Problem solving seminar
Number Theory

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

Some usefull results from number theory.

Def. *Let m be an integer number. We say that integers a, b are* ***congruent modulo*** *m and write $a \equiv b \pmod{m}$ or $a \underset{m}{\equiv} b$ if m divides $a - b$, or the same a and b leave the same remainder when they are divided by m.*

Congruence modulo n is an equivalence relation; the equivalence classes are called congruence classes modulo n. You can work with congruences in the same way like with equalities, i.e. sum, subtract, multiply and delete (be careful on conditions) .

GCD and LCM. For any integer a and b there are exist integers x and y such that $\gcd(a, b) = ax + by$. GCD and LCM are connected by $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Chinese remainder theorem. Let a and b be natural numbers with $\gcd(a, b) = 1$, and let c and d be arbitrary integers. Then there is a solution to the simultaneous congruences

$$x \equiv c \pmod{a}, \quad x \equiv d \pmod{b}.$$

Moreover, the solution is unique modulo ab, i.e. if x_1 and x_2 are two solutions, then $x_1 \equiv x_2 \pmod{ab}$.

Fermat's theorem Let p be a prime number. Then $n^p \equiv n \pmod{p}$ for any natural number n.

Wilson's theorem Let p be a prime number. Then $(p-1)! \equiv -1 \pmod{p}$.

What are all divisors of n? If n is an arbitrary integer with prime expansion $n = p_1^{\alpha_1} p_1^{\alpha_2} \dots p_k^{\alpha_k}$, then there are $d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ divisors of form $d = p_1^{\beta_1} p_1^{\beta_2} \dots p_k^{\beta_k}$ with $\beta_i \le \alpha_i$.

What is the prime expansion of $n!$? For any prime p and integer n the biggest degree of p^k such that $p^k \mid n!$ is $k = \sum\limits_{i=1}^{\infty} \left[\dfrac{n}{p^i}\right]$, where $[x]$ is the integer part of x, i.e. biggest integer less or equal to x.

Problems.

Warm-up

1. Let x, y, and z be integers such that $S = x^2 + y^2 + z^2 + t^2$ is divisible by 8. Show that $16 \mid xyzt$.

2. Find the gcd $\left(17^{17^{17^{17}-1}-1} - 1, 17^{17^{17}-1} - 1\right)$.

Finite or infinite sets. Consecutive integers.

3. Is the set of positive integers n such that $n!+1$ divides $(2014n)!$ finite or infinite?

Relatively prime numbers.

4. Let p and q be relatively prime positive integers. Prove that

$$\sum_{k=0}^{pq-1} (-1)^{\left[\frac{k}{p}\right]+\left[\frac{k}{q}\right]} = \begin{cases} 0, & \text{if } pq \text{ is even,} \\ 1, & \text{if } pq \text{ is odd.} \end{cases}$$

5. We call the set A consist of integers *magic*, if for any $x, y \in A$ and $k \in \mathbf{Z}$ we have $x^2 + kxy + y^2 \in A$. Find all integer pairs (m, n) such that there is only one *magic* set which contains both m and n.

Fermat's and Wilson's theorems

6. Suppose p is an odd prime. Prove that

$$\sum_{k=0}^{p} \binom{p}{k}\binom{p+k}{k} \equiv 2^p + 1 \pmod{p^2}.$$

Homework

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

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

3. Show that for each positive integer n,

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