Math 445 Number Theory

November 19, 2004

Theorem: If abc is square-free, then $ax^2+by^2+cz^2=0$ has a (non-trfvial!) solution $x,y,z\in\mathbb{Z}\Leftrightarrow$ a,b,c do not all have the same sign, and each of the equations
$w^2\equiv -ab \pmod{c}, w^2\equiv -ac \pmod{b}, w^2\equiv -bc \pmod{a}$ have solutions.

($\Rightarrow$:) WOLOG x,y,z have no common factor. If $(c,x)>1$, then choosing some prime $p|c,x$ we have $p|-ax^2-cz^2=by^2$ but $p\not|b$, so $p|y$. Then $p^2|ax^2+by^2=-cz^2$, so either $p^2|c$ or $p|z$ (both contradictions) . so $(c,x)=1$. Choosing u so that $ux\equiv 1 \pmod{c}$ we have, mod c, $0\equiv(u^2b)(ax^2+by^2)=(ab)(ux)^2+(uby)^2\equiv ab+(uby)^2$, so $w^2=(uby)^2\equiv -ab$. A similar argument establishes the other two congruences.

So, for example, $35x^2+23y^2-6z^2=0$ has no integer solutions, because $35\cdot 23\cdot -6=-2\cdot 3\cdot 5\cdot 7\cdot 23$ is square-free and $w^2\equiv -23\cdot -6=138 \pmod{35}$ has no solutions, since $\left(\frac{138}{5}\right)=\left(\frac{3}{5}\right)=-1$, so $w^2\equiv 138 \pmod{5}$ has no solutions. On the other hand, $5x^2+7y^2=13z^2$ has integer solutions, since $\left(\frac{91}{5}\right)=\left(\frac{65}{7}\right)=\left(\frac{-35}{13}\right)=1$, as we can readily compute; they are, respectively, $\left(\frac{1}{5}\right)=1$, $\left(\frac{2}{7}\right)=(-1)^6=1$, and $\left(\frac{4}{13}\right)=\left(\frac{2}{13}\right)^2=1$.

And if abc is not square-free? If $d^2|$ one of a,b,c, say $d^2|a$, then we write $a=d^2a'$ and if $ax^2+by^2+cz^2=0$, then $a'(dx)^2+by^2+cz^2=0$ so $a'X^2+bY^2+cZ^2=0$ has a solution. Conversely, if $a'X^2+bY^2+cZ^2=0$, then $a'd^2X^2+bd^2Y^2+cd^2Z^2=0=aX^2+b(dY)^2+c(dZ)^2$, so $ax^2+by^2+cz^2=0$ has solution. So we can test for solutions to $ax^2+by^2+cz^2=0$ by checking $a'X^2+bY^2+cZ^2=0$, with $a'bc=abc/d^2<abc$. And if $d|$ two of a,b,c, say $d|a,b$, then $a=dA, b=dB$ and if $ax^2+by^2+cz^2=0$, then $Adx^2+Bdy^2+cz^2=0$ so $Ad^2x^2+Bd^2y^2+cdz^2=0=A(dx)^2+B(dy)^2+(cd)z^2=0$ with $AB(cd)=abc/d<abc$. Conversely, if $AX^2+BY^2+(cd)Z^2=0$, then $AdX^2+BdY^2+cd^2Z^2=0=aX^2+bY^2+c(dZ)^2=0$ so $ax^2+by^2+cz^2=0$ has a solution. So by induction, we can test whether $ax^2+by^2+cz^2=0$ has solutions by testing if some $a'x^2+b'y^2+c'z^2=0$, with $a'b'c'$ square-free, has solutions.

If we actually want to <u>find</u> the solutions, we can use an approach from geometry. We'll start by illustrating this with an equation we already know how to solve: $x^2+y^2-z^2=0$. If we write this as $\left(\frac{x}{z}\right)^2+\left(\frac{y}{z}\right)^2=1$, we find ourselves looking for *rational* solutions to $a^2+b^2=1$, i.e., rational points on the unit circle. The key idea is to look at how *lines* intersect the circle $x^2+y^2-1=0$. If we set $y=rx+s$ and plug in, we have a quadratic equation $x^2+(rx+s)^2-1=0$ in x, describing the x-coordinates of the points of intersection of line and circle. If we know one of these points (x_0,y_0), then $(x-x_0)|(x^2+(rx+s)^2-1)$, and so the <u>other</u> factor of $x^2+(rx+s)^2-1$ is also linear, and setting it equal to 0 gives the x-coordinate of the <u>other</u> point of intersection. But the <u>real</u> key idea is that if x_0,y_0 and r are all rational (i.e., we know a rational point on the circle, e.g., $(1,0)$) then the other point of intersection has rational coordinates, because that other linear factor has rational coefficients. Conversely, the slope of a line between points with rational coordinates is rational; this means that this process will find <u>all</u> rational points on the unit circle.

Putting this into practice, if we start with $(x_0,y_0)=(1,0)$, which is a solution to $x^2+y^2=1$, and look at the line through $(1,0)$ with rational slope r, having equation $y=r(x-1)=rx-r$, and plug in, we need to solve $x^2+r^2(x^2-2x+1)-1=0=(1+r^2)x^2-2r^2x+(r^2-1)=(x-1)((r^2+1)x-(r^2-1))$, so $x=1$ (our original solution) or $x=\frac{r^2-1}{r^2+1}$, which implies (by plugging into $y=rx-r$) that $y=\frac{2r}{r^2+1}$. If we write $r=\frac{u}{v}$ and simplify, we have $(x,y)=(\frac{u^2-v^2}{u^2+v^2},\frac{2uv}{u^2+v^2})$, giving solutions $(u^2-v^2,2uv,u^2+v^2)$ to $x^2+y^2=z^2$. Which are all of the Pythagorean triples, as we have seen before!