Math 445 Number Theory

November 17, 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.

($\Leftarrow$:) After possible renaming variables and taking negatives, we may assume that $a > 0$ and $b, c < 0$. Suppose $r^2 \equiv -ab \pmod{c}$ and $aA \equiv 1 \pmod{c}$. Then for any $x, y \in \mathbb{Z}$, mod c we have $ax^2 + by^2 + cz^2 \equiv ax^2 + by^2 \equiv aA(ax^2 + by^2) \equiv A(a^2x^2 + aby^2) = A(a^2x^2 - r^2y^2) = A(ax - ry)(ax + ry) \equiv (x - Ary + 0z)(ax + ry + 0z)$. Similarly, mod b (with $s^2 \equiv -ac$) we have $ax^2 + by^2 + cz^2 \equiv (x + 0y - Asz)(ax + 0y + sz)$ and, mod a (with $t^2 \equiv -bc$ and $bB \equiv 1$) we have $ax^2 + by^2 + cz^2 \equiv (0x + y - Btz)(0x + by + tz)$. Using the Chinese Remainder Theorem, we can solve $\alpha \underset{a}{\equiv} 1, \alpha \underset{b}{\equiv} 1, \alpha \underset{c}{\equiv} 0$, $\beta \underset{a}{\equiv} -A, \beta \underset{b}{\equiv} 0, \beta \underset{c}{\equiv} 1$, $\gamma \underset{a}{\equiv} 0, \gamma \underset{b}{\equiv} -As, \gamma \underset{c}{\equiv} -Bt$, $\delta \underset{a}{\equiv} a, \delta \underset{b}{\equiv} a, \delta \underset{c}{\equiv} 0$, $\epsilon \underset{a}{\equiv} r, \epsilon \underset{b}{\equiv} 0, \epsilon \underset{c}{\equiv} b$, and $\eta \underset{a}{\equiv} 0, \eta \underset{b}{\equiv} s, \eta \underset{c}{\equiv} t$. Then, mod abc , $ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\delta x + \epsilon y + \eta z)$. Then we need a

Lemma : If $\lambda, \mu, \nu \in \mathbb{R}$ and positive, with $\lambda\mu\nu = M \in \mathbb{Z}$, then for any $\alpha, \beta, \gamma \in \mathbb{Z}$, $\alpha x + \beta y + \gamma z \equiv 0 \pmod{M}$ has a solution with $x, y, z \in \mathbb{Z}$, $(x, y, z) \neq (0, 0, 0)$, and $|x| \leq \lfloor\lambda\rfloor, |y| \leq \lfloor\mu\rfloor, |z| \leq \lfloor\nu\rfloor$.

The proof is simply that, among $0 \leq x \leq \lfloor\lambda\rfloor, 0 \leq y \leq \lfloor\mu\rfloor, 0 \leq z \leq \lfloor\nu\rfloor$, we have $(1 + \lfloor\lambda\rfloor)(1 + \lfloor\mu\rfloor)(1 + \lfloor\nu\rfloor) > \lambda\mu\nu = M$ triples (x, y, z) to choose from, so $\alpha x + \beta y + \gamma z \equiv \alpha x_1 + \beta y_1 + \gamma z_1$ for some pair of triples, and so $\alpha(x - x_1) + \beta(y - y_1) + \gamma(z - z_1) \equiv 0$.

Setting $\lambda = \sqrt{bc}, \mu = \sqrt{-ac}, \nu = \sqrt{-ab}$, we then can solve $\alpha x + \beta y + \gamma z \equiv 0 \pmod{abc}$ (so $ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}$) with $|x| \leq \sqrt{bc}, |y| \leq \sqrt{-ac}, |z| \leq \sqrt{-ab}$. But since abc is square-free, none of these square roots are integers (unless they are 1). So $x^2 \leq bc, y^2 \leq -ac, z^2 \leq -bc$, and equality occurs for any only if the corresponding right-hand side is 1.

Then, unless $b = c = -1$, we have $x^2 < bc$ and $abc | ax^2 + by^2 + cz^2$ with $ax^2 + by^2 + cz^2 \leq ax^2 < abc$ and $ax^2 + by^2 + cz^2 \geq by^2 + cz^2 > b(-ac) + c(-ab) = -2abc$. [The last inequality is reversed, since $b, c < 0$. It is strict, unless $a = 1$ as well.] So $ax^2 + by^2 + cz^2 = 0$ or $= -abc$. In the first case we are done; in the second, setting $X = -by + xz, Y = ax + yz, Z = z^2 + ab$ we have $aX^2 + bY^2 + cZ^2 = a(-by + xz)^2 + b(ax + yz)^2 + c(z^2 + ab)^2 = (ab^2y^2 - 2abxyz + ax^2z^2) + (a^2bx^2 + 2abxyz + by^2z^2) + (cz^4 + 2abcz^2 + a^2b^2c) = (ax^2 + by^2 + cz^2)z^2 + ab^2y^2 + a^2bx^2 + 2abcz^2 + a^2b^2c = -abcz^2 + ab^2y^2 + 2abcz^2 + a^2bx^2 + a^2b^2c = ab(ax^2 + by^2 + cz^2) + a^2b^2c = (ab)(-abc) + (ab)(abc) = 0$. This gives a non-trivial solution, unless $0 = -by + xz, 0 = ax + yz, 0 = z^2 + ab$, so $z^2 = -ab$, so $a = 1, b = -1$ since ab is square-free; and then $(x, y, z) = (1, 1, 0)$ is a solution.

Finally, in the special case $b = c = -1$, we have $w^2 \equiv -bc = -1 \pmod{a}$, has a solution, so every prime factor p of a also has $w^2 \equiv -1 \pmod{p}$, so $p \equiv -1 \pmod{4}$ for every prime factor, so $y^2 + z^2 = a$ has a solution, so $(1, y, z)$ is a solution to $ax^2 + by^2 + cy^2 = ax^2 - y^2 - z^2 = 0$, as desired.