These are some notes (written by Tejaswi Navilarekallu) used at Indian National Mathematical Olympiad Training Camp (INMOTC) 2014, held in Bengaluru during the first week of January, 2014.

1 Basic definitions and results

Definition 1.1. Given integers a and b, we say that a divides b if there exists an integer m such that $b = am$. We also say that a is a divisor (or a factor) of b. We write $a \mid b$.

Definition 1.2. A positive integer p is called a prime number if it has exactly two positive divisors (namely 1 and itself). A composite number is an integer $n > 1$ that is not a prime.

Here are some properties.

- If $a \mid b$ then $a \mid bc$.
- If $a \mid b$ and $b \mid c$ then $a \mid c$.
- If $a \mid b$ and $a \mid c$ then $a \mid (b \pm c)$.
- If $a \mid b$ and $a \mid c$ then $a^2 \mid bc$.
- If $a \mid b$ then $a^k \mid b^k$.

By the definition of prime number it is easy to prove the following:

Proposition 1.3. *If $n > 1$ is an integer then n has a prime divisor.*

Proof. By induction. If n is a prime then we are done. Otherwise, let m be a divisor of n, with $m \neq 1, n$. Then $1 < m < n$. So, by induction m has a prime divisor p. It is easy to see that p divides n. □

Corollary 1.4. *There infinitely many prime numbers.*

Proof. If $p_1, \ldots, p_k$ are all the primes, then let $n = p_1 p_2 \cdots p_k + 1$. Then, by the above proposition we get a prime factor p of n, which will have to equal one of the p_i's. This gives a contradiction. □

The following are two very important results in number theory.

Theorem 1.5. *If p is a prime number, a and b are integers such that p divides ab then p divides a or p divides b.*

Theorem 1.6. *Every integer $n > 1$ can be uniquely written as*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where $p_1 < p_2 < \cdots < p_k$ are primes and α_i's are positive integers.

Here is a simple formula for the number of positive divisors of a given number. Let n be a positive integer. From the prime factorization, we can write n as

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

where p_i's are distinct prime numbers, and α_i's are positive integers. In this case, the number of positive divisors of n is

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

From the above formula we get:

Proposition 1.7. *The number of positive divisors of n is odd if and only if n is a square of an integer.*

Definition 1.8. The greatest common divisor of two positive integers m and n is defined as the highest integer that divides both m and n. We denote this by $gcd(m, n)$ or by just (m, n). We say that two integers m and n are coprime to each other if their gcd is 1.

Definition 1.9. The least common multiple of two positive integers m and n is defined as the smallest integer that is divisible by both m and n. We denote this by $lcm(m, n)$.

Here are some properties:

- $gcd(m, n) \cdot lcm(m, n) = mn$.
- If $d = (m, n)$ then there are integers x and y such that $mx + ny = d$.
- $(m, n) = (m, rm + n)$ for any integer r.
- If $m \mid ab$ and $(m, a) = 1$ then $m \mid b$.
- If $m \mid a, n \mid a$ and $(m, n) = 1$ then $mn \mid a$.

Given integers m and n, we can write

$$m = nq + r$$

where q and r are integers with $0 \leq r \leq n - 1$. We call q the quotient and r the remainder.

Example. Common factors (or the lack thereof) between variables is something to look for in number theory problems. For example, consider the equation

$$x^2 + y^2 = z^2 \,, \tag{1.10}$$

with x, y, z being positive integers. If $d = (x, y, z)$ then $(x/d)^2 + (y/d)^2 = (z/d)^2$ and $(x/d, y/d, z/d) = 1$. In other words, all the solutions to (1.10) can be obtained by *primitive* solutions, i.e., solutions in which $(x, y, z) = 1$. For a primitive solution, we note that one of x and y has to be odd, and the other even. Without loss of generality we suppose that y is even. We can then rewrite (1.10) as

$$x^2 = (z^2 - y^2) = (z - y)(z + y) \,.$$

Note that one in fact has $(y, z) = 1$ for primitive solutions, and since z is odd it follows that $(z+y, z-y) = 1$. It follows then that both $z + y$ and $z - y$ have to be squares (of odd coprime integers). Thus any primitive solution to (1.10) is given by $\left(rs, \frac{r^2-s^2}{2}, \frac{r^2+s^2}{2}\right)$ for some odd coprime integers $r > s$.

---

2 Congruences

Definition 2.1. For integers a, b and m, we say that a is congruent to b modulo m if m divides $(a - b)$. We write

$$a \equiv b \pmod{m}.$$

The idea is to get a good handle on the remainder obtained when a is divided by b. Some properties of congruences are as follows:

Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then

- $b \equiv a \pmod{m}$.
- If $b \equiv e \pmod{m}$ then $a \equiv e \pmod{m}$.
- $a \pm c \equiv b \pm d \pmod{m}$.
- $ac \equiv bd \pmod{m}$.
- $a^k \equiv b^k \pmod{m}$.

Proposition 2.2. *Let a and m be integers with $(a, m) = 1$. Then*

1. *there is an integer b such that $ab \equiv 1 \pmod{m}$.*
2. *there is a positive integer k such that $a^k \equiv 1 \pmod{m}$.*

If $(a, m) = 1$, then the smallest positive integer k such that $a^k \equiv 1 \pmod{m}$ is called the *order* of a modulo m. For example, the order of 2 modulo 15 is 4.

Theorem 2.3 (Wilson's Theorem). *If p is a prime then $(p-1)! \equiv -1 \pmod{p}$.*

Theorem 2.4 (Fermat's little theorem). *Let p be a prime number and a be an integer. Then $a^p \equiv a \pmod{p}$. Equivalently, if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 2.5. *Let n be an integer and let p be a prime dividing $n^2 + 1$. Then either $p = 2$ or $p \equiv 1 \pmod{4}$.*

3 Problems

1. For a positive integer n, let $d(n)$ denote the number of it's positive divisors. For example, $d(15) = 4$ since the divisors of 15 are 1, 3, 5 and 15. Determine whether the sum $d(1) + d(2) + \cdots + d(2014)$ is even or odd.
2. Find all positive integers a such that $a + 3$ divides the $lcm(a, a+1, a+2)$.
3. What is the last digit of $(7777)^{7777}$?
4. If $n = 4k + 3$ then show that there is a prime $p \equiv 3 \pmod{4}$ that divides n.
5. Use the above and imitate the proof of Corollary 1.4 to show that there are infinitely many primes of the form $4k + 3$.
6. Show that there exists a positive integer n such that $n!$ has exactly 1993 zeros at the end.
7. Show that $n^5 - n$ is divisible by 30 for all $n > 0$.
8. Let m and n be integers such that 24 divides $mn + 1$. Prove that 24 divides $m + n$.
9. Show that the tenth digit of 3^k is even for all $k \geq 1$.
10. Show that 3 does not divide $n^2 + 1$ for any integer n. Show that the same result holds true if we replace by 3 by 7. (Do not use Theorem 2.5).
11. Show that $19^{93} - 13^{99}$ is a positive integer divisible by 162.
12. Find all solutions to the equation $p^x = y^4 + 4$ where p is a prime and x, y are positive integers.
13. Show that $n^4 + 4^n$ is not a prime number for $n > 1$.
14. Find all positive integers m and n such that $2^m + 3^n$ is a square.
15. Find all non-negative integers x, y, z such that $3^x + 4^y = 5^z$.
16. Find all primes p such that $\frac{2^{p-1}-1}{p}$ is a square.
17. Determine all the integers n such that $n^2 + 19n + 92$ is a square.
18. Find all integer solutions to the equation $x^2 + 7x - 14(q^2 + 1) = 0$.
19. Find all pairs of integers (x, y) such that $y^2 = x^3 + 7$.
20. If m and n are integers show that $4mn - m - n$ is not a square.
21. Show that there are infinitely many prime numbers of the form $4k + 1$. (Hint: If $p_1, \ldots, p_k$ are the only such primes then look at $n = (2p_1p_2 \cdots p_k)^2 + 1$.)
22. Prove that for every positive integer n there exists an n-digit number divisible by 5^n all of whose digits are odd.

23. Find all primes p and q such that pq divides $2^p + 2^q$.

24. Prove that there always exists three numbers a, b, c from any given seven integers such that $a^2 + b^2 + c^2 - ab - bc - ca$ is divisible by 7.

25. Show that every rational number can be written as a quotient of products of factorials of (not necessarily distinct) primes, and that the representation is unique up to rearranging and cancelling common factors.

26. Find all primes p for which there are positive integers a and b such that $p = a^2 + b^2$ and p divides $a^3 + b^3 - 4$.

27. Find all natural numbers n and k such that $2^n + 3 = 11^k$.

28. Let $f(n)$ denote the least positive integer such that $\sum_{k=1}^{f(n)} k$ is divisible by n. Prove that $f(n) = 2n - 1$ if and only if n is a power of 2.

29. Find all integers x and y such that $x^4 + x^3 + x^2 + x + 1 = y^2$.

30. Let $f(x)$ be a non-constant polynomial with integer coefficients. Prove that there exists an integer k such that $f(k)$ is not a prime.

31. Let $P(x)$ be a polynomial with integer coefficients. Prove that the polynomial

$$Q(x) = P(x^4)P(x^3)P(x^2)P(x) + 1$$

has no integer roots.

32. Let $f(x)$ be a polynomial with integer coefficients. If $g(x) = f(x) + 77$ has an integer root, prove that $f(x)$ has at most four distinct integer roots.