



2010 Squad Assignment One — Solutions

Number Theory

Due: Wednesday, 17th February 2010

1. Determine all primes p such that $5^p + 4p^4$ is a square number.

Solution: If $5^p + 4p^4 = n^2$ then

$$5^p = n^2 - 4p^4 = (n - 2p^2)(n + 2p^2).$$

Since 5 is prime we must have $n - 2p^2 = 5^a$, $n + 2p^2 = 5^b$ for integers $0 \leq a < b$ such that $a + b = p$.

If $a = 0$ then $n = 2p^2 + 1$, and $5^p = n + 2p^2 = 4p^2 + 1 \equiv 1 \pmod{p}$. This shows that 5 and p are coprime, so by Fermat's Little Theorem we also have $5^p = 5 \cdot 5^{p-1} \equiv 5 \pmod{p}$. It follows that $4 \equiv 0 \pmod{p}$, so p must be 2. But $5^2 + 4(2^4) = 89$ is not square, so $a = 0$ does not give a solution.

If $a > 0$ then 5 divides $\gcd(n - 2p^2, n + 2p^2) = \gcd(n - 2p^2, 4p^2)$, so 5 must divide $4p^2$. Since p is prime this implies $p = 5$. Since $5^5 + 4 \cdot 5^4 = 5^4(5 + 4) = 3^2(5^2)^2$ this does indeed give a solution. So the only solution is $p = 5$. \square

2. For each positive integer a we consider the sequence $\langle a_n \rangle$ with $a_0 = a$ and $a_n = a_{n-1} + 40^{n!}$. Prove that every such sequence contains infinitely many numbers that are divisible by 2009.

Solution: Since 40 and 2009 are coprime we have $40^{k \cdot \phi(2009)} \equiv 1 \pmod{2009}$, where ϕ is the Euler totient function (also known as the Euler phi function). For $n > \phi(2009)$ the exponent $n!$ is a multiple of $\phi(2009)$, and we therefore have $a_{n+1} \equiv a_n + 1 \pmod{2009}$. This means that for $n > \phi(2009)$ all values modulo 2009 are taken cyclicly and periodically, and all values are obtained infinitely often. In particular, this holds for the value 0. \square

3. Find all integers k such that for every integer n , the numbers $4n + 1$ and $kn + 1$ are relatively prime.

Solution: Since $4n + 1$ is odd, the identity $k - 4 = k(4n + 1) - 4(kn + 1)$ shows that $4n + 1$ and $kn + 1$ are relatively prime if $k - 4$ has no odd divisor $p > 1$, that is, if $k - 4 = \pm 2^m$ for some nonnegative integer m .

On the other hand, if $k - 4$ has an odd divisor $p > 1$, then we can easily find a multiple of p of the form $4n + 1$ (for example, the number p^2 , or simply one of the numbers $p, 3p$). For any number $4n + 1$ divisible by p , the above identity implies that $p \mid kn + 1$, hence $4n + 1$ and $kn + 1$ are not relatively prime.

So the answer is $k = 4 \pm 2^m$, where $m = 0, 1, 2, \dots$ \square

4. Let n be a positive integer. Prove that if the sum of all of the positive divisors of n is a perfect power of 2, then the number of those divisors is also a perfect power of 2.

Solution: If $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where p_1, \dots, p_k are distinct primes and $r_i \geq 1$ for each i , then n has

$$\prod_{i=1}^k (r_i + 1)$$

divisors and their sum is

$$\prod_{i=1}^k (1 + p_i + p_i^2 + \cdots + p_i^{r_i})$$

(check that when this product is expanded every number of the form $p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ with $s_i \leq r_i$ occurs exactly once). If this is a power of two then each of the factors

$$f_i = 1 + p_i + p_i^2 + \cdots + p_i^{r_i}$$

must also be a power of two. Since $f_i > 1$, both p_i and r_i must be odd. We will show that $r_i = 1$ for all i , so that the number of divisors is simply 2^k .

Suppose that $r_i > 1$. Then we may factor f_i as

$$f_i = (1 + p_i)(1 + p_i^2 + p_i^4 + \cdots + p_i^{r_i-1});$$

and since f_i has no odd divisor greater than one the even integer $r_i - 1$ (which is assumed to be positive) must be of the form $4k + 2$. This implies that we can factor further to get

$$f_i = (1 + p_i)(1 + p_i^2)(1 + p_i^4 + p_i^8 + \cdots + p_i^{r_i-3}).$$

It follows that both $1 + p_i$ and $1 + p_i^2$ are both powers of two. However, this implies $1 + p_i$ divides $1 + p_i^2$, which is impossible: $1 + p_i^2 = (1 + p_i)(p_i - 1) + 2$, and $1 + p_i \nmid 2$. This completes the proof.

Alternate solution: The factorisation procedure above can be continued to get

$$f_i = (1 + p_i)(1 + p_i^2)(1 + p_i^4) \cdots (1 + p_i^{2^{t_i}}),$$

giving $r_i = 2^{t_i+1} - 1$. This gives a way to complete the problem without arguing that $1 + p_i$ and $1 + p_i^2$ cannot both be powers of two. \square

5. (a) Show that there are infinitely many pairs of positive integers (m, n) such that

$$k = \frac{m+1}{n} + \frac{n+1}{m} \tag{1}$$

is a positive integer.

- (b) Find all positive integers k such that (1) has a positive integer solution (m, n) .

Solution: Suppose that m_0, n_0 and k are positive integers such that

$$k = \frac{m_0+1}{n_0} + \frac{n_0+1}{m_0},$$

and consider the equation

$$k = \frac{m+1}{n_0} + \frac{n_0+1}{m},$$

obtained by fixing n_0 and allowing m to vary. This is equivalent to

$$m^2 + (1 - kn_0)m + n_0^2 + n_0 = 0,$$

a quadratic in m with at least one root $m = m_0$. As such it will typically have a second root $m = m'_0$, and if this is a positive integer we will get a second solution to (1). With any luck we'll then be able to apply this again to get a third, and so on; so, let's find the second root and see if we can use this technique to generate an infinite sequence of solutions, given one as a starting point.

To find the second root, observe that if $x^2 + ax + b = 0$ has roots α_1, α_2 , then

$$a = -(\alpha_1 + \alpha_2), \quad b = \alpha_1\alpha_2$$

(simply expand $(x - \alpha_1)(x - \alpha_2)$ and match co-efficients). So, if we know α_1 is root, we obtain the second as $\alpha_2 = -a - \alpha_1 = b/\alpha_1$. In our case this gives $m'_0 = kn_0 - m_0 - 1 = (n_0^2 + n_0)/m_0$. The first expression for m'_0 shows that it's an integer, and the second that it's positive; thus, if (m_0, n_0) satisfies the conditions of the problem, so does

$$(m_1, n_1) = (n_0, kn_0 - m_0 - 1) = (n_0, (n_0^2 + n_0)/m_0), \quad (2)$$

with the same value of k .

Suppose now that $m_0 \leq n_0$. Then

$$n_1 = \frac{n_0^2 + n_0}{m_0} \geq \frac{n_0(n_0 + 1)}{n_0} = n_0 + 1 > m_1,$$

so our new solution satisfies $m_0 \leq n_0 = m_1 < n_1$. Our new solution is therefore "larger" than our original one (in the sense that $m_0 + n_0 < m_1 + n_1$), so if the equation has at least one solution for a given value of k , it has infinitely many. To prove part (a) it therefore suffices to find a single small solution; and since $m = n = 1$ clearly works (with $k = 4$) we are done. Applying the transformation (2) to this solution we get the sequence $(1, 1)$, $(1, 2)$, $(2, 6)$, $(6, 21)$, \dots

To prove part (b) we used (2) to show that, given one solution to the problem, we could always find a larger one. To prove part (b) we will use the transformation to create smaller solutions instead. Suppose this time that $m_0 > n_0$. Then

$$n_1 = \frac{n_0^2 + n_0}{m_0} < \frac{n_0(n_0 + 1)}{n_0} = n_0 + 1,$$

which gives $n_1 \leq n_0 = m_1 \geq n_1$. So our new solution satisfies $m_0 > n_0 = m_1 \geq n_1$, and is "smaller" in the sense that $m_1 + n_1 < m_0 + n_0$. This gives a descending sequence of positive integer solutions (m_i, n_i) , all with the same value of k , that must terminate after

finitely many steps. Since it can only terminate if $m_i = n_i$ for some i , if there is a solution for a given value of k , there must be one such that $m = n$. In this case we have

$$k = 2 \frac{m+1}{m} = 2 + \frac{2}{m},$$

so $m(k-2) = 2$. Therefore $k = 3$ (with solutions $(2, 2)$, $(2, 3)$, $(3, 6)$, $(6, 14)$, \dots), or $k = 4$, as found above.

Remark: The technique used here is known as *root-flipping* or *Vieta jumping*. □

6. (a) Find all primes p for which $\frac{7^{p-1} - 1}{p}$ is a perfect square.

(b) Find all primes p for which $\frac{11^{p-1} - 1}{p}$ is a perfect square.

Solution: It is easy to check that $p = 2$ is not a solution to either equation, so we may assume that p is odd. Suppose then that $q^{p-1} - 1 = pn^2$ for q odd and p an odd prime. Then

$$q^{p-1} - 1 = (q^{(p-1)/2} - 1)(q^{(p-1)/2} + 1) = pn^2,$$

and since $\gcd(q^{(p-1)/2} - 1, q^{(p-1)/2} + 1) = 2$ we must have either

- (i) $q^{(p-1)/2} - 1 = 2pa^2$, $q^{(p-1)/2} + 1 = 2b^2$, or
- (ii) $q^{(p-1)/2} - 1 = 2a^2$, $q^{(p-1)/2} + 1 = 2pb^2$

for some integers a and b .

(a) Let $q = 7$. In (ii) above we would have $-1 \equiv 2a^2 \equiv (3a)^2 \pmod{7}$, which is impossible because -1 is not a square mod 7. So we must be in case (i). Since $7 \equiv 1 \pmod{6}$ we have $6 \mid (q^{(p-1)/2} - 1) = 2pa^2$, so $3 \mid pa^2$. When $p = 3$ we have $(7^2 - 1)/3 = 4^2$, so 3 is a solution. When $p \neq 3$ we must have $3 \mid a^2$, so $9 \mid (q^{(p-1)/2} - 1)$; and since the order of 7 modulo 9 is 3, we must then have $3 \mid (p-1)/2$.

Let $k = (p-1)/6$. Then $2a^2 = (7^k + 1)(7^{2k} - 7^k + 1)$ implies that $7^{2k} - 7^k + 1$ is a perfect square. But this is not possible, because $(7^k - 1)^2 < 7^{2k} - 7^k + 1 < (7^k)^2$. We conclude that $p = 3$ is the only solution.

(b) Let $q = 11$. In (i) above we would have $1 \equiv 2b^2 \pmod{11}$, which is impossible as 2 is not a square mod 11. So this time we are in case (ii). From $11^{(p-1)/2} + 1 = 2pb^2$ we have $11^{(p-1)/2} \equiv -1 \pmod{p}$, so $2a^2 = 11^{(p-1)/2} - 1 \equiv -2 \pmod{p}$. Hence $a^2 \equiv -1 \pmod{p}$, implying $p \equiv 1 \pmod{4}$. We can therefore factor to get

$$2a^2 = 11^{(p-1)/2} - 1 = (11^{(p-1)/4} - 1)(11^{(p-1)/4} + 1),$$

so either

- i. $11^{(p-1)/4} + 1 = c^2$, giving $11^{(p-1)/4} = (c-1)(c+1)$, which is impossible, since $c-1$ and $c+1$ can't both be powers of 11; or
- ii. $11^{(p-1)/4} + 1 = 2d^2$, which is impossible since 2 is not a square mod 11.

We conclude that there is no prime p for which the given quotient is a square.

□

7. Prove that there exist infinitely many natural numbers n with the following properties: n can be expressed as a sum of two squares, $n = a^2 + b^2$, and as a sum of two cubes, $n = c^3 + d^3$, but can't be expressed as a sum $n = x^6 + y^6$ of two sixth powers, where a, b, c, d, x, y are natural numbers.

Solution: We show that numbers of the form $n = 8(s^6 + t^6)$ satisfy the requirements. Clearly, such a number is a sum of cubes; to see that it can be represented as a sum of squares observe that

$$n = 2(2s^3)^2 + 2(2t^3)^2 = (2s^3 - 2t^3)^2 + (2s^3 + 2t^3)^2.$$

We must now show that such a number cannot be expressed as a sum of sixth powers. Suppose that there is a natural number solution (s, t, u, v) to $8(s^6 + t^6) = u^6 + v^6$, and consider one such that the sum $s + t + u + v$ is minimal. Our aim is to find a second solution (s', t', u', v') such that $s' + t' + u' + v' < s + t + u + v$, and we will do this by showing that u and v are even.

Clearly, u and v must have the same parity in order for the sum of their cubes to be even. However, if they are both odd then $u^6 \equiv v^6 \equiv 1 \pmod{4}$, so $u^6 + v^6 \not\equiv 0 \pmod{8}$, a contradiction. So we must have $u = 2x$, $v = 2y$ for natural numbers x and y . But then $8(s^6 + t^6) = u^6 + v^6 = 64(x^6 + y^6)$, yielding $x^6 + y^6 = 8(s^6 + t^6)$. So (x, y, s, t) is a second solution to the Diophantine equation, and since $x + y = (u + v)/2 < u + v$, we have $x + y + s + t < s + t + u + v$. This contradicts our choice of solution (s, t, u, v) , so no such solution exists.

Alternate solutions. The $n = 8(s^6 + t^6)$ rabbit out of a hat in the “official” solution above isn't the only way to solve this problem. Here are some alternate solutions.

Multiplying by 64. Suppose that $n = a^2 + b^2 = c^3 + d^3$, but that n cannot be expressed as a sum of two sixth powers. Arguing as above we may show that $64n = (8a)^2 + (8b)^2 = (4c)^3 + (4d)^3$ cannot be expressed as a sum of sixth powers either: Again, if $64n = x^6 + y^6$ then x and y must have the same parity; if they are both odd, then $x^6 + y^6 \equiv 2 \pmod{4}$, and if they are both even, then n is a sum of sixth powers. Thus, it suffices to find a single solution. Ha Young Shin used this approach with the initial solution $637 = 14^2 + 21^2 = 8^3 + 5^3$. It's easy to check that this is not a sum of sixth powers, because $2 \times 2^6 = 128 < 637 < 729 = 3^6$.

Working mod seven. A sixth power is congruent to 0 or 1 mod 7, so a sum of two sixth powers is congruent to 0, 1 or 2 mod 7. Thus, if we can find n such that $n = a^2 + b^2 = c^3 + d^3$ and n is not congruent to 0, 1 or 2 mod 7, then n is not a sum of sixth powers. Moreover $(7k + 1)^6 n$ is both a sum of squares and a sum of cubes, and is congruent to $n \pmod{7}$, so it's not a sum of sixth powers either. Thus, it suffices to find a single solution satisfying the conditions above. Tom Yan used this approach and found $370 = 7^3 + 3^3 = 3^2 + 19^2 \equiv 6 \pmod{7}$ as an initial solution.

Manipulating a factorisation. Chiao Lin considered the factorisation

$$\begin{aligned} c^3 + d^3 &= (c + d)(c^2 - cd + d^2) \\ &= (c + d)((c - d)^2 + cd) \\ &= (c + d)(c - d)^2 + (c + d)cd. \end{aligned}$$

If c and d can be chosen such that $c + d$ and cd are both squares then $c^3 + d^3$ will be a sum of squares. This can be achieved by letting $c = j^2(j^2 + 1)$, $d = j^2 + 1$, giving $n = (j^2 + 1)^3(j^6 + 1)$. To complete the problem, we may restrict our attention to j odd. Then n is even, so as above, if $n = x^6 + y^6$ then x and y have the same parity. If they are both odd then $x^6 + y^6 \equiv 2 \pmod{8}$, and if they are both even then $64 \mid x^6 + y^6$, so we might hope to show that the highest power of 2 dividing n lies between 2 and 2^6 . Indeed, when $j = 1$ we have $n = 16$, so $j \equiv 1 \pmod{32}$ gives $n \equiv 16 \pmod{32}$ and we are done. (In fact it turns out that $(j^2 + 1)^3(j^6 + 1) \equiv 16 \pmod{32}$ for all odd j , so we needn't restrict to $j \equiv 1 \pmod{32}$.)

Exploiting primes. Malcolm Granville found yet another family of solutions. There are infinitely many primes of the form $p = 4k + 1$ (by Dirichlet's Theorem, or otherwise), and for such a prime p , theorems about sums of squares tell us that $n = 2p^3$ is a sum of two squares. The factorisation $x^6 + y^6 = (x^2 + y^2)(x^4 - x^2y^2 + y^2)$ and the inequality $x^4 - x^2y^2 + y^4 \geq \frac{1}{4}(x^2 + y^2)^2$ can then be used to show that $2p^3$ is not a sum of sixth powers. \square

8. (a) Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k . Prove that $b = A^n$ for some integer A .
- (b) Does the conclusion still hold if we only know that for every prime p there is an integer a_p such that $b - a_p^n$ is divisible by p ?

Solution: Let the prime factorisation of b be $b = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, where the p_i are distinct primes. Our goal is to show that all the exponents are divisible by n , so that we may set $A = p_1^{\alpha_1/n} \cdots p_s^{\alpha_s/n}$.

To this end, apply the condition with $k = b^2$. The number $b - a_k^n$ is divisible by b^2 and hence, for each $1 \leq i \leq s$, it is divisible by $p_i^{2\alpha_i} > p_i^{\alpha_i}$ as well. Therefore

$$a_k^n \equiv b \equiv 0 \pmod{p_i^{\alpha_i}},$$

and

$$a_k^n \equiv b \not\equiv 0 \pmod{p_i^{\alpha_i+1}}.$$

This implies that the highest power of p_i dividing a_k^n is $p_i^{\alpha_i}$. Since a_k^n is an n th power, this implies that α_i is divisible by n , as desired.

For the second part, let $n = 8$ and $b = 16$. Then $x^8 - 16 \equiv 0 \pmod{p}$ factors as

$$(x^2 - 2)(x^2 + 2)(x^2 - 2x + 2)(x^2 + 2x + 2) \equiv 0 \pmod{p}.$$

If -1 is a square mod p then $x^2 + 2x + 2 = (x + 1)^2 + 1$ has a solution mod p ; and if it is not, then one of $x^2 \equiv 2$ and $x^2 \equiv -2$ must have a solution (using the fact that the

Legendre symbol (x/p) is multiplicative — this means that the product of two quadratic non-residues must be a quadratic residue). This shows that the conclusion does not hold under the weaker condition on b . \square

9. Show that there are infinitely many pairs of distinct primes (p, q) such that $p \mid (2^{q-1} - 1)$ and $q \mid (2^{p-1} - 1)$.

Solution: We're looking for pairs of primes (p, q) such that the order of 2 modulo p divides $q - 1$, and the order of 2 modulo q divides $p - 1$. To do so, it's obviously in our interest to choose primes where we have some control over the multiplicative order of 2. Consider a prime p dividing $2^k + 1$. We have $2^k \equiv -1 \pmod{p}$, and $2^{2k} \equiv (-1)^2 \equiv 1 \pmod{p}$, so the order of 2 modulo p divides $2k$ but not k . We can control this completely if we choose k of the form $k = 2^n$, because then the order of 2 must equal 2^{n+1} ; so, if p divides $F_n = 2^{2^n} + 1$, then 2 has order 2^{n+1} modulo p .

So, let p be a divisor of F_n , and q a divisor of F_m , with $n < m$. Then p and q are distinct (otherwise the order of 2 mod p is equal to both 2^{n+1} and 2^{m+1} , a contradiction), and in addition we have $p \mid (2^{q-1} - 1)$: certainly 2^{n+1} divides 2^{m+1} , and 2^{m+1} must divide $q - 1$, by Fermat's theorem. So, it remains to show that we can choose m so that 2^{m+1} divides $p - 1$. We already have $2^{n+1} \mid (p - 1)$ (again by Fermat's theorem), so let's try $m = n + 1$ — we'll then be halfway there (so to speak).

One way we could show that 2^{n+2} divides $p - 1$ is to show that there's an integer a such that the multiplicative order of $a \pmod{p}$ is 2^{n+2} . Now, we already know that 2 has order $2^{n+1} \pmod{p}$, so if we can choose a such that $a^2 \equiv 2 \pmod{p}$ we'll be done. It's known that 2 is a square mod p if and only if $p \equiv \pm 1 \pmod{8}$ (this is "Supplement II" to the Law of Quadratic Reciprocity); and since $2^{n+1} \mid (p - 1)$, such an a exists provided we restrict ourselves to $n \geq 2$.

In summary: if p and q are primes dividing F_n and F_{n+1} respectively, with $n \geq 2$, then p and q are distinct and satisfy the conditions of the problem. Moreover, the first sentence of the second paragraph shows that we get a different pair (p, q) for each n . This completes the proof. \square

February 2010

www.mathsolympiad.org.nz