Number Theory

Alec Zabel-Mena

Text

K. Ireland, M. Rosen. "A Classical Introduction to the Modern Theory of Numbers". 2^{ed}, (1998).

September 13, 2020

Chapter 1

Unique Factorization

1.1 Unique Factorization in $\mathbb{Z}$

We begin with a few preliminary definitions and results about divisibility in $\mathbb{Z}$. The main goal of this section is to prove that the integers have a unique factorization in primes. This is a fundamental aspect in all of number theory, and a great deal of results in number theory depend on this notion.

Definition. For a and b integers, we say that a **divides** b if there exists some $c \in \mathbb{Z}$ such that $b = ac$. We also call a a **divisor** of b and we write $a|b$.

Definition. We say that a positive integer p is **prime** if it has only 1 and itself as divisors.

Example 1.1. The first few primes of $\mathbb{Z}$ are $2, 3, 5, 7, 11, \ldots$. Notice that 2 is the only odd prime

Example 1.2. $2|8.$, $3|15$, but $6 \not| 21$. Also see that $180 = 18 \cdot 10 = 2 \cdot 2 \cdot 9 \cdot 5 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5$. This is as far as we can factor 180, and it is also a unique representation of the factors of 180.

We also admit the following properties of divisibility:

(1) $a|a$ for $a \neq 0$.

(2) If $a|b$ and $b|a$, then $a = \pm b$.

(3) If $a|b$ and $b|c$, then $a|c$.

(4) If $a|b$ and $c|d$, then $ac|bd$.

(5) If $a|b$ and $a|c$, then $a|(bx + cy)$ for $x, y \in \mathbb{Z}$.

Lemma 1.1.1 (The Division Theorem)**.** *If a and b are integers, then there exist $r, q \in \mathbb{Z}$ unique such that $a = qb + r$ and $0 \leq r < b$.*

Proof. Consider the set $s = \{a - xb : x \in \mathbb{Z}\}$. S contains positive integers, for take $x = -|a|$, so by the Well Ordering Principle, let $r = a - qb$ be the smallest such integer. Now if $r = a - qb \geq b$, then $0 \leq a - (q+1)b < r$, contradicting the minimality of r, hence $0 \leq r < b$. The proof of uniqueness is left as an exercise. ■

Now for $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, let $(a_1, a_2, \ldots, a_n) = \{a_1x_1 + a_2x_2 + \ldots a_nx_n : x_1, x_2, \ldots x_n \in \mathbb{Z}\}$. We claim that this set is an ideal in $\mathbb{Z}$, for let $A = (a_1, a_2, \ldots, a_n)$. If $x_1, \ldots, x_n, y_1, \ldots, y_n, \in A$ then $x_1 + y_1, \ldots, x_n + y_n \in A$ by direct computation; moreover, for some $r \in \mathbb{Z}$, then $r(a_1x_1 + a_2x_2 + \ldots a_nx_) = a_1(rx_1) + a_2(rx_2) + \ldots a_n(rx_n)$ so $rx_1, \ldots, rx_n \in A$. We now use this to treat an object fundamental to divisibility.

Lemma 1.1.2. *If $a, b \in \mathbb{Z}$, then there exists some $d \in \mathbb{Z}$ such that $(a, b) = (d)$.*

Proof. Suppose a and b are not both 0, then (a, b) has positive elements; then again, by the Well Ordering Principle, let $d \in (a, b)$ be the smallest such positive element. Now if $r \in (d)$, then $r = dq = (am + bn)q = a(qm) + b(qn)$, for $m, n, q \in \mathbb{Z}$; hence $(d) \subseteq (a, b)$.

Now let $c \in (a, b)$. Then by the division theorem, there exist $r, q \in \mathbb{Z}$ unique such that $c = dq + r$ and $0 \leq r < d$. Since $d \in (a, b)$, then $r = c - dq \in (a, b)$, and by the minimality of d, $r = 0$. Hence $c = dq \in (d)$. So $(a, b) \subseteq (d)$, hence $(a, b) = (d)$. ■

Definition. Let a and b be positive integers. We call a positive integer d the **greatest common divisor** of both a and b if:

(1) $d|a$ and $d|b$.

(2) For some $c \in \mathbb{Z}$, if $c|a$ and $c|b$, then $c|d$.

Lemma 1.1.3. *Let $a, b, d \in \mathbb{Z}$. If $(a, b) = (d)$, then d is the greatest common divisor of a and b and is unique.*

Proof. Suppose that $(a, b) = (d)$. Then $a \in (d)$ and $b \in (d)$, hence $d|a$ and $d|b$. Now let $c|a$ and $c|b$ for some $c \in \mathbb{Z}$. Then $c|(ax + by)$ for $x, y \in \mathbb{Z}$. In particular, $c|d$. This makes d the greatest common divisor.

Now suppose that c is another greatest common divisor of a and b. Then we get that $c|d$ but also that $d|c$. Hence $c = \pm d$, and since $c \in \mathbb{Z}^+$ by definition, we have that $c = d$. ■

The lemmas say much more than just stating the existence and uniqueness of the greatest common divisor. First of all, uniqueness is determined up to sign, if we do not require the greatest common divisor to be a positive integer, then it is not unique; namely we have two greatest common divisors d and $-d$. Far more important, is that they tell us the form of the greatest common divisor. Considering the structure of (a, b),and since $d \in (a, b)$ is the smallest such element, then $d = am+bn$ for some particular choice of $m, n \in \mathbb{Z}$ (this does not tell us how to find them however). With this in mind, we can denote the greatest common divisor of a and b by (a, b), which is a justified notation with our development.

Definition. We say that two integers a and b are **coprime** (or **relatively prime**) if $(a, b) = 1$.

Proposition 1.1.4. *If $a|bc$ and $(a, b) = 1$ then $a|c$.*

Proof. Since $(a, b) = 1$, there exist $m, n \in \mathbb{Z}$ such that $am + bn = 1$. Then $acm + bcn = c$. Since $a|bc$, $acm + bcn = acm + adn = a(cm + dn) = c$ for some $d \in \mathbb{Z}$. Thus $a|c$. ■

Corollary. *If p is prime, and $p|bc$, then either $p|b$ or $p|c$.*

Proof. Notice for any integer a, $(a, p) = 1$ if $p \nmid a$, or $(a, p) = p$ if $p|a$. Now if $p|b$, we are done. If not, then $(b, p) = 1$, and hence by 1.1.4, $p|c$. ■

We are now in a position to prove unique factorization in $\mathbb{Z}$.

Lemma 1.1.5. *Evey nonzero integer can be written as a product of primes.*

Proof. Suppose not. Let N be the smallest such positive integer that cannot be written as a product of primes (then any integer smaller than N can); then N cannot be a prime number. Hence, $n = mn$ where $1 < m, n < N$ for $m, n \in \mathbb{Z}$. Then m and n can be written as a product of prime factors, but since $N = mn$, this contradicts our supposition. So every integer can be written as a product of primes. ■

By lemma 1.1.5, we can factor n into a product of primes, and group them into the form $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ where p_i is prime and $a_i \in \mathbb{Z}^+$ for $1 \leq i \leq m$. We would like to shorten this into the form:

$$n = (-1)^{\epsilon(n)} \prod_p p^{a(p)}$$

Where $\epsilon(n) = 0$ if $n \geq 0$ or $\epsilon(n) = 1$ of $n < 0$. This form will let us prove unique factorization in a quicker mannr than what is usual.

Definition. Let $n \in \mathbb{Z}$ and let p be a prime. The **order** of n about p is the smallest integer a such that $p^a|n$ but $p^{a+1} \nmid n$. We denote it $\operatorname{ord}_p n = a$. We take $\operatorname{ord}_p 0 = \infty$.

Lemma 1.1.6. $\operatorname{ord}_p n = 0$ *if and only if* $p \nmid n$.

Proof. If $\operatorname{ord}_p n = 0$, then $p^o = 1|n$ but $p^1 = p \nmid n$. Now suppose that $p \nmid n$. Then $p^1 \nmid n$, but $1 = p^0|n$, hence $\operatorname{ord}_p n = 0$. ■

Proposition 1.1.7. *Suppose that p is prime. Then for $a, b \in \mathbb{Z}$,* $\operatorname{ord}_P ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.

Proof. Let $\operatorname{ord}_p a = \alpha$ and $\operatorname{ord}_p b = \beta$. Then $p^\alpha|a$ and $p^\beta|b$, hence $p^{\alpha+\beta}|ab$. Now consider $p^{\alpha+\beta+1} = p^{(\alpha+1)+\beta} = p^{\alpha+(\beta+1)}$. If $p^{\alpha+\beta+1}|ab$, then this contradicts the orders of a or b respectively, hence $p^{\alpha+\beta+1} \nmid ab$. Therefore $\operatorname{ord}_p ab = \alpha + \beta = \operatorname{ord}_p a + \operatorname{ord}_p b$. ■

Theorem 1.1.8. *For every nonzero integer n, there exists a unique prime factorization:*

$$n = (-1)^{\epsilon(n)} \prod_p p^{a(p)} \tag{1.1}$$

Where $\operatorname{ord}_p(n) = a(p)$.

Proof. By lemma 1.1.5, we can write n as:

$$n = (-1)^{\epsilon(n)} \prod_p p^{a(p)}$$

Now, consider for some other prime q, ord_q. Then

$$\begin{aligned}
\text{ord}_q\, n &= \text{ord}_q\, ((-1)^{\epsilon(n)} \prod_p p^{a(p)}) \\
&= \text{ord}_q\, ((-1)^{\epsilon(n)}) + \text{ord}_q\, (\prod_p p^{a(p)}) \\
&= \epsilon(n)\, \text{ord}_q\, (-1) + \sum_p a(p)\, \text{ord}_q(p) \\
\text{ord}_q\, n &= \sum_p a(p)\, \text{ord}_q(p)
\end{aligned}$$

We have now that $\text{ord}_q\, p = 0$ if $q \neq p$ and $\text{ord}_q\, p = 1$ if $q = p$ (this proves uniqueness), and so $\sum_p a(p)\, \text{ord}_q(p) = a(q)$. Hence $\text{ord}_q(n) = a(q)$. ■

1.2 Unique Factorization in $K[x]$

Consider now an arbitrary field K. We denote $K[x] = \{\sum_{i=0}^{n} a_i x^i : a_i \in K\}$ to be the polynomial ring over K. Defining $+$ and $\cdot$ as the usual addition and multiplication for polynomials, and denoting two polynomials to be equal if their coefficients are equal, it can be shown that $K[x]$ indeed forms a ring. We would rather like to characterize unique factorization for such polynomials however. This means carrying over the same arguments and definitions which were used for $\mathbb{Z}$ over to $K[x]$. We denote polynomials in $K[x]$ as $f(x)$, or simply just f.

Definition. Let $f, g \in K[x]$ be polynomials. We say that f **divides** g if for some $h \in K[x]$, $g(x) = f(x)h(x)$. We write $f|g$.

We denote the **degree** of a polynomial f as the highest power of x; we denote it $\deg f$. In other words, we can define the degree of a ploynomial to be a map $\deg : K[x] \to \mathbb{Z}^+$. We also have that for two polynomials f, g that $\deg fg = \deg f + \deg g$. We have that $\deg f = 0$ if and only if $f \in K$. We call such polynomials **constant polynomials**, or just **constants**. We will call all nonzero elements of K **units** of $K[x]$.

Definition. We call a polynomial $p \in K[x]$ **irreducible** if for $q \in K[x]$, $q|p$ implies that either q is a unit, or $q(x) = cp(x)$ for some unit c.

Definition. A polynomial $f \in K[x]$ is called **monic** if it's leading coefficient is 1.; i.e. $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^n$ where $\deg f = n$.

Lemma 1.2.1 (The Division Theorem)**.** *Let $f, g \in K[x]$ with $g \neq 0$. Then there exists $q, r \in K[x]$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r < \deg g$.*

Proof. If $g|f$, the take $q(x) = \frac{f(x)}{g(x)}$ and $r(x) = 0$, and we are done. Now suppose that $g \not| f$. Consider the set $\{l(x) : f(x) - l(x)g(x)\}$. Since $\deg : K[x] \to \mathbb{Z}^+$, the set of degrees of polynomials of the form $f(x) - l(x)g(x)$ forms a subset of $\mathbb{Z}^+$, hence by the WOP, there exists a least degree of that set; and so there exists a polynomial of least degree, $r(x) = f(x) - q(x)g(x)$ of that set. Now If $r(x) = 0$, we are done, so suppose that $r(x) \neq 0$. If it happens that $\deg r \geq \deg g$, let $d = \deg r$, $m = \deg g$ and consider the leading terms ax^d, bx^m of r and g respectively. Then $r(x) - ab^{-1}x^{d-m}g(x) = f(x) - (q(x) + ab^{-1}x^{d-m})g(x)$ which has smaller degree than r, contradicting its minimality. And so $\deg r < \deg g$. ■

Now if $f_1, \ldots, f_n \in K[x]$, let $(f_1, \ldots, f_n) = \{f_1h_1 + \cdots + f_nh_n : h_i \in K[x]\}$. Then $f_1, \ldots, f_n)$ forms an ideal in $K[x]$.

Lemma 1.2.2. *Let $f, g \in K[x]$. Then there exists a $d \in K[x]$ such that $(f, g) = (d)$.*

Proof. Let $d \in (f, g)$. Be the polynomial of least degree (this is guaranteed by the WOP). Then $d(x) = f(x)h_1(x) + g(x)h_2(x)$ for $h_1, h_2 \in K[x]$. Hence for $q \in K[x]$, $d(x)q(x) = f(x)(q(x)h_1(x)) + g(x)(q(x)h_2(x))$, so $(d) \subseteq (f, g)$. Now let $c \in (f, g)$. If $d|c$, we are done. If not, then for $q, r \in K[x[$, $c(x) = q(x)d(x) + r(x)$ with $\deg r < \deg d$. Since $c, d \in (f, g)$, $r(x) = c(x) - q(x)d(x) \in (f, g)$, contradicting the minimality of d. so $d \not| c$ cannot occur. So $c \in (d)$; hence $(f, g) \subseteq (d)$. Therefore $(f, g) = (d)$. ■

We can now define the greatest common divisor of two polynomials, analogous to the greatest common divisor of two integers.

Definition. We say that a polynomials $d \in K[x]$ is a **greatest common divisor** of two polynomials $f, g \in K[x]$ if:

(1) $d|f$ and $d|g$.

(2) If $c|f$ and $c|g$ for $c \in K[x]$, then $c|d$.

The greatest common divisor is determined up to the constant multiplication by a unit, however if we require the greatest common divisor to be a monic polynomial, then it is unique. What is left, is then for us to show that such an object exists.

Lemma 1.2.3. *Let $f, g \in K[x]$. If for some $d \in K[x]$, $(f, g) = (d)$, then d is the greatest common divisor.*

Proof. By lemma 1.2.2 such a d exists in (f, g). Now let $(f, g) = (d)$, then $f, g \in (d)$, and so $d|f$ and $d|g$.

Now let $c \in K[x]$ such that $c|f$ and $c|g$. Then in particular, $c|fn+gm$ for all $m, n \in K[x]$. In particular, $c|d$. ■

We shall denote the greatest common divisor as $(f, g) = (d)$, or when we are only considering monic polynomials, we may write $(f, g) = d$.

Definition. Two polynomials $f, g \in K[x]$ are **coprime** or (**relatively prime**) if the only common divisor is a unit, i.e. $(f, g) = c$ for some $c \in K$. We also write $(f, g) = (1)$.

Definition. Let p be a monic irreducible polynomial, and let $f \in K[x]$. We define the **order** of f at p to be the smallest integer a such that $p^a | f$ but $p^{a+1} \nmid f$. We denote it $\operatorname{ord}_p f = a$.

Again, $\operatorname{ord}_p f = 0$ if and only if $p \nmid f$.

Proposition 1.2.4. *If f and g are relatively prime, and $f|gh$, then $f|h$.*

Proof. Let $(f, g) = c$ for some $c \in K$. Then there are polynomials n, m such that $fn+gm = c$. Hence $fhn + ghm = fhn + fkm = f(hn + km) = c$. Since c is a unit, $f \nmid c$, so it must be that $f|h$. ■

Corollary. *If p is irreducible, and $p|fg$, then $p|f$ or $p|g$.*

Proof. Since p is irreducible, then either $(f, p) = (p)$ or $(f, p) = (1)$. If $(f, p) = (p)$, then $p|f$ and we are done. Suppose the latter case then. If $p \nmid f$, but $p|fg$, then it must be that $p|g$. ■

Corollary. *If p is a monic irreducible polynomial, and $f, g \in K[x]$, then* $\operatorname{ord}_p fg = \operatorname{ord}_p f + \operatorname{ord}_p g$.

Lemma 1.2.5. *Every nonconstant polynomial is the product of irreducible polynomials.*

Proof. By induction on the degree. If $\deg f = 1$, then by the division theorem, there exists $q, r \in K[x]$ such that $f(x) = q(x)g(x) + r(x)$ where $r(x) = 0$ or $\deg r < \deg g$. Likewise, both $\deg q, \deg g \leq \deg f = 1$. Hence Either q or g is a unit, and the latter is a polynomial of deg $= 1$. Hence choose g. Then $\deg r < 1$, and so r is also a unit or 0. Hence f is nonconstant, and is irreducible.

Now suppose for all polynomials of deg $< n$ that the result is true, and let $\deg f = n$. If f is irreducible, we are done; so suppose not. Then $f(x) = g(x)q(x)$ with $1 \leq \deg g, \deg q < n$. So by hypothesis, g and q can be expressed as a product of irreducible polynomials, and since $f = gq$, hence so is f. ■

In particular, some irreducible factors of f may be monic irreducible, so we simply factor out all the units of the nonmonic polynomials and get a factorization completely in terms of monic irreducible polynomials.

Theorem 1.2.6. *Let $f \in K[x]$. Then*

$$f(x) = c \prod_p p(x)^{a(p)} \tag{1.2}$$

Where the product is over all monic irreducible polynomials that divide f, and c is a unit, and $a(p) = \operatorname{ord}_p f$.

Proof. By lemma 1.2.5 we can express the irreducible factorization of f as

$$f(x) = c\prod_p p(x)^{a(p)}$$

Where the product is over all monic irreducible factors of f. Then let q be a monic irreducible polynomial of f. Then applying ord_q to both sides:

$$\begin{aligned}\operatorname{ord}_q f &= \operatorname{ord}_q c\prod_p p(x)^{a(p)} \\ &= \operatorname{ord}_q c + \sum_p a(p)\operatorname{ord}_q p(x) \\ \operatorname{ord}_q f &= \sum_p a(p)\operatorname{ord}_q p(x)\end{aligned}$$

Now since q is monic irreducible, we have that $\operatorname{ord}_q p = 0$ when $q \neq p$, and $\operatorname{ord}_q p = 1$ when $q = p$. So we get that $\operatorname{ord}_q f = a(q)$. ■

1.3 Unique Factorization in a Principle Ideal Domain

Both $\mathbb{Z}$ and $K[x]$ aren't unique in terms of rings where unique factorization holds. In fact, there are a whole class of rings in which this is true. We now examine such rings. We first not that a ring R is an **integral domain** if for $a, b \in R$ the expression $ab = 0$ implies that either $a = 0$ or $b = 0$ (i.e. there exist no zero-divisors). We will be working in integral domains.

Definition. Let R be an integral domain. We call R a **Euclidean domain**, if ther is a map $\lambda : R^* \to \mathbb{Z}^+$ such that for $a \in R$ and $b \in R^*$, there exists $q, r \in R$ such that $a = qb + r$ and $r = 0$ or $\lambda(r) < \lambda(b)$.

Example 1.3. Both $\mathbb{Z}$ and $K[x]$ were shown to be Euclidean domains, for $\mathbb{Z}$, we took $\lambda = |\cdot|$, and for $K[x]$, we took $\lambda = \deg$.

Proposition 1.3.1. *If R is a Euclidean domain, and $I \subseteq R$ is an ideal in R, then there exists an $a \in R$ such that $I = Ra$.*

Proof. Consider the set $\{\lambda(b) : b \in I \text{ and } b \neq 0\}$. This set clearly forms a subset of $\mathbb{Z}^+$, and so by the WOP, there is a least element $\lambda(a)$ for $a \in I$ and $a \neq 0$. So $\lambda(a) \leq \lambda(b)$ for all $b \neq 0 \in I$. Now consider $Ra = \{ra : r \in R\}$. Since I is an ideal, and $a \in I$, we get that $Ra \subseteq I$. Now let $b \in I$. Then there are $q, r \in R$ such that $b = qa + r$ where $r = 0$ or $\lambda(r) < \lambda(a)$; but by the minimality of $\lambda(a)$, we get that $r = 0$. So $b = qa \in Ra$. Hence $I \subseteq Ra$, and so $I = Ra$. ■

Before proceeding further, we make some preliminary definitions. First, let for $a_1, \ldots, a_n \in R$, and define $(a_1, \ldots, a_n) = Ra_1 + \ldots Ra_n = \{\sum_{i=1}^n r_i a_i : r_i \in R\}$. This is an ideal in R.

Definition. We say that an ideal I in R is **finitely generated** if $I = (a_1, \ldots, a_n)$ for $a_1, \ldots, a_n \in I$. We say that I is a **principle ideal** if $I = (a)$ for some $a \in I$.

Definition. We say that an integral domain R is a **Principle Ideal Domain** (PID) if every ideal in R is a principle ideal.

Hence, we have show that any Euclidean domain is a PID. However, the converse is not necessarily true. For the coming definitions, assume that R is a Euclidean domain.

Definition. Let $a, b \in R$ and $b \neq 0$, we say that b **divides** a if for some $c \in R$, $a = bc$. We write $b|a$.

The usual properties of divisibility can be shown.

Definition. An element $u \in R$ is called a **unit** if $u|1$.

Definition. Two elements $a, b \in R$ are associates if $a = bu$ for some unit u.

Definition. An element $p \in R$ is **irreducible** if for $q \in R$, $q|p$ implies that q is either a unit, or an associate of p.

Definition. A nonunit $p \in R^*$ is **prime** if for $a, b \in R$, $p|ab$ implies that $p|a$ or $p|b$.

As unlike in $\mathbb{Z}$ and $K[x]$, it is not the case in a general Euclidean domain that the notions of a prime, and irreducible coincide.

Definition. An element $d \in R$ is ca;;ed a **greatest common divisor** of two elements $a, b \in R$ if:

(1) $d|a$ and $d|b$.

(2) If $c|a$ and $c|b$, then $c|d$, for $c \in R$.

If both d and d' are greatest common divisors of a and b, then $d|d'$ and $d'|d$, so $d = d'u$, for some unit u. Hence, d and d' are associate.

Proposition 1.3.2. *Let R be a PID, and let $a, b \in R$. Then a and b have a greatest common divisor $d \in R$, and $(a, b) = (d)$.*

Proof. Since R is a PID, there exists such a $d \in R$ such that $(a, b) = (d)$. Now we have that $(a) \subseteq (d)$ and $(b) \subseteq (d)$. So $d|a$ and $d|b$.

Now let $c|a$ and $c|b$. Then $(a) \subseteq (c)$ and $(b) \subseteq (d)$, hence $(a, b) = (d) \subseteq (c)$, so $c|d$. Thus d is the greatest common divisor of a and b. ■

The existence of a greatest common divisor is completely dependent on whether R is a PID.

Definition. Two elements $a, b \in R$ are **coprime** (or **relatively prime**) if (a, b) is a unit in R

Corollary. *If R is a PID, and $a, b \in R$ are coprime, then $(a, b) = R$.*

Corollary. *If R is a PID, and $p \in R$ is irreducible, then p is prime.*

Proof. Suppose for $a, b \in R$ that $p|ab$ and that $p \not| a$. Then $(a, p) = R$, thus $(ab, bp) = (b)$. Now since $ab \in (p)$, and $bp \in (p)$, then $(ab, bp) = (b) \subseteq (p)$ and so $p|b$. ■

Lemma 1.3.3. *Let R be a PID and consider the sequence $\{(a_1), (a_2), \dots, (a_n), \dots\}$ of ideals in R such that $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \dots$. Then there is a $k \in \mathbb{Z}^+$ such that $(a_k) = (a_{k+l})$ for $l \in \mathbb{Z}^+$. That is the sequence $\{(a_1), (a_2), \dots, (a_n), \dots\}$ is not infinite and terminates at (a_k).*

Proof. Let $I = \bigcup_{i=1}^{\infty}(a_i)$. Since (a_i) is an ideal for all $1 \leq i$, then it follows that I is also an ideal; and since R is a PID, there is some $a \in R$ such that $I = (a)$. That is $(a) = \bigcup_{i=1}^{\infty}(a_i)$. So $a \in \bigcup_{i=1}^{\infty}(a_i)$, and hence $a \in (a_k)$ for some $k \in \mathbb{Z}^+$. So $I = (a) \subseteq (a_k)$. Now suppose that $a \in (a_{k+l})$ for $l \in \mathbb{Z}^+0$. Then $I = (a_{k+l})$, and since $(a_k) \subseteq (a_{k+l})$, we have that $(a_k) \subseteq I$. Hence $(a_k) = I$, so $(a_k) = (a_{k+l})$. ■

Proposition 1.3.4. *Every nonunit of a PID R can be expressed as a product of irreducibles.*

Proof. We first show that every nonunit is divisible by an irreducible. Let $a \in R^*$ be a nonunit. If a is irreducible we are done. If not, then $a = a_1b_1$ for $a_1, b_1 \in R^*$ nonunits. It is sufficient to just look at one of the terms. If a_1 is irreducible, we are done. If not, $a_1 = a_2b_2$ where $a_2, b_2 \in R^*$ are nonunits. Continuing this way, we get a sequence $\{(a_1), (a_2), \dots\}$ such that $(a_1) \subseteq (a_2) \subseteq \dots$. By lemma 1.3.3, this sequence ends at some (a_k), i.e. for some positive integer k, (a_k) is irreducible. And so there is some irreducible element $a_k|a$.

Now we show that a is a product of irreducible elements. If a is irreducible, then we are done. If not, then $a = p_1c_1$ where $p_1|a$. Now if c_1 is a unit, we are done. If not, $c_1 = p_2c_2$ where $p_2|c_1$. Continuing along this line, we get a sequence $\{(c_1), (c_2), \dots\}$ such that $(c_1) \subseteq (c_2) \subseteq \dots$, then again by lemma 1.3.3, there is some positive integer k for which c_k is a unit. Hence $a = p_1p_1 \dots p_kc_k$, where p_kc_k is irreducible. ■

Lemma 1.3.5. *Let p be a prime, and let $a \neq 0$. Then there is an $n \in \mathbb{Z}^+$ for which $p^n|a$ but $p^{n+1} \not| a$.*

Proof. Suppose to the contrary. Then for every $m > 0 \in \mathbb{Z}^+$, there is a $b_m \in R$ such that $a = p^m b_m$. Then let $b_m = pb_{m+1}$. The $(b1) \subseteq (b_2) \subseteq \dots$ is infinite ascending, which contradicts lemma 1.3.3. ■

Now we have that n is uniquely determined by p and a, so we can define:

Definition. Let $a \in R^*$ and let p be a prime. The **order** of a at p is the least integer $n \in \mathbb{Z}^+$ such that $p^n|a$ but $p^{n+1} \not| a$. We denote it $\operatorname{ord}_p a = n$.

We have again that $\operatorname{ord}_p a = 0$ if and only if $p \not| a$.

Lemma 1.3.6. *If $a, b \in R^*$, then $\operatorname{ord}_p ab = \operatorname{ord}_p a + \operatorname{ord}_p b$.*

Theorem 1.3.7. *Let R be a PID, and let S be a set of primes in R such that every prime in R is associate to a prime in S, and no two primes in S are associate. Then if $a \in R^*$ we can write*

$$a = u \prod_{p \in S} p^{e(p)} \tag{1.3}$$

Where u is a unit. Both u and $e(p)$ are uniquely determined by a, in fact, $e(p) = \operatorname{ord}_p a$.

Proof. By proposition 1.3.4, we can factorize a into

$$a = u \prod_p p^{e(p)}$$

Where u is a unit and the product is over all $p \in S$. Now let $q \in S$. Then applying ord_q to both sides

$$\begin{aligned} \operatorname{ord}_q a &= \operatorname{ord}_q u \prod_{p \in S} p^{e(p)} \\ &= \operatorname{ord}_q u + \sum_{p \in S} e(p) \operatorname{ord}_q p \end{aligned}$$

Now since u is a unit, $q \not| u$, so $\operatorname{ord}_q u = 0$. Now we also have that since $q, p \in S$, they are not associate, so if $q \neq p$, $\operatorname{ord}_q p = 0$. So $\operatorname{ord}_q p = 1$ whenever $q = p$. Hence $e(q) = \operatorname{ord}_q(a)$ is uniquely determined. Since $e(q)$ is uniquely determined, then so is u. ■

Chapter 2

Application of Unique Factorization

2.1 Basic prime distribution in $\mathbb{Z}$

Theorem 2.1.1. *There are infinitely many primes in $\mathbb{Z}$.*

Proof. We give a proof attributed to Euclid. Suppose there are finitely many primes in $\mathbb{Z}$. Then we can list them as $p_1, p_2, \ldots, p_n$, such that $p_1 < p_2 < \cdots < p_n$. Now let $N = p_1 p_2 \ldots p_n + 1$. Now $N > 1$, and we also have that $p_i \not| N$ for all $1 \leq i \leq n$. However, by theorem 1.1.8, N has a prime factorization, and there exists some prime p dividing N. Now we have that $p \not| p_1 p_2 \ldots p_n$, so $p \not| p_i$, and since p cannot be in the list of primes, we have that $p_n < p$; contradicting that there are finitely many primes. ■

We now consider another set of numbers. Let p be a prime, and let $\mathbb{Z}_p = \{\frac{a}{b} : a, b \in \mathbb{Z} \text{ and } p \not| b\}$. We note that $\mathbb{Z}_p \subseteq \mathbb{Q}$. Now we have that $\frac{ad+cb}{bd}, \frac{ac}{bd} \in \mathbb{Z}_p$ as $ad + bc, ac, bd \in \mathbb{Z}$ and $p \not| b$ and $\not| d$ implies that $p \not| bd$. Likewise, we have that $\frac{-a}{b} \in \mathbb{Z}_p$ whenever $\frac{a}{b} \in \mathbb{Z}_p$. So $\mathbb{Z}_p$ is a subring of $\mathbb{Q}$, and hence a ring.

Lemma 2.1.2. *An element $\frac{a}{b} \in \mathbb{Z}_p$ is a unit if and only if $p \not| a$ and $p \not| b$.*

Proof. An element $\frac{a}{b} \in \mathbb{Z}_p$ is a unit if for some $\frac{c}{d} \in \mathbb{Z}_p$, $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} = 1$. Then $ac = bd$, and since $p \not| bd$, then $p \not| ac$, hence $p \not| a$. Now suppose that $p \not| a$ and $p \not| b$. Consider $c, d \in \mathbb{Z}$ such that $ac = pbd$dividing by p, we get $ac' = bd'$ where $p \not| c', d'$ and hence $\frac{c'}{d'} \in \mathbb{Z}_p$ and $\frac{a}{b}\frac{c'}{d'} = 1$. This makes $\frac{a}{b}$ into a unit of $\mathbb{Z}_p$. ■

Now suppose that $\frac{a}{b} \in \mathbb{Z}_p$, and let $a = p^l a'$ where $p \not| a$. Then $\frac{a}{b} = p^l \frac{a'}{b}$ and since $p \not| b$, then $\frac{a'}{b}$ is a unit in $\mathbb{Z}_p$. Hence, every element of $\mathbb{Z}_p$ is a prime power times a unit. That is, every element is associate to a prime power.

Lemma 2.1.3. *Every prime in $\mathbb{Z}_p$ is associate to another prime in $\mathbb{Z}_p$.*

Proof. Let $\frac{a}{b} \in \mathbb{Z}_p$ be a prime. We have that $\frac{a}{b} = p^l \frac{a'}{b}$ where $\frac{a'}{b}$ is a unit. Then since $\frac{a}{b}$ is prime, and $\frac{a'}{b}$ is a unit, then it follows that p^l itself must be a prime, thus $\frac{a}{b}$ is associate to p^l. ■

Lemma 2.1.4. *If $\frac{a}{b} \in \mathbb{Z}_p$ is not a unit, then $\frac{a}{b} + 1$ is a unit in $\mathbb{Z}_p$.*

Proof. Let $\frac{a}{b} \in \mathbb{Z}_p$ not be a unit. Then $p|a$. Now then, $\frac{a}{b} + 1 = \frac{a+b}{b}$. Now since $p \not| b$, it follows that even though $p|a$, that $p \not| a + b$. Hence $\frac{a+b}{b}$ is a unit. ■

Theorem 2.1.5. *There are finitely many primes in $\mathbb{Z}_p$*

Proof. Suppose there are infinitely many primes in $\mathbb{Z}_p$. Let $q_1, \ldots, q_n$ be a list of primes in $\mathbb{Z}_p$, and let $q \in \mathbb{Z}_p$ be another prime. By proposition 2.1.3, we have that q is associate to some prime, say q_i in $\mathbb{Z}_p$. Then $q = q_i \frac{a'}{b}$ with $\frac{a'}{b}$ a unit. Now, notice that $q_i|q$, however, since both q, q_i are prime, then $q = q_i$. We also have that $q + 1$ is a unit by proposition 2.1.4, and hence cannot be prime. ■

The ring $\mathbb{Z}_p$ shows, that in general, there need not be an infinite number of primes. We now give Euclid's proof for prime distribution in $K[x]$. Here by prime, we mean a monic irreducible polynomial.

First notice that if the field K is finite (the existence of such fields will be discussed later), that the polynomial ring $K[x]$ is also finite, and by consequence, there must be finitely many monic irreducible polynomials (this serves as another example of a finite prime distribution in a given ring). So let K be infinite, and suppose there are finitely many monic irreducible polynomials $p_!, p_2, \ldots, p_n$ such that $\deg p_1 < \deg p_2 < \cdots < \deg p_n$. Now let $N \in K[x]$ be such that $N(x) = p_1(x)p_2(x)\ldots p_n(x) + c$ where $c \in K$. We have that $\deg N > 1$, so N is not a unit. Likewise, $p_i \not| N$ for $1 \leq i \leq n$. However, by theorem 1.2.6 there is some monic irreducible polynomial p that divides N. Now we have that $\deg p \leq \deg p_1 p_2 \ldots p_n$, but p cannot be in the list, so we have that $\deg p_n < \deg p$, which contradicts that there are finitely many monic irreducible polynomials in $K[x]$.

2.2 Arithmetic Functions

One of the most important concepts in number theory, is that of an arithmetic function. That is a function or map that takes integers into integers. We will study such functions.

Definition. An integer $a \in \mathbb{Z}$ is **square free** if it is not divisible by the square of any other integer greater than 1.

Proposition 2.2.1. *If $n \in \mathbb{Z}$, then $n = ab^2$ where $a, b \in \mathbb{Z}$ and a is square free.*

Proof. Let $n = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$. Now let $a_i = 2b_i + r_i$ where $r_i = 0$ or $r_i = 1$ for $1 \leq i \leq l$.Then $n = (p_1^{r_1} p_2^{r_2} \ldots p_l^{r_l})(p_1^{b_1} p_2^{b_2} \ldots p_l^{b_l})^2$, letting $a = p_1^{r_1} p_2^{r_2} \ldots p_l^{r_l}$, then it is clear that a is square free. ■

Now let $\tau : \mathbb{Z}^+ \to \mathbb{Z}^+$ be such that $\tau(n)$ is the number of positive divisors of n. Let $\sigma : \mathbb{Z}^+ \to \mathbb{Z}^+$ be such that $\sigma(n)$ is the sum of all positive divisors of n. We notice that:

$$\tau(n) = \sum_{d|n} 1 \text{ and } \sigma(n) = \sum_{d|n} d$$

Definition. We say that an arithmetic function, i.e. a map $f : \mathbb{Z} \to \mathbb{Z}$ is **multiplicative** if for $m, n \in \mathbb{Z}$ and $(m, n) = 1$, then $f(mn) = f(m)f(n)$.

Lemma 2.2.2. *τ is multiplicative*

Proof. Let $m, n \in \mathbb{Z}$ with $(m, n) = 1$. Then

$$\tau(mn) = \sum_{d|mn} 1$$

Now if $d|mn$, let $d = d_1 d_1'$ such that $d_1|m$ and $d_1'|n$. Now since $(m, n) = 1$ we have that $d_1 \nmid n$ and $d_1 \nmid m$. We also have as a consequence of theorem 1.1.8, that the number of divisors of an integer is finite, Hence there is a set of divisors of mn: $S = \{d_1, d_2, \ldots, d_l, d_1', d_2', \ldots, d_r'\}$ that can be partitioned into $S = \{d_1, d_2, \ldots, d_l\} \cup \{d_1', d_2', \ldots, d_r'\}$ where $d_i|m$ and $d_j'|n$ for $1 \leq i \leq l$ and $1 \leq j \leq r$. Let $M = \{d_1, d_2, \ldots, d_l\}$ and $N = \{d_1', d_2', \ldots, d_r'\}$. Then $S = M \cup N$ and:

$$\begin{aligned}\tau(mn) &= \sum_{S} 1 = \sum_{M \cup N} 1 \\ &= \sum_{M} \sum_{N} 1 \\ \tau(mn) &= (\sum_{d_i|m} 1)(\sum_{d_j'|n} 1) = \tau(m)\tau(n)\end{aligned}$$

■

Lemma 2.2.3. *Let $n = p^a$ for p prime and $a \in \mathbb{Z}^+$. Then $\tau(n) = a + 1$*

Proof. We have that the divisors of p^a are $1, p, p^2, \ldots, p^a$, and there are $a + 1$ of them.

$$\tau(n) = \sum_{d|p^a} 1 = \underbrace{1 + 1 + \cdots + 1}_{a+1 \text{ times}} = a + 1$$

■

Lemma 2.2.4. *σ is multiplicative*

Proof. Let $m, n \in \mathbb{Z}$ such that $(m, n) = 1$. As in the proof of lemma 2.2.2, we have that the set of divisors of mn can partitioned into the set $S = M \cup N$ where $M = \{d_1, d_2, \ldots, d_l\}$ and $N = \{d_1', d_2', \ldots, d_r'\}$ such that $d_i|m$ and $d_j'|n$ for $1 \leq i \leq l$ and $1 \leq j \leq r$. We get that for any divisor d of mn, that $d = d_i d_j'$. Then

$$\begin{aligned}\sigma(mn) &= \sum_{d|mn} d = \sum_{S} d \\ &= \sum_{M \cup N} d_i d_j' = \sum_{d_i|m} \sum_{d_j'|n} d_i d_j' \\ \sigma(mn) &= (\sum_{d_i|m} d_i)(\sum_{d_j'|n} d_j') = \sigma(m)\sigma(n)\end{aligned}$$

■

Lemma 2.2.5. *Let $n = p^a$ where p is prime and $a \in \mathbb{Z}^+$. Then $\sigma(n) = \frac{p^{a+1}-1}{p-1}$*

Proof. We first note that for any integers $a, k \in \mathbb{Z}$ that $a^{k+1} - 1 = (a-1)(a^k + a^{k-1} + \cdots + a^2 + a + 1)$.

Now let $n = p^a$ for p a prime, and $a \in \mathbb{Z}^+$. Then

$$\sigma(n) = \sum_{d|p^a} d = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

■

We now can find general formulas for τ and σ.

Proposition 2.2.6. *Let $n \in \mathbb{Z}^+$ and let $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$. Then:*

(1) $\tau(n) = (a_1 + 1)(a_2 + 1) \dots (a_l + 1)$

(2) $\sigma(n) = (\frac{p_1^{a_1+1}-1}{p_1-1})(\frac{p_2^{a_2+1}-1}{p_2-1}) \dots (\frac{p_l^{a_l+1}-1}{p_l-1})$

Proof. We make use of the multiplicity of τ and σ. First notice that since p_i is prime for $1 \leq i \leq l$, then $(p_i, p_j) = 1$ whenever $i \neq j$. Hence

(1) $\tau(n) = \tau(p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}) = \tau(p_1^{a_1})\tau(p_2^{a_2}) \dots \tau(p_l^{a_l}) = (a_1 + 1)(a_2 + 1) \dots (a_l + 1)$.

(2) $\sigma(n) = \sigma(p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}) = \sigma(p_1^{a_1})\sigma(p_2^{a_2}) \dots \sigma(p_l^{a_l}) = (\frac{p_1^{a_1+1}-1}{p_1-1})(\frac{p_2^{a_2+1}-1}{p_2-1}) \dots (\frac{p_l^{a_l+1}-1}{p_l-1}$.

■

There does exist a proof of proposition 2.2.6 independent of multiplicity, and if we assume such proof, then we can use proposition 2.2.6 to prove that τ and σ are multiplicative. We now go through some immediate applications of these arithmetic functions.

Definition. An integer n is **perfect** if $\sigma(n) = 2n$.

Lemma 2.2.7. *If for $m \in \mathbb{Z}^+$, $2^{m+1} - 1$ is prime, then $n = 2^m(2^{m+1} - 1)$ is perfect.*

Proof. Let $n = 2^m(2^{m+1} - 1)$ with $m \in \mathbb{Z}^+$ and $2^{m+1} - 1$ prime. Then $\sigma(n) = \sigma(2^m)\sigma(2^{m+1} - 1) = 2^{m+1}(2^{m+1} - 1) = 2(2^m(2^{m+1} - 1)) = 2n$ ■

Definition. Let $m \in \mathbb{Z}^+$. A **Mersenne prime** is any prime of the form $2^{m+1} - 1$

Lemma 2.2.8. *If for $a \in \mathbb{Z}$, and $n \in \mathbb{Z}^+$, $a^n - 1$ is prime, then $a = 2$, and n is prime.*

Proof. We have that $a^n - 1 = (a - 1)(a^{n-1} + \cdots + a^2 + a + 1)$. Now both $a - 1$ and $a^{n-1} + \cdots + a^2 + a + 1$ divide $a^n - 1$, so let $a - 1 = 1$, hence $a = 2$. So we get $2^n - 1 = 2^{n-1} + \cdots + 2^2 + 2 + 1$.

Now suppose $n = ab$, with $(a, b) = 1$. Then $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a)^{b-1} + \cdots + (2^a)^2 + 2^a + 1$, so $2^n - 1 = 2^{ab-a} + \cdots + 2^{2a} + 2^a + 1 = 2^{n-a} + \cdots + 2^{2a} + 2^a + 1$. Now since $2^n - 1$ is prime, and has the form $2^{n-1} + \cdots + 2^2 + 2 + 1$, then necessarily, $a = 1$, which makes n a prime. ■

Hence if $2^{m+1}-1$ is a Mersenne prime for some $m \in \mathbb{Z}^+$, then $m+1$ is prime. We call general numbers of the form $2^{m+1}-1$ **Mersenne numbers**.

Definition. An integer n is **multiplicatively perfect** if the product of its divisors is n^2.

So n is multiplicatively perfect if $\prod_{d|n} d = n^2$. We go over a few requirements for a number to be multiplicatively perfect. If n is prime, then $\prod_{d|n} d = 1 \cdot n = n$, so n cannot be prime.What if $n = p^2$, with p a prime? Then $\prod_{d|n} d = 1 \cdot p \cdot p^2 = p^3$, so n cannot be the square of a prime.

Now suppose n is not prime, nor the square of a prime. Then there is a proper divisor $d \neq \frac{n}{d}$ of n, and $\prod_{d|n} d = 1 \cdot d \cdot \frac{n}{d} \cdot n = n^2$. Now suppose that n is multiplicatively perfect. Then there es a divisor d of n such that $n \cdot d = n^2$, hence $d = n$. So $d = d' \frac{n}{d}$, where $d' \neq \frac{n}{d}$. Now suppose there is a third perfect divisor $\frac{n}{d_1}$. Then $1 \cdot \frac{n}{d_1} \cdot d \cdot n = \frac{n^3}{d_1}$, which contradicts that n is multiplicatively perfect. Hence we get the lemma:

Lemma 2.2.9. *An integer n is multiplicatively perfect, if and only if n is the product of exactly two prefect divisors.*

From this lemma we can see that integers of the form p^3 and $p^l q^r$, with p, q prime, are multiplicatively perfect.

Example 2.1. $27 = 3^3$, so 27 is multiplicatively perfect. $1 \cdot 3 \cdot 3^2 \cdot 27 = 729 = 27^2$. Likewise, $10 = 2^1 5^1$, so 10 is multiplicatively perfect. $1 \cdot 2 \cdot 5 \cdot 10 = 100 = 10^2$.

Definition. We define the **Möbius μ function** to be the map $\mu : \mathbb{Z}^+ \to \mathbb{Z}$ such that:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^l & \text{if for } p_i \text{ prime, } n = p_1 p_2 \dots p_l \\ 0 & \text{if } n \text{ is not square free} \end{cases} \tag{2.1}$$

Lemma 2.2.10. *μ is multiplicative.*

Proof. Let $m, n \in \mathbb{Z}^+$ with $(m, n) = 1$. Consider when $m = 1$ or, when $m = 1$ and $n = 1$. We get $\mu(mn) = \mu(n) = 1 \cdot \mu(n) = \mu(m)\mu(n)$; or $\mu(mn) = 1 = 1 \cdot 1 = \mu(m)\mu(n)$. Now suppose that $m, n \neq 1$, and that m is not square free. Then if m is not square free, then $a^2 | m$ for some $a \in \mathbb{Z}$. So $a^2 | mn$, so mn is not square free. Hence $\mu(mn) = 0 = 0 \cdot \mu(n) = \mu(m)\mu(n)$.

Now suppose that $m, n \neq 1$, and that m and n are both square free. Then mn is square free. Let $m = p_1 p_2 \dots p_l$ and $n = q_1 q_2 \dots q_r$ for p_i, q_j distinct primes where $1 \leq i \leq l$ and $1 \leq j \leq r$. Then $mn = p_1 \dots p_l q_1 \dots q_r$. Hence $\mu(mn) = (-1)^{l+r} = (-1)^l (-1)^r = \mu(m)\mu(n)$. ∎

Proposition 2.2.11. *If $n > 1$, then*

$$\sum_{d|n} \mu(d) = 0$$

Proof. Let $n = p_1^{a_1} p_2^{a_2} \dots p_l^{a_l}$. Then

$$\begin{aligned}\sum_{d|n} \mu(d) &= \sum_{(e_1,e_2,\dots,e_l)} \mu(p_1^{e_1} p_2^{e_2} \dots p_l^{e_l}) \text{ where } e_i = 0, 1. \\ &= \sum_{(e_1,e_2,\dots,e_l)} \mu(p_1^{e_1})\mu(p_2^{e_2}) \dots \mu(p_l^{e_l}) \\ &= (-1)^1 + (-1)^2 + (-1)^3 \cdots + (-1)^l = (-1) + 1 + (-1) + \cdots + (-1)^l \\ &= 1 + (-1)^l = (1-1)^l = 0\end{aligned}$$

■

Definition. Let $f : \mathbb{Z}^+ \to \mathbb{C}$ and $g : \mathbb{Z}^+ \to \mathbb{C}$ be complex valued functions over $\mathbb{Z}^+$. We define the **Dirichlet product** of f and g to be $f \circ g(n) = \sum_{(d_1,d_2)} f(d_1)g(d_2)$, where $n = d_1 d_2$.

Lemma 2.2.12. *The Dirichlet product is associative.*

Proof. Let f, g, h be complex valued functions over $\mathbb{Z}^+$. Then $f \circ (g \circ h)(n) = f \circ \sum_{(d_2,d_3)} g(d_2)h(d_3) = \sum_{d_1} f(d_1) \sum_{(d_2,d_3)} g(d_2)h(d_3) = \sum_{(d_1,d_2,d_3)} f(d_1)g(d_2)h(d_3) = \sum_{(d_1,d_2)} f(d_1)g(d_2) \sum_{d_3} h(d_3) = (f \circ g) \circ h(n)$. ■

We now define the functions $\iota : \mathbb{Z}^+ \to \mathbb{Z}^+$ and $I : \mathbb{Z}^+ \to \mathbb{Z}^+$ to be $\iota(1) = 1$ and $\iota(n) = 0$ for $n > 1$; and $I(n) = 1$ for all $n \in \mathbb{Z}^+$. Then for some complex valued function $f : \mathbb{Z}^+ \to \mathbb{C}$, $f \circ \iota(n) = \iota \circ f(n)$, and $f \circ I(n) = I \circ f(n)$.

Lemma 2.2.13. $I \circ \mu = \iota$.

Lemma 2.2.14. *Let $n = 1$. Then $\iota \circ \mu(1) = I(1)\mu(1) = 1 = \iota$. Now let $n > 1$. Then $\mathbb{I} \circ \mu(n) = \sum_{(d_1,d_2)} I(d_1)\mu(d_2) = \sum_{d_2|n} \mu(d_2) = 0 = \iota(n)$.*

The Möbius Inversion Theorem. *Let $f : \mathbb{Z}^+ \to \mathbb{Z}$ and $F : \mathbb{Z}^+ \to \mathbb{Z}$ be l=multiplicative functions such that: $F(n) = \sum_{d|n} f(d)$. Then*

$$f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d}) = \sum_{d|n} F(\frac{n}{d})\mu(d). \tag{2.2}$$

Proof. We have thst $f \circ I(n) = \sum_{(d_1,d_2)} f(d_1)I(d_2) = \sum_{d_1} f(d_1)$. Hence $F = f \circ I = I \circ f$. Thus, $F \circ \mu = (f \circ I) \circ \mu = f \circ (I \circ \mu) = f \circ \iota = f$. Hence $f(n) = F \circ \mu(n) = \sum_{(d_1,d_2)} F(d_1)\mu(d_2)$. Now since $n = d_1 d_2$, we can take them to be perfect divisors. Hence letting $d_1 = d$, and $d_2 = \frac{n}{d}$, we get $f(n) = \sum_{d|n} F(d)\mu(\frac{n}{d})$; letting $d_1 = \frac{n}{d}$ and $d_2 = d$, we get $f(n) = \sum_{d|n} F(\frac{n}{d})\mu(d)$. ■

Definition. We define the **Euler ϕ function** to be the map $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ such that $\phi(1) = 1$, and $\phi(n)$ is the number of positive integers coprime to n, for $n > 1$.

Observing a little better the definition of ϕ, we can see that $\phi(n) = |\{a \in \mathbb{Z} : (a, n) = 1\}|$. We would like to use this notion when proving the multiplicity of ϕ.

Lemma 2.2.15. *ϕ is multiplicative.*

Proof. Let $m, n \in \mathbb{Z}^+$ such that $(m, n) = 1$. Firs notice that for any integer $a \in \mathbb{Z}^+$ if $(a, mn) = 1$, then for $\alpha, \beta \in \mathbb{Z}$, $a\alpha + mn\beta = a\alpha + m(n\beta) = a\alpha + n(m\beta) = 1$, so $(a, m) = 1$ and $(a, n) = 1$. Hence $\{a \in \mathbb{Z}^+ : (a, mn) = 1\} \subseteq \{a \in \mathbb{Z}^+ : (a, m) = 1 \text{ and } (a, n) = 1\}$. We also have that if $(a, m) = 1$ and $(a, n) = 1$, then clearly $(a, mn) = 1$ (this result is an easy exercise), and so $\{a \in \mathbb{Z}^+ : (a, m) = 1 \text{ and } (a, n) = 1\} \subseteq \{a \in \mathbb{Z}^+ : (a, m) = 1 \text{ and } (a, n) = 1\}$. Thus $\{a \in \mathbb{Z}^+ : (a, mn) = 1\} = \{a \in \mathbb{Z}^+ : (a, m) = 1 \text{ and } (a, n) = 1\}$.

Now, we have that $\phi(mn) = |\{a \in \mathbb{Z}^+ : (a, mn) = 1\}| = |\{a \in \mathbb{Z}^+ : (a, m) = 1 \text{ and } (a, n) = 1\}|$ (by our previous observation). Now Notice that there are $\phi(m)$ integers coprime to m and $\phi(n)$ integers coprime to n. Hence there are $\phi(m)\phi(n)$ integers coprime to both m and n. Hence $\phi(m)\phi(n) = |\{a \in \mathbb{Z}^+ : (a, m) = 1 \text{ and } (a, n) = 1\}|$. That is, $\phi(mn) = \phi(m)\phi(n)$. ■

Lemma 2.2.16. *Let $n = p^a$ with p prime and $a \in \mathbb{Z}^+$. Then $\phi(n) = p^a - p^{a-1} = p^a(1 - \frac{1}{p})$.*

Proof. Let $n = p^a$. We have that $\phi(p^a)$ is the number of integers coprime to p^a. Consider the divisors of p^a, $1, p, p^2, \ldots, p^a$. Now $(1, p^a) = 1$, but $(p^i, p^a) = p^i$ for all $1 \leq i \leq a$. Hence $p, p^2, \ldots, p^a$ are the only integers not coprime with p^a, and there are p^{a-1} of them. So we just take $\phi(p^a) = p^a - p^{a-1}$. ■

Proposition 2.2.17. *Let $n = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$. Then:*

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_l}) \tag{2.3}$$

Proof. Let $p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$. Then since p_i is prime for all $1 \leq i \leq l$, we have that $(p_i, p_j) = 1$ whenever $i \neq j$. Thus

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}) = \phi(p_1^{a_1})\phi(p_2^{a_2}) \ldots \phi(p_l^{a_l}) \\
&= p_1^{a_1}(1 - \frac{1}{p_1}) p_2^{a_2}(1 - \frac{1}{p_2}) \ldots p_l^{a_l}(1 - \frac{1}{p_l}) \\
&= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_l})
\end{aligned}$$

■

The Euler ϕ function will be of great importance later, so we will consider a last result.

Proposition 2.2.18. $\sum_{d|n} \phi(d) = n$

Proof. Consider the rational numbers $\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$. Reducing each to lowest terms, we will find that the denominators will be divisors of n. Now if $d|n$, since the fractions are in lowest terms, there are exactly $\phi(d)$ such denominator. Hence adding them up, we get that $\sum_d \phi(d) = n$. ■

Chapter 3

Congruence

3.1 Some Elementary Observations

Consider the equation $x^2 - 117x + 31 = 0$. We claim that there are no integer solutions to this equation. Let n be an integer , then n is either even or odd. If n is even, then so is n^2 and $17n$; hence $x^2 - 117x + 31$ is odd. Likewise if n is odd, then so is n^2 and $117n$, thus $x^2 - 117x + 31$ is even and so we see that $x^2 - 117x + 31$ is never 0.

3.2 Congruence in $\mathbb{Z}$

3.3 The Congruence $ax \equiv b \mod n$.

3.4 The Chinese Remainder Theorem

Bibliography