Using Quadratic Reciprocity
Lecture 4

<u>Correction</u>: when $p \equiv 1 \bmod 4$, $\left(\frac{a}{p}\right)=1$, and solve $x^2 \equiv a \bmod p$ by Tonelli–Shanks, it need <u>not</u> happen that half the b's with $\left(\frac{b}{p}\right)=-1$ lead to one solution and half to the other.

<u>Ex</u> $x^2 \equiv 3 \bmod 13$ has $x_1 = 9$ and $\underline{y_1 = 1}$, so
$\equiv 4^2$ Tonelli–Shanks terminates before we use b (well, c)

What can be said about $\left(\frac{a}{p}\right)$ as p varies and $a \in \mathbb{Z}$ is fixed ($a \neq 0$)?

① $a = \square$ in $\mathbb{Z} \Rightarrow \left(\frac{a}{p}\right)=1$ if $p \nmid 2a$

② $a \neq \square$ in $\mathbb{Z} \Rightarrow \left(\frac{a}{p}\right)=1$ for inf. many p

Thm: If $f(x) \in \mathbb{Z}[x]$ is not constant then $f(x) \equiv 0 \bmod p$ has a root for inf. many p. See MSE 1019538. Apply this to $f(x) = x^2 - a$.

③ $a \neq \square$ in $\mathbb{Z} \Rightarrow \left(\frac{a}{p}\right) = -1$ for inf. many p.

See Ireland/Rosen p.57 (2nd ed.)

Proof can be made simpler using Jacobi symbols.

<u>Rk</u>: Using QR + Dirichlet's theorem, one can show the sets of primes

$$\left\{p : \left(\frac{a}{p}\right) = 1\right\} \text{ and } \left\{p : \left(\frac{a}{p}\right) = -1\right\}$$

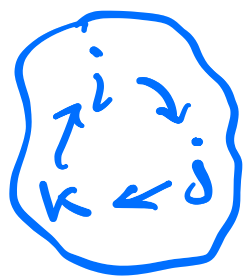
both have density 1/2.

Let's apply this result to division rings, which are "possibly noncommutative fields."

<u>Ex</u>: Hamilton's quaternions

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k,$$

with $i^2 = -1$, $j^2 = -1$, $k = ij = -ji$, $k^2 = -1$, $ik = -j$, $ki = j$, $jk = i$, $kj = -i$.



For $q = a + bi + cj + dk$, set

$$\bar{q} = a - bi - cj - dk \text{ and}$$

$N(q) = q\bar{q} = \bar{q}q = a^2 + b^2 + c^2 + d^2 > 0$ if $q \neq 0$,

so q has mult. inverse $\frac{1}{N(q)}\bar{q}$.

The center of $\mathbb{H}$ is $\mathbb{R}$ and

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$
$$= \mathbb{R} + \mathbb{R}i + (\mathbb{R} + \mathbb{R}i)j$$
$$= \mathbb{C} + \mathbb{C}j,$$

with $jz = \bar{z}j$ for $z \in \mathbb{C}$.

<u>Thm</u> (Frobenius) The <u>only</u> fin-dim $\mathbb{R}$-central noncomm division ring is $\mathbb{H}$.

For $\mathbb{Q}_p$ in place of $\mathbb{R}$ we have

- finitely many $\mathbb{Q}_p$-central div. rings of each dimension
- <u>one</u> noncomm 4-dim $\mathbb{Q}_p$-central div ring (for $p=2$ it's $\mathbb{H}(\mathbb{Q}_2)$)

<u>Defn</u> For a field F of characteristic $\neq 2$ a <u>quaternion algebra</u> over F is a ring

$$F + Fi + Fj + Fk$$

where $i^2 = a \in F^\times$, $j^2 = b \in F^\times$, $k = ij = -ji$
$\Rightarrow k^2 = -ab \in F^\times$.

Denote this by $(a,b)_F$.

Ex $(2,5)_{\mathbb{Q}} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ with $i^2=2$, $j^2=5$, $k=ij=-ji$ has $k^2=-10$.

Note $(2,5)_{\mathbb{Q}} = \mathbb{Q}+\mathbb{Q}i + (\mathbb{Q}+\mathbb{Q}i)j$
$= \mathbb{Q}(\sqrt{2}) + \mathbb{Q}(\sqrt{2})j$
and $j\alpha = \bar{\alpha}j$ for $\alpha \in \mathbb{Q}(\sqrt{2})$.

Properties
1. $(a,b)_F \cong (b,a)_F$.
2. $(1,b)_F \cong M_2(F)$
3. If $(a,b)_F \not\cong M_2(F)$ then $(a,b)_F$ is a division ring.

Thm For $a \in \mathbb{Z}-\{0\}$ and odd prime p,

$\left(\frac{a}{p}\right) = -1 \Rightarrow (a,p)_{\mathbb{Q}}$ is a division ring

Ex $\left(\frac{2}{5}\right) = -1 \Rightarrow (2,5)_{\mathbb{Q}}$ is division ring.

Ex $\left(\frac{3}{11}\right) = 1$, $\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1$, so $(3,11)_{\mathbb{Q}} \cong (11,3)_{\mathbb{Q}}$ is a division ring.

Rk: For odd primes $p \neq q$,

$(p,q)_{\mathbb{Q}}$ is a div ring $\iff \left(\frac{p}{q}\right) = -1$ or $\left(\frac{q}{p}\right) = -1$

Thm: For $a \in \mathbb{Z}$ and distinct odd primes p and q,

$\left(\frac{a}{p}\right) = -1$ and $\left(\frac{a}{q}\right) = -1 \Rightarrow (a,p)_{\mathbb{Q}}$ and

$(a,q)_{\mathbb{Q}}$ are nonisom. quat. algebras.

Ex Inf. many primes p are 3 mod 4 so all div rings $(-1,p)_{\mathbb{Q}}$ for such p are nonisomorphic.

For all $a \in \mathbb{Z}$, $a \neq \square$ in $\mathbb{Z}$, there are inf. many odd primes p s.t. $\left(\frac{a}{p}\right) = -1$, so we get inf many nonisom div rings

$(a,p)_{\mathbb{Q}} = \mathbb{Q}(\sqrt{a}) + \mathbb{Q}(\sqrt{a})j$ with $j^2 = p$

and $j\alpha = \bar{\alpha} j$ $\forall \alpha \in \mathbb{Q}(\sqrt{a})$

Last time: if $\mathbb{Z}[\sqrt{d}]$ is UFD and p is prime, then

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

can remove minus sign if $-1 = x^2 - dy^2$ in $\mathbb{Z}$

Replace $\mathbb{Z}$ with $\mathbb{Z}[i]$, where units $= \{\pm 1, \pm i\}$ and the primes are $1+i$ and "odd" primes: the primes with odd norm like $1+2i, 1-2i, 3, 7, -11, 4-i, \ldots$

The only prime in $\mathbb{Z}[i]$ up to unit multiple dividing 2 is $1+i$:

$$2 = (1+i)(1-i) = (1+i)(1+i)(-i) = -i(1+i)^2$$

For π = odd prime in $\mathbb{Z}[i]$ and $\alpha \in \mathbb{Z}[i]$, set

$$\left(\frac{\alpha}{\pi}\right) = \begin{cases} 1 & \text{if } \alpha \equiv \square \bmod \pi,\ \pi \nmid \alpha \\ -1 & \text{if } \alpha \not\equiv \square \bmod \pi \\ 0 & \text{if } \alpha \equiv 0 \bmod \pi \end{cases}$$

Then $\alpha \equiv \beta \bmod \pi \Rightarrow \left(\frac{\alpha}{\pi}\right) = \left(\frac{\beta}{\pi}\right)$. Since $|\mathbb{Z}[i]/\pi| = N(\pi)$, we get $\left(\frac{\alpha}{\pi}\right) \equiv \alpha^{\frac{N\pi - 1}{2}} \bmod \pi$ and $\left(\frac{\alpha\beta}{\pi}\right) = \left(\frac{\alpha}{\pi}\right)\left(\frac{\beta}{\pi}\right)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.

Calculating $\left(\frac{\alpha}{\pi}\right)$ is thus reduced to a main law for $\left(\frac{\pi'}{\pi}\right)$ for odd primes π, π' that are not unit multiples and supplementary laws for $\left(\frac{i}{\pi}\right), \left(\frac{1+i}{\pi}\right)$.

Main law: $\left(\frac{\pi'}{\pi}\right) = (-1)^{T(\pi,\pi')}\left(\frac{\pi}{\pi'}\right)$

where $T(\pi,\pi') \in \mathbb{Z}/(2)$ is det. by π, π' mod $4\mathbb{Z}[i]$, $\left(\frac{i}{\pi}\right)$ is det. by π mod $4\mathbb{Z}[i]$ and $\left(\frac{1+i}{\pi}\right)$ is determined by π mod $4(1+i)\mathbb{Z}[i]$. Details are in notes.

Thm: If $\delta \in \mathbb{Z}[i]$ is not a square and $\mathbb{Z}[i][\sqrt{\delta}]$ is UFD then for primes π in $\mathbb{Z}[i]$,

$\delta \equiv \square \bmod \pi \iff u\pi = x^2 - \delta y^2$ in $\mathbb{Z}[i]$ for some unit u and we can avoid u-factor if $i = x^2 - \delta y^2$ in $\mathbb{Z}[i]$

Ex: $x^2-(1+i)y^2 \stackrel{?}{=} \pi$

Fact: $\mathbb{Z}[i][\sqrt{1+i}] = \mathbb{Z}[\sqrt{1+i}]$ is UFD and

$$i = x^2-(1+i)y^2 \quad \text{for } x=i, y=i.$$

Thus

$$1+i \equiv \square \bmod \pi \iff \pi = x^2-(1+i)y^2 \text{ in } \mathbb{Z}[i]$$

Try $\pi = 2+i$:

$1+i \equiv 4 \bmod 2+i$, so we must be able to solve

$$x^2-(1+i)y^2 = 2+i \text{ in}$$

$\mathbb{Z}[i]$: $x=3$, $y=2-i$.

Try $\pi = 2-5i$

$1+i \equiv 100 \bmod 2-5i$, so we must have a soln to

$$x^2-(1+i)y^2 = 2-5i$$

in $\mathbb{Z}[i]$: $x = 2-i$, $y=1$.