Using Quadratic Reciprocity
Lecture 2

Useful to memorize that

$\left(\frac{-1}{p}\right)=1 \Leftrightarrow p \equiv 1 \bmod 4$

$\left(\frac{2}{p}\right)=1 \Leftrightarrow p \equiv 1,7 \equiv \pm 1 \bmod 8$

The nonzero squares modulo p have $\frac{p-1}{2}$ terms are

$p=3$: 1

$p=5$: $1,4$

$p=7$: $1,2,4$

a odd $\Rightarrow a \equiv 1,3,5,7 \equiv \pm 1, \pm 3 \ (8)$

$\Rightarrow a^2 \equiv 1 \bmod 8.$

Last time: when $d \in \mathbb{Z}$, $d \neq \square$ and p is prime,

$p = x^2 - dy^2$ in $\mathbb{Z} \Rightarrow d \equiv \square \bmod p.$

The converse is true when $d=-1, d=2$:

$-1 \equiv \square \bmod p \Rightarrow p = x^2 + y^2$ in $\mathbb{Z}$ $(d=-1)$

$2 \equiv \square \bmod p \Rightarrow p = x^2 - 2y^2$ in $\mathbb{Z}$ $(d=2)$

Converse false when $d=10$ & $p=3$ and $d=3$ & $p=11$.

$10 \equiv \square \bmod 3$, $3 \neq x^2 - 10y^2$

$3 \equiv \square \bmod 11$, $11 \neq x^2 - 3y^2$

Theorem: When $d \in \mathbb{Z}$, $d \neq \square$ and $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d}\}$ has unique factorization (it's a UFD), for primes p

$$d \equiv \square \bmod p \Rightarrow \pm p = x^2 - dy^2 \text{ in } \mathbb{Z}$$

so in this case

$$d \equiv \square \bmod p \Leftrightarrow \pm p = x^2 - dy^2 \text{ in } \mathbb{Z}$$

Rk: $\mathbb{Z}[\sqrt{d}]$ is UFD for $d = -1$ ($\mathbb{Z}[i]$), $d = \pm 2$, $d = 3$ (not $d = -3$ or ± 5)

Ex $\mathbb{Z}[\sqrt{3}]$ is UFD, $3 \equiv \square \bmod 11$, $11 \neq x^2 - 3y^2$, $-11 = 1^2 - 3 \cdot 2^2$

Proof $d \equiv \square \bmod p \Rightarrow d \equiv n^2 \bmod p$

$$\Rightarrow p \mid (n^2 - d) \text{ in } \mathbb{Z} \subset \mathbb{Z}[\sqrt{d}]$$

In $\mathbb{Z}[\sqrt{d}]$, $n^2 - d = (n + \sqrt{d})(n - \sqrt{d})$

($d = -1$: $n^2 + 1 = (n+i)(n-i)$)

So $p \mid (n + \sqrt{d})(n - \sqrt{d})$ in $\mathbb{Z}[\sqrt{d}]$,

where p may or may not be irreducible

(In $\mathbb{Z}[i]$, 3 is irreducible but $2 = (1+i)(1-i)$ and $5 = (1+2i)(1-2i)$.)

Let's show p is reducible in $\mathbb{Z}[\sqrt{d}]$ by not being irreducible in $\mathbb{Z}[\sqrt{d}]$: if p is irreducible in UFD $\mathbb{Z}[\sqrt{d}]$ then

$$p \mid (n+\sqrt{d})(n-\sqrt{d}) \Rightarrow p \mid (n+\sqrt{d}) \text{ or } p \mid (n-\sqrt{d})$$

So some $p(a+b\sqrt{d}) = n+\sqrt{d}$ or $n-\sqrt{d}$

$\Rightarrow pb = 1$ or -1 in $\mathbb{Z}$ N2.

Thus p is reducible in $\mathbb{Z}[\sqrt{d}]$:

$p = \alpha\beta$ for α, β in $\mathbb{Z}[\sqrt{d}]$ not units.

Now we use norms on both sides.

$N: \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$ by $N(a+b\sqrt{d}) = a^2 - db^2$

or $N(\alpha) = \alpha\bar{\alpha}$

$= (a+b\sqrt{d})(a+b\sqrt{d})$

- $N(\alpha\beta) = N(\alpha)N(\beta)$
- $N(a) = a^2$ for $a \in \mathbb{Z}$

Back to $p = \alpha\beta$ in $\mathbb{Z}[\sqrt{d}]$:

$N(p) = N(\alpha\beta)$

$p^2 = N\alpha \, N\beta$ in $\mathbb{Z}$

$\Rightarrow N(\alpha) = \pm 1, \pm p$, or $\pm p^2$.

$d < 0 \Rightarrow a^2 - db^2 > 0$ but $d > 0 \Rightarrow a^2 - db^2$ could be > 0 or < 0

$N(1+2\sqrt{2}) = -7$

$N(3+\sqrt{2}) = 7$

$N(\alpha)=1 \Rightarrow \alpha\bar{\alpha}=1 \Rightarrow \alpha = \text{unit}$: NO

$N(\alpha)=-1 \Rightarrow \alpha\bar{\alpha}=-1$

$\Rightarrow \alpha(-\bar{\alpha})=1 \Rightarrow \alpha = \text{unit}$: NO

Similarly, $N(\beta) \neq \pm 1$.

Thus $N(\alpha) = \pm p$. Write $\alpha = x+y\sqrt{d}$ to get $\pm p = N(x+y\sqrt{d}) = x^2 - dy^2$. □

If $d<0$ then $-p = x^2 - dy^2$ is impossible

So if

$\mathbb{Z}[\sqrt{d}]$ = UFD, $d<0$ then

$d \equiv 0 \bmod p \iff p = x^2 - dy^2$

For $d>0$, sometimes

$-p = x^2 - dy^2 \Rightarrow p = x'^2 - dy'^2$

but sometimes not ($-11 = 1^2 - 3\cdot 2^2$, $11 \neq x'^2 - 3y'^2$)

$-p = x^2 - dy^2 \Rightarrow p = -N(x+y\sqrt{d})$. (If)

-1 is a norm ($-1 = a^2 - db^2$) then

$p = N(a+b\sqrt{d})N(x+y\sqrt{d})$

$= N((a+b\sqrt{d})(x+y\sqrt{d})) = N(x'+y'\sqrt{d})$

$= x'^2 - dy'^2$

Ex $d=2$:

$-7 = 1 - 2\cdot 2^2 = N(1+2\sqrt{2})$

$\Rightarrow 7 = -N(1+2\sqrt{2})$ & $-1 = N(1+\sqrt{2})$

$= N(1+\sqrt{2})N(1+2\sqrt{2})$

$= N((1+\sqrt{2})(1+2\sqrt{2}))$

$= N(5+3\sqrt{2}) = 25-18$ ✓

$= 5^2 - 2\cdot 3^2$

Ex $d=3$ we saw $11 \neq x^2-3y^2, -11 = 1^2-3\cdot 2^2$

and $-1 \neq a^2-3b^2 = N(a+b\sqrt{3})$

Question: when $\pm p = x^2-dy^2$ has a $\mathbb{Z}$-solution, how can we find x, y?

Or for any $n \in \mathbb{Z}-\{0\}$ and $d \in \mathbb{Z}^+$, $d \neq \square$, how can we decide if $n = x^2-dy^2$ and solve for x, y when they exist?

$n=1$: $x^2-dy^2=1$ has a solution (x,y) in $\mathbb{Z}^+$ (Pell's equation)

Could rewrite as $x^2 = dy^2 + 1$ and let $y = 1, 2, 3, \ldots$ until $dy^2 + 1 = \square$. This algorithm will terminate (better: use continued fraction of $\sqrt{d}$)

Fact: In terms of some (any) solution (x_0, y_0) to $x^2 - dy^2 = 1$ in $\mathbb{Z}^+$, d, and $n \in \mathbb{Z} - \{0\}$, there is a finite search space for existence of a $\mathbb{Z}^+$-soln to $x^2 - dy^2 = n$.

Cor: If $d \equiv \square \bmod p$ and $\pm p \neq x^2 - dy^2$ for some prime p (both signs) then $\mathbb{Z}[\sqrt{d}]$ is not UFD.

Ex $10 \equiv \square \bmod 3$, $\pm 3 \neq x^2 - 10y^2$ (both signs) so $\mathbb{Z}[\sqrt{10}]$ is not a UFD

If $\mathbb{Z}[\sqrt{d}]$ is not UFD is there always such p?

Ex $d = -5$: $\mathbb{Z}[\sqrt{-5}]$ is not UFD since

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

(all irreducible)

Check for prime $p \equiv 3, 7 \bmod 20$ that $-5 \equiv \square \bmod p$ but $\pm p \neq x^2 + 5y^2$

Rk: ① If $d \in \mathbb{Z}$ is not squarefree, then $\mathbb{Z}[\sqrt{d}] \neq$ UFD since it fails the rational roots theorem (it is not integrally closed).

② If $d \in \mathbb{Z}$ is sqfree and $d \equiv 1 \bmod 4$, then $\mathbb{Z}[\sqrt{d}] \neq$ UFD since it fails the rational roots theorem (same reason as in ①).

③ If $d \in \mathbb{Z}$ is sqfree and $d \not\equiv 1 \bmod 4$, then $\mathbb{Z}[\sqrt{d}] \neq$ UFD $\Rightarrow$ there are infinitely many primes p such that $d \equiv \square \bmod p$ but $\pm p \neq x^2 - dy^2$ for $x, y \in \mathbb{Z}$.

(both signs)

A combinatorial interpretation of the norm: for $x, y \in \mathbb{Z}$,

$$|x^2 - dy^2| = |\underbrace{\mathbb{Z}[\sqrt{d}]/(x+y\sqrt{d})}_{\text{quotient ring}}|$$

So saying we can write p or $-p$ as $x^2 - dy^2$ means $|\mathbb{Z}[\sqrt{d}]/(x+y\sqrt{d})| = p$: there's a principal ideal $(x+y\sqrt{d})$ in $\mathbb{Z}[\sqrt{d}]$ with index p.

When $d \equiv \square \bmod p$ and we can't write p or $-p$ as $x^2 - dy^2$ for $x, y \in \mathbb{Z}$, there's no principal ideal in $\mathbb{Z}[\sqrt{d}]$ with index p but there might be a non-principal ideal in $\mathbb{Z}[\sqrt{d}]$ with index p.

Ex $10 \equiv \square \bmod 3$ and $\pm 3 \neq x^2 - 10y^2$ in $\mathbb{Z}$, so in $\mathbb{Z}[\sqrt{10}]$ no principal ideal has index 3, but the nonprincipal ideal $I = (3, 1+\sqrt{10})$ has index 3:

$$I = (3, 1+\sqrt{10}) = 3\mathbb{Z}[\sqrt{10}] + (1+\sqrt{10})\mathbb{Z}[\sqrt{10}]$$
$$\overset{!}{=} 3\mathbb{Z} + (1+\sqrt{10})\mathbb{Z}$$

and $\mathbb{Z}[\sqrt{10}] = \mathbb{Z}[1+\sqrt{10}] = \mathbb{Z} + (1+\sqrt{10})\mathbb{Z}$, so

$$\mathbb{Z}[\sqrt{10}]/I = (\mathbb{Z} \oplus (1+\sqrt{10})\mathbb{Z})/(3\mathbb{Z} \oplus (1+\sqrt{10})\mathbb{Z})$$
$$\cong \mathbb{Z}/3\mathbb{Z} \oplus (1+\sqrt{10})\mathbb{Z}/(1+\sqrt{10})\mathbb{Z}$$
$$\cong \mathbb{Z}/3\mathbb{Z} \text{ has order } 3, \text{ so}$$

(as additive groups)

$$|\mathbb{Z}[\sqrt{10}]/I| = 3.$$