Primes of the Form $x^2 + ny^2$

GandAlF Talk: Notes

Steven Charlton

28 November 2012

1 Introduction

On Christmas day 1640, Pierre de Fermat announced in a letter to Marin Mersenne his theorem on when a prime number can be written as the sum of two squares. He claimed that $p = x^2 + y^2$ if and only if $p = 2$, or $p \equiv 1 \pmod 4$.

Fourteen year later, in a letter to Blaise Pascal he unveiled another two strikingly similar criteria for when a prime can be written as other combinations of squares – as square and twice a square, or as a square and three times a square. Of course, Fermat didn't bother to prove any of these claims.

Does anyone have a favourite prime they want to check? [Ask for primes, go to maple to calculate]

This naturally raises many questions:

Q1) How can we prove these claims? How were they proven?

A1) That I'll come to throughout the presentation.

Q2) Can we say anything about other cases? Generally?

A2) If we couldn't, it would make a pretty silly fourth year project, and a very short talk.

Euler added $n = 5$ to the list. We've also got $n = -2$. [Check some primes again.]

Then to throw a spanner in the works, this is what condition we get for $n = 17$. Pretty horrible, but we can still find criteria. And here's the one for $n = -142$.

[Try out criteria with some primes]

Q3) You'll notice each of these has a very distinctive form. In the first set: some congruence holds, and in the second set something is a square mod p and some polynomial has a solution mod p. Why?

A3) In fact the congruences can also be put in this form: $p \equiv 1, 9 \pmod{20}$ is the same as $(-5/p) = 1$ and $x^2 + 1 \equiv 0 \pmod p$ has a solution – it's just quadratic reciprocity. And this is equivalent to $x^4 + 12x^2 + 16 \equiv 0 \pmod p$ has a solution. This screams "WHY?" even more, but also demands to know what's so different about 3 and 17 that the condition for 3 is a nice congruence, and for 17 involves a messy polynomial.

2 Quadratic Forms

2.1 Binary Quadratic Forms

To lay the groundwork we need to introduce the notion of a binary quadratic form, and understand some properties and results about them.

A binary quadratic form is a polynomial like:

$$ax^2 + bxy + cy^2$$

We're interested in integral quadratic forms (the coefficients are integers) since this is number theory. Also the form should be primitive, i.e. the coefficients are coprime otherwise we can look at the quadratic form we get by dividing out the common factor.

The discriminant of the form is defined naturally as $b^2 - 4ac$. Roughly speaking it tells us what sort of values the form represent. If $D < 0$ then the form is positive definite (or negative definite if $a < 0$) – the form only represents positive (or negative if $a < 0$) integers. If $D > 0$ then the form is indefinite so represents both positive and negative values.

For the quadratic forms we have before:

$$\begin{aligned} x^2 + y^2 &\rightsquigarrow D = -4 \\ x^2 + 2y^2 &\rightsquigarrow D = -8 \\ x^2 + 3y^2 &\rightsquigarrow D = -12 \\ x^2 + 5y^2 &\rightsquigarrow D = -20 \\ x^2 + 17y^2 &\rightsquigarrow D = -54 \\ x^2 - 2y^2 &\rightsquigarrow D = 8 \\ x^2 - 142y^2 &\rightsquigarrow D = 568 \end{aligned}$$

So the problem we have now is to determine which primes a given quadratic form $f(x, y)$ represents.

2.2 Equivalence

To this end, first we define an equivalence between quadratic forms. With every mathematical object we want a notion of equivalence.

There are at least three different notions of equivalence between quadratic forms (SL, GL and signed-GL equivalence). The most suitable notion here is the following:

Act on quadratic forms by $\mathrm{SL}(2, \mathbb{Z})$. This genuinely is a group action. This is most easily seen by writing the quadratic form and the action in matrix form:

$$ax^2 + bxy + cy^2 = \begin{pmatrix} x \\ y \end{pmatrix}^\top \underbrace{\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}}_{=:M} \begin{pmatrix} x \\ y \end{pmatrix}$$

Then the action of $A := \left(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}\right)$ on $f(x, y)$ is:

$$A \cdot f(x, y) = A \cdot (\underline{\boldsymbol{x}}^\top M \underline{\boldsymbol{x}}) = \underline{\boldsymbol{x}}^\top A^\top M A \underline{\boldsymbol{x}}$$

From this we can see:

$$B \cdot A \cdot f(x, y) = (BA) \cdot f(x, y)$$

and it was already that $I \cdot f(x,y) = f(x,y)$. So it's a group action. This means the set of quadratic forms breaks up into equivalence classes under this.

Also notice the discriminant of $f(x,y)$ is just $4\det M$. Since $A \in \mathrm{SL}(2,\mathbb{Z})$, the new discriminant is:

$$4\det A^\top MA = 4\det A^\top \det M \det A = 4 \cdot 1 \cdot \det M \cdot 1 = 4\det M$$

So the action preserves discriminants.

Since A is invertible, equivalent forms represent the same integers. If $g = A\cdot f$ and g represents m, then write

$$m = g(x_0', y_0') = \underline{\boldsymbol{x_0'}}^\top A^\top MA\underline{\boldsymbol{x_0'}} = \underline{\boldsymbol{x_0}}^\top M\underline{\boldsymbol{x_0}} = f(x_0, y_0)$$
$$\text{where } \underline{\boldsymbol{x_0}} = A\underline{\boldsymbol{x_0}}'$$

So f represents anything g represents. But we can also write $f = A^{-1} \cdot g$, and so g represents anything f represents. They represent the same.

So it suffices to look at equivalence classes of forms.

The next point is vitally important. For a given discriminant D there are only finitely many equivalence classes. Using the matrices:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad T^k = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$$

we can 'reduce' the coefficients of an arbitrary form in a controlled way. We get down to a form with coefficients satisfying:

$$\operatorname{abs} b \leq a \leq c \quad \text{for positive definitne forms}$$
$$\operatorname{abs} b \leq \operatorname{abs} a \leq \operatorname{abs} c \quad \text{for indefinite forms}$$

The relation $D = b^2 - 4ac$ then puts bounds on a such that only finitely many values for a are possible.

In the positive definite case these forms are mutually different, so we get exactly a set of representatives for the equivalence classes. In the indefinite case some of the reduced forms can agree, and a more refined method is needed to determine the equivalence classes.

In either case it is possible to algorithmically determine the reduced forms and which ones are equivalent. This gives an algorithmic way of listing the classes and determining their number.

2.3 Ideals in Quadratic Fields

Now we're going to relate these quadratic forms to objects we know how to work with. We already see a hint of the connection to number fields by noticing how the norm of an integer $a + b\sqrt{d}$ give us a quadratic form $a^2 - db^2$. The way to extend this to get all quadratic forms is to look at ideals rather than elements. We define the following map: ....

We need the ideal to have an oriented basis for some suitable definition of oriented, we won't worry about that. To ensure things work nicely for real quadratic fields / indefinite forms we need the narrow ideal class. For imaginary quadratic fields the narrow class and the ordinary class agree.

For example looking at: $K = \mathbb{Q}(\sqrt{-5})$. The (narrow) class number is 2, we ideal classes are represented by: $\mathcal{O}_K = [1, -\sqrt{-5}]$ of norm 1, and $\mathfrak{p}_3 = [3, 1 + \sqrt{-5}]$ of norm 3. Let's see what quadratic forms we get:

$$\mathcal{O}_K \mapsto x^2 + 5y^2$$
$$\mathfrak{p}_3 \mapsto 3x^2 + 2xy + 2y^2$$

These are in fact all the quadratic forms of discriminant -20, so the map is a 1:1 correspondence in this case.

Also at $K = \mathbb{Q}(\sqrt{10})$, with $\mathcal{O}_K = [1, -\sqrt{10}] \mapsto x^2 - 10y^2$, and $\mathfrak{p}_2 = [2, -\sqrt{10}] \mapsto 2x^2 - 5y^2$. Also a 1:1 correspondence.

This holds generally.

Proof of bijectivity: Well-defined: changing basis $\underline{\boldsymbol{y}} = A\underline{\boldsymbol{x}}$ have $A \in \mathrm{GL}(2, \mathbb{Z})$. By the definition of oriented we get in fact $A \in \mathrm{SL}(2, \mathbb{Z})$. Explicitly writing out the map for each basis shows that the two forms are equivalent.

Going to an equivalent ideal $\mathfrak{a}\mathfrak{b}^{-1} = (\lambda)$ changes the basis and the norm by λ, so this cancels in the computation.

Surjectivity comes from looking at $[a, \frac{b-\sqrt{D}}{2}]$.

Injectivity is a little fiddlier/trickier, but overall is not too difficult. It's a case of using the quadratic form equivalence to explicitly construct a change of oriented bases for the ideals, so they're equal.

2.4 Representing Integers

I'm going to skip the proof of the lemma. Mostly it's just a case a taking an ideal $\mathfrak{b}$ of norm m, relating it to $\mathfrak{a}$, and following the map through in one direction. And taking a representation of m and using this to construct a norm m ideal out of $\mathfrak{a}$.

This gives us our first real criteria on primes being represented by quadratic forms.

Proof: 2 or primes dividing D are the primes which ramify. Exclude these. Then a prime is represented by some form if and only if there is some ideal of norm p in the number field, which is if and only if the ideal (p) splits (recall that an ideal divides its norm), and this is well known to be if and only if $(D/p) = 1$

Actually this also holds for non-fundamental discriminants. This gives a criteria for quadratic forms of $\underline{\text{any}}$ discriminant.

2.5 Class Number One

Well this is good, we can now completely solve the problem for class number one.

This gives a proof of Fermat's three claims. Each discriminant has class number one. The criteria comes from using quadratic reciprocity on (D/p) to find the congruences.

Show this for $x^2 + y^2$. $(-4/p) = (4/p)(-1/p) = (-1/p)$, and this is 1 for $p \equiv 1 \pmod 4$ by a supplement to quadratic reciprocity.

There aren't many negative discriminants with class number one, in fact there are only 9 fundamental discriminants / imaginary quadratic fields with class number one. There are 4 more non-fundamental discriminants with class number one which we can also tackle. $D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$.

For indefinite forms / real quadratic fields, it is unknown how many fields have (narrow) class number one / fundamental discriminants have class number one. There are infinitely many non-fundamental discriminants with class number one. Every discriminant $D = 4 \cdot 13 \cdot 169^n$ has class number one, we can get criteria for families like:

$$p = x^2 - 13 \cdot 169^n \iff (13/p) = 1 \iff p \equiv 1, 3, 4, 9, 10, 12 \pmod{13}$$

But there are still plenty of cases with class number not-one. We want some way of dealing with these, and it all comes down to finding when (p) splits into principal ideals, so in particular telling when an ideal is principal. For this class field theory comes to the rescue.

3 Class Field Theory

3.1 Generalised Ideal Class Groups

The basic notion in class field theory is of a generalised ideal class group (leading to the notion of a class field and hence class field theory). It takes a bit of work to set up the notions.

A modulus in a number field K is a formal product of valuations (both finite and infinite), subject to some conditions on the exponents. Roughly speaking, finite primes are just prime ideals, and infinite primes correspond to embeddings of K into $\mathbb{C}$. In a modulus complex embeddings appear with exponent 0, and real embeddings with exponent at most 1. This means a modulus is just a product of prime ideals and distinct real embeddings.

Then we define the group of fractional ideals for the modulus $\mathfrak{m}$ as the fractional ideals of K which are prime to $\mathfrak{m}_0$, where $\mathfrak{m}_0$ is just the product of prime ideals of the modulus (i.e. the finite valuations bit). The subgroup of principal fractional ideals for the modulus $\mathfrak{m}$ are those whose generator is $1 \pmod{\mathfrak{m}_0}$, and is strictly positive under any real embedding σ.

Then a congruence subgroup is one sitting between these two groups of ideals. And the quotient of the fractional ideals by the subgroup gives us a generalised ideal class group.

We already (implicitly) know two generalised ideal class groups (which will also explain the name).

- (Class Group) If we take the modulus $\mathfrak{m} = 1$, i.e. no prime ideals and no real embeddings, we find that $\mathcal{I}_K(1) = \mathcal{I}(K)$ is just the group of <u>all</u> fractional ideals of K, since there are no conditions to check: every ideal is prime to 1.

  Similarly there are no conditions to check for the principal ideals: we don't have any real embeddings so that the image is strictly positive is vacuously true, as is the congruence. So this just gives all principal fractional ideals $\mathcal{P}(K)$.

  Then $\mathcal{P}(K)$ is a congruence subgroup since it satisfies the condition. The generalised ideal subgroup then is $\mathcal{I}(K)/\mathcal{P}(K) = \mathcal{C}(K)$, the ordinary class group.

- (Narrow Class Group) If the modulus just consists of all real embeddings of K, then $\mathcal{I}_K(\mathfrak{m}) = \mathcal{I}(K)$ is just all fractional ideals – there is no condition to check. And the principal ideals are those generated by totally positive elements (i.e. positive under all real embeddings (the definition of totally positive)). This gives the subgroup of totally positive principal ideals $\mathcal{P}^+(K)$.

  The quotient is $\mathcal{I}(K)/\mathcal{P}^+(K) = \mathcal{C}^+(K)$, by definition the narrow class group.

There are many many other generalised ideal class groups, but these are the two important ones for us.

3.2 The Artin Map

Now we're going to relate these generalised ideal class groups to certain extensions of the number field K. The basic idea is these generalised ideal class groups are exactly the Galois groups of Abelian extensions of K. We do this with the artin map.

We take a Galois extension L/K and an unramified prime $\mathfrak{p}$ which has a prime $\mathfrak{P}$ above it in L. (We need unramified otherwise the isomorphism in the line below doesn't work). The ring of integers $\mathcal{O}$ is a Dedekind domain so the prime ideals are maximal (by definition) so the quotients $\mathcal{O}_L/\mathfrak{P}$, etc, are fields. So this gives an extension of finite fields. This is Galois.

The group $D_{\mathfrak{P}}$ is called the decomposition group and its the stabiliser of $\mathfrak{P}$ under the action of the Galois group – the Galois groups action on elements becomes an action of prime ideals of L above $\mathfrak{p}$, which elements act trivially? This is a subgroup of $\mathrm{Gal}(L/K)$. The isomorphism in the middle is a standard result: the action of elements of $D_{\mathfrak{P}}$ descends to the residue field extension, it is surjective with trivial kernel for an unramified prime, so FIT gives the result.

Now the Galois group on the left has a canonical generator, the Frobenius. Through this isomorphism this picks out an element of $\mathrm{Gal}(L/K)$. We define this to be the Artin symbol of the prime $\mathfrak{P}$.

When the extension is Abelian (i.e. has Abelian Galois group) then the Artin symbol doesn't depend on the prime $\mathfrak{P}$ above $\mathfrak{p}$. It just depends on $\mathfrak{p}$. Picking any other prime above $\mathfrak{p}$ we can write it as $\mathfrak{Q} = \sigma\mathfrak{P}$ because the action of $\mathrm{Gal}(L/K)$ here is transitive. Then the following result holds:

$$((L/K)/\mathfrak{Q}) = ((L/K)/\sigma\mathfrak{P}) = \sigma((L/K)/\mathfrak{P})\sigma^{-1} = ((L/K)/\mathfrak{P})$$

After defining ramification index e_i (exponent of $\mathfrak{P}_i$ above $\mathfrak{p}$), and inertial degree f_i (the degree of $\frac{\mathcal{O}_L/\mathfrak{P}_i}{\mathcal{O}_K/\mathfrak{p}}$ as a field extension) the splitting completely result is pretty much a tautology. In a Galois extension e_i are the same for all primes $\mathfrak{P}_i$, as are f_i. Splitting completely is $e = f = 1$. But we assumed $\mathfrak{p}$ is unramified so $e = 1$. The order of the Artin symbol is f since it generated this field extension, hence if it is trivial $f = 1$ – splits completely. This is a useful fact we will return to later.

Now the artin map extends this multiplicatively to a suitable subset of all ideals. In an extension L/K only finitely many primes can ramify, so let $\mathfrak{m}$ be a modulus divisible by all such primes. Then the Artin symbol extends multiplicatively to $\mathcal{I}_K(\mathfrak{m})$ giving a group homomorphism: ....

3.3 The Theorems of Class Field Theory

The theorem is pretty much as is stated here. We can relate Galois groups, congruence subgroups and Artin maps. It's called the reciprocity theorem as it encodes/generalises the various reciprocity laws: quadratic, cubic, biquadratic, etc. None of which I (except for its relation to quadratic reciprocity which Jens strongly suggested I look at) investigated much.

The Galois group is a generalised ideal class group follows from the First Isomorphism Theorem as we have:

$$\Phi\colon \mathcal{I}_K(\mathfrak{m}) \twoheadrightarrow \mathrm{Gal}(L/K), \text{ with kernel a congruence subgroup}$$

The existence theorem allows us to construct Abelian extensions with very strictly controlled properties. We'll make use of this to get an answer to our question.

Roughly speaking these two theorems tell us that Galois groups of abelian extensions of generalised ideal class groups.

4 Hilbert Class Field

We define the Hilbert class field using the existence theorem. We apply it to the indicated data. This gives a unique extension of K, which we call the Hilbert class field.

An alternative characterisation of the Hilbert class is given by the following theorem. The Hilbert class field is the maximal unramified abelian extension of K. Unramified follows since the ramified prims divide the modulus. The maximality follows from another theorem of class field theory.

So what does this get us?

Since there are no exponents in the modulus to change, the Artin map here must be surjective and by construction it's kernel is $\mathcal{P}_{1,K}(\mathfrak{m}) = \mathcal{P}(K)$. This means $\mathrm{Gal}(L/K) \cong \mathcal{C}(K)$. So we know the degree of the Hilbert class field. Then we can check unramified and Abelian. If this has the right degree then is must be the Hilbert class field as the Hilbert class field would be a degree 1 extension of this unramified Abelian extension. We can (in principal) prove things are the Hilbert class field.

Now let's pick a prime $\mathfrak{p}$ of K, and see what happens to it in the Hilbert class field. We have the following chain of equivalences:

$$\mathfrak{p} \text{ is principal } \iff ((L/K)/\mathfrak{p}) = 1 \iff \mathfrak{p} \text{ splits completely in } L$$

Bingo! We can determine when a prime ideal of K is principal by finding the Hilbert class field. We're within sight of our goal. Let's apply this to quadratic forms.

4.1 Positive-Definite Forms

Field diagram $L = K(\alpha) \supset K \supset \mathbb{Q}$.

Let $Q(x,y)$ be the quadratic form corresponding to the principal ideal class of $K = \mathbb{Q}(\sqrt{-d})$, so $Q(x,y) \approx x^2 - dy^2$. Excluding $p = 2, d \mid D$, then $Q(x,y)$ represents p if and only if (p) splits into principals ideal in K. These principal ideals split completely in L/K, so (p) splits completely in $L/\mathbb{Q}$. Conversely if (p) splits completely in $L/\mathbb{Q}$, then there is some prime $\mathfrak{R}$ above $\mathfrak{P}$ above $\mathfrak{p}$ with $e = f = 1$. This means $\mathfrak{R}$ above $\mathfrak{P}$ has $e = f = 1$, so this ideal splits completely in L/K meaning it's principal. This is a principal ideal of norm p. So $p = Q(x,y)$ if and only if p splits in $L/\mathbb{Q}$.

Dedekind's Theorem tells us how a prime decomposes in an extension by relating this decomposition to the factorisation of the polynomial generating the extension. Excluding primes dividing the discriminant of the generating polynomial of $L/\mathbb{Q}$ (where Dedekind's Theorem doesn't work), splitting completely in $L/\mathbb{Q}$ means the generating polynomial $f(t)$ splits into linear factors (so $f = 1$, and $e = 1$ since we're excluded ramified primes which divide the discriminant). Linear factors correspond to roots. And we're done.

The last equivalence one involves a little technical work, but roughly complete splitting $L/\mathbb{Q}$ implies complete splitting $\mathbb{Q}(\alpha)/\mathbb{Q}$, $K/\mathbb{Q}$, which is fine. Going the other way the complete splitting in $\mathbb{Q}(\alpha)/\mathbb{Q}$ is related by complete splitting in $K(\alpha)/K$, and this means complete splitting in $L/\mathbb{Q}$.

Now we have this, we see why all the criteria before have their particular form, they are all special cases of this theorem. With this we can churn out criteria once we know the appropriate Hilbert class fields. Cohen has a table of Hilbert class fields in Appendix C of Advanced Computational Number Theory. Also Magma can calculate Hilbert class fields.

Go through $\mathbb{Q}(\sqrt{-5})$, $x^2 + 5y^2$ example, seeing how to get congruence conditions? The Hilbert class field is $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ apparently. This gives the criteria I had before.

5 Narrow Class Field

Now comes déjà vu. We do most of this again but change Hilbert for narrow, and principal for totally positive principal. And we get the equivalent result for indefinite forms, and life is good.

Cohen doesn't give a table of narrow class fields, but Magma can compute them, so we can still churn out results.

6 Cubic Forms

Since it was so easy to handle indefinite quadratic forms with the theory we have, let's be a little big more ambitious, and see how our theory can handle this question.

The plan of attack is roughly as follows.

1. Recognize this as a norm form

   I chose this cubic form for a very particular reason. I already know this is the norm on $\mathbb{Z}[\sqrt[3]{11}]$, the ring of integers of $\mathbb{Q}(\sqrt[3]{11})$. $a^3 + 11b^3 + 121c^3 - 33abc = \mathrm{N}(a + b\sqrt[3]{11} + c\sqrt[3]{11^2})$.

2. Now turn this into a question about number fields

   This means we're looking for an element α of norm p in $\mathbb{Q}(\sqrt[3]{11})$. Since -1 has norm -1 here, a principal ideal of norm p has a generator of norm $\pm p$, which can be chosen to have norm p. So we're looking for principal ideals of norm p.

   Ideals of norm p are easy: if (p) splits then one of the factors has norm p. But we want to know when the factor of norm p is principal. The class number of K is 2, so the factor is not necessarily principal, we need to do some work.

3. Throw some class field at it

   We have the Hilbert class field of K.

   As we argued before, if (p) has a principal ideal of norm p above it, then this splits completely in the Hilbert class field. So (p) splits in L where some prime $\mathfrak{R}$ has $e = f = 1$. This gives a root of the polynomial generating the Hilbert class field over $\mathbb{Q}$. Always taking p to not divide the discriminant.

   Conversely if the polynomial has a root, then we get a prime $\mathfrak{R}$ in L with $e = f = 1$. This lies above some prime $\mathfrak{P}$ of K, so this prime of K must split completely in L/K as L/K is Galois. Then this is an ideal of norm p (as it has $f = 1$ and is a factor of (p)).

4. Black magic and magma happens here to find the Hilbert class field and its generating polynomial.

5. And we get the criteria…

7 Modular Forms

7.1 Representation Numbers

Going back to quadratic forms: now we can determine when there are solutions, another natural question to consider is how many solutions are there?

The theta series of a quadratic form is obtained as the following sum. It can be rearranged to explicitly show how it counts the representation numbers (number of solutions/number of ways of representing a number by the quadratic form). The theta series is a modular form for some group, weight, character etc that I don't really care about. But for a particular discriminant they are all the same regardless of which quadratic form you look at.

Let's have a running example throughout. The quadratic forms of discriminant -20 are:

$$\begin{aligned} Q_1 &= x^2 + 5y^2 \\ Q_2 &= 2x^2 + 2xy + 3y^2 \end{aligned}$$

The theta series are:

$$\begin{aligned} \Theta_{Q_1} &= 1 + 2q + 2q^4 + 2q^5 + 4q^6 + 6q^9 + \cdots \\ \Theta_{Q_2} &= 1 + 2q^2 + 4q^3 + 4q^7 + 2q^8 + 2q^{10} + \cdots \end{aligned}$$

We're going to look at linear combinations of all these theta series, corresponding to certain characters of the class group. That is, look at maps $\chi\colon \mathcal{C}(K) \to \mathbb{C}^*$, and the linear combinations coming from these.

In this case the class group is $\mathbb{Z}_2$, so the characters are $\chi\colon 1 \mapsto 1$, and $\phi\colon 1 \mapsto -1$. So we get two combinations:

$$\begin{aligned} f_\chi &= \frac{1}{2}(\Theta_{Q_1} + \Theta_{Q_2}) \\ f_\psi &= \frac{1}{2}(\Theta_{Q_1} - \Theta_{Q_2}) \end{aligned}$$

That $\frac{1}{2}$ is there to normalize things.

7.2 L-series

We can look at the L-series associated to this modular form to sometimes extract formulae for the representation numbers. From the general theory about this sort of thing, one knows that the linear combinations above have Euler products, that is can be written as a product over primes like this .... Where a_i is just the i-th coefficicent of the modular form.

In our cases:

$$L(f_\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + (D/p)p^{-2s}}$$

where

$$a_p = \begin{cases} 1 & p \text{ ramifies} \\ 0 & p \text{ inert} \\ 2 & p \text{ splits into principal} \\ 2 & p \text{ splits into non-principal} \end{cases}$$

Have:

$$a_p = 1 + (-20/p)$$

So

$$L(f_\chi, s) = \prod_{p \text{ prime}} \frac{1}{(1 - p^{-s})(1 - (-20/p)p^{-s})} = L(1, s)L((-20/\cdot), s)$$

And this tells us the coefficient $a_n = \sum_{d|n}(-20/d)$. This arithmetic convolution of the coefficients of the two series we are multiplying.

Similarly:

$$L(f_\phi, s) = \prod_{p \text{ prime}} \frac{1}{1 - b_p p^{-s} + (D/p)p^{-2s}}$$

$$b_p = \begin{cases} 0 & p \text{ inert} \\ 1 & p \text{ ramifies into principal} \\ -1 & p \text{ ramifies into non-principal} \\ 2 & p \text{ splits into principal} \\ -2 & p \text{ splits into non-principal} \end{cases}$$

Have:

$$b_p = (-4/p) + (5/p)$$

(This follows from our criteria before using splitting in $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-5})$. So

$$L(f_X, s) = \prod_{p \text{ prime}} \frac{1}{(1-(-4/p)p^{-s})(1-(5/p)p^{-s})} = L((-4/\cdot), s)L((5/\cdot), s)$$

So the general coefficient is $b_n = \sum_{d|n}(-4/d)(5/n/d)$.

Now notice the sum of the two series gives us the rep numbers $r_{x^2+5y^2}(n)$ and the difference $r_{2x^2+2xy+3y^2}(n)$, so we have formulae for the number of representations as follows. . . .

By specialising them to a prime we get things like:

$$\begin{aligned} r_{x^2+5y^2}(p) =& ((-20/1) + (-4/1)(5/p)) + ((-20/p) + (-4/p)(5/1)) \\ =& (1 + (5/p)) + ((-20/p) + (-4/p)) \\ =& (1 + (-4/p))(1 + (5/p)) \end{aligned}$$

If this is non-zero (so the prime p is represented) then both factors must be non-zero, i.e. $(5/p) = 1$ and $(-4/p) = 1$, so these formulae allow us to derive our earlier criteria.

8 Epilogue

There is still plenty to be done, and plenty of different directions we can look at.

Non-fundamental discriminants: class field theory can also handle non-fundamental discriminants but we would first need to make a study of orders in quadratic fields, things like $\mathbb{Z}[2\sqrt{-1}] \subsetneq \mathbb{Z}[\sqrt{-1}] = \mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-1})$.

Separating all forms of discriminant D. With class field theory we can make some headway here. Subgroups of the (narrow) class group (corresponding to subgroups of quadratic forms) are themselves generalised ideal class groups. (They are the inverse image of a quotient map, so define a subgroup sitting between $\mathcal{P}^{(+)}(K)$ and $\mathcal{I}(K)$.) Hence they give rise to class fields. These are in fact intermediate fields between the Hilbert/Narrow class field and K as the Galois group is isomorphic to the (narrow) class group. With a bit of inclusion/exclusion type reasoning we can sometimes isolate some or all quadratic forms. For examples $\mathbb{Q}(\sqrt{-17})$ has class group $\mathbb{Z}_2 \times \mathbb{Z}_2$, corresponding to four forms $Q_{11}, Q_{12}, Q_{21}, Q_{22}$. We can separate Q_{11}, and Q_{11}, Q_{12}, so can separate Q_{12} by negating the criteria for the principal form.

But what if we have $\mathbb{Q}(\sqrt{-47})$ where the class group is $\mathbb{Z}_5$. There are no non-trivial subgroups. So either we find a condition for the principal form, or we find a condition for all forms and all forms less the principal form. We can't separate any of the non-principal forms.

But the coefficients of the theta series modular forms can separate out these forms.

Counting other rep numbers: well this L-series factorisation stuff works fine when the class group is $\mathbb{Z}_2^m$ (when so called genus theory works), but doesn't work otherwise. (Here the characters would take values other than ±1 and the L-series don't necessarily factor in this nice way. Modular forms and their connection with elliptic curves can still be used to put bounds on the rep numbers. Also what do you do in the indefinite case. . . the rep numbers are infinite, but is there a sensible way mod out the units and count the rep numbers? The Theta series now have a non-holomorphic (in fact non-meromorphic) part, so how?

The last bit about more general polynomial equations leading to non-abelian class field theory and the Langlands program I just throw in because Jens insists it sounds good.