Codes and Modular Curves

Alain Couvreur
GT Grace

April 18, 2023

Overview

Question 1

For fixed $n > k$, what is the best possible minimum distance of an $[n, k]_q$–code over $\mathbb{F}_q$?

Overview

Question 1

For fixed $n > k$, what is the best possible minimum distance of an $[n, k]_q$–code over $\mathbb{F}_q$?

- Some upper bounds exist, Singleton, Plotkin, Griesmer, Sphere packing, Bassalygo Elias, etc...

Overview

Question 1

For fixed $n > k$, what is the best possible minimum distance of an $[n,k]_q$–code over $\mathbb{F}_q$?

- Some upper bounds exist, Singleton, Plotkin, Griesmer, Sphere packing, Bassalygo Elias, etc...
- Some databases of best known codes `MinT`, `codetables.de`;

Overview

Question 1

For fixed $n > k$, what is the best possible minimum distance of an $[n, k]_q$–code over $\mathbb{F}_q$?

- Some upper bounds exist, Singleton, Plotkin, Griesmer, Sphere packing, Bassalygo Elias, etc...
- Some databases of best known codes `MinT`, `codetables.de`;

Question 2 (And Asymptotically?)

For a sequence $(\mathcal{C}_s)_{s\in\mathbb{N}}$ of $[n_s, k_s, d_s]_q$ codes with $n_s \to +\infty$ and $\frac{k_s}{n_s} \to R$, $\frac{d_s}{n_s} \to \delta$; which pairs (δ, R) are achievable?

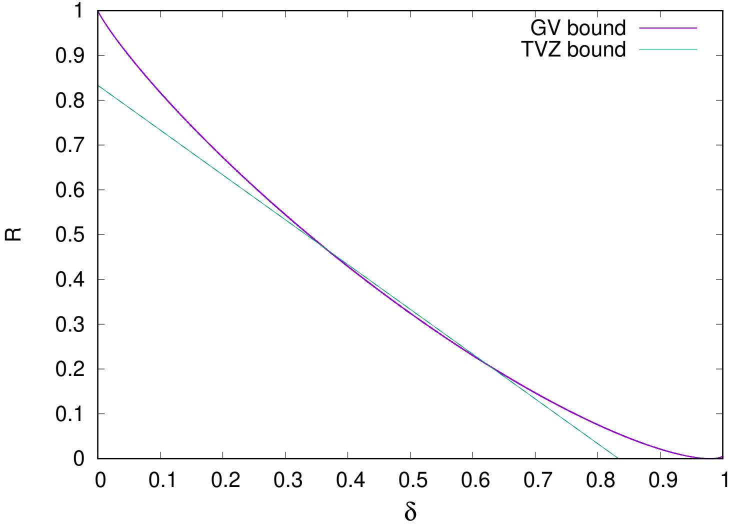
The unbelievable theorem...

Theorem 1 (Tsfasman, Vlăduț, Zink 1982)

Let $q = p^{2m}$ for p prime. There exists a sequence of codes $(\mathcal{C}_s)_s$ over $\mathbb{F}_q$ with parameters $[n_s, k_s, d_s]_q$ such that $R \stackrel{\text{def}}{=} \lim_{s\to+\infty} \frac{k_s}{n_s}, \delta \stackrel{\text{def}}{=} \lim_{s\to+\infty} \frac{d_s}{n_s}$ and

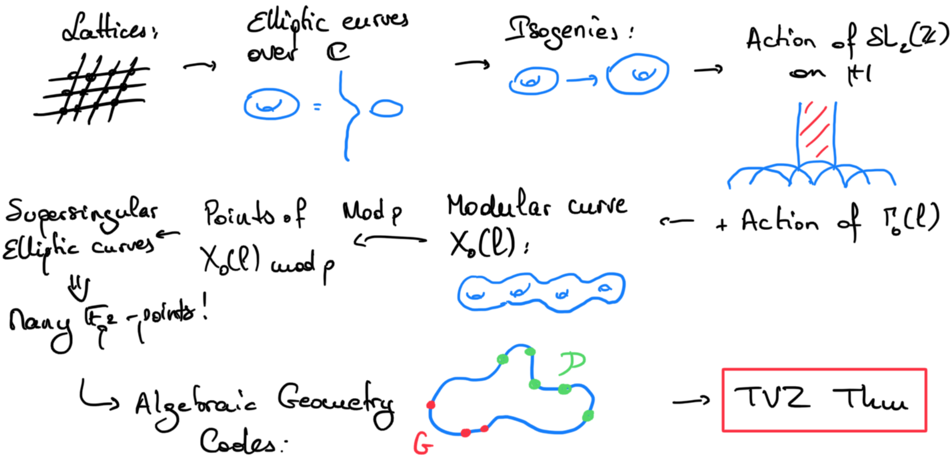
$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q}-1}.$$

The unbelievable picture (for $q = 49$)



How was it possible?

How was it possible?



My advice

Let us start

Definition 1

A code is a linear subspace $\mathcal{C} \subseteq \mathbb{F}_q^n$. Its parameters $[n, k, d]_q$ are

- *its* length *n;*
- *its dimension $k \stackrel{\text{def}}{=} \dim_{\mathbb{F}_q} \mathcal{C}$;*
- *its minimum distance $d \stackrel{\text{def}}{=} \min_{\boldsymbol{c} \in \mathcal{C} \setminus \{0\}} \{w_H(\boldsymbol{c})\}$, where $w_H(\cdot)$ denotes the* Hamming weight.

It is well–known that any $[n, k, d]_q$–code satisfies

$$k + d \leqslant n + 1 \qquad \text{(Singleton Bound)}$$

The Gilbert Varshamov bound

Theorem 2

Let n, d be positive integers, then there exists a (possibly nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with minimum distance d such that

$$\sharp\mathcal{C} \cdot \underbrace{\left(\sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j\right)}_{\text{Volume of a ball of radius } d-1} \geqslant q^n.$$

The Gilbert Varshamov bound

Theorem 2

Let n, d be positive integers, then there exists a (possibly nonlinear) code $\mathcal{C} \subseteq \mathbb{F}_q^n$ with minimum distance d such that

$$\sharp\mathcal{C} \cdot \underbrace{\left(\sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j\right)}_{\text{Volume of a ball of radius } d-1} \geqslant q^n.$$

Asymptotically we get the existence of sequences of codes with parameters (δ, R) such that

$$R = 1 - H_q(\delta),$$

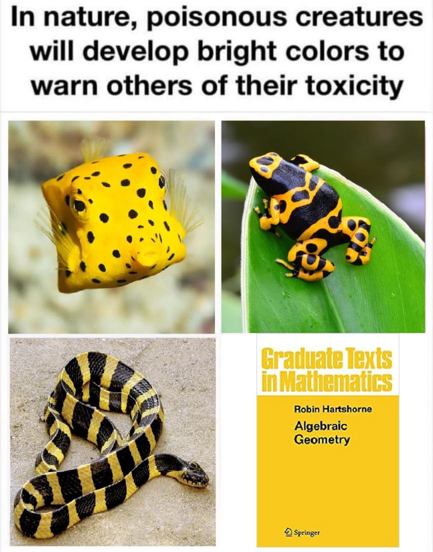
where $H_q(\cdot)$ denotes the q–ary entropy function (see Lecture Notes p. 4)

Facts

1. For a long time, Gilbert Varshamov bound was supposed to be optimal;
2. Actually, at least for large enough q, there is room for improvement.

My advice if you wish to discover algebraic geometry

My advice if you wish to discover algebraic geometry



Curves

In the sequel, $\mathbb{K}$ denotes a perfect field.

Definition 2

An affine curve $\mathscr{X} \subseteq \mathbb{A}^2(\overline{\mathbb{K}})$ is the vanishing locus of a polynomial $F \in \mathbb{K}[x, y]$. If F is irreducible over $\overline{\mathbb{K}}$, then the curve is said to be absolutely irreducible.

Definition 3

A rational point *or* $\mathbb{K}$–point *of $\mathscr{X}$ is an element of $\mathscr{X} \subseteq \mathbb{A}^2(\overline{\mathbb{K}})$ whose coordinates lie in $\mathbb{K}$. For any extension $\mathbb{L}/\mathbb{K}$, an $\mathbb{L}$–point is an element of $\mathscr{X}$ whose coordinates lie in $\mathbb{L}$. The set of $\mathbb{K}$– (resp. $\mathbb{L}$–) points is denoted $\mathscr{X}(\mathbb{K})$ (resp. $\mathscr{X}(\mathbb{L})$).*

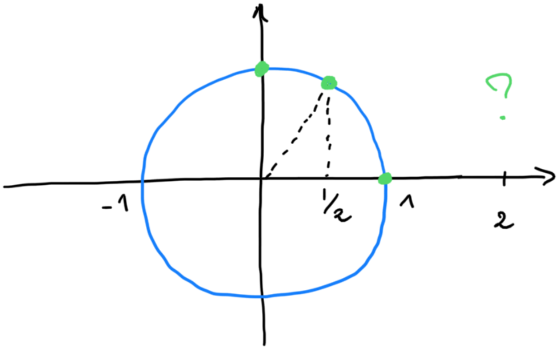
Remark

In particular, $\mathscr{X} = \mathscr{X}(\overline{\mathbb{K}})$. Moreover $\mathscr{X}(\mathbb{K})$ is the subset of $\mathscr{X}$ invariant under the action of Gal$(\overline{\mathbb{K}}/\mathbb{K})$.

Example I

Example 1

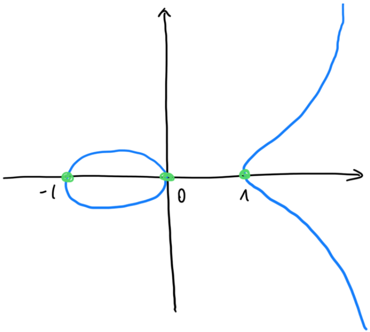
$\mathbb{K} = \mathbb{Q}$ and $F(x, y) = x^2 + y^2 - 1$. The points $(1, 0), (0, 1)$ are $\mathbb{Q}$–points. The point $(\frac{1}{2}, \frac{\sqrt{3}}{2})$ is a $\mathbb{Q}(\sqrt{3})$–point. The point $(2, -i\sqrt{3})$ is a $\mathbb{C}$–point (actually also a $\mathbb{Q}(i\sqrt{3})$–point).



Example II

Example 2

$\mathbb{K} = \mathbb{Q}$ and $F(x,y) = y^2 - x(x-1)(x+1)$. The points $(-1,0), (0,0)$ and $(1,0)$ are $\mathbb{Q}$–points.



Singularities

Definition 4

Let $\mathscr{X} \subseteq \mathbb{A}^2(\mathbb{K})$ be a curve defined as the vanishing locus of $F \in \mathbb{K}[x, y]$. A point P of $\mathscr{X}$ is said to be singular *if both $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ vanish at P. A curve with no singular points is said to be* smooth*.*

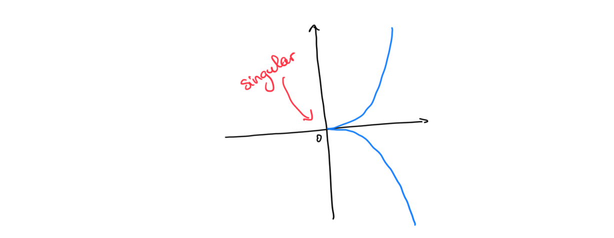
Singularities

Definition 4

Let $\mathscr{X} \subseteq \mathbb{A}^2(\mathbb{K})$ be a curve defined as the vanishing locus of $F \in \mathbb{K}[x, y]$. A point P of $\mathscr{X}$ is said to be singular *if both $\frac{\partial F}{\partial x}$ and $\frac{\partial F}{\partial y}$ vanish at P. A curve with no singular points is said to be* smooth.

Example 3

The curve of equation $y^2 = x^3$ is singular at $(0, 0)$.



From now on...

From now on, any “curve” is smooth and absolutely irreducible.

Regular and rational functions

Definition 5 (Regular functions)

Let $\mathscr{X} \subseteq \mathbb{A}^2(\mathbb{K})$ *be a curve defined as the vanishing locus of* $F \in \mathbb{K}[x, y]$*. A* regular function *on* $\mathscr{X}$ *is the restriction to* $\mathscr{X}$ *of an element of* $\mathbb{K}[x, y]$*. The ring of regular functions on* $\mathscr{X}$ *is noting but*

$$\mathbb{K}[x, y]/(F).$$

Definition 6 (Rational functions)

A rational function *on* $\mathscr{X}$ *is the restriction to* $\mathscr{X}$ *of an element of* $\mathbb{K}(x, y)$ *whose denominator is prime to* F*. Since* $\mathscr{X}$ *is irreducible (*i.e. F *is irreducible), then the* function field *of* $\mathscr{X}$ *is defined as*

$$\mathbb{K}(\mathscr{X}) \stackrel{\text{def}}{=} \mathit{Frac}\left(\mathbb{K}[x, y]/(F)\right).$$

Regular and rational maps

Definition 7

Let $\mathscr{X}, \mathscr{Y}$ be two curves. A regular *(resp.* rational*)* map *from $\mathscr{X}$ to $\mathscr{Y}$ is a map*

$$\phi : \left\{ \begin{array}{ccc} \mathscr{X} & \longrightarrow & \mathscr{Y} \\ (x,y) & \longmapsto & (\phi_1(x,y), \phi_2(x,y)) \end{array} \right.$$

where ϕ_1, ϕ_2 are regular *(resp.* rational*) functions on $\mathscr{X}$.*
If there is $\psi : \mathscr{Y} \to \mathscr{X}$ such that $\psi \circ \phi = Id_{\mathscr{X}}$ and $\phi \circ \psi = Id_{\mathscr{Y}}$, then ϕ is said to be an isomorphism *(resp.* a birational map*).*

Remark

Such a function might be defined only on $\mathscr{X}$ minus a finite number of points.

Example

Example 4

The affine line $\mathbb{A}^1$ and the circle $\mathscr{C}$ of equation $x^2 + y^2 = 1$ are birational to each other via the map:

$$\left\{ \begin{array}{ccc} \mathbb{A}^1 & \longrightarrow & \mathscr{C} \\ t & \longmapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \end{array} \right.$$

Example

Example 4

The affine line $\mathbb{A}^1$ and the circle $\mathscr{C}$ of equation $x^2+y^2=1$ are birational to each other via the map:

$$\left\{\begin{array}{ccc} \mathbb{A}^1 & \longrightarrow & \mathscr{C} \\ t & \longmapsto & \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right) \end{array}\right.$$

Remark

The map is undefined at $\{\pm i\}$.

Link with function fields

Proposition 1

Given a rational map $\phi : \mathscr{X} \to \mathscr{Y}$, there is a field extension $\phi^\star : \mathbb{K}(\mathscr{Y}) \hookrightarrow \mathbb{K}(\mathscr{X})$ given by

$$\phi^\star f \stackrel{\text{def}}{=} f \circ \phi.$$

Divisors

Definition 8

On a curve $\mathscr{X}$ over $\mathbb{K}$, a rational divisor is a finite formal sum $\sum a_P P$ of $\overline{\mathbb{K}}$–points which is globally invariant under the action of Gal$(\overline{\mathbb{K}}/\mathbb{K})$. The degree *of a divisor $\sum a_P P$ is the integer $\sum a_P$.*

Divisors

Definition 8

On a curve $\mathscr{X}$ over $\mathbb{K}$, a rational divisor is a finite formal sum $\sum a_P P$ of $\overline{\mathbb{K}}$–points which is globally invariant under the action of Gal$(\overline{\mathbb{K}}/\mathbb{K})$. The degree *of a divisor $\sum a_P P$ is the integer $\sum a_P$.*

Example 5

On $\mathscr{C}$ of equation $x^2 + y^2 = 1$, the following object is a rational divisor:

$$3 \cdot (1,0) - 2 \cdot (0,1) + 4(2, -i\sqrt{3}) + 4(2, i\sqrt{3})$$

and that one is not:

$$3 \cdot (1,0) - 2 \cdot (0,1) + 4\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) + 2\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$$

Divisors

Definition 8

On a curve $\mathscr{X}$ over $\mathbb{K}$, a rational divisor is a finite formal sum $\sum a_P P$ of $\overline{\mathbb{K}}$–points which is globally invariant under the action of Gal$(\overline{\mathbb{K}}/\mathbb{K})$. The degree of a divisor $\sum a_P P$ is the integer $\sum a_P$.

Example 5

On $\mathscr{C}$ of equation $x^2 + y^2 = 1$, the following object is a rational divisor:

$$3 \cdot (1,0) - 2 \cdot (0,1) + 4(2, -i\sqrt{3}) + 4(2, i\sqrt{3})$$

and that one is not:

$$3 \cdot (1,0) - 2 \cdot (0,1) + 4\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right) + {\color{red}2}\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$$

Valuations

Definition 9 (Informal)

Let $\mathscr{X}$ be a curve. To any point $P \in \mathscr{X}(\overline{\mathbb{K}})$ we associate a map $\nu_P : \overline{\mathbb{K}}(\mathscr{X})^\times \to \mathbb{Z}$ called the valuation at P *describing the order of pole or zero of any function on $\mathscr{X}$. A* local parameter at P *is a function of valuation 1 at P.*

Principal divisors

Definition 10

To any function $f \in \mathbb{K}(\mathscr{X})^{\times}$ *one associates a divisor called* principal divisor *and defined as*

$$(f) = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} \nu_P(f) \cdot P.$$

Proposition 2

The degree of a principal divisor is always 0.

Principal divisors

Definition 10

To any function $f \in \mathbb{K}(\mathscr{X})^{\times}$ *one associates a divisor called* principal divisor *and defined as*

$$(f) = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} \nu_P(f) \cdot P.$$

Proposition 2

The degree of a principal divisor is always 0.

Principal divisors

Definition 10

To any function $f \in \mathbb{K}(\mathscr{X})^\times$ *one associates a divisor called* principal divisor *and defined as*

$$(f) = \sum_{P \in \mathscr{X}(\overline{\mathbb{K}})} \nu_P(f) \cdot P.$$

Proposition 2

The degree of a principal divisor is always 0.

Example 6

On the blackboard.

Riemann–Roch spaces

Definition 11

The divisor group on $\mathscr{X}$ *is endowed with a partial order. Let* $A = \sum a_P P$ *and* $B = \sum b_P P$,

$$A \geqslant B \iff \forall P \in \mathscr{X}(\overline{\mathbb{K}}), a_P \geqslant b_P$$

Definition 12

Let $\mathscr{X}$ *be a curve over* $\mathbb{K}$ *and* G *be a divisor on* $\mathscr{X}$, *we define the space*

$$L(G) \stackrel{\text{def}}{=} \left\{ f \in \mathbb{K}(\mathscr{X})^\times \mid (f) + G \geqslant 0 \right\} \cup \{0\},$$

Properties of Riemann–Roch spaces

Proposition 3

- *If* $G < 0$, *then* $L(G) = \{0\}$
- *For any* G, *the space* $L(G)$ *has finite dimension and* $\dim L(G) \leqslant \deg G + 1$.

Properties of Riemann–Roch spaces

Proposition 3

- *If* $G < 0$, *then* $L(G) = \{0\}$
- *For any* G, *the space* $L(G)$ *has finite dimension and* $\dim L(G) \leqslant \deg G + 1$.

Definition 13 (Genus)

The genus of a curve $\mathscr{X}$ *is defined as*

$$g \stackrel{\textbf{\textit{def}}}{=} 1 - \min_{D}\{\dim L(D) - \deg D\}.$$

Properties of Riemann–Roch spaces

Proposition 3

- *If $G < 0$, then $L(G) = \{0\}$*
- *For any G, the space $L(G)$ has finite dimension and $\dim L(G) \leqslant \deg G + 1$.*

Definition 13 (Genus)

The genus of a curve $\mathscr{X}$ is defined as

$$g \stackrel{\textit{def}}{=} 1 - \min_{D}\{\dim L(D) - \deg D\}.$$

Theorem 3 (Riemann–Roch)

Let G be a divisor on a curve, then

$$\dim L(G) \geqslant \deg G + 1 - g \qquad \textit{with equality if} \quad \deg G > 2g - 2.$$

Construction

Definition 14 (Goppa 1981, Vlăduț–Manin 1984)

Let $\mathscr{X}$ be a curve over a finite field $\mathbb{F}_q$, G be a divisor on $\mathscr{X}$ and $\mathcal{P} = (P_1, \ldots, P_n)$ an n–tuple of distinct rational points of $\mathscr{X}$. We define

$$\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G) \stackrel{\textbf{def}}{=} \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\}.$$

Construction

Definition 14 (Goppa 1981, Vlăduț–Manin 1984)

Let $\mathscr{X}$ be a curve over a finite field $\mathbb{F}_q$, G be a divisor on $\mathscr{X}$ and $\mathcal{P} = (P_1, \dots, P_n)$ an n–tuple of distinct rational points of $\mathscr{X}$. We define

$$\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G) \stackrel{\text{def}}{=} \{(f(P_1), \dots, f(P_n)) \mid f \in L(G)\}.$$

Theorem 4

The code $\mathcal{C}_L(\mathscr{X}, \mathcal{P}, G)$ as parameters

$$\begin{aligned} k &\geqslant \deg G + 1 - g \\ d &\geqslant n - \deg G. \end{aligned}$$

How to provide excellent codes from curves?

First we can construct $[n, k, d]$ codes with

$$n + 1 - g \leqslant k + d$$

How to provide excellent codes from curves?

First we can construct $[n, k, d]$ codes with

$$n + 1 - g \leqslant k + d \qquad (\leqslant n + 1, \quad \text{By Singleton bound})$$

Definition 15 (Ihara constant)

$$A(q) \stackrel{\textit{def}}{=} \limsup_{g \to +\infty} \left(\max_{\mathscr{X} \text{ of genus } g} \frac{\sharp X(\mathbb{F}_q)}{g} \right)$$

How to provide excellent codes from curves?

Theorem 5 (Tsfasman–Vlăduț–Zink 1982)

Let $q = p^{2m}$ for p prime.

$$A(q) \geqslant \sqrt{q} - 1$$

How to provide excellent codes from curves?

Theorem 5 (Tsfasman–Vlăduț–Zink 1982)

Let $q = p^{2m}$ for p prime.

$$A(q) \geqslant \sqrt{q} - 1$$

Corollary 1

There exists a sequence of codes $(\mathcal{C}_s)_s$ over $\mathbb{F}_q$ with parameters $[n_s, k_s, d_s]_q$ such that $R \stackrel{\textbf{def}}{=} \lim_{s\to+\infty} \frac{k_s}{n_s}, \delta \stackrel{\textbf{def}}{=} \lim_{s\to+\infty} \frac{d_s}{n_s}$ and

$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q} - 1}.$$

How to provide excellent codes from curves?

Theorem 5 (Tsfasman–Vlăduț–Zink 1982)

Let $q = p^{2m}$ for p prime.

$$A(q) \geqslant \sqrt{q} - 1$$

Corollary 1

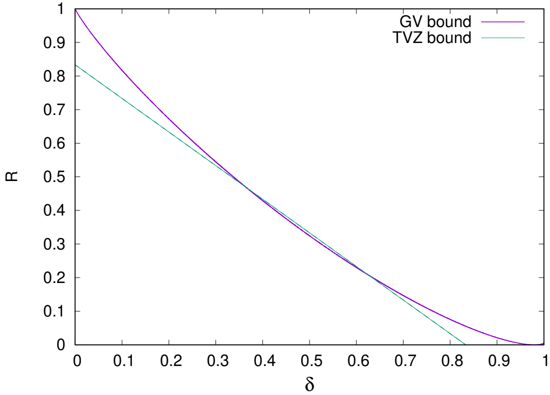
There exists a sequence of codes $(\mathcal{C}_s)_s$ over $\mathbb{F}_q$ with parameters $[n_s, k_s, d_s]_q$ such that $R \overset{\textbf{def}}{=} \lim_{s \to +\infty} \frac{k_s}{n_s}, \delta \overset{\textbf{def}}{=} \lim_{s \to +\infty} \frac{d_s}{n_s}$ and

$$R + \delta \geqslant 1 - \frac{1}{\sqrt{q} - 1}.$$

Theorem 6 (Drinfeld Vlăduț 1894)

For any prime power q, $A(q) \leqslant \sqrt{q} - 1$. i.e. *TVZ is optimal.*

How to get this?



Goal. Exhibit a family of curves $(\mathscr{X}_s)_{s\in\mathbb{N}}$ over $\mathbb{F}_q$ such that

$$\limsup_{s\to+\infty} \frac{\sharp X_s(\mathbb{F}_q)}{g(\mathscr{X}_s)} = \sqrt{q} - 1.$$

Elliptic curves

Definition 16

Let $\mathbb{K}$ *be a field of characteristic* $\neq 2, 3$. *An* elliptic curve $\mathscr{E}$ *over* $\mathbb{K}$ *is a genus one curve with one rationa point. Such a curve can be represented with an equation* $y^2 = f(x)$ *where* $f \in \mathbb{K}[x]$ *is squarefree of degree* 3. *In addition, it can be put in* Weierstrass *form*

$$y^2 = x^3 + Ax + B \qquad \textit{for some } A, B \in \mathbb{K}.$$

Elliptic curves

Definition 16

Let $\mathbb{K}$ be a field of characteristic $\neq 2, 3$. An elliptic curve $\mathscr{E}$ *over $\mathbb{K}$ is a genus one curve with one rationa point. Such a curve can be represented with an equation $y^2 = f(x)$ where $f \in \mathbb{K}[x]$ is squarefree of degree 3. In addition, it can be put in* Weierstrass *form*

$$y^2 = x^3 + Ax + B \qquad \text{for some } A, B \in \mathbb{K}.$$

Remark

Weierstrass form is not unique. For instance, a change of variables:

$$\begin{array}{rcl} x & \mapsto & u^2 x \\ y & \mapsto & u^3 y \end{array}$$

for some $u \in \mathbb{K}^\times$ provides an equation of an isomorphic curve with Weierstrass equation:

$$y^2 = x^3 + Au^{-4}x + u^{-6}B.$$

The j–invariant

Definition 17

Let $\mathscr{E}$ be an elliptic curve with Weierstrass equation: $y^2 = x^3 + Ax + B$. The j–invariant of $\mathscr{E}$ is defined as

$$j \stackrel{\text{def}}{=} 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

The j–invariant

Definition 17

Let $\mathscr{E}$ be an elliptic curve with Weierstrass equation: $y^2 = x^3 + Ax + B$. The j–invariant of $\mathscr{E}$ is defined as

$$j \stackrel{def}{=} 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Theorem 7

Two elliptic curves are isomorphic over $\overline{\mathbb{K}}$ if and only if they have the same j–invariant. Conversely, for any $j_0 \in \overline{\mathbb{K}}$ there is an elliptic curve defined over $\mathbb{K}(j_0)$ with j–invariant j_0.

The j–invariant

Definition 17

Let $\mathscr{E}$ be an elliptic curve with Weierstrass equation: $y^2 = x^3 + Ax + B$. The j–invariant of $\mathscr{E}$ is defined as

$$j \stackrel{\text{def}}{=} 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

Theorem 7

Two elliptic curves are isomorphic over $\overline{\mathbb{K}}$ if and only if they have the same j–invariant. Conversely, for any $j_0 \in \overline{\mathbb{K}}$ there is an elliptic curve defined over $\mathbb{K}(j_0)$ with j–invariant j_0.

$\overline{\mathbb{K}}$–isomorphism classes of elliptic curves are parameterised by $\mathbb{A}^1(\overline{\mathbb{K}})$.

The group law

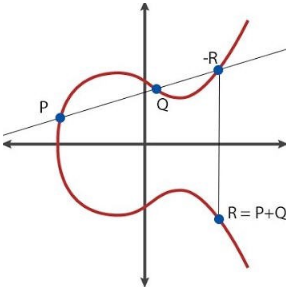
Theorem 8

Let $\mathscr{E}$ be an elliptic curve over $\mathbb{K}$, then for any algebraic extension $\mathbb{L}/\mathbb{K}$, the set $\mathscr{E}(\mathbb{L})$ has an abelian group structure.

The group law

Theorem 8

Let $\mathscr{E}$ be an elliptic curve over $\mathbb{K}$, then for any algebraic extension $\mathbb{L}/\mathbb{K}$, the set $\mathscr{E}(\mathbb{L})$ has an abelian group structure.



The group structure is inherited from that of $\mathrm{Pic}^0(\mathscr{E}) \simeq \mathrm{Div}^0_{\mathbb{K}}(\mathscr{E})/\mathrm{Princ}(\mathscr{E})$.

Torsion

Definition 7

Given an elliptic curve $\mathscr{E}$ over $\mathbb{K}$ and an integer $m > 1$, the m–torsion of $\mathscr{E}$ is defined as

$$\mathscr{E}[m] \stackrel{\text{def}}{=} \{P \in \mathscr{E}(\overline{\mathbb{K}}) \mid mP = 0\}.$$

Torsion

Definition 7

Given an elliptic curve $\mathscr{E}$ over $\mathbb{K}$ and an integer $m > 1$, the m–torsion of $\mathscr{E}$ is defined as

$$\mathscr{E}[m] \stackrel{\text{def}}{=} \{P \in \mathscr{E}(\overline{\mathbb{K}}) \mid mP = 0\}.$$

Remark

$\mathscr{E}[m]$ is not necessarily composed of rational points but is **globally** *stable under the action of $Gal(\overline{\mathbb{K}}/\mathbb{K})$.*

Torsion

Definition 7

Given an elliptic curve $\mathscr{E}$ over $\mathbb{K}$ and an integer $m > 1$, the m–torsion of $\mathscr{E}$ is defined as

$$\mathscr{E}[m] \stackrel{\text{def}}{=} \{P \in \mathscr{E}(\overline{\mathbb{K}}) \mid mP = 0\}.$$

Remark

$\mathscr{E}[m]$ is not necessarily composed of rational points but is **globally** *stable under the action of $Gal(\overline{\mathbb{K}}/\mathbb{K})$.*

Proposition 4

For an elliptic curve $\mathscr{E}$ and $m \in \mathbb{N}$

$$\mathscr{E}[m] \simeq \begin{cases} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \text{if } m \text{ is prime to } Char(\mathbb{K}); \\ 0 \text{ or } \mathbb{Z}/m\mathbb{Z} & \text{otherwise} \end{cases}$$

Isogenies

Definition 18

An isogeny between elliptic curves is a regular map $\mathscr{E} \to \mathscr{E}'$ *sending* $O_{\mathscr{E}}$ *onto* $O_{\mathscr{E}'}$.

Isogenies

Definition 18

An isogeny between elliptic curves is a regular map $\mathscr{E} \to \mathscr{E}'$ sending $O_{\mathscr{E}}$ onto $O_{\mathscr{E}'}$.

Proposition 5

An isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ induces a group morphism. Moreover, when ϕ is separable, then

$$\sharp ker \phi = \deg \phi$$

Conversely, for any finite subgroup $K \subseteq \mathscr{E}(\overline{\mathbb{K}})$ which is globally invariant under Gal$(\overline{\mathbb{K}}/K)$, there exists an isogeny $\psi : \mathscr{E} \to \mathscr{E}'$ defined over $\mathbb{K}$ with kernel K. We denote

$$\mathscr{E}' \stackrel{\text{def}}{=} \mathscr{E}/K.$$

Isogenies

Proposition 5

An isogeny $\phi : \mathscr{E} \to \mathscr{E}'$ induces a group morphism. Moreover, when ϕ is separable, then

$$\sharp ker \phi = \deg \phi$$

Conversely, for any finite subgroup $K \subseteq \mathscr{E}(\overline{\mathbb{K}})$ which is globally invariant under Gal$(\overline{\mathbb{K}}/K)$, there exists an isogeny $\psi : \mathscr{E} \to \mathscr{E}'$ defined over $\mathbb{K}$ with kernel K. We denote

$$\mathscr{E}' \stackrel{\textbf{def}}{=} \mathscr{E}/K.$$

Proposition 6

For any degree m isogeny $\phi : \mathscr{E} \to \mathscr{E}'$, there exists a unique $\hat{\phi} : \mathscr{E}' \to \mathscr{E}$ such that

$$\hat{\phi} \circ \phi = [m]_{\mathscr{E}} : \left\{ \begin{array}{ccc} \mathscr{E} & \longrightarrow & \mathscr{E} \\ P & \longmapsto & mP \end{array} \right. \quad \text{and} \quad \phi \circ \hat{\phi} = [m]_{\mathscr{E}'} : \left\{ \begin{array}{ccc} \mathscr{E}' & \longrightarrow & \mathscr{E}' \\ P & \longmapsto & mP. \end{array} \right.$$

The idea behind dual isogenies

- On a curve $\mathscr{E}$, the map $P \mapsto mP$ induces an isomorphism $\mathscr{E} \xrightarrow{\sim} \mathscr{E}/\mathscr{E}[m]$;
- Let $K \subseteq \mathscr{E}[m]$ of cadinality m and $\phi : \mathscr{E} \to \mathscr{E}' = \mathscr{E}/K$ the corresponding isogeny;
- The dual isogeny is $\hat{\phi} : \mathscr{E}' \to \mathscr{E}'/\phi(\mathscr{E}[m]) \simeq \mathscr{E}'/(\mathscr{E}[m]/K) \simeq \mathscr{E}$

The idea behind dual isogenies

- On a curve $\mathscr{E}$, the map $P \mapsto mP$ induces an isomorphism $\mathscr{E} \xrightarrow{\sim} \mathscr{E}/\mathscr{E}[m]$;
- Let $K \subseteq \mathscr{E}[m]$ of cadinality m and $\phi : \mathscr{E} \to \mathscr{E}' = \mathscr{E}/K$ the corresponding isogeny;
- The dual isogeny is $\hat{\phi} : \mathscr{E}' \to \mathscr{E}'/\phi(\mathscr{E}[m]) \simeq \mathscr{E}'/(\mathscr{E}[m]/K) \simeq \mathscr{E}$

$$\begin{tikzcd} \mathscr{E} \arrow[r, "\phi"] \arrow[rr, bend right, "P \mapsto mP"'] & \mathscr{E}' \arrow[r, "\hat{\phi}"] & \mathscr{E} \end{tikzcd}$$

Lattices and Elliptic curves over $\mathbb{C}$

Theorem 9

Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. Then, the quotient $\mathbb{C}/\Lambda$ is biholomorphic to a complex elliptic curve. Conversely, for any elliptic curve $\mathscr{E}$ over $\mathbb{C}$, there exists a lattice $\Lambda \subseteq \mathbb{C}$ such that $\mathscr{E}$ is biholomorphic to $\mathbb{C}/\Lambda$.

Lattices and Elliptic curves over $\mathbb{C}$

Theorem 9

Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. Then, the quotient $\mathbb{C}/\Lambda$ is biholomorphic to a complex elliptic curve. Conversely, for any elliptic curve $\mathscr{E}$ over $\mathbb{C}$, there exists a lattice $\Lambda \subseteq \mathbb{C}$ such that $\mathscr{E}$ is biholomorphic to $\mathbb{C}/\Lambda$.

Sketch of proof for $\mathbb{C}/\Lambda \to \mathscr{E}$.

The connection is made by the *Weierstrass $\wp_\Lambda$–function*:

$$\forall z \in \mathbb{C} \setminus \Lambda, \quad \wp_\Lambda(z) \stackrel{\text{def}}{=} \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

together with the map $\left\{ \begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{A}^2 \\ z & \longmapsto & (\wp_\Lambda(z), \wp'_\Lambda(z)) \end{array} \right.$ (Λ being sent onto $O_{\mathscr{E}}$). $\square$

Lattices and Elliptic curves over $\mathbb{C}$

Sketch of proof for $\mathbb{C}/\Lambda \to \mathscr{E}$.

The series $\wp_\Lambda(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ is even an vanishes at 0

$$\wp_\Lambda(z) = \frac{1}{z^2} + O(z^2)$$

$\square$

Lattices and Elliptic curves over $\mathbb{C}$

Sketch of proof for $\mathbb{C}/\Lambda \to \mathscr{E}$.

The series $\wp_\Lambda(z) - \frac{1}{z^2} = \sum_{\omega\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$ is even an vanishes at 0

$$
\begin{aligned}
\wp_\Lambda(z) &= \frac{1}{z^2} + O(z^2) \\
\wp'_\Lambda(z) &= -\frac{2}{z^3} + O(z)
\end{aligned}
$$

$\square$

Lattices and Elliptic curves over $\mathbb{C}$

Sketch of proof for $\mathbb{C}/\Lambda \to \mathscr{E}$.

The series $\wp_\Lambda(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ is even an vanishes at 0

$$\begin{aligned}
\wp_\Lambda(z) &= \frac{1}{z^2} + O(z^2) \\
\wp'_\Lambda(z) &= -\frac{2}{z^3} + O(z) \\
\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 &= O(\frac{1}{z^2})
\end{aligned}$$

$\square$

Lattices and Elliptic curves over $\mathbb{C}$

Sketch of proof for $\mathbb{C}/\Lambda \to \mathscr{E}$.

The series $\wp_\Lambda(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ is even an vanishes at 0

$$
\begin{aligned}
\wp_\Lambda(z) &= \frac{1}{z^2} + O(z^2) \\
\wp'_\Lambda(z) &= -\frac{2}{z^3} + O(z) \\
\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 &= O(\frac{1}{z^2}) \\
\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z) &= O(1) \quad \text{(for some } g_2 \text{ in } \mathbb{C})
\end{aligned}
$$

$\square$

Lattices and Elliptic curves over $\mathbb{C}$

Sketch of proof for $\mathbb{C}/\Lambda \to \mathscr{E}$.

The series $\wp_\Lambda(z) - \frac{1}{z^2} = \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$ is even an vanishes at 0

$$
\begin{aligned}
\wp_\Lambda(z) &= \frac{1}{z^2} + O(z^2) \\
\wp'_\Lambda(z) &= -\frac{2}{z^3} + O(z) \\
\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 &= O(\frac{1}{z^2}) \\
\wp'_\Lambda(z)^2 - 4\wp_\Lambda(z)^3 - g_2\wp_\Lambda(z) &= O(1) \quad \text{(for some } g_2 \text{ in } \mathbb{C})
\end{aligned}
$$

Liouville $\implies$ $\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 + g_2\wp_\Lambda(z) + g_4$ for some $g_2, g_4 \in \mathbb{C}$. □

Things happen well!

Theorem 10

For any lattice $\Lambda \subset \mathbb{C}$, The biholomorphic map $\mathbb{C}/\Lambda \xrightarrow{\sim} \mathscr{E}$ is a group isomorphism from $(\mathbb{C}/\Lambda, +)$ to $(\mathscr{E}, +_{\mathscr{E}})$.

Things happen well!

Theorem 10

For any lattice $\Lambda \subset \mathbb{C}$, The biholomorphic map $\mathbb{C}/\Lambda \xrightarrow{\sim} \mathscr{E}$ is a group isomorphism from $(\mathbb{C}/\Lambda, +)$ to $(\mathscr{E}, +_{\mathscr{E}})$.

Remark

For any $m > 0$, the structure of $\mathscr{E}[m]$ can be understood from that of $\left(\frac{1}{m}\Lambda\right)/\Lambda$

Isogenies regarded from tori

Theorem 11

Let $\Lambda, \Lambda' \subset \mathbb{C}$ *be two lattices and* $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ *sending* 0 *to* 0*. Then,* f *lifts to a holomorphic ma* $f_0 : \mathbb{C} \to \mathbb{C}$ *which is a similitude,* i.e. *there exists* $a \in \mathbb{C}$ *such that* $\forall z \in \mathbb{C}$*,* $f_0(z) = az$*.*

Isogenies regarded from tori

Theorem 11

Let $\Lambda, \Lambda' \subset \mathbb{C}$ *be two lattices and* $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ *sending* 0 *to* 0*. Then,* f *lifts to a holomorphic ma* $f_0 : \mathbb{C} \to \mathbb{C}$ *which is a similitude,* i.e. *there exists* $a \in \mathbb{C}$ *such that* $\forall z \in \mathbb{C}$, $f_0(z) = az$.

Remark

(Up to some similitude) For ℓ *prime, a degree* ℓ*–isogeny between two tori corresponds to the data of two lattices* Λ, Λ' *such that* $\Lambda \subseteq \Lambda'$ *and* $\sharp(\Lambda'/\Lambda) = \ell$.

Complex elliptic curves with nontrival automorphisms

Theorem 12

Let $\mathbb{C}/\Lambda$ be a complex torus with an automorphism $a \mapsto az$ and $|a| = 1$, $a \neq \pm 1$. Then, up to a similitude, Λ equals either $\mathbb{Z} \oplus \mathbb{Z}i$ or $\mathbb{Z} \oplus \mathbb{Z}\rho$, where $\rho = e^{\frac{2i\pi}{6}}$

Complex elliptic curves with nontrival automorphisms

Theorem 12

Let $\mathbb{C}/\Lambda$ be a complex torus with an automorphism $a \mapsto az$ and $|a| = 1$, $a \neq \pm 1$. Then, up to a similitude, Λ equals either $\mathbb{Z} \oplus \mathbb{Z}i$ or $\mathbb{Z} \oplus \mathbb{Z}\rho$, where $\rho = e^{\frac{2i\pi}{6}}$

The corresponding elliptic curves can be proved to have respective equations:

$$
\begin{array}{rclcrcll}
y^2 & = & x^3 + x & \text{for} & \Lambda & = & \mathbb{Z} \oplus \mathbb{Z}i & (j\text{–invariant } 1728) \\
y^2 & = & x^3 + 1 & \text{for} & \Lambda & = & \mathbb{Z} \oplus \mathbb{Z}\rho & (j\text{–invariant } 0).
\end{array}
$$

The corresponding automorphisms being respectively

$$
\begin{array}{rcl}
(x, y) & \longmapsto & (-x, iy) \\
(x, y) & \longmapsto & (\rho x, -y).
\end{array}
$$

The Poincaré upper half plane

Question 3

How to classify complex elliptic curves up to isogeny? Equivalently, how to classify lattices up to similitude?

The Poincaré upper half plane

Question 3

How to classify complex elliptic curves up to isogeny? Equivalently, how to classify lattices up to similitude?

- Start with a basis $\Lambda = \mathbb{Z}\omega_2 \oplus \mathbb{Z}\omega_1$;

The Poincaré upper half plane

Question 3

How to classify complex elliptic curves up to isogeny? Equivalently, how to classify lattices up to similitude?

- Start with a basis $\Lambda = \mathbb{Z}\omega_2 \oplus \mathbb{Z}\omega_1$;
- after a possible swap, one can suppose the basis is “direct”, *i.e.* $\operatorname{Im}(\frac{\omega_2}{\omega_1}) > 0$.

The Poincaré upper half plane

Question 3

How to classify complex elliptic curves up to isogeny? Equivalently, how to classify lattices up to similitude?

- Start with a basis $\Lambda = \mathbb{Z}\omega_2 \oplus \mathbb{Z}\omega_1$;
- after a possible swap, one can suppose the basis is "direct", *i.e.* $\mathrm{Im}(\frac{\omega_2}{\omega_1}) > 0$.
- for any $A \in \mathrm{SL}_2(\mathbb{Z})$,

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \stackrel{\text{def}}{=} A \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

  is another direct basis of the **same lattice**.

The Poincaré upper half plane

Question 3

How to classify complex elliptic curves up to isogeny? Equivalently, how to classify lattices up to similitude?

- Start with a basis $\Lambda = \mathbb{Z}\omega_2 \oplus \mathbb{Z}\omega_1$;
- after a possible swap, one can suppose the basis is "direct", *i.e.* $\mathrm{Im}(\frac{\omega_2}{\omega_1}) > 0$.
- for any $A \in \mathrm{SL}_2(\mathbb{Z})$,
$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \stackrel{\textbf{def}}{=} A \cdot \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$
is another direct basis of the **same lattice**.
- Rescale by the similitude $z \mapsto \frac{z}{\omega_1}$ to get $\mathbb{Z} \oplus \mathbb{Z}\tau$, where $\tau \stackrel{\textbf{def}}{=} \frac{\omega_2}{\omega_1}$ is in the open upper half plane ($\mathrm{Im}(\tau) > 0$).

The poincaré upper half plane

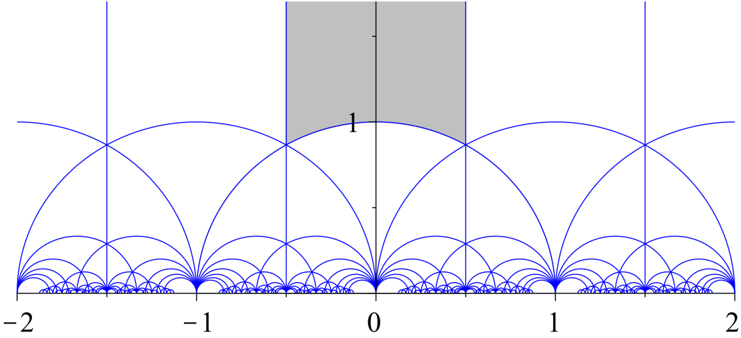
Summary: lattices are classified by elements $\tau \in \mathbb{H}$ up to this action of $\mathsf{SL}_2(\mathbb{Z})$:

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z}), \quad A \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

The poincaré upper half plane

Summary: lattices are classified by elements $\tau \in \mathbb{H}$ up to this action of $\mathrm{SL}_2(\mathbb{Z})$:

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad A \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$



In summary

Elliptic curves up to isomorphism	$\longleftrightarrow$	Complex tori up to biholomorphic isomorphisms	$\longleftrightarrow$	Lattices of $\mathbb{C}$ up to similitudes	$\longleftrightarrow$	Points of $\mathbb{H}$ modulo the action of $\mathrm{SL}_2(\mathbb{Z})$

The curve $X_0(1)$

Theorem 13

The Riemann surface $Y_0(1) \overset{\textit{def}}{=} \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *is biholomorphic to* $\mathbb{A}^1$ *it can be made explicit via the map* $\tau \mapsto \mathscr{E}_\tau \mapsto j(\mathscr{E}_\tau)$. *It can be compactified as*

$$X_0(1) \overset{\textit{def}}{=} \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \quad \textit{where} \quad \mathbb{H}^* \overset{\textit{def}}{=} \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

An the compactification is the Riemann sphere : $X_0(1) \simeq \mathbb{P}^1(\mathbb{C})$.

The curve $X_0(1)$

Theorem 13

The Riemann surface $Y_0(1) \stackrel{def}{=} \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}$ *is biholomorphic to* $\mathbb{A}^1$ *it can be made explicit via the map* $\tau \mapsto \mathscr{E}_\tau \mapsto j(\mathscr{E}_\tau)$. *It can be compactified as*

$$X_0(1) \stackrel{def}{=} \mathrm{SL}_2(\mathbb{Z})\backslash\mathbb{H}^* \quad \text{where} \quad \mathbb{H}^* \stackrel{def}{=} \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}).$$

An the compactification is the Riemann sphere : $X_0(1) \simeq \mathbb{P}^1(\mathbb{C})$.

Remark

$\mathrm{SL}_2(\mathbb{Z})$ *acts transitively on* $\mathbb{P}^1(\mathbb{Q})$ *as* $x \mapsto \frac{ax+b}{cx+d}$.

The curve $X_0(\ell)$

Question 4

Let ℓ be a prime number. How to classify degree ℓ isogenies $\phi : \mathscr{E} \to \mathscr{E}'$ up to isomorphism?

Remark

"up to ismomorphism" means that two isogenies $\phi_1 : \mathscr{E}_1 \to \mathscr{E}_1'$ and $\phi_2 : \mathscr{E}_2 \to \mathscr{E}_2'$ are isomorphic if there exist two isomorphisms $\eta : \mathscr{E}_1 \to \mathscr{E}_2$ and $\nu : \mathscr{E}_1' \to \mathscr{E}_2'$ such that the following diagram commutes.

$$\begin{tikzcd}
\mathscr{E}_1 \arrow[r, "\phi_1"] \arrow[d, "\eta"'] & \mathscr{E}_2 \arrow[d, "\nu"] \\
\mathscr{E}_1' \arrow[r, "\phi_2"] & \mathscr{E}_2'
\end{tikzcd}$$

The curve $X_0(\ell)$

This leads to some "enhanced" version of $X_0(1)$ which is

$$X_0(\ell) \stackrel{\text{def}}{=} \Gamma_0(\ell)\backslash\mathbb{H}^*,$$

where

$$\Gamma_0(\ell) \stackrel{\text{def}}{=} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod \ell \right\}.$$

The modular equation

Actually, modular curves are algebraic!

Theorem 8

There exists an irreducible polynomial $\Phi_\ell \in \mathbb{Z}[x, y]$ such that for any pair $\mathscr{E}, \mathscr{E}'$ of elliptic curves related with a degree ℓ isogeny $\mathscr{E} \to \mathscr{E}'$, then $\Phi_\ell(j(\mathscr{E}), j(\mathscr{E}')) = 0$.

The modular equation

Actually, modular curves are algebraic!

Theorem 8

There exists an irreducible polynomial $\Phi_\ell \in \mathbb{Z}[x, y]$ such that for any pair $\mathscr{E}, \mathscr{E}'$ of elliptic curves related with a degree ℓ isogeny $\mathscr{E} \to \mathscr{E}'$, then $\Phi_\ell(j(\mathscr{E}), j(\mathscr{E}')) = 0$.

Remark

Unfortunately, such a plane representation of $X_0(\ell)$ is highly singular...

The modular equation

Actually, modular curves are algebraic!

Theorem 8

There exists an irreducible polynomial $\Phi_\ell \in \mathbb{Z}[x, y]$ such that for any pair $\mathscr{E}, \mathscr{E}'$ of elliptic curves related with a degree ℓ isogeny $\mathscr{E} \to \mathscr{E}'$, then $\Phi_\ell(j(\mathscr{E}), j(\mathscr{E}')) = 0$.

Remark

Unfortunately, such a plane representation of $X_0(\ell)$ is highly singular...

But... reduction modulo p makes sense.

The genus of $X_0(\ell)$

Theorem 9

For a prime number $\ell > 3$, the genus g_ℓ of $X_0(\ell)$ equals

$$g_\ell = \begin{cases} \frac{\ell-1}{12} - 1 & \text{if } \quad \ell \equiv 1 \mod [12] \\ \frac{\ell-5}{12} & \text{if } \quad \ell \equiv 5 \mod [12] \\ \frac{\ell-7}{12} & \text{if } \quad \ell \equiv 7 \mod [12] \\ \frac{\ell+1}{12} & \text{if } \quad \ell \equiv 11 \mod [12]. \end{cases}$$

The genus of $X_0(\ell)$

Theorem 9

For a prime number $\ell > 3$, the genus g_ℓ of $X_0(\ell)$ equals

$$g_\ell = \begin{cases} \frac{\ell-1}{12} - 1 & \text{if} \quad \ell \equiv 1 \mod [12] \\ \frac{\ell-5}{12} & \text{if} \quad \ell \equiv 5 \mod [12] \\ \frac{\ell-7}{12} & \text{if} \quad \ell \equiv 7 \mod [12] \\ \frac{\ell+1}{12} & \text{if} \quad \ell \equiv 11 \mod [12]. \end{cases}$$

The proof rests on the following well–known statement.

Theorem 14 (Riemann–Hurwitz formula (tame version))

Let $\phi : \mathscr{X} \to \mathscr{Y}$ be a rational map between two curves over $\mathbb{K}$ of characteristic 0. Then, the genera $g_{\mathscr{X}}, g_{\mathscr{Y}}$ of $\mathscr{X}, \mathscr{Y}$ are related by the following formula.

$$(2g_{\mathscr{X}} - 2) = \deg \varphi \cdot (2g_{\mathscr{Y}} - 2) + \sum_{Q \in \mathscr{Y}(\overline{\mathbb{K}})} (e_Q - 1).$$

About Riemann–Hurwitz

Sketch of proof 1/2

Sketch of proof 2/2

Supersingular elliptic curves

Theorem 10

Let $\mathscr{E}$ be an elliptic curve over $\mathbb{F}_q$ (of characteristic p), then

$$\textit{either} \quad \mathscr{E}[p] \simeq \mathbb{Z}/p\mathbb{Z} \quad \textit{or} \quad \mathscr{E}[p] = \{0\}$$

In the latter case the curve is said to be supersingular.

Supersingular elliptic curves

Theorem 10

Let $\mathscr{E}$ be an elliptic curve over $\mathbb{F}_q$ (of characteristic p), then

$$\textit{either}\quad \mathscr{E}[p] \simeq \mathbb{Z}/p\mathbb{Z} \quad \textit{or} \quad \mathscr{E}[p] = \{0\}$$

In the latter case the curve is said to be supersingular.

Theorem 11

A supersingular curve defined over some extension of $\mathbb{F}_p$ is actually always defined over $\mathbb{F}_{p^2}$ and the number of their $\overline{\mathbb{F}}_p$–isomorphism classes is

$$\left\lfloor \frac{p}{12} \right\rfloor + \begin{cases} 0 & \text{if} \quad p \equiv 1 \mod 12 \\ 1 & \text{if} \quad p \equiv 5 \mod 12 \\ 1 & \text{if} \quad p \equiv 7 \mod 12 \\ 2 & \text{if} \quad p \equiv 11 \mod 12. \end{cases}$$

Why are supersingular curves always defined over $\mathbb{F}_{p^2}$?

The main theorem

Theorem 15

The sequence of curves $\mathscr{X}_0(\ell)$ *over* $\mathbb{F}_{p^2}$ *for* $\ell \equiv 11 \mod 12$ *satisfy*

$$\lim_{\ell \to +\infty} \frac{\sharp X_0(\ell)(\mathbb{F}_{p^2})}{g_\ell} = p - 1.$$

Sketch of proof 1/2

Sketch of proof 2/2

What else?

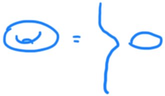
There are other approaches to provide good sequences of curves

- **Still in the modular world**: Shimira curves, Drinfeld modular curves;
- Recursive towers like Garcia Sticthenoth towers;
- Class field towers.

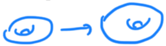
That's all, thank you!

Lattices: →

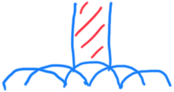
Elliptic curves over $\mathbb{C}$ →



Isogenies: →



Action of $SL_2(\mathbb{Z})$ on $\mathcal{H}$



Supersingular Elliptic curves ← Points of $X_0(\ell)$ mod p ← Mod p ← Modular curve $X_0(\ell)$: ← + Action of $\Gamma_0(\ell)$

$\Downarrow$

Many $\mathbb{F}_{p^2}$-points!

↳ Algebraic Geometry Codes:

→ $\boxed{\text{TVZ Thm}}$