Problem solving seminar
Number Theory

Mihail Poplavskyi, M.Poplavskyi@warwick.ac.uk

Homework

1. Let x, y, and z be integers such that $S = x^4 + y^4 + z^4$ is divisible by 29. Show that $29^4 \mid S$.

(IMC 2007, 2.2)

Hint: Consider all possible congruence classes of x^4 modulo 29 and prove that $29 \mid x, y, z$.

Solution: We claim that $29 \mid x, y, z$. Then, $x^4 + y^4 + z^4$ is clearly divisible by 29^4. Assume, to the contrary, that 29 does not divide all of the numbers x, y, z. Without loss of generality, we can suppose that $29 \nmid x$. Since the residue classes modulo 29 form a field, there is some $w \in Z$ such that $xw \equiv 1 \pmod{29}$. Then, $(xw)^4 + (yw)^4 + (zw)^4$ is also divisible by 29. So we can assume that $x \equiv 1 \pmod{29}$. Thus, we need to show that $y^4 + z^4 \equiv 1 \pmod{29}$, i.e. $y^4 \equiv -1 - z^4 \pmod{29}$, is impossible. There are only eight fourth powers modulo 29,

$$0 \equiv 0^4, 1 \equiv 1^4 \equiv 12^4 \equiv 17^4 \equiv 28^4 \pmod{29},$$

$$7 \equiv 8^4 \equiv 9^4 \equiv 20^4 \equiv 21^4 \pmod{29},$$

$$16 \equiv 2^4 \equiv 5^4 \equiv 24^4 \equiv 27^4 \pmod{29},$$

$$20 \equiv 6^4 \equiv 14^4 \equiv 15^4 \equiv 23^4 \pmod{29},$$

$$23 \equiv 3^4 \equiv 7^4 \equiv 22^4 \equiv 26^4 \pmod{29},$$

$$24 \equiv 4^4 \equiv 10^4 \equiv 19^4 \equiv 25^4 \pmod{29},$$

$$25 \equiv 11^4 \equiv 13^4 \equiv 16^4 \equiv 18^4 \pmod{29}.$$

The differences $-1 - z^4$ are congruent to $28, 27, 21, 12, 8, 5, 4$, and 3. None of these residue classes is listed among the fourth powers.

2. Find the number of positive integers x satisfying the following two conditions: $x < 10^{2014}$ and $10^{2014} \mid x^2 - x$.

(IMC 2006, 1.2)

Hint: Note that $x^2 - x = x(x-1)$ and $\gcd(x, x-1) = 1$.

Solution: Since $x^2 - x = x(x-1)$ and the numbers x and $x-1$ are relatively prime,one of them must be divisible by 2^{2014} and one of them (maybe the same) must be divisible by 5^{2014}.Therefore, x must satisfy the following two conditions:

$$x \equiv 0 \text{ or } 1 \pmod{2^{2014}}; \quad x \equiv 0 \text{ or } 1 \pmod{5^{2014}}$$

Altogether we have 4 cases.The Chinese remainder theorem yields that in each case there is a unique solution among the numbers $0, 1, \ldots ; 10^{2014} - 1$. These four numbers are different because each two gives different residues modulo 2^{2014} or 5^{2014}. Moreover, one of the numbers is 0 which is not allowed. Therefore there exist 3 solutions.

3. Show that for each positive integer n,

$$n! = \prod_{i=1}^{n} \operatorname{lcm}\left\{1, 2, \ldots, \left[\frac{n}{i}\right]\right\}.$$

(Putnam 2003, B3)

Hint: For each prime $p \le n$ calculate the power of p in t prime expansion for l.h.s and r.h.s

Solution: Consider each prime p such that $p \le n$. We must determine that the number of times p appears as a factor of the product on the right hand side is equal to the number of times p appears as a factor of $n!$. The first thing we note that the highest power of p that divides $n!$ is $\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$. (Of course, this is not an infinite sum.) To see this, note that $\lfloor n/p \rfloor$ is the number of multiples of p that are $\le n$. We count all of these, once, then return to separately count one more factor of p from each of the multiples of p^2, and so forth.

The power of p in lcm$\{1, 2, \ldots, \lfloor n/i \rfloor\}$ is the largest k such that $p^k \le n/i$. This power is exactly k whenever $ip^k \le n < ip^{k+1}$ or $n/p^{k+1} < i \le n/p^k$. Hence, the power p^k occurs $\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor$ times. Therefore the total power of p in the l.h.s. is $\sum_{k=1}^{\infty} k\left(\lfloor n/p^k \rfloor - \lfloor n/p^{k+1} \rfloor\right) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$. With the same power of p dividing each side for each prime p, the two sides have the same prime factorization and are hence by the Fundamental Theorem of Arithmetic equal to the same integer.