Math 445 Number Theory

November 22, 2004

Rational points on curves:

The geometric process we have developed works for any equation $ax^2+by^2+cz^2=0$, i.e., $aX^2+bY^2+c=0$, for which we know a single rational solution (X_0, Y_0), to find all rational solutions to $aX^2+bY^2+c=0$ (and hence all integer solutions to $ax^2+by^2+cz^2=0$). Looking at lines with rational slope through our known solution, we can find its points of intersection with the ellipse/hyperbola $aX^2+bY^2+c=0$ by finding the roots of a quadratic equation

$aX^2+b(r(X-X_0)+y_0)^2+c=0$

with rational coefficients, for which we already know one root, X_0. The other root (which depends on the variable r) is then also rational.

For example, knowing that $2x^2+3y^2=5$ has solution $(x_0, y_0)=(1,1)$ we find, using the line $y=r(x-1)+1$ with rational slope r through $(1,1)$, that

$0=2x^2+3y^2-5=2x^2+3(rx-r+1)^2-5=2x^2+3(r^2x^2-2r^2x+2rx+r^2-2r+1)-5=(2+3r^2)x^2+(6r-6r^2)x+(3r^2-6r-2)=((x-1)((2+3r^2)x-(3r^2-6r-2))$, so $x=1$ or $x=\dfrac{3r^2-6r-2}{3r^2+2}$, giving $y=rx-r+1=r\dfrac{3r^2-6r-2}{3r^2+2}-r+1=-\dfrac{3r^2+4r-2}{3r^2+2}$. Setting $r=\dfrac{u}{v}$, we get, as before,

$2(3u^2-6uv-2v^2)^2+3(3u^2+4uv-2v^2)^2=5(3u^2+2v^2)$. For example, setting $u=11, v=4$, we have $2(67)^2+3(507)^2=5(395)^2$.

Or, starting from $2^2+5^2=29$, we find, after solving

$x^2+(r(x-2)+5)^2-29=0=(r^2+1)x^2+(10r-4r^2)x+(4r^2-20r-4)=(x-2)((r^2+1)-(2r^2-10r-2))$, that $x=\dfrac{2r^2-10r-2}{r^2+1}$ and $y=r(\dfrac{2r^2-10r-2}{r^2+1}-2)+5=-\dfrac{5r^2+4r-5}{r^2+1}$. So setting $r=\dfrac{u}{v}$, we get $(2u^2-10uv-2v^2)^2+(5u^2+4uv-5v^2)^2=29(u^2+v^2)^2$. This gives (after dividing these three terms by their common g.c.d., and then multplying by a common factor) all integer solutions to $x^2+y^2=29z^2$. For example, setting $u=11, v=28$, we have $(1754)^2+(4547)^2=29(905)^2$.

The hard part: finding the first solution! For the special situation $x^2+y^2=nz^2$, we know from a homework problem awhile back that if $X^2+Y^2=n$ has a rational solution, then it has an *integer* solution, which we can look for by an exhaustive search among $0\leq X, Y\leq\sqrt{n}$! Note that our newest result gives us a quick criterion to decide if $x^2+y^2=n$ has an integer solution, when n is square-free; we need $\left(\dfrac{-1}{n}\right)=1$. The interested reader can check that this really is equivalent to the (slightly more long-winded) answer we found before...