IMC preparation 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 $\beta_i \leq \alpha_i$ with the sum equal to $\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}$.

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 $k = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right]$, where $[x]$ is the integer part of x, i.e. the biggest integer less or equal to x.

Problems.

1. Find all integer x, y, x, t which satisfy

$$x^2 + y^2 + z^2 + t^2 = 2xyzt.$$

(Moscow City Olympiad 1949, I.10.1)

Answer: $x = y = z = t = 0$.

Hint: Consider remainders modulo 8 of the l.h.s and r.h.s and prove that x, y, z, t are infinitely divisible by 2.

Solution: We will use simple observation: for odd integers n one has $n^2 \equiv 1 \pmod 8$. The r.h.s. is even, so we have even number of odds on the l.h.s. If all x, y, z, t are odd, then the l.h.s.$\equiv 4 \pmod 8$ and the r.h.s.$\equiv 2 \pmod 4$, and we get contradiction. If there are exactly two odds, then the l.h.s.$\equiv 2 \pmod 4$, but the r.h.s.$\equiv 0 \pmod 8$. Therefore all values are even. Changing variables to $x_1 = x/2, \ldots, t_1 = t/2$ we obtain new equation

$$x_1^2 + y_1^2 + z_1^2 + t_1^2 = 8x_1y_1z_1t_1.$$

Same arguments yield that $x_1, \ldots, t_1$ are even. Continuing the above scheme we prove x, y, z, t are infinitely divisible by 2, and therefore the only possible solution is given by $(0, 0, 0, 0)$. Finally we just need to check that this set satisfy the equation, which is evident.

2. For a given positive integer m, find all triples $(n; x; y)$ of positive integers, with n relatively prime to m, which satisfy

$$\left(x^2 + y^2\right)^m = (xy)^n .$$

(Putnam 1992, A3)

Answer: If m is odd, then there are no such triples; otherwise $n = m + 1$,$x = y = 2^{m/2}$.

Hint: Change x, y to $x' \cdot \gcd(x, y)$ and $y' \cdot \gcd(x, y)$ with x', y' relatively prime.

Solution: Inequality $x^2 + y^2 > xy$ yield $m < n$. For any pair of integer numbers x, y we can find relatively prime x', y' such that $x = x' \cdot \gcd(x, y)$ and $y = y' \cdot \gcd(x, y)$. Then our equation can be rewritten as

$$\left(x'^2 + y'^2\right)^m = \left(x'y'\right)^m \gcd(x, y)^{2(n-m)} .$$

R.h.s is divisible by any prime factor of x', so the l.h.s. does. But $\gcd\left(x'^2 + y'^2, x'\right) = 1$, therefore $x' = 1$. Analogously $y' = 1$ and we get

$$2^m = \gcd(x, y)^{2(n-m)} .$$

It s easy to see that $\gcd(x, y) = 2^k$ for some integer k. And m, n, k satisfy

$$m = 2(n - m)k.$$

m has to be even and divisible by $n-m$. As m and n are relatively prime with $n>m$ we have $n-m=1$. Now one can see, that the unique solution of this equation with relatively prime m and n is given by $m=2k$, $n=2k+1$.

3. Let $d(n)$ be a number of all divisors of n. Find all integer positive n such that

$$\frac{n}{d(n)}=p,$$

for some prime p.

(Moscow City Olympiad 1967, II.8.2)

Answer: $n=8,9,12,18,24,8p,12p$ for prime $p>3$.

Hint: Use the Euler's formula for the number of divisors and fact that n is divisible by p.

Solution: It is obvious that $p\,|\,n$. Consider prime factorization of n in the following form

$$n=p^{\alpha}p_1^{\alpha_1}\dots p_k^{\alpha_k},$$

where p_i are different primes, and $\alpha_i\geq 1$. By using the Euler's formula for the number of divisors initial equation can be rewritten as

$$\frac{p^{\alpha-1}}{\alpha+1}\prod_{i=1}^{k}\frac{p_i^{\alpha_i}}{\alpha_i+1}=1.$$

The main idea of the following solution is to prove that all these fractions are big enough and the product can be small just in few cases.
Observe, that for any prime q and integer β we have $q^{\beta}\geq\beta+1$ and equality is only possible for $q=2$, $\beta=1$. So if $p^{\alpha-1}=\alpha+1$, then number of prime factors p_i is at most 1, and p_1 can be equal only to 2 with $\alpha_1=1$, and if $p^{\alpha-1}>\alpha+1$ then there are no solutions.
Now we are going to find all possible pairs (p,α) such that the first fraction is small enough.

- If $\alpha\geq 2$ and $p\geq 5$, then $p^{\alpha-1}>\alpha+1$;
- If $\alpha>2$ and $p\geq 3$, then $p^{\alpha-1}>\alpha+1$;
- If $\alpha>3$ and $p\geq 2$, then $p^{\alpha-1}>\alpha+1$.

Remark 1. *All inequalities can be easily checked by induction, or using derivatives technique.*

So finally we are left only with the following possibilities

- $p=2$, $\alpha=1,2,3$
  - * $\alpha=3$: $\dfrac{p^{\alpha-1}}{\alpha+1}=1\Rightarrow \underline{n=8}$.
  - * $\alpha=2$: $\dfrac{p^{\alpha-1}}{\alpha+1}=2/3\Rightarrow 3\,|\,n$. Let $p_1=3$, then $\dfrac{p_1^{\alpha_1}}{\alpha_1+1}\geq 3/2$ and the unique solution is $\underline{n=12}$.

* $\alpha = 1$: $\dfrac{p^{\alpha-1}}{\alpha+1} = 1/2$ but $2 \nmid \prod_{i=1}^{k} p_i^{\alpha_i}$, and this case is impossible.

- $p = 3$, $\alpha = 1, 2$

* $\alpha = 2$: $\dfrac{p^{\alpha-1}}{\alpha+1} = 1 \Rightarrow \underline{n = 9, 18}$.

* $\alpha = 1$: $\dfrac{p^{\alpha-1}}{\alpha+1} = 1/2$, so n is even. Let $p_1 = 2$ then equation can be rewritten in the form

$$\frac{2^{\alpha_1-1}}{\alpha_1+1} \prod_{i=2}^{k} \frac{p_i^{\alpha_i}}{\alpha_i+1} = 1,$$

and we finish with initial equation for the case $p = 2$ with the only one restriction $p_i \neq 3$ for any i. So the unique answer in this case is $\underline{n = 24}$.

- $p > 3$, $\alpha = 1$ in this case we have $\dfrac{p^{\alpha-1}}{\alpha+1} = 1/2$ and as well as in the previous case we end up with equation

$$\frac{2^{\alpha_1-1}}{\alpha_1+1} \prod_{i=2}^{k} \frac{p_i^{\alpha_i}}{\alpha_i+1} = 1,$$

which is fully solved above, and we get solutions of the form $\underline{n = 8p, 12p}$.

Homework

1. Prove that there is no number of the form 10^{3n+1} which can be expressed as a sum of two perfect cubes.

2. Prove that, for any integers a, b, c, there exists a positive integer n such that $\sqrt{n^3 + an^2 + bn + c}$ is not an integer.

3. Prove that p and $p + 2$ are twin primes if and only if

$$p^2 + 2p \quad | \quad 4\left((p-1)! + 1\right) + p.$$

Additional problem[1]

4. Let S_n denote the sum of the first n prime numbers. Prove that for any n there exists the square of an integer between S_n and S_{n+1}.

[1] If we do not start the problem during the class, then it is a part of your homework