These are some notes (written by Tejaswi Navilarekallu) used at the International Mathematical Olympiad Training Camp (IMOTC) 2013 held in Mumbai during April-May, 2013.

1 Divisibility and congruences

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 (Fundamental theorem of arithmetic)**.** *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.

Definition 1.7. *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 1.8. *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 $lcm(m, n)$.*

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

$$x^2 + y^2 = z^2\,, \tag{1.9}$$

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 (1.9) 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 (1.9) 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 (1.9) is given by $\left(rs, \frac{r^2-s^2}{2}, \frac{r^2+s^2}{2}\right)$ for some odd coprime integers $r > s$.

Here are some properties of greatest common divisors which are often useful:

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

Before going further, we introduce the notion of congruences. The theory of congruences is essentially a notational simplification of the divisibility properties.

Definition 1.10. *For integers a, b and m, we say that a is congruent to b modulo n if n divides $(a - b)$. We write*

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

The idea is to get a good handle on the remainder obtained when a is divided by n. The basic properties of divisibility mentioned in the earlier section can be translated in congruence notation as follows. Let $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then

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

Proposition 1.11. *Let a and n be integers with $(a, n) = 1$. Then*

(a) there is an integer b such that $ab \equiv 1 \pmod{n}$; and,

(b) there is a positive integer k such that $a^k \equiv 1 \pmod{n}$.

Proof. (a) Since $(a, n) = 1$ we have from the properties of gcds that there exists integers b and c such that $ab + nc = 1$ and hence $ab \equiv 1 \pmod{n}$.

(b) Consider $\{1, a, a^2, \ldots, a^{n+1}\}$. Since there are only n possible remainders modulo n it follows that at least two elements in this set are congruent modulo n, and hence we get $a^k \equiv 1 \pmod{n}$ for some k. □

Theorem 1.12 (Chinese remainder theorem)**.** *Let m, n be positive integers with $(m, n) = 1$ and let a, b be integers. Then there is a unique integer x_0 such that $0 \leq x_0 \leq mn - 1$, $x_0 \equiv a \pmod{m}$ and $x_0 \equiv b \pmod{n}$. Morevoer, any x which satisfies $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ equals $x_0 + kmn$ for some integer k.*

Proof. Let $0 \leq a_0 \leq m$ be such that $a \equiv a_0 \pmod{m}$. Consider the set $\{a_0, a_0 + m, a_0 + 2m, \ldots, a_0 + mn - m\}$. Since $(m, n) = 1$ it follows that no two elements from this set leave same remainder when divided by n. Therefore there is a unique q with $0 \leq q \leq n - 1$ such that $x_0 = a_0 + qm \equiv b \pmod{n}$. The second part of the theorem follows from the uniqueness of x_0. □

Definition 1.13 (Euler's totient function)**.** *For a natural number n we denote by $\varphi(n)$ the number of integers between 1 and n (both inclusive) that are coprime to n.*

Let S_n denote the set $\{1, 2, \ldots, n\}$ and $T_n = \{a | 1 \leq a \leq n, (a, n) = 1\} \subseteq S_n$. Then by definition we have $\varphi(n) = |T_n|$. We shall think of elements of these sets as "remainders" when integers are divided by n. Therefore we distinguish between elements in T_m and T_n for $m \neq n$.

Proposition 1.14. *The function φ from the set of natural numbers to itself is multiplicative, i.e., if m and n are coprime positive integers then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. Consider the map $f : T_{mn} \to T_m \times T_n$ defined by $a \mapsto (\bar{a}, \bar{a})$, where the image of a in T_m (and T_n, respectively) is the remainder when a is divided by m (resp. n). Given remainders c and d modulo m and n, respectively, by Chinese remainder theorem it follows that the equations $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$ have a unique solution modulo mn. This shows that f is a bijection and hence the result. □

Theorem 1.15. *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ with $p_1, p_2, \ldots, p_k$ distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_k$ positive integers then*

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Proof. Both the sides in the statement of the theorem are multiplicative, and therefore it is enough to prove the result when n is a power of prime. If $n = p^\alpha$ then $\varphi(n) = p^\alpha - p^{\alpha-1} = n\left(1 - \frac{1}{p}\right)$, and hence the theorem follows. □

There are many identities involving the totient function that are not difficult to prove. We give here one example which is motivated by the study of cyclotomic polynomials.

Proposition 1.16. *For a positive integer n one has*

$$\sum_{d|n} \varphi(d) = n.$$

We first prove a useful lemma.

Lemma 1.17. *Let f be a multiplicative function from the set of positive integers to itself. Define $F(n) = \sum_{d|n} f(d)$. Then F is also multiplicative.*

Proof. Suppose that m, n are positive integers such that $(m, n) = 1$. Then

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) = \sum_{d_1|m, d_2|n} f(d_1 d_2) \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) = \sum_{d_1|m} f(d_1) F(n) = F(m)F(n). \end{aligned}$$

□

Proof of Proposition 1.16. From the previous lemma it follows that both the sides of the required identity are multiplicative functions. Therefore it is enough to prove the result for prime powers. If $n = p^\alpha$ then the left-hand side equals

$$\sum_{d|p^\alpha} \varphi(d) = 1 + \sum_{k=1}^{\alpha} (p^k - p^{k-1}) = p^\alpha .$$

□

Remark. One of the motivations for studying Euler's totient function comes from the theory of cyclotomic fields. Let n be a positive integer. While solving certain diophantine equations, it is handy to have a factorisation of the polynomial $x^n - 1$ into polynomials with integer coefficients. For example, when we looked the solutions to Pythagoras equation, the we used the factorisation of the polynomial $x^2 - 1$.

The polynomial $F_n(x) = x^n - 1$ has exactly n distinct complex roots. In fact, if $\zeta_n = e^{2\pi i/n}$ then $\{\zeta_n^r\}_{0 \le r \le n-1}$ is the set of all roots. Similar to the notion of order modulo an integer, we can define the order of a root ζ_n^r of unity as the least positive integer k such that $(\zeta_n^r)^k = 1$. In particular, the order of ζ_n is n.

It then follows that for any d dividing n, there are exactly $\varphi(d)$ roots of order d. This gives the identity $\sum_{d|n} \varphi(d) = n$. Define $\Phi_d(x) = \prod(x - \zeta)$, where the product runs over all the roots of $x^n - 1 = 0$ of order d. Then $\Phi_d(x)$ is a polynomial of degree $\varphi(d)$, and in fact, it is irreducible and all its coefficients are integers (why?). Moreover, $\Phi_d(x)$ is independent of n. This polynomial is called the d-th cyclotomic polynomial.

Here are some identities left as an exercise for the reader.

Exercise 1.18. *Prove that*

$$\sum_{1 \le k \le n, (k,n)=1} k = \frac{n\varphi(n)}{2} .$$

Exercise 1.19. *Find a closed expression in terms of n and its prime factorisation for the number of integers k between 1 and n such that $(k, n) = (k - 1, n) = 1$.*

Exercise 1.20. *Find a closed expression in terms of n and its prime factorisation for sum of integers k between 1 and n such that $(k, n) = (k - 1, n) = 1$.*

There are also many conjectures related to the totient function. Here are two examples.

Conjecture 1.21. *For a positive integer n, if $\varphi(n)$ divides $n - 1$ then n is a prime.*

Conjecture 1.22. *For a positive integer n, if n divides $\varphi(n)d(n) + 2$, where $d(n)$ is the number of positive divisors of n.*

We now state some of the very powerful results.

Theorem 1.23 (Wilson's Theorem)**.** *If p is a prime then $(p - 1)! \equiv -1 \pmod p$.*

Theorem 1.24 (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 1.25. *Let n be a positive integer and a an integer such that $(a, n) = 1$. Then $a^{\varphi(n)} \equiv 1 \pmod n$.*

Squares play an important role in analysing the properties of integer solutions to diophantine equations. (We have already seen this while looking at the solutions to Pythagoras equation.) Therefore it is good to know and keep track of properties of squares. In particular, it is very useful to know the following simple results.

- If $n^2 = ab$ and $(a, b) = 1$ then a and b are squares.
- If n is not divisible by 3 then $n^2 \equiv 1 \pmod 3$.
- If n is odd then $n^2 \equiv 1 \pmod 4$ and in fact, $n^2 \equiv 1 \pmod 8$.
- If p is a prime, then the equation $x^2 \equiv a \pmod p$ has a solution for precisly $(p + 1)/2$ values of a with $0 \leq a \leq p - 1$.

Slightly more non-trivial results are below.

Theorem 1.26. *Let n be an integer and let p be a prime dividing $n^2 + 1$. Then either $p = 2$ or $p \equiv 1 \pmod 4$. Conversely, if $p = 2$ or $p \equiv 1 \pmod 4$ then there exists an integer n such that p divides $n^2 + 1$.*

Theorem 1.27. *If $p = 2$ or $p \equiv 1 \pmod 4$ then there exists integers a and b such that $p = a^2 + b^2$.*

Definition 1.28. *If $(a, n) = 1$, then the smallest positive integer k such that $a^k \equiv 1 \pmod n$ is called the* order *of a modulo n, and is denoted by $o_n(a)$.*

The importance of orders is somewhat apparent from the following result.

Theorem 1.29. *Let n be a positive integer and a an integer such that $(a, n) = 1$. If $a^d \equiv 1 \pmod n$ then $o_n(a)$ divides k. In particular, $o_n(a)$ divides $\varphi(n)$.*

Example. Suppose that p is a prime dividing $a^2 + 1$, or in other words $a^2 \equiv -1 \pmod p$. Squaring both the sides we get $a^4 \equiv 1 \pmod p$. Therefore $o_p(a)$ divides 4, but does not divide 2. This proves that $o_p(a) = 4$ and hence 4 divides $p - 1$.

Example. Let a, b be relatively prime positive integers. Let p be a prime dividing $a^{6^n} + b^{6^n}$. Then $a^{6^n} + b^{6^n} \equiv 0 \pmod p$. Note that $(a, b) = 1$ implies that $(a, p) = (b, p) = 1$. Therefore b has an "inverse" modulo p, i.e., there exists c such that $bc \equiv 1 \pmod p$. We therefore get $(ac)^{6^n} \equiv -(bc)^{6^n} \equiv -1 \pmod p$. Squaring we get $(ac)^{2 \cdot 6^n} \equiv 1 \pmod p$. Therefore $o_p(ac)$ divides $2 \cdot 6^n$ and does not divide 6^n. This shows that $o_p(ac) = 2^{n+1} \cdot d$ for some odd integer d. Since $o_p(ac)$ divides $p - 1$ it follows that $p \equiv 1 \pmod{2^{n+1}}$.

There are a few reasons why orders are important: (a) if something is congruent to one modulo n then its k-th power is also congruent to one modulo n; (b) if $a^k \equiv 1 \pmod n$ then a^{k-1} is the multiplicative inverse of a modulo n; (c) if $a^k \equiv -1 \pmod n$ then $v_2(\varphi(n)) \geq v_2(k) + 1$ where $v_q(m)$ denotes the exponent of q dividing m.

2 Problems

When dealing with a diophantine equation, there are few systematic steps that one can go through to get a better idea of the problem.

- To start with, if possible, find any small solution by plugging in small values. If there exists a solution, and you expect only finitely many solutions, then you cannot get a contradition unless you assume something more about the variables.
- Identify the possible parities of all the variables.

- Try to rearrange the terms so that both the sides are *nice*. The following are nice to have in an equation:
  - factorisable polynomials;
  - squares or higher powers;
  - sum of two squares (and in particular n^2+1 for some integer n).
- Consider the equations modulo small primes.
- Look for the properties of the prime divisors of each side of the (rearranged) equation.

Example. Consider the equation $y^2 = x^3+7$. We would like to find all integer solutions to this equation.

- To start with, we plug is small values of x and y to see if there are any simple solutions, and find that there are are no *small* solutions.
- We next consider the parity of x and y. Clearly, they have to be of opposite parity. Also, if x is even then $x^2+7 \equiv 3 \pmod 4$ while $y^2 \equiv 1 \pmod 4$. Hence x is odd and y is even.
- Now we try to manipulate the equation to get nice terms on both the sides. Even though y^2 is nice x^3+7 is not-so-nice, so there is need of manipulation. Note that adding 1 to both the sides make them nice since we will have sum of two squares on the left-hand side and a factorisable polynomial on the right-hand side. So we rewrite the equation as
$$y^2+1 = (x+2)(x^2-2x+4)\,.$$
- The prime divisors of left-hand side have special property, and therefore all the prime divisors of the right-hand side should also have the same property. That is, if a prime p divides the right-hand side then $p \equiv 1 \pmod 4$. In particular, this implies that $x^2-2x+4 \equiv 1 \pmod 4$. But since x is odd, $x^2-2x+4 = (x-1)^2+3 \equiv 3 \pmod 4$. Hence we have a contradition.

We have thus shown that there are no solutions to the given equation.

---

1. Find all pairs (x, y) of positive integers such that $y^2 = x^3 + 7$.
2. Find all pairs (m, n) of positive integers such that $2^m + 3^n$ is a square.
3. Find all pairs (m, n) of positive integers such that $2^m + 3 = 11^n$.
4. Find all primes p such that $(2^{p-1} - 1)/p$ is a square.
5. Find all positive integers m and n such that $2^n - 1$ divides $m^2 + 9$.
6. Find all positive integers m and n such that $m^2 + n^2$ is a prime and it divides $m^3 + n^3 - 4$.
7. Find all pairs (x, y) of positive integers such that $\frac{x^7-1}{x-1} = y^5 - 1$.
8. For a positive integer n let $f(n)$ denote the smallest positive integer k such that n divides $1 + 2 + \cdots + k$. Find all positive integers n such that $f(n) = 2n - 1$.
9. Given an integer $k \geq 2$, prove that there infinitely many positive integers n such that $2^{2^n} + k$ is composite.