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 we consider

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

Thus there is a prime number p dividing n. p can not be any of p_i for $1 \leq i \leq t$; otherwise p would divide the difference $n - p_1 p_2 \cdots p_t = 1$. That is, $p \neq p_i$ for $1 \leq i \leq t$, contrary to the assumption. $\square$

Supplement (Due to Euclid).

(1) *Show that $k[x]$, with k a field, has infinitely many irreducible polynomials.* If $f_1, f_2, \dots, f_t$ were all irreducible polynomials, then we consider

$$g = f_1 f_2 \cdots f_t + 1 \in k[x].$$

So there is an irreducible polynomial f dividing g (since $\deg g = \deg f_1 + \deg f_2 + \cdots + \deg f_t \geq 1$). f can not be any of $c_i f_i$ for $1 \leq i \leq t$ and $c_i \in k - \{0\}$; otherwise f would divide the difference $g - f_1 f_2 \cdots f_t = 1$. That is, $f \neq c_i f_i$ for $1 \leq i \leq t$ and $c_i \in k - \{0\}$, contrary to the assumption.

(2) *Show that any algebraically closed field is infinite.* Let k be an algebraically closed field. If $a_1, \dots, a_n$ were all elements in k, then we consider a monic polynomials

$$F(X) = (X - a_1) \cdots (X - a_n) + 1 \in k[X].$$

Since k is algebraically closed, there is an element $a \in k$ such that $F(a) = 0$. By assumption, $a = a_i$ for some $1 \leq i \leq n$, and thus $F(a) = F(a_i) = 1$, contrary to the fact that a field is a commutative ring where $0 \neq 1$ and all nonzero elements are invertible.

$\square$

Proof (Unique factorization theorem). Given N.

(1) *Show that* $\sum_{n\le N}\frac{1}{n}\le\prod_{p\le N}\left(1-\frac{1}{p}\right)^{-1}$.
By the unique factorization theorem on $n\le N$,

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

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

□

Proof (Due to Eckford Cohen).

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

$$\begin{aligned}\mathrm{ord}_p n! &= \left(\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]\right)+2\left(\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]\right)+3\left(\left[\frac{n}{p^3}\right]-\left[\frac{n}{p^4}\right]\right)+\cdots\\ &= \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots.\end{aligned}$$

(2) $ord_p n!\le\frac{n}{p-1}$ *and that* $n!^{\frac{1}{n}}\le\prod_{p\mid n!}p^{\frac{1}{p-1}}$.

$$\begin{aligned}\mathrm{ord}_p n! &= \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots\\ &\le \frac{n}{p}+\frac{n}{p^2}+\frac{n}{p^3}+\cdots\\ &= \frac{\frac{n}{p}}{1-\frac{1}{p}}\\ &= \frac{n}{p-1}.\end{aligned}$$

Thus,

$$n!=\prod_{p\mid n!}p^{\mathrm{ord}_p n!}\le\prod_{p\mid n!}p^{\frac{n}{p-1}}=\left(\prod_{p\mid n!}p^{\frac{1}{p-1}}\right)^n,$$

or

$$n!^{\frac{1}{n}}\le\prod_{p\mid n!}p^{\frac{1}{p-1}}.$$

(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, $\sqrt{n} \to \infty$ as $n \to \infty$, which leads to a contradiction. Hence there are infinitely many primes.

□

Proof (Formula for $\phi(n)$). If $p_1, p_2, \ldots, p_t$ 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 ϕ. By the formula for ϕ,

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

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

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 summation index:

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

(3) By (1)(2),

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

□

Supplement. Some exercises without proof.

(1) *Let x be a nilpotent element of A. Show that $1+x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.* (Exercise 1.1 in the textbook: *Atiyah and Macdonald, Introduction to Commutative Algebra*)

(2) *Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0\,(p)$ if $p-1 \nmid k$ and $-1(p)$ if $p-1 \mid k$.* (Exercise 4.11 in the textbook: *Kenneth Ireland and Michael Rosen, A Classical Introduction to Modern Number Theory, 2nd edition*)

(3) *Use the existence of a primitive root to give another proof of Wilson's theorem $(p-1)! \equiv -1\ (p)$.* (Exercise 4.12 in the textbook: *Kenneth Ireland and Michael Rosen, A Classical Introduction to Modern Number Theory, 2nd edition*)

(4) *Suppose n and F are integers and $n, F > 0$. Show that*

$$B_n(Fx) = F^{n-1}\sum_{a=0}^{F-1} B_n\left(x + \frac{a}{F}\right).$$

where $B_n(x)$ are Bernoulli polynomials. (Exercise 15.19 in the textbook: *Kenneth Ireland and Michael Rosen, A Classical Introduction to Modern Number Theory, 2nd edition*)

(5) Exercise 1.3.

(6) Exercise 1.4.

$\square$

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. $\square$

Exercise 1.6. *Prove that every nonempty set of positive integers contains a smallest member. This is called the well-ordering principle.*

Proof. Use mathematical induction to establish that the well-ordering principle.

(1) Given a set S of positive integers, let $P(n)$ be the proposition 'If $m \in S$ for some $m \leq n$, then S has a least element'. Want to show $P(n)$ is true for all $n \in \mathbb{N}$.

   (a) $P(1)$ is true. For $m \in S$ with $m \leq n = 1$, or $m = 1$ by the minimality of $1 \in \mathbb{N}$, S has a least element 1 (m itself) in $\mathbb{N}$.

   (b) Suppose $P(n)$ is true. If $n + 1 \in S$, then there are only two possible cases.

      (i) There is a positive integer $m \in S$ less than $n + 1$. So $n \geq m \in S$. Since $P(n)$ is true, S has a least element.

      (ii) There is no positive integer $m \in S$ less than $n + 1$. In this case $n + 1$ is the least element in S.

      In any cases (i)(ii), S has a least element, or $P(n + 1)$ is true.

   By mathematical induction, $P(n)$ is true for all $n \in \mathbb{N}$.

(2) *Show that the well-ordering principle holds.* Let T be a nonempty subset of $\mathbb{N}$, so there exists a positive integer $k \in T$. Notice that $P(k)$ is true by (1), thus T has a least element since $k \leq k$.

$\square$

Supplement. *Show that the well-ordering principle implies the principle of mathematical induction.*

Proof. Suppose that

(1) $P(n)$ be a proposition defined for each $n \in \mathbb{N}$,

(2) $P(1)$ is true,

(3) $[P(n) \Rightarrow P(n+1)]$ is true.

Consider the set
$$S = \{n \in \mathbb{N} : P(n) \text{ is false}\} \subseteq \mathbb{N}.$$
Want to show S *is empty, or the principle of mathematical induction holds.* If S were nonempty, by the well-ordering principle S has a smallest element m. m cannot be 1 by (2). Say $m > 1$. Therefore, $m - 1 \in \mathbb{N}$ and $P(m-1)$ is true by the minimality of m. By (3), $P((m-1)+1) = P(m)$ is true, which is absurd. $\square$

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

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

(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.

$\square$

Upper bounds

Inequalities

Exercise 1.23. *Prove Lagrange's identity for real numbers:*

$$\left(\sum_{k=1}^{n} a_k b_k\right)^2 = \left(\sum_{k=1}^{n} a_k\right)^2 \left(\sum_{k=1}^{n} b_k\right)^2 - \sum_{1\le k<j\le n} (a_k b_j - a_j b_k)^2.$$

Note that this identity implies the Cauchy-Schwarz inequality.

Proof. Put $(a_k, b_k, A_k, B_k) \mapsto (a_k, b_k, a_k, b_k)$ in the following generalization (Binet-Cauchy identity). $\square$

Generalization (Binet-Cauchy identity).

$$\begin{aligned} &\sum_{1\le k<j\le n} (a_k b_j - a_j b_k)(A_k B_j - A_j B_k) \\ &= \left(\sum_{k=1}^{n} a_k A_k\right)\left(\sum_{k=1}^{n} b_k B_k\right) - \left(\sum_{k=1}^{n} a_k B_k\right)\left(\sum_{k=1}^{n} b_k A_k\right). \end{aligned}$$

Proof.

$$\begin{aligned} &\sum_{1\le k<j\le n} (a_k b_j - a_j b_k)(A_k B_j - A_j B_k) \\ &= \sum_{1\le k<j\le n} (a_k b_j A_k B_j + a_j b_k A_j B_k) - \sum_{1\le k<j\le n} (a_k b_j A_j B_k - a_j b_k A_k B_j) \\ &= \sum_{1\le k<j\le n} (a_k A_k b_j B_j + a_j A_j b_k B_k) - \sum_{1\le k<j\le n} (a_k B_k b_j A_j + a_j B_j b_k A_k) \\ &= \sum_{1\le k\ne j\le n} a_k A_k b_j B_j - \sum_{1\le k\ne j\le n} a_k B_k b_j A_j \\ &= \sum_{1\le k,j\le n} a_k A_k b_j B_j - \sum_{1\le k,j\le n} a_k B_k b_j A_j \\ &\quad (\text{since } a_k A_k b_j B_j - a_k B_k b_j A_j = 0 \text{ as } k = j) \\ &= \left(\sum_{k=1}^{n} a_k A_k\right)\left(\sum_{j=1}^{n} b_j B_j\right) - \left(\sum_{k=1}^{n} a_k B_k\right)\left(\sum_{j=1}^{n} b_j A_j\right) \\ &= \left(\sum_{k=1}^{n} a_k A_k\right)\left(\sum_{k=1}^{n} b_k B_k\right) - \left(\sum_{k=1}^{n} a_k B_k\right)\left(\sum_{k=1}^{n} b_k A_k\right). \end{aligned}$$

$\square$

Supplement ($\mathbb{Z}[i]$). As $n = 2$, $(a_1^2+a_2^2)(b_1^2+b_2^2) = (a_1b_1+a_2b_2)^2+(a_1b_2-a_2b_1)^2$.

Define $N : \mathbb{Z}[i] \to \mathbb{Z}$ by $N(a + bi) = a^2 + b^2$.

(1) *Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or using the fact that $N(a+bi) = (a+bi)(a-bi)$. Conclude that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.*

(2) *Let $\alpha \in \mathbb{Z}[i]$. Show that α is a unit iff $N(\alpha) = 1$. Conclude that the only unit are ± 1 and $\pm i$.*

(3) *Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.*

(4) *Show that $1 - i$ is irreducible in $\mathbb{Z}$ and that $2 = u(1-i)^2$ for some unit u.*

(5) *Show that every nonzero, non-unit Gaussian integer α is a product of irreducible elements, by induction on $N(\alpha)$.*

(6) *Use the unique factorization in $\mathbb{Z}[i]$ to prove that every prime $p \equiv 1 \pmod 4$ is a sum of two squares.*

(7) *Describe all irreducible elements in $\mathbb{Z}[i]$.*

Complex numbers

Exercise 1.48. *Prove Lagrange's identity for complex numbers:*

$$\left|\sum_{k=1}^{n} a_k b_k\right|^2 = \sum_{k=1}^{n} |a_k|^2 \sum_{k=1}^{n} |b_k|^2 - \sum_{1 \le k < j \le n} \left|a_k\overline{b_j} - a_j\overline{b_k}\right|^2.$$

Proof. Put $(a_k, b_k, A_k, B_k) \mapsto (a_k, \overline{b_k}, \overline{a_k}, b_k)$ in the generalization to Exercise 1.23 (Binet-Cauchy identity) and use the identity $|z| = z\overline{z}$.