1. The integers

---

1. *Unique factorization*

Let $\mathbb{Z}$ denote the integers. Say d **divides** m, equivalently, that m is a **multiple** of d, if there exists an integer q such that $m = qd$. Write $d|m$ if d divides m.

It is easy to prove, from the definition, that if $d|x$ and $d|y$ then $d|(ax + by)$ for any integers x, y, a, b: let $x = rd$ and $y = sd$, and

$$ax + by = a(rd) + b(sd) = d \cdot (ar + bs)$$

[1.0.1] **Theorem:** Given an integer N and a non-zero integer m there are unique integers q and r, with $0 \le r < |m|$ such that

$$N = q \cdot m + r$$

The integer r is the **reduction modulo** m of N.

Proof: Let S be the set of all non-negative integers expressible in the form $N - sm$ for some integer s. The set S is non-empty, so by well-ordering has a least element $r = N - qm$. Claim that $r < |m|$. If not, then still $r - |m| \ge 0$, and also

$$r - |m| = (N - qm) - |m| = N - (q \pm 1)m$$

(with the sign depending on the sign of m) is still in the set S, contradiction. For uniqueness, suppose that both $N = qm + r$ and $N = q'm + r'$. Subtract to find

$$r - r' = m \cdot (q' - q)$$

Thus, $r - r'$ is a multiple of m. But since $-|m| < r - r' < |m|$ we have $r = r'$. And then $q = q'$. ///

[1.0.2] **Remark:** The conclusion of the theorem is that in $\mathbb{Z}$ one can divide and obtain a remainder *smaller* than the divisor. That is, $\mathbb{Z}$ is **Euclidean**.

As an example of nearly trivial things that can be proven about divisibility, we have:

A divisor d of n is **proper** if it is neither $\pm n$ nor ± 1. A positive integer p is **prime** if it has no proper divisors and if $p > 1$.

[1.0.3] **Proposition:** A positive integer n is prime if and only if it is not divisible by any of the integers d with $1 < d \leq \sqrt{n}$.

Proof: Suppose that n has a proper factorization $n = d \cdot e$, where $d \leq e$. Then

$$d = \frac{n}{e} \leq \frac{n}{d}$$

gives $d^2 \leq n$, so $d \leq \sqrt{n}$. ///

[1.0.4] **Remark:** The previous proposition suggests that to test an integer n for primality we attempt to divide n by all integers $d = 2, 3, \ldots$ in the range $d \leq \sqrt{n}$. If no such d divides n, then n is prime. This procedure is **trial division**.

Two integers are **relatively prime** or **coprime** or **mutually prime** if for every integer d if $d|m$ and $d|n$ then $d = \pm 1$.

An integer d is a **common divisor** of integers $n_1, \ldots, n_m$ if d divides each n_i. An integer N is a **common multiple** of integers $n_1, \ldots, n_m$ if N is a multiple of each. The following peculiar characterization of the greatest common divisor of two integers is fundamental.

[1.0.5] **Theorem:** Let m, n be integers, not both zero. Among all *common* divisors of m, n there is a unique $d > 0$ such that for *every* other common divisor e of m, n we have $e|d$. This d is the *greatest common divisor* of m, n, denoted $\gcd(m, n)$. And

$$\gcd(mn) = \text{least positive integer of the form } xm + yn \text{ with } x, y \in \mathbb{Z}$$

Proof: Let $D = x_o m + y_o n$ be the least positive integer expressible in the form $xm + yn$. First, we show that any divisor d of both m and n divides D. Let $m = m'd$ and $n = n'd$ with $m', n' \in \mathbb{Z}$. Then

$$D = x_o m + y_o n = x_o(m'd) + y_o(n'd) = (x_o m' + y_o n') \cdot d$$

which presents D as a multiple of d.

On the other hand, let $m = qD + r$ with $0 \leq r < D$. Then

$$0 \leq r = m - qD = m - q(x_o m + y_o n) = (1 - qx_o) \cdot m + (-y_o) \cdot n$$

That is, r is expressible as $x'm + y'n$. Since $r < D$, and since D is the smallest positive integer so expressible, $r = 0$. Therefore, $D|m$, and similarly $D|n$. ///

Similarly:

[1.0.6] **Corollary:** Let m, n be integers, not both zero. Among all *common* multiples of m, n there is a unique positive one N such that for *every* other common multiple M we have $N|M$. This multiple N is the *least common multiple* of m, n, denoted $\text{lcm}(m, n)$. In particular,

$$\text{lcm}(m, n) = \frac{mn}{\gcd(m, n)}$$

Proof: Let

$$L = \frac{mn}{\gcd(m,n)}$$

First we show that L is a multiple of m and n. Indeed, let

$$m = m' \cdot \gcd(m,n) \qquad n = n' \cdot \gcd(m,n)$$

Then

$$L = m \cdot n' = m' \cdot n$$

expresses L as an integer multiple of m and of n. On the other hand, let M be a multiple of both m and n. Let $\gcd(m,n) = am + bn$. Then

$$1 = a \cdot m' + b \cdot n'$$

Let $N = rm$ and $N = sn$ be expressions of N as integer multiples of m and n. Then

$$N = 1 \cdot N = (a \cdot m' + b \cdot n') \cdot N = a \cdot m' \cdot sn + b \cdot n' \cdot rm = (as + br) \cdot L$$

as claimed. ///

The innocent assertion and perhaps odd-seeming argument of the following are essential for what follows. Note that the key point is the peculiar characterization of the *gcd*, which itself comes from the Euclidean property of $\mathbb{Z}$.

[1.0.7] Theorem: A prime p divides a product ab if and only if $p|a$ or $p|b$.

Proof: If $p|a$ we are done, so suppose p does not divide a. Since p is prime, and since $\gcd(p,a) \neq p$, it must be that $\gcd(p,a) = 1$. Let r, s be integers such that $1 = rp + sa$, and let $ab = kp$. Then

$$b = b \cdot 1 = b(rp + sa) = p \cdot (rb + sk)$$

so b is a multiple of p. ///

Granting the theorem, the proof of unique factorization is nearly an afterthought:

[1.0.8] Corollary: *(Unique Factorization)* Every integer n can be written in an *essentially unique* way (up to reordering the factors) as $\pm$ a product of primes:

$$n = \pm\, p_1^{e_1}\, p_2^{e_2} \dots p_m^{e_m}$$

with positive integer exponents and primes $p_1 < \dots < p_m$.

Proof: For *existence,* suppose $n > 1$ is the least integer *not* having a factorization. Then n cannot be prime itself, or just '$n = n$' is a factorization. Therefore n has a proper factorization $n = xy$ with $x, y > 1$. Since the factorization is *proper*, both x and y are strictly smaller than n. Thus, x and y both can be factored. Putting together the two factorizations gives the factorization of n, contradicting the assumption that there exist integers lacking prime factorizations.

Now *uniqueness.* Suppose

$$q_1^{e_1} \dots q_m^{e_m} = N = p_1^{f_1} \dots p_n^{f_n}$$

where $q_1 < \dots < q_m$ are primes, and $p_1 < \dots < p_n$ are primes, and the exponents e_i and f_i are positive integers. Since q_1 divides the left-hand side of the equality, it divides the right-hand side. Therefore, q_1 must divide one of the factors on the right-hand side. So q_1 must divide some p_i. Since p_i is prime, it must be that $q_1 = p_i$.

If $i > 1$ then $p_1 < p_i$. And p_1 divides the left-hand side, so divides one of the q_j, so is some q_j, but then

$$p_1 = q_j \geq q_1 = p_i > p_1$$

which is impossible. Therefore, $q_1 = p_1$.

Without loss of generality, $e_1 \leq f_1$. Thus, by dividing through by $q_1^{e_1} = p_1^{e_!}$, we see that the corresponding exponents e_1 and f_1 must also be equal. Then do induction. ///

[1.0.9] Example: The simplest meaningful (and standard) example of the failure of unique factorization into primes is in the collection of numbers

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$$

The relation

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{5})$$

gives two different-looking factorizations of 6. We must verify that 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are *primes* in R, in the sense that they cannot be further factored.

To prove this, we use *complex conjugation*, denoted by a bar over the quantity to be conjugated: for real numbers a and b,

$$\overline{a + b\sqrt{-5}} = a - b\sqrt{-5}$$

For α, β in R,

$$\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$$

by direct computation. Introduce the **norm**

$$N(\alpha) = \alpha \cdot \overline{\alpha}$$

The multiplicative property

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta)$$

follows from the corresponding property of conjugation:

$$N(\alpha) \cdot N(\beta) = \alpha\overline{\alpha}\beta\overline{\beta} = (\alpha\beta) \cdot (\overline{\alpha}\,\overline{\beta})$$

$$= (\alpha\beta) \cdot (\overline{\alpha\beta}) = N(\alpha\beta)$$

Note that $0 \leq N(\alpha) \in \mathbb{Z}$ for α in R.

Now suppose $2 = \alpha\beta$ with α, β in R. Then

$$4 = N(2) = N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

By unique factorization in $\mathbb{Z}$, $N(\alpha)$ and $N(\beta)$ must be $1, 4$, or $2, 2$, or $4, 1$. The middle case is impossible, since no norm can be 2. In the other two cases, one of α or β is ± 1, and the factorization is not *proper*. That is, 2 cannot be factored further in $\mathbb{Z}[\sqrt{-5}]$. Similarly, 3 cannot be factored further.

If $1 + \sqrt{-5} = \alpha\beta$ with α, β in R, then again

$$6 = N\left(1 + \sqrt{-5}\right) = N(\alpha\beta) = N(\alpha) \cdot N(\beta)$$

Again, the integers $N(\alpha)$ and $N(\beta)$ must either be $1, 6$, $2, 3$, $3, 2$, or $6, 1$. Since the norm cannot be 2 or 3, the middle two cases are impossible. In the remaining two cases, one of α or β is ± 1, and the factorization is not *proper*. That is, $1 + \sqrt{-5}$ cannot be factored further in R. Neither can $1 - \sqrt{-5}$. Thus,

$$6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{5}\right)$$

is a factorization of 6 in two different ways *into primes* in $\mathbb{Z}[\sqrt{-5}]$.

[1.0.10] Example: The **Gaussian integers**

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

where $i^2 = -1$ do have a Euclidean property, and thus have unique factorization. Use the *integer-valued* norm

$$N(a + bi) = a^2 + b^2 = (a + bi) \cdot \overline{(a + bi)}$$

It is important that the notion of size be integer-valued and respect multiplication. We claim that, given $\alpha, \delta \in \mathbb{Z}[i]$ there is $q \in \mathbb{Z}[i]$ such that

$$N(\alpha - q \cdot \delta) < N(\delta)$$

Since N is *multiplicative* (see above), we can divide through by δ inside

$$\mathbb{Q}(i) = \{a + bi : a, b, \in \mathbb{Q}\}$$

(where $\mathbb{Q}$ is the rationals) to see that we are asking for $q \in \mathbb{Z}[i]$ such that

$$N(\frac{\alpha}{\delta} - q) < N(1) = 1$$

That is, given $\beta = \alpha/\delta$ in $\mathbb{Q}(i)$, we must be able to find $q \in \mathbb{Z}[i]$ such that

$$N(\beta - q) < 1$$

With $\beta = a + bi$ with $a, b \in \mathbb{Q}$, let

$$a = r + f_1 \qquad b = s + f_2$$

with $r, s \in \mathbb{Z}$ and f_1, f_2 rational numbers with

$$|f_i| \leq \frac{1}{2}$$

That this is possible is a special case of the fact that any *real* number is at distance at most $1/2$ from some integer. Then take

$$q = r + si$$

Then

$$\beta - q = (a + bi) - (r + si) = f_1 + if_2$$

and

$$N(\beta - q) = N(f_1 + if_2) = f_1^2 + f_2^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$

Thus, indeed $\mathbb{Z}[i]$ has the Euclidean property, and, by the same proof as above, has unique factorization.

---

2. *Irrationalities*

The usual proof that there is no square root of 2 in the rationals $\mathbb{Q}$ uses a little bit of unique factorization, in the notion that it is possible to put a fraction into lowest terms, that is, having relatively prime numerator and denominator.

That is, given a fraction a/b (with $b \neq 0$), letting $a' = a/\gcd(a, b)$ and $b' = b/\gcd(a, b)$, one can and should show that $\gcd(a', b') = 1$. That is, $a'b/b'$ is **in lowest terms**. And

$$\frac{a'}{b'} = \frac{a}{b}$$

[2.0.1] **Example:** Let p be a prime number. We claim that there is no $\sqrt{p}$ in the rationals $\mathbb{Q}$. Suppose, to the contrary, that $a/b = \sqrt{p}$. Without loss of generality, we can assume that $\gcd(a,b) = 1$. Then, squaring and multiplying out,

$$a^2 = pb^2$$

Thus, $p|a^2$. Since $p|cd$ implies $p|c$ or $p|d$, necessarily $p|a$. Let $a = pa'$. Then

$$(pa')^2 = pb^2$$

or

$$pa'^2 = b^2$$

Thus, $p|b$, contradicting the fact that $\gcd(a,b) = 1$. ///

The following example illustrates a possibility that will be subsumed later by *Eisenstein's criterion*, which is itself an application of *Newton polygons* attached to polynomials.

[2.0.2] **Example:** Let p be a prime number. We claim that there is no rational solution to

$$x^5 + px + p = 0$$

Indeed, suppose that a/b were a rational solution, in lowest terms. Then substitute and multiply through by b^5 to obtain

$$a^5 + pab^4 + pb^5 = 0$$

From this, $p|a^5$, so, since p is prime, $p|a$. Let $a = pa'$. Then

$$(pa')^5 + p(pa')b^4 + pb^5 = 0$$

or

$$p^4a'^5 + p^2a'b^4 + b^5 = 0$$

From this, $p|b^5$, so $p|b$ since p is prime. This contradicts the lowest-terms hypothesis.

---

3. $\mathbb{Z}/m$, the integers mod m

Recall that a *relation* R on a set S is a subset of the cartesian product $S \times S$. Write

$$x \; R \; y$$

if the ordered pair (x,y) lies in the subset R of $S \times S$. An **equivalence relation** R on a set S is a relation satisfying

- **Reflexivity**: $x \; R \; x$ for all $x \in S$
- **Symmetry**: If $x \; R \; y$ then $y \; R \; x$
- **Transitivity**: If $x \; R \; y$ and $y \; R \; z$ then $x \; R \; z$

A common notation for an equivalence relation is

$$x \sim y$$

that is, with a tilde rather than R.

Let $\sim$ be an equivalence relation on a set S. For $x \in S$, the $\sim$ - **equivalence class** $\bar{x}$ containing x is the subset

$$\bar{x} = \{x' \in S : x' \sim x\}$$

The **set of equivalence classes** of $\sim$ on S is denoted by

$$S/\sim$$

(as a quotient). Every element $z \in S$ is contained in an equivalence class, namely the equivalence class $\bar{z}$ of all $s \in S$ so that $s \sim z$. Given an equivalence class A inside S, an x in the set S such that $\bar{x} = A$ is a **representative** for the equivalence class. That is, any element of the subset A is a representative.

A set $\mathcal{S}$ of non-empty subsets of a set S whose union is the whole S, and which are mutually disjoint, is a **partition** of S. One can readily check that the equivalence classes of an equivalence relation on a set S form a partition of S, and, conversely, any partition of S defines an equivalence relation by positing that $x \sim y$ if and only if they lie in the same set of the partition. ///

If two integers x, y differ by a multiple of a non-zero integer m, that is, if $m|(x-y)$, then x is **congruent to** y **modulo** m, written

$$x \equiv y \bmod m$$

Such a relation is a **congruence** modulo m, and m is the **modulus**. When Gauss first used this notion 200 years ago, it was sufficiently novel that it deserved a special notation, but, now that the novelty has worn off, we will simply write

$$x = y \bmod m$$

and (unless we want special emphasis) simply say that x is **equal to** y modulo m.

[3.0.1] **Proposition:** (For fixed modulus m) equality modulo m is an equivalence relation. ///

Compatibly with the general usage for equivalence relations, the **congruence class** (or **residue class** or **equivalence class**) of an integer x modulo m, denoted $\bar{x}$ (with only implicit reference to m) is the set of all integers equal to x mod m:

$$\bar{x} = \{y \in \mathbb{Z} : y = x \bmod m\}$$

The **integers mod** m, denoted $\mathbb{Z}/m$, is the collection of *congruence classes* of integers modulo m. For some $X \in \mathbb{Z}/m$, a choice of ordinary integer x so that $\bar{x} = X$ is a **representative** for the congruence class X.

[3.0.2] **Remark:** A popular but unfortunate notation for $\mathbb{Z}/m$ is $\mathbb{Z}_m$. We will not use this notation. It is unfortunate because for primes p the notation $\mathbb{Z}_p$ is the *only* notation for the *p-adic integers*.

[3.0.3] **Remark:** On many occasions, the bar is dropped, so that x-mod-m may be written simply as 'x'.

[3.0.4] **Remark:** The traditionally popular collection of representatives for the equivalence classes modulo m, namely

$$\{\bar{0}, \bar{1}, \bar{2}, \dots \overline{m-2}, \overline{m-1}\}$$

is not the only possibility.

The benefit Gauss derived from the explicit notion of congruence was that congruences behave much like equalities, thus allowing us to benefit from our prior experience with equalities. Further, but not surprisingly with sufficient hindsight, congruences behave nicely with respect to the basic operations of addition, subtraction, and multiplication:

[3.0.5] **Proposition:** Fix the modulus m. If $x = x' \bmod m$ and $y = y' \bmod m$, then

$$x + y = x' + y' \bmod m$$

$$xy = x'y' \bmod m$$

Proof: Since $m|(x'-x)$ there is an integer k such that $mk = x'-x$. Similarly, $y' = y+\ell m$ for some integer ℓ. Then

$$x'+y' = (x+mk)+(y+m\ell) = x+y+m\cdot(k+\ell)$$

Thus, $x'+y' = x+y \bmod m$. And

$$x'\cdot y' = (x+mk)\cdot(y+m\ell) = x\cdot y + xm\ell + mky + mk\cdot m\ell = x\cdot y + m\cdot(k+\ell+mk\ell)$$

Thus, $x'y' = xy \bmod m$. ///

As a corollary, congruences *inherit* many basic properties from ordinary arithmetic, simply because $x = y$ implies $x = y \bmod m$:
• *Distributivity:* $x(y+z) = xy+xz \bmod m$
• *Associativity of addition:* $(x+y)+z = x+(y+z) \bmod m$
• *Associativity of multiplication:* $(xy)z = x(yz) \bmod m$
• *Property of* 1*:* $1\cdot x = x\cdot 1 = x \bmod m$
• *Property of* 0*:* $0+x = x+0 = x \bmod m$

In this context, a **multiplicative inverse mod** m to an integer a is an integer b (if it exists) such that

$$a\cdot b = 1 \bmod m$$

[3.0.6] **Proposition:** An integer a has a multiplicative inverse modulo m if and only if $\gcd(a,m) = 1$.

Proof: If $\gcd(a,m) = 1$ then there are r,s such that $ra+sm = 1$, and

$$ra = 1-sm = 1 \bmod m$$

The other implication is easy. ///

In particular, note that if a is invertible mod m then any a' in the residue class of a mod m is likewise invertible mod m, and any other element b' of the residue class of an inverse b is also an inverse. Thus, it makes sense to refer to elements of $\mathbb{Z}/m$ as being invertible or not. Notation:

$$(\mathbb{Z}/m)^\times = \{\bar{x}\in\mathbb{Z}/m : \gcd(x,m) = 1\}$$

This set $(\mathbb{Z}/m)^\times$ is the **multiplicative group** or **group of units** of $\mathbb{Z}/m$.

[3.0.7] **Remark:** It is easy to verify that the set $(\mathbb{Z}/m)^\times$ is **closed under multiplication** in the sense that $a,b\in(\mathbb{Z}/m)^\times$ implies $ab\in(\mathbb{Z}/m)^\times$, and is **closed under inverses** in the sense that $a\in(\mathbb{Z}/m)^\times$ implies $a^{-1}\in(\mathbb{Z}/m)^\times$.

[3.0.8] **Remark:** The superscript is not an 'x' but is a 'times', making a reference to multiplication and multiplicative inverses mod m. Some sources write $\mathbb{Z}/m^*$, but the latter notation is inferior, as it is too readily confused with other standard notation (for *duals*).

---

4. *Fermat's little theorem*

[4.0.1] **Theorem:** Let p be a prime number. Then for any integer x

$$x^p = x \bmod p$$

Proof: First, by the binomial theorem

$$(x+y)^p = \sum_{0\le i\le p} \binom{p}{i} x^i\, y^{p-i}$$

In particular, the binomial coefficients are *integers*. Now we can show that the prime p divides the binomial coefficients

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

with $1 \le i \le p-1$. We have

$$\binom{p}{i} \cdot i! \cdot (p-i)! = p!$$

(Since we know that the binomial coefficient is an integer, the following argument makes sense.) The prime p divides the right-hand side, so divides the left-hand side, but does not divide $i!$ nor $(p-i)!$ (for $0 < i < p$) since these two numbers are products of integers smaller than p and (hence) not divisible by p. Again using the fact that $p|ab$ implies $p|a$ or $p|b$, p does not divide $i! \cdot (p-i)!$, so p must divide the binomial coefficient.

Now we prove Fermat's Little Theorem for *positive* integers x by induction on x. Certainly $1^p = 1 \bmod p$. Now suppose that we know that

$$x^p = x \bmod p$$

Then

$$(x+1)^p = \sum_{0\le i\le p} \binom{p}{i} x^i\, 1^{p-i} = x^p + \sum_{0<i<p} \binom{p}{i} x^i + 1$$

All the coefficients in the sum in the middle of the last expression are divisible by p, so

$$(x+1)^p = x^p + 0 + 1 = x + 1 \bmod p$$

This proves the theorem for positive x. ///

[4.0.2] Example: Let p be a prime with $p = 3 \bmod 4$. Suppose that a is a **square modulo** p, in the sense that there exists an *integer* b such that

$$b^2 = a \bmod p$$

Such b is a **square root modulo** p of a. Then we claim that $a^{(p+1)/4}$ is a square root of $a \bmod p$. Indeed,

$$\left(a^{(p+1)/4}\right)^2 = \left((b^2)^{(p+1)/4}\right)^2 = b^{p+1} = b^p \cdot b = b \cdot b \bmod p$$

by Fermat. Then this is $a \bmod p$. ///

[4.0.3] Example: Somewhat more generally, let q be a prime, and let p be another prime with $p = 1 \bmod q$ but $p \neq 1 \bmod q^2$.

$$r = q^{-1} \bmod \frac{p-1}{q}$$

Then when a is a q^{th} power modulo p, a q^{th} root of $a \bmod p$ is given by the formula

$$q^{th} \text{ root of } a \bmod p = a^r \bmod p$$

If a is *not* a q^{th} power mod p then this formula does *not* product a q^{th} root.

[4.0.4] **Remark:** For prime q and prime $p \neq 1 \bmod q$ there is an even simpler formula for q^{th} roots, namely let

$$r = q^{-1} \bmod p-1$$

and then

$$q^{th} \text{ root of } a \bmod p = a^r \bmod p$$

Further, as can be seen from the even-easier proof of this formula, *everything* mod such p is a q^{th} power.

For a positive integer n, the **Euler phi-function** $\varphi(n)$ is the number of integers b so that $1 \leq b \leq n$ and $\gcd(b,n) = 1$. Note that

$$\varphi(n) = \text{cardinality of } (\mathbb{Z}/n)^\times$$

[4.0.5] **Theorem:** *(Euler)* For x relatively prime to a positive integer n,

$$x^{\varphi(n)} = 1 \bmod n$$

[4.0.6] **Remark:** The special case that n is prime is Fermat's Little Theorem.

Proof: Let $G = (\mathbb{Z}/m)^\times$, for brevity. First note that the product

$$P = \prod_{g \in G} g = \text{product of all elements of } G$$

is again in G. Thus, P has a multiplicative inverse mod n, although we do not try to identify it. Let x be an element of G. Then we claim that the map $f : G \longrightarrow G$ defined by

$$f(g) = xg$$

is a bijection of G to itself. First, check that f really maps G to itself: for x and g both invertible mod n,

$$(xg)(g^{-1}x^{-1}) = 1 \bmod n$$

Next, injectivity: if $f(g) = f(h)$, then $xg = xh \bmod n$. Multiply this equality by $x^{-1} \bmod n$ to obtain $g = h \bmod n$. Last, surjectivity: given $g \in G$, note that $f(x^{-1}g) = g$.

Then

$$P = \prod_{g \in G} g = \prod_{g \in G} f(g)$$

since the map f merely permutes the elements of G. Then

$$P = \prod_{g \in G} f(g) = \prod_{g \in G} xg = x^{\varphi(n)} \prod_{g \in G} g = x^{\varphi(n)} \cdot P$$

Since P is invertible mod n, multiply through by $P^{-1} \bmod n$ to obtain

$$1 = x^{\varphi(n)} \bmod n$$

This proves Euler's Theorem. ///

[4.0.7] **Remark:** This proof of Euler's theorem, while subsuming Fermat's Little Theorem as a special case, strangely uses fewer specifics. There is no mention of binomial coefficients, for example.

[4.0.8] **Remark:** The argument above is a prototype example for the basic Lagrange's Theorem in basic group theory.

5. Sun-Ze's theorem

The result of this section is sometimes known as the **Chinese Remainder Theorem**. Indeed, the earliest results (including and following Sun-Ze's) were obtained in China, but such sloppy attribution is not good. Sun-Ze's result was obtained before 850, and the statement below was obtained by Chin Chiu Shao about 1250. Such results, with virtually the same proofs, apply much more generally.

[5.0.1] **Theorem:** *(Sun-Ze)* Let m and n be relatively prime positive integers. Let r and s be integers such that

$$rm + sn = 1$$

Then the function

$$f : \mathbb{Z}/m \times \mathbb{Z}/n \longrightarrow \mathbb{Z}/mn$$

defined by

$$f(x, y) = y \cdot rm + x \cdot sn$$

is a bijection. The inverse map

$$f^{-1} : \mathbb{Z}/mn \longrightarrow \mathbb{Z}/m \times \mathbb{Z}/n$$

is

$$f^{-1}(z) = (x\text{-mod-}m, y\text{-mod-}n)$$

Proof: First, the peculiar characterization of $\gcd(m, n)$ as the smallest positive integer expressible in the form $rm + sn$ assures (since here $\gcd(m, n) = 1$) that integers r and s exist such that $rm + sn = 1$. Second, the function f is well-defined, that is, if $x' = x + am$ and $y' = y + bn$ for integers a and b, then still

$$f(x', y') = f(x, y)$$

Indeed,

$$f(x', y') = y'rm + x'sn = (y + an)rm + (x + am)sn$$

$$= yrm + xsn + mn(ar + bs) = f(x, y) \bmod mn$$

proving the well-definedness.

To prove surjectivity of f, for any integer z, let $x = z$ and $y = z$. Then

$$f(x, y) = zrm + zsn = z(rm + sn) = z \cdot 1 \bmod mn$$

(To prove injectivity, we *could* use the fact that $\mathbb{Z}/m \times \mathbb{Z}/n$ and $\mathbb{Z}/mn$ are finite sets of the same size, so a surjective function is necessarily injective, but a more direct argument is more instructive.) Suppose

$$f(x', y') = f(x, y)$$

Then modulo m the yrm and $y'rm$ are 0, so

$$xsn = x'sn \bmod m$$

From $rm + sn = 1 \bmod mn$ we obtain $sn = 1 \bmod m$, so

$$x = x' \bmod m$$

Symmetrically,

$$y = y' \bmod n$$

giving injectivity.

Finally, by the same reasoning,

$$f(x,y) = yrm + xsn = y \cdot 0 + x \cdot 1 \bmod m = x \bmod m$$

and similarly

$$f(x,y) = yrm + xsn = y \cdot 1 + x \cdot 0 \bmod n = y \bmod n$$

This completes the argument. ///

[5.0.2] **Remark:** The above result is the simplest prototype for a very general result.

---

6. *Worked examples*

[1.1] Let D be an integer that is not the square of an integer. Prove that there is no $\sqrt{D}$ in $\mathbb{Q}$.

Suppose that a, b were integers ($b \neq 0$) such that $(a/b)^2 = D$. The fact/principle we intend to invoke here is that fractions can be put in *lowest terms*, in the sense that the numerator and denominator have greatest common divisor 1. This follows from *existence* of the *gcd*, and from the fact that, if $\gcd(a,b) > 1$, then let $c = a/\gcd(a,b)$ and $d = b/\gcd(a,b)$ and we have $c/d = a/b$. Thus, still $c^2/d^2 = D$. One way to proceed is to prove that c^2/d^2 is still in lowest terms, and thus cannot be an integer unless $d = \pm 1$. Indeed, if $\gcd(c^2, d^2) > 1$, this *gcd* would have a prime factor p. Then $p|c^2$ implies $p|c$, and $p|d^2$ implies $p|d$, by the critical proven property of primes. Thus, $\gcd(c,d) > 1$, contradiction.

[1.2] Let p be prime, $n > 1$ an integer. Show (directly) that the equation $x^n - px + p = 0$ has no rational root (where $n > 1$).

Suppose there were a rational root a/b, without loss of generality in lowest terms. Then, substituting and multiplying through by b^n, one has

$$a^n - pb^{n-1}a + pb^n = 0$$

Then $p|a^n$, so $p|a$ by the property of primes. But then p^2 divides the first two terms, so must divide pb^n, so $p|b^n$. But then $p|b$, by the property of primes, contradicting the lowest-common-terms hypothesis.

[1.3] Let p be prime, b an integer not divisible by p. Show (directly) that the equation $x^p - x + b = 0$ has no rational root.

Suppose there were a rational root c/d, without loss of generality in lowest terms. Then, substituting and multiplying through by d^p, one has

$$c^p - d^{p-1}c + bd^p = 0$$

If $d \neq \pm 1$, then some prime q divides d. From the equation, $q|c^p$, and then $q|c$, contradiction to the lowest-terms hypothesis. So $d = 1$, and the equation is

$$c^p - c + b = 0$$

By Fermat's Little Theorem, $p|c^p - c$, so $p|b$, contradiction.

[1.4] Let r be a positive integer, and p a prime such that $\gcd(r, p-1) = 1$. Show that every b in $\mathbb{Z}/p$ has a unique r^{th} root c, given by the formula

$$c = b^s \bmod p$$

where $rs = 1 \bmod (p-1)$. [*Corollary of Fermat's Little Theorem.*]

[1.5] Show that $R = \mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ are Euclidean.

First, we consider $R = \mathbb{Z}[\sqrt{-D}]$ for $D = 1, 2, \ldots$. Let $\omega = \sqrt{-D}$. To prove Euclidean-ness, note that the Euclidean condition that, given $\alpha \in \mathbb{Z}[\omega]$ and non-zero $\delta \in \mathbb{Z}[\omega]$, there exists $q \in \mathbb{Z}[\omega]$ such that

$$|\alpha - q \cdot \delta| < |\delta|$$

is equivalent to

$$|\alpha/\delta - q| < |1| = 1$$

Thus, it suffices to show that, given a complex number α, there is $q \in \mathbb{Z}[\omega]$ such that

$$|\alpha - q| < 1$$

Every complex number α can be written as $x + y\omega$ with real x and y. The simplest approach to analysis of this condition is the following. Let m, n be integers such that $|x - m| \leq 1/2$ and $|y - n| \leq 1/2$. Let $q = m + n\omega$. Then $\alpha - q$ is of the form $r + s\omega$ with $|r| \leq 1/2$ and $|s| \leq 1/2$. And, then,

$$|\alpha - q|^2 = r^2 + Ds^2 \leq \frac{1}{4} + \frac{D}{4} = \frac{1+D}{4}$$

For this to be strictly less than 1, it suffices that $1 + D < 4$, or $D < 3$. This leaves us with $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$.

In the second case, consider $Z[\omega]$ where $\omega = (1 + \sqrt{-D})/2$ and $D = 3 \bmod 4$. (The latter condition assures that $\mathbb{Z}[x]$ works the way we hope, namely that everything in it is expressible as $a + b\omega$ with $a, b \in \mathbb{Z}$.) For D=3 (the Eisenstein integers) the previous approach still works, but fails for $D = 7$ and for $D = 11$. Slightly more cleverly, realize that first, given complex α, integer n can be chosen such that

$$-\sqrt{D}/4 \leq \text{imaginary part}(\alpha - n\omega) \leq +\sqrt{D}/4$$

since the imaginary part of ω is $\sqrt{D}/2$. *Then* choose integer m such that

$$-1/2 \leq \text{ real part}(\alpha - n\omega - m) \leq 1/2$$

Then take $q = m + n\omega$. We have chosen q such that $\alpha - q$ is in the *rectangular* box of complex numbers $r + s\sqrt{-7}$ with

$$|r| \leq 1/2 \quad \text{and} \quad |s| \leq 1/4$$

Yes, $1/4$, not $1/2$. Thus, the size of $\alpha - q$ is at most

$$1/4 + D/16$$

The condition that this be strictly less than 1 is that $4 + D < 16$, or $D < 12$ (and $D = 1 \bmod 4$). This gives $D = 3, 7, 11$.

[1.6] Let $f : X \longrightarrow Y$ be a function from a set X to a set Y. Show that f has a left inverse if and only if it is injective. Show that f has a right inverse if and only if it is surjective. (Note where, if anywhere, the Axiom of Choice is needed.)

[1.7] Let $h : A \longrightarrow B$, $g : B \longrightarrow C$, $f : C \longrightarrow D$. Prove the associativity

$$(f \circ g) \circ h = f \circ (g \circ h)$$

Two functions are equal if and only if their values (for the same inputs) are the same. Thus, it suffices to evaluate the two sides at $a \in A$, using the definition of composite:

$$((f \circ g) \circ h)(a) = (f \circ g)(h(a)) = f(g((h(a))) = f((g \circ h)(a)) = (f \circ (g \circ h))(a)$$

[1.8] Show that a set is infinite if and only if there is an injection of it to a proper subset of itself. Do not set this up so as to trivialize the question.

The other definition of *finite* we'll take is that a set S is finite if there is a surjection to it from one of the sets

$$\{\},\ \{1\},\ \{1,2\},\ \{1,2,3\},\ \dots$$

And a set is *infinite* if it has no such surjection.

We find a denumerable subset of an infinite set S, as follows. For infinite S, since S is not empty (or there'd be a surjection to it from $\{\}$), there is an element s_1. Define

$$f_1 : \{1\} \longrightarrow S$$

by $f(1) = s_1$. This cannot be surjective, so there is $s_2 \neq s_1$. Define

$$f_2 : \{1,2\} \longrightarrow S$$

by $f(1) = s_1$, $f(2) = s_2$. By induction, for each natural number n we obtain an injection $f_n : \{1,\dots\} \longrightarrow S$, and distinct elements $s_1, s_2, \dots$. Let S' be the complement to $\{s_1, s_2, \dots\}$ in S. Then define $F : S \longrightarrow S$ by

$$F(s_i) = s_{i+1} \quad F(s') = s' \text{ (for } s' \in S')$$

This is an injection to the proper subset $S - \{s_1\}$.

On the other hand, we claim that no set $\{1,\dots,n\}$ admits an injection to a proper subset of itself. If there were such, by Well-Ordering there would be a least n such that this could happen. Let f be an injection of $S = \{1,\dots,n\}$ to a proper subset of itself.

By hypothesis, f restricted to $S' = \{1,2,\dots,n-1\}$ does *not* map S' to a proper subset of itself. The restriction of an injective function is still injective. Thus, either $f(i) = n$ for some $1 \leq i < n$, or $f(S')$ is the *whole* set S'. In the former case, let j be the least element not in the image $f(S)$. (Since $f(i) = n$, $j \neq n$, but this doesn't matter.) Replace f by $\pi \circ f$ where π is the permutation of $\{1,\dots,n\}$ that interchanges j and n and leaves everything else fixed. Since permutations are bijections, this $\pi \circ f$ is still an injection of S to a proper subset. Thus, we have reduced to the second case, that $f(S') = S'$. By injectivity, $f(n)$ can't be in S', but then $f(n) = n$, and the image $f(S)$ is not a proper subset of S after all, contradiction. ///

In a similar vein, one can *prove* the Pigeon-Hole Principle, namely, that for $m < n$ a function

$$f : \{1,\dots,n\} \longrightarrow \{1,\dots,m\}$$

cannot be injective. Suppose this is false. Let n be the smallest such that there is $m < n$ with an injective map as above. The restriction of an injective map is still injective, so f on $\{1,\dots,n-1\}$ is still injective. By the minimality of n, it must be that $n - 1 = m$, and that f restricted to $\{1,\dots,m\}$ is a bijection of that set to itself. But then there is no possibility for $f(n)$ in $\{1,\dots,m\}$ without violating the injectivity. Contradiction. Thus, there is no such injection to a smaller set.

Exercises

1.[6.0.1] Let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ be a polynomial with integer coefficients a_i. Show that if $f(x) = 0$ has a root in $\mathbb{Q}$, then this root is an integer dividing a_0.

1.[6.0.2] Show that $x^2 - y^2 = 102$ has no solutions in integers.

1.[6.0.3] Show that $x^3 - y^3 = 3$ has no solutions in integers.

1.[6.0.4] Show that $x^3 + y^3 - z^3 = 4$ has no solutions in integers.

1.[6.0.5] Show that $x^2 + 3y^2 + 6z^3 - 9w^5 = 2$ has no solutions in integers.

1.[6.0.6] The defining property of *ordered pair* (a, b) is that $(a, b) = (a', b')$ if and only if $a = a'$ and $b = b'$. Show that the set-theoretic construction $(a, b) = \{\{a\}, \{a, b\}\}$ succeeds in making an object that behaves as an ordered pair is intended. (*Hint:* Beware: if $x = y$, then $\{x, y\} = \{x\}$.)

1.[6.0.7] Let p be a prime, and q a positive integer power of p. Show that p divides the binomial coefficients $\binom{q}{i} = q!/i!(q-i)!$ for $0 < i < q$.

1.[6.0.8] Show that the greatest common divisor of non-zero integers x, y, z is the smallest positive integer expressible as $ax + by + cz$ for integers a, b, c.

1.[6.0.9] Let m, n be relatively prime integers. Without using factorizations, prove that $m|N$ and $n|N$ implies $mn|N$.

1.[6.0.10] (*A warm-up to Hensel's lemma*) Let $p > 2$ be a prime. Suppose that b is an integer not divisible by p such that there is a solution y to the equation $y^2 = b \bmod p$. Show (by induction on n) that for $n \geq 1$ there is a unique $x \bmod p^n$ such that $x = b \bmod p$ and

$$x^p = b \bmod p^n$$

1.[6.0.11] (*Another warm-up to Hensel's lemma*) Let $p > 2$ be a prime. Let y be an integer such that $y \equiv 1 \bmod p$. Show (by induction on n) that for $n \geq 1$ there is a unique $x \bmod p^n$ so that

$$x^p = y \bmod p^n$$

1.[6.0.12] Let φ be Euler's phi-function, equal to the number of integers ℓ such that $1 \leq \ell < n$ with ℓ relatively prime to n. Show that for a positive integer n

$$n \;=\; \sum_{d|n,\ d>0} \varphi(d)$$