

# Notes on Number Theory

October 19, 2023

## Contents

<b>1</b>	<b>Logic</b>	<b>2</b>
<b>2</b>	<b>Binomial Theorem</b>	<b>3</b>
2.1	Proof of Binomial Theorem . . . . .	3
<b>3</b>	<b>Modular Arithmetic</b>	<b>5</b>
3.1	Divisibility . . . . .	5
3.1.1	Division Algorithm . . . . .	5
3.1.2	Congruences . . . . .	6
<b>4</b>	<b>Abstract Algebra</b>	<b>7</b>
4.1	Preliminaries . . . . .	7
4.1.1	Division Algorithm . . . . .	7

# 1 Logic

Original Statement	$P \rightarrow Q$
Contrapositive	$\neg Q \rightarrow \neg P$
Converse	$Q \rightarrow P$
Inverse	$\neg P \rightarrow \neg Q$

Table 1: The contrapositive is equivalent to the original statement; the Converse to the inverse.

## 2 Binomial Theorem

### 2.1 Proof of Binomial Theorem

The following was taken from an exercise in chapter 1 of Complex Variables and Applications from Brown and Churchill.

Use mathematical induction to verify the binomial formula. More precisely, note that the formula is true when  $n = 1$ . Then, then assuming it is valid when  $n = m$  where  $m$  denotes any positive integer, show that it must hold when  $n = m + 1$ .

Suggestion: when  $n = m + 1$ , write

$$\begin{aligned}(z_1 + z_2)^{m+1} &= (z_1 + z_2)(z_1 + z_2)^m = (z_1 + z_2) \sum_{k=0}^m \binom{m}{k} z_1^k z_2^{m-k} \\ &= \sum_{k=0}^m \binom{m}{k} z_1^k z_2^{m+1-k} + \sum_{k=0}^m \binom{m}{k} z_1^{k+1} z_2^{m-k}\end{aligned}$$

Reaplace  $k$  by  $k - 1$  in the last sum. To see how this would work take this example,

$$\sum_{k=0}^{n-1} ar^k = \sum_{k=1}^n ar^{k-1}$$

So

$$\begin{aligned}\sum_{k=0}^m \binom{m}{k} z_1^{k+1} z_2^{m-k} &= \sum_{k=1}^{m+1} \binom{m}{k-1} z_1^k z_2^{m-(k-1)} \\ &= \sum_{k=1}^{m+1} \binom{m}{k-1} z_1^k z_2^{m+1-k} \\ &= \sum_{k=1}^m \binom{m}{k-1} z_1^k z_2^{m+1-k} + z_1^{m+1}\end{aligned}$$

Note that in the last operation we explicitly did the very last summation to reduce the summation back from  $k$  to  $m$ .

Then we can take the sum we didn't shift as

$$\sum_{k=0}^m \binom{m}{k} z_1^k z_2^{m+1-k} = z_2^{m+1} + \sum_{k=1}^m \binom{m}{k} z_1^k z_2^{m+1-k}$$

Putting these back together we get

$$(z_1 + z_2)^{m+1} = z_2^{m+1} + \sum_{k=1}^m \left[ \binom{m}{k} + \binom{m}{k-1} \right] z_1^k z_2^{m+1-k} + z_1^{m+1}$$

One more thing to note, is that the binomial coefficients met the following recurrence relation

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

Note that

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

and

$$\binom{n}{k-1} = \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!}{(k-1)!(n-k+1)(n-k)!}$$

So

$$\begin{aligned} \binom{n}{k} + \binom{n}{k-1} &= n! \left[ \frac{1}{k(k-1)!(n-k)!} + \frac{1}{(k-1)!(n-k+1)(n-k)!} \right] \\ &= n! \left[ \frac{n-k+1}{k(k-1)!(n-k+1)(n-k)!} + \frac{k}{k(k-1)!(n-k+1)(n-k)!} \right] \\ &= n! \left[ \frac{n-k+1+k}{k(k-1)!(n-k+1)(n-k)!} \right] \\ &= n! \left[ \frac{(n+1)n!}{k(k-1)!(n-k+1)(n-k)!} \right] \\ &= \frac{(n+1)!}{k!(n-k+1)!} \\ &= \binom{n+1}{k} \end{aligned}$$

Using this result, we can rewrite our previous sum as

$$\begin{aligned} (z_1 + z_2)^{m+1} &= z_2^{m+1} + \sum_{k=1}^m \left[ \binom{m}{k} + \binom{m}{k-1} \right] z_1^k z_2^{m+1-k} + z_1^{m+1} \\ &= z_1^{m+1} + z_2^{m+1} + \sum_{k=1}^m \binom{m+1}{k} z_1^k z_2^{m+1-k} \end{aligned}$$

Now the magic is in seeing that the 2 stragglers are the "endpoint" terms of a binomial expansion: think how  $(x+y)^2 = x^2 + 2xy + y^2$ , the first and last term are raised to the  $n$ -th power of the binomial expansion and have a coefficient of 1 (and this pattern is seen in all such expansions). This means we can start the sum at  $k=0$  by including  $z_1^{m+1}$  and end the sum at  $m+1$  by adding the  $z_2^{m+1}$  term, thus

$$(z_1 + z_2)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} z_1^k z_2^{m+1-k}$$

## 3 Modular Arithmetic

### 3.1 Divisibility

Rosen's "Discrete Mathematics and its Applications"'s chapter 4 along with Gallian's "Contemporary Abstract Algebra" chapter 0 make great references for this material.

An  $a \neq 0 \in \mathbb{Z}$  is called a **divisor** of a  $b \in \mathbb{Z}$  if there is a  $c \in \mathbb{Z}$ , such that  $b = ac$ . We write  $a|b$ , "a divides b". We also commonly say that "b is a multiple of a".

Note that this working definition means that  $a|b$  is an integer. So for example,  $3 \nmid 7$  since  $7/3 \notin \mathbb{Z}$  but  $3|12$  since  $12/3 \in \mathbb{Z}$ .

If  $n$  and  $d$  are positive integers, how many positive integers not exceeding  $n$  are divisible by  $d$ ?

In order to be divisible by  $d$ , an integer must be of the form  $dk$ , for some positive integer  $k$ . So the integers divisible by  $d$  and not greater than  $n$  are the integers with  $k$  such that  $0 \leq dk < n$  or  $0 < k < n/d$ . Thus, the number of integers divisible by  $d$ , not exceeding  $n$ , is  $\lfloor n/d \rfloor$ .

**Theorem describing the transitive properties of division:**

$$\text{If } a|b \text{ and } a|c, \text{ then } a|(b+c) \quad (3.1)$$

To prove this use the fact that  $a|b$  means that  $b = as$ ,  $a|c$  means that  $c = at$ , and  $b + c = a(s + t)$ . Hence  $a|(b + c)$ .

$$\text{If } a|b, \text{ then } a|bc, \text{ for } c \in \mathbb{Z} \quad (3.2)$$

To prove it use the fact that  $a|b$  means  $b = as$ , so  $b * c = as * c$ .

$$\text{If } a|b, \text{ and } b|c, \text{ then } a|c \quad (3.3)$$

To prove it use  $b = as$ ,  $c = bt$ . Then  $c = bt = ast$  and hence  $a|c$ .

**Corollary: If a, b, and c are integers, where  $a \neq 0$ , such that  $a|b$  and  $a|c$ , then  $a|mb + nc$  whenever  $m, n \in \mathbb{Z}$ .**

Use if  $a|b$  and  $a|c$ , then  $a|(b + c)$  and if  $a|b$ , then  $a|bc$ , for  $c \in \mathbb{Z}$ , to prove it.

#### 3.1.1 Division Algorithm

- If  $a = dq + r$  where  $0 \leq r < d$  and  $d > 0$

- $q = a \text{ div } d = \lfloor a/d \rfloor$
- $r = a \pmod{d} = a - dq$

For example, when 101 is divided by 11,  $11|101$

$$101 = 11 \cdot 9 + 2$$

When -11 is divided by 3,  $3|-11$

$$-11 = 3 \cdot (-4) + 1$$

### 3.1.2 Congruences

If  $a$  and  $b$  are congruent modulo  $m$  ( $a, b \in \mathbb{Z}, m > 0$ ),  $a \equiv b \pmod{m}$ , then  $m$  divides  $a - b$ . Another way of seeing it is that  $a$  and  $b$  have the same remainder when divided by  $m$ .

If  $m$  divides  $a - b$ , then  $a - b = mc$  for some integer  $c$ .

If both  $a$  and  $b$  have the same remainders when divided by  $m$ , then:  $r = a - mq$ ,  $r = b - mp$ ,  $0 = a - mq - b + mp$  or  $a - b = mq - mp = m(q - p) = mc$ , where  $c = q - p$ .

The above also means that  $a = b + mk$ , for some integer  $k$ .

Equivalently,  $a \equiv b \pmod{m}$  **implies that**  $a \pmod{m} = b \pmod{m}$ .

#### Theorem about multiplications and additions in congruences:

If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then

$$a + c \equiv b + d \pmod{m} \quad (3.4)$$

and

$$ac \equiv bd \pmod{m} \quad (3.5)$$

To prove these, you can use something like the following reasoning:

$$a - b = mp \text{ and } c - d = mq \implies a + c - (b + d) = m(p + q)$$

$$\text{Since } c = d + mq$$

$$ac = (b + mp)(d + mq) = bd + bmq + dmp + mmpq = bd + mc$$

#### Corollary detailing more forms of addition and multiplication

$$(a + b) \pmod{m} = [(a \pmod{m}) + (b \pmod{m})] \pmod{m} \quad (3.6)$$

To show this,

$a = mk + r = mk + (a \pmod{m})$  hence  $a \equiv (a \pmod{m}) \pmod{m}$  and so  $b \equiv (b \pmod{m}) \pmod{m}$ . So  $a + b \equiv [(a \pmod{m}) + (b \pmod{m})] \pmod{m}$

Because  $a \equiv b \pmod{m}$  implies  $a \pmod{m} = b \pmod{m}$ , the above can be written as  $(a + b) \pmod{m} = [(a \pmod{m}) + (b \pmod{m})] \pmod{m}$ .

$$ab \pmod{m} = [(a \pmod{m})(b \pmod{m})] \pmod{m} \quad (3.7)$$

Following a similar logic as in the above proof, we can obtain the former equation by using  $ab \equiv [(a \pmod{m})(b \pmod{m})] \pmod{m}$ .

## 4 Abstract Algebra

### 4.1 Preliminaries

#### 4.1.1 Division Algorithm

The following is meant to help make sense of the proof for the division algorithm presented in Gallian's Contemporary Abstract Algebra.

If  $0 \leq r' - r \leq r < b$ . And if  $b(q - q') = r' - r$ . Since  $b$  divides  $r' - r$  ( $b|r' - r$ ), then  $r' - r = bu$  for some  $u$ . Which means that  $r' - r$  is between  $[0, b)$  (we are looking at an open interval on the right due to the requirement that  $r' - r \leq r < b$ ). Since it is not an option for  $r' - r = b$ , then  $r' - r$  must be 0 (no other factor).

UPC example: Correct code is  $a_1a_2a_3a_4a_5$ , incorrect code is  $a_2a_1a_3a_4a_5$ . So correct check digit is  $(3a_1 + a_2 + 3a_3 + a_4 + 3a_5) \bmod 10$ . Incorrect check digit is  $(3a_2 + a_1 + 3a_3 + a_4 + 3a_5) \bmod 10$ .

If  $x \bmod 10$  and  $y \bmod 10$  are equal, then  $x \equiv y \pmod{10}$ , which implies that  $x - y = 10k$ .

Error won't be caught is  $(3a_1 + a_2 + 3a_3 + a_4 + 3a_5) - (3a_2 + a_1 + 3a_3 + a_4 + 3a_5)$  is a multiple of 10. The above simplifies to  $[3a_1 \bmod 10 + a_1 \bmod 10 + \dots - 3a_2 \bmod 10 - a_1 \bmod 10 - \dots] \bmod 10$ . Which can be simplified to  $3a_1 \bmod 10 + a_1 \bmod 10 - 3a_2 \bmod 10 - a_1 \bmod 10 \bmod 10$ . Or  $(3a_1 + a_2 - 3a_2 - a_1) \bmod 10 = 0$ . Which means  $(2a_1 - 2a_2) \bmod 10 = 0$ . No error caught if  $a_1 - a_2$  is a multiple of  $10/2 = 5$  same as writing  $|a_1 - a_2| = 5$ .

#### GCD is a linear combination

Since  $S = am + bn : am + bn > 0$ . Well ordering axiom says there must exist a  $d$  s.t.  $d = as + bt$ . Claim is that  $d$  is also  $\gcd(a, b)$  meaning that  $a = dq + r$  where  $0 \leq r < d$ . If  $r = 0$ : then  $r$  is not in  $S$ , and we have no member in  $S$  smaller than  $d$ . If  $r > 0$ : then any linear combination that was equal to  $r$  would have  $r$  in  $S$  and because  $0 \leq r < d$ , it would be smaller than  $d$ , leading to a contradiction.

#### Euclid's lemma

If  $p$  is a prime, and if  $p$  does not divide another integer  $a$ , then it means that  $a \neq pu$  (no common factor). And since a prime only has 1 and itself as divisors (factors), then the only other possibility is 1. Hence  $p$  not dividing  $a \geq \gcd(p, a) = 1$ . if  $p|ab$ :  $ab = pc$ , for some integer  $c$ . Thus,  $b = abs + ptp = pcs + ptb$ .