

# Chapter 1: The Real And Complex Number Systems

Author: Meng-Gen Tsai

Email: plover@gmail.com

## Integers

**Exercise 1.1** Prove that there is no largest prime. (A proof was known to Euclid.)

There are many proofs of this result. We provide some of them.

*Proof (Due to Euclid).* If  $p_1, p_2, \dots, p_t$  were all primes, then write

$$n = p_1 p_2 \cdots p_t + 1$$

and there were a prime number  $p$  dividing  $n$ .

- (1)  $p$  can not be any of  $p_i (1 \leq i \leq t)$ , otherwise  $p$  would divide the difference  $n - p_1 p_2 \cdots p_t = 1$ .
- (2) This prime  $p$  is another prime  $\neq p_i$  for  $1 \leq i \leq t$ , which is absurd.

□

*Proof (Unique factorization theorem).* Given  $N$ .

- (1) Show that  $\sum_{n \leq N} \frac{1}{n} \leq \prod_{p \leq N} \left(1 - \frac{1}{p}\right)^{-1}$ .

By the unique factorization theorem on  $n \leq N$ ,

$$\sum_{n \leq N} \frac{1}{n} \leq \prod_{p \leq N} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right) = \prod_{p \leq N} \left(1 - \frac{1}{p}\right)^{-1}.$$

- (2) By (1) and the fact that  $\sum \frac{1}{n}$  diverges, there are infinitely many primes.

□

*Proof (Due to Eckford Cohen).*

- (1)  $\text{ord}_p n! = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$ . For any  $k = 1, 2, \dots, n$ , we can express  $k$  as  $k = p^s t$  where  $s = \text{ord}_p k$  is a non-negative integer and  $(t, p) = 1$ . There are  $\left[\frac{n}{p^a}\right]$  numbers such that  $p^a \mid k$  for  $a = 1, 2, \dots$ . Therefore, there are

$$\left[\frac{n}{p^a}\right] - \left[\frac{n}{p^{a+1}}\right]$$

numbers such that  $\text{ord}_p k = a$  for  $a = 1, 2, \dots$ . Hence,

$$\begin{aligned}\text{ord}_p n! &= \left( \left\lfloor \frac{n}{p} \right\rfloor - \left\lfloor \frac{n}{p^2} \right\rfloor \right) + 2 \left( \left\lfloor \frac{n}{p^2} \right\rfloor - \left\lfloor \frac{n}{p^3} \right\rfloor \right) + 3 \left( \left\lfloor \frac{n}{p^3} \right\rfloor - \left\lfloor \frac{n}{p^4} \right\rfloor \right) + \dots \\ &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots.\end{aligned}$$

(2)  $\text{ord}_p n! \leq \frac{n}{p-1}$  and that  $n!^{\frac{1}{n}} \leq \prod_{p|n!} p^{\frac{1}{p-1}}$ .

$$\begin{aligned}\text{ord}_p n! &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \\ &\leq \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \dots \\ &= \frac{\frac{n}{p}}{1 - \frac{1}{p}} \\ &= \frac{n}{p-1}.\end{aligned}$$

Thus,

$$n! = \prod_{p|n!} p^{\text{ord}_p n!} \leq \prod_{p|n!} p^{\frac{n}{p-1}} = \left( \prod_{p|n!} p^{\frac{1}{p-1}} \right)^n,$$

or

$$n!^{\frac{1}{n}} \leq \prod_{p|n!} p^{\frac{1}{p-1}}.$$

- (3)  $(n!)^2 \geq n^n$ . Write  $(n!)^2 = \prod_{k=1}^n k \prod_{k=1}^n (n+1-k) = \prod_{k=1}^n k(n+1-k)$ , and  $n^n = \prod_{k=1}^n n$ . It suffices to show that  $k(n+1-k) \geq n$  for each  $1 \leq k \leq n$ . Notice that  $k(n+1-k) - n = (n-k)(k-1) \geq 0$  for  $1 \leq k \leq n$ . The inequality holds.
- (4) By (3)(4),  $\prod_{p|n!} p^{\frac{1}{p-1}} \geq \sqrt{n}$ . Assume that there are finitely many primes, the value  $\prod_{p|n!} p^{\frac{1}{p-1}}$  is a finite number whenever the value of  $n$ . However,  $\sqrt{n} \rightarrow \infty$  as  $n \rightarrow \infty$ , which leads to a contradiction. Hence there are infinitely many primes.

□

*Proof (Formula for  $\phi(n)$ ).* If  $p_1, p_2, \dots, p_t$  were all primes, then let  $n = p_1 p_2 \cdots p_t$  and all numbers between 2 and  $n$  are NOT relatively prime to  $n$ . Thus,  $\phi(n) = 1$  by the definition of  $\phi$ . By the formula for  $\phi$ ,

$$\begin{aligned}\phi(n) &= n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_t} \right) \\ 1 &= (p_1 p_2 \cdots p_t) \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \cdots \left( 1 - \frac{1}{p_t} \right) \\ &= (p_1 - 1)(p_2 - 1) \cdots (p_t - 1) > 1,\end{aligned}$$

which is a contradiction (since 3 is a prime). Hence there are infinitely many primes.  $\square$

**Exercise 1.2** If  $n$  is a positive integer, prove the algebraic identity

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

*Proof.*

(1)

$$\begin{aligned} (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} &= a \sum_{k=0}^{n-1} a^k b^{n-1-k} - b \sum_{k=0}^{n-1} a^k b^{n-1-k} \\ &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k}. \end{aligned}$$

(2) Arrange index in summation symbols.

$$\begin{aligned} \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} &= \sum_{k=1}^n a^k b^{n-k} = a^n + \sum_{k=1}^{n-1} a^k b^{n-k}, \\ \sum_{k=0}^{n-1} a^k b^{n-k} &= b^n + \sum_{k=1}^{n-1} a^k b^{n-k}. \end{aligned}$$

(3) By (1)(2),

$$\begin{aligned} (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k} &= \left( a^n + \sum_{k=1}^{n-1} a^k b^{n-k} \right) - \left( b^n + \sum_{k=1}^{n-1} a^k b^{n-k} \right) \\ &= a^n - b^n. \end{aligned}$$

$\square$

**Exercise 1.3** If  $2^n - 1$  is a prime, prove that  $n$  is prime. A prime of the form  $2^p - 1$ , where  $p$  is prime, is called a Mersenne prime.

It suffices to prove that: If  $a^n - 1$  is a prime, show that  $a = 2$  and that  $n$  is a prime. Primes of the form  $2^p - 1$  are called Mersenne primes. For example,  $2^3 - 1 = 7$  and  $2^5 - 1 = 31$ . It is not known if there are infinitely many Mersenne primes.

*Proof.*

- (1) *n is a prime.* Assume *n* were not prime, say  $n = rs$  for some  $r, s > 1$ . By Exercise 1.2,  $a^{rs} - 1 = (a^s - 1)(\sum_{k=0}^{r-1} a^{sk})$ .  $a^s - 1 = 1$  since  $a^s - 1 < a^{rs} - 1$  and  $a^{rs} - 1$  is a prime. Hence  $s = 1$  and  $(a = 2)$ , which is absurd.
- (2)  $a = 2$ . If *a* is odd, then  $a^p - 1 > 2$  is even, which is not a prime. If  $a > 2$  is even,  $a^p - 1 = (a - 1)(\sum_{k=0}^{p-1} a^k)$ . Both  $a - 1 > 1$  and  $\sum_{k=0}^{p-1} a^k > 1$ , which is absurd.

By (1)(2),  $a = 2$  and that  $n$  is a prime if  $a^n - 1$  is a prime.  $\square$

## Rational and irrational numbers

**Exercise 1.11** *Given any real  $x > 0$ , prove that there is an irrational number between 0 and  $x$ .*

*Proof.* There are only two possible cases:  $x$  is rational, or  $x$  is irrational.

- (1) *x is rational.* Pick  $y = \frac{x}{\sqrt{89}} \in (0, x) \subseteq \mathbb{R}$ .  $y$  is irrational.
- (2) *x is irrational.* Pick  $y = \frac{x}{\sqrt{64}} \in (0, x) \subseteq \mathbb{R}$ .  $y$  is irrational.

$\square$

*Proof (Exercise 4.12).* Pick

$$y = \lim_{m \rightarrow \infty} [\lim_{n \rightarrow \infty} \cos^{2n}(m!\pi x)] \cdot \frac{x}{\sqrt{89}} + (1 - \lim_{m \rightarrow \infty} [\lim_{n \rightarrow \infty} \cos^{2n}(m!\pi x)]) \cdot \frac{x}{\sqrt{64}}.$$

- (1) *x is rational.*  $y = \frac{x}{\sqrt{89}} \in (0, x) \subseteq \mathbb{R}$  is irrational.
- (2) *x is irrational.*  $y = \frac{x}{\sqrt{64}} \in (0, x) \subseteq \mathbb{R}$  is irrational.

$\square$