Using Quadratic Reciprocity

Lecture 4

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

**Example:** \( x^2 \equiv 3 \mod 13 \) has \( x_1 = 9 \) and \( y_1 = 1 \), so 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. \( a = \Omega \) in \( \mathbb{Z} \) \( \Rightarrow \ \left( \frac{a}{p} \right) = 1 \) if \( p \nmid 2a \)
2. \( a + \Omega \) in \( \mathbb{Z} \) \( \Rightarrow \ \left( \frac{a}{p} \right) = 1 \) for infinitely many \( p \)

Thm: If \( f(x) \in \mathbb{Z}[x] \) is not constant, then \( f(a) \equiv 0 \mod p \) has a root for infinitely many \( p \). See MSE 109538. Apply this to \( f(x) = x^2 - a \).
3. \(a \neq 0 \text{ in } \mathbb{Z} \Rightarrow (\frac{a}{p}) = -1 \) for infinitely many \(p\).

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

Proof can be made simpler using Jacobi symbols.

**Rk:** Using QR + Dirichlet's theorem, one can show the sets of primes

\[ \exists p: (\frac{a}{p}) = 1 \text{ and } \exists p: (\frac{a}{p}) = -1 \]

both have density \(\frac{1}{2}\).

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

**Ex:** Hamilton's quaternions

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

with \(i^2 = j^2 = k^2 = -1\), \(ij = -ji = k\).

For \(q = a + bi + cj + dk\), set

\[ \overline{q} = a - bi - cj - dk \text{ and } N(q) = q\overline{q} = a^2 + b^2 + c^2 + d^2 > 0 \text{ if } q \neq 0. \]

So \(q\) has mult. inverse \(\frac{1}{N(q)}\) \(\overline{q}\).
The center of $H$ is $R$ and

$$H = R + Ri + Rj + RK = R + Ri + (R + Ri)j = C + Cj,$$

with $j^2 = cij$ for $i \in C$.

**Thm (Frobenius)** The only fin-dim $R$-central noncomm division ring is $H$.

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

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

---

**Defn** For a field $F$ of characteristic $\neq 2$

- a quaternion algebra over $F$ is a ring $F + Fi + Fj + Fk$

where $i^2 = a \in F^x$, $j^2 = b \in F^x$, $k = ij = -ji$ and $k^2 = -ab \in F^x$. 
Denote this by \((a,b)_F\).

\[ \text{Ex} \ (2,5)_Q = \alpha + \alpha i + \alpha j + \alpha k \ \text{with} \]
\[ i^2 = 2 \quad j^2 = 5, \quad k = ij = -j i \ \text{has} \ \alpha^2 = -10. \]

Note \((2,5)_Q = \alpha + \alpha i + (\alpha + \alpha i)j = \alpha(\sqrt{2}) + \alpha(\sqrt{5})j \]
and \(ja = \overline{a}i \) for \(a \in \mathbb{Q}(\sqrt{5})\).

**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 \(a \in \mathbb{Z} - \{0, 1\}\) and odd prime \(p\),

\[(\frac{a}{p}) = -1 \Rightarrow \ (a, p)_Q \ \text{is a division ring}.\]

**Ex** \((\frac{2}{5}) = -1 \Rightarrow \ (2, 5)_Q \ \text{is a division ring}.\)

**Ex** \((\frac{3}{11}) = 1, \ (\frac{1}{3}) = (\frac{2}{3}) = -1\), \(\alpha \in \mathbb{Q}(3, \sqrt{3})\), \((3, \sqrt{3})_Q \cong (11, \sqrt{3})_Q\) is a division ring.
Rk: For odd primes $p \neq 3$, $(p, 8) \mathbb{Q}$ is a division ring $\iff (\frac{8}{p}) = -1$ or $(\frac{8}{p}) = -1$

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

$$(\frac{a}{p}) = -1 \text{ and } (\frac{a}{q}) = -1 \implies (a, p) \mathbb{Q} \text{ and } (a, q) \mathbb{Q} \text{ are nonisomorphic algebras.}$$

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

For all $a \in \mathbb{Z}$, $a \neq 0$ in $\mathbb{Z}$, there are inf. many odd primes $p$ s.t. $(\frac{a}{p}) = -1$, so we get inf many nonisomorphic div rings

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

and $j a = x j \forall x \in \mathbb{Q}(\sqrt{a})$
Last time: if \( \mathbb{Z}[(\sqrt{d})] \) is UFD and \( p \) is prime, then

\[
\pm p = x^2 - dy^2 \quad \text{in } \mathbb{Z}
\]

can remove minus sign if \( p = 2 \) or \( p \equiv 1 \text{ mod } 4 \).

Replace \( \mathbb{Z} \) with \( \mathbb{Z}[i] \), where units are \( \{1, -1, i, -i\} \) and the primes are \( 1 + i \) and "odd" primes:

the primes with odd norm like \( 1 + 2i, 1 - 2i, 3, 7, -11, 4 - i, \ldots \) up to unit multiple.

The only prime in \( \mathbb{Z}[i] \) dividing \( 2 \) is \( 1 + i \):

\[
2 = (1+i)(1-i) = (1+i)(1+i)(-i) = (-i)(1+i)^2
\]

For \( \pi = \text{odd prime in } \mathbb{Z}[i] \) and \( \alpha, \beta \in \mathbb{Z}[i] \), set

\[
\left( \frac{\alpha}{\pi} \right) = \begin{cases} 
1 & \text{if } \alpha \equiv \beta \mod \pi, \pi \nmid \alpha \\
-1 & \text{if } \alpha \equiv -\beta \mod \pi \\
0 & \text{if } \alpha \equiv 0 \mod \pi
\end{cases}
\]

Then \( \alpha \equiv \beta \mod \pi \Rightarrow \left( \frac{\alpha}{\pi} \right) = \left( \frac{\beta}{\pi} \right) \). Since

\[
| \mathbb{Z}[i]/\pi | = N(\pi), \quad \text{we get } \left( \frac{\alpha}{\pi} \right) \equiv \alpha^{N(\pi) - 1} \mod \pi \]

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 \( \left( \frac{d}{n} \right) \) is thus reduced to a main law for \( \left( \frac{d}{p} \right) \) for odd primes \( p, p' \) that are not unit multiples and supplementary laws for \( \left( \frac{d}{p} \right), \left( \frac{d}{p'} \right) \).

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

where \( T(p, p') \in \mathbb{Z}/4 \) is determined by \( p, p' \mod 4 \), \( \left( \frac{d}{p} \right) \) is determined by \( p \mod 4 \) and \( \left( \frac{d}{p'} \right) \) is determined by \( p' \mod 4 \). Details are in notes.

Thm: If \( 8c \in \mathbb{Z}[i] \) is not a square and \( \mathbb{Z}[i][\sqrt{8}] \) is UFD then for primes \( p \) in \( \mathbb{Z}[i] \),

\[ d \equiv 0 \mod p \iff u = x + Sy^2 \text{ in } \mathbb{Z}[i] \text{ for some unit } u \text{ and we can avoid } u \text{-factor if } \]

\[ i = x^2 - Sy^2 \text{ in } \mathbb{Z}[i] \]
Ex: \(x^2 - (1+i)y^2 = \pi\)

Fact: \(\mathbb{Z}[i][\sqrt{1+i}] = \mathbb{Z}[\sqrt{1+i}]\) is UFD and
\[i = x^2 - (1+i)y^2 \quad \text{for} \quad x=i, y=i.\]
Thus
\[1+i \equiv 0 \pmod{\pi} \iff \pi = x^2 - (1+i)y^2 \quad \text{in} \quad \mathbb{Z}[i] \]

Try \(\pi = 2+i\):

\[1+i \equiv 4 \pmod{2+i}, \quad \text{so we must be able to solve} \]
\[x^2 - (1+i)y^2 = 2+i \quad \text{in} \quad \mathbb{Z}[i]: \ x = 3, \ y = 2-i.\]

Try \(\pi = 2-5i\)

\[1+i \equiv 100 \pmod{2-5i}, \quad \text{so we must have a soln to} \]
\[x^2 - (1+i)y^2 = 2-5i \quad \text{in} \quad \mathbb{Z}[i]: \ x = 2-i, \ y = 1.\]