Singapore International Mathematical Olympiad
Training Problems

15 February 2003

1. Let n be an odd integer which is not a multiple of 5. Prove that there exists a strictly positive integer k such that n divides a string of k 1's, i.e.

$$n|\underbrace{11...11}_{k\text{1's}}.$$

2. Determine all natural numbers (k, m, n) such that

$$n! = m^k.$$

3. Show that for all integers A, B, there exists an integer C such that the following sets $M_1 = \{x^2 + Ax + B : x \in \mathbf{Z}\}$ and $M_2 = \{2x^2 + 2x + C : x \in \mathbf{Z}\}$ are disjoint.

4. Let m be a strictly positive integer. Show that there exists infinitely many pairs of integers (x, y) such that
   (a) x, y are relatively prime
   (b) y divides $x^2 + m$
   (c) x divides $y^2 + m$
   (d) $x + y \geq m + 1$

5. Let m and k be positive integers such that $\gcd(m, k) = a$.
   (a) Suppose that $a = 1$. Show that there exists integers $a_1, a_2, ..., a_m$ and $b_1, b_2, ..., b_k$ such that each of the products a_ib_j $(i = 1, 2, ..., m, j = 1, 2, ..., k)$ gives a different remainder modulo mk.
   (b) Suppose that $a > 1$. Show that for all integers $a_1, a_2, ..., a_m$ and $b_1, b_2, ..., b_k$ there exists two products a_ib_j and a_sb_t $((i, j) \neq (s, t))$ such that they have the same remainder modulo mk.

6. Let n be a non negative integer. Suppose that there exists rational numbers p, q, r such that

$$n = p^2 + q^2 + r^2.$$

Prove that there exists integers a, b, c such that

$$n = a^2 + b^2 + c^2.$$

Solutions

1. From the given conditions $\gcd(n, 10) = 1$. But $\gcd(9, 10) = 1$ and hence $\gcd(9n, 10) = 1$. Thus by Euler's Theorem,
$$10^{\phi(9n)} \equiv 1 \pmod{9n},$$
which implies the desired result.

2. Using Bertrand's Postulate, there exists a prime p satisfying $\frac{n}{2} < p < n$ for all $n \geq 3$. Now note that $2p > n$, hence p only has a single power in $n!$, i.e. $k = 1$. Hence $(m, n, k) = (n!, n, 1)$ is a solution triplet. If $n = 2$, we have $2 = m^k$, hence we must have $m = 2, k = 1$. If $n = 1$, we must have $1 = m^k$, or $m = 1, k \in \aleph$ thus $(m, n, k) = (1, 1, k)$ is another solution triplet. Thus the only solutions to the equation are
$$(m, n, k) = (1, 1, k), (n!, n, 1), \qquad n, k \in \aleph.$$

3. If A is odd, $x^2 + Ax + B \equiv x(x + A) + B \equiv B \pmod 2$, but $2x^2 + 2x + C \equiv C \pmod 2$. So we may choose $C = B + 1$.
If A is even, $x^2 + Ax + B = (x + \frac{A}{2})^2 + B - \frac{A^2}{4} \equiv B - \frac{A^2}{4}$ or $B - \frac{A^2}{4} + 1 \pmod 4$, but $2x^2 + 2x + 1 \equiv C \pmod 4$, so we may choose $C = B - \frac{A^2}{4} + 2$ in this case.

4. Note that $(1, 1)$ satisfies the given conditions. Now if (x, y) is a solution with $y \geq x$, consider (x_1, y) where
$$y^2 + m = xx_1$$
All common divisors of x_1 and y must by the above a divisor of m, and since $y|x^2+xx_1-y^2$, we must have $y|x(x+x_1)$, and since $\gcd(x, y) = 1$, we must have $y|(x+x_1)$, and hence the common divisor of y and x_1 must divide x too, but $\gcd(x, y) = 1$, we have $\gcd(x_1, y) = 1$. It is clear that $x_1|y^2 + m$, and
$$x^2(x_1^2 + m) = (y^2 + m)^2 + x^2 m = y^4 + 2my^2 + m(x^2 + m),$$
but $y|(x^2 + m)$ implies that $y|x^2(x_1^2 + m)$, but $\gcd(x, y) = 1$ implies that $y|(x_1^2 + m)$. Now $x_1 > y \leq x$. Repeat the same argument to generate y_1, but instead consider
$$x_1^2 + m = yy_1.$$
Then (x_1, y_1) is also a solution, with $x_1 + y_1 > x + y$. Continue this process to generate (x_2, y_2),... and since m is fixed, $x_n + y_n \geq m + 1$ for some n, thus $(x_n, y_n), (x_{n+1}, y_{n+1}), \ldots$ is a set of infinitely many solution pairs which satisfies all given conditions.

5. (a) Consider $a_i = ki + 1$, $b_j = mj + 1$. Suppose that two of the residues are the same. Then mk divides $a_i b_j - a_s b_t = (ki + 1)(mj + 1) - (ks + 1)(mt + 1) = km(ij - st) + m(j - t) + k(i - s)$, and thus $m|k(i - s)$ but $\gcd(m, k) = 1$, hence $m|(i - s)$, and since $|i - s| < m$, we must have $i = s$ and similarly $j = t$ and we are done.

   (b) Suppose all the residues are distinct. Then 0 is one the residues. WLOG, suppose $mk|a_1 b_1$. Hence there exists a', b' such that $a'|a_1, b'|b_1$ and $mk = a'b'$. Suppose now that for $i \neq s$, $a'|(a_i - a_s)$. Then we have $mk = a'b'|(a_i b_1 - a_s b_1)$, which is a contradiction. Hence all the a_i's cannot have the same residue modulo a', similarly, all the b_j's cannot have the same residue modulo b'. Thus we must have $a' \geq m, b' \geq k$ thus $a' = m, b' = k$.
   Now let p be a prime divisor of m and k. $p > 1$ since $\gcd(m, k) > 1$. Since all the a_i's form a distinct set of residues modulo m, there are $m - \frac{m}{p}$ between them which are not divisible by p. Similarly, there are $k - \frac{k}{p}$ b_j's which are not divisible by p. On the other hand all the $a_i b_j$'s form a set of reduced residues modulo mk by our assumption, and hence between them, there are $mk - \frac{mk}{p}$ which are not divisible by p. But
$$\left(m - \frac{m}{p}\right)\left(k - \frac{k}{p}\right) = \left(mk - \frac{mk}{p}\right)$$
   if and only if $m = 0, k = 0$ or $p = 1$, which is a contradiction.

6. If $n = 0$, the result is clear. So suppose $n > 0$. Suppose the set of points (x_1, x_2, x_3) which lies on the sphere

$$n = x^2 + y^2 + z^2$$

are all rational points. We will obtain a contradiction. Now there exists an integer point $u = (u_1, u_2, ..., u_n)$ such that $ad = u$, where $d \geq 2$. Suppose that a and u are chosen such that d is minimal. Then let $x', y'z'$ be the integers closest to x, y, z, where $a = (x, y, z)$. Then $|x - x'| \leq \frac{1}{2}$, $|y - y'| \leq \frac{1}{2}$ and $|z - z'| \leq \frac{1}{2}$, hence $||a - a'|| < 1$, where $a' = (x', y', z')$. Now consider the line connecting a and a'. This will intersect the sphere $x^2 + y^2 + z^2 = n$ at two points, one at a and the other which we call b. The equation of the line is given by $a' + \lambda(a - a')$. Now b lies on the sphere so

$$n = ||b||^2 = ||a'||^2 + 2\lambda < a', a - a' > + \lambda^2 ||a - a'||^2.$$

One of the solutions to this equation is given by $\lambda = 1$, which correspond to the point a. The other thus is given by $\lambda = \frac{||a'||^2 - n}{||a - a'||^2}$. Now

$$||a - a'||^2 = ||a'||^2 + ||a||^2 - 2 < a', a >= ||a'||^2 + n - \frac{2}{d} < a', u >= \frac{d_1}{d},$$

where $d_1 \in \aleph$ and since $||a - a'||^2 < 1$ we have $d_1 < d$. Hence $\lambda = \frac{d(||a'||^2 - n)}{d_1}$ and we have

$$\begin{aligned} b &= a' + \lambda(a - a') \\ &= a' + \frac{||a'||^2 - n}{d_1}(u - da') \\ &= \frac{v}{d_1} \end{aligned}$$

where v is an integer point. Now $b = vd_1$ with $d_1 < d$ contradicts our assumption that d is minimal.
Note that a generalisation is not possible using this method since $||a - a'||^2 < 1$ will NOT be satisfied for higher dimension spaces. For a one dimensional space, i.e. the real line, this result is obvious. For a two dimensional space, i.e. the plane, this argument works.