

# Notes for Undergraduate Algebra by Serge Lang

Zhao Wenchuan

April 9, 2021

# Chapter 1

## The Integers

### 1.1 Terminology of Sets

### 1.2 Basic Properties

**Theorem 1.2.1** (Induction: First Form). Suppose that for each integer  $n \geq 1$  we are given an assertion  $A(n)$ , and that we can prove the following two properties:

- (1) The assertion  $A(1)$  is true.
- (2) For each integer  $n \geq 1$ , if  $A(n)$  is true, then  $A(n+1)$  is true.

Then for all integers  $n \geq 1$ , the assertion  $A(n)$  is true.

**Theorem 1.2.2** (Induction: Second Form). Suppose that for each integer  $n \geq 0$  we are given an assertion  $A(n)$ , and that we can prove the following two properties:

- (i') The assertion  $A(0)$  is true;
- (ii') For each integer  $n > 0$ , if  $A(k)$  is true for every integer  $k$  with  $0 \leq k < n$ , then  $A(n)$  is true.

Then the assertion  $A(n)$  is true for all integers  $n \geq 0$ .

**Theorem 1.2.3** (Euclidean Algorithm). Let  $m, n$  be integers and  $m > 0$ . Then there exists integers  $q, r$  with  $0 \leq r < m$  such that

$$n = qm + r.$$

The integers  $q, r$  are uniquely determined by these conditions.

*Proof.* For  $m = n$ , then  $q = 1$  and  $r = 0$  are unique.

For  $m < n$ , there is a greatest integer  $q$  such that

$$0 \leq n - qm < m.$$

Because if  $q$  is not the greatest, then there must be  $q+1$  such that the inequality holds. But

$$0 \leq n - (q+1)m \iff m \leq n - qm,$$

which is impossible. Thus  $q$  must be the greatest one.

Secondly, there is a smallest integer  $q$  such that

$$0 \leq n - qm < m.$$

Because if it is not, then  $q-1$  makes the inequality holds. But

$$n - (q-1)m < m \iff n - qm < 0,$$

which is impossible. Thus  $q$  must be the smallest one.

As  $q$  is the greatest as well as the smallest one, then  $q$  is unique.

Suppose  $r$  is not unique, then there must be  $s \in \mathbb{Z}_{[0,m)}$  with  $s \neq r$  such that

$$n = qm + r, \text{ and}$$

$$n = qm + s.$$

then, we have

$$0 = r - s \neq 0,$$

a contradiction. So  $r$  is unique. □

## Exercises

1. If  $m, n$  are integers  $\geq 1$  and  $n \geq m$ , define the **binomial coefficient**

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

As usual,  $n! = n \cdot (n-1) \cdots 1$  is the product of the first  $n$  integers. We define  $0! = 1$  and  $\binom{n}{0} = 1$ . Prove that

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

*Proof.* This one can be straightly proved by the definition of binomial coef-

ficient as following.

$$\begin{aligned}
\binom{n}{m-1} + \binom{n}{m} &= \frac{n!}{(m-1)!(n-m+1)!} + \frac{n!}{m!(n-m)!} \\
&= \frac{n!m}{m!(n-m+1)!} + \frac{n!(n-m+1)}{m!(n-m+1)!} \\
&= \frac{n!}{m!(n-m+1)!} (m + n - m + 1) \\
&= \frac{(n+1)!}{m!(n+1-m)!} \\
&= \binom{n+1}{m}.
\end{aligned}$$

□

2. Prove by induction that for any integers  $x, y$  we have

$$(x+y)^n = \sum_{i=1}^n \binom{n}{i} x^i y^{n-i} = y^n + \binom{n}{1} xy^{n-1} + \binom{n}{2} x^2 y^{n-2} + \cdots + x^n.$$

*Proof.* The equation holds for  $n = 1$ , because

$$(x+y)^1 = x+y.$$

Assume the equation holds for any integer  $n \geq 1$ , then

$$\begin{aligned}
(x+y)^{n+1} &= (x+y) \sum_{i=0}^n \binom{n}{i} x^i y^{n-i} \\
&= \sum_{i=0}^n \left[ \binom{n}{i} x^i y^{n+i} + \binom{n}{i} x^{i+1} y^{n-i-1} \right].
\end{aligned}$$

By Exercise 1, it is easy to prove that

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

Then the equation is

$$\begin{aligned}
&\sum_{i=0}^{n+1} \left[ \binom{n+1}{i} x^i y^{n+1-i} - \binom{n}{i} x^i y^{n+1-i} + \binom{n}{i} x^i y^{n+1-i} \right] \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} x^i y^{n+1-i} \Big|_{\text{let } k = n+1} \\
&= \sum_{i=0}^k \binom{k}{i} x^i y^{k-i}.
\end{aligned}$$

□

3. Prove the following statements for all positive integers:

- (a)  $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ ;
- (b)  $1^2 + 2^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6$ ;
- (c)  $1^3 + 2^3 + 3^3 + \cdots + n^3 = [n(n + 1)/2]^2$ .

*Proof.* (a) Clearly the equation holds for  $n = 1$ . Suppose it holds for all integer  $n \geq 1$ , then we have

$$\sum_{i=1}^{n+1} (2i - 1) = n^2 + 2n + 1 = (n + 1)^2$$

(b) Clearly the equation holds for  $n = 1$ . Suppose it holds for all integer  $n \geq 1$ , then we have

$$\begin{aligned} \sum_{i=1}^{n+1} i^2 &= \frac{n(n + 1)(2n + 1)}{6} + (n + 1)^2 \\ &= \frac{n(n + 1)(2n + 1) + 6(n + 1)^2}{6} \\ &= \frac{(n + 1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n + 1)(n + 2)(2n + 3)}{6} \Big|_{\text{let } k = n + 1} \\ &= \frac{k(k + 1)(2k + 1)}{6}. \end{aligned}$$

(c) Clearly the equation holds for  $n = 1$ . Suppose it holds for all integer  $n \geq 1$ , then we have

$$\begin{aligned} \sum_{i=1}^{n+1} i^3 &= \left( \frac{n(n + 1)}{2} \right)^2 + (n + 1)^3 \\ &= \frac{n^2(n + 1)^2 + 4(n + 1)^3}{4} \\ &= \frac{(n + 1)^2(n + 2)^2}{4} \\ &= \left( \frac{(n + 1)(n + 2)}{2} \right)^2 \Big|_{\text{let } k = n + 1} \\ &= \left( \frac{k(k + 1)}{2} \right)^2 \end{aligned}$$

□

4. Prove that

$$\left(1 + \frac{1}{1}\right)^1 \left(1 + \frac{1}{2}\right)^2 \cdots \left(1 + \frac{1}{n-1}\right)^{n-1} = \frac{n^{n-1}}{(n+1)!}$$

*Proof.* The equation holds for  $n = 2$ , because

$$\left(1 + \frac{1}{1}\right)^1 = 2 = \frac{2}{1!}.$$

Assume the equation holds for any integer  $n \geq 2$ , then

$$\begin{aligned} \prod_{i=1}^n \left(1 + \frac{1}{i}\right)^i &= \frac{n^{n-1}}{(n-1)!} \left(1 + \frac{1}{n}\right)^n \\ &= \frac{n^{n-1}}{(n-1)!} \frac{(n+1)^n}{n^n} \\ &= \frac{n^{n-1}(n+1)^n}{n!n^{n-1}} \\ &= \frac{(n+1)^n}{n!} \Big|_{\text{let } k = n+1} \\ &= \frac{k^{k-1}}{(k-1)!}. \end{aligned}$$

□

5. Let  $x$  be a real number. Prove that there exists an integer  $q$  and a real number  $s$  with  $0 \leq s < 1$  such that  $x = q + s$ , and that  $q, s$  are uniquely determined. Can you deduce the Euclidean algorithm from this result without using induction?

*Proof.* This is just a straight corollary of Euclidean algorithm. □

## 1.3 Greatest Common Divisor

**Definition 1.3.1.** Given  $n, d \in \mathbb{Z} \setminus \{0\}$ , we shall say that  $d$  divides  $n$ , or  $d$  is a divisor of  $n$ , denoted  $d|n$ , iff

$$\exists q \in \mathbb{Z}, \quad n = dq.$$

The divisors of  $n$  is a set

$$\text{div}(n) = \{d \in \mathbb{Z} \setminus \{0\} : d|n\}.$$

For example,

$$\begin{aligned} \text{div}(8) &= \{\pm 1, \pm 2, \pm 4, \pm 8\}, \\ \text{div}(-24) &= \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12\}, \\ \text{div}(35) &= \{\pm 1, \pm 5, \pm 7, \pm 35\}. \end{aligned}$$

Clearly, for all  $n \in \mathbb{Z} \setminus \{0\}$ , for all  $x \in \text{div}(n) \setminus \{\pm n\}$

$$|x| \leq \frac{|n|}{2}.$$

**Definition 1.3.2.** Given  $m, n \in \mathbb{Z} \setminus \{0\}$ , the *common divisor* is defined to be the set

$$\text{cd}(m, n) = \{d \in \mathbb{Z}_{>0} : d|m \wedge d|n\}.$$

Thus,

$$\text{cd}(m, n) = \text{div}(m)_{>0} \cap \text{div}(n)_{>0}$$

For example,

$$\text{cd}(18, 12) = \{2, 3, 6\},$$

$$\text{cd}(-18, 12) = \{2, 3, 6\},$$

$$\text{cd}(24, -20) = \{2, 4\},$$