Math 445 Number Theory

December 1, 2004

We can now apply our geometric approach to more general polynomial equations, in particular to *cubic* equations. $f(x,y)$ has rational coefficients, and the line $y = mx+r$ meets $\mathcal{C}_f(\mathbb{R})$ in two rational solutions, then $p(x) = f(x, mx+r)$ is a cubic polynomial with rational coefficients and two rational roots, and so, as before, the third root is also rational, and gives a third rational point on $\mathcal{C}_f(\mathbb{R})$. But in this case there are three ways to find such lines:

(a): find two distinct rational points, and the line through them,
(b): find a double point (x_0, y_0) in $\mathcal{C}_f(\mathbb{R})$, then any line with rational slope through (x_0, y_0) will give $f(x, mx+r)$ has x_0 as a double root,
(c): find a rational point (x_0, y_0), then for the tangent line to the graph of $\mathcal{C}_f(\mathbb{R})$, $f(x, mx+r)$ has x_0 as a double root.

Taken in turn, these can in many cases find infinitely many rational points on a cubic curve.

For example, on the curve $x^3 + y^3 = 9$, starting from the point $(2,1)$, with $f(x,y) = x^3 + y^3 - 9$, we can compute $f_x(2,1) = 12, f_y(2,1) = 3$, and so the tangent line is $(12,3) \bullet (x-2, y-1) = 0$ so $y = 9-4x$, and so $x^3 + (9-4x)^3 - 9 = (x-2)^2(180-63x)$, giving a new solution $(20/7, -17/7)$. Repeatedly using their tangent lines, we can find further solutions.

A double point example: $f(x,y) = y^2 - x^3 + 2x^2 = 0$ has $f_x = -3x^2 + 4x$, $f_y = 2y$, and all three are 0 at $(0,0)$. If we look at the lines through $(0,0)$ with rational slope, $y = mx$, and solve $m^2x^2 - x^3 + 2x^2 = x^2((m^2+2) - x) =$ gives $x = m^2 + 2$ and $y = m^3 + 2m$.

Why do tangent lines $y = mx + b$ give double roots of $f(x, mx+b) = 0$ at the point of tangency? This is just a little (multivariate) calculus. If (a,b) is our rational point, then the equation for its tangent line is

$f_x(a,b)(x-a) + f_y(a,b)(y-b) = 0$, and so we wish to solve

$p(x) = f(x, -\dfrac{f_x(a,b)}{f_y(a,b)}(x-a) + b) = 0$, which has $p(a) = 0$ and

$p'(a) = f_x(a,b) + f_y(a,b)L'(a) = f_x(a,b) + f_y(a,b)(-\dfrac{f_x(a,b)}{f_y(a,b)}) = 0$, as desired.

Integer points on $\mathcal{C}_f(\mathbb{R})$, $f(x,y) = x^3+y^3-M$? $x^3+y^3 = M = (x+y)(x^2-xy+y^2) = AB$, then $|M| \geq |B| = |x^2 - xy + y^2| = (x - \frac{y}{2})^2 + \frac{3}{4}y^2 \geq \frac{3}{4}y^2$ so $|y| \leq \frac{2}{\sqrt{3}}\sqrt{|M|}$ (and, by symmetry, $|x| \leq \frac{2}{\sqrt{3}}\sqrt{|M|}$), so we can check for integer solutions, by hand.