

Chapter 8

Appendix

8.1 Number Theory and Group Theory

In this section we work with the set of integers

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

We say that x divides y , and write $x|y$ if $y = qx$. Using the terminology from section 2.3, $x|y$ if and only if $y = \text{div}(x, y) \cdot x$.

Claim 8.1. *If p is a prime, and $p|a_1a_2 \dots a_n$, then $p|a_i$ for some i .*

Proof. It is enough to show that if $p|ab$ then $p|a$ or $p|b$. Let $g = \text{gcd}(a, b)$. Then $g|p$, and since p is a prime, there are two cases. Case 1, $g = p$, then since $g|a$, $p|a$. Case 2, $g = 1$, so there exist u, v such that $au + bv = 1$ (see problem 2.17), so $abu + pbv = b$. Since $p|ab$, and $p|p$, it follows that $p|(abu + pbv)$, so $p|b$. \square

Theorem 8.1 (Fundamental Theorem of Arithmetic). *For $a \geq 2$, $a = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, where p_i are prime numbers, and other than rearranging primes, this factorization is unique.*

Proof. We first show the existence of the factorization, and then its uniqueness. The proof of existence is by complete induction; the basis case is $a = 2$, where 2 is a prime. Consider an integer $a > 2$; if a is prime then it is its own factorization (just as in the basis case). Otherwise, if a is composite, then $a = b \cdot c$, where $1 < b, c < a$; apply the induction hypothesis to b and c .

To show uniqueness suppose that $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ where we have written out all the primes, that is, instead of writing p^e we write $p \cdot p \dots p$, e times. Since $p_1|a$, it follows that $p_1|q_1 q_2 \dots q_t$. So $p_1|q_j$ for some

j , by claim 8.1, but then $p_1 = q_j$ since they are both primes. Now delete p_1 from the first list and q_j from the second list, and continue. Obviously we cannot end up with a product of primes equal to 1, so the two lists must be identical. \square

Let $m \geq 1$ be an integer. We say that a and b are *congruent modulo* m , and write $a \equiv b \pmod{m}$ (or sometimes $a \equiv_m b$) if $m \mid (a - b)$. Another way to say this is that a and b have the same remainder when divided by m ; using the terminology of section 2.3, we can say that $a \equiv b \pmod{m}$ if and only if $\text{rem}(m, a) = \text{rem}(m, b)$.

Problem 8.1. Show that if $a_1 \equiv_m b_1$ and $a_2 \equiv_m b_2$, then $a_1 \pm b_1 \equiv_m a_2 \pm b_2$ and $a_1 \cdot b_1 \equiv_m a_2 \cdot b_2$.

Proposition 8.1. If $m \geq 1$, then $a \cdot b \equiv_m 1$ for some b if and only if $\text{gcd}(a, m) = 1$.

Proof. (\Rightarrow) If there exists a b such that $a \cdot b \equiv_m 1$ then for the same b we have $m \mid (ab - 1)$ and so there exists a c such that $ab - 1 = cm$, i.e., $ab - cm = 1$. So $\text{gcd}(a, m) \mid 1$ and so it must be equal to 1.

(\Leftarrow) Suppose that $\text{gcd}(a, m) = 1$. By the Extended Euclidean algorithm (see problem 2.17) there exist u, v such that $au + mv = 1$, so $au - 1 = -mv$, so $m \mid (au - 1)$, so $au \equiv_m 1$. So $b = u$. \square

Let $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. We call \mathbb{Z}_m the set of integers modulo m . To add or multiply in the set \mathbb{Z}_m , we add and multiply the corresponding integers, and then take the remainder of the division by m as the result. Let $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \text{gcd}(a, m) = 1\}$. By proposition 8.1 we know that \mathbb{Z}_m^* is the subset of \mathbb{Z}_m consisting of those elements which have multiplicative inverses in \mathbb{Z}_m .

The function $\phi(n)$ is called the *Euler totient function*, and it is the number of elements less than n that are co-prime to n , i.e., $\phi(n) = |\mathbb{Z}_n^*|$. If we are able to factor, we are also able to compute $\phi(n)$: suppose that $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$, then it is not hard to see that $\phi(n) = \prod_{i=1}^l p_i^{k_i-1} (p_i - 1)$.

Theorem 8.2 (Fermat's Little Theorem). Let p be a prime and $\text{gcd}(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. For any a such that $\text{gcd}(a, p) = 1$ the following numbers

$$1 \cdot a, 2 \cdot a, 3 \cdot a, \dots, (p-1) \cdot a, \quad (8.1)$$

all taken mod p , are pairwise distinct. To see this suppose that $ja \equiv ka \pmod{p}$. Then $(j - k)a \equiv 0 \pmod{p}$, and so $p \mid (j - k)a$. But since by

assumption $\gcd(a, p) = 1$, it follows that $p \nmid a$, and so by claim 8.1 it must be the case that $p \mid (j - k)$. But since $j, k \in \{1, 2, \dots, p-1\}$, it follows that $-(p-2) \leq j - k \leq (p-2)$, so $j - k = 0$, i.e., $j = k$.

Thus the numbers in (8.1) are just a re-ordering of $\{1, 2, \dots, p-1\}$. Therefore

$$a^{p-1}(p-1)! \equiv_p \prod_{j=1}^{p-1} j \cdot a \equiv_p \prod_{j=1}^{p-1} j \equiv_p (p-1)!. \quad (8.2)$$

Since all the numbers in $\{1, 2, \dots, p-1\}$ have inverses in \mathbb{Z}_p , as $\gcd(i, p) = 1$ for $1 \leq i \leq p-1$, their product also has an inverse. That is, $(p-1)!$ has an inverse, and so multiplying both sides of (8.2) by $((p-1)!)^{-1}$ we obtain the result. \square

Problem 8.2. *Given a second proof of Fermat's Little Theorem using the binomial expansion, i.e., $(x+y)^n = \sum_{j=0}^n \binom{n}{j} x^j y^{n-j}$ applied to $(a+1)^p$.*

We say that $(G, *)$ is a *group* if G is a set and $*$ is an operation, such that if $a, b \in G$, then $a * b \in G$ (this property is called *closure*). Furthermore, the operation $*$ has to satisfy the following three properties:

- (1) **Identity Law:** There exists an $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
- (2) **Inverse law:** For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. This element b is called an *inverse* and it can be shown that it is unique; hence it is often denoted as a^{-1} .
- (3) **Associative law:** For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

If $(G, *)$ also satisfies the **Commutative law**, that is, for all $a, b \in G$, $a * b = b * a$, then it is called a *commutative* or *Abelian group*.

Typical examples of groups are $(\mathbb{Z}_p, +)$ (integers mod p under addition) and (\mathbb{Z}_p^*, \cdot) (integers mod p under multiplication). Note that both these groups are Abelian. These are, of course, the two groups of concern for us; but there are many others: $(\mathbb{Q}, +)$ is an infinite group (rationals under addition), $\mathbf{GL}(n, \mathbb{F})$ (which is the group of $n \times n$ invertible matrices over a field \mathbb{F}), and S_n (the *symmetric group* over n elements, consisting of permutations of $[n]$ where $*$ is function composition).

We let $|G|$ denote the number of elements in G (note that G may be infinite, but we are concerned mainly with finite groups). If $g \in G$ and $x \in \mathbb{N}$, then $g^x = g * g * \dots * g$, x times. Note that if the operation $*$ is clear from the context then we write ab instead of $a * b$.

Suppose that G is a finite group and $a \in G$; then the smallest $d \in \mathbb{N}$ such that $a^d = e$ is called the *order* of a , and it is denoted as $\text{ord}_G(a)$ (or just $\text{ord}(a)$ if the group G is clear from the context).

Proposition 8.2. *If G is a finite group, then for all $a \in G$ there exists a $d \in \mathbb{N}$ such that $a^d = e$. If $d = \text{ord}_G(a)$, and $a^k = e$, then $d|k$.*

Proof. Consider the list a^1, a^2, a^3, \dots . If G is finite there must exist $i < j$ such that $a^i = a^j$. Then, $(a^{-1})^i$ applied to both sides yields $a^{i-j} = e$. Let $d = \text{ord}(a)$ (by the LNP we know that it must exist!). Suppose that $k \geq d$, $a^k = e$. Write $k = dq + r$ where $0 \leq r < d$. Then $e = a^k = a^{dq+r} = (a^d)^q a^r = a^r$. Since $a^d = e$ it follows that $a^r = e$, contradicting the minimality of $d = \text{ord}(a)$. \square

If $(G, *)$ is a group we say that H is a *subgroup* of G , and write $H \leq G$ if $H \subseteq G$ and H is closed under $*$. That is, H is a subset of G , and H is itself a group. Note that for any G it is always the case that $\{e\} \leq G$ and $G \leq G$; these two are called the *trivial subgroups* of G . If $H \leq G$ and $g \in G$, then gH is called a *left coset* of G , and it is simply the set $\{gh|h \in H\}$. Note that gH is not necessarily a subgroup of G .

Theorem 8.3 (Lagrange). *If G is a finite group and $H \subseteq G$, then $|H|$ divides $|G|$, i.e., the order of H divides the order of G .*

Proof. If $g_1, g_2 \in G$, then the two cosets g_1H and g_2H are either identical or $g_1H \cap g_2H = \emptyset$. To see this, suppose that $g \in g_1H \cap g_2H$, so $g = g_1h_1 = g_2h_2$. In particular, $g_1 = g_2h_2h_1^{-1}$. Thus, $g_1H = (g_2h_2h_1^{-1})H$, and since it can be easily checked that $(ab)H = a(bH)$ and that $hH = H$ for any $h \in H$, it follows that $g_1H = g_2H$.

Therefore, for a finite $G = \{g_1, g_2, \dots, g_n\}$, the collection of sets $\{g_1H, g_2H, \dots, g_nH\}$ is a partition of G into subsets that are either disjoint or identical; from among all subcollections of identical cosets we pick a representative, so that $G = g_{i_1}H \cup g_{i_2}H \cup \dots \cup g_{i_m}H$, and so $|G| = m|H|$, and we are done. \square

Problem 8.3. *If G is a group, and $\{g_1, g_2, \dots, g_k\} \subseteq G$, then the set $\langle g_1, g_2, \dots, g_n \rangle$ is defined as follows*

$$\{x_1x_2 \cdots x_p | p \in \mathbb{N}, x_i \in \{g_1, g_2, \dots, g_k, g_1^{-1}, g_2^{-1}, \dots, g_k^{-1}\}\}.$$

Show that $\langle g_1, g_2, \dots, g_n \rangle \leq G$. This subgroup is called the subgroup generated by $\{g_1, g_2, \dots, g_n\}$. Also show that when G is finite $|\langle g \rangle| = \text{ord}_G(g)$.

Theorem 8.4 (Euler). For every n and every $a \in \mathbb{Z}_n^*$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. First it is easy to check that (\mathbb{Z}_n^*, \cdot) is a group. Then by definition $\phi(n) = |\mathbb{Z}_n^*|$, and since $\langle a \rangle \leq \mathbb{Z}_n^*$, it follows by Lagrange's theorem that $\text{ord}(a) = |\langle a \rangle|$ divides $\phi(n)$. \square

Note that Fermat's Little Theorem is an immediate consequence of Euler's Theorem, since when p is a prime, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, and $\phi(p) = (p-1)$.

Theorem 8.5 (Chinese Remainder). Given two sets of numbers of equal size, r_0, r_1, \dots, r_n , and m_0, m_1, \dots, m_n , such that

$$0 \leq r_i < m_i \quad 0 \leq i \leq n \quad (8.3)$$

and $\text{gcd}(m_i, m_j) = 1$ for $i \neq j$, then there exists an r such that $r \equiv r_i \pmod{m_i}$ for $0 \leq i \leq n$.

Proof. The proof we give is by counting; the distinct values of r , $0 \leq r < \prod m_i$, represent distinct sequences. To see that, note that if $r \equiv r' \pmod{m_i}$ for all i , then $m_i | (r - r')$ for all i , and so $(\prod m_i) | (r - r')$ (since the m_i 's are pairwise co-prime). So $r \equiv r' \pmod{(\prod m_i)}$, and so $r = r'$ if both $r, r' \in \{0, 1, \dots, (\prod m_i) - 1\}$.

But the total number of sequences r_0, \dots, r_n such that (8.3) holds is precisely $\prod m_i$. Hence every such sequence must be a sequence of remainders of some r , $0 \leq r < \prod m_i$. \square

Note that the CRT can be stated in the language of group theory as follows:

$$\mathbb{Z}_{m_1 \cdot m_2 \cdot \dots \cdot m_n} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_n}$$

where the m_i 's are pairwise co-prime.

Problem 8.4. The proof of theorem 8.5 (CRT) is non-constructive. Show how to obtain the r that meets the requirement of the theorem—efficiently, i.e., without using brute force search.

8.2 Answers to selected exercises

Exercise 8.2. $(a+1)^p \equiv_p \sum_{j=0}^p \binom{p}{j} a^{p-j} 1^j \equiv_p (a^p + 1) + \sum_{j=1}^{p-1} \binom{p}{j} a^{p-j}$. Note that $\binom{p}{j}$ is divisible by p for $1 \leq j \leq p-1$, and so we have that $\sum_{j=1}^{p-1} \binom{p}{j} a^{p-j} \equiv_p 0$. Thus we can prove our claim by induction on a . The

case $a = 1$ is trivial, and for the induction step we use the above observation to conclude that $(a+1)^p \equiv_p (a^p+1)$ and we apply the induction hypothesis to get $a^p \equiv_p a$. Once we have proved $a^p \equiv_p a$ we are done since for a such that $\gcd(a, p) = 1$ we have an inverse a^{-1} , so we multiply both sides by it to obtain $a^{p-1} \equiv_p 1$.

Exercise 8.4. Construct the r in stages, so that at stage i it meets the first i congruences, that is, at stage i we have that $r \equiv r_j \pmod{m_j}$ for $j \in \{1, 2, \dots, i\}$. Stage 1 is simple: just set $r \leftarrow r_1$. Suppose the first i stages have been completed; let $r \leftarrow r + (\prod_{j=1}^i m_j)x$, where x satisfies $x \equiv (\prod_{j=1}^i m_j)^{-1}(r_{i+1} - r) \pmod{m_{i+1}}$. We know that the inverse of $(\prod_{j=1}^i m_j)$ exists (in $\mathbb{Z}_{m_{i+1}}$) since $\gcd(m_{i+1}, (\prod_{j=1}^i m_j)) = 1$, and furthermore, this inverse can be obtained efficiently with the Extended Euclidean algorithm.