Math 445 Number Theory

November 29, 2004

Equations of higher degree:

Our geometric approach to finding rational solutions to quadratic equations can be applied to higher degree equations as well. If $f(x,y)$ is a polynomial of two variables, with total degree d, we will use the notation $\mathcal{C}_f(\mathbb{R}) = \{(x,y) \in \mathbb{R}^2 : f(x,y) = 0\}$
Our goal is to find the rational points $(x, y \in \mathbb{Q})$ in $\mathcal{C}_f(\mathbb{R})$.

Since, as before, the line through two rational solutions has rational slope, we can try to search for rational solutions, given one solution, by looking at lines with rational slope. The most generic equation for a line is $ax + by + c = 0$, but we will typically think of it as $y = mx + r$. A point lying on a line L and on $\mathcal{C}_f(\mathbb{R})$ satisfies both $f(x,y) = 0$ and $y = mx + r$, so it satisfies $p(x) = f(x, mx + r) = 0$. Since this is a polynomial in x of degree at most d, it has at most d roots, unless it is identically 0. But if $p(x)$ is identically 0, then $y = mx + r$ implies $f(x,y) = 0$. So $L \subseteq \mathcal{C}_f(\mathbb{R})$. So we have:

Theorem: If $f(x,y)$ is a polynomial of degree d, and the line L intersects $\mathcal{C}_f(\mathbb{R})$ in more than d points, then $L \subseteq \mathcal{C}_f(\mathbb{R})$.

In fact, even more is true: using polynomial long division (thinking of $f(x,y)$ as a polynomial in y with coefficients being polynomials in x), if L, given by $ax+by+c = 0$ meets $\mathcal{C}_f(\mathbb{R})$ in more than d=degree(f) points, then $f(x,y) = (ax + by + c)k(x,y)$ for some polynomial k. And perhaps just as important for our purposes, if f has rational coefficients, and a, b, c are rational, then k has rational coefficients. The same is true if we have integer coefficients.

This can be further refined if we introduce the *multplicity* of a root of $f(x,y) = 0$. Building in analogy with the one variable case: $x = 1$ is a multiple root of $f(x) = x^3 - x^2 - x + 1$ means $(x-1)^2 | f(x)$ (in this case, $f(x) = (x-1)^2(x+1)$), which in turn means $f(1) = 0$ and $f'(1) = 0$. In the two-variable case, the multiplicity M of a solution (a,b) to $f(x,y) = 0$ is the largest M so that $(\frac{\partial}{\partial x})^i(\frac{\partial}{\partial y})^j f(a,b) = 0$ for all $i + j \leq M$. Then the count of roots of $f(x,y) = 0$ can include their multiplicity, and the result above is still true. A point on $\mathcal{C}_f(\mathbb{R})$ with multiplicity 1 is called *smooth*, a point with multiplicity 2 is a *double point*, etc. A point with multiplicity greater than 1 is called *singular*. If all points are smooth, then $\mathcal{C}_f(\mathbb{R})$ is called smooth.