Notes on Number Theory

Manjil P. Saikia
(Diploma Student)
Mathematics Group
The Abdus Salam ICTP[*]
Strada Costiera 11
34151 Trieste, Italy
Email: manjil@gonitsora.com

July 4, 2014

Abstract

These are the sketch notes of the lectures delivered at Darrang College, Tezpur in July 2014 to Olympiad enthusiasts.

1 Lecture 1

The theory of numbers is a beautiful discipline of study in mathematics. It mainly concerns with the properties of integers and how they interplay with various other things. The modern study of numbers began with the publication of the classic book by Gauss, *Discourses in Arithmetics*. The subject has a rich history since time immemorial and has been studied by some of the greatest names of antiquity like Euclid, Pythagoras, etc. In these course of lectures, we shall attempt to give a very brief introduction to the theory of numbers from an Olympiad standpoint. We do not survey all of number theory, but only the very basic parts. The reader who is interested in pursuing the subject further may consult the beautiful textbooks [1] and [4]. For more problems, they may look into [2] and [3].

Before beginning our study, we fix the following notations. We denote by $\mathbb{N}$ the set of natural numbers, by $\mathbb{Z}$ the set of integers and by $\mathbb{Z}^+$ the set of all positive integers. We shall also employ the factorial notation $n!$ to denote the product of the first n natural numbers and the binomial coefficient $\binom{n}{r}$ to denote $\dfrac{n!}{r!(n-r)!}$.

The study of any subject begins with some prerequisites and in this lecture we shall study a few results that shall be useful to us in our further study.

We begin with the following principle called the **Well Ordering Principle (WOP)**, which states that *every nonempty set S of nonegative integers contains a least element.* This principle will be used to prove a few results as demonstrated below.

Proposition 1.1 (Archimedean Principle)**.** *If $a, b \in \mathbb{Z}^+$, then there exists $n \in \mathbb{N}$ such that $na \leq b$.*

Proof. We assume that $na < b$ for all such values of a, b and n. Then the elements of $S = \{b - na \mid n \in \mathbb{N}\}$ are all positive. So by the WOP, S has a least element, say $b - ma$. Also, $b - ma \in S$, so we have $b - (m+1)a < b - ma$ and hence this contradicts the minimality of $b - ma$. This, our initial assumption is wrong and hence this completes the proof. □

We now state and prove a result which has immense application and importance in all of mathematics, specially so in number theory.

[*] International Centre for Theoretical Physics

Theorem 1.2 (First principle of mathematical induction)**.** *Let S be a set of positive integers such that the following holds*

1. $1 \in S$, *and*
2. *If* $k \in S$, *then* $k+1 \in S$.

Then $S = \mathbb{N}$.

Proof. Let T be the set of all positive integers not in S, and let T be non-empty. Then by WOP we have a least element in T, say a. Since $1 \in S$, so $a > 1$ and hence $0 < a-1 < a$. Hence $a-1 \in S$. Thus, S must contain $(a-1)+1 = a$ also. So our assumption that T is non-empty is wrong. Hence $T = \phi$ and so $S = \mathbb{N}$. □

As an example, we have the following.

Example 1.3.

$$1+2+\cdots+n = \frac{n(n+1)}{2}.$$

Proof. Putting $n = 1$ in the above formula, we see that it is correct. So 1 is in the set of positive integers for which this formula holds. Now, we assume that the formula holds for some k, that is

$$1+2+\cdots+k = \frac{k(k+1)}{2}.$$

Adding $k+1$ to both the sides of the above formula and after some algebraic simplification, we get the following

$$1+2+\cdots+k+(k+1) = \frac{(k+1)(k+2)}{2}.$$

Hence the formula is verified for all $n \in \mathbb{N}$ by Theorem 1.2. □

There is another version of Theorem 1.2 which is stated below.

Theorem 1.4 (Second principle of mathematical induction)**.** *Let S be a set of positive integers such that the following holds*

1. $1 \in S$, *and*
2. *If* $1, 2, \ldots, k \in S$, *then* $k+1 \in S$.

Then $S = \mathbb{N}$.

The following exercises will give some idea of how to use the two forms of mathematical induction. In each case, prove the identities stated.

Exercise 1.5.

$$1^2+2^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Exercise 1.6.

$$1^3+2^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}.$$

Exercise 1.7.

$$1+2+2^2+\cdots+2^{k-1}+2^k = s^{k+1}-1.$$

Exercise 1.8 (Lucas' Sequence)**.** *We define the sequence $a_1 = 1$, $a_2 = 3$ and $a_n = a_{n-1} + a_{n-2}$ for all $n > 2$. Prove that $a_n < \frac{7^n}{4^n}$.*

Exercise 1.9 (Bernoulli's Inequality)**.** *If $1 + a > 0$, then prove that $(1+a)^n \geq 1 + na$.*

Exercise 1.10. *Prove that for $n \geq 1$, $2.6.10.14.\ldots.(4n-2) = \frac{(2n)!}{n!}$. Hence or otherwise, prove that $2^n(n!)^2 \leq (2n)!$ for all $n \geq 1$.*

We shall now state another result, first proved by Sir Issac Newton that is of paramount importance in elementary number theory below.

Theorem 1.11 (Binomial Theorem)**.** *For $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$, we have*

$$(a+b)^n = \binom{n}{0}a^n b^0 + \binom{n}{1}a^{n-1}b^1 + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}a^{n-(n-1)}b^{n-1} + \binom{n}{n}a^{n-n}b^n$$

or

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n. \tag{1.1}$$

The result is not very difficult to prove, and we leave the proof of this theorem as an exercise.

The following problems can be done using Theorem 1.11 or otherwise. In each case, prove the identity.

Exercise 1.12 (Newton)**.**

$$\binom{n}{k}\binom{k}{r} = \binom{n}{r}\binom{n-r}{k-r}.$$

Exercise 1.13 (Pascal)**.**

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

Example 1.14.

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Proof. We put $a = 1 = b$ in (1.1) to get the above identity. □

Exercise 1.15.

$$\binom{n}{0} - \binom{n}{1} + \cdots + (-1)^n\binom{n}{n} = 0.$$

Exercise 1.16.

$$\binom{n}{1} + 2\binom{n}{2} + \cdots + n\binom{n}{n} = n2^{n-1}.$$

We now come to a very important and fundamental result which we have been using since our primary school in various ways.

Theorem 1.17 (Division Algorithm)**.** *Given $a, b \in \mathbb{Z}$ with $b > 0$, there exists unique integers q and r satisfying $a = qb + r$ with $0 \leq r < b$.*

Proof. Let $S = \{a - xb \mid x \in \mathbb{Z}, a - xb \geq 0\}$. We now show that S is non-empty.

Since $b \geq 1$ we have $|a|\, b \geq |a|$ and so $a - (-|a|)b \geq a + |a| \geq 0$. Thus for $x = -|a|$, $a - xb \in S$ and hence S is non-empty.

Now, by the WOP, S has a least element say r. So, $r = a - qb$, where $r \geq 0$. Let if possible $r \geq b$, then $a - (q+1)b = (a - qb) - b = r - b \geq 0$. So, $a - (q+1)b \in S$. But $a - (q+1)b < r$ and hence is a contradiction. So, $r < b$.

Now suppose that $a = qb + r = q' + r'$, where $0 \leq r < b$ and $0 \leq r' < b$. Then $r - r' = b(q - q')$ and $|r' - r| = b\,|q - q'|$. We then get, $-b < -r \leq 0$ and $0 \leq r' < b$ and hence $-b < r' - r < b$ which implies $|r' - r| < b$ and hence $b\,|q - q'| < b$. So, $0 \leq |q - q'| < 1$.

Thus, $|q - q'| = 0$ and hence $q = q'$, $r = r'$. □

The following exercises uses the Division Algorithm in one form or the other.

Exercise 1.18. *Show that $a(a^2+2)/3$ is an integer for all $a \geq 1$.*

Exercise 1.19. *Prove that $3a^2 - 1$ is never a perfect square.*

Exercise 1.20. *Show that if n is an odd integer, then $n^4 + 4n^2 + 11$ is of the form $16k$.*

Exercise 1.21. *Prove that $n(n+1)(2n+1)/6$ is always an integer for all $n \in \mathbb{N}$.*

2 Lecture 2

In this lecture, we shall study about the greatest common divisor and its properties. We have already encountered the greatest common divisor or gcd in our school in the form of highest common factor. We shall use the notation (a, b) to denote the gcd of a and b and so on. Before going into it, let us fix the notation $a|b$ to mean that a divides b. We also have the following very easy properties that shall be used repeatedly.

Proposition 2.1. *If $a|b$ and $a|c$, then a divides any linear combination of b and c. Also, if $a|b$, then $b = aq$ for some integer q and hence $a \leq b$.*

Definition 2.2 (Greatest Common Divisor)**.** *The greatest common divisor of two integers a and b is said to be d if $d|a$, $d|b$ and for any c such that $c|a$, $c|b$, we have $c \leq d$. And we write $(a, b) = d$.*

The above definition can be easily extended to more than two numbers. If $(a, b) = 1$, then we say that a and b are co-prime to one another.

We have the following very important result for gcd function.

Theorem 2.3. *Given integers a and b, there exists integers x and y such that $(a, b) = ax + by$.*

Proof. Let $S = \{au + bv \mid au + bv \geq 0; u, v \in \mathbb{Z}\}$. Clearly S is non-empty, so by the WOP let $d = ax + by$ be the least element of S. We claim that $d = (a, b)$.

By the Division ALgorithm, we have for some q and r, $a = qd + r$, where $0 \leq r < d$. Hence

$$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy).$$

If $r > 0$, then $r \in S$ contradicting that d is the least element of S. So, $r = 0$ and hence $a = qd$ so that $d|a$. Similarly, we can show that $d|b$.

Now, if there is a c such that $c|a$ and $c|b$, then $c|(ax+by)$ and so $c \leq d$. Thus, $d = (a, b)$ and we are done. □

The following results are immediate from the above theorem.

Theorem 2.4. *For any two integers a and b, $(a, b) = 1$ if and only if $ax + by = 1$ for some $x, y \in \mathbb{Z}$.*

Corollary 2.5. *If $(a, b) = d$, then $(a/d, b/d) = 1$.*

Lemma 2.6 (Euclid)**.** *If $a|bc$ and $(a, b) = 1$, then $a|c$.*

The following exercises uses the results described in this section.

Exercise 2.7. *Show that $12|(a^2 + (a + 2)^2 + (a + 4)^2 + 1)$.*

Exercise 2.8. *Show that $6|a(a^2 + 11)$ for any $a \in \mathbb{N}$.*

Exercise 2.9. *Show that $24|a(a^2 - 1)$ for any odd $a \in \mathbb{N}$.*

Example 2.10. *Show that the product of four consecutive integers is one less than a perfect square.*

Proof. Let the four consecutive numbers be $a, a + 1, a + 2$ and $a + 3$. Then we have

$$\begin{aligned} a(a + 1)(a + 2)(a + 3) &= (a^2 + 3a)(a^2 + 3a + 2) \\ &= (a^2 + 3a)^2 + 2(a^2 + 3a). \end{aligned}$$

It is now a matter of simple algebra to complete the example. □

Exercise 2.11. *Prove that the sum of the squares of two odd integers cannot be a perfect square.*

Exercise 2.12. *Show that $(2a + 1, 9a + 4) = 1$.*

Example 2.13. *If $a|(b + c)$, is it true that $a|b$ or $a|c$?*

No, since $5|(3 + 2)$ and so on.

Exercise 2.14. *If $(a, b) = 1$, then show that $(a + b, a - b)$ is either 1 or 2.*

Exercise 2.15. *If $d|n$, then show that $2^d - 1|2^n - 1$.*

We are now in a position to state and prove another very interesting result called the Euclidean Algorithm. But before that we have the following simple lemma.

Lemma 2.16. *If $a = bq + r$ for some integers a, b, q and r, where $0 \leq r < b$ then we have $(a, b) = (b, r)$.*

Proof. The proof is very straightforward and is left as an exercise. □

Theorem 2.17 (Euclidean Algorithm)**.** *Given apair of integers a and b, we can get a set of equations as follows*

$$\begin{aligned}
a &= qb + r, 0 \leq r < b \\
b &= rq_1 + r_1, 0 \leq r_1 < r \\
r &= r_1q_2 + r_2, 0 \leq r_2 < r_1
\end{aligned} \tag{2.2}$$

$$\vdots$$

$$r_n = r_{n-1}q_n.$$

Then $(a, b) = r_{n-1}$.

Proof. This is a straightforward application of Lemma 2.16 and the proof is left as an exercise. □

The following is a beautiful application of the Euclidean Algorithm. This problem appeared in the first International Mathematical Olympiad (IMO) held in 1959 at Romania.

Exercise 2.18 (IMO (1959))**.** *For every integer n prove that $\dfrac{21n + 4}{14n + 3}$ cannot be reduced any further.*

3 Lecture 3

In this lecture, we shall study something about the structure of numbers and see why prime numbers are so important in mathematics. Infact, the study of prime numbers and the way in which they are distributed is the sole purpose of analytic number theory, a branch of number theory that uses complex analysis to derive results. We begin with a result which is so important that it has been called the **Fundamental Theorem of Arithmetic**.

Theorem 3.1 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ can be expressed as a product of primes, this representation is unique, apart from the order in which the factors occur.*

Proof. Either n is a prime or a composite. If it is a prime, then we have nothing to prove. So, we assume that n is composite. Then, there is some d such that $d|n$ and $1 < d < n$. We can choose the smallest such d by the WOP and say it is p_1. Then p_1 must be a prime else it would alse have some divisor q which will divide n also and thus contadict the minimality of p_1. So, we may write $n = p_1n_1$. Now we, repeat the process for n_1 and so on to get a representation of n as a product of some primes or powers of primes. The first part of the result now follows.

To prove the uniqueness part, we suppose that there are two such possible representations, and then it is an easy exercise to show that each prime in one representation corresponds to some prime in the other representation. □

Thus, we see that the prime numbers are the building blocks of all the integers and hence they are of utmost importance in number theory and in fact in all of mathematics. As a consequence of the above, we shall prove a remarkable result.

Theorem 3.2 (Euclid)**.** *There are infinitely many primes.*

Proof. Suppose, there were only finitely many primes say $p_1, p_2, \ldots, p_k$. Then we have a number

$$N + p_1 p_2 \cdots p_k + 1.$$

It is clear that neither of the p_i divides N for $i = 1, 2, \ldots, k$. So, either N is itself a new prime number, or some other prime not in our list divides N. Thus, we see that our list is incomplete and hence repeating this process over and over again will give us infinitely many primes. □

Using the fundamental theorem of arithmetic, we can now have the following result for two integers a and b.

Proposition 3.3. *For $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ where some of the p_i's can be zero, we have*

$$(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_k^{\min(a_k, b_k)}$$

and

$$[a, b] = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_k^{\max(a_k, b_k)},$$

where $[a, b]$ denotes the lowest common multiple of a and b.

Proof. The proof is left as an exercise. □

The problem of determining which number is a prime number has left mathematicians baffled for centuries. One of the first methods derived to find out which numbers upto and including a particular number is prime was first given by Eratosthenes and is called the **Sieve of Eratosthenes**. In this method, first we list all the numbers from 1 to n, then we cross out 1 since it is not a prime, and then keep the next number and cross out all its multiples. After this is done, we keep the next uncrossed number and cross out all it multiples. We keep on repeating this process untill no more crossing out is possible. The numbers that remains are the prime numbers upto and including n.

Theorem 3.4 (Pythagoras). *$\sqrt{2}$ is irrational.*

Proof. Suppose $\sqrt{2}$ is rational, say $\sqrt{2} = \frac{a}{b}$, then $2b^2 = a^2$. This implies that $2|a$, because here we have implicitly assumed $(a, b) = 1$. Thus, $a = 2k$ for some integer k. So, we now have $b^2 = 2k^2$ and hence by a similar logic $2|b$, which shows that (a, b) is not one. Thus our assumption that $\sqrt{2}$ is irrational is wrong and hence we have the result. □

The following exercises can be done using some of the techniques of this section or some of the techniques that the reader may have learned in school.

Exercise 3.5. *Prove that any prime of the form $3m + 1$ is also of the form $6m + 1$.*

Exercise 3.6. *How many zeroes are there at the end of 2014!?*

Exercise 3.7. *Prove that every integer of the form $n^4 + 4$ for $n > 1$ is composite.*

Exercise 3.8. *Show that 5 is the only prime of the form $n^2 - 4$.*

Exercise 3.9. *Show that any integer can be written as $n = 2^k m$ for $k \geq 0$ and odd m.*

Exercise 3.10. *Prove that $\sqrt{p}$ is irrational for any prime p.*

There is an important class of functions called arithmetic functions that appear in number theory. We shall not discuss these functions here, except the following two examples; but the interested reader can look into [1] for more details.

Exercise 3.11. *We define the arithmetic function $\tau(n)$ to be the number of factors of n. Show that*

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

for $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

Exercise 3.12. *We define the arithmetic function $\sigma(n)$ to be the sum of the divisors of n. Show that*

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{a_1})(1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{a_k})$$

for $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

4 Lecture 4

In this lecture, we shall study about congruences and a few of their properties. The idea of congruences was first put forward by the great mathematician *Carl F. J. Gauss* in his book *Disquisitiones Arithmeticae* which he wrote when he was just 24 years old.

Definition 4.1. *Let n be a fixed positive integer and two integers a and b are said to be congruent to each other modulo n if $n|(a-b)$ and we write it as $a \equiv b \pmod{n}$.*

An easy consequence of the above definition is the following theorem, the proof of which is left as an exercise.

Theorem 4.2. *For arbitary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b leave the same remainder when divided by n.*

We also have the following basic properties of congruences.

Proposition 4.3. *Let $n > 1$ be fixed and a, b, c, d be arbitary integers. Then the following properties hold:*

1. $a \equiv a \pmod{n}$,
2. *If* $a \equiv b \pmod{n}$ *then* $b \equiv a \pmod{n}$,
3. *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$,
4. *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ *and* $ac \equiv bd \pmod{n}$,
5. *If* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$, *and*
6. *If* $a \equiv b \pmod{n}$, *then* $a^k \equiv b^k \pmod{n}$ *for any positive integer* k.

The proof of the above is very easy, we shall just show the proof of (3) in the above and the rest is left as an exercise.

Proof. Suppose $a \equiv b \pmod{n}$ and also $m \equiv c \pmod{n}$. Then there exists integers h and k satisfying $a-b = hn$ and $b - c = kn$. It follows that $a - c = (a - b) + (b - c) = (h + k)n$ and hence $a \equiv c \pmod{n}$. □

Exercise 4.4. *Find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 12.*

Exercise 4.5. *Show that 41 divides $2^{20} - 1$.*

Theorem 4.6. *If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = (c, n)$.*

Proof. We have $c(a - b) = kn$ for some integer k. If $(c, n) = d$, then there exists some relatively prime integers r and s such that $c = dr$ and $n = ds$. Thus, we have $r(a - b) = ks$. Hence $s|r(a - b)$ and $(r, s) = 1$. So Lemma 2.6 yields $s|(a - b)$ which is nothing but what we wanted. □

The following are some easy consequences of the above theorem.

Corollary 4.7. *If $ca \equiv cb \pmod{n}$ and $(c, n) = 1$, then $a \equiv b \pmod{n}$.*

Corollary 4.8. *If $ca \equiv cb \pmod{p}$ and p does not divide c where p is a prime number, then $a \equiv b \pmod{p}$.*

Exercise 4.9. *What is the remainder when the following sum is divided by 4?*

$$1^5 + 2^5 + \cdots + 99^5 + 100^5$$

Exercise 4.10. *If p is a prime satisfying $n < p < 2n$, then show that*

$$\binom{2n}{n} \equiv 0 \pmod{p}.$$

Now, we shall discuss two very important results in the theory of congruences and then end our course.

Theorem 4.11 (Fermat's Little Theorem (FLT))**.** *Let p be a prime and suppose that p does not divide a. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Corollary 4.12. *If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.*

The proof of the above theorem is not very difficult, but we omit it here for lack of time. The proof can be found in [1].

Exercise 4.13. *If p and q are distinct primes, then prove that*

$$p^{q-1} + q^{p-1} \equiv 1 \text{ (mod } pq).$$

Exercise 4.14. *Prove that $2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$.*

Exercise 4.15. *Prove that for any integer n, $13|(11^{12n+6} + 1)$.*

Exercise 4.16. *If p is an od prime, then prove that*

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

The next important result is the following.

Theorem 4.17 (Wilson)**.** *If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.*

The proof is a little more involved than the proof of Theorem 4.11 and the interested reader can consult [1] for a proof of Theorem 4.17.

Exercise 4.18. *Determine whether 17 is a prime using Theorem 4.17.*

Exercise 4.19. *Verify that $4(29)! + 5!$ is divisible by 31.*

Exercise 4.20. *Given any prime number p, prove that*

$$(p-1)! \equiv p-1 \text{ (mod } 1 + 2 + 3 + \cdots + (p-1)).$$

Exercise 4.21. *If p is a prime, prove that for any integer a, $p|(a^p + (p-1)!a)$ and $p|((p-1)!a^p + a)$.*

5 Problems

In this section, we list a few problems without solution which uses some of the techniques that we have discussed so far. It must be however noted that some of the problems may be quite difficult and the reader is advised not to get frustrated if he or she is unable to solve a problem in the first attempt. Some of the problems can be found in the references listed below and may use techniques which have not been discussed so far.

Exercise 5.1.

- *Find all natural numbers n for which 7 divides $2^n - 1$.*
- *Prove that there is no natural number n for which 7 divides $2^n + 1$.*

Exercise 5.2. *Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1, \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \cdots k_n - 1$ is the product of two consecutive integers.*

Exercise 5.3. *Determine the values of the positive integer n for which*

$$\sqrt{\frac{9n-1}{n+7}}$$

is rational.

Exercise 5.4. *Suppose a, b are integers satisfying $24a^2 + 1 = b^2$. Prove that exactly one of a, b is divisible by 5.*

Exercise 5.5. *Let $x = abcd$ be a 4-digit number such that the last 4 digits of x^2 are also abcd. Find all possible values of x.*

Exercise 5.6. *Let a and b be positive integers and let $u = a + b$ and $v = lcm(a, b)$. Prove that*

$$gcd(u, v) = gcd(a, b).$$

Exercise 5.7. *Determine the units digit of the numbers a^2, b^2 and ab (in base 10), where*

$$a = 2^{2002} + 3^{2002} + 4^{2002} + 5^{2002}$$

and

$$b = 3^1 + 3^2 + 3^3 + \cdots + 3^{2002}.$$

Exercise 5.8. *Let p be an odd prime. Let k be a positive integer such that $\sqrt{k^2 - pk}$ also a positive integer. Find k.*

Exercise 5.9. *An integer $n > 1$ has the property, that for every (positive) divisor d of n, d + 1 is a divisor of n + 1. Prove that n is prime.*

Exercise 5.10. *Let N be the number of ordered pairs (x, y) of integers such that*

$$x^2 + xy + y^2 \leq 2007.$$

Prove that N is odd.

Exercise 5.11. *Given a finite set P of prime numbers, there exists a positive integer x such that it can be written in the form $a^p + b^p$ (a, b are positive integers), for each $p \in P$, and cannot be written in that form for each p not in P.*

Exercise 5.12. (Primitive Pythagoras Triangles) *Let $x, y, z \in \mathbb{N}$ with $x^2 + y^2 = z^2$, $gcd(x, y) = 1$, and $x \equiv 0 \pmod 2$ Then, there exists positive integers p and q such that $gcd(p, q) = 1$ and*

$$(x,\ y,\ z) = \left(2pq,\ p^2 - q^2,\ p^2 + q^2\right).$$

Exercise 5.13. *The equation $x^4 + y^4 = z^2$ has no solution in positive integers.*

Exercise 5.14. *Let a and b be positive integers. Show that if $4ab - 1$ divides $\left(4a^2 - 1\right)^2$, then $a = b$.*

Exercise 5.15. *Let $\mathbb{N} = \{1, 2, 3, \cdots\}$ denote the set of positive integers. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that for all m, $n \in \mathbb{N}$: $f(2) = 2$, $f(mn) = f(m)f(n)$, $f(n + 1) > f(n)$.*

Exercise 5.16. *Is $4^{545} + 545^4$ a prime?*

Russia

Exercise 5.17. *If $n > 1$, then prove that $n^4 + 4^n$ is never a prime.*

Kürschak, 1978

Exercise 5.18. *Can a number, A consisting of 600 sixes and some zeroes be a square?*

Exercise 5.19. *Prove that the equation $15x^2 - 7y^2 = 9$ has no integral solutions.*

Exercise 5.20. *Show that the equation $x^2 + y^2 + z^2 = 2xyz$ has no integral solutions except $x = y = z = 0$.*

Exercise 5.21. *Prove that a number with 3^n equal digits is divisible by 3^n.*

Exercise 5.22. *How many zeroes are at the end of 2012!?*

Exercise 5.23. *Prove that $1000\ldots001$ with 1961 zeroes is composite.*

Exercise 5.24. *If $n \in \mathbb{N}$ and $3n + 1$ and $4n + 1$ are perfect squares, then prove that $56 \mid n$.*

Exercise 5.25. *Given seven distinct integers that add up to* 100*, prove that some three of them add upto at least* 50*.*

Exercise 5.26. *Consider* $2n$ *distinct positive integers* $a_1, a_2, \ldots, a_{2n}$ *not exceeding* n^2*, where* $n > 2$*. Prove that some three of the differences* $a_i - a_j$ *are equal.*

Exercise 5.27. *Consider seven distinct positive integers not exceeding* 1706*. Prove that there are three of them say* a, b, c *such that* $a < b + c < 4a$*.*

Exercise 5.28. *Prove that for every positive integer* m*, there is a positive integer* n *such that* $m + n + 1$ *is a perfect square and* $mn + 1$ *is a perfect cube.*

Exercise 5.29. *Show that* $\frac{(2m)!(2n)!}{(m+n)!m!n!}$ *is an integer.*

Exercise 5.30. *Prove that* $36^{41} + 41^{36}$ *is divisible by* 77*.*

6 Concluding Remarks

In these lecture notes, an attempt has been made to show some of the theory and applications of elementary number theory. Since number theory is a vast subject so it is not possible to show all the beauties of the subject is just four lectures. The choice of the material that is presented here is purely at the discretion of the author and in no way reflects the sort of things that attract the attention of number theorists. However, it is believed that with this background, any interested reader can pursue the subject further on his own. For the reader who wants to know more about the subject, a good starting place is [1] and if he wants to know more advanced topics then the author's favourite book is [4]. For the sort of problems that appear in mathematical olympiads, a good place to look for is [2] and [3]. The author's website [5] also contains lot of problems and materials for olympiad students.

Acknowledgements

I would like to thank Ram Charan Deka for the kind invitation to deliver these lectures and the support of the Assam Academy of Mathematics.

References

[1] D. M. Burton, *Elementary Number Theory* 6th ed., Tata McGraw Hill, 2007.

[2] D. Djukić, V. Janković, I. Matić and N. Petrović, *The IMO Compedium* 2nd ed., Springer, 2010.

[3] P. J. Mahanta and M. P. Saikia, *The Pursuit of Joy, Volume I*, LAP Lambert Academic Publishing, Germany, 2011.

[4] M. B. Nathanson, *Methods in Number Theory*, GTM 195, Springer, 2000.

[5] M. P. Saikia, *http://www.manjilsaikia.in/olympiads/*, 2013 – 2014.