Solutions to the book: *Ireland and Rosen, A Classical Introduction to Modern Number Theory, 2nd edition*

Meng-Gen Tsai
plover@gmail.com

July 20, 2021

Contents

Chapter 1: Unique Factorization

Exercise 1.10.

Suppose that $(u, v) = 1$. *Show that* $(u + v, u - v)$ *is either* 1 *or* 2.

Each case is possible:

(1) $u = 3, v = 2$. $(u, v) = 1$ and $(u + v, u - v) = 1$.

(2) $u = 3, v = 1$. $(u, v) = 1$ and $(u + v, u - v) = 2$.

Proof (Exercise 1.6). Since $(u, v) = 1$, there is $m, n \in \mathbb{Z}$ such that $mu + nv = 1$ (Exercise 1.4). So

$$\begin{aligned} mu + nv = 1 &\Longleftrightarrow 2mu + 2nv = 2 \\ &\Longleftrightarrow ((u + v) + (u - v))m + ((u + v) - (u - v))n = 2 \\ &\Longleftrightarrow (m + n)(u + v) + (m - n)(u - v) = 2, \end{aligned}$$

or $(x, y) = (m + n, m - n)$ is an integer solution to $(u + v)x + (u - v)y = 2$. So $2 \mid (u + v, u - v)$ (Exercise 1.6). Hence $(u + v, u - v) = 1$ or 2. □

Exercise 1.11.

Show that $(a, a + k) \mid k$.

Proof (Exercise 1.6). The equation $ax + (a + k)y = k$ has solution $(x, y) = (-1, 1) \in \mathbb{Z}^2$. Hence $(a, a + k) \mid k$ (Exercise 1.6). □

Exercise 1.31.

Show that 2 *is divided by* $(1 + i)^2 \in \mathbb{Z}[i]$.

$1 + i$ is irreducible in $\mathbb{Z}[i]$.

The ring morphism $\mathbb{Z} \to \mathbb{Z}[i]$ corresponds to a map of schemes $f : \mathrm{Spec}(\mathbb{Z}[i]) \to \mathrm{Spec}(\mathbb{Z})$. Suppose (p) is a prime ideal of $\mathbb{Z}$. Might find the points of $f^{-1}(p) \in \mathrm{Spec}(\mathbb{Z}[i])$.

Proof. $(1 + i)^2 = 2i \in \mathbb{Z}[i]$. Thus $2 \mid (1 + i)^2 \in \mathbb{Z}[i]$. □

Exercise 1.34.

Show that 3 *is divided by* $(1-\omega)^2 \in \mathbb{Z}[\omega]$.

Proof. $(1-\omega)^2 = 1 - 2\omega + \omega^2 = (1 + \omega + \omega^2) - 3\omega = -3\omega \in \mathbb{Z}[\omega]$. Thus $3 \mid (1-\omega)^2 \in \mathbb{Z}[\omega]$. $\square$

Chapter 2: Applications of Unique Factorization

Exercise.

If $\frac{a}{b} \in \mathbb{Z}_p$ is not a unit, prove that $\frac{a}{b} + 1$ is a unit.

Proof. $\frac{a}{b} \in \mathbb{Z}_p$ is not a unit iff $p \mid a$ and $p \nmid b$. Thus $p \nmid (a+b)$. That is, $\frac{a}{b} + 1 = \frac{a+b}{b} \in \mathbb{Z}_p$ is a unit. □

Exercise 2.6. (p-adic valuation)

For a rational number r let $[r]$ be the largest integer less than or equal to r, e.g., $[\frac{1}{2}] = 0$, $[2] = 2$, $[3\frac{1}{3}] = 3$. Prove

$$ord_p n! = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots .$$

Notice that $[\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}] + \cdots$ is a finite sum.

Proof. For any $k = 1, 2, ..., n$, 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 $a = 1, 2, ...$ 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 $a = 1, 2, ...$ Hence,

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

□

Supplement 2.6.1.

Related problems.

(1) *Prove that*

$$\frac{(m+n)!}{m!n!}$$

is an integer for all non-negative integers m and n.

Proof. It is sufficient to show that

$$\mathrm{ord}_p(m+n)! \geq \mathrm{ord}_p m! + \mathrm{ord}_p n!$$

for any prime p, or show that

$$\left[\frac{m+n}{p^k}\right] \geq \left[\frac{m}{p^k}\right] + \left[\frac{n}{p^k}\right]$$

for any prime p and $k \in \mathbb{Z}^+$ by Exercise 4.6, or show that

$$[x+y] \geq [x] + [y]$$

for any rational (or real) numbers x and y. It is trivial by considering that the sum of two fractional parts $\{x\} = x - [x]$ might be greater than or equal to 1, so $[x+y] = [x] + [y]$ or $[x] + [y] + 1$. □

Note. $\frac{(m+n)!}{m!n!}$ is a binomial coefficient. Similarly, a multinomial coefficient is

$$\frac{(n_1 + n_2 + \cdots + n_k)!}{n_1! n_2! \cdots n_k!}.$$

We can show that the multinomial coefficient is an integer by using the above argument.

(2) *Prove that*

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

is an integer for all non-negative integers m and n.

Proof. Similar to (1), it is sufficient to show that

$$[2x] + [2y] \geq [x] + [y] + [x+y]$$

for any rational (or real) numbers x and y. Notice that $[2x] = [x] + [x + \frac{1}{2}]$, and thus we might show that $[x + \frac{1}{2}] + [y + \frac{1}{2}] \geq [x+y]$. Again it is trivial and we omit the tedious calculation. □

(3) *Hermite's identity:* $[nx] = \sum_{k=0}^{n-1} [x + \frac{k}{n}]$ *for* $n \in \mathbb{Z}^+$.

Let $n = 2$ and we can get $[2x] = [x] + [x + \frac{1}{2}]$ too.

Proof. Consider the function $f(x) = \sum_{k=0}^{n-1} [x + \frac{k}{n}] - [nx]$. Notice that $f(x + \frac{1}{n}) = f(x)$. f has period $\frac{1}{n}$. It then suffices to prove that $f(x) = 0$ on $[0, \frac{1}{n})$. But in this case, the integral part of each summand in f is equal to 0. Therefore $f = 0$ on $\mathbb{R}$. □

(4) *Show*

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

is an integer for all non-negative integers m and n.

Try to deduce the inequality $[5x]+[5y] \geq [x]+[y]+[3x+y]+[3y+x]$.

Exercise 2.7.

Deduce from Exercise 2.6 that $\mathrm{ord}_p n! \leq \frac{n}{p-1}$ and that $n!^{\frac{1}{n}} \leq \prod_{p|n!} p^{\frac{1}{p-1}}$.

Proof.

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

Thus,

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

or

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

□

Exercise 2.8.

Use Exercise 2.7 to show that there are infinitely many primes. [Hint: $(n!)^2 \geq n^n$.] (This proof is due to Eckford Cohen.)

Proof.

(1) *Show that $(n!)^2 \geq n^n$.* 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.

2 By Exercise 2.7 and (1),

$$\prod_{p|n!} p^{\frac{1}{p-1}} \geq (n!)^{\frac{1}{n}} \geq \sqrt{n}.$$

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.

□

Exercise 2.27.

Show that $\sum' \frac{1}{n}$, the sum being over square free integers, diverges. Conclude that $\prod_{p \leq N}(1+\frac{1}{p}) \to \infty$ as $N \to \infty$. Since $e^x > 1+x$, conclude that $\sum_{p \leq N} \frac{1}{p} \to \infty$. (This proof is due to I. Niven.)

There are many proofs of $\sum_p \frac{1}{p}$ diverges.

Proof.

(1) For any positive integers n, we can write $n = a^2 b$ where $a \in \mathbb{Z}^+$ and b is a square free integer. Given N,

$$\sum_{n \leq N} \frac{1}{n} \leq \left(\sum_{a=1}^{\infty} \frac{1}{a^2} \right) \left(\sum_{b \leq N}{}' \frac{1}{b} \right).$$

Notices that $\sum_{a=1}^{\infty} \frac{1}{a^2}$ converges. Since $\sum_{n \leq N} \frac{1}{n} \to \infty$ as $N \to \infty$, $\sum'_{b \leq N} \frac{1}{b} \to \infty$ as $N \to \infty$.

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

$$\prod_{p \leq N} \left(1 + \frac{1}{p}\right) \geq \sum_{n \leq N}{}' \frac{1}{n}.$$

Since $\sum_{n \leq N}{}' \frac{1}{n} \to \infty$ as $N \to \infty$, $\prod_{p \leq N}(1+\frac{1}{p}) \to \infty$ as $N \to \infty$.

(3) By applying the inequality $e^x > 1 + x$ on any prime p,

$$\exp\left(\frac{1}{p}\right) > 1 + \frac{1}{p}.$$

Now multiplying the inequality over all primes $p \leq N$ and noticing that $\exp(x) \cdot \exp(y) = \exp(x+y)$, we have

$$\exp\left(\sum_{p \leq N} \frac{1}{p} \right) > \prod_{p \leq N} \left(1 + \frac{1}{p}\right).$$

So $\exp\left(\sum_{p\leq N}\frac{1}{p}\right)\to\infty$ as $N\to\infty$, or $\sum_{p\leq N}\frac{1}{p}\to\infty$ as $N\to\infty$. $\square$

Chapter 3: Congruence

Exercise 3.12.

Let

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

be a binomial coefficient, and suppose that p is a prime. If $1 \leq k \leq p-1$, show that p divides $\binom{p}{k}$. Deduce $(a+1)^p \equiv a^p + 1 \pmod{p}$.

Proof.

(1) If $1 \leq k \leq p-1$, then $p \nmid k!$ and $p \nmid (p-k)!$ since p is a prime number.

(2) Write $a = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$.

$$\begin{aligned} a = \frac{p!}{k!(p-k)!} &\iff p! = ak!(p-k)! \\ &\implies p \mid p! \text{ or } p \mid ak!(p-k)! \\ &\implies p \mid a \qquad ((1)) \end{aligned}$$

Hence p divides $\binom{p}{k}$ if $1 \leq k \leq p-1$.

(3)

$$\begin{aligned} (a+1)^p &\equiv \sum_{k=0}^{p} \binom{p}{k} a^k \\ &\equiv 1 + \left(\sum_{k=1}^{p-1} \binom{p}{k} a^k \right) + a^p \\ &\equiv 1 + a^p \\ &\equiv a^p + 1 \pmod{p}. \end{aligned}$$

□

Chapter 4: The Structure of $U(\mathbb{Z}/n\mathbb{Z})$

Theorem 1.

$U(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group.

Proof. Let $p-1 = q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t} = \prod_q q^e$ be the prime decomposition of $p-1$. Consider the congruences

(1) $x^{q^{e-1}} \equiv 1(p)$

(2) $x^{q^e} \equiv 1(p)$

Therefore,

(1) Every solution to $x^{q^{e-1}} \equiv 1\,(p)$ is a solution of $x^{q^e} \equiv 1\,(p)$.

(2) $x^{q^e} \equiv 1\,(p)$ has more solutions than $x^{q^{e-1}} \equiv 1\,(p)$. In fact, $x^{q^{e-1}} \equiv 1\,(p)$ has q^{e-1} solutions and $x^{q^e} \equiv 1\,(p)$ has q^e solutions by Proposition 4.1.2.

Therefore, there exists $g_i \in \mathbb{Z}/p\mathbb{Z}$ generating a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $q_i^{e_i}$ for all $i = 1, ..., t$. Pick $g = g_1 g_2 \cdots g_t \in \mathbb{Z}/p\mathbb{Z}$ generating a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t} = p-1$. That is, $\langle g \rangle = U(\mathbb{Z}/p\mathbb{Z})$. □

Exercise 4.1.

Show that 2 is a primitive root module 29.

Proof. $2^1 \equiv 2\,(29)$, $2^2 \equiv 4\,(29)$, $2^3 \equiv 8\,(29)$, $2^4 \equiv 16\,(29)$, $2^5 \equiv 3\,(29)$, $2^6 \equiv 6\,(29)$, $2^7 \equiv 12\,(29)$, $2^8 \equiv 24\,(29)$, $2^9 \equiv 19\,(29)$, $2^{10} \equiv 9\,(29)$, $2^{11} \equiv 18\,(29)$, $2^{12} \equiv 7\,(29)$, $2^{13} \equiv 14\,(29)$, $2^{14} \equiv 28\,(29)$, $2^{15} \equiv 27\,(29)$, $2^{16} \equiv 25\,(29)$, $2^{17} \equiv 21\,(29)$, $2^{18} \equiv 13\,(29)$, $2^{19} \equiv 26\,(29)$, $2^{20} \equiv 23\,(29)$, $2^{21} \equiv 17\,(29)$, $2^{22} \equiv 5\,(29)$, $2^{23} \equiv 10\,(29)$, $2^{24} \equiv 20\,(29)$, $2^{25} \equiv 11\,(29)$, $2^{26} \equiv 22\,(29)$, $2^{27} \equiv 15\,(29)$, $2^{28} \equiv 1\,(29)$. Thus $U(\mathbb{Z}/29\mathbb{Z}) = \langle 2 \rangle$. □

Proof (A shorter version). $2^{28} \equiv 1\,(29)$. It suffices to show that $2^{14} \not\equiv 1\,(29)$ and $2^4 \not\equiv 1\,(29)$. Actually, $2^{14} \equiv 28\,(29)$ and $2^4 \equiv 16\,(29)$. □

Exercise 4.11.

Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0\,(p)$ if $p-1 \nmid k$ and $-1(p)$ if $p-1 \mid k$.

Proof. Write $\langle g\rangle = U(\mathbb{Z}/p\mathbb{Z})$, and $S = 1^k + 2^k + \cdots + (p-1)^k \equiv g^k + (g^k)^2 + \cdots + (g^k)^{p-1}\ (p)$.

If $p-1 \mid k$, $g^k \equiv 1\ (p)$. Thus $S \equiv 1+1+\cdots+1 = p-1 \equiv -1\ (p)$.

If $p-1 \nmid k$, g^k is also a generator of $U(\mathbb{Z}/p\mathbb{Z})$ by Exercise 13. There are three proofs of this case.

(1) S is the sum of a geometric series. So $(1-g^k)S = g^k(1-(g^k)^{p-1}) = g^k(1-(g^{p-1})^k) \equiv 0\ (p)$. Since $g^k \not\equiv 1\ (p)$, $S \equiv 0\ (p)$.

(2) $\left\langle g^k \right\rangle = U(\mathbb{Z}/p\mathbb{Z})$. So $S \equiv g^k + (g^k)^2 + \cdots + (g^k)^{p-1} \equiv 1+2+\cdots+(p-1) \equiv \frac{p(p-1)}{2} \equiv 0\ (p)$ since p is odd and thus $\frac{p-1}{2}$ is an integer. (If $p=2$ is even, then there does not exist any k such that $p-1 \nmid k$.)

(3) Similar to (2), write $S \equiv 1+2+\cdots+(p-1)\ (p)$. Notice that the equation $x^{p-1}-1 \equiv (x-1)(x-2)\cdots(x-(p-1))\ (p)$ holds by Proposition 4.1.1. So $S \equiv 0\ (p)$ by comparing the coefficient of x^{p-2} on the both sides if $p > 2$. (Again $p=2$ is impossible in this case.)

□

Exercise 4.12.

Use the existence of a primitive root to give another proof of Wilson's theorem $(p-1)! \equiv -1\ (p)$.

Proof. Say $p > 2$. ($p = 2$ is trivial.) Let g be a primitive root of $U(\mathbb{Z}/p\mathbb{Z})$. So $(p-1)! \equiv g \cdot g^2 \cdots g^{p-1} \equiv g^{\frac{p(p-1)}{2}}\ (p)$.

The equation $x^2 \equiv 1\ (p)$ has exactly 2 solutions $x \equiv 1, -1\ (p)$ by Proposition 4.1.2. Notice that $x \equiv g^{\frac{p-1}{2}}\ (p)$ is a solution of the equation $x^2 \equiv 1\ (p)$ and $g^{\frac{p-1}{2}} \not\equiv 1\ (p)$ since g is a primitive root of $U(\mathbb{Z}/p\mathbb{Z})$. Therefore,

$$g^{\frac{p-1}{2}} \equiv -1\ (p).$$

So $(p-1)! \equiv g^{\frac{p(p-1)}{2}} \equiv (-1)^p \equiv -1\ (p)$ since p is an odd prime. □

Supplement 4.12.1.

There are many proofs of Wilson's theorem.

(1) Exercise 3.9. Use a reduced residue system modulo p.

(2) Corollary of Proposition 4.1.1. $x^{p-1}-1 \equiv (x-1)(x-2)\cdots(x-p+1)\ (p)$.

(3) Exercise 4.12. Use the existence of a primitive root.

(4) Inclusion-exclusion principle (Enrique Trevio, An Inclusion-Exclusion Proof of Wilson's Theorem).
Lemma.

$$n! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^n.$$

Proof of lemma. Consider the number of permutations on $S = \{1, 2, ..., n\}$. On the one hand, the number is $n!$. On the other hand, we can think of a permutation on S as a function $f : S \to S$ that is onto. The number of functions $g : S \to S$ is n^n. To find the onto functions, we have to remove whichever ones are not onto. Therefore, we must remove those that miss at least 1 value. There are $\binom{n}{1}$ ways of choosing the missed value and $(n-1)^n$ functions missing that particular value. But when we remove all of these functions, we took out some too many times, indeed, any function that misses at least 2 values was over counted. So we have to add it back in. We get $\binom{n}{2}(n-2)^n$ such functions. Continue this process. □

Proof. Now we use the equation $n! = \sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^n$ by substituting $n = p-1$ and then get

$$(p-1)! = \sum_{k=0}^{p-1} (-1)^k \binom{p-1}{k} (p-1-k)^{p-1}.$$

Now look at the k-term in the summation.

$k!(p-1-k)! \equiv (-1)^k(p-k)(p-(k-1))\cdots(p-1)\cdot(p-1-k)! \equiv (-1)^k(p-1)!\ (p)$. So $\binom{p-1}{k} = \frac{(p-1)!}{k!(p-1-k)!} \equiv (-1)^k\ (p)$. Also, $(p-1-k)^{p-1} \equiv (-1-k)^{p-1} \equiv (1+k)^{p-1}\ (p)$ since $(-1)^{p-1} = 1$ if $p > 2$. ($p = 2$ is trivial.) Therefore,

$$(p-1)! \equiv \sum_{k=0}^{p-1} (-1)^k \cdot (-1)^k \cdot (1+k)^{p-1} \equiv \sum_{k=1}^{p-1} k^{p-1}\ (p).$$

(We adjust the index of the summation and notice that $p^{p-1} \equiv 0\ (p)$). By Fermats Little Theorem, $k^{p-1} \equiv 1\ (p)$. Therefore, the right-hand sum consists of $(p-1)$ ones and the proof is completed. □

The original proof in the paper is not very beautiful. We don't need to use the inclusion-exclusion expression of $p!$ and then cancel out p on the both sides. Please use $(p-1)!$ directly.

(5) One combinatorial proof (Cheenta, Wilson's Theorem and It's Geometric proof).

Proof. Consider a circumference with p points that correspond to the vertices of a regular p-gon. There are $\frac{(p-1)!}{2}$ (non-regular or regular) polygons that we form by joining these vertices.

Now among $\frac{(p-1)!}{2}$ of them, we have $\frac{p-1}{2}$ unaltered when rotated by $\frac{2\pi}{p}$ radian. That is, there are $\frac{p-1}{2}$ regular polygons due to the rotational symmetry.

Therefore, there are $\frac{(p-1)!}{2} - \frac{p-1}{2}$ non-regular polygons. Notices that the number of non-regular polygons is divided by p since p is a prime.

So $\frac{(p-1)!}{2} - \frac{p-1}{2} \equiv 0\,(p)$. Hence, $(p-1)! \equiv p-1 \equiv -1\,(p)$ if $p > 2$. ($p = 2$ is trivial.) $\square$

Supplement 4.12.2.

Related problems.

(1) (ProjectEuler 381: (prime-k) factorial). *Let* $S(p) = \sum_{1\le k\le 5}(p-k)!\,(p)$ *for a prime* p. *Find* $\sum_{1\le p\le 10^8} S(p)$ (by using computer programs).

(2) *Let* g *be a primitive root modulo the odd prime* p. *Prove that* $g^{\frac{p-1}{2}} \equiv -1(p)$. *Deduce that if* g, h *are primitive roots modulo the odd prime* p *then* $g \cdot h$ *cannot be a primitive root.*

Exercise 4.13. (Generators of a cyclic group)

Let G *be a finite cyclic group and* $g \in G$ *is a generator. Show that all the other generators are of the form* g^k, *where* $(k, n) = 1$, n *being the order of* G.

Proof. Suppose that $h = g^k$ with $(k, n) = 1$. Then clearly $\langle h\rangle \subseteq \langle g\rangle$ as a subset. For the reverse containment ($\supseteq$), write $rk + sn = 1$ where $r, s \in \mathbb{Z}$. Then $h^r = g^{kr} = g^{1-sn} = g \cdot (g^n)^{-s} = g \cdot 1 = g$. Then again $\langle g\rangle \subseteq \langle h\rangle$ as a subset.

Now suppose that $\langle g\rangle = \langle h\rangle$. Then $h = g^k$ for some $k \in \mathbb{Z}$. Also, $g = h^r$ for some $r \in \mathbb{Z}$. So $g = h^r = g^{kr}$ or $g^{kr-1} = 1$. So $n|(kr-1)$, or $ar + ns = 1$ for some $s \in \mathbb{Z}$, that is, $(a, n) = 1$. $\square$

Reference: R. C. Daileda, The Structure of $U(\mathbb{Z}/n\mathbb{Z})$.

Corollary. *Let G be a finite cyclic group of order n. Then G has exactly $\phi(n)$ generators.*

Corollary. *$U(\mathbb{Z}/p\mathbb{Z})$ has exactly $\phi(p-1)$ generators. $U(\mathbb{Z}/p^l\mathbb{Z})$ has exactly $\phi(p^{l-1}(p-1))$ generators if p is odd.*

Exercise 4.22.

If a has order 3 modulo p, show that $1+a$ has order 6.

Proof. Since a has order 3, $0 \equiv a^3 - 1 \equiv (a-1)(a^2+a+1)\,(p)$. Since p is a prime, $a-1 \equiv 0\,(p)$ or $a^2+a+1 \equiv 0\,(p)$. a cannot be 1 since a has order $3 \neq 1$. Therefore,

$$a^2 + a + 1 \equiv 0\,(p),$$

or $1 + a \equiv -a^2 \equiv -a^{-1}\,(p)$. So

$$\begin{aligned}(1+a)^6 &\equiv (-a^{-1})^6 \equiv 1\,(p),\\ 1+a &\not\equiv 1\,(p),\\ (1+a)^2 &\equiv a \not\equiv 1\,(p),\\ (1+a)^3 &\equiv -1 \not\equiv 1\,(p).\end{aligned}$$

Hence $1+a$ has order 6. □

Chapter 5: Quadratic Reciprocity

Exercise 5.2.

Show that the number of solutions to $x^2 \equiv a\,(p)$ *is given by* $1 + (a/p)$.

p is an odd prime.

Proof.

(1) If $x \equiv t\,(p)$ is a solution of the equation $x^2 \equiv a\,(p)$, then $x \equiv -t\,(p)$ is also a solution. Notice that $t \not\equiv -t\,(p)$ if $t \not\equiv 0\,(p)$ by using the fact that p is odd.

(2) (Lemma 4.1.) Let $f(x) \in k[x]$, k a field. Suppose that $\deg f(x) = n$. Then f has at most n distinct roots.

(3) If $a = 0$, then $x^2 \equiv 0\,(p)$ has only one solution $x \equiv 0\,(p)$, or $1 + (a/p)$ solution (where $(a/p) = 0$ in this case).

(4) If $a \neq 0$ is a quadratic residue mod p, then by (1)(2) the equation $x^2 \equiv a(p)$ has exactly 2 solutions, or $1 + (a/p)$ solutions (where $(a/p) = 1$ in this case).

(5) If a is not a quadratic residue mod p, then there is no solutions of the equation $x^2 \equiv a\,(p)$, or $1 + (a/p)$ solutions (where $(a/p) = -1$ in this case).

By (3)(4)(5), in any case the number of solutions to $x^2 \equiv a\,(p)$ is given by $1 + (a/p)$. □

Exercise 5.4.

Prove that $\sum_{a=1}^{p-1}(a/p) = 0$.

Note. $\sum_{a=0}^{p-1}(a/p) = 0$ since $(0/p) = 0$.

Proof. There are as many residues as nonresidues mod p (Corollary to Proposition 5.1.2). □

Exercise 5.5.

Prove that $\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0$ *provided that* $p\nmid a$.

Proof. Since x $(x=1,\ldots,p-1)$ is a reduced residue system modulo p, ax $(x=1,\ldots,p-1)$ is again a reduced residue system modulo p if $p\nmid a$ (Exercise 3.6). Hence

$$\sum_{x=1}^{p-1}\left(\frac{ax}{p}\right)=0.$$

Note that $\left(\frac{0}{p}\right)=0$, and thus $0=\sum_{x=0}^{p-1}\left(\frac{ax}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{a(x+a^{-1}b)}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)$.
□

Exercise 5.6.

Show that the number of solutions to $x^2-y^2\equiv a\,(p)$ *is given by*

$$\sum_{y=0}^{p-1}\left(1+\left(\frac{y^2+a}{p}\right)\right).$$

Proof. Write $x^2\equiv y^2+a\,(p)$. For every fixed $y=0,\ldots,p-1$, the number of solutions x to $x^2\equiv y^2+a\,(p)$ is given by $1+\left(\frac{y^2+a}{p}\right)$ (Exercise 5.2). Hence, the number of solutions (x,y) to $x^2-y^2\equiv a\,(p)$ is

$$\sum_{y=0}^{p-1}\left(1+\left(\frac{y^2+a}{p}\right)\right).$$

□

Exercise 5.7.

By calculating directly show that the number of solutions to $x^2-y^2\equiv a\,(p)$ *is* $p-1$ *if* $p\nmid a$ *and* $2p-1$ *if* $p\mid a$. *(Hint: Use the change of variables* $u=x+y, v=x-y$.*)*

Proof (Hint). Write $(x+y)(x-y)\equiv a(p)$ or $uv\equiv a(p)$ where $u=x+y, v=x-y$. For any a, either $a\equiv 0\,(p)$ or $a\not\equiv 0\,(p)$.

(1) $a\equiv 0\,(p)$. Then $u=0$ or $v=0$. Consider three possible cases (may be overlapped).

(a) $u = 0$, or $x + y = 0$. In this case, the number of solutions is p. ($x = k, y = -k$ for $k = 0, \ldots, p-1$.)

(b) $v = 0$. Similar to (a), the number of solutions is p. ($x = k, y = k$ for $k = 0, \ldots, p-1$.)

(c) $u = v = 0$. $x = y = 0$.

By (a)(b)(c), there are $2p - 1$ solutions to $x^2 - y^2 \equiv 0\ (p)$.

(2) $a \not\equiv 0\ (p)$. $u \neq 0$ and $v \neq 0$. For each $u = k$ for $k = 1, \ldots, p-1$, there is one unique $v = ak^{-1}$ such that $uv \equiv a\ (p)$. Solve u and v to get $(x, y) = (2^{-1}(k + ak^{-1}), 2^{-1}(k - ak^{-1})) \in \mathbb{Z}/p\mathbb{Z}$ for $k = 1, \ldots, p-1$. So there are $p - 1$ solutions to $x^2 - y^2 \equiv a\ (p)$ where $a \not\equiv 0\ (p)$.

By (1)(2), the result holds. □

Exercise 5.8.

Combining the results of Exercise 5.6 and 5.7 show that

$$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p} \right) = \begin{cases} -1, & \text{if } p \nmid a, \\ p - 1, & \text{if } p \mid a. \end{cases}$$

Proof. By Exercise 5.6 and 5.7,

$$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p} \right) \right) = \begin{cases} p - 1, & \text{if } p \nmid a, \\ 2p - 1, & \text{if } p \mid a. \end{cases}$$

Hence the result holds. □

Chapter 6: Quadratic Gauss Sums

Exercise 6.1.

Show that $\sqrt{2}+\sqrt{3}$ is an algebraic integer.

Proof. Let $\alpha = \sqrt{2}+\sqrt{3}$. So $\alpha - \sqrt{2} = \sqrt{3}$. Eliminating $\sqrt{3}$ by squaring: $(\alpha-\sqrt{2})^2 = (\sqrt{3})^2$, or $\alpha^2-2\sqrt{2}\alpha+2 = 3$, or $\alpha^2-1 = 2\sqrt{2}\alpha$. Eliminating $\sqrt{2}$ by squaring again: $(\alpha^2-1)^2 = (2\sqrt{2}\alpha)^2$, or $\alpha^4-2\alpha^2+1 = 8\alpha^2$, or $\alpha^4-10\alpha^2+1 = 0$. That is, α is a root of $x^4-10x^2+1=0$, i.e., α is an algebraic integer. □

Actually, $x^4-10x^2+1 = (x-\sqrt{2}-\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}+\sqrt{3})$.

Proof (Proposition 6.1.5). Since $\sqrt{2}$ and $\sqrt{3}$ are algebraic integers, then $\sqrt{2}+\sqrt{3}$ is an algebraic integer by Proposition 6.1.5. (The set of algebraic integers forms a ring.) □

Exercise 6.2.

Let α be an algebraic number. Show that there is an integer n such that $n\alpha$ is an algebraic integer.

It is trivial if taking $n=0$. So we assume that $n \neq 0$.

Proof. There exists a polynomial $f(x) = a_0x^m + a_1x^{m-1} + \cdots + a_m \in \mathbb{Q}[x]$ with $a_0 \neq 0$, such that $f(\alpha) = 0$. There exists an integer $d \neq 0$ such that $b_i = d \cdot a_i \in \mathbb{Z}$ for all $i = 1, 2, ..., m$. Therefore,

$$b_0\alpha^m + b_1\alpha^{m-1} + \cdots + b_m = 0,$$

which is not necessary a monic polynomial in $\mathbb{Z}[x]$. So we need to do a trick to absort b_0 into α, and that is why we come out multipling α by an non-zero integer $b_0 = d \cdot a_0$.

Multiply b_0^{m-1} on the both sides.

$$b_0^m\alpha^m + b_0^{m-1}b_1\alpha^{m-1} + b_0^{m-1}b_2\alpha^{m-2} + \cdots + b_0^{m-1}b_m = 0.$$
$$(b_0\alpha)^m + b_1(b_0\alpha)^{m-1} + b_0b_2(n\alpha)^{m-1} + \cdots + b_0^{m-1}b_m = 0.$$

That is, the monic polynomial $g(x) = x^m + c_1x^{m-1} + c_2x^{m-2} + \cdots + c_m \in \mathbb{Z}[x]$ (with $c_i = b_0^{i-1}b_i$ for $i = 1, 2, ..., m$) has a root $x = b_0\alpha$, i.e., $b_0\alpha$ is an algebraic integer for some integer b_0. □

Exercise 6.4.

A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be primitive if the greatest common divisor of its coefficients is 1. Prove that the product of primitive polynomials is again primitive. This is one of the many results knows as Gauss' lemma.

Proof. Let

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n,$$
$$g(x) = b_0x^m + b_1x^{n-1} + \cdots + b_m$$

be primitive.

(1) Given prime p. Let a_i and b_j be the coefficients with the smallest index such that $p \nmid a_i$ and $p \nmid b_j$ respectively. Consider the coefficient of x^{i+j} in $f(x)g(x)$,

$$(\cdots + a_{i-1}b_{j+1}) + a_ib_j + (a_{i+1}b_{j-1} + \cdots).$$

$p \nmid a_ib_j$ since p is a prime. $p \mid (\cdots + a_{i-1}b_{j+1})$ by the definition of index i. $p \mid (a_{i+1}b_{j-1} + \cdots)$ by the definition of index j. That is, the coefficient of x^{i+j} in $f(x)g(x)$ is not divided by p.

(2) If $h(x) = f(x)g(x)$ is not primitive, there exists a prime p such that p divides all coefficients of $h(x)$. By (1), such i or j does not exist. That is, p is a factor of the greatest common divisor of $f(x)$'s or $g(x)$'s coefficients. So $f(x)$ or $g(x)$ is not primitive, which is absurd.

□

Exercise 6.16.

Let α be an algebraic number with minimal polynomial $f(x)$. Show that $f(x)$ does not have repeated roots α in $\mathbb{C}$.

Proof. Assume not true, write $f(x) = (x-\alpha)^2g(x)$, where $g(x) \in \mathbb{C}[x]$. Differentiating $f(x)$ to get new polynomial $f'(x) \in \mathbb{Q}[x]$ and

$$\begin{aligned} f'(x) &= 2(x-\alpha)g(x) + (x-\alpha)^2g'(x) \\ &= (x-\alpha)(2g(x) + (x-\alpha)g'(x)). \end{aligned}$$

So $f'(\alpha) = 0$. Notices that $\deg f(x) \geq 2$ and thus $\deg f'(x) = \deg f(x) - 1 \geq 1$. $f'(x)$ is not zero. Thus $f(x) \mid f'(x)$ by Proposition 6.1.7, which contradicts the fact $0 < \deg f'(x) < \deg f(x)$. □

Exercise 6.17.

Show that the minimal polynomial for $\sqrt[3]{2}$ is $x^3 - 2$.

Proof. Let $f(x) = x^3 - 2$. $f(\sqrt[3]{2}) = 0$. By Eisenstein's irreducibility criterion, $f(x)$ is irreducible over $\mathbb{Q}$. By Proposition 6.1.7, $f(x) = x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$. $\square$

Exercise 6.18.

Show that there exist algebraic numbers of arbitrarily high degree.

A generalization to Exercise 6.17.

If p is a prime, then $x^n - p$ is irreducible over $\mathbb{Q}$, by Eisenstein's irreducibility criterion, so $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$. (Example 1.16 in Patrick Morandi, Field and Galois Theory.)

Proof. Let $\alpha = \sqrt[n]{p}$ for any positive integer n with $n \geq 2$ and prime p. Apply the similar argument in Exercise 6.17 to show that $f(x) = x^n - p$ is the minimal polynomial of $\sqrt[n]{p}$. $\square$

Exercise 6.23.

If $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $a_i \in \mathbb{Z}$ and p is a prime such that $p \mid a_i$, $i = 1, ..., n$, $p^2 \nmid a_n$. Show that $f(x)$ is irreducible over $\mathbb{Q}$ (Eisenstein's irreducibility criterion).

Proof.

(1) *If $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, $a_i \in \mathbb{Z}$ and p is a prime such that $p \mid a_i$, $i = 1, ..., n$, $p^2 \nmid a_n$. Then $f(x)$ is irreducible over $\mathbb{Z}$.* Assume not true. Write $f(x) = g(x)h(x)$ as a product of two non-trivial polynomials in $\mathbb{Z}[x]$,

$$g(x) = b_0 x^s + b_1 x^{s-1} + \cdots + b_s,$$
$$h(x) = c_0 x^t + c_1 x^{t-1} + \cdots + c_t,$$

where $b_0 = c_0 = 1$, $0 < s < n$, and $0 < t < n$.

Since $p \nmid b_0$, there exists largest index i such that $p \nmid b_i$. (Therefore $p \mid b_{i+1}$, $p \mid b_{i+2}$, and so on.) Similarly, there exists largest index j such that $p \nmid c_j$. ($p \mid c_{j+1}$, $p \mid c_{j+2}$, and so on.) Now we consider the coefficient a_{i+j}.

$$a_{i+j} = (\cdots + b_{i-1}c_{j+1}) + b_i c_j + (b_{i+1}c_{j-1} + \cdots).$$

$p \nmid b_i c_j$ since p is a prime. $p \mid (b_{i+1}c_{j-1} + \cdots)$ by the definition of index i. $p \mid (\cdots + b_{i-1}c_{j+1})$ By the definition of index j. Thus, $p \nmid a_{i+j}$. Hence $i = 0$ and $j = 0$. Especially, $p \mid b_s$ and $p \mid c_t$. $p^2 \mid b_s c_t$, or $p^2 \mid a_n$ which contradicts. □

(2) *$f(x)$ is irreducible over $\mathbb{Q}$ if $f(x)$ is primitive and irreducible over $\mathbb{Z}$.* Assume $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ is reducible. Let a and b be the least common multiple of the denominators of $g(x)$ and $h(x)$ respectively. Then

$$ab \cdot f(x) = (a \cdot g(x))(b \cdot h(x)) = cg_0(x)dh_0(x),$$

where $g_0(x)$, $h_0(x)$ are primitive polynomials in $\mathbb{Z}[x]$, and c and d are the greatest common divisor of $(a \cdot g(x))$'s and $(b \cdot h(x))$'s coefficients respectively Since $g_0(x)h_0(x)$ is again primitive (Exercise 4),

$$ab = \pm cd, f(x) = g_0(x)h_0(x).$$

Notice that $\deg(g_0(x)) = \deg(g(x))$ and $\deg(h_0(x)) = \deg(h(x))$. So $f(x)$ is reducible over $\mathbb{Z}$, which is absurd.

□

Chapter 15: Bernoulli Numbers

Supplement.

Equation (4) on page 231. *Prove that*

$$x \cot x = 1 - 2 \sum_{n=1}^{\infty} \frac{x^2}{n^2\pi^2 - x^2}.$$

Proof (Exercise 6.73 in the book Graham, Knuth and Patashnik, Concrete Mathematics, Second Edition).

(1) *Show that*

$$\cot x = \frac{1}{2^n} \sum_{k=0}^{2^n-1} \cot \frac{x + k\pi}{2^n}$$

for all integers $n \geq 1$. Notice that

$$\begin{aligned} \cot(x + \pi) &= \cot x, \\ \cot\left(x + \frac{\pi}{2}\right) &= -\tan x, \\ \cot x &= \frac{1}{2}\left(\cot\frac{x}{2} - \tan\frac{x}{2}\right). \end{aligned}$$

Use mathematical induction. The case $n = 1$ is the same as the note. Assume the case $n = m$ holds. For $n = m + 1$,

$$\begin{aligned} \sum_{k=0}^{2^{m+1}-1} \cot \frac{x + k\pi}{2^{m+1}} &= \sum_{k=0}^{2^m-1} \cot \frac{x + k\pi}{2^{m+1}} + \sum_{k=2^m}^{2^{m+1}-1} \cot \frac{x + k\pi}{2^{m+1}} \\ &= \sum_{k=0}^{2^m-1} \cot \frac{x + k\pi}{2^{m+1}} + \sum_{k=0}^{2^m-1} \cot \frac{x + (2^m + k)\pi}{2^{m+1}} \\ &= \sum_{k=0}^{2^m-1} \cot \frac{x + k\pi}{2^{m+1}} + \sum_{k=0}^{2^m-1} \cot \left(\frac{x + k\pi}{2^{m+1}} + \frac{\pi}{2}\right) \\ &= \sum_{k=0}^{2^m-1} \left(\cot \frac{x + k\pi}{2^{m+1}} - \tan \frac{x + k\pi}{2^{m+1}}\right) \\ &= \sum_{k=0}^{2^m-1} \left(\cot \frac{x + k\pi}{2^{m+1}} - \tan \frac{x + k\pi}{2^{m+1}}\right) \\ &= 2 \sum_{k=0}^{2^m-1} \cot \frac{x + k\pi}{2^m}. \end{aligned}$$

Therefore,

$$\begin{aligned}\frac{1}{2^{m+1}}\sum_{k=0}^{2^{m+1}-1}\cot\frac{x+k\pi}{2^{m+1}} &= \frac{1}{2^{m+1}}\cdot 2\sum_{k=0}^{2^m-1}\cot\frac{x+k\pi}{2^m}\\ &= \frac{1}{2^m}\sum_{k=0}^{2^m-1}\cot\frac{x+k\pi}{2^m}\\ &= \cot x.\end{aligned}$$

(2) By rearranging the index of summation of the identity in (1), we have

$$x\cot x = \frac{x}{2^n}\cot\frac{x}{2^n} - \frac{x}{2^n}\tan\frac{x}{2^n} + \sum_{k=1}^{2^{n-1}-1}\frac{x}{2^n}\left(\cot\frac{x+k\pi}{2^n}+\cot\frac{x-k\pi}{2^n}\right)$$

for all integers $n \geq 1$.

(3) Notice that $\lim_{x\to 0} x\cot x = 1$. Let $n \to \infty$, the result is established.

□

Exercise 15.1.

Using the definition of the Bernoulli number show $B_{10} = \frac{5}{66}$ *and* $B_{12} = -\frac{691}{2730}$.

Proof.

(1) It is known that $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$, and $B_m = 0$ for odd $m > 1$.

(2) Recall the implicit recurrence relation,

$$\sum_{k=0}^{m}\binom{m+1}{k}B_k = [m=0],$$

where $[m = 0]$ is the Iverson brackets which is equal to the Kronecker delta δ_{m0}.

(3) So

$$\begin{aligned}0 &= 1 + 9B_1 + 36B_2 + 84B_3 + 126B_4 + 126B_5 + 84B_6 + 36B_7 + 9B_8,\\ 0 &= 1 + 9B_1 + 36B_2 + 126B_4 + 84B_6 + 9B_8,\\ 0 &= 1 + 9\left(-\frac{1}{2}\right) + 36\left(\frac{1}{6}\right) + 126\left(-\frac{1}{30}\right) + 84\left(\frac{1}{42}\right) + 9B_8,\\ 0 &= \frac{3}{10} + 9B_8,\end{aligned}$$

Thus $B_8 = -\frac{1}{30}$.

(4) Again,

$$\begin{aligned}
0 =& 1 + 11B_1 + 55B_2 + 165B_3 + 330B_4 + 462B_5 + 462B_6 + \\
& 330B_7 + 165B_8 + 55B_9 + 11B_{10}, \\
0 =& 1 + 11B_1 + 55B_2 + 330B_4 + 462B_6 + 165B_8 + 11B_{10}, \\
0 =& 1 + 11\left(-\frac{1}{2}\right) + 55\left(\frac{1}{6}\right) + 330\left(-\frac{1}{30}\right) + 462\left(\frac{1}{42}\right) + \\
& 165\left(-\frac{1}{30}\right) + 11B_{10}, \\
0 =& -\frac{5}{6} + 11B_{10},
\end{aligned}$$

Thus $B_{10} = \frac{5}{66}$.

(4) Finally,

$$\begin{aligned}
0 =& 1 + 13B_1 + 78B_2 + 286B_3 + 715B_4 + 1287B_5 + 1716B_6 + \\
& 1716B_7 + 1287B_8 + 715B_9 + 286B_{10} + 78B_{11} + 13B_{12}, \\
0 =& 1 + 13B_1 + 78B_2 + 715B_4 + 1716B_6 + 1287B_8 + 286B_{10} + 13B_{12}, \\
0 =& 1 + 13\left(-\frac{1}{2}\right) + 78\left(\frac{1}{6}\right) + 715\left(-\frac{1}{30}\right) + 1716\left(\frac{1}{42}\right) + \\
& 1287\left(-\frac{1}{30}\right) + 286\left(\frac{5}{66}\right) + 13B_{12}, \\
0 =& \frac{691}{210} + 13B_{12},
\end{aligned}$$

Thus $B_{12} = -\frac{691}{2730}$.

□

Exercise 15.2.

If $a \in \mathbb{Z}$, show $a(a^m - 1)B_m \in \mathbb{Z}$ for all $m > 0$.

Proof.

(1) *Trivial cases.* If $m = 1$, $a(a-1)B_1 = -\frac{1}{2}a(a-1) \in \mathbb{Z}$ for any $a \in \mathbb{Z}$. For odd $m > 1$, $B_m = 0$ or $a(a^m - 1)B_m = 0 \in \mathbb{Z}$ (Proposition 15.1.1).

(2) *Consider that $m > 1$ and even.* By Theorem 3,

$$B_{2m} + \sum_{p-1|2m} \frac{1}{p} \in \mathbb{Z}$$

where the sum is over all primes p such that $p - 1 \mid 2m$. So it suffices to show

$$a(a^{2m} - 1) \sum_{p-1|2m} \frac{1}{p} \in \mathbb{Z},$$

or

$$a(a^{2m} - 1)\frac{1}{p} \in \mathbb{Z}$$

for any $a \in \mathbb{Z}$ and any prime p such that $p - 1 \mid 2m$.

(3) *Consider all possible a.* If $p \mid a$, it is trivial. If $p \nmid a$, $a^{p-1} \equiv 1\ (p)$ by Fermat's Little Theorem, or $a^{2m} \equiv 1\ (p)$ by $p - 1 \mid 2m$. In any cases, $a(a^{2m} - 1)\frac{1}{p} \in \mathbb{Z}$.

□

Exercise 15.6.

For $m \geq 3$, show $|B_{2m+2}| > |B_{2m}|$. (Hint: Use Theorem 2.)

Proof. By Theorem 2,

$$2\zeta(2m) = (-1)^{m+1}\frac{(2\pi)^{2m}}{(2m)!}B_{2m}.$$

Thus,

$$\frac{|B_{2m+2}|}{|B_{2m}|} = \frac{\zeta(2m+2)(2m+2)(2m+1)}{\zeta(2m)(2\pi)^2} > \frac{1 \cdot 8 \cdot 7}{\zeta(6) \cdot (2\pi)^2} = \frac{13230}{\pi^8} > 1,$$

or $|B_{2m+2}| > |B_{2m}|$. □

Exercise 15.8.

Consider the power series expansion of $\tan x$ *about the origin;*

$$\sum_{k=1}^{\infty} T_k \frac{x^{2k-1}}{(2k-1)!}.$$

Show

$$T_k = (-1)^{k-1}\frac{B_{2k}}{2k}(2^{2k}-1)2^{2k}.$$

Note that $T_k \in \mathbb{Z}$ for all k by Exercise 3.

Proof.

(1) By the equation (6) on page 232,

$$x\cot x = 1 + \sum_{k=2}^{\infty} B_k \frac{(2ix)^k}{k!}.$$

Since $B_k = 0$ for odd $k > 1$,

$$x\cot x = 1 + \sum_{k=1}^{\infty} B_{2k}\frac{(2ix)^{2k}}{(2k)!} = 1 + \sum_{k=1}^{\infty}\frac{(-1)^k 2^{2k} B_{2k}}{(2k)!}x^{2k},$$

or

$$\cot x = \frac{1}{x} + \sum_{k=1}^{\infty}\frac{(-1)^k 2^{2k} B_{2k}}{(2k)!}x^{2k-1}.$$

Combine the first term $\frac{1}{x}$ into the summation,

$$\cot x = \sum_{k=0}^{\infty}\frac{(-1)^k 2^{2k} B_{2k}}{(2k)!}x^{2k-1}.$$

(2) Note that $\tan x = \cot x - 2\cot(2x)$. By (1),

$$\begin{aligned}\tan x &= \sum_{k=0}^{\infty}\frac{(-1)^k 2^{2k} B_{2k}}{(2k)!}x^{2k-1} - 2\sum_{k=0}^{\infty}\frac{(-1)^k 2^{2k} B_{2k}}{(2k)!}(2x)^{2k-1} \\ &= \sum_{k=0}^{\infty}\frac{(-1)^k (1-2^{2k}) 2^{2k} B_{2k}}{(2k)!}x^{2k-1} \\ &= \sum_{k=1}^{\infty}\frac{(-1)^k (1-2^{2k}) 2^{2k} B_{2k}}{(2k)!}x^{2k-1}.\end{aligned}$$

Write $T_k = (-1)^{k-1}(2^{2k}-1)2^{2k}\frac{B_{2k}}{2k}$. Therefore, $\tan x = \sum_{k=1}^{\infty} T_k \frac{x^{2k-1}}{(2k-1)!}$.

By Exercise 15.3, $(2^{2k}-1)2^{2k}\frac{B_{2k}}{2k} \in \mathbb{Z}$, or $T_k \in \mathbb{Z}$ for all k. □

Exercise 15.12.

Recall the definition of the Bernoulli polynomials;

$$B_m(x) = \sum_{k=0}^{m} \binom{m}{k} B_k x^{m-k}.$$

Show that

$$\frac{te^{tx}}{e^t - 1} = \sum_{m=0}^{\infty} B_m(x) \frac{t^m}{m!}.$$

Proof. By Lemma 1,

$$\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}.$$

So

$$\frac{te^{tx}}{e^t - 1} = \left(\sum_{m=0}^{\infty} B_m \frac{t^m}{m!} \right) \left(\sum_{m=0}^{\infty} x^m \frac{t^m}{m!} \right).$$

Write $\frac{te^{tx}}{e^t-1} = \sum_{m=0}^{\infty} b_m(x) \frac{t^m}{m!}$ and we want to check if $b_m(x) = B_m(x)$ or not. The result is established if $b_m(x) = B_m(x)$ holds. Equating coefficients of t^m gives

$$\begin{aligned}
\frac{b_m(x)}{m!} &= \sum_{k=0}^{m} \frac{B_k x^{m-k}}{k!(m-k)!}, \\
b_m(x) &= \sum_{k=0}^{m} \frac{m!}{k!(m-k)!} B_k x^{m-k} \\
&= \sum_{k=0}^{m} \binom{m}{k} B_k x^{m-k} \\
&= B_m(x).
\end{aligned}$$

□

Exercise 15.13.

Show $B_m(x+1) - B_m(x) = mx^{m-1}$.

Proof. Let $f(t,x) = \frac{te^{tx}}{e^t-1}$.

(1)

$$f(t, x+1) - f(t,x) = \frac{te^{t(x+1)}}{e^t - 1} - \frac{te^{tx}}{e^t - 1} = te^{tx}.$$

Expand te^{tx} in a power series about the origin as follows

$$\begin{aligned} te^{tx} &= t\sum_{m=0}^{\infty} x^m \frac{t^m}{m!} \\ &= \sum_{m=0}^{\infty} x^m \frac{t^{m+1}}{m!} \\ &= \sum_{m=1}^{\infty} x^{m-1} \frac{t^m}{(m-1)!} \\ &= \sum_{m=1}^{\infty} m x^{m-1} \frac{t^m}{m!} \\ &= \sum_{m=0}^{\infty} m x^{m-1} \frac{t^m}{m!}. \end{aligned}$$

So,

$$f(t, x+1) - f(t, x) = \sum_{m=0}^{\infty} m x^{m-1} \frac{t^m}{m!}.$$

(2) By Exercise 15.12,

$$\begin{aligned} f(t, x+1) - f(t, x) &= \sum_{m=0}^{\infty} B_m(x+1)\frac{t^m}{m!} - \sum_{m=0}^{\infty} B_m(x)\frac{t^m}{m!} \\ &= \sum_{m=0}^{\infty} (B_m(x+1) - B_m(x))\frac{t^m}{m!}. \end{aligned}$$

By (1)(2), comparing coefficients of t^m yields

$$m x^{m-1} = B_m(x+1) - B_m(x).$$

□

Exercise 15.14.

Use Exercise 13 to give a new proof of Theorem 1:

$$S_m(n) = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}).$$

Proof. By Exercise 13,

$$B_{m+1}(k) - B_{m+1}(k-1) = (m+1)(k-1)^m$$

for any k. So,

$$\sum_{k=1}^{n}(B_{m+1}(k)-B_{m+1}(k-1))=\sum_{k=1}^{n}(m+1)(k-1)^m,$$
$$B_{m+1}(n)-B_{m+1}(0)=(m+1)S_m(n).$$

Note that $B_{m+1}(0)=B_{m+1}$ for any m. So Theorem 1 is established by a new proof. □

Exercise 15.15.

Suppose $f(x)=\sum_{k=0}^{n}a_kx^k$ be a polynomial with complex coefficients. Use Exercise 13 to find a polynomial $F(x)$ such that $F(x+1)-F(x)=f(x)$.

Proof. By Exercise 15.13,

$$x^k=\frac{1}{k+1}(B_{k+1}(x+1)-B_{k+1}(x))$$

for $k\geq 0$. Thus,

$$\begin{aligned}f(x)&=\sum_{k=0}^{n}a_kx^k\\&=\sum_{k=0}^{n}a_k\cdot\frac{1}{k+1}(B_{k+1}(x+1)-B_{k+1}(x))\\&=\sum_{k=0}^{n}\frac{a_k}{k+1}B_{k+1}(x+1)-\sum_{k=0}^{n}\frac{a_k}{k+1}B_{k+1}(x).\end{aligned}$$

Let

$$F(x)=\sum_{k=0}^{n}\frac{a_k}{k+1}B_{k+1}(x),$$

and we get $f(x)=F(x+1)-F(x)$. □

Exercise 15.16.

For $n\geq 1$, show $\frac{d}{dx}B_n(x)=nB_{n-1}(x)$.

Proof. For $n\geq 1$,

$$\frac{d}{dx}B_n(x)=\sum_{k=0}^{n}(n-k)\binom{n}{k}B_kx^{n-k-1}=\sum_{k=0}^{n-1}(n-k)\binom{n}{k}B_kx^{n-k-1}.$$

Note that

$$(n-k)\binom{n}{k} = n\binom{n-1}{k}.$$

So

$$\begin{aligned}\frac{d}{dx}B_n(x) &= \sum_{k=0}^{n-1} n\binom{n-1}{k}B_k x^{n-k-1} \\ &= n\sum_{k=0}^{n-1}\binom{n-1}{k}B_k x^{n-k-1} \\ &= nB_{n-1}(x).\end{aligned}$$

□

Exercise 15.17.

Show $B_n(1-x) = (-1)^n B_n(x)$.

Proof. Let $f(t,x) = \frac{te^{tx}}{e^t-1}$.

(1) $f(t,1-x) = f(-t,x)$.

$$f(t,1-x) = \frac{te^{t(1-x)}}{e^t-1} = e^t \cdot \frac{te^{-tx}}{e^t-1} = \frac{-te^{-tx}}{e^{-t}-1} = f(-t,x).$$

(2) By Exercise 15.12,

$$\begin{aligned}f(t,1-x) &= \sum_{n=0}^{\infty} B_n(1-x)\frac{t^n}{n!} \\ f(-t,x) &= \sum_{n=0}^{\infty}(-1)^n B_n(x)\frac{t^n}{n!}.\end{aligned}$$

By (1), comparing coefficients of t^n yields $B_n(1-x) = (-1)^n B_n(x)$.

□

Exercise 15.18.

Use Exercise 13 and 17 to give a new proof that $B_n = 0$ *for* n *odd and* $n > 1$.

Proof.

(1) $B_m(1) - B_m(0) = 0$ *for any* $m > 1$. Taking $x = 0$ in Exercise 15.13 and keeping $m - 1 > 0$ or $m > 1$.

(2) $B_m(1) = -B_m(0)$ *for any odd* m. Taking $x = 0$ in Exercise 15.17 and keeping m is odd.

$$f(t, 1-x) = \sum_{n=0}^{\infty} B_n(1-x)\frac{t^n}{n!}$$
$$f(-t, x) = \sum_{n=0}^{\infty} (-1)^n B_n(x)\frac{t^n}{n!}.$$

By (1)(2), for m odd and $m > 1$, $B_m(0) = 0$ or $B_m = 0$. □

Exercise 15.19. (Multiplication theorem for Bernoulli polynomial)

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

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

(Hint: Use Exercise 12.)

Proof. By $x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1})$ (Exercise 1.24),

$$e^{Ft} - 1 = (e^t - 1)(1 + e^t + e^{2t} + \cdots + e^{(F-1)t}) = (e^t - 1)\sum_{a=0}^{F-1} e^{at}.$$

So,

$$\begin{aligned}
\frac{1}{e^t - 1} &= \frac{1}{e^{Ft} - 1}\sum_{a=0}^{F-1} e^{at}, \\
\frac{te^{tFx}}{e^t - 1} &= \frac{te^{tFx}}{e^{Ft} - 1}\sum_{a=0}^{F-1} e^{at} \\
&= \sum_{a=0}^{F-1} \frac{te^{(Fx+a)t}}{e^{Ft} - 1} \\
&= \sum_{a=0}^{F-1} \frac{te^{(Fx+a)t}}{e^{Ft} - 1} \\
&= \sum_{a=0}^{F-1} F^{-1}\frac{(Ft)e^{(x+\frac{a}{F})(Ft)}}{e^{Ft} - 1}.
\end{aligned}$$

By Exercise 15.12,

$$\begin{aligned}\sum_{n=0}^{\infty} B_n(Fx)\frac{t^n}{n!} &= \sum_{a=0}^{F-1} F^{-1} \sum_{n=0}^{\infty} B_n\left(x+\frac{a}{F}\right)\frac{(Ft)^n}{n!} \\ &= \sum_{n=0}^{\infty}\sum_{a=0}^{F-1} F^{-1} B_n\left(x+\frac{a}{F}\right)\frac{(Ft)^n}{n!} \\ &= \sum_{n=0}^{\infty}\sum_{a=0}^{F-1} F^{n-1} B_n\left(x+\frac{a}{F}\right)\frac{t^n}{n!}.\end{aligned}$$

Comparing coefficients of t^n on the both sides of the above equation and yields $B_n(Fx) = F^{n-1}\sum_{a=0}^{F-1} B_n\left(x+\frac{a}{F}\right)$. $\square$

Supplement 15.19.1. (Multiplication Theorem for $\frac{1}{\exp(z)-1}$)

$$\frac{1}{\exp(nz)-1} = \frac{1}{n}\sum_{k=0}^{n-1}\frac{1}{\exp\left(z+\frac{2k\pi i}{n}\right)-1}.$$

Proof. Let ζ be one n-th root of unity. Write $f(x) = x^n - 1 = \prod_{k=0}^{n-1}(x-\zeta^k)$. By Lagrange interpolation,

$$\begin{aligned}\frac{1}{f(x)} &= \sum_{k=0}^{n-1}\frac{1}{f'(\zeta^k)}\cdot\frac{1}{x-\zeta^k} \\ \frac{1}{x^n-1} &= \sum_{k=0}^{n-1}\frac{1}{n\zeta^{-k}}\cdot\frac{1}{x-\zeta^k} \\ &= \frac{1}{n}\sum_{k=0}^{n-1}\frac{\zeta^k}{x-\zeta^k}.\end{aligned}$$

Let $x = \exp(z)$, $\zeta = \exp\left(-\frac{2\pi i}{n}\right)$. $\square$

Supplement 15.19.2. (Multiplication theorem for $\cot z$)

$$\cot z = \frac{1}{n}\sum_{k=0}^{n-1}\cot\frac{z+k\pi}{n}.$$

This equation yields $x\cot x = 1 - 2\sum_{n=1}^{\infty}\frac{x^2}{n^2\pi^2-x^2}$ again.

Proof. By Supplement 15.12.1,

$$\frac{1}{\exp(z)-1} = \frac{1}{n}\sum_{k=0}^{n-1} \frac{1}{\exp\left(\frac{z+2k\pi i}{n}\right)-1}.$$
$$\frac{1}{\exp(2iz)-1} = \frac{1}{n}\sum_{k=0}^{n-1} \frac{1}{\exp\left(\frac{2i(z+k\pi)}{n}\right)-1}.$$

Notice that $\cot z = i + \frac{2i}{e^{2iz}-1}$, $\cot z = \frac{1}{n}\sum_{k=0}^{n-1} \cot\frac{z+k\pi}{n}$. □

Supplement 15.19.3. (Multiplication theorem for Gamma function)(Gauss's multiplication formula)

$$\Gamma(z)\Gamma\left(z+\frac{1}{k}\right)\Gamma\left(z+\frac{2}{k}\right)\cdots\Gamma\left(z+\frac{k-1}{k}\right) = (2\pi)^{\frac{k-1}{2}} k^{\frac{1-2kz}{2}} \Gamma(kz).$$

Exercise 15.20.

Suppose $H(x)$ is a polynomial of degree n with complex coefficients. Suppose that for all integers n, $F > 0$ we have $H(Fx) = F^{n-1}\sum_{a=0}^{F-1} H(x+\frac{a}{F})$. Show that $H(x) = CB_n(x)$ for some constant C. (Hint: Use Exercise 16 and induction on n.)

Use induction on n to show that $H(x) = CB_n(x)$ where C is the leading coefficient of $H(x)$ (since the leading coefficient of every Bernoulli polynomial is 1).

(1) As $n = 1$, write $H(x) = C_1x + C_0 \in \mathbb{C}$. Then

$$\begin{aligned} H(Fx) &= \sum_{a=0}^{F-1} H(x+\frac{a}{F}), \\ C_1Fx + C_0 &= \sum_{a=0}^{F-1}\left(C_1\left(x+\frac{a}{F}\right)+C_0\right) \\ &= C_1Fx + C_1\cdot\frac{F-1}{2} + C_0F, \\ C_0 &= \frac{-1}{2}C_1 \end{aligned}$$

if $F > 1$. That is, $H(x) = C_1B_1(x)$ where $C = C_1$ is a constant. In fact, C is the leading coefficient of $H(x)$.

(2) Assume that the conclusion holds for $n = k$. As $n = k + 1$, it suffices to show $f(x) = H(x) - CB_{k+1}(x) = 0$, where C is the leading coefficient of $H(x)$.

(3) Differentiate $f(x) = H(x) - CB_{k+1}(x)$ and use Exercise 15.16,

$$f'(x) = H'(x) - C \cdot (k+1) \cdot B_k(x).$$

Might show $f'(x) = 0$ and then get that $H(x) - CB_{k+1}(x)$ is a constant.

(4) Notice that the leading coefficient of $H'(x)$ is $C \cdot (k+1)$. Besides, by differentiating $H(Fx) = F^k \sum_{a=0}^{F-1} H(x + \frac{a}{F})$,

$$H'(Fx) \cdot F = F^k \sum_{a=0}^{F-1} H'(x + \frac{a}{F}),$$
$$H'(Fx) = F^{k-1} \sum_{a=0}^{F-1} H'(x + \frac{a}{F}).$$

By the induction hypothesis, $H'(x) = (C \cdot (k+1))B_k(x)$ since $H'(x)$ has degree $(k+1)-1 = k$. Therefore, $f'(x) = 0$ or $f(x) = H(x) - CB_{k+1}(x) = A$ is a constant.

(5) By $f(Fx) = H(Fx) - CB_{k+1}(Fx) = A$,

$$\begin{aligned} A &= F^k \sum_{a=0}^{F-1} H\left(x + \frac{a}{F}\right) - CF^k \sum_{a=0}^{F-1} B_{k+1}\left(x + \frac{a}{F}\right) \\ &= F^k \sum_{a=0}^{F-1} \left(H\left(x + \frac{a}{F}\right) - CB_{k+1}\left(x + \frac{a}{F}\right)\right) \\ &= F^k \sum_{a=0}^{F-1} A \\ &= F^{k+1} A, \end{aligned}$$

or $(F^{k+1} - 1)A = 0$. For $F > 1$, $A = 0$. That is, $H(x) = CB_{k+1}(x)$.

By mathematical induction the result is established. □

Exercise 15.21.

Show $2^{n-1}B_n(\frac{1}{2}) = (1 - 2^{n-1})B_n$.

The original identity $B_n(\frac{1}{2}) = (1 - 2^{n-1})B_n$ is wrong. For $n = 2$, $B_2(x) = x^2 - x + \frac{1}{6}$ and thus $-\frac{1}{12} = B_2(\frac{1}{2}) \neq (1 - 2^{2-1})B_2 = -\frac{1}{6}$.

Proof. Taking $F = 2$ in Exercise 15.19,

$$\begin{aligned} B_n(2x) &= 2^{n-1} \sum_{a=0}^{1} B_n\left(x + \frac{a}{2}\right) \\ &= 2^{n-1} B_n(x) + 2^{n-1} B_n\left(x + \frac{1}{2}\right). \end{aligned}$$

Let $x = 0$,

$$B_n(0) = 2^{n-1} B_n(0) + 2^{n-1} B_n\left(\frac{1}{2}\right),$$

So

$$2^{n-1} B_n\left(\frac{1}{2}\right) = (1 - 2^{n-1}) B_n(0) = (1 - 2^{n-1}) B_n.$$

□

Exercise 15.22.

More generally, show that $(1 - F^{n-1})B_n = F^{n-1} \sum_{a=1}^{F-1} B_n(\frac{a}{F})$.

The original identity $(1 - F^{n-1})B_n = \sum_{a=1}^{F-1} B_n(\frac{a}{F})$ is wrong again.

Proof. Let $x = 0$ in Exercise 15.19,

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

So

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

□