New Zealand Mathematical Olympiad Committee

2011 Squad Assignment Three

Number Theory

Due: Monday 14th March 2011

1. *The two pairs of consecutive natural numbers* $(8, 9)$ *and* $(288, 289)$ *have the following property: in each pair, each number contains each of its prime factors to a power not less than 2. Prove that there are infinitely many such pairs of consecutive natural numbers.*

   Solution: Given a pair $(a, a+1)$ satisfying the conditions of the problem, we claim that $(4a(a+1), 4a(a+1)+1) = (4a(a+1), (2a+1)^2)$ does too. Indeed, any prime factor of $4a(a+1)$ must divide 4, a or $a+1$, and will divide this to a power not less than 2; and any prime factor of $(2a+1)^2$ must divide it to an even power, hence to a power at least 2. Since $4a(a+1) > a$, and we know there is at least one solution $(8, 9)$, this gives us an infinite sequence of solutions. $\square$

2. *Suppose that* N *is a positive integer such that there are exactly 2005 ordered pairs* (x, y) *of positive integers satisfying*

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{N}.$$

   Prove that N *is a perfect square.*

   Solution: The given equation is equivalent to $(x+y)N = xy$, which we may rewrite as

$$(x-N)(y-N) = N^2.$$

   Since x and y are positive we have $1/x < 1/x + 1/y = 1/N$, so $x > N$, and similarly for y. Therefore $x - N$, $y - N$ are both positive, and it follows that solutions to the given equation are in 1-1 correspondence with factorisations of N^2 as $N^2 = ab$.

   Let $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ be the prime factorisation of N, where we assume that $\alpha_i \geq 1$ for $1 \leq i \leq k$. Then N^2 has $\prod_{i=1}^{k}(2\alpha_i + 1)$ factors, so we must have

$$\prod_{i=1}^{k}(2\alpha_i + 1) = 2005 = 5 \times 401$$

   (note that 5 and 401 are both prime). Thus either $k = 1$ and $\alpha_1 = 1002$, or $k = 2$ and without loss of generality $\alpha_1 = 2$, $\alpha_2 = 200$. Thus either

$$N = p_1^{1002} = (p_1^{501})^2 \qquad \text{or} \qquad N = p_1^2 p_2^{200} = (p_1 p_2^{100})^2,$$

   and in either case N is square. $\square$

3. *Find all quadruples* (a, b, p, n) *of positive integers such that* p *is prime and*

$$a^3 + b^3 = p^n.$$

Solution: Suppose first that a and b have a common factor $d > 1$. Then $a = a'd$, $b = b'd$ for positive integers a', b', and

$$a^3 + b^3 = d^3(a'^3 + b'^3) = p^n,$$

so d must be a power of p. Writing $d = p^t$ we have

$$a'^3 + b'^3 = p^{n-3t},$$

and since $a'^3 + b'^3$ is a positive integer greater than 1 it must be the case that $n - 3t$ is positive. Thus, if a and b have a common factor, then $(a, b, p, n) = (p^t a', p^t b', p, m + 3t)$, where (a', b', p, m) is a solution with $\gcd(a', b') = 1$. Conversely, if (a, b, p, n) is a solution then so is $(p^t a, p^t b, p, n + 3t)$, so it suffices to find the solutions for which $\gcd(a, b) = 1$.

We therefore assume that $\gcd(a, b) = 1$. First note that we can factor the given equation as

$$(a + b)(a^2 - ab + b^2) = p^n,$$

and since a, b are positive integers, we have $a+b \geq 2$, so $p|(a+b)$. In addition, $a^2-ab+b^2 = (a-b)^2+ab$, so either $a = b = 1$, or $a^2-ab+b^2 \geq 2$. If $a^2-ab+b^2 \geq 2$ then p is a divisor of both $a + b$ and $a^2 - ab + b^2$, hence also of $(a + b)^2 - (a^2 - ab + b^2) = 3ab$. This means that either $p = 3$, or p is a divisor of ab. However, if $p|ab$ then either $p|a$ or $p|b$, and since also $p|(a + b)$, this implies p divides both a and b. This contradicts our assumption that a and b have no common factor, so either $a = b = 1$, or $p = 3$.

If $a = b = 1$ then we get the unique solution $(1, 1, 2, 1)$, so it remains to consider the case $p = 3$. In this case $a^2 - ab + b^2 \geq 2$, so we must have $a^2 - ab + b^2 = 3^s$ for some $s \geq 1$. We will show that our assumption that $\gcd(a, b) = 1$ forces $s = 1$. Indeed, suppose that $3^2|(a^2 - ab + b^2)$. Then, since $3|(a + b)$, we have that 3^2 divides $(a^2 - ab + b^2) - (a + b)^2 = 3ab$, so $3|ab$. But by the same argument as above this implies 3 divides both a and b, contradicting our assumption that $\gcd(a, b) = 1$. So under this assumption we must have $a^2 - ab + b^2 = 3$.

We now have $3 = a^2-ab+b^2 = (a-b)^2+ab$, so either $(a-b)^2 = 0$, $ab = 3$, or $(a-b)^2 = 1$, $ab = 2$. The former case has no solution, and in the latter we have either $a = 1, b = 2$ or $a = 2, b = 1$. So finally we have exactly three solutions with $\gcd(a, b) = 1$, namely $(1, 1, 2, 1)$, $(1, 2, 3, 2)$ and $(2, 1, 3, 2)$, and by the first paragraph all solutions are given by

- $(2^t, 2^t, 2, 3t + 1)$,
- $(3^t, 2 \cdot 3^t, 3, 3t + 2)$,
- $(2 \cdot 3^t, 3^t, 3, 3t + 2)$,

for t a non-negative integer. $\square$

4. *Does there exist a function $f:\mathbb{N}\to\mathbb{N}$ such that $f(f(n))=n^2$ for all values of n?*

Solution: Yes, such a function does exist, and there are many ways to construct one. Here are several ways to do it.

Construction 1. Let $p_1, p_2, p_3, \ldots$ be the sequence of prime numbers, and set $f(1)=1$, $f(p_{2k-1})=p_{2k}$, and $f(p_{2k})=p_{2k-1}^2$ for all $k\geq 1$. Furthermore, if n has prime factorisation

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots,$$

where $\alpha_i\geq 0$ for all i, we set

$$f(n)=f(p_1)^{\alpha_1}f(p_2)^{\alpha_2}\cdots.$$

Then

$$f(f(n))=f(p_2^{\alpha_1}p_1^{2\alpha_2}p_4^{\alpha_3}p_3^{2\alpha_4}\cdots)=p_1^{2\alpha_1}p_2^{2\alpha_2}\cdots=n^2$$

for every positive integer n, as required.

Construction 2. Let $a_1, a_2, a_3, \ldots$ be the sequence of numbers that are not square. Then each positive integer $n\geq 2$ may be written uniquely in the form $n=a_i^{2^k}$, and we define

$$f(1)=1, \qquad f(a_{2j-1}^{2^k})=a_{2j}^{2^k}, \qquad f(a_{2j}^{2^k})=a_{2j-1}^{2^{k+1}}.$$

It's straightforward to check that this works.

Construction 3. Each number may be written uniquely in the form $n=a^2+b$, where $0\leq b\leq 2a$ (here a is simply $\lfloor\sqrt{n}\rfloor$. Using this representation we define f for $n\geq 2$ by

$$f(n)=f(a^2+b)=\begin{cases} a^2+b+1 & \text{if } b \text{ is odd,}\\ (a^2+b-1)^2 & \text{if } b>0 \text{ is even,}\\ (f(a))^2 & \text{if } b=0\end{cases}$$

(of course we must have $f(1)=1$). This defines the same function as in the previous construction, but now we need to argue by induction that the function has been defined for all n (in particular, we need to check that it has been defined for fourth powers).

Construction 4. It suffices to construct a function $g:\mathbb{N}\cup\{0\}\to\mathbb{N}\cup\{0\}$ such that $g(g(n))=2n$ for all n, because then we may define f on prime factorisations by

$$f(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k})=p_1^{g(\alpha_1)}p_2^{g(\alpha_2)}\cdots p_k^{g(\alpha_k)}.$$

Clearly $g(0)$ must be 0. To define g for $n\geq 1$ we write each positive integer in the form $n=2^k\ell$, where ℓ is odd, and define

$$g(2^k(4m+1))=2^k(4m+3),$$
$$g(2^k(4m+3))=2^{k+1}(4m+1).$$

It's easy to check that this works.

$\square$

5. *Let*

$$f(n) = 1 + n + n^2 + \cdots + n^{2010}.$$

Prove that for every integer m with $2 \leq m \leq 2010$, there is no non-negative integer n such that $f(n)$ is divisible by m.

Solution: Assume that m divides $f(n)$ for some integer n and $2 \leq m \leq 2010$. As $f(1) = 2011$ and 2011 is a prime number, m cannot divide $f(1)$, so we may assume $n \neq 2$. In this case we can write $f(n)$ as

$$f(n) = \frac{n^{2011} - 1}{n - 1}.$$

Let p be a prime divisor of m. Then we have $p \mid f(n) \mid n^{2011} - 1$, which results in

$$n^{2011} \equiv 1 \bmod p.$$

This implies n and p are coprime.

Let k be the smallest positive exponent of n such that $n^k \equiv 1 \bmod p$, i.e. $k = \mathrm{ord}_p(n)$. As $n^{2011} \equiv 1 \bmod p$ we have k is a divisor of 2011. As 2011 is prime we have $k = 1$ or $k = 2011$.

If $k = 1$ then $n \equiv 1 \bmod p$ and by the original definition of $f(n)$ we obtain $0 \equiv f(n) \equiv 2011 \bmod p$. This implies that p divides 2011 and therefore $p = 2011$, which is a contradiction since $p < 2011$.

We conclude that $k = 2011$. By Fermat's theorem, k must divide $p - 1$, so $p - 1$ is a multiple of 2011 which is again a contradiction to $1 < p < 2011$. $\square$

6. *An integer m is a* perfect power *if there exist positive integers a and n with $n > 1$ such that $m = a^n$.*

   (a) *Prove that there exist 2011 distinct positive integers such that no subset of them sums to a perfect power.*

   (b) *Prove that there exist 2011 distinct positive integers such that every subset of them sums to a perfect power.*

Solution:

(a) We give three constructions.

Construction 1. Let p_i be the ith prime number, and consider the 2011 numbers

$$p_1,\ p_1^2 p_2,\ p_1^2 p_2^2 p_3,\ \ldots,\ p_1^2 p_2^2 \cdots p_{2010}^2 p_{2011}.$$

They are clearly all distinct, and if $p_1^2 \cdots p_k^2 p_{k+1}$ is the least number occurring in some subset of them, then the sum of this subset is divisible by p_{k+1} but not p_{k+1}^2. It cannot therefore be a perfect power.

Construction 2. Let p be a prime larger than $\sum_{k=1}^{2011} k = 2011 \cdot 1006$, and consider the set $A = \{kp : 1 \le k \le 2011\}$. The sum of any subset of A has the form mp for some $m \le \sum_{k=1}^{2011} k < p$, and so cannot be a perfect power.

Construction 3. If p is prime then the numbers $p!$, $(p+1)!$, $\dots$, $(2p-1)!$ each contain p as a prime factor with exponent 1, and so cannot be perfect powers. It follows that that there exist arbitrarily long intervals of consecutive numbers, none of which is a perfect power. Using this fact we may inductively construct the required set as follows.

Suppose that for some $n \ge 1$ we have an n-element set A_n of positive integers such that no subset-sum of A_n is a perfect power. Let $M = \max A_n$, and let S be the sum of the elements of A_n. By the paragraph above there exists a positive integer $N > M$ such that none of the numbers $N, N+1, \dots, N+S$ is a perfect power, and we let $A_{n+1} = A_n \cup \{N\}$. Then A_{n+1} contains $n+1$ distinct positive integers, and a subset-sum of A_{n+1} is either a subset-sum of A_n, N, or N plus a subset-sum of A_n, and in the last two cases it lies in the interval $[N, N+S]$, and so cannot be a perfect power. Letting A_1 equal say $\{2\}$ completes the induction.

(b) We first show that, given any integers $a_1, \dots, a_n$, there exists $b \in \mathbb{N}$ such that ba_i is a perfect power for each i. Again let p_i be the ith prime number, and write each a_i in the form
$$a_i = p_1^{\alpha_{i,1}} p_2^{\alpha_{i,2}} \cdots p_k^{\alpha_{i,k}},$$
where k is fixed and $\alpha_{i,j} \ge 0$ for all i, j. Similarly let
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}.$$
Then
$$ba_i = p_1^{\alpha_{i,1}+\beta_1} p_2^{\alpha_{i,2}+\beta_2} \cdots p_k^{\alpha_{i,k}+\beta_k},$$
so if ba_i is to be a perfect power then there must be some $q_i \ge 2$ such that the numbers $\alpha_{i,1} + \beta_1$, $\alpha_{i,2} + \beta_2$, $\dots$, $\alpha_{i,k} + \beta_k$ are all divisible by q_i.

Choose q_i to be the ith prime number. Then for each $j \in \{1, 2, \dots, k\}$ we have the system of congruences
$$\begin{aligned} \beta_j &\equiv -\alpha_{1,j} \bmod q_1, \\ \beta_j &\equiv -\alpha_{2,j} \bmod q_2, \\ &\vdots \\ \beta_j &\equiv -\alpha_{n,j} \bmod q_n, \end{aligned}$$
and by the Chinese Remainder Theorem this system has a solution. Choosing the exponents β_j according to the solutions to these systems gives us the required b.

Now, to construct the required set of 2011 distinct integers, choose $x_1, x_2, \dots, x_{2011}$ arbitrarily, and let $a_1, a_2, \dots, a_{2^{2011}-1}$ be the sums formed from each nonempty subset of them. From above there is $b \in \mathbb{N}$ such that $ba_1, \dots, ba_{2^{2011}-1}$ are all perfect powers, and so we may take our integers to be $bx_1, bx_2, \dots, bx_{2011}$.

$\square$

7. *Let p be a prime, and let $q(x)$ be a polynomial with integer co-efficients such that $q(0) = 0$, $q(1) = 1$, and $q(n)$ is congruent to 0 or 1 mod p for all $n \in \mathbb{N}$. Show that the degree of q is at least $p-1$.*

Solution: The case $p = 2$ is trivial: the function is nonconstant, so it has degree at least 1. Assume then for some $p \geq 3$ that q has degree less then $p-1$. Then

$$q(x) = \sum_{j=0}^{p-2} a_j x^j = a_0 + a_1 x + \cdots + a_{p-3}x^{p-3} + a_{p-2}x^{p-2},$$

in which any co-efficient may be zero. Noting that $a_0 = q(0) = 0$, we consider

$$\sum_{k=1}^{p-1} q(k) = \sum_{k=1}^{p-1}\sum_{j=1}^{p-2} a_j k^j = \sum_{j=1}^{p-2}\left(a_j \sum_{k=1}^{p-1} k^j\right).$$

We claim that for each $1 \leq j \leq p-2$ the sum $\sum_{k=1}^{p-1} k^j$ is zero mod p. This implies the result, because then $\sum_{k=1}^{p-1} q(k)$ is congruent to zero mod p. Since $q(k)$ is congruent to 0 or 1 mod p, this is only possible if $q(k) \equiv 0 \bmod p$ for $1 \leq k \leq p-1$, which contradicts the fact that $q(1) = 1$.

To prove the claim, we will use the fact that for each $1 \leq j \leq p-2$ there must exist $1 \leq x \leq p-1$ such that $x^j \not\equiv 1 \bmod p$. The existence of x follows from either the existence of a primitive root mod p (that is, an integer of multiplicative order $p-1$ mod p), or the fact that a polynomial of degree m can have at most m roots mod p. Since x has an inverse mod p the elements of the set $\{xt | 1 \leq t \leq p-1\}$ are a complete system of nonzero residues mod p, so

$$\sum_{k=1}^{p-1} k^j = \sum_{k=1}^{p-1} (xk)^j = x^j \sum_{k=1}^{p-1} k^j,$$

and since $x^j \not\equiv 1 \bmod p$, the sum must be zero, as claimed. The result then follows by the preceding paragraph. $\square$

Remark. We note that the bound in the problem is sharp, as the polynomial $q(x) = x^{p-1}$ satisfies the conditions of the problem, by Fermat's Theorem.

April 19, 2011

www.mathsolympiad.org.nz