Elliptic Curves: complex multiplication, application, and generalization

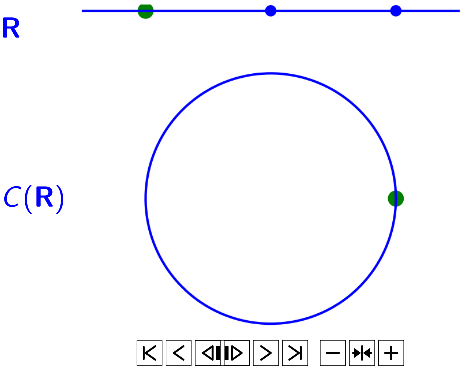
Marco Streng

Mathematisch Instituut
Universiteit Leiden

General Mathematics Colloquium
Universiteit Leiden
14th November 2013

Part 0: The unit circle

- $C(\mathbf{R}) = \{(x, y) \in \mathbf{R}^2 : x^2 + y^2 = 1\}$
- parametrized by $\mathbf{R} \to C(\mathbf{R}) : z \mapsto (\cos(2\pi z), \sin(2\pi z))$
- bijection $\mathbf{R}/\mathbf{Z} \to C(\mathbf{R})$



- Addition in $\mathbf{R}$ is addition of angles.
- $\cos(v + w) = \cos(v)\cos(w) - \sin(v)\sin(w)$

Addition on the circle

Addition formulas:

- $\cos(v+w) = \cos(v)\cos(w) - \sin(v)\sin(w)$
- $\sin(v+w) = \sin(v)\cos(w) + \cos(v)\sin(w)$
- $\sin(v)^2 = 1 - \cos(v)^2$

Repeated application:

- $\cos(n\cdot v) = \cos((n-1)\cdot v)\cos(v) - \sin((n-1)\cdot v)\sin(v) = \cdots$
- $\cos(n\cdot v) = P_n(\cos(v))$ for some polynomial $P_n \in \mathbf{Q}[X]$

Example:

- $P_5(X) = 16X^5 - 20X^3 + 5X$

Conclusion:

- Given $\frac{m}{n} \in \mathbf{Q}$, get $P_n\left(\cos(2\pi\frac{m}{n})\right) = \cos(2\pi m) = 1$
- so $\cos(2\pi\frac{m}{n})$ is a root of $P_n - 1$.

Angle multiplication

Polynomials

- $\cos(b \cdot v) = P_b(\cos(v))$

Roots

- $x = \cos(2\pi \frac{a}{b})$ is a root of $P_b - 1$ (x is algebraic over $\mathbf{Q}$)
- One root $x_1 = \cos(2\pi \frac{1}{b})$ yields all roots $x = P_a(x_1)$ with $a \in \mathbf{Z}$ (x is Galois over $\mathbf{Q}$)
- $P_a(P_c(x)) = P_{ac}(x) = P_c(P_a(x))$ (x is abelian over $\mathbf{Q}$)

Kronecker-Weber Theorem (K-W-Hilbert 19th century).

- The maximal real abelian extension of $\mathbf{Q}$ is generated by

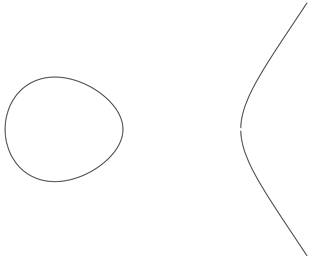
$$\{\cos(2\pi z) \ : \ z \in \mathbf{Q}\}.$$

Part 1: elliptic curves

Let k be a field of characteristic not 2 or 3
(e.g., $k = \mathbf{R}$, $k = \mathbf{C}$, $k = \mathbf{F}_p = (\mathbf{Z}/p\mathbf{Z})$ for $p \geq 5$ prime).

- An elliptic curve is a smooth projective curve

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

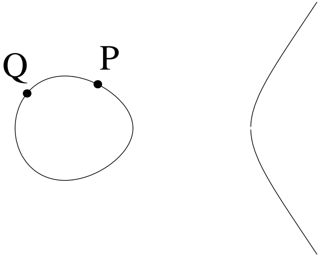


Part 1: elliptic curves

Let k be a field of characteristic not 2 or 3
(e.g., $k = \mathbf{R}$, $k = \mathbf{C}$, $k = \mathbf{F}_p = (\mathbf{Z}/p\mathbf{Z})$ for $p \geq 5$ prime).

- An elliptic curve is a smooth projective curve

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

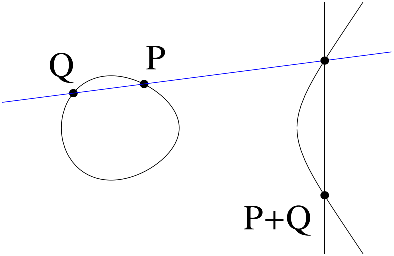


Part 1: elliptic curves

Let k be a field of characteristic not 2 or 3
(e.g., $k = \mathbf{R}$, $k = \mathbf{C}$, $k = \mathbf{F}_p = (\mathbf{Z}/p\mathbf{Z})$ for $p \geq 5$ prime).

- An elliptic curve is a smooth projective curve

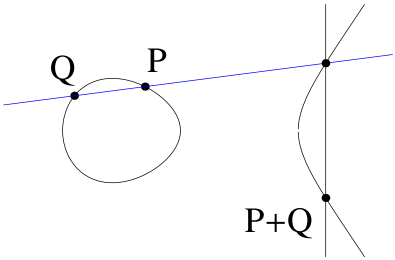
$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$



- $E(k)$ is a commutative algebraic group with unit ∞

Part 1: elliptic curves

- $$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

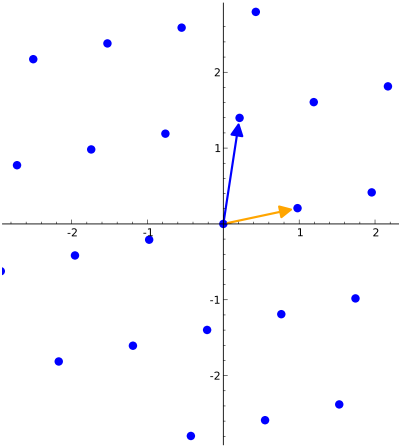


- $E(k)$ is a commutative algebraic group with unit ∞
- $nP = P + P + \cdots + P$
- $x(nP) = F_n(x(P))$ with $F_n \in \mathbf{Q}(X)$

Lattices

Definition:

- A lattice $\Lambda \subset \mathbf{C}$ is a subgroup that can be written as $\Lambda = \omega_1\mathbf{Z} + \omega_2\mathbf{Z}$ with $\tau = \frac{\omega_1}{\omega_2} \in \mathbf{C} \setminus \mathbf{R}$.



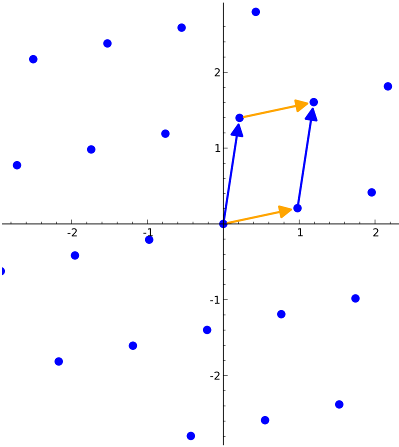
Lattices

Definition:

- A lattice $\Lambda \subset \mathbf{C}$ is a subgroup that can be written as $\Lambda = \omega_1\mathbf{Z} + \omega_2\mathbf{Z}$ with $\tau = \frac{\omega_1}{\omega_2} \in \mathbf{C} \setminus \mathbf{R}$.

Complex torus:

- $\mathbf{C}/\Lambda$
- $\mathbf{C}/\Lambda \cong E(\mathbf{C})$ complex analytically for some $E(\mathbf{C})$
- Compare to $\mathbf{R}/\mathbf{Z} \cong C(\mathbf{R})$



Endomorphisms

The endomorphism ring:

Let $\mathcal{O} = \{\alpha \in \mathbf{C} : \alpha\Lambda \subset \Lambda\}$. Then

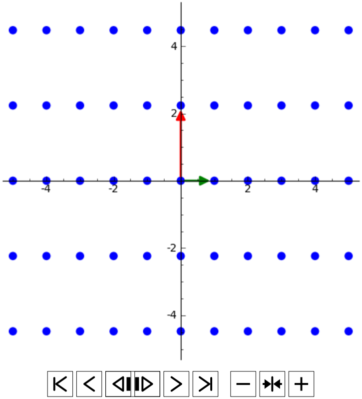
- Either $\mathcal{O} = \mathbf{Z}$ or $\mathcal{O} = \alpha\mathbf{Z} + \mathbf{Z}$ for some $\alpha \in \mathbf{C} \setminus \mathbf{R}$.
- Second case: "complex multiplication"

Example:

- Given $n \in \mathbf{Z}_{>0}$, let $\Lambda = \sqrt{-n}\mathbf{Z} + \mathbf{Z}$. Then $\sqrt{-n}\Lambda \subset \Lambda$.
- In fact, $\mathcal{O} = \sqrt{-n}\mathbf{Z} + \mathbf{Z}$.

Facts:

- For $\alpha \in \mathcal{O}$, get point αP
- and formula $x(\alpha P) = F_\alpha(x(P))$



$\mathbf{Z}[i]$

Example:

- $i = \sqrt{-1}$, $\mathcal{O} = \Lambda = i\mathbf{Z} + \mathbf{Z}$
- Fact: corresponds to $E : y^2 = x^3 + x$
- Multiplication-by-i formula on E, given by $i : (x, y) \mapsto (-x, iy)$

More generally:

- Let $K = \mathbf{Q}(i) = \mathbf{Q} + i\mathbf{Q}$
- Multiplication-by-α formula for each $\alpha \in \mathcal{O}$
- $x(\alpha P) = F_\alpha(x(P))$ with $F_\alpha \in K(X)$

Example:

- $F_{2+i} = -\dfrac{(4i-3)\,x^5 + (20i+10)\,x^3 + 25\,x}{25\,x^4 + (20i+10)\,x^2 + 4i - 3}$

$\mathbf{Z}[i]$

More generally:

- Let $K = \mathbf{Q}(i) = \mathbf{Q} + i\mathbf{Q}$
- Multiplication-by-α formula for each $\alpha \in \mathcal{O}$
- $x(\alpha P) = F_\alpha(x(P))$ with $F_\alpha \in K(X)$

Example:

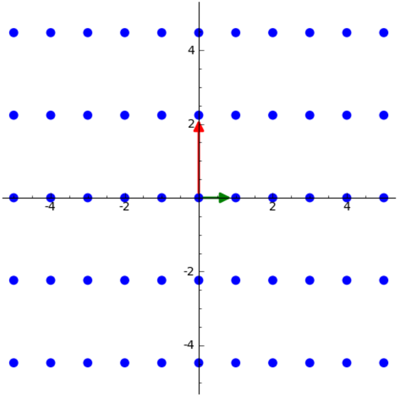
- $F_{2+i} = -\dfrac{(4i-3)\,x^5 + (20i+10)\,x^3 + 25\,x}{25\,x^4 + (20i+10)\,x^2 + 4i - 3}$

Facts:

- The poles of F_n generate abelian extensions of K
- This yields all abelian extensions of K

Bigger example: $\mathbf{Z}[\sqrt{-5}]$

$\Lambda = \sqrt{-5}\mathbf{Z} + \mathbf{Z}$



corresponds to

$$E : y^2 = x^3 + (-3609a - 8070)\,x + (-176356a - 394344)\,, \quad a = \sqrt{5}$$

$$\sqrt{-5} : (x, y) \mapsto \left(\frac{x^5 + (94a + 210)\,x^4 + \cdots + 8661458880a + 19367610840}{-(ax^2 + (105a + 235)\,x + 5117a + 11442)^2}, \cdots \right.$$

The Hilbert class polynomial

Definition: The j-invariant is

$$j(E) = 1728 \frac{4b^3}{4b^3 + 27c^2} \quad \text{for} \quad E : y^2 = x^3 + bx + c.$$

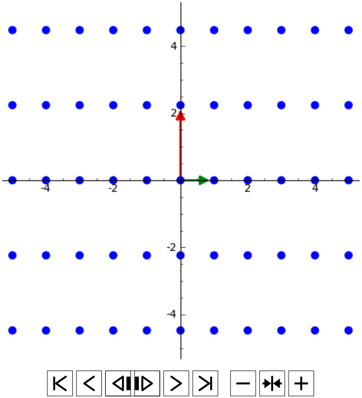
Bijection:

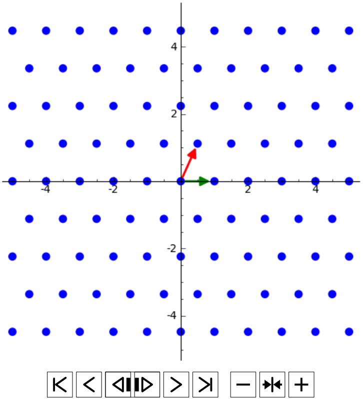
$$j : \frac{\{\text{lattices } \Lambda\}}{\mathbf{C}^*\text{-scaling}} = \frac{\{\text{ell. curves } E(\mathbf{C})\}}{\cong} \longrightarrow \mathbf{C}$$

Definition:
For any $\mathcal{O}$ as before, the Hilbert class polynomial of $\mathcal{O}$ is

$$H_{\mathcal{O}} = \prod_{\substack{\Lambda \text{ up to scaling} \\ \mathcal{O}(\Lambda)=\mathcal{O}}} \big(X - j(\Lambda)\big) \quad \in \mathbf{Z}[X].$$

Example: $\mathcal{O} = \mathbf{Z}[\sqrt{-5}]$ again





$j(\sqrt{-5}\mathbf{Z} + \mathbf{Z}) \approx 1264538.90947514$ $j(\frac{\sqrt{-5}+1}{2}\mathbf{Z}+\mathbf{Z}) \approx -538.90947514$

So $H_{\mathcal{O}} \approx (X - 1264538.90947514)(X + 538.90947514)$
$\approx X^2 - 1264000.000X - 681471999.999$

In fact, $H_{\mathcal{O}} = X^2 - 1264000X - 681472000$

Applications

Application 1:

Generate all abelian extensions of $\mathbf{Q}(\sqrt{-n})$.

Application 2:

Construct elliptic curves of prescribed order:

- Let $\mathcal{O} = \mathbf{Z} + \mathbf{Z}\sqrt{-n}$, with $d = -n < 0$.
- Given $\pi = x + y\sqrt{-n}$, suppose $p = x^2 + ny^2$ is prime.
- Then ($H_{\mathcal{O}}$ mod p) can be used for constructing an elliptic curve E over $\mathbf{F}_p$ with $N := p + 1 - 2x$ points.
- By choosing suitable π, can make sure $N/2$ is a large prime.

Intermezzo: cryptography

Symmetric encryption (private-key):

Alice	(communication channel)	Bob
$M \xrightarrow[\text{key } k]{} C$	C	$C \xrightarrow[\text{key } k]{} M$

Efficient, but need to agree on a key k first.

Asymmetric encryption (public-key):

Alice	(communication channel)	Bob
$M \xrightarrow[\text{public key } e]{} C$	C	$C \xrightarrow[\text{private key } d]{} M$

Other asymmetric schemes:

- key agreement
- signatures and identification
- ...

RSA

Public-key scheme by Rivest, Shamir and Adleman (1977).

- When generating the keys, take two random primes p and q of (say) 200 digits each.
- Part of the public key: the product $N = p \cdot q$.
- Finding p and q is factoring N, and breaks the encryption.

Currently used in

- almost all secure web pages

- all Dutch bank cards

Diffie-Hellman key exchange (1976)

Goal: agree on a key for symmetric encryption

Alice	(communication channel)	Bob
random $a \in \mathbf{Z}$ and some $x \in \mathbf{F}_p^*$	$p, x, x^a \longrightarrow$	random $b \in \mathbf{Z}$
	$\longleftarrow x^b$	
shared key: $x^{(ab)} = (x^b)^a$		shared key: $x^{(ab)} = (x^a)^b$

- Given only p, x, x^a, x^b, it is believed to be computationally hard to find $x^{(ab)}$.
- Finding a is the discrete logarithm problem in $\mathbf{F}_p^*$, and breaks the scheme.

Elliptic curve crypto, Koblitz and Miller (1985)

Replace $\mathbf{F}_p^*$ by $E(\mathbf{F}_p)$ in any discrete log cryptosystem, e.g.:

Alice	(communication channel)	Bob
random $a \in \mathbf{Z}$ and some $P \in E(\mathbf{F}_p)$	$E, P, a \cdot P \longrightarrow$	random $b \in \mathbf{Z}$
	$\longleftarrow b \cdot P$	
shared key: $(ab) \cdot P = a \cdot (b \cdot P)$		shared key: $(ab) \cdot P = b \cdot (a \cdot P)$

- Given only E, P, $a \cdot P$, $b \cdot P$, it is believed to be computationally hard to find $(ab) \cdot P$.
- Finding a is the discrete logarithm problem in $E(\mathbf{F}_p)$, and breaks the scheme.

Fastest known attacks

Let $s = \begin{cases} \log(N) & \text{for RSA,} \\ \log(p) & \text{otherwise.} \end{cases}$

problem	best known attack
factoring / discrete log in $\mathbf{F}_p^*$	Number Field Sieve time $\exp(c\ s^{1/3}\ \log(s)^{2/3})$
discrete log on ell. curves	time $\sqrt{p} = \exp(\frac{1}{2}s)$

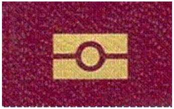
Code-breaking computers get bigger, so N and p need to grow (less badly for elliptic curves).

Recommended number of digits for N and p:

year	2014	2020	2030	2040
RSA / $\mathbf{F}_p^*$	376	535	733	978
Elliptic curve	49	58	68	78
ratio	7.7	9.2	10.8	12.5

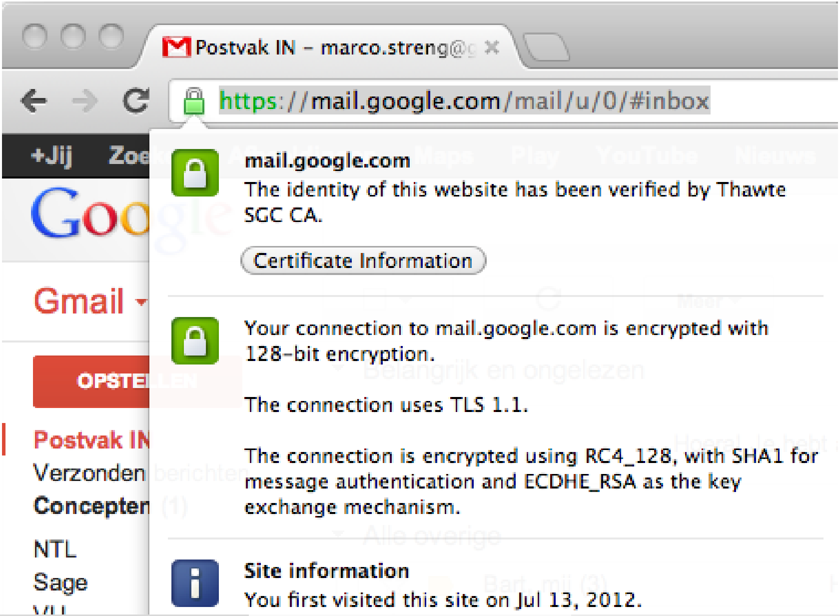
Need for efficiency

Crypto-using computers become smaller



Crypto is used more widely

Google switched to elliptic curve crypto!

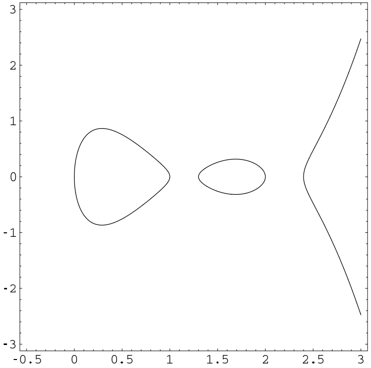


Part 2: curves of genus 2

A curve of genus 2 is a smooth projective curve given by

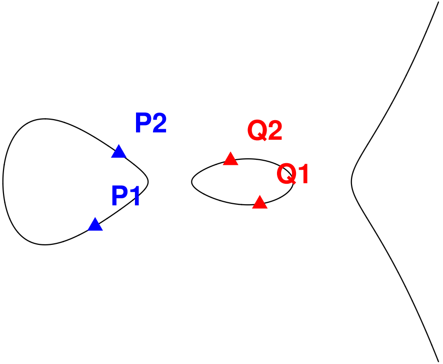
$$y^2 = f(x), \quad \deg(f) \in \{5, 6\},$$

where f has no double roots.



The group law on the Jacobian

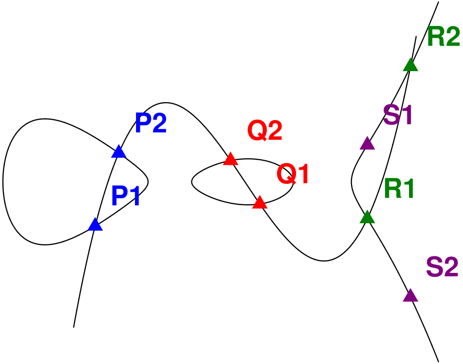
The Jacobian $J(C)$: group of (equivalence classes of) pairs of points.



$\{P_1, P_2\} + \{Q_1, Q_2\} = ?$

The group law on the Jacobian

The Jacobian $J(C)$: group of (equivalence classes of) pairs of points.



$\{P_1, P_2\} + \{Q_1, Q_2\} = \{S_1, S_2\}$

Complex multiplication and invariants

Lattices:

- $J(C)(\mathbf{C}) \cong \mathbf{C}^2/\Lambda$ for a 4-dimensional lattice Λ
- Endomorphism ring $\mathcal{O} = \{\alpha \in \mathrm{Mat}_{2\times 2}(\mathbf{C}) : \alpha\Lambda \subset \Lambda\}$
- "Complex multiplication" if $\mathcal{O} = \mathbf{Z}[\sqrt{-a + b\sqrt{\delta}}]$.
  (Shimura-Taniyama 1950's)

Class polynomials

- Analogues of the j-invariant exist
- Get analogues of Hilbert class polynomials

Applications

Higher-dimensional alternative to elliptic curve cryptography:

- use $J(C)(\mathbf{F}_p)$ instead of $E(\mathbf{F}_p)$.
- advantage: $\sim p^2$ pairs of points instead of only $\sim p$ points, reduces $\log(p)$ by factor 2
- advantage: many more curves to choose from

Construct abelian extensions of $\mathbf{Q}(\sqrt{-a+b\sqrt{\delta}})$.

Class invariants

- The Hilbert class polynomial of $\mathcal{O} = \mathbf{Z}[\frac{\sqrt{-71}+1}{2}]$ is

$$X^7 + 313645809715X^6 - 3091990138604570X^5$$
$$+ 98394038810047812049302X^4$$
$$- 823534263439730779968091389X^3$$
$$+ 5138800366453976780323726329446X^2$$
$$- 425319473946139603274605151187659X$$
$$+ 737707086760731113357714241006081263.$$

- Weber (around 1900), by replacing j by other modular functions, obtains

$$X^7 + X^6 - X^5 - X^4 - X^3 + X^2 + 2X - 1.$$

- I have a Veni for finding, studying, and using class invariants in higher dimension

(end)

j and its generalizations

The j-function was:

$$j : \frac{\{\text{lattices } \Lambda\}}{\mathbf{C}^*\text{-scaling}} = \frac{\{\text{ell. curves } E(\mathbf{C})\}}{\cong} \longrightarrow \mathbf{C}$$

More general modular functions:

$$\frac{\{\text{ell. curves } E(\mathbf{C}) \text{ with additional structure}\}}{\cong} \longrightarrow \mathbf{C} \cup \{\infty\}$$

There is a theory of modular functions f, and their special values $f(\tau)$, and how the automorphism groups of fields of functions and values relate.

This is where Weber's results are most naturally proven and generalized, good alternatives to j are called class invariants.

Example, using Riemann theta functions

- Write $\Lambda = \tau \mathbf{Z}^2 + \mathbf{Z}^2$
- For $a, b, c, d \in \{0, 1\}$, let $c_1 = \frac{1}{2}(a, b)$, $c_2 = \frac{1}{2}(c, d)$, $n = c + 2d + 4a + 8b \in \{0, 1, \ldots, 15\}$, and

$$\theta_n(\tau) = \sum_{v \in \mathbf{Z}^g} \exp(\pi i (v + c_1)\tau(v + c_1)^{\mathrm{t}} + 2\pi i (v + c_1) c_2^{\mathrm{t}})$$

- The function

$$f = i \frac{\theta_{12}^6}{\theta_8^2 \theta_9^2 \theta_{15}^2} \in \mathcal{F}_8$$

is a class invariant for some τ with $Q(\mathcal{O}) = \mathbf{Q}(\sqrt{\frac{-27+\sqrt{521}}{2}})$

For comparison, the smallest Igusa invariant is

$$i_1 = \frac{\text{hom. pol. of degree 20 in } \theta\text{'s}}{(\theta_0\theta_1\theta_2\theta_3\theta_4\theta_6\theta_8\theta_9\theta_{12}\theta_{15})^2}.$$

Example

With Igusa invariants:

$$
\begin{aligned}
H_{i_1} = 2 \cdot 101^2 y^7 &+(-310410324232717295510\sqrt{13} \\
&\quad + 111920034044187774220)y^6 \\
&+(-30481537539492039035184150107118830510\sqrt{13} \\
&\quad + 109902746553618991251794127223638571880)y^5 \\
&+(-2201909580030523730272623848434538048317834513875\sqrt{13} \\
&\quad + 7939097894735431844153019089320973153011210882125)y^4 \\
&+(-2094350525854786365698329174961782735189420898791141250\sqrt{13} \\
&\quad + 7551288209764401665731458692859504138760400195691473750)y^3 \\
&+(-907392914800494855136752991106041311116404713247380607234375\sqrt{13} \\
&\quad + 3271651681305911192688931423723753094763461200379169938284375)y^2 \\
&+(-3002833209931303972009176044594248822678130105181013997490812500\sqrt{13} \\
&\quad + 10826869110073438157121196889117387978616706370281073195682212500)y \\
&+(-3208541702911513221287770105217518905131207705054905377767632898437 5\sqrt{13} \\
&\quad + 115685616293120067038709321144324285012570966768326545991798727929687 5)
\end{aligned}
$$

Example

With class invariant:

$$
\begin{aligned}
H_f = 3^8 101^2 y^7 &+ (21911488848\sqrt{13} \\
&\quad - 76603728240) y^6 \\
&+ (-203318356742784\sqrt{13} \\
&\quad + 733099844294784) y^5 \\
&+ (-280722122877358080\sqrt{13} \\
&\quad + 1012158088965439488) y^4 \\
&+ (-234912038356251443 2\sqrt{13} \\
&\quad + 8469874588158623744) y^3 \\
&+ (-785912031217487708 16\sqrt{13} \\
&\quad + 28336461342113110425 6) y^2 \\
&+ (250917334141632512\sqrt{13} \\
&\quad - 904696010264018944) y \\
&+ (-364471595827200\sqrt{13} \\
&\quad + 1312782658043904)
\end{aligned}
$$