Computing Hilbert Class Fields

Primes of the form $X^2 + nY^2$

Surya Teja Gavva
IIT Bombay

September 2010

Primes of the form $X^2 + nY^2$

Question: Which primes are represented by the form $X^2 + nY^2$

Primes of the form $X^2 + nY^2$

Question: Which primes are represented by the form $X^2 + nY^2$

There are some obvious congruence restrictions. For instance if $p = x^2 + ny^2$, then we have

$$x^2 + ny^2 \equiv 0 \mod p \implies t^2 = -n \mod p$$

So we need $\left(\frac{-n}{p}\right) = 1$.

Primes of the form $X^2 + nY^2$

Question: Which primes are represented by the form $X^2 + nY^2$

There are some obvious congruence restrictions. For instance if $p = x^2 + ny^2$, then we have

$$x^2 + ny^2 \equiv 0 \mod p \implies t^2 = -n \mod p$$

So we need $\left(\frac{-n}{p}\right) = 1$. Is this enough?

For some values of of n, yes!

Primes of the form $X^2 + Y^2$

If we have $p = x^2 + y^2$, either $p = 2$ or we have

$$\left(\frac{-1}{p}\right) = 1 \implies p = 1 \mod 4.$$

In fact, if we take any $p = 1 \mod 4$, we have solution to

$$b^2 = -4 \mod 4p \implies b^2 - 4pc = -4$$

Thus we have a form $pX^2 + bXY + cY^2$ of discriminant -4 which represents p. (Take $X = 1, Y = 0$)

Primes of the form $X^2 + Y^2$

But any two form of discriminant -4 are "equivalent". The class number $h(-4) = 1$.

$$f(ax + by, cx + dy) = g(x, y), f \sim g, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

There is only one class in the class group, so we can transform the form $pX^2 + bXY + cY^2$ to $X^2 + Y^2$.

Equivalent forms represent the same numbers $\implies$ $p = x^2 + y^2$.

Primes of the form $X^2 + nY^2$

Similarly we can prove the following for an odd prime p

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \bmod 8$$
$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3 \text{ or } p \equiv 1 \bmod 3.$$

In both of these cases, the class numbers are $h(-8) = 1$ and $h(-12) = 1$, and congruence conditions allow us to construct one form that can be transformed to the principal form $X^2 + nY^2$

What if there are multiple reduced classes?

Primes of the form $X^2 + nY^2$

$h(-4n) > 1$: Multiple reduced classes.

We can still use the conditions $\left(\frac{-n}{p}\right) = 1$ to construct the form $pX^2 + bXY + cY^2$ of discriminant $-4n$ representing p.

The reduction of form be any of the reduced forms. For instance for $n = 5$, we get

$$p \equiv 1, 3, 7, 9 \bmod 20 \iff \left(\frac{-5}{p}\right) = 1$$
$$\iff p = x^2 + 5y^2 \text{ or } 2x^2 + 2xy + 3y^2.$$

$X^2 + 5Y^2$

$h(-20) = 2$.

The principal form $X^2 + 5Y^2$ only represents the classes $1, 9$ in mod 20, and

$2x^2 + 2xy + 3y^2$ represents $3, 7$ in $(\mathbb{Z}/20\mathbb{Z})^*$

So we have

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \bmod 20$$
$$p = 2x^2 + 2xy + 3y^2 \iff p \equiv 3, 7 \bmod 20$$

And so we could describe the primes represented by $X^2 + 5Y^2$ by congruence conditions.

$X^2 + 14Y^2$

$$h(-56) = 4$$

And we get

$$p = x^2 + 14y^2 \text{ or } 2x^2 + 7y^2 \iff p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$$

$$p = 3x^2 \pm 2xy + 5y^2 \iff p \equiv 3, 5, 13, 19, 27, 45 \bmod 56$$

Using the congruence conditions we can just get this information, but how do we decide which of the primes are of the form $X^2 + 14y^2$?

$X^2 + 14Y^2$

There is no congruence (abelian) way to tell which primes are represented by $X^2 + 14Y^2$. Both forms $p = x^2 + 14y^2,\ 2x^2 + 7y^2$ (the principal "genus" of forms) represent the same values modulo an given integer. So primes in a fixed congruence class can be represented by any of the forms in the genus, we need more information about the prime to decide it is of the form $x^2 + 14y^2$

Genus Theory, Characters

Let' say p_i are the odd prime factor of $D = -4n$

$$f = aX^2 + bXY + cY^2 \to \left(\left(\frac{a}{p_1}\right), \ldots, \left(\frac{a}{p_r}\right)\right)$$

This is a well defined map. (We might have to include more characters depending on $n \mod 8$, but this is enough for $n = 3 \mod 4$)
The set of form in any particular genus have the same "complete character". That is the genus can be defined by these characters. In fact, the principal genus can be seen to be the subgroup of squares in the class group.

But yes, all of these conditions just define the genus - and we cannot distinguish between the forms of the genus.

Forms to Quadratic Fields

We can translate composition of forms to mutliplication of ideal classes in quadratic fields.

$$aX^2 + bXY + cY^2 \to \left\langle a, \frac{-b + \sqrt{D}}{2} \right\rangle \subset \mathbb{Q}[\sqrt{D}]$$

Proper equivalence of the primitive forms corresponds to equivalence under principal ideals $(\alpha), \alpha \in \mathbb{Q}(\sqrt{D})$

The class of $X^2 + nY^2$ corresponds to the trivial class $[(1)] = [O_K]$

We might have to take an order instead of ring of integers if the discriminant is not fundamental

Primes of the form $X^2 + nY^2$ in the field

$p = X^2 + nY^2$ means that $p = (X + \sqrt{-n}Y)(X - \sqrt{-n}Y)$

That is $p = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p} = (X + \sqrt{-n}Y)$ is a principal ideal

So we need to capture $\mathfrak{p}$ being principal, how do we do that?

Hilbert Class Field

Class Field Theory: There is an maximum abelian unramified extension H of $K = Q(\sqrt{D})$ such that the split primes of K are exactly the principal ones. In fact we have the Artin map which is an isomorphism

$$Cl(D) = Cl(\mathcal{O}_K) \xrightarrow{\sim} \mathrm{Gal}(H/K) : \quad \mathfrak{p} \to \left(\frac{H/K}{\mathfrak{p}}\right)$$

Hilbert Class Field

The Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$ is $H = K(\alpha)$, where $\alpha = \sqrt{2\sqrt{2} - 1}$

$\mathfrak{p}$ splitting in $K(\alpha)$ means that the the minimal polynomial $f(x) = (x^2 + 1)^2 - 8$ splits modulo p.

This concretely gives that for an odd prime $p \neq 7$,

$$p = x^2 + 14y^2 \iff \begin{cases} (-14/p) = 1 \text{ and } (x^2 + 1)^2 \equiv 8 \bmod p \\ \text{has an integer solution.} \end{cases}$$

Primes of the form $X^2 + nY^2$, Hilbert Class Field

The general case (of fundamental discriminants) similarly is
$p = x^2 + ny^2 \iff p$ splits completely in H

$$\iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

where $f_n(x)$ is the minimal polynomial defining the Hilbert Class field.

Primes of the form $X^2 + nY^2$, Ray Class Fields

For non-fundamental discriminants, we have to consider orders and the class group of the quadratic forms is the class group of an order which is a ray class group. (defined with some congruence)
Now the Artin map is defined on ideals prime to some modulus and we have

$$\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \longrightarrow \mathrm{Gal}(L/K)$$

Every abelian extension unramified L outside of $\mathfrak{m}$ has the property that

$$P_{K,1}(\ \mathrm{m}) \subset \ker(\Phi_{\mathrm{m}}) \subset I_K(\ \mathrm{m})$$

where $P_{K,1}(\ \mathrm{m})$ are principal ideals (α) with $\alpha = 1 \mod \mathfrak{m}$.

Primes of the form $X^2 + nY^2$, Ray Class Fields

In general, we have to consider the ray class field and the minimal polynomial defining the ray class field.

$$p = x^2 + ny^2 \iff \begin{cases} (-n/p) = 1 \text{ and } f_n(x) \equiv 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

That is $f_n(x)$ is the minimal polynomial of the ray class field L corresponding to the order/discriminant $D = -4n$ inside $k = \mathbb{Q}(\sqrt{D})$

Examples

The ring class field of the order $\mathbb{Z}[\sqrt{-27}] \subset K = \mathbb{Q}(\sqrt{-3})$ is $L = K(\sqrt[3]{2})$.

$$p = x^2 + 27y^2 \iff \begin{cases} p \equiv 1 \bmod 3 \text{ and } x^3 \equiv 2 \bmod p \\ \text{has an integer solution.} \end{cases}$$

The ring class field of the order $\mathbb{Z}[\sqrt{-64}] \subset K = \mathbb{Q}(i)$ is $L = K(\sqrt[4]{2})$

$$p = x^2 + 64y^2 \iff \begin{cases} p \equiv 1 \bmod 4 \text{ and } x^4 \equiv 2 \bmod p \\ \text{has an integer solution.} \end{cases}$$

Computing Hilbert (Ray) Class Fields

Given a field (order), how do we find the Hilbert (Ring) Class Field and the minimal polynomials defining them?

Complex Multiplication

Just like abelian extensions of rationals are generated of roots of unity $e^{\frac{2\pi x}{p}}$ is the analytic function of importance, the Hilbert(Ring) Class fields of the imaginary quadratic fields are generated the modular function $j(z)$. (and related functions like $j(Nz)$)

j function

For any lattice $\Lambda \subset \mathbb{C}$, consider

$$\wp_\Lambda : z \mapsto \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left[\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right]$$

$$E_\Lambda : \wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

$$g_2(\Lambda) = 60 \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-4}, \quad g_3(\Lambda) = 140 \sum_{\lambda \in \Lambda \setminus \{0\}} \lambda^{-6}, \Delta(\Lambda) = g_2^3 - 27 g_3^2$$

The j-invariant $j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{\Delta(\Lambda)} = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}$ defines the lattice up to homothety $\Lambda \to a\Lambda$.

Hilbert Class Polynomial

The values $j([\mathfrak{a}])$ for $[\mathfrak{a}] \in \mathrm{Cl}_K$ are well defined. Because j is weight zero (invariant under scaling the lattice)

$$\mathrm{Hil}_K(X) = \prod_{[\mathfrak{a}] \in \mathrm{Cl}_K} (X - j(\mathfrak{a})) \in \mathbb{Z}[X]$$

is an integer polynomial and generates the class field of $\mathbb{Q}(\sqrt{-D})$

$$\mathfrak{a} = \langle a, \frac{-b + \sqrt{-D}}{2} \rangle \to \Lambda = \langle 1, \tau \rangle = \langle 1, -\frac{-b + \sqrt{-D}}{2a} \rangle$$

So the Hilbert Class Field of K is given by $K(j(\mathbb{Z}_K))$. In fact, if we take $j([\mathfrak{a}])$ for $[\mathfrak{a}] \in \mathrm{Cl}_O$ in a order, we get the corresponding Ray Class Field.

Example

$K = \mathbb{Q}(\sqrt{-5})$. The maximal order $\mathbb{Z}[\sqrt{-5}]$ has class number $h(-20) = 2$. The reduced classes are given by

$$\mathfrak{a}_1 = [1, \sqrt{-5}], \quad \mathfrak{a}_2 = [2, 1 + \sqrt{-5}]$$

$$j(\mathfrak{a}_1) = j(\sqrt{-5}) = 2^3(25 + 13\sqrt{5})^3$$

$$j(\mathfrak{a}_2) = j\left(\frac{1 + \sqrt{-5}}{2}\right) = 2^3(25 - 13\sqrt{5})^3$$

$$\mathrm{Hil}_K(X) = X^2 - 1264000X - 681472000$$

Example

The Hilbert Class Field of $\mathbb{Z}[\sqrt{-5}]$ is generated by the polynomial.

$$\mathrm{Hil}_K(X) = X^2 - 1264000X - 681472000$$

This extension is abelian over $\mathbb{Q}$, hence we can describe primes of the form $X^2 + 5Y^2$ bu congruence conditions. We already saw before that each genus just had one class.

$$p = x^2 + 5y^2 \iff \begin{cases} \left(\frac{-20}{p}\right) = 1, \quad X^2 - 1264000X - 681472000 = 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

$$X^2 - 1264000X - 681472000 = 0 \bmod p \iff (X - 632000)^2 - 1600421888000 = 0 \bmod p$$

$$\iff \left(\frac{1600421888000}{p}\right) = \left(\frac{5}{p}\right) = 1$$

$$p = x^2 + 5y^2 \iff p \equiv 1, 9 \mod 20$$

Example

$K = \mathbb{Q}(\sqrt{-14})$, the maximal order is $\mathbb{Z}[\sqrt{-14}]$. $h(-46) = 4$. The reduced classes are

$$\mathfrak{a}_1 = [1, \sqrt{-14}], \mathfrak{a}_2 = \left[2, \frac{\sqrt{-14}}{2}\right], \mathfrak{a}_3, \mathfrak{a}_4 = \left[3, \frac{2 \pm \sqrt{-14}}{2}\right]$$

$$\mathrm{Hil}_K(X) = (X - j(\mathfrak{a}_1))(X - j(\mathfrak{a}_2))(X - j(\mathfrak{a}_3))(X - j(\mathfrak{a}_4))$$

$$= X^4 - 16220384512X^3 + 2059647197077504X^2 + 225776734208891296X +$$

$$+ 1006408604432156380364 8$$

$$p = x^2 + 14y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1, \quad \mathrm{Hil}_K(X) = 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

The field defined by $\mathrm{Hil}_K(X)$ is equal to $\mathbb{Q}(\sqrt{\sqrt{2}-1})$ with another defining polynomial $x^4 + 2x^2 - 7$, so we get the characterization mentioned before.

$$p = x^2 + 14y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1, \quad x^4 + 2x^2 - 7 = 0 \bmod p \\ \text{has an integer solution.} \end{cases}$$

Example: $K = \mathbb{Q}(\sqrt{-27})$, Cubic reciprocity

$O = \mathbb{Z}[\sqrt{-27}]$ is not maximal, the maximal order is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.
$h(K) = 1$, so the Hilbert Class Field is just K. But the class number of the order $h(\mathcal{O}) = h(-108) = 3$. The order is of conductor 6, hence class group of the order is a ray class group of K of modulus $6\mathcal{O}_K$. The reduced classes are

$$\mathfrak{a}_1 = [1, \sqrt{-27}], \mathfrak{a}_2 = \left[4, \frac{-2-\sqrt{-108}}{2}\right], \mathfrak{a}_3 = \left[4, \frac{-2+\sqrt{-108}}{2}\right]$$

$$\mathrm{Hil}_{\mathcal{O}}(X) = X^3 - 1510132287060000X^2 + 22417946218800000000X - 1879994705688000000000$$

Note that $\mathrm{Hil}_{\mathcal{O}_K}(X) = X$ because $j(\omega) = 0$.
The field defined by $\mathrm{Hil}_{\mathcal{O}}(X)$ is the ring class field of $O = Z[\sqrt{-27}]$ and is defined by the above equation. In fact this field can be seen to equal to $(\sqrt[3]{2})$ and we the following cubic reciprocity!

$$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1 \iff p = 1 \bmod 3 \text{ and} \\ x^3 = 2 \bmod p \text{ has an integer solution.} \end{cases}$$

Example: $K = \mathbb{Q}(\sqrt{-64})$, biquadratic reciprocity

$O = \mathbb{Z}[\sqrt{-64}]$ is not maximal, the maximal order is $\mathbb{Z}[i]$.
$h(K) = 1$, so the Hilbert Class Field is just K. But the class number of the order $h(\mathcal{O}) = h(-256) = 4$. The order is of conductor 8, hence class group of the order is a ray class group of K of modulus $8\mathcal{O}_K$. The reduced classes are

$$\mathfrak{a}_1 = [1, \sqrt{-64}], \mathfrak{a}_2 = \left[4, \frac{-4+\sqrt{-256}}{2}\right], \mathfrak{a}_3 = \left[5, \frac{2+\sqrt{-256}}{2}\right], \mathfrak{a}_4 = \left[5, \frac{-2+\sqrt{-256}}{2}\right]$$

$\mathrm{Hil}_{\mathcal{O}}(X) = X^4 - 676116697478186216331 2^3 - 18265926735062072009041727 52X^2 + 269256233966630083113758909667 84X - 106441068118186952103720850523914 2408$

Note that $\mathrm{Hil}_{\mathcal{O}_{\mathbb{Z}[i]}}(X) = X - 1728$ because $j(i) = 1728$
The field defined by $\mathrm{Hil}_{\mathcal{O}}(X)$ is the ring class field of $O = Z[\sqrt{-64}]$ and is defined by the above equation. In fact this field can be seen to equal to $(\sqrt[4]{2})$ and we the following biquadratic reciprocity!

$$p = x^2 + 27y^2 \iff \begin{cases} \left(\frac{-14}{p}\right) = 1 \iff p = 1 \bmod 4 \text{ and} \\ x^4 = 2 \bmod p \text{ has an integer solution.} \end{cases}$$

How do we compute the j values?

To compute the Hilbert/Ring Class fields we need the Hilbert Class polynomial of the corresponding order which can be computed from the $j-values$ at the $h(O)$ reduced classes. One way is to use the q expansion of j.

$$j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + \cdots \text{ with } c(n) \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}n^{3/4}}$$

The coefficients can be computed by manipulating some product

$$\text{expansion } j(\tau) = 1728\frac{g_2(\tau)^3}{\Delta(\tau)} = \frac{\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}, q = e^{2\pi i\tau}$$

How do we compute the j values?

How do we compute $j(\frac{-b+\sqrt{D}}{2a})$? For example

$$i(2\sqrt{2}i) = \frac{125}{216}(19+13\sqrt{2})^3$$

$$i(4i) = \frac{1}{64}(724+513\sqrt{2})^3$$

$$i\left(\frac{1+2i}{2}\right) = \frac{1}{64}(724-513\sqrt{2})^3$$

$$i\left(\frac{1+2\sqrt{2}i}{3}\right) = \frac{125}{216}(19-13\sqrt{2})^3$$

$$i(3i) = \frac{1}{27}(2+\sqrt{3})^2(21+20\sqrt{3})^3$$

$$i(2\sqrt{3}i) = \frac{125}{16}(30+17\sqrt{3})^3$$

$$i\left(\frac{1+7\sqrt{3}i}{2}\right) = -\frac{64000}{7}(651+142\sqrt{21})^3$$

$$j(\sqrt{-14}) = 2^3(323+228\sqrt{2}+(231+161\sqrt{2})\sqrt{2\sqrt{2}-1})^3$$

Computing j values

$$\eta(\tau) = q^{1/24}\prod_{n\geq 1}(1-q^n) = q^{1/24}\sum_{n\in\mathbf{Z}}(-1)^n q^{n(3n-1)/2}$$

$$f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}q^{1/24}\prod_{n=1}^{\infty}(1+q^n)$$

Compute the values of η, $\mathfrak{f}_2$ and use them to compute j.

$$j(\tau) = \frac{(\mathfrak{f}_2^{24}(\tau)+16)^3}{f_2^{24}(\tau)}$$

Example: To compute $j(\sqrt{-n})$ with $q = e^{-2\pi\sqrt{n}}$, compute numerical approximations to $\eta, \mathfrak{f}_2, j$ using finite truncations of the q-series.

Computing j values: q-series approximations

This method is helpful when the class number is one, because j is an integer in this case and we can find it by approximating and rounding to nearest integers.

Example: Take $n = 7$. $h(-28) = 1$. We want to compute $j(\sqrt{-7})$

If we use the expansion
$j(q) = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$,
$q = e^{-2\pi\sqrt{7}}$, truncating to 10 terms we get

$$j(\sqrt{-7}) \approx 16581374.99$$

But the actual answer is $j = 16581375$

Computing j values: q-series approximations

If we compute 100 terms, we get the approximation
$j = 16581374.99999993$
The convergence is too slow! We need a better method. That's why we compute η and $\mathfrak{f}_2$

$$\eta(\tau) = q^{1/24}\left(1 - q - q^2 + q^5 + + \cdots\right)$$

$$\eta(\tau) \approx 0.50024558 \implies \mathfrak{f}_2(\tau) = 0.70745417427$$

$$\implies j(\tau) \approx 16581374.999$$

Therefore $j(\sqrt{-7}) = 16581375$ and the Hilbert Class Polynomial is $X - 16581375$.

But these computations are helpful for $h = 1$. What about other cases? We can still work with numerical approximations say using the symmetrical polynomials of $j(\mathfrak{a})$ to compute $\mathrm{Hil}_{\mathcal{O}}(X)$ etc, but let's look for another method!

Weber functions

Weber functions:

$$\mathfrak{f}(\tau) = \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)} = q^{-1/48}\prod_{n=1}^{\infty}\left(1+q^{n-1/2}\right)$$

$$f_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)} = q^{-1/48}\prod_{n=1}^{\infty}\left(1-q^{n-1/2}\right)$$

$$f_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)} = \sqrt{2}q^{1/24}\prod_{n=1}^{\infty}\left(1+q^{n}\right)$$

$$\gamma_2(\tau) = \sqrt[3]{j(\tau)} = 12\frac{g_2(\tau)}{\sqrt[3]{\Delta(\tau)}}$$

For our singular moduli τ, the modular functions j, g_2, g_3 all are algebraic integers defined over the Hilbert Class Field H. Hence the elliptic curve $E_\tau = \mathbb{C}/Z_K$ is defined over H.

H is generated by $j(Z_K)$ over the field K. But what about the ring class fields. They are generated by $j(\mathfrak{a})$ for $\mathfrak{a}$ in the order, but can we describe the values just in terms of $j(Z_K)$?
Consider the Weber function

$$f_K(z) = \frac{g_2(\mathbf{Z}_K)\, g_3(\mathbf{Z}_K)}{\Delta(\mathbf{Z}_K)} \wp_{\mathbf{Z}_K}(z)$$

Ray Class Field in terms of $\mathbf{C}/\mathbf{Z}_K$

Ray class field of conductor m is generated by $j(\mathbf{Z}_K)$, and the values of the Weber function f_K at the non-zero m -torsion points of $\mathbf{C}/\mathbf{Z}_K$. That is at $z = \frac{a}{m}\tau + \frac{b}{m}$

This is just analogous to cycltomic fields which are generated by roots of unity. The multiplicative group G_m is replaced by E.

Also These values f_K values (in most cases) are the values of the x-coordinates of the m-torsion points on the elliptic curve $\mathbf{C}/\mathbf{Z}_K$. (Can be computed using the division polynomials which have these x-coordinates as roots)

Class Equation and Modular Equation

$$\Phi_m(X, j(\tau)) = \prod_{i}^{|C(m)|} (X - j(m\gamma_i\tau))$$

$$\Phi_m(j(m\tau), j(\tau)) = 0$$

$\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$ is called the Modular Equation defining $X_0(m)$.

$$\Phi_m(X, X) = c_m \prod_{\mathcal{O}} H_{\mathcal{O}}(X)^{r(\mathcal{O},m)}$$

Where

$$r(\mathcal{O}, \boldsymbol{m}) = \mid \{\alpha \in \mathcal{O} : \alpha \text{ is primitive, } N(\alpha) = m\}/\mathcal{O}^* \mid \ ,$$

Thus the Class polynomial is a factor of the Modular polynomial.

Computing Modular Equations

We said we could avoiding the q series manipulations by this method, but we need to computing the modular equations!
First reduce to m a prime. (Relations between the polynomials ϕ_m, ϕ_n). For the prime case try to find a polynomial of degree $p+1$ which satisfies

$$\Phi_p(j(p\tau), j(\tau)) = 0$$

$$\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \bmod p\mathbb{Z}[X, Y]$$

by substituting the q-expansion.