & | \\
\mathbb{R} & & k_\infty \\
| & & | \\
\mathbb{Q} & & \mathbb{F}_\ell(T) \\
| & & | \\
\mathbb{Z} & & \mathbb{F}_\ell[T]
\end{array}$$

$\mathbb{Z}$-lattices inside $\mathbb{C}$ $\rightarrow$ rank 1 or 2

$\mathbb{F}_\ell[T]$-lattices inside C_∞ $\rightarrow$ arbitrary high rank possible

Drinfeld modules

Lattices $\leftrightarrow$ Drinfeld modules

Supersingular Drinfeld modules of rank r and their isogenies can be defined over a degree r extension$\rightarrow$ $\mathbb{F}_{q^r}$-rational points.

Moduli space is $(r-1)$-dimensional. Find suitable curves passing through the supersingular points.

Almost all known recursive towers with good asymptotic behavior have a modular interpretation.

Elkies "Fantasia": All "optimal" recursive towers are modular!

Towers over prime fields?

Towers over prime fields

B.–Ritzenthaler

Assume $q > 3$. There is an explicit recursive tower $(\mathcal{C}_r)_{r\geq 0}$ over $\mathbb{F}_q$ with limit

$$\lambda \geq \frac{2}{q-2}.$$

Equations can be given explicitly (depend on q).

$$\frac{y^{q+1}+b}{y^q-y} = \frac{2b(x^{q+1}+n)}{(b+n)(x^q-x)},$$

where $-n, -b \in \mathbb{F}_q^\times$ are non-squares with $n \neq \pm b$.

Related to Singer subgroups of $\mathrm{Aut}_{\mathbb{F}_q}(\mathbb{P}^1) \simeq \mathrm{PGL}_2(\mathbb{F}_q)$.