Using Quadratic Reciprocity
Lecture 1

Main law: $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$

$= \begin{cases} \left(\frac{p}{q}\right) \text{ if } p \text{ or } q \equiv 1 \ (4) \\ -\left(\frac{p}{q}\right) \text{ if } p \& q \equiv 3 \ (4) \end{cases}$

Supp. laws: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } p \equiv 1 \ (4) \\ -1 \text{ if } p \equiv 3 \ (4) \end{cases}$

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ if } p \equiv 1, 7 \equiv \pm 1 \ (8) \\ -1 \text{ if } p \equiv 3, 5 \equiv \pm 3 \ (8) \end{cases}$

1st use: Describe for $a \in \mathbb{Z}$ which primes $p > 2$ s.t. $\left(\frac{a}{p}\right) = 1$.

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

$\Leftrightarrow \left(\frac{-1}{p}\right) = 1$ and $\left(\frac{2}{p}\right) = 1$ OR $\left(\frac{-1}{p}\right) = -1, \left(\frac{2}{p}\right) = -1$

$p \equiv 1 \ (4)$ $p \equiv 1, 7 \ (8)$ $p \equiv 3 \ (4)$ $p \equiv 3, 7 \ (8)$

$p \equiv 1 \ (8)$ $p \equiv 3 \ (8)$

$\Leftrightarrow p \equiv 1, 3 \ (8)$

Ex $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \stackrel{?}{=} 1$

$\Leftrightarrow$ $(-1)^{\frac{p-1}{2}} = 1, \left(\frac{p}{3}\right) = 1$ or $(-1)^{\frac{p-1}{2}} = -1, \left(\frac{p}{3}\right) = -1$

$p \equiv 1 (4)$ $p \equiv 1 (3)$ $\quad$ $p \equiv 3 (4)$ $p \equiv 2 (3)$

$p \equiv 1 (12)$ $\quad$ $p \equiv 11 (12)$

$\Leftrightarrow$ $p \equiv 1, 11 \ (12)$

$\Leftrightarrow$ $p \equiv \pm 1 \ (12)$

In general, $\left\{\left(\frac{a}{p}\right) = 1\right\}$ is a set of p given by congruences mod $4|a|$

$\{p : 2 = \text{cube mod } p\}$ is not described by congruences.

Dirichlet's Theorem: if $(a, m) = 1$, there are infinitely many primes p such that $p \equiv a \bmod m$.

Theorem: There are inf. primes $p \equiv 1 (4)$ and infinitely many $p \equiv 3 (4)$.

Proof First treat $p \equiv 3 (4)$.

Let $p_1, \dots, p_r$ be primes that are $3 (4)$ like $3, 7, \dots$ and set

$$N = \underbrace{4 p_1 \cdots p_r}_{\text{odd}} - 1 > 1$$

So $N > 1$ and $N \equiv 3 (4) \Rightarrow$ the prime factors of N are not all $1 \bmod 4$. So N has a prime factor p s.t. $p \equiv 3 (4)$.
Since $p \neq$ any p_i, $\{p_1, \dots, p_r\}$ is not complete

Now we treat $p \equiv 1 \bmod 4$.

Let $p_1, \dots p_r$ be primes that are $1 \bmod 4$ like $5, 13, 17, \dots$ and set

$$N = \underbrace{(2 p_1 \cdots p_r)^2}_{\text{odd}} + 1 \equiv 1 \bmod 4, \quad N > 1$$

Let $p \mid N$ be a prime factor, so $p \neq 2$ or any p_i

$p \mid N \Rightarrow N \equiv 0 \bmod p \Rightarrow (2p_1 \cdots p_r)^2 + 1 \equiv 0 \ (p)$

$\Rightarrow -1 \equiv (2p_1 \cdots p_r)^2 \bmod p$

$\equiv \square \bmod p$

$\Rightarrow p \equiv 1 \ (4)$ and $p \neq$ any p_i

So $\{p_1, \ldots, p_r\}$ is not complete. $\square$

Rk: Use rules for when $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{2}{p}\right) = 1$, $\left(\frac{-2}{p}\right) = 1$ we can show in same way that inf. many primes p satisfy $p \equiv 3 \ (8)$ or $p \equiv 5 \ (8)$ or $p \equiv 7 \ (8)$

Mordell's equation $y^2 = x^3 + k$ $k \in \mathbb{Z} - \{0\}$.

Thm (Siegel) For each $k \neq 0$ in $\mathbb{Z}$, the eqn $y^2 = x^3 + k$ has only finitely many $\mathbb{Z}$-solutions.

Ex (Fermat) $y^2 = x^3 - 2$ has $\mathbb{Z}$-solns $(x, y) = (3, \pm 5)$ and no others.

Thm The equation $y^2 = x^3 + 11$ has no $\mathbb{Z}$-solutions.

Rk It does have $\mathbb{Q}$-solns: $(-\frac{7}{4}, \frac{19}{8})$

Proof Assume (x,y) is a $\mathbb{Z}$-solution.

We'll show $x \equiv 1 \pmod 4$

y	$y^2 \bmod 4$	x	$x^3+11 \bmod 4$
0	0	0	3
1	1	1	0
2	0	2	3
3	1	3	2

→ $x \equiv 1 (4)$ and y is even.

$y^2 = x^3 + 11 \Rightarrow y^2 + 16 = x^3 + 27 = x^3 + 3^3$

$= (x+3)(x^2 - 3x + 9)$

$(x - \frac{3}{2})^2 + \frac{27}{4} > 0$

$x \equiv 1 (4) \Rightarrow x^2 - 3x + 9 \equiv 3 (4)$

& $x^2 - 3x + 9$ is in $\mathbb{Z}^+$ and it's 3 mod 4

It has a prime factor $p \equiv 3 \bmod 4$.

Then $y^2 + 16 \equiv 0 \bmod p$, so $-16 \equiv y^2 (p)$

$\equiv \square (p)$

Since $p > 2$, $-1 \equiv \square (p)$. That implies $p \equiv 1 (4)$ ∎

Rk: You can't prove some $y^2 = x^3 + k$ has no $\mathbb{Z}$-solns just by reduction mod m because $y^2 \equiv x^3 + k \bmod m$ always has a soln (for each m)

See MSE 875983, MO 134352

Question: Given $d \in \mathbb{Z}$, $d \neq \square$, what are the prime values of $x^2 - dy^2$ as x, y run over $\mathbb{Z}$?

Ex $(d=-1)$ $p = x^2 + y^2$ in $\mathbb{Z} \iff p \equiv 1 (4)$

Ex $p = x^2 - 2y^2$ in $\mathbb{Z} \iff p \equiv 1, 7 (8)$

There's a link between

$p = x^2 - dy^2$ and $d \equiv \square \bmod p$.

Thm If $p = x^2 - dy^2$ then $d \equiv \square \bmod p$.

Pf: When $p = x^2 - dy^2$ in $\mathbb{Z}$, $p \nmid y$: if $p | y$ then $p | x^2$ so $p | x$ and then $x^2 - dy^2$ is div. by p^2: $\Rightarrow \Leftarrow$.

Now reduce mod p: $0 \equiv x^2 - dy^2 \bmod p$

so $x^2 \equiv dy^2 \bmod p$.

From $p \nmid y$, $y \not\equiv 0 \bmod p$, so can divide by y^2 to get $\square \equiv d \bmod p$: $d \equiv \square \bmod p$.

□

What about converse?

If $d \equiv \square \bmod p$ does $p = x^2 - dy^2$ for some $x, y \in \mathbb{Z}$?

No in general.

Ex $10 \equiv \square \bmod 3$ but $3 \neq x^2 - 10y^2$ in $\mathbb{Z}$ since $3 \not\equiv \square \bmod 5$.

Ex $3 \equiv \square \bmod 11$, but $11 \neq x^2 - 3y^2$ in $\mathbb{Z}$ since $11 \not\equiv \square \bmod 3$.