PROBLEM OF THE WEEK

Solution of Problem No. 4 (Fall 2002 Series)

Problem: Suppose x and y are rational numbers satisfying the equation $y^2 = x^3 + ax + b$, where a, b are integers. Show that there are integers r, s, t with s, r and t, r relatively prime such that $x = \dfrac{s}{r^2}$, $y = \dfrac{t}{r^3}$.

Solution (by Jason Andersson, Fr. Math)

x and y are rational, so write $x = \dfrac{s}{p}$ and $y = \dfrac{t}{q}$ where $GCD(s,p) = GCD(t,q) = 1$. Also may assume $p > 0$, $q > 0$. Then $t^2p^3 = s^3q^2 + asp^2q^2 + bp^3q^2$. All numbers here are integers. q^2 divides the right hand side, so q^2 must also divide t^2p^3. Since $GCD(t,q) = 1$, $q^2|p^3$. Similarly, p^3 must divide $s^3q^2 + asp^2q^2 = (s^3 + asp^2)q^2$. $GCD(s^3 + asp^2, p) = 1$, since if the prime u divides both $s^3 + asp^2$ and p, then u divides p^2 and so u divides s^3 and hence s, which contradicts the fact that $GCD(s,p) = 1$. Consequently, p^3 divides q^2.

Thus the numbers p^3 and q^2 divide each other and therefore $p^3 = q^2$. Suppose there is a prime r which occurs an odd number of times in the prime factorization of p. Then r divides p^3 an odd number of times and so it divides q^2 an odd number of times. But this is impossible. Hence every prime divides p an even number of times, and it is deduced that $p = r^2$ for some integer r. Then $q^2 = p^3 = r^6$, so $q = r^3$, which proves the assertion.

Also solved by:

Undergraduates: Ryan Machtmes (Sr. E&AS), Eric Tkaczyk (Sr. MA/EE)

Graduates: Chris Lomont (MA)

Faculty: Steven Landy (Physics at IUPUI)

Others: Jonathan Landy (Fr., Cal Tech), Dharmashankar Subramanian (Honeywell Labs, Minneapolis, MN) jointly with Prasenjeet Ghosh (Exxonmobil Research, New Jersey)

Four unacceptable solutions were received.

Three late solutions of problem 3 were received, two incorrect and one incomplete.