

# Number Theory

2018A7PS0193P



## CHAPTER 1

### Fundamentals

#### 1. Notation

For the rest of this course, the following notation will be followed:

- (1)  $\mathbb{N}$  is the set of natural numbers
- (2)  $\mathbb{Z}$  is the set of integers
- (3)  $\mathbb{W}$  is the set of whole numbers, i.e.  $\mathbb{W} = \mathbb{N} \cup \{0\}$

#### 2. Induction

Often in number theory, we use inductive proofs to prove our arguments. Induction consists of the following steps:

- (1) Define an induction hypothesis  $P(k)$
- (2) Verify it works for some base case  $k = b$ . It is possible multiple base cases need to be verified.
- (3) Assuming  $P(k)$  is true, show that it implies that  $P(k + 1)$  is true

Remember that  $P(k)$  is a statement, not a function. You cannot multiply it by some constant or perform any operations on it.

In weak induction (like in the steps given above), we only assume that  $P(k)$  is true. However in strong induction, we assume that  $P(i)$  is true  $\forall i \in [b, k]$ , and use this to prove that  $P(k+1)$  is true.

EXERCISE. Prove that the principle of strong induction is true given that the principle of weak induction is true.

SOLUTION. Let us assume that  $P(1), \dots, P(b)$  is true. If  $P(1), \dots, P(k)$  are true for some  $k \geq b$ , then  $P(k + 1)$  is true. Then, we must show that  $P(n)$  is true for all  $n \geq 1$ .

Let  $Q(n)$  be the statement that  $P(1), \dots, P(n)$  are true. Of course, in the base case,  $Q(1)$  is true. Let  $Q(k)$  be true, where  $K \geq 1$ . This means that  $P(1), \dots, P(k)$  is true, so  $P(k + 1)$  must be true. Hence,  $Q(k + 1)$  is true.

So, by Weak induction,  $Q(n)$  is true  $\forall n \geq 1$ , which implies that  $P(n)$  is true  $\forall n \geq 1$ . ■

### 3. Well Ordering Principle

**THEOREM 3.1** (Well Ordering Principle). Every non empty set of non-negative integers has a least element.

This is not true about negative integers - consider the case of infinite sets, like the set of all integers. There is no well defined least element.

**LEMMA 3.2.** The well ordering principle is equivalent to the principle of mathematical induction.

**PROOF.** First, let us prove that WOP  $\Rightarrow$  PMI. Let  $P(n)$  be a statement that depends on  $n \in \mathbb{N}$ . Suppose that:

- $P(1)$  is true
- $P(k)$  is true implies  $P(k+1)$  is true for all  $k \in \mathbb{N}$ .

We have to show that  $P(n)$  is true for all  $n \in \mathbb{N}$ . Let :

$$S = \{n \in \mathbb{N} : P(n) \text{ is true}\}$$

This means we must show that  $S = \mathbb{N}$ . Let  $T := \mathbb{N} \setminus S$ , i.e.  $T$  is the complement. Let us assume that  $S \neq \mathbb{N}$ .

By WOP,  $T$  has a least element, say  $m$ . Note that  $m \geq 2$  since  $1 \in S$ . Then,  $m-1 \notin T$  and  $m-1 \in S$ . As such,  $P(m-1)$  must be true! However, by our initial assumptions, that would mean  $P(m)$  is true as well, so  $m \in S$ . This creates a contradiction, since  $m \in T$ . Hence,  $S = \mathbb{N}$ .

Now, let us prove that PMI  $\Rightarrow$  WOP.

Consider the statement  $P(n)$  that every non empty set of non-negative integers of size  $n$  has a least element. It is clear that the base case  $P(1)$  is true. Now, let us assume that  $P(k)$  is true - what can we say about  $P(k+1)$ . When we insert an element, we have two cases:

- (1) The inserted element is less than the least element. In this case, there is a new least element, and  $P(k+1)$  is true.

- (2) The inserted element is not less than the least element. In this case, the least element is the same, and  $P(k+1)$  is true.

Hence, by PMI, we can say that  $P(n)$  is true  $\forall n \in \mathbb{N}$ , i.e., WOP is true.

Since  $\text{PMI} \Rightarrow \text{WOP}$  and  $\text{WOP} \Rightarrow \text{PMI}$ ,  $\text{PMI} \Leftrightarrow \text{WOP}$ .

□

#### 4. Binomial Theorem

**THEOREM 4.1** (Binomial Theorem). Let  $x, y \in \mathbb{C}$  and let  $n \in \mathbb{N}$ , then

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

**COROLLARY 4.1.1.**

$$\sum_{k=0}^n \binom{n}{k} = 2^n$$

**LEMMA 4.2** (Pascal's Identity).

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

**LEMMA 4.3.**

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n-k}{k} = F_n$$

#### 5. Pigeonhole Principle

**THEOREM 5.1.** If  $n$  items are put into  $m$  containers, with  $n > m$ , then at least one container must contain more than one item.



## CHAPTER 2

### Division

#### 1. Division Algorithm

**THEOREM 1.1.** Let  $a, b \in \mathbb{Z}$  with  $b > 0$ . Then, there exist unique integers  $q$  and  $r$  such that  $a = bq + r$ ,  $r \in [0, b)$ .

**PROOF.** Let  $S = \{a - bn : n \in \mathbb{Z}, a - bn \geq 0\}$ . This set is always non-empty:

- If  $a \geq 0$ , then  $a \in S$
- If  $a < 0$ , then if  $n = a$ , we have  $a - ab \in S$  since  $b \geq 1$ .

By WOP,  $S$  has a least element, say  $r$ . So, there exists  $q \in \mathbb{Z}$  such that  $r = a - bq$ . Since  $r \in S$ , we have  $r \geq 0$ .

Suppose  $r \geq b$ . Then:

$$\begin{aligned} a - b(q + 1) &= a - bq - b = r - b \geq 0 \\ &\Rightarrow a - b(q + 1) \in S \\ &\Rightarrow r - b \in S \end{aligned}$$

However,  $r - b < r$ , and  $r$  is the least element! This gives us a contradiction. So,  $r < b$ .

As such, we have proved the existence of this solution. Now we must prove it's uniqueness.

Suppose there exists  $p, r, q', r'$ , such that:

$$\begin{aligned} a &= bq + r, 0 \leq r < b \\ a &= bq' + r', 0 \leq r' < b \end{aligned}$$

Assume WLOG  $q \geq q'$ . Now,

$$r' - r = b(q - q')$$

If  $q > q'$ , then  $r' - r \geq b$ . However,  $r' - r < b$ . So, this is a contradiction, and  $q' = q$ . The solution must be unique.

□

DEFINITION 1. If  $a, b \in \mathbb{Z}$ , we say that  $a$  divides  $b$  if  $b = ak$  for some  $k \in \mathbb{Z}$ . This is denoted by  $a|b$

Some properties of division are:

- If  $a|b$ , then  $\pm a|\pm b$
- If  $a|b$  and  $b|c$  then  $a|c$  (Transitivity)
- If  $a|b$  and  $a|c$  then  $a|bx + cy$  (Linear Combination)
- If  $a|b$  and  $b \neq 0$ , then  $|a| \leq |b|$  (Bounds by divisibility)
- $a|b$  and  $b|a$ , then  $b = \pm a$ .

## 2. Base $b$ representations

THEOREM 2.1. Let  $b \in \mathbb{N}$  with  $b \geq 2$ . Then every positive integer can be expressed uniquely as

$$N = a_k b^k + \dots + a_1 b + a_0$$

where  $k \geq 0, a_k \neq 0$  and  $0 \leq a_i < b$  for  $i = 0, \dots, k$ . This is denoted by  $N = (a_k, \dots, a_1 a_0)_b$

PROOF. By the division algorithm, there exist unique integers  $q_0$  and  $a_0$  such that:

$$N = q_0 b + a_0, a_0 \in [0, b)$$

Note that  $q_0 < N$ . If  $q_0 \neq 0$  we apply the division algorithm again to find unique integers  $q_1$  and  $a_1$  such that:

$$q_0 = q_1 b + a_1, a_1 \in [0, b)$$

Then,

$$N = (q_1 b + a_1)b + a_0 = q_1 b^2 + a_1 b + a_0$$

We continue till we get a quotient  $q_k = 0$ . This will terminate since  $q_k < \dots < q_2 < q_1 < q_0 < N$ , forming a decreasing sequence of non-negative integers and eventually reaching zero. From this, we get:

$$N = a_k b^k + \dots + a_1 b + a_0$$

Hence, the solution always exists.



Suppose  $N$  has two distinct expansions. We can write it as:

$$\begin{aligned} N &= a_k b^k + \dots + a_1 b + a_0 \\ &= c_k b^k + \dots + c_1 b + c_0 \end{aligned}$$

where  $0 \leq a_i, c_j < b$  for all  $i, j$ . Let  $d_i = a_i - c_i$ . Then,  $\sum_{i=0}^k d_i b^i = 0$ . The  $d_i$  cannot all be zero as the two expansions are assumed distinct. Let  $j$  be the least integer,  $0 \leq j \leq k$ , such that  $d_j \neq 0$ . Then,  $\sum_{i=j}^k d_i b^i = 0$ . Dividing by  $b^j$ , we find that  $\sum_{i=j}^k d_i b^{i-j} = 0$ . Thus,

$$d_j + b \left( \sum_{i=j+1}^k d_i b^{i-j-1} \right) = 0$$

This implies that the  $b|d_j$  and since  $d_j \neq 0$ , we get that  $b = |b| \leq |d_j|$ . However,  $|d_j| < b$ . Hence, we have a contradiction, and the two expansions cannot be distinct. Hence, the solution is also always unique.  $\square$

LEMMA 2.2. If  $N = (a_k \dots a_1 a_0)_b$ , then:

$$\begin{aligned} bN &= (a_k \dots a_1 a_0 0)_b \\ \left\lfloor \frac{N}{b} \right\rfloor &= (a_k \dots a_1)_b \end{aligned}$$

This is a trivial result, which can be thought of as a left or right bitwise shift.

LEMMA 2.3 (Particular case of Legendre's formula). Let  $n \in \mathbb{N}$  and let  $e$  denote the highest power of 2 dividing  $n!$ . Then

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$$

This is always a finite sum. This can alternatively expressed as, if  $n = (a_k \dots a_1 a_0)_2$ , then:

$$e = n - (a_k + \dots + a_1 + a_0)$$

PROOF. It is clear that  $e$  is the sum of the no. of positive multiples of  $2^i$  which are  $\leq n$ , for all  $i$ . So, this can be calculated by:

$$e = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{2^k} \right\rfloor$$

$\square$

Thus, if  $r$  denotes the number of ones in the binary expansion of  $n$ , then  $2^{n-r}$  is the highest power of 2 dividing  $n!$ . Further,

- $2^n \nmid n!$  for  $n \in \mathbb{N}$
- $2^{n-1} \mid n!$  if and only if  $n$  is a power of 2.

## CHAPTER 3

### Properties of Numbers

#### 1. Prime and Composite Numbers

DEFINITION 2. A positive integer  $p > 1$  is called prime if its only positive divisors are 1 and  $p$ . A positive integer which is not prime is called composite.

The number 1 is neither prime nor composite.

LEMMA 1.1. Every integer  $n \geq 2$  has a prime factor.

PROOF. Let  $P(n)$  be the statement that  $n$  has a prime factor. Then  $P(2)$  is true, since 2 is a prime factor of 2. Let  $k \geq 2$ . Assume  $P(2) \dots P(k)$  are true.

If  $k + 1$  is prime, then  $k + 1$  is a prime factor of itself. So  $P(k + 1)$  is true.

If  $k + 1$  is composite, then there exists  $d \in [2, k]$  such that  $d | k + 1$ . By the induction hypothesis,  $d$  has a prime factor  $p$ . Since  $p | d$  and  $d | k + 1$ ,  $p | k + 1$ . So  $p$  is a prime factor of  $k + 1$ , and  $P(k + 1)$  is true. By PSI,  $P(n)$  is true for all  $n \geq 2$ .  $\square$

THEOREM 1.2 (Euclid). There are infinitely many primes.

PROOF. Suppose there are finitely many primes  $p_1, \dots, p_k$ . Let

$$N = p_1 \dots p_k + 1$$

Since  $N \geq 2$ , it must have a prime factor. Hence, there exists  $i \in [1, k]$  such that  $p_i | N$ . Since  $p_i | N$  and  $p_i | p_1 p_2 \dots p_k$ , we get that  $p_i | N - p_1 p_2 \dots p_k$ , i.e.,  $p_i | 1$ . However,  $p_i \geq 2$ , which gives us a contradiction. So, there must be infinitely many primes.  $\square$

EXERCISE. For  $n \geq 1$ , let  $p_n$  be the  $n$ th prime. Prove that

$$p_n \leq 2^{2^{n-1}}$$

SOLUTION. Let  $P(n)$  be the statement that  $p_n \leq 2^{2^{n-1}}$ . It is clear that this is true for the base case  $P(1)$ . Let us assume that  $P(1), \dots, P(k)$  is true for  $k \geq 1$ . We observed in

Euclid's proof that  $p_1 \dots p_k + 1$  is not divisible by any of  $p_1 \dots p_k$ . Hence if  $p_i$  denotes a prime factor of  $p_1 \dots p_k + 1$ , then  $i \geq k + 1$ .

$$p_{k+1} \leq p_i \leq p_1 \dots p_k + 1$$

Using the inductive hypothesis, we find that

$$\begin{aligned} p_{k+1} &\leq p_1 \dots p_k + 1 \leq 2 \cdot 2^2 \cdot 2^{2^2} \dots 2^{2^{k-1}} + 1 \\ &= 2^{\sum_{j=0}^{k-1} 2^j} + 1 = 2^{2^k - 1} + 1 \leq 2^{2^k} \end{aligned}$$

So,  $P(k + 1)$  is true. So, by PSI, the result has been proven. ■

DEFINITION 3. The product of the first  $n$  prime numbers is called the  $n^{th}$  primorial and is denoted by  $p_n\#$ .

DEFINITION 4. Euclid numbers are integers of the form  $E_n = p_n\# + 1$ .

All Euclid numbers are not primes -  $E_6$  is not a prime!

THEOREM 1.3. Every composite number  $n$  has a prime factor  $\leq \lfloor \sqrt{n} \rfloor$

PROOF. Since  $n$  is composite, there exists integers  $k, l \in (1, n)$  such that

$$n = kl$$

If  $k > \sqrt{n}$  and  $l > \sqrt{n}$  then  $kl > n$ , which is false. So, one of them must be less than or equal to  $\sqrt{n}$ . □

So, if  $n > 1$  has no prime factors  $\leq \lfloor \sqrt{n} \rfloor$ , then  $n$  is prime. We can use this as a test of primality.

It is faster to do this using the Sieve of Eratosthenes. Using this, we can test primality of the first  $n$  integers in  $O(n \log \log n)$  instead of  $O(n\sqrt{n})$ .