Number Theory Problems From APMO 1989-2012

Masum Billal

March 4, 2013

Abstract. This note is a compilation of all the number theory problems that have appeared at APMO so far.

1. Problems

1 (1989, 2)**.** Prove that

$$5n^2 = 36a^2 + 18b^2 + 6c^2$$

has no integer solutions except $a = b = c = n = 0$.

2 (1991, 4)**.** A sequence of values in the range $0, 1, 2, ..., k - 1$ is defined as follows:

$$a_1 = 1, a_n = a_{n-1} + n \pmod{k}$$

For which values of k does the sequence assume all possible values?

3 (1992, 3)**.** Given three distinct positive integers $\frac{n}{2} < a, b, c \leq n$. Prove that, the 8 numbers we get using one multiplication and and addition

$$a + b + c, a + bc, b + ac, c + ab, (a + b)c, (b + c)a, (c + a)b$$

are all distinct. Show that if p is a prime and $n \geq p^2$, then there are $\tau(p - 1)$ ways to choose two distinct numbers b, c from

$$\{p + 1, p + 2, ..., n\}$$

so that the 8 numbers derived from p, b, c are not all distinct.

4 (1992, 4)**.** Find all possible pairs of positive integers (m, n) such that if you draw n lines which intersect in $\frac{n(n-1)}{2}$ distinct points and m parallel lines which meet the n lines in further mn points other than the first $\frac{n(n-1)}{2}$ points, then we can find exactly 1992 regions.

5 (1992, 5)**.** $a_1, a_2, ..., a_n$ is a sequence of non-zero integers such that the sum of any 7 consecutive terms is positive, whereas the sum of any 11 consecutive terms is negative. What is the largest possible value of n?

6 (1993, 2)**.** How many different values can be taken by the expression

$$[x] + [2x] + \left[\frac{5x}{3}\right] + [3x] + [4x]$$

for real $x \in [0, 100]$?

7 (1993, 3)**.**

$$P(X) = (X + a)Q(X)$$

is a real polynomial of degree n. The largest absolute value of the coefficients of $P(X)$ is h and the largest value of the coefficients of $Q(X)$ is k. Prove that $k \leq hn$.

8 (1993, 4)**.** Find all positive integers n for which

$$x^n + (x + 2)^n + (2 - x)^n = 0$$

has an integral solution.

9 (1994, 3)**.** Find all positive integers n such that

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

with $\gcd(a, b) = 1$ and every prime less than or equal to $\sqrt{n}$ divides ab.

10 (1994, 5)**.** Prove that, for any $n > 1$, there is a power of 10 with n digits in base 2 or in base 5 but not both.

11 (1995, 2)**.** Find the smallest n such that any sequence $a_1, a_2, ..., a_n$ whose values are relatively prime square-free integers between 2 and 1995 must contain a prime. n is square-free if it divisible by no square other than 1.

12 (1995, 5)**.** $F : \mathbb{Z} \to \{1, 2, ..., n\}$ is a function such that $F(a)$ and $F(b)$ are not equal whenever a and b differ by $5, 7$ or 12. Find the smallest value of n.

13 (1996, 4)**.** For which n in $[1, 1996]$ is it possible to divide n married couples into exactly 17 groups of single gender, so that the size of any two groups differ by at most 1?

14 (1997, 2)**.** Find an $n \in [100, 1997]$ such that n divides $2^n + 2$.

15 (1998, 2)**.** Show that, $(36m + n)(36n + m)$ is never a power of 2.

16 (1998, 5)**.** What is largest possible positive integer divisible by all positive integers less than its cube root?

17 (1999, 1)**.** Find the smallest positive integer n such that no arithmetic progression of 1999 real contains just n integers.

18 (1999, 4)**.** Find all pairs of positive integers (m, n) such that

$$m^2 + 4n \text{ and } n^2 + 4m$$

are perfect squares.

19 (2000, 2)**.** Find all permutations $(a_1, a_2, ..., a_9)$ of $1, 2, ..., 9$ such that

$$a_1 + a_2 + a_3 + a_4 = a_4 + a_5 + a_6 + a_7 = a_7 + a_8 + a_9 + a_1$$

and

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = a_4^2 + a_5^2 + a_6^2 + a_7^2 = a_7^2 + a_8^2 + a_9^2 + a_1^2$$

20 (2012, 3)**.** Find all positive integer n and prime p with $\dfrac{n^p + 1}{p^n + 1}$ an integer

2. Solutions

1. We can write the equation as

$$5n^2 = 6(6a^2 + 3b^2 + c^2)$$

Since $\gcd(6, 5) = 1$ and 6 is square-free, $6|n$[1]. Then 9 divides the right side. This gives $c = 3c_1$ for some c_1. Dividing the equation by 9, we get

$$5n_1^2 = 4a^2 + 2b^2 + 6c_1^2$$

where $n = 3n_1$ i.e. n_1 even. The square residues of 16 are $0, 1, 4, 9$, therefore $4a^2$ and $5n_1^2$ has residue 0 or 4. Thus, the left side gives a remainder of 4 upon division by 16. So $2b^2 + 6c_1^2 \equiv 0, 4$ or $12 \pmod{16}$. But since $2b^2 \equiv 0, 2, 8 \pmod{16}$ and $6c_1^2 \equiv 0, 6, 8 \pmod{16}$ we have that b, c_1 both are even. If a is even, then dividing the whole equation by 4 would produce a smaller solution than the smallest one. For that sake, we assume a is odd. But this gives a contradiction to the following equation we get from the previous one after dividing by 4,

$$5n_2^2 = a^2 + 2b_1^2 + 6c_2^2$$

Because n_2 is odd, we get again that $5n_2^2 - a^2 \equiv 4$ or $12 \pmod{16}$ which leaves that $2b_1^2 + 6c_2^2 \equiv 4, 12 \pmod{16}$.

2. It's obvious that $a_n \equiv \dfrac{n(n+1)}{2} \pmod{k}$. So, we look for m, n such that $2k|m(m+1) - n(n+1) = (m-n)(m+n+1)$ for some $m, n < k$. In this view, we see this is attainable with $m = k - n$ if k odd. Therefore, we look for only even k and thus, the relation is like a recursive one. If $k = 2^r s$ with s odd, then the same must be true for s as well forcing $s = 1$. But now we have to prove it is valid for powers of two. That's pretty straight forward from $2^r|(m-n)(m+n+1)$ since we take $m-n, m+n+1 < 2^r$. And one of $m-n, m+n+1$ is odd since $m+n+1-(m-n) = 2n+1$, thus doesn't contribute any two's. This completes the proof of our claim.

3.

[1] $a|b$ means b is divisible by a.

4. We can re-state the relation as

$$p^n + 1 | n^p + 1$$

Firstly, we exclude the case $p = 2$. In this case,

$$2^n + 1 | n^2 + 1$$

Obviously, we need

$$n^2 + 1 \geq 2^n + 1 \Rightarrow n^2 \geq 2^n$$

But, using induction we can easily say that for $n > 4$, $2^n > n^2$ giving a contradiction. Checking $n = 1, 2, 3, 4$ we easily get the solutions:

$$(n, p) = (2, 2), (4, 2)$$

We are left with p odd. So, $p^n + 1$ is even, and hence $n^p + 1$ as well. This forces n to be odd. Say, q is an arbitrary prime factor of $p + 1$. If $q = 2$, then $q | n + 1$ and since

$$n^p + 1 = (n + 1)(n^{p-1} - .... + 1)$$

and p odd, there are p terms in the right factor, therefore odd. So, we infer that $2^k | n+1$ where k is the maximum power of 2 in $p + 1$.

We will use the following lemmas without proof for being well-known.

Lemma 1. *If $a|b$ and $a|c$, then $a| \gcd(b, c)$.*

Lemma 2. *If*

$$a^x \equiv b^x \pmod{n}$$

and,

$$a^y \equiv b^y \pmod{n}$$

then

$$a^{\gcd(x,y)} \equiv b^{\gcd(x,y)} \pmod{n}$$

Lemma 3.

$$\lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n = e$$

where e is the Euler constant.

Now, we prove the following lemmas.

Lemma 4. *If x is the smallest positive integer such that*

$$a^x \equiv 1 \pmod{n}$$

then if,

$$a^m \equiv 1 \pmod{n}$$

m is divisible by x.

Proof. Let, $m = xk + r$ with $r < x$. Then, since $a^x \equiv 1$,

$$a^m \equiv (a^x)^k \cdot a^r \equiv 1$$

This implies,

$$a^r \equiv 1 \pmod{n}$$

But this is a contradiction for the minimum $x > r$. So, we must have $r = 0$ that is, $x|m$. $\square$

LEMMA 5. *If* $g = \gcd\left(a+1, \frac{a^p+1}{a+1}\right)$*, then* $g|p$.

PROOF:

$$\frac{a^p+1}{a+1} = (a^{p-1} - a^{p-2}... - a + 1)$$

From Euclid's algorithm,

$$\gcd\left(a+1, \frac{a^p+1}{a+1}\right) = \gcd(a+1, (-1)^{p-1} - (-1)^{p-2} + .. + 1) = \gcd(a+1, p)$$

$\square$

LEMMA 6. *If* p *is an odd prime, then* $p^n \leq n^p$ *for* $p \leq n$.

PROOF. This is true for $n = 1$. Say, this is also true for some smaller values of n. Now, we prove this for $n+1$.

Since $p \leq n$,

$$(pn + p)^p \leq (pn + n)^p$$

and therefore,

$$(n+1)^p = n^p(1 + \frac{1}{n})^p \leq p^n(1 + \frac{1}{p})^p \leq p^n \cdot e < p^{n+1}$$

$\square$

Back to the problem. Assume that q is odd.

$$q|p^n + 1|n^p + 1$$

Write them using congruence. And we have,

$$n^p \equiv -1 \pmod{q}$$

$$\Rightarrow n^{2p} \equiv 1 \pmod{q}$$

Suppose, $e = ord_q(n)$ i.e. e is the smallest positive integer such that

$$n^e \equiv 1 \pmod{q}$$

Then, $e|2p$ and $e|q-1$ from lemma 4.

Also, from Fermat's theorem,

$$n^{q-1} \equiv 1 \pmod{q}$$

Therefore,

$$n^{\gcd(2p,q-1)} \equiv 1 \pmod{q}$$

From p odd and $q|p+1$, $p > q$ and so p and $q-1$ are co-prime. Thus,

$$\gcd(2p, q-1) = \gcd(2, q-1) = 2$$

From lemma 1, $e|\gcd(2p, q-1)$ and so we must have $e = 2$. Again, since p odd, if $p = 2r+1$,

$$n^{2r+1} \equiv n \pmod{q}$$

Hence, $q|n+1$. If $q|\frac{n^p+1}{n+1}$, then by the lemma above we get

$$q|\gcd\left(n+1, \frac{n^p+1}{n+1}\right)|p$$

which would imply $q = 1$ or p. Both of the cases are impossible. So, if s is the maximum power of q so that $q^s|p+1$, then we have $q^s|n+1$ too for every prime factor q of $p+1$. This leads us to the conclusion $p+1|n+1$ or $p \leq n$ which gives $p^n \geq n^p$. But from the given relation,

$$p^n + 1 \leq n^p + 1 \Rightarrow p^n \leq n^p$$

Combining these two, $p = n$ is the only possibility to happen.

Thus, the solutions are

$$(n, p) = (2, 4), (p, p)$$