34.1. Primes of the form $x^2 + ny^2$. (Ref: Cox)

We saw on the first day,

<u>Thm.</u> If $p \neq 2$, then

$$p = x^2 + y^2 \longleftrightarrow p \equiv 1 \pmod 4.$$

Can push it further. If $p \neq 2$,

$$p = x^2 + 2y^2 \longleftrightarrow x^2 + 2y^2 \text{ factors} \pmod p$$

$$\updownarrow$$

$$\left(\frac{-2}{p}\right) = 1$$

$$\updownarrow$$

$$p \equiv 1, 3 \pmod 8.$$

Really? $x^2 + 2y^2$

x \ y	0	1	2	3	4
1	1	3	9	19	33
2	4	6	12	22	36
3	9	11	17	27	41
4	16	18	24	34	

This seems to actually work!

If $p \neq 2, 3$,

$$p = x^2 + 3y^2 \longleftrightarrow x^2 + 3y^2 \text{ factors} \pmod p$$

$$\updownarrow$$

$$\left(\frac{-3}{p}\right) = 1 \longleftrightarrow p \equiv 1, 11 \pmod{12}.$$

$11 = 2^2 + 3 \cdot 1^2$, $13 = 1^2 + 3 \cdot 2^2$, $23 = 3^2 + 2 \cdot 2^2$, ...

If $p \neq 2, 5$,

$$p = x^2 + 5y^2 \longleftrightarrow x^2 + 5y^2 \text{ factors} \pmod p$$

$$\updownarrow$$

$$\left(\frac{-5}{p}\right) = 1 \longleftrightarrow \left(\frac{-1}{p}\right) \cdot \left(\frac{p}{5}\right) = 1$$

$$\updownarrow$$

$$p \equiv 1, 3, 7, 9 \pmod{20}.$$

List: Do you see 3 or 7?
Nope. [SHIT].

34.2.

Wait, so how did the proof go?

"Reciprocity Step": If $p \equiv 1 \pmod{4}$ then $p \mid x^2 + y^2$ for some coprime x, y.

For example, write $p = 4k + 1$

$$x^{4k} - 1 \equiv 0 \pmod{p}$$
$$\text{|||}$$
$$(x^{2k} - 1)(x^{2k} + 1)$$

Find some x with $p \nmid x^{2k} - 1$.

"Descent Step".

Recognize $x^2 + y^2$ as the norm form from $\mathbb{Z}[i]$.

Write $x^2 + y^2 = (x + iy)(x - iy)$ with $p \mid x^2 + y^2$

and factor into primes.

By <u>unique factorization in $\mathbb{Z}[i]$</u>, p equals a product of two primes.

i.e. $p = (a + ib)(a - ib)$

and $p = a^2 + b^2$.

But $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

In fact,

$p = x^2 + 5y^2 \longleftrightarrow p \equiv 1, 9 \pmod{20}$

$2p = x^2 + 5y^2 \longleftrightarrow p \equiv 3, 7 \pmod{20}$.

And,

$p = \left\{ \begin{matrix} x^2 + 14y^2 \\ 2x^2 + 7y^2 \end{matrix} \right\} \longleftrightarrow p \equiv 1, 9, 15, 23, 25, 39 \pmod{56}$

$3p = x^2 + 14y^2 \longleftrightarrow p \equiv 3, 5, 13, 19, 27, 45 \pmod{56}$.

$\left(\frac{-14}{p}\right) = 1$.

34.3.

This can be explained by quadratic forms.

Multiple genera.

But how to get just $p = x^2 + 14y^2$?

Theorem. If $p \neq 7$ is an odd prime, then

$$p = x^2 + 14y^2 \longleftrightarrow \begin{cases} \left(\frac{-14}{p}\right) = 1 \text{ and } (x^2+1)^2 \equiv 8 \pmod p \\ \text{has an integer solution.} \end{cases}$$

How do we get this?

$x^2 + 14y^2$ is the norm form from $\mathbb{Z}[\sqrt{-14}]$ to $\mathbb{Z}$.

So, $p = x^2 + 14y^2 = (x + \sqrt{-14}\,y)(x - \sqrt{-14}\,y)$

$\Updownarrow$

p is the norm of a principal ideal.

So, we need two things to happen:

(1) p has to split as $p = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ in $\mathbb{Z}[\sqrt{-14}]$. So, $\left(\frac{-14}{p}\right) = 1$.

(2) $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ have to be principal.

$Cl(\mathbb{Z}[\sqrt{-14}])$ has size 4, so there's a $\frac{1}{4}$ chance.

How do we guarantee that?

Class field theory.

34.4. Recall that the Artin map gives an isomorphism

$$Cl(\mathbb{Z}[\sqrt{-14}]) \xrightarrow{\sim} Gal(H/K)$$

where H is the Hilbert class field of $K = \mathbb{Q}(\sqrt{-14})$.

So, $p = x^2 + 14y^2 \longleftrightarrow \left(\frac{-14}{p}\right) = 1$ and

$(\mathfrak{p}, H/K) = 1$ in $Gal(H/K)$.

(By the way: $(\mathfrak{p}, H/K) = (\bar{\mathfrak{p}}, H/K)^{-1}$ so it doesn't matter which $\mathfrak{p}$ we pick.)

Now how do we guarantee $(\mathfrak{p}, H/K) = 1$?

Use our theorem on Frobenius and cycle structure.

The trivial elt. of $(\mathfrak{p}, H/K)$ fixes all the roots mod $\mathfrak{p}$.

So $(\mathfrak{p}, H/K) = 1 \longleftrightarrow \mathfrak{p}$ splits completely in H

$\updownarrow$

p does too.

~~Now H is Galois over $\mathbb{Q}$ also, because if τ generates Gal(K/$\mathbb{Q}$) then $\tau(L)$ is an UR abelian ext. of $\tau(K) = K$.~~

~~In fact, $L = K(a)$ for a~~

So, $p = x^2 + 14y^2 \longleftrightarrow p$ splits in $\mathbb{Q}(\sqrt{-14})$ and then again in H. (so: splits completely in H)

Now, H is Galois over $\mathbb{Q}$, because for any auto. $\tau: H \hookrightarrow \mathbb{C}$, $\tau(H)$ is also an UR abelian extension of K, hence contained in H.

$$\begin{tikzcd}[column sep=small]
 & H \arrow[d, dash] \\
E \arrow[ur, dash] \arrow[d, dash] & K \\
\mathbb{Q} \arrow[ur, dash] &
\end{tikzcd}$$

Let $E := H \cap \mathbb{R}$ be fixed field of complex conjugation. Min poly $f(x)$. Also generates H/K.
(It's Galois)

Then, p splits completely in H

$\updownarrow$

p splits completely in E and K.

(To show $\longrightarrow$: By Galoisness, enough to show $f(x)$ has a root in $\mathbb{Z}/(p)$ $\longleftrightarrow$ it does in $\mathcal{O}_K/\mathfrak{p}$ ... but these are isomorphic.)

By "brute force" we find $L = K(\alpha)$ with $\alpha = \sqrt{2\sqrt{2} - 1}$

also $E = \mathbb{Q}(\alpha)$,

and α has min poly $x^4 + 2x^2 - 7 = (x^2+1)^2 - 8$.

Discriminant is $-2^{14} \cdot 7$.

So, apart from 2 and 7,

$$p = x^2 + 14y^2 \Longleftrightarrow \begin{cases} \left(\frac{-14}{p}\right) = 1 \text{ and } (x^2+1)^2 \equiv 8 \mod p \\ \text{has an integer solution.} \end{cases}$$

36.1. Some additional related topics.

* More about relative extensions.
  (Rel discriminants, etc.)

* Function fields.

* Class field theory. — Basic proofs
  - Kronecker - Weber theorem.
  - Adeles and ideles. (Given abelian L/K, Artin map $\mathbb{A}_K^\times / K^\times \to \mathrm{Gal}(L/K)$ etc., surjective.)
  - Cohomology, etc.

* Analytic number theory. Relation to above.
  Tate's thesis. (Artin L-functions)

* Iwasawa theory.

* Commutative ring theory.] next year!
* Algebraic geometry.]

* Elliptic curves. (same sort of machinery)

* Geometry of numbers.