Lecture 24
Rational Points on Conics

Rational points on conics

(Definition) Conic: A **conic** is a plane curve cut by a polynomial of total degree 2

$$ax^2 + by^2 + cxy + dx + ey + f = 0$$

We usually want $a \dots f$ to be in $\mathbb{Q}$ or even in $\mathbb{Z}$. (Called ”conic” because plane sections of a cone - interested in smooth conics.)

Principle - if we can find one (rational) point on a sonic, then we can parametrize all rational points, and there are infinitely many of them. Method: slope method.

Eg. $x^2 + y^2 = 5$, $(1, 2)$ is a trivial point. Take (x, y), slope between the two is $m = \frac{y-2}{x-1} \Rightarrow y = 2 + m(x - 1)$. Plug into $x^2 + y^2 = 5$

$$\begin{aligned}
x^2 + y^2 = 5 &\Rightarrow x^2 = (1 + m(x-1))^2 = 5 \\
&\Rightarrow x^2 + 4 + 4m(x-1) + m^2(x-1)^2 = 5 \\
&\Rightarrow 4m(x-1) + m^2(x-1)^2 = 1 - x^2 = (1-x)(1+x) \\
&\Rightarrow 4m + m^2(x-1) = -(1+x)
\end{aligned}$$

Linear in x so solve for x in terms of m, then plug into $y = 2 + m(x - 1)$ to get both x, y in terms of m

How to tell if there are any rational points on conic (C) (doesn't always have rational points - eg., $x^2 + y^2 + 1 = 0$)

$$ax^2 + by^2 + cxy + dx + ey + f = 0$$

Can make a few reductions.

Reduction 1 - homogenization: Replace x with $\frac{x}{z}$, y with $\frac{y}{z}$, resulting in equation (H)

$$ax^2 + by^2 + cxy + dxz + eyz + fz^2 = 0$$

Theorem 84. *(C) has a rational point if and only if (H) has a non-trivial integer (x, y, z) solution with x, y, z not all 0*

Proof - C to H. If (C) has a rational point, can produce $x, y, z \in \mathbb{Z}$ with solution of (H) with $z \neq 0$, so non-trivial □

Proof - H to C. If (H) has a nontrivial solution, then one of x, y, z must be nonzero. If $z \neq 0$ then done. If $z = 0$, say wlog $x \neq 0$. Then divide out by x^2 to see there's a rational point on new conic (C') given by

$$a + by^2 + cy + dz + eyz + fz^2 = 0$$

But then, there are infinitely many, by the slope parametrization. At least one of them will have $z \neq 0$ (at most 2 solutions with $z = 0$). ie., call this solution $(\frac{y}{x}, \frac{z}{x})$ of (C'). This implies that (x, y, z) satisfies (H) with $z \neq 0$. ■

Reduction 1.5: (H) has a nontrivial integer solution if and only if it has a nontrivial rational solution ($\mathbb{Z} \subset \mathbb{Q}$, find common denominator of rationals to produce ints)

Reduction 2: complete squares and diagonalize

$$\begin{aligned}
&ax^2 + by^2 + cz^2 + dxy + eyz + fxz \\
&= a\left(\underbrace{x + \frac{d}{2a}y + \frac{e}{2a}z}_{x'}\right)^2 + (\dots)y^2 + (\dots)yz + (\dots)z^2 \\
&= ax'^2 + (\dots)y^2 + (\dots)yz + (\dots)z^2 \\
&= ax'^2 + (\dots)(y + (\dots)z)^2 + (\dots)z^2 \\
&= ax'^2 + b'y'^2 + c'z^2 = 0 \quad (H')
\end{aligned}$$

Point is - if (x, y, z) is rational non-trivial solution, then we get a non-trivial rational solution to (H'). Conversely if (H') has a nontrivial rational solution, so does (H). End result - we've produced a degree 2 homogenous equation which has only x^2, y^2, z^2 terms, where a nontrivial solution solution means that the original does as well.

So from now on assume $(H) = ax^2 + by^2 + cz^2 = 0$.

Reduction 3: assume a, b, c integers (by removing common denominators). Assume that they are nonzero integers (equivalent to saying we have a smooth conic), since it's easy to solve when one of a, b, c is zero. We can assume a, b, c are squarefree and that $\gcd(a, b, c) = 1$. Can go further - claim that we can arrange so that a, b, c are coprime in pairs, if and only if abc is squarefree.

Why? If $p | a, b, p \nmid c$, then replace z' by pz', set $a = pa'$ and $b = pb'$, so $pa'x^2 + pb'y^2 + c(pz')^2 = 0$, iff $a'x^2 + b'y^2 + pcz'^2 = 0$ gets rid of common factor p of a, b. Keep doing this as long as a, b, c are not coprime in pairs. Terminates as at each stage, product decreases (from $p^2a'b'c$ to $pa'b'c$).

End result: $ax^2 + by^2 + cz^2 = 0$, with $abc \neq 0, \in \mathbb{Z}$, and squarefree

Theorem 85 (Legendre Theorem)**.** *Let a, b, c be nonzero integers such that abc is squarefree. Then $ax^2 + by^2 + cz^2 = 0$ has a nontrivial integer/rational (global) solution* *if and only if both these conditions are satisfied: (1) a, b, c don't all have the same sign, and (2) $-ab$ is square mod c, $-bc$ is square mod a, and $-ac$ is square mod b. (1, 2 called local conditions - easy to check if given an equation)*

Proof - Necessity. If a, b, c have the same sign, then no real solution since x^2, y^2, z^2 are all ≥ 0, and $ax^2 + by^2 + cz^2 = 0$ only if trivial solution.

Let p be a prime dividing a. We'll show that $-bc$ is a square mod p (make assumption that there is a nontrivial integer solution to $ax^2 + by^2 + cz^2 = 0$). Let (x, y, z) be nontrivial integer solution. Can get rid of common factors, so $\gcd(x, y, z) = 1$. Then claim that x, y, z are coprime in pairs. Suppose not $\Rightarrow$ say, l divides x, y but not z. $ax^2 + by^2$ is divisible by $l^2 \Rightarrow l^2$ divides $-cz^2 \Rightarrow$ since c is squarefree, forces $l|z$ so $\gcd(y, z) = 1$. Reduce $ax^2 + by^2 + cz^2 = 0 \mod p$ to $by^2 + cz^2 \equiv 0 \mod p$. We know p cannot divide both y and z, so let's say wlog that $p \nmid y$.

$$\begin{aligned}
&\Rightarrow by^2 \equiv -cz^2 \mod p \\
&\Rightarrow b \equiv -\frac{cz^2}{y^2} \mod p \\
&\Rightarrow -bc \equiv (-c)\left(\frac{-cz^2}{y^2}\right) \equiv \left(\frac{cz}{y}\right)^2 \mod p
\end{aligned}$$

So $-bc \equiv \square \mod p \Rightarrow -bc \equiv 0 \mod a$ by CRT. Others by symmetry. $\square$

Proof - Sufficiency. Let's assume (by negating all of a, b, c if necessary) that $a > 0, b, c < 0$. Assume not in the case $a = 1, b, c, = -1$ because $x^2 - y^2 - z^2 = 0$ obviously has nontrivial solutions (such as $(1, 1, 0)$). Since $-bc$ is a square mod a, say $-bc \equiv k^2 \mod a$. So look at polynomial congruence.

$$\begin{aligned}
ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \mod a \\
&\equiv b\left(y^2 + \frac{c}{b}z^2\right) \mod a \\
&\equiv b\left(y^2 - \frac{k^2}{b^2}z^2\right) \mod a \\
&\equiv b\left(y + \frac{k}{b}z\right)\left(y - \frac{k}{b}z\right) \mod a
\end{aligned}$$

Point is that factors into linear factors mod a, similarly with mod b and mod c. Write

$$\begin{aligned}
ax^2 + by^2 + cz^2 &\equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\rho_1 x + \sigma_1 y + \tau_1 z) \mod a \\
&\equiv (\alpha_2 x + \beta_2 y + \gamma_2 z)(\rho_2 x + \sigma_2 y + \tau_2 z) \mod b \\
&\equiv (\alpha_3 x + \beta_3 y + \gamma_3 z)(\rho_3 x + \sigma_3 y + \tau_3 z) \mod c
\end{aligned}$$

by CRT choose $\alpha \equiv \alpha_1 \mod a \equiv \alpha_2 \mod b \equiv \alpha_3 \mod c$, and similarly $\beta, \gamma, \rho, \sigma, \tau$ to get

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\rho x + \sigma y + \tau z) \mod (abc)$$

Consider all the integer points in box $0 \le x < \sqrt{|bc|}$, $0 \le y < \sqrt{|ca|}$, $0 \le z < \sqrt{|ab|}$. (Note - not all square roots are integers.) The number of possible x is $\sqrt{|bc|}$ if $|bc|$ is integer, or $\lfloor \sqrt{|bc|} \rfloor + 1 > \sqrt{|bc|}$ if not.

So, the number of integer points in box is $> \sqrt{|bc|}\sqrt{|ab|}\sqrt{|ac|} = |abc| = abc$. But abc is the number of residue classes mod (abc), so there are 2 points (x_1, y_1, z_1) and (x_2, y_2, z_2) in box such that

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \mod (abc)$$

With this, $x = x_1 - x_2, y = y_1 - y_2, z = z_1 - z_2$ gives integer point not $(0, 0, 0)$ such that $\alpha x + \beta y + \gamma z \equiv 0 \mod (abc)$, and so

$$ax^2 + by^2 + cz^2 \equiv (\underbrace{\alpha x + \beta y + \gamma z}_{\equiv 0})(\rho x + \sigma y + \tau z) \equiv 0 \mod (abc)$$

Also,

$$\begin{aligned} |x| &< \sqrt{|bc|} \\ |y| &< \sqrt{|ca|} \\ |z| &< \sqrt{|ab|} \end{aligned}$$

so

$$\begin{aligned} ax^2 + by^2 + cz^2 &\le ax^2 \\ &< abc \\ ax^2 + by^2 + cz^2 &\ge by^2 + cz^2 \\ &> -2abc \end{aligned}$$

and so

$$-2abc < \underbrace{ax^2 + by^2 + cz^2}_{\text{multiple of } abc} < abc$$

so $ax^2 + by^2 + cz^2$ is either 0 or $-abc$. If $-abc$, consider

$$\begin{aligned} x' &= xz - by \\ y' &= yz + ax \\ z' &= z^2 + ab \\ &\Rightarrow ax'^2 + by'^2 + cz'^2 = 0 \end{aligned}$$

If x', y', z' trivial, then $z' = 0 \Rightarrow z^2 = -ab \Rightarrow a = 1, b = -1$ (since a, b are coprime) $\Rightarrow$ conic is $x^2 - y^2 + cz^2$, which has nontrivial $(1, 1, 0)$ solution. $\blacksquare$