HW5 due now.

Cheat sheet for fictional exam due tomorrow.

Today: HW5 Discussion

Grand Finale

Problem 3: Pell's Equation.

Solve $x^2 - 13y^2 = \pm 1$.

Algorithm: Compute continued fraction expansion of $\sqrt{13}$.

$\alpha_0 = \sqrt{13} = 3.6056$ $\quad a_0 = 3$

$\alpha_1 = \frac{1}{0.6056} = 1.6513$ $\quad a_1 = 1$

$\alpha_2 = \frac{1}{0.6513} = 1.5354$ $\quad a_2 = 1$

$\alpha_3 = \frac{1}{0.5354} = 1.8678$ $\quad a_3 = 1$

$\alpha_4 = \frac{1}{0.8678} = 1.1523$ $\quad a_4 = 1$

$\alpha_5 = \frac{1}{0.1523} = 6.5660$ $\quad a_5 = 6 = 2a_0$ STOP

$\sqrt{13} = [3; \overline{1,1,1,1,6}]$ period 5

$\frac{p}{q} = [3; 1,1,1,1]$

$= 18/5$

Fundamental Unit

$u = 18 + 5\sqrt{13}$

$N(u) = -1$ because period 5 (odd)

Conclusion:

$x^2 - 13y^2 = -1 \iff \pm x \pm y\sqrt{13} = u^{2k+1}$

$x^2 - 13y^2 = +1 \iff \pm x \pm y\sqrt{13} = u^{2k}$

$= (u^2)^k = (649 + 180\sqrt{13})^k$

$|x^2 - 13y^2| = 1 \iff \pm x \pm y\sqrt{13} = u^k$.

Grand Finale:

"Number Theory is Hard"

As I understand it, the problem of number theory is to solve (systems of) Diophantine equations

$$f(x_1, \cdots, x_n) = 0,$$

i.e., $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1, \cdots, x_n]$

and we want solutions

$$x_1, x_2, \cdots, x_n \in \mathbb{Z}, \mathbb{Q}, \mathbb{Z}/m\mathbb{Z}$$

Linear Equations:

$$ax + by = c.$$

This led us to $\gcd(a,b)$ & the Euclidean Algorithm.

$$A\vec{x} = \vec{b}$$

System of linear equations can be solved via Smith Normal Form

$$PAQ = D$$

Can also be used to solve systems of linear congruences:

$$\begin{cases} ax + by \equiv c \mod m \\ dx + ey \equiv f \mod n. \end{cases}$$

$$\begin{cases} ax + by + mk = c \\ dx + ey + nl = f \end{cases}$$

2 equations & 4 unknowns x, y, k, l.

However the C.R.T. is nicer & has more theoretical applications.

Nonlinear Equations:

Now there are many different questions.

- solutions in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/n\mathbb{Z}$ have different behavior.
- # variables is important.
- We will only consider
  2 $\mathbb{Q}$-variables or 3 $\mathbb{Z}$-variables

from now on, because anything beyond that is completely impossible.

Also we will mostly restrict ourselves to degree 2.

Quadratic Equations:

Example:

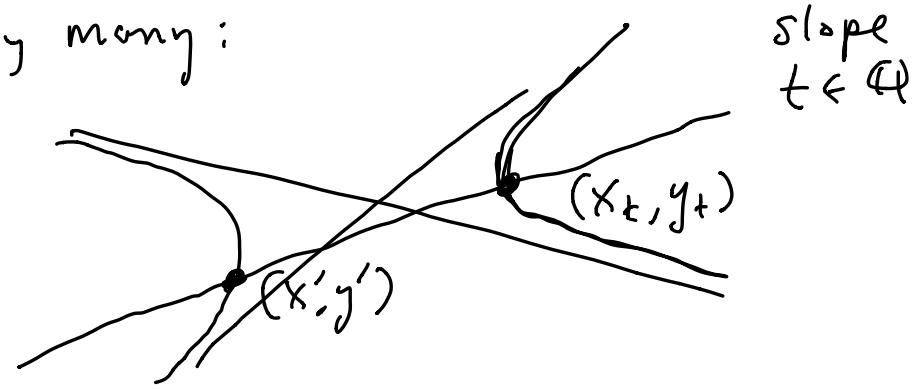
primitive $\mathbb{Z}$-solutions $\longleftrightarrow$ $\mathbb{Q}$-solutions of

$x^2+y^2=z^2$ (homogeneous)

$x^2+y^2=1$ (non-homogeneous)

Let $f(x,y) \in \mathbb{Z}[x,y]$ have degree 2.

If $f(x,y)=0$ has one rational solution $x', y' \in \mathbb{Q}$, then it has infinitely many:



Get almost-bijection

$\mathbb{Q} \longleftrightarrow$ rational points on $f(x,y) = 0$

$t \qquad\qquad (x_t, y_t)$

But how can we tell if a rational point exists?

Legendre: First translate coordinates to "complete the squares" and "rotate" to eliminate the xy term:

$$ax^2 + by^2 + c = 0 \quad (a,b,c \in \mathbb{Z})$$
$$[ax^2 + by^2 + cz^2 = 0]$$

Has $\mathbb{Q}$ solution (x,y)
or $\mathbb{Z}$ solution (x,y,z)

if and only if
$$\begin{cases} -ab = \square \bmod c \\ -ac = \square \bmod b \\ -bc = \square \bmod a. \end{cases}$$

Furthermore, if a solution exists then a "small" solution exists and you can find it by brute force.

This leads us to consider quadratic congruences in one variable:

$$ax^2 + bx + c \equiv 0 \mod n$$
with $\gcd(a, n) = 1$.

Enough to solve

$$ax^2 + bx + c \equiv 0 \mod p^k$$

for all primary factors $p^k \| n$, then stitch them together with C.R.T.

Furthermore, this problem reduces to

$$ax^2 + bx + c \equiv 0 \mod p.$$

Quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2}$$ Does this Exist?

i.e., is b^2-4ac square mod p?

Everything comes down to the equation

$$d = x^2 \bmod p,$$

which is solved by Quadratic Reciprocity.

This completes the story of rational points on conic sections.

Next: Integer Points.

$f(x,y) \in \mathbb{Z}[x,y]$ of degree 2.

It is harder to "change coordinates" while preserving integer solutions. However, the equation $f(x,y) = 0$ can be broken into special cases, the hardest of which are Pell-type

equations:

$$x^2 - dy^2 = n$$

I will tell you the complete solution.

Let $u_+ = p + q\sqrt{d}$ be the smallest solution > 1 to $p^2 - dq^2 = +1$, which can be computed via continued fraction expansion of $\sqrt{d}$.

Theorem: Every solution $x^2 - dy^2 = n$ has the form

$$x + y\sqrt{d} = (x' + y'\sqrt{d})\, u_+^k$$

where x', y' is some solution $x'^2 - dy'^2 = n$ satisfying

$$|x'| \leq \sqrt{|n| u_+}, \quad |y'| \leq \sqrt{|n| u_+}/\sqrt{d}.$$

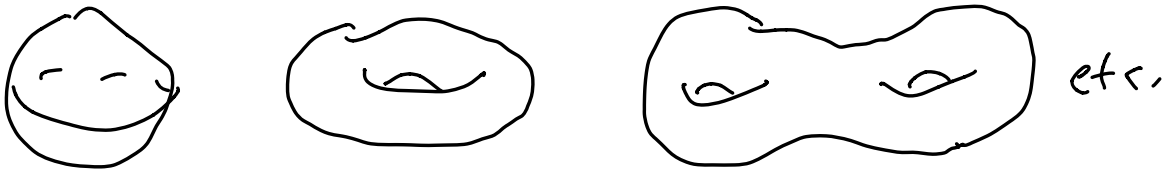
There are a finite number of such pairs (x', y'). (Brute force search.)

This completes the story of integer points on conic sections.

Where next?

Given $f(x,y) \in \mathbb{Q}[x,y]$ there is an integer $g \geq 0$ called the "genus" of the equation/curve $f(x,y) = 0$.
It is tricky to compute, but has an intuitive meaning:
Complex solutions $(x,y) \in \mathbb{C}^2$ to $f(x,y) = 0$. These form a "complex 1D curve in complex 2D plane."
In terms of <u>real</u> numbers we can think of it as a "real 2D surface living in real 4D space."

2D surfaces are classified by the number of donut holes:



$g=0$ $g=1$ $g=2$

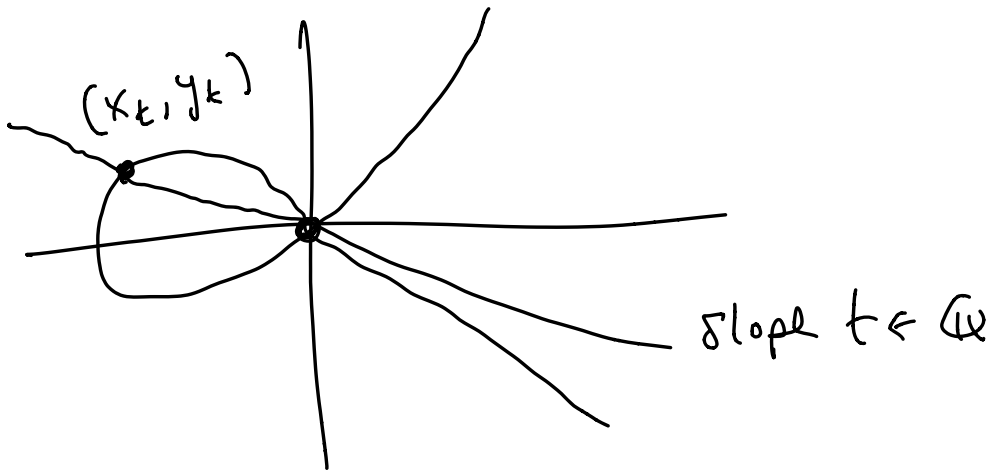
It is amazing that this number g strongly influences the $\mathbb{Q}$ solutions & $\mathbb{Z}$ solutions of $f(x,y)=0$.

TRICHOTOMY

$g=0$	$g=1$	$g \geq 2$
rational points on $f(x,y)=0$ $\Leftrightarrow$ $\mathbb{Q}$	sweet spot "elliptic curves"	Faltings' Theorem says there are at most finitely many rational points.

$g=0$: Behaves just like rational points on conic sections.

e.g. $y^2 = x^2(x+1)$



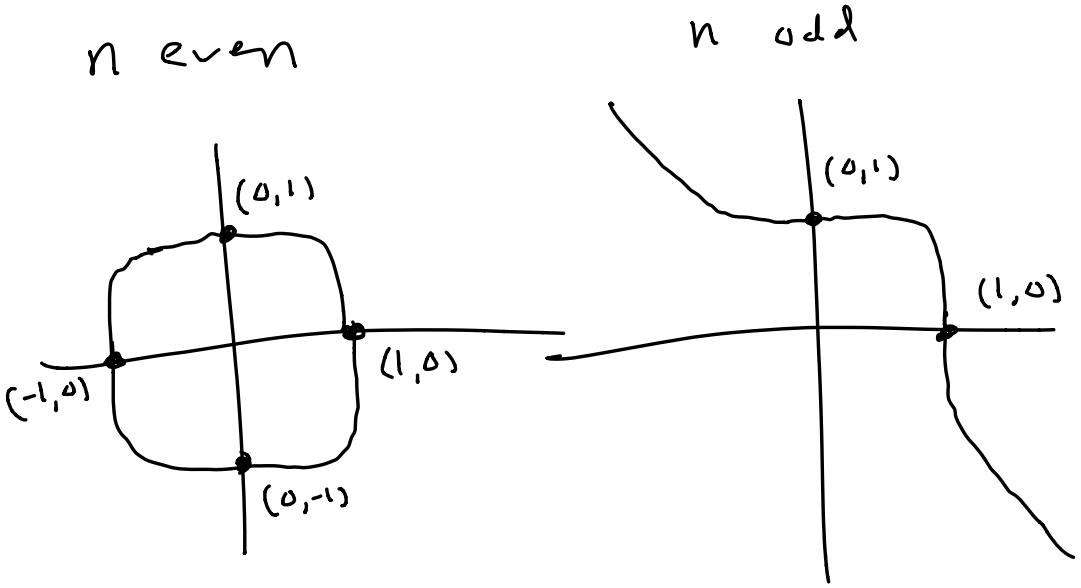
For any $t \in \mathbb{Q}$ there is a unique rational point $(x_t, y_t) \in \mathbb{Q}^2$ on the curve.

$g \geq 2$: Finitely many rational points.

The only interesting question is to count them. Sadly, this is impossible.

Thm (Matjasevic, Robinson, ...)
There is no algorithm to determine if # rational points $= 0$. ||

Example: Wiles (1994) proved that the curve $x^n + y^n = 1$ $(n \geq 3)$ has no rational points except for $(\pm 1, 0)$ & $(0, \pm 1)$.



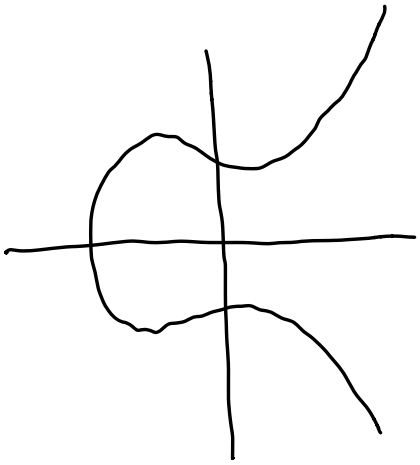
The proof was very hard.

$g = 1$: Called "Elliptic curves"

Canonical coordinates:

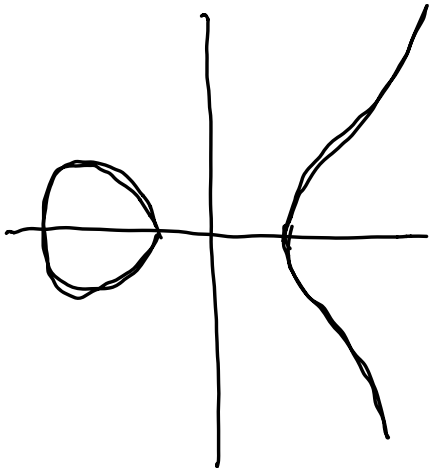
$y^2 = f(x)$ where $f(x) \in \mathbb{Q}[x]$ has degree 3 and distinct roots.

Two cases:



When $f(x)$ has

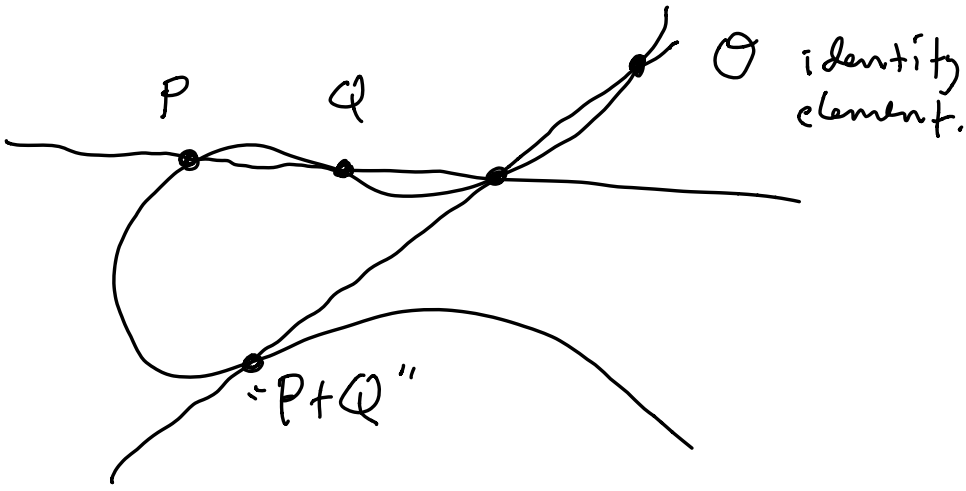
1 real
2 complex roots



When $f(x)$ has

3 real roots.

Rational points on an elliptic curve have the structure of an abelian group.



There are many open questions about this group. One could teach a whole course about it!

See "Rational Points on Elliptic Curves" by Silverman & Tate.