Number of Rational Points of Shimura Curves over Finite Fields

Virgile Ducet[1]

[1]Institut de Mathématiques de Luminy

Arithmetic Geometry and Coding Theory, 3-7 June 2013

Motivation

Theorem (Drinfel'd-Vlăduț)
For any sequence of curves $(C_i)_{i\geqslant 0}$ over $\mathbb{F}_q$ such that $g(C_i) \to \infty$, we have

$$\lim_{i\to\infty} |C_i(\mathbb{F}_q)|/g(C_i) \leqslant \sqrt{q} - 1.$$

When there is equality, we say that $(C_i)_i$ is *optimal*.

Motivation

Theorem (Drinfel'd-Vlăduț)
For any sequence of curves $(C_i)_{i\geqslant 0}$ over $\mathbb{F}_q$ such that $g(C_i) \to \infty$, we have

$$\lim_{i\to\infty} |C_i(\mathbb{F}_q)|/g(C_i) \leqslant \sqrt{q} - 1.$$

When there is equality, we say that $(C_i)_i$ is *optimal*.

If $C_i = X_0(N_i)$ is a modular curve over $\mathbb{F}_p$, then it turns out that the sequence is optimal over $\mathbb{F}_{p^2}$ (Ihara, Tsfasman-Vlăduț-Zink,...).

Motivation

Theorem (Drinfel'd-Vlăduț)
For any sequence of curves $(C_i)_{i\geqslant 0}$ over $\mathbb{F}_q$ such that $g(C_i) \to \infty$, we have

$$\lim_{i\to\infty} |C_i(\mathbb{F}_q)|/g(C_i) \leqslant \sqrt{q} - 1.$$

When there is equality, we say that $(C_i)_i$ is *optimal*.

If $C_i = X_0(N_i)$ is a modular curve over $\mathbb{F}_p$, then it turns out that the sequence is optimal over $\mathbb{F}_{p^2}$ (Ihara, Tsfasman-Vlăduț-Zink,...).

QUESTION: *What happens for the Shimura curves $X_0^{\mathfrak{D}}(\mathfrak{N})$?*

Modular curves

Let N be a positive integer and k a field in which $N \neq 0$. The modular curve $Y_0(N)$ parametrizes elliptic curves E over k together with a cyclic subgroup of $E[N]$ of order N, and $X_0(N)$ is the projective closure of $Y_0(N)$.

Modular curves

Let N be a positive integer and k a field in which $N \neq 0$. The modular curve $Y_0(N)$ parametrizes elliptic curves E over k together with a cyclic subgroup of $E[N]$ of order N, and $X_0(N)$ is the projective closure of $Y_0(N)$.

When $k = \mathbb{C}$, $X_0(N)$ is the compactification of the quotient $\Gamma_0(N)\backslash\mathcal{H}$, where $\mathcal{H}$ is the Poincaré upper half-plane, and $\Gamma_0(N)$ is the subgroup of matrices with determinant 1 of the $\mathbb{Z}$-order

$$\mathcal{O}_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

of $B = \mathrm{M}_2(\mathbb{Q})$.

Modular curves

Let N be a positive integer and k a field in which $N \neq 0$. The modular curve $Y_0(N)$ parametrizes elliptic curves E over k together with a cyclic subgroup of $E[N]$ of order N, and $X_0(N)$ is the projective closure of $Y_0(N)$.

When $k = \mathbb{C}$, $X_0(N)$ is the compactification of the quotient $\Gamma_0(N)\backslash\mathcal{H}$, where $\mathcal{H}$ is the Poincaré upper half-plane, and $\Gamma_0(N)$ is the subgroup of matrices with determinant 1 of the $\mathbb{Z}$-order

$$\mathcal{O}_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

of $B = \mathrm{M}_2(\mathbb{Q})$.

Remark:

B is a quaternion algebra over $\mathbb{Q}$, $\mathcal{O}_0(N)$ is an Eichler order of level N, and $\Gamma_0(N)/\{\pm 1\}$ is a Fuchsian group (that is, a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$).

Quaternion algebras

DEFINITION:

A *quaternion algebra* B *over a field* F *is a central simple algebra of dimension* 4 *over* F.

Quaternion algebras

DEFINITION:

A *quaternion algebra* B *over a field* F *is a central simple algebra of dimension* 4 *over* F.

A quaternion algebra possesses an involution $x \mapsto \bar{x}$, *and we define the reduced norm of* B *by*

$$\mathrm{nrd} : x \mapsto x\bar{x}.$$

Quaternion algebras

DEFINITION:

A *quaternion algebra* B *over a field* F *is a central simple algebra of dimension* 4 *over* F.

A quaternion algebra possesses an involution $x \mapsto \bar{x}$, *and we define the reduced norm of* B *by*

$$\mathrm{nrd} : x \mapsto x\bar{x}.$$

EXAMPLE:

- *The matrix algebra* $B = \mathrm{M}_2(F)$ *is a quaternion algebra, the involution is*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

  and the reduced norm is the determinant.
- *When* $F = \mathbb{R}$, *there is only one division quaternion algebra, the Hamilton quaternions* $\mathbb{H}$.

Ramification

We now let F be a number field. A (finite or infinite) prime $\mathfrak{p}$ of F at which the localisation $B_{\mathfrak{p}} = B \otimes_F F_{\mathfrak{p}}$ is not the matrix algebra $\mathrm{M}_2(F_{\mathfrak{p}})$ is *ramified*.

Ramification

We now let F be a number field. A (finite or infinite) prime $\mathfrak{p}$ of F at which the localisation $B_{\mathfrak{p}} = B \otimes_F F_{\mathfrak{p}}$ is not the matrix algebra $\mathrm{M}_2(F_{\mathfrak{p}})$ is *ramified*.

THEOREM:

The set of ramified places of a quaternion algebra B is finite and even and determines B up to F-isomorphism.
Conversely, for every finite even set S of (finite or infinite) primes of F there exists a quaternion algebra over F which is ramified exactly at the primes of S.

Ramification

We now let F be a number field. A (finite or infinite) prime $\mathfrak{p}$ of F at which the localisation $B_{\mathfrak{p}} = B \otimes_F F_{\mathfrak{p}}$ is not the matrix algebra $\mathrm{M}_2(F_{\mathfrak{p}})$ is *ramified*.

THEOREM:

The set of ramified places of a quaternion algebra B is finite and even and determines B up to F-isomorphism.
Conversely, for every finite even set S of (finite or infinite) primes of F there exists a quaternion algebra over F which is ramified exactly at the primes of S.

DEFINITION:

The discriminant of B is the integral ideal

$$\mathfrak{D}_B = \prod_{\mathfrak{p} \in \mathrm{Ram}(B)^f} \mathfrak{p},$$

where $\mathrm{Ram}(B)^f$ is the set of finite primes of F which are ramified in B.

Eichler orders

DEFINITION:

An *order* $\mathcal{O}$ *in* B *is a subring which is also a* $\mathbb{Z}_F$*-module of finite rank such that* $\mathcal{O} \otimes_{\mathbb{Z}_F} F = B$.

Eichler orders

DEFINITION:

An *order* $\mathcal{O}$ *in* B *is a subring which is also a* $\mathbb{Z}_F$*-module of finite rank such that* $\mathcal{O} \otimes_{\mathbb{Z}_F} F = B$.

Let $\mathfrak{N}$ *be an integral ideal of* F *prime to* $\mathfrak{D}_B$ *and let* $\mathcal{O}(1)$ *be a maximal order. Choose an embedding* $\iota_{\mathfrak{N}} : \mathcal{O}(1) \hookrightarrow \mathcal{O}(1) \otimes \mathbb{Z}_{F,\mathfrak{N}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}})$. *The sub-order* $\mathcal{O}_0(\mathfrak{N})$ *of* $\mathcal{O}(1)$ *such that* $\iota_{\mathfrak{N}}$ *provides an identification*

$$\mathcal{O}_0(\mathfrak{N}) \xrightarrow{\cong} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}}) : c \in \mathfrak{N}\mathbb{Z}_{F,\mathfrak{N}} \right\}$$

is called an Eichler order of level $\mathfrak{N}$.

Eichler orders

Definition:

An *order* $\mathcal{O}$ *in* B *is a subring which is also a* $\mathbb{Z}_F$*-module of finite rank such that* $\mathcal{O} \otimes_{\mathbb{Z}_F} F = B$.

Let $\mathfrak{N}$ *be an integral ideal of* F *prime to* $\mathfrak{D}_B$ *and let* $\mathcal{O}(1)$ *be a maximal order. Choose an embedding* $\iota_{\mathfrak{N}} : \mathcal{O}(1) \hookrightarrow \mathcal{O}(1) \otimes \mathbb{Z}_{F,\mathfrak{N}} \cong \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}})$. *The sub-order* $\mathcal{O}_0(\mathfrak{N})$ *of* $\mathcal{O}(1)$ *such that* $\iota_{\mathfrak{N}}$ *provides an identification*

$$\mathcal{O}_0(\mathfrak{N}) \xrightarrow{\cong} \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_{F,\mathfrak{N}}) : c \in \mathfrak{N}\mathbb{Z}_{F,\mathfrak{N}} \right\}$$

is called an Eichler order of level $\mathfrak{N}$.

Example:

If $B = \mathrm{M}_2(\mathbb{Q})$ *and* $\mathfrak{N} = N$ *is an integer, the subring* $\mathcal{O}_0(N)$ *of the maximal order* $\mathrm{M}_2(\mathbb{Z})$ *is clearly an Eichler order of level* $N\mathbb{Z}$.

Shimura curves

Remark:

In order to have an action of B/F on $\mathcal{H}$, we need an embedding $B \hookrightarrow \mathrm{M}_2(\mathbb{R})$, that is we need at least one unramified real place. And in order to work with Fuchsian groups, we need that F is a totally real number field and that the number of unramified real places is *exactly* 1.

Shimura curves

REMARK:

In order to have an action of B/F on $\mathcal{H}$, we need an embedding $B \hookrightarrow \mathrm{M}_2(\mathbb{R})$, that is we need at least one unramified real place. And in order to work with Fuchsian groups, we need that F is a totally real number field and that the number of unramified real places is *exactly* 1.

So our data will be:

- *B: a quaternion algebra of discriminant $\mathfrak{D}$ over a totally real number field F of degree d over $\mathbb{Q}$.*
- *$\iota_1, \ldots, \iota_d$: the real embeddings of F, such that only for ι_1 we have $B \otimes_{F,\iota_1} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$.*
- *An Eichler order $\mathcal{O}_0(\mathfrak{N})$ of level $\mathfrak{N}$ for an integral ideal $\mathfrak{N}$ prime to $\mathfrak{D}$, and its subgroup $\mathcal{O}_0^1(\mathfrak{N})$ of elements of norm 1.*
- *The Shimura curve $X_0^{\mathfrak{D}}(\mathfrak{N}) = \iota_1(\mathcal{O}_0^1(\mathfrak{N}))\backslash\mathcal{H} = \Gamma_0^{\mathfrak{D}}(\mathfrak{N})\backslash\mathcal{H}$.*

Modular forms

We now assume that $B \neq M_2(\mathbb{Q})$, so that $X_0^{\mathfrak{D}}(\mathfrak{N})$ is compact (thus there are no cusps).

Modular forms

We now assume that $B \neq M_2(\mathbb{Q})$, so that $X_0^{\mathfrak{D}}(\mathfrak{N})$ is compact (thus there are no cusps).

DEFINITION:

A *modular form (of level 2) for* $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ *is a holomorphic function* $f : \mathcal{H} \to \mathbb{C}$ *such that for every*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0^{\mathfrak{D}}(\mathfrak{N})$$

we have the transformation property:

$$f(\gamma \cdot \tau) = f\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{1}{(c\tau + d)^2} f(\tau).$$

The $\mathbb{C}$*-vector space of modular forms for* $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ *is denoted by* $S_2^{\mathfrak{D}}(\mathfrak{N})$.

Modular forms

We now assume that $B \neq M_2(\mathbb{Q})$, so that $X_0^{\mathfrak{D}}(\mathfrak{N})$ is compact (thus there are no cusps).

DEFINITION:

A *modular form (of level 2) for* $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ *is a holomorphic function* $f : \mathcal{H} \to \mathbb{C}$ *such that for every*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0^{\mathfrak{D}}(\mathfrak{N})$$

we have the transformation property:

$$f(\gamma \cdot \tau) = f\left(\frac{a\tau + b}{c\tau + d}\right) = \frac{1}{(c\tau + d)^2} f(\tau).$$

The $\mathbb{C}$*-vector space of modular forms for* $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$ *is denoted by* $S_2^{\mathfrak{D}}(\mathfrak{N})$*. Equivalently, this is the set of global sections of the sheaf of holomorphic differential* 1*-forms on* $X_0^{\mathfrak{D}}(\mathfrak{N})$ *(there is an isomorphism* $f \mapsto f(\tau)d\tau$*).*

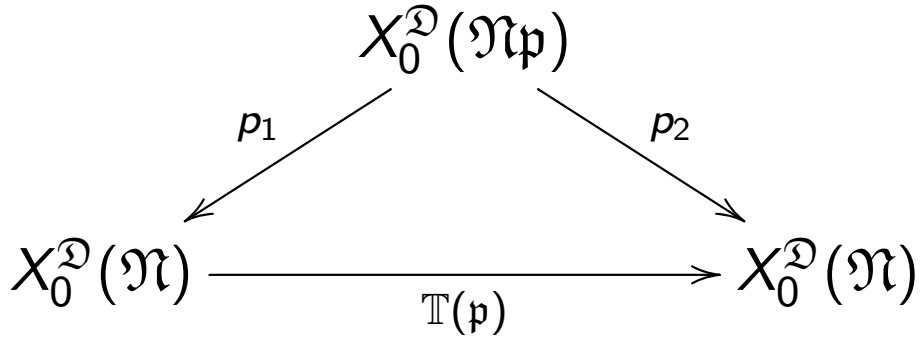
Hecke correspondences

From now on, we assume that the narrow class number h^+ of F is 1, which means that every ideal of F admits a totally positive generator.

Hecke correspondences

From now on, we assume that the narrow class number h^+ of F is 1, which means that every ideal of F admits a totally positive generator.

For every prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ of F, we have the *Hecke correspondence*

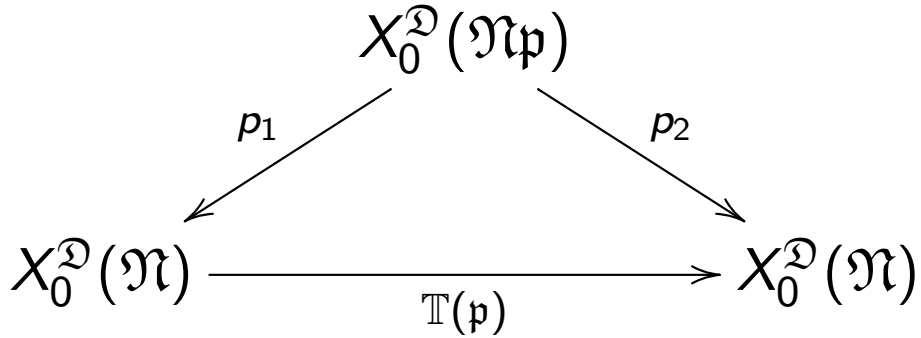


which induces the well defined Hecke operator $\mathbb{T}(\mathfrak{p}) = {p_2}_* \circ {p_1}^*$ *on* $S_2^{\mathfrak{D}}(\mathfrak{N}) = \mathrm{H}^0(X_0^{\mathfrak{D}}(\mathfrak{N}), \Omega^1)$.

Hecke correspondences

From now on, we assume that the narrow class number h^+ of F is 1, which means that every ideal of F admits a totally positive generator.

For every prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$ of F, we have the *Hecke correspondence*



which induces the well defined Hecke operator $\mathbb{T}(\mathfrak{p}) = {p_2}_* \circ {p_1}^*$ *on* $S_2^{\mathfrak{D}}(\mathfrak{N}) = \mathrm{H}^0(X_0^{\mathfrak{D}}(\mathfrak{N}), \Omega^1)$.

Finally, note that we have

$$\mathrm{Jac}(X_0^{\mathfrak{D}}(\mathfrak{N})) = \mathrm{H}^0(X_0^{\mathfrak{D}}(\mathfrak{N}), \Omega^1)^\vee / \mathrm{H}_1(X_0^{\mathfrak{D}}(\mathfrak{N}), \mathbb{Z}),$$

so the Hecke operator induces a well-defined endomorphism on $\mathrm{Jac}(X_0^{\mathfrak{D}}(\mathfrak{N}))$, *of degree* $\mathrm{N}(\mathfrak{p}) + 1$.

Eichler-Shimura congruence relation

The curve $X_0^{\mathfrak{D}}(\mathfrak{N})$ admits a model $\mathrm{Sh}_0^{\mathfrak{D}}(\mathfrak{N})$ over F, which has good reduction $\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N})$ at any prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$. Let $\mathbb{F}_q = \mathbb{F}_{\mathfrak{p}}$.

After reduction modulo $\mathfrak{p}$, we have an equality

$$\widetilde{\mathbb{T}}(\mathfrak{p}) = \mathrm{Frob}(\mathfrak{p}) + \mathrm{Ver}(\mathfrak{p}).$$

Eichler-Shimura congruence relation

The curve $X_0^{\mathfrak{D}}(\mathfrak{N})$ admits a model $\mathrm{Sh}_0^{\mathfrak{D}}(\mathfrak{N})$ over F, which has good reduction $\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N})$ at any prime $\mathfrak{p} \nmid \mathfrak{D}\mathfrak{N}$. Let $\mathbb{F}_q = \mathbb{F}_{\mathfrak{p}}$.

After reduction modulo $\mathfrak{p}$, we have an equality

$$\widetilde{\mathbb{T}}(\mathfrak{p}) = \mathrm{Frob}(\mathfrak{p}) + \mathrm{Ver}(\mathfrak{p}).$$

COROLLARY:

- We have
$$Z(\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N}), t) = \frac{\det(1 - \mathbb{T}(\mathfrak{p})t + qt^2)}{(1-t)(1-qt)}.$$
- For any $r \geqslant 1$, we have
$$|\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N})(\mathbb{F}_{q^r})| = q^r + 1 - \mathrm{Tr}(\mathbb{T}(\mathfrak{p}^r) - q\mathbb{T}(\mathfrak{p}^{r-2})),$$
with the conventions $\mathbb{T}(\mathfrak{p}^{-1}) = 0$ and $\mathbb{T}(\mathfrak{p}^0) = \mathrm{Id}$.

Eichler-Selberg trace formula

For every $r \geqslant 1$, the trace of $\mathbb{T}(\mathfrak{p}^r)$ on $S_2^{\mathfrak{D}}(\mathfrak{N})$ is equal to

$$\delta(r)\frac{\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))}{4\pi} - \frac{1}{2}\sum_{\mathcal{P}(\mathfrak{p}^r)}\sum_{R}\frac{h(R)}{[R^\times : \mathbb{Z}_F^\times]}m(R),$$

where

- $\delta(r) = 1$ if r is even, and 0 else.
- vol is the volume for the hyperbolic measure $(dx^2 + dy^2)/y^2$ on $\mathcal{H}$.
- $\mathcal{P}(\mathfrak{p}^r)$ is the set of polynomials $P(X) = X^2 - tX + p^r \in \mathbb{Z}_F[X]$ such that p^r is a totally positive generator of $\mathfrak{p}^r$, and $t^2 - 4p^r$ is totally negative.
- For every such $P(X)$, R runs through all the orders of $K = F[X]/P(X)$ containing $\mathbb{Z}_F[X]/P(X)$.
- $m(R)$ is the number of classes of embeddings $\iota : K \hookrightarrow B$ which are optimal, that is such that $\iota(K) \cap \mathcal{O}_0(\mathfrak{N}) = R$, modulo conjugation by $\mathcal{O}_0(\mathfrak{N})^\times$.

Consequences

Set $\sum(-1) = 0$, and for every integer $r \geqslant 0$

$$\sum(r) = \sum_{\mathcal{P}(\mathfrak{p}^r)} \sum_{R} \frac{h(R)}{[R^\times : \mathbb{Z}_F^\times]} m(R).$$

PROPOSITION:

For every integer $r \geqslant 1$, $N_r = |\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N})(\mathbb{F}_{q^r})|$ is equal to

$$q^r + 1 + \delta(r)(q-1)\frac{\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))}{4\pi} + \frac{1}{2}\left(\sum(r) - q\sum(r-2)\right).$$

Proposition:

$\sum(r) - q\sum(r-2)$ is positive.

As a consequence, we have that $N_r \geqslant \delta(r)(q-1)\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))/4\pi$.

PROPOSITION:

$\sum(r) - q\sum(r-2)$ is positive.

As a consequence, we have that $N_r \geqslant \delta(r)(q-1)\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))/4\pi$.

Now the genus g of $X_0^{\mathfrak{D}}(\mathfrak{N})$ satisfies

$$2g - 2 = \frac{1}{2\pi}\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N})) - \sum_q e_q \left(1 - \frac{1}{q}\right),$$

where e_q is the number of elliptic points of order q in $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$.

PROPOSITION:
$\sum(r) - q\sum(r-2)$ is positive.

As a consequence, we have that $N_r \geqslant \delta(r)(q-1)\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))/4\pi$.

Now the genus g of $X_0^{\mathfrak{D}}(\mathfrak{N})$ satisfies

$$2g - 2 = \frac{1}{2\pi}\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N})) - \sum_q e_q \left(1 - \frac{1}{q}\right),$$

where e_q is the number of elliptic points of order q in $\Gamma_0^{\mathfrak{D}}(\mathfrak{N})$.

Putting these together, we obtain:

$$N_2/(g-1) \geqslant \frac{(q-1)\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))/4\pi}{\mathrm{vol}(X_0^{\mathfrak{D}}(\mathfrak{N}))/4\pi} = q - 1 = \sqrt{q^2} - 1,$$

so by the Drinfel'd-Vlăduț theorem, sequences of Shimura curves of the form $X_0^{\mathfrak{D}}(\mathfrak{N})$ will form asymptotically optimal sequences of curves over $\mathbb{F}_{q^2}$.

Recursive Towers

Let $\mathfrak{N}$ and $\mathfrak{n}$ be two relatively prime integral ideals of F such that $(\mathfrak{D}, \mathfrak{N}\mathfrak{n}) = 1$. For every index $i \geqslant 1$ we can define an Atkin-Lehner involution ω_i on $X_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^i)$.

Define the maps $f = \pi_0$ and $g = \omega_1 \circ \pi_0 \circ \omega_2$, where $\pi_0 : X_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^2) \to X_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n})$ is the projection map.

Recursive Towers

Let $\mathfrak{N}$ and $\mathfrak{n}$ be two relatively prime integral ideals of F such that $(\mathfrak{D}, \mathfrak{Nn}) = 1$. For every index $i \geqslant 1$ we can define an Atkin-Lehner involution ω_i on $X_0^{\mathfrak{D}}(\mathfrak{Nn}^i)$.

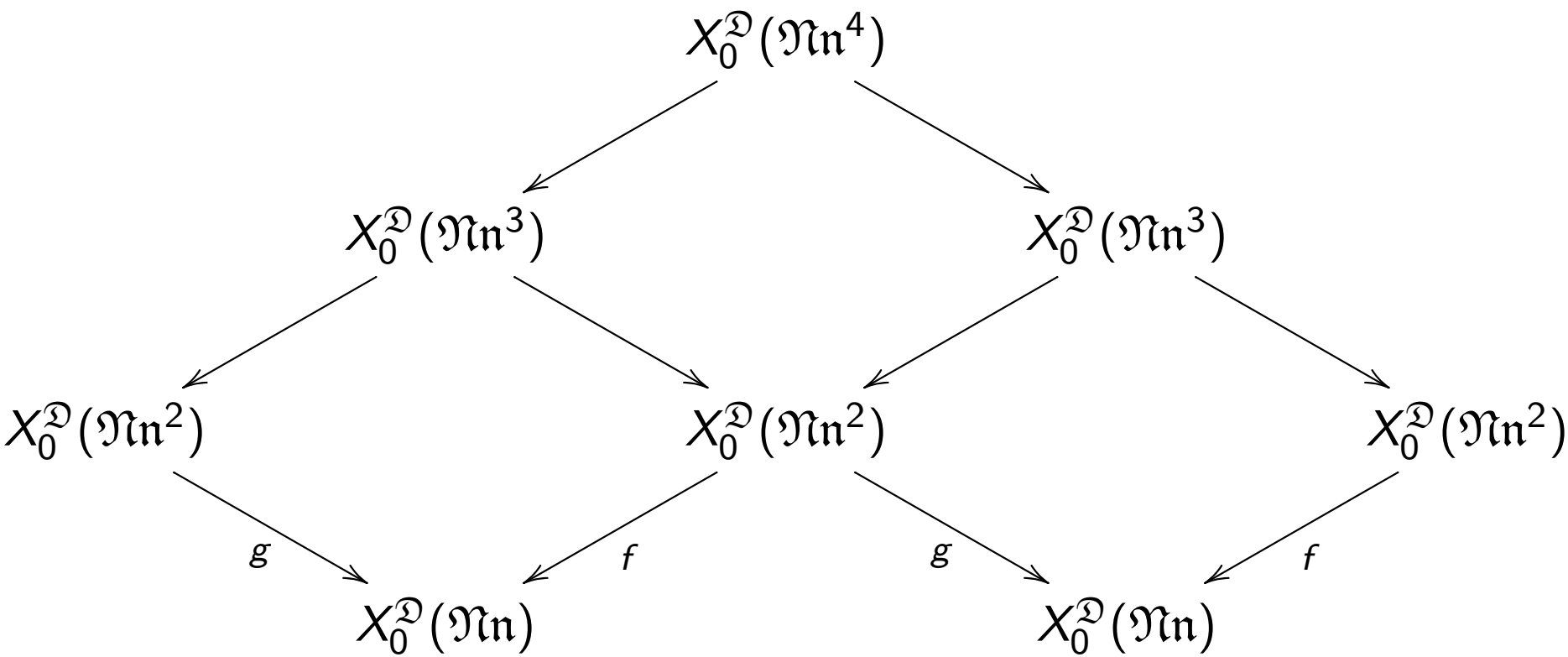
Define the maps $f = \pi_0$ and $g = \omega_1 \circ \pi_0 \circ \omega_2$, where $\pi_0 : X_0^{\mathfrak{D}}(\mathfrak{Nn}^2) \to X_0^{\mathfrak{D}}(\mathfrak{Nn})$ is the projection map.

PROPOSITION:
For every $i \geqslant 3$, $X_0^{\mathfrak{D}}(\mathfrak{Nn}^i)$ is the i-th floor of the recursive tower defined by the maps g and f.

Concretely, this means that for $i \geqslant 3$ we have a bijection between $X_0^{\mathfrak{D}}(\mathfrak{Nn}^i)$ and

$$\{(P_1, \ldots, P_{i-1}) \in X_0^{\mathfrak{D}}(\mathfrak{Nn}^2)^{i-1} : g(P_j) = f(P_{j+1}) \text{ for } j = 1, \ldots, i-2\}.$$

Example: 4-th floor



Over finite fields

For any prime $\mathfrak{p}$ not dividing $\mathfrak{D}\mathfrak{N}\mathfrak{n}$, the previous description descends over $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$ to the curves $\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^i)$.

Consequence: The curves $(\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^i))_{i\geqslant 3}$ form asymptotically optimal recursive towers over $\mathbb{F}_{q^2}$.

Over finite fields

For any prime $\mathfrak{p}$ not dividing $\mathfrak{D}\mathfrak{N}\mathfrak{n}$, the previous description descends over $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q$ to the curves $\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^i)$.

Consequence: The curves $(\widetilde{\mathrm{Sh}}_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^i))_{i\geqslant 3}$ form asymptotically optimal recursive towers over $\mathbb{F}_{q^2}$.

Example:
A computer search for Shimura curves of the form $X_0^{\mathfrak{D}}(\mathfrak{N}\mathfrak{n}^2)$ of small genus, together with the computation of the maps f and g should provide new equations of recursive towers, or a modular interpretation for already known ones (John Voight).

Under the rug: modular interpretation

Definition:

We say that B is *definite* (*resp.* *totally indefinite*) *if all real places of* F *are ramified (resp. unramified).*

Theorem (Albert)

A complex abelian variety has quaternionic multiplication by B *only if* B *is either definite or totally indefinite.*

Under the rug: modular interpretation

Definition:
We say that B is *definite* *(resp. totally indefinite)* *if all real places of F are ramified (resp. unramified).*

Theorem (Albert)
A complex abelian variety has quaternionic multiplication by B only if B is either definite or totally indefinite.

Therefore, when $F \neq \mathbb{Q}$ there is no natural interpretation of $X_0^{\mathfrak{D}}(\mathfrak{N})$ as a moduli space of complex abelian varieties, and thus no natural moduli definition of Hecke and Atkin-Lehner operators. One has to consider a quadratic extension F' of F and consider a moduli problem there.

Under the rug: adèlic theory

The natural way to work with quaternion algebras and to define Hecke and Atkin-Lehner operators is via matrices, which is not possible globally except if $B = \mathrm{M}_2(\mathbb{Q})$ (modular curves). But this is possible locally since $B \otimes F_{\mathfrak{p}} \cong \mathrm{M}_2(F_{\mathfrak{p}})$ if $\mathfrak{p} \nmid \mathfrak{D}$. We thus need to adèlize everything, which leads to the definition of a *Shimura curve as a quotient*

$$X(K) = B^{\times} \backslash (\mathcal{H}^{\pm} \times \hat{B}) / K,$$

where $\hat{B} = B \otimes \hat{\mathbb{Z}}$ *and* K *is a compact open subgroup of* $\hat{B}^{\times}$.

Under the rug: adèlic theory

The natural way to work with quaternion algebras and to define Hecke and Atkin-Lehner operators is via matrices, which is not possible globally except if $B = \mathrm{M}_2(\mathbb{Q})$ (modular curves). But this is possible locally since $B \otimes F_{\mathfrak{p}} \cong \mathrm{M}_2(F_{\mathfrak{p}})$ if $\mathfrak{p} \nmid \mathfrak{D}$. We thus need to adèlize everything, which leads to the definition of a *Shimura curve as a quotient*

$$X(K) = B^{\times} \backslash (\mathcal{H}^{\pm} \times \hat{B}) / K,$$

where $\hat{B} = B \otimes \hat{\mathbb{Z}}$ *and* K *is a compact open subgroup of* $\hat{B}^{\times}$.

PROBLEM: *This curve is generally not connected, it can be written as a finite disjoint union of connected compact Riemann surfaces of the form* $X_i = \Gamma_i \backslash \mathcal{H}$*:*

$$X(K) = \bigsqcup X_i.$$

Under the rug: link with the classical theory

When $K = \hat{\mathcal{O}}_0(\mathfrak{N})$ for an Eichler order $\mathcal{O}_0(\mathfrak{N})$, the disjoint union is indexed by the narrow class group $\mathrm{Cl}^+(F)$, and we can define Hecke operators $\mathbb{T}(\mathfrak{p})$ on $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ and Atkin-Lehner operators $\omega(\mathfrak{p})$ on $X(\hat{\mathcal{O}}_0(\mathfrak{N}\mathfrak{p}^i))$ locally everywhere, and thus globally. The set of connected components is fixed pointwise if and only if $[\mathfrak{p}] = 0$ in $\mathrm{Cl}^+(F)$ (for instance if $h^+ = 1$).

Under the rug: link with the classical theory

When $K = \hat{\mathcal{O}}_0(\mathfrak{N})$ for an Eichler order $\mathcal{O}_0(\mathfrak{N})$, the disjoint union is indexed by the narrow class group $\mathrm{Cl}^+(F)$, and we can define Hecke operators $\mathbb{T}(\mathfrak{p})$ on $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ and Atkin-Lehner operators $\omega(\mathfrak{p})$ on $X(\hat{\mathcal{O}}_0(\mathfrak{N}\mathfrak{p}^i))$ locally everywhere, and thus globally. The set of connected components is fixed pointwise if and only if $[\mathfrak{p}] = 0$ in $\mathrm{Cl}^+(F)$ (for instance if $h^+ = 1$).

The 'neutral' component of $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ is the quotient $X_0^+(\mathfrak{N}) = \iota_1(\mathcal{O}_0^+(\mathfrak{N}))\backslash\mathcal{H}$, where $\mathcal{O}_0^+(\mathfrak{N})$ is the subgroup of elements of $\mathcal{O}_0(\mathfrak{N})$ of totally positive norm. When $h^+ = h$ (for instance if $h^+ = 1$), we have an isomorphism $X_0^+(\mathfrak{N}) = X_0^{\mathfrak{D}}(\mathfrak{N})$, which is the reason why we have a good arithmetic theory for $X_0^{\mathfrak{D}}(\mathfrak{N})$.

Under the rug: link with the classical theory

When $K = \hat{\mathcal{O}}_0(\mathfrak{N})$ for an Eichler order $\mathcal{O}_0(\mathfrak{N})$, the disjoint union is indexed by the narrow class group $\mathrm{Cl}^+(F)$, and we can define Hecke operators $\mathbb{T}(\mathfrak{p})$ on $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ and Atkin-Lehner operators $\omega(\mathfrak{p})$ on $X(\hat{\mathcal{O}}_0(\mathfrak{N}\mathfrak{p}^i))$ locally everywhere, and thus globally. The set of connected components is fixed pointwise if and only if $[\mathfrak{p}] = 0$ in $\mathrm{Cl}^+(F)$ (for instance if $h^+ = 1$).

The 'neutral' component of $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ is the quotient $X_0^+(\mathfrak{N}) = \iota_1(\mathcal{O}_0^+(\mathfrak{N}))\backslash\mathcal{H}$, where $\mathcal{O}_0^+(\mathfrak{N})$ is the subgroup of elements of $\mathcal{O}_0(\mathfrak{N})$ of totally positive norm. When $h^+ = h$ (for instance if $h^+ = 1$), we have an isomorphism $X_0^+(\mathfrak{N}) = X_0^{\mathfrak{D}}(\mathfrak{N})$, which is the reason why we have a good arithmetic theory for $X_0^{\mathfrak{D}}(\mathfrak{N})$.

CONSEQUENCE: Concerning the arithmetic theory, the natural analogues of the modular curves $X_0(N)$ are $X_0^+(\mathfrak{N})$, rather than $X_0^{\mathfrak{D}}(\mathfrak{N})$.

Generalization of results

The curve $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ admits a model over F, whereas $X_0^+(\mathfrak{N})$ admits a model over the narrow Hilbert class field F^+ of F. In the case where $[\mathfrak{p}] = 0$ in $\mathrm{Cl}^+(F)$, we have Hecke and Atkin-Lehner operators on $X_0^+(\mathfrak{N})$.

Generalization of results

The curve $X(\hat{\mathcal{O}}_0(\mathfrak{N}))$ admits a model over F, whereas $X_0^+(\mathfrak{N})$ admits a model over the narrow Hilbert class field F^+ of F. In the case where $[\mathfrak{p}] = 0$ in $\mathrm{Cl}^+(F)$, we have Hecke and Atkin-Lehner operators on $X_0^+(\mathfrak{N})$.

By class field theory, $\mathfrak{p}$ is totally split in F^+, so if we take a prime $\mathfrak{P}$ of F^+ over $\mathfrak{p}$ and reduce modulo it, we will obtain a curve defined over $F_{\mathfrak{P}} = F_{\mathfrak{p}} = F_q$. Therefore with our formulas the ratio "number of points / genus" will be greater than

$$q - 1 = \mathrm{N}(\mathfrak{p}) - 1 = \mathrm{N}(\mathfrak{P}) - 1 = \sqrt{\mathrm{N}(\mathfrak{P})^2} - 1$$

and the results on optimality will remain true.