Singapore International Mathematical Olympiad
Training Problems

08 March 2003

1. Let p be a prime number congruent to 1 modulo 4. Define the set

$$S = \{(a,b,c) \in \mathbf{N}^2 \times (\mathbf{Z} - \{0\}), 4ab + c^2 = p\}.$$

Now consider

$$S_1 = \{(a,b,c) \in S, a > b + c\}.$$

Assume that $|S_1|$ is odd. Show that p can be expressed as a sum of two squares.

2. Prove that the circle with equation $x^2 + y^2 = 1$ contains an infinite number of points with rational coordinates such that the distance between each pair of the points is irrational.

3. Let $f : \mathbf{R} \to \mathbf{R}$ be a function such that

(a) $f(2x) = 2\,[f(x)]^2 - 1$, for all $x \in \mathbf{R}$;

(b) There exists a real number x_0 such that $f(2^n x_0) \leq 0$ for all natural numbers n.

Determine the value of $f(x_0)$.

Solutions

1. S is non empty since $(k,1,1) \in S$ and $|S|$ is also finite since if $(a,b,c) \in S$, $a, b, |c|$ are all bounded by p. Now consider

$$S_1 = \{(a,b,c) \in S, a > b + c\} \qquad S_2 = \{(a,b,c) \in S, a < b + c\}.$$

Then S_1 and S_2 are clearly disjoint, and if $a = b + c$, we have $p = 4b(b+c) + c^2 = (c+2b)^2$, which is a contradiction. Hence S is the disjoint union of S_1 and S_2. Consider now $(a,b,c) \to (b,a,-c)$. This is a bijection from S_1 to S_2. Hence $|S_1| = |S_2|$.
Since $|S_1|$ is odd, we have $|S| \equiv 2 \pmod 4$. Now consider

$$S_3 = \{(a,b,c) \in S, a \neq b\}.$$

Then for all $(a,b,c) \in S$, with $a \neq b$, we can associate 4 distinct triplets

$$(a,b,c), (a,b,-c), (b,a,c), (b,a,-c)$$

in S. Hence $|S_3|$ is divisible by 4. This shows that $S_3 \subset S$ (strict inclusion). Hence there exists a triplet $(a,a,c) \in S$. Thus $p = 4a^2 + c^2 = (2a)^2 + c^2$, as required. Note that the assumption that $|S_1|$ is odd can be proven. (As Andre pointed out, consider the map f which maps $(a,b,c) \to (a-b-c, b, -2b-c)$ from S_1 to itself. $f^2 = \mathrm{Id}$, and we can check that a 'fixed point' is $(\frac{p-1}{4}, 1, -1)$. A pairing up will give you the result.)

2. Let p be a prime and $p \equiv 1 \pmod 4$. Then there exists integers a and b such that $p = a^2 + b^2$, and by Dirichlet's Theorem, there exists infinitely primes of the form $4k+1$, thus consider the set of points given by

$$\mathbf{x_p} = \left(\frac{a^2 - b^2}{p}, \frac{2ab}{p}\right)$$

All these points lie on the unit circle, and are irreducible fractions. If $p \neq q$, we have

$$||\mathbf{x_p x_q}|| = \frac{2|ad - bc|}{\sqrt{pq}}$$

and since $p \neq q$ are primes, the above fraction is irrational and we are done.

3. Note that if $f(x_0)$ is a solution, $-f(x_0)$ is also a solution. It is clear that $f(x_0) \neq 0$. So assume WLOG $f(x_0) = p < 0$. Then we have $f(2^{n-1}x_0) = 2\left[f(2^{n-2}x_0)\right]^2 - 1 \geq -1$, and thus $-1 \leq f(2^{n-1}x_0) < 0$ for all natural numbers n. Now we obtain a better upper bound. We claim that we have $-1 \leq f(2^{n-1}x_0) \leq -\frac{1}{4}$. Suppose that there exists a natural number m such that $0 > f(2^{m-1}x_0) > -\frac{1}{4}$. Then we have $-1 \leq f(2^m x_0) < -\frac{7}{8}$, and hence $1 > f(2^{m+1}x_0) > \frac{17}{32} > 0$, a contradiction. Now from the given functional, we have

$$f(2x) + \frac{1}{2} = 2\left(f(x) - \frac{1}{2}\right)\left(f(x) + \frac{1}{2}\right),$$

and hence for all natural numbers n, we have

$$\left|f(2^n x_0) + \frac{1}{2}\right| = 2\left|f(2^{n-1}x_0) - \frac{1}{2}\right|\left|f(2^{n-1}x_0) + \frac{1}{2}\right| \geq 2\left(\frac{1}{2} + \frac{1}{4}\right)\left|f(2^{n-1}x_0) + \frac{1}{2}\right|,$$

or equivalently

$$\left|f(2^{n-1}x_0) + \frac{1}{2}\right| \leq \frac{2}{3}\left|f(2^n x_0) + \frac{1}{2}\right|.$$

Hence we have

$$\left|f(x_0) + \frac{1}{2}\right| \leq \frac{2}{3}\left|f(2x_0) + \frac{1}{2}\right| \leq \ldots \leq \left(\frac{2}{3}\right)^{n+1}\left|f(2^{n+1}x_0) + \frac{1}{2}\right| \leq \left(\frac{2}{3}\right)^{n+1}\left(1 + \frac{1}{2}\right) \leq \left(\frac{2}{3}\right)^n,$$

and letting $n \to \infty$, we have

$$\left|f(x_0) + \frac{1}{2}\right| \to 0,$$

and thus $f(x_0) = -\frac{1}{2}$. Hence we have $f(x_0) = \pm\frac{1}{2}$.