Mathematics Course 111: Algebra I
Part III: Rings, Polynomials and Number Theory

D. R. Wilkins

Academic Year 1996-7

7 Rings

Definition. A *ring* consists of a set R on which are defined operations of *addition* and *multiplication* satisfying the following axioms:

- $x + y = y + x$ for all elements x and y of R (i.e., addition is *commutative*);
- $(x + y) + z = x + (y + z)$ for all elements x, y and z of R (i.e., addition is *associative*);
- there exists an an element 0 of R (known as the *zero element*) with the property that $x + 0 = x$ for all elements x of R;
- given any element x of R, there exists an element $-x$ of R with the property that $x + (-x) = 0$;
- $x(yz) = (xy)z$ for all elements x, y and z of R (i.e., multiplication is *associative*);
- $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all elements x, y and z of R (the *Distributive Law*).

The first four of these axioms (the axioms that involve only the operation of addition) can be summarized in the statement that a ring is an Abelian group (i.e., a commutative group) with respect to the operation of addition.

Example. The set $\mathbb{Z}$ of integers is a ring with the usual operations of addition and multiplication.

Example. The set $\mathbb{Q}$ of rational numbers is a ring with the usual operations of addition and multiplication.

Example. The set $\mathbb{R}$ of real numbers is a ring with the usual operations of addition and multiplication.

Example. The set $\mathbb{C}$ of complex numbers is a ring with the usual operations of addition and multiplication.

Example. The set $\mathbb{Z}[x]$ of all polynomials with integer coefficients is a ring with the usual operations of addition and multiplication of polynomials.

Example. The set $\mathbb{Q}[x]$ of all polynomials with rational coefficients is a ring with the usual operations of addition and multiplication of polynomials.

Example. The set $\mathbb{R}[x]$ of all polynomials with real coefficients is a ring with the usual operations of addition and multiplication of polynomials.

Example. The set $\mathbb{C}[x]$ of all polynomials with complex coefficients is a ring with the usual operations of addition and multiplication of polynomials.

Example. Given a positive integer n, the set of all $n \times n$ matrices with real coefficients is a ring with operations of matrix addition and matrix multiplication.

Example. Given a positive integer n, the set of all $n \times n$ matrices with complex coefficients is a ring with operations of matrix addition and matrix multiplication.

Example. Let n be a positive integer. We construct the ring $\mathbb{Z}_n$ of *congruence classes of integers* modulo n. Two integers x and y are said to be *congruent* modulo n if and only if $x - y$ is divisible by n. The notation '$x \equiv y \bmod n$' is used to denote the congruence of integers x and y modulo n. One can readily verify that congruence modulo the given integer n is an equivalence relation on the set $\mathbb{Z}$ of all integers: $x \equiv x \bmod n$ for all integers x (the relation is reflexive); if $x \equiv y \bmod n$ then $y \equiv x \bmod n$ (the relation is symmetric); if $x \equiv y \bmod n$ and $y \equiv z \bmod n$ then $x \equiv z \bmod n$ (the relation is transitive). The equivalence classes of integers with respect to congruence modulo n are referred to as *congruence classes* modulo n: two integers x and y belong to the same congruence class modulo n if and only if $x - y$ is divisible by n. The set of congruence classes of integers modulo n is denoted by $\mathbb{Z}_n$; this set has n elements which are the congruence classes of the integers $0, 1, \ldots, n-1$.

Let x, y, u and v be integers, where $x \equiv u \bmod n$ and $y \equiv v \bmod n$. Then $x - u$ and $y - v$ are divisible by n. It follows directly from this that $(x + y) - (u + v)$ is divisible by n and thus $x + y \equiv u + v \bmod n$. Also $xy - uv = (x-u)y + u(y-v)$, from which it follows that $xy - uv$ is divisible by n and thus $xy \equiv uv \bmod n$. We conclude that there are well-defined operations of addition and multiplication on the set $\mathbb{Z}_n$ of congruence classes of integers modulo n: the sum of the congruence classes of integers x and y is the congruence class of $x + y$, and the product of these congruence classes is the congruence class of xy. These operations of addition and multiplication on congruence classes do not depend on the choice of representatives of those congruence classes: if x and u belong to the same congruence class and if y and v belong to the same congruence class, then we have shown that $x + y$ and $u + v$ belong to the same congruence class; we have also shown that xy and uv belong to the same congruence class. It is now a straightforward exercise to verify that the ring axioms are satisfied by addition and multiplication on $\mathbb{Z}_n$. Thus the set $\mathbb{Z}_n$ of congruence classes of integers modulo n is a ring with respect to the operations of addition and multiplication of congruence classes.

Example. A *quaternion* is an expression of the form $a + xi + yj + zk$, where a, x, y and z are real numbers. Addition and multiplication of quaternions are defined by the following formulae:

$$\begin{aligned}(a + xi + yj + zk) + (b + ui + vj + wk) &= (a + b) + (x + u)i + (y + v)j + (z + w)k \\ (a + xi + yj + zk)(b + ui + vj + wk) &= (ab - xu - yv - zw) + (au + xb + yw - zv)i \\ &\quad + (av + yb + zu - xw)j + (aw + zb + xv - yu)k\end{aligned}$$

Straightforward calculations establish that the set of quaternions is a ring with respect to these operations of addition and multiplication. This ring is non-commutative (i.e., the commutative law is not satisfied in general when quaternions are multiplied together.) One can readily verify that

$$i^2 = j^2 = k^2 = ijk = -1.$$

This formula was discovered by Hamilton on the 16th of October, 1843, and carved by him on a stone of Broome Bridge, Cabra. One can also verify that

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

There are close connections between quaternion algebra and the algebra of vectors in 3-dimensional space: the components x, y and z of i, j and k respectively in the quaternion $a + xi + yj + zk$ can be thought of as the three components of a vector (x, y, z) in 3-dimensional space, and the formula for quaternion multiplication can be expressed using the scalar product and vector product of 3-dimensional vector algebra. Quaternions are used today for algebraic computations involving rotations in three-dimensional space.

Lemma 7.1. *Let a and b be elements of a ring R. Then there exists a unique element x of R satisfying $x + b = a$.*

Proof. The ring axioms ensure the existence of an element $-b$ of R with the property that $b+(-b) = 0$, where 0 is the zero element of R. The identity $x + b = a$ is satisfied when $x = a + (-b)$, since

$$(a + (-b)) + b = a + ((-b) + b) = a + (b + (-b)) = a + 0 = a.$$

(Here we have used the fact that addition is required to be both commutative and associative.) If now x is any element of R satisfying $x + b = a$ then

$$x = x + 0 = x + (b + (-b)) = (x + b) + (-b) = a + (-b).$$

This proves that there is exactly one element x of R satisfying $x+b = a$, and it is given by the formula $x = a + (-b)$. ∎

Let a and b be elements of a ring R. We denote by $a - b$ the unique element x of R with the property satisfying $x + b = a$. Note that $a - b = a + (-b)$ for all elements a and b of R. This defines the operation of *subtraction* on any ring.

If x is an element of a ring R and if there exists at least one element b for which $b + x = b$ then Lemma 7.1 ensures that $x = 0$. It follows immediately from this that the zero element of a ring is uniquely determined.

Lemma 7.1 also ensures that, given any element b of a ring R there exists exactly one element $-b$ of R with the property that $b + (-b) = 0$.

Lemma 7.2. *Let R be a ring. Then $x0 = 0$ and $0x = 0$ for all elements x of R.*

Proof. The zero element 0 of R satisfies $0 + 0 = 0$. Therefore

$$x0 + x0 = x(0 + 0) = x0 \text{ and } 0x + 0x = (0 + 0)x = 0x$$

for any element x of R. The elements $x0$ and 0 of R must therefore be equal to one another, since both are equal to the unique element y of R that satisfies $y + x0 = x0$. Similarly the elements $0x$ and 0 of R must therefore be equal to one another, since both are equal to the unique element z of R that satisfies $z + 0x = 0x$. ∎

Lemma 7.3. *Let R be a ring. Then $(-x)y = -(xy)$ and $x(-y) = -(xy)$ for all elements x and y of R.*

Proof. It follows from the Distributive Law that $(-x)y = -(xy)$, since $xy + (-x)y = (x + (-x))y = 0y = 0$.

Similarly $x(-y) = -(xy)$, since $xy + x(-y) = x(y + (-y)) = x0 = 0$. ∎

Ideals and Quotient Rings

Definition. A subset I of a ring R is said to be an *ideal* if the following conditions are satisfied:

$0 \in I$;

$x + y \in I$ for all $x \in I$ and $y \in I$;

$-x \in I$ for all $x \in I$;

$rx \in I$ and $xr \in I$ for all $x \in I$ and $r \in R$.

The *zero ideal* of any ring is the ideal that consists of just the zero element.

Note that any ideal of a ring is a subgroup of that ring with respect to the operation of addition.

Ideals play a role in ring theory analogous to the role of normal subgroups in group theory.

Example. Let $\mathbb{Z}$ be the ring of integers and, for any non-negative integer n, let $n\mathbb{Z}$ be the subset of $\mathbb{Z}$ consisting of those integers that are multiples of n. Then $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proposition 7.4. *Every ideal of the ring $\mathbb{Z}$ of integers is generated by some non-negative integer n.*

Proof. The zero ideal is of the required form with $n = 0$. Let I be some non-zero ideal of $\mathbb{Z}$. Then I contains at least one strictly positive integer (since $-m \in I$ for all $m \in I$). Let n be the smallest strictly positive integer belonging to I. If $j \in I$ then we can write $j = kn + q$ for some integers k and q with $0 \leq q < n$. Now $q \in I$, since $q = j - kn$, $j \in I$ and $kn \in I$. But $0 \leq q < n$, and n is by definition the smallest strictly positive integer belonging to I. We conclude therefore that $q = 0$, and thus $j = kn$. This shows that $I = n\mathbb{Z}$, as required. ∎

Lemma 7.5. *The intersection of any collection of ideals of a ring R is itself an ideal of R.*

Proof. Let x and y be elements of R. Suppose that x and y belong to all the ideals in the collection. Then the same is true of 0, $x + y$, $-x$, rx and xr for all $r \in R$. ∎

Definition. Let X be a subset of the ring R. The ideal of R *generated* by X is defined to be the intersection of all the ideals of R that contain the set X.

Note that the ideal of a ring R generated by a subset X of R is contained in every other ideal that contains the subset X.

Let R be a ring. We denote by $(f_1, f_2, \ldots, f_k)$ the ideal of R generated by any finite subset $\{f_1, f_2, \ldots, f_k\}$ of R.

An ideal I of the ring R is said to be *finitely generated* if there exists a finite subset of I which generates the ideal I.

Let I be an ideal of a ring R. We construct a corresponding *quotient ring* R/I.

Two elements x and y of R belong to the same coset of I if and only if $x - y \in I$. Let $\sim_I$ be the binary relation of R where elements x and y of R satisfy $x \sim_I y$ if and only if they belong to the same coset of I. One can readily verify that $\sim_I$ is an equivalence relation on R: $x \sim_I x$ for all elements x of R (the relation is reflexive); if $x \sim_I y$ then $y \sim_I x$ (the relation is symmetric); if $x \sim_I y$ and $y \sim_I z$ then $x \sim_I z$ (the relation is transitive).

Let x, y, u and v be elements of R, where $x \sim_I u$ and $y \sim_I v$. Then $x - u \in I$ and $y - v \in I$. It follows directly from this that $(x+y)-(u+v) \in I$, since $(x+y)-(u+v) = (x-u)+(y-v)$ and the sum of two elements of an ideal I belongs to I. Thus $x+y \sim_I u+v$. Also $xy-uv = (x-u)y+u(y-v)$. But $(x-u)y \in I$ and $u(y-v) \in I$ since a product of an element of I with an element of R (in any

order) must belong to the ideal I. Using the fact that a sum of two elements of an ideal belongs to that ideal, we see that $xy - uv \in I$ and thus $xy \sim_I uv$. We conclude that there are well-defined operations of addition and multiplication on the set R/I of cosets of I: the sum of the cosets containing the elements x and y of R is the coset containing $x + y$, and the product of these cosets is the coset containing xy. These operations of addition and multiplication on cosets do not depend on the choice of representatives of those cosets: if x and u belong to the same coset and if y and v belong to the same coset, then we have shown that $x + y$ and $u + v$ belong to the same coset; we have also shown that xy and uv belong to the same coset. It is now a straightforward exercise to verify that the ring axioms are satisfied by addition and multiplication on R/I. Thus the set R/I of cosets of elements of R is a ring with respect to the operations of addition and multiplication of cosets.

The coset of I in R containing an element x is denotes by $I + x$. The operations of addition and multiplication of cosets satisfy

$$(I + x) + (I + y) = I + (x + y), \qquad (I + x)(I + y) = I + xy$$

for all elements x and y of R. The zero element of R/I is the ideal I itself. (Any ideal I is a coset of itself, and $I = I + 0$.) Note that $I + (-x)$ is the additive inverse of the coset $I + x$ for any element x of R.

Example. Let $\mathbb{Z}$ be the ring of integers, let n be a positive integer, and let $n\mathbb{Z}$ be the ideal of $\mathbb{Z}$ consisting of all integers that are divisible by n. Then the quotient ring $\mathbb{Z}/n\mathbb{Z}$ can be identified with the ring $\mathbb{Z}_n$ of congruence classes of integers modulo n: given any integer x, the coset $n\mathbb{Z} + x$ is the congruence class of x modulo n.

Homomorphisms

Definition. A function $\theta: R \to S$ from a ring R to a ring S is said to be a *homomorphism* (or *ring homomorphism*) if and only if $\theta(x + y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in R$.

Example. The function that sends a complex number to its complex conjugate is a homomorphism from the ring $\mathbb{C}$ of complex numbers to itself.

Example. The function that sends each polynomial $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ with complex coefficients to the polynomial $\overline{a}_0 + \overline{a}_1x + \overline{a}_2x^2 + \cdots + \overline{a}_nx^n$, where $\overline{a}_i$ is the complex conjugate of a_i for each i, is a homomorphism from the ring $\mathbb{C}[x]$ of polynomials with complex coefficients to itself.

Example. Let c be an integer. The function that sends each polynomial $f(x)$ with integer coefficients to its value $f(c)$ at c is a homomorphism from the ring $\mathbb{Z}[x]$ of polynomials with integer coefficients to the ring $\mathbb{Z}$ of integers.

Example. One can verify by straightforward calculations that the function

$$a + xi + yj + zk \mapsto \begin{pmatrix} a + iz & x + iy \\ -x + iy & a - iz \end{pmatrix}$$

that sends each quaternion $a + xi + yj + xk$ to a corresponding 2×2 matrix is a homomorphism from the ring of quaternions to the ring of all 2×2 matrices of complex numbers.

Lemma 7.6. *Let $\theta: R \to S$ be a homomorphism from a ring R to a ring S. Then $\theta(0) = 0$ (where 0 denotes the zero element in the ring R and also in the ring S). Also $\theta(-x) = -\theta(x)$ for all elements x of R.*

Proof. Let $z = \theta(0)$. Then $z + z = \theta(0) + \theta(0) = \theta(0 + 0) = \theta(0) = z$. The result that $\theta(0) = 0$ now follows from the fact that an element z of S satisfies $z + z = z$ if and only if z is the zero element of S.

Let x be an element of R. The element $\theta(-x)$ satisfies $\theta(x) + \theta(-x) = \theta(x + (-x)) = \theta(0) = 0$. The result now follows using Lemma 7.1. ∎

Definition. Let R and S be rings, and let $\theta: R \to S$ be a ring homomorphism. The *kernel* $\ker\theta$ of the homomorphism θ is the set $\{x \in R : \theta(x) = 0\}$ of all elements of R that are mapped by θ onto the zero element of S.

Lemma 7.7. *Let $\theta: R \to S$ be a homomorphism from a ring R to a ring S. Then the kernel $\ker\theta$ of θ is an ideal of R.*

Proof. Let x and y be elements of $\ker\theta$, and let r be an element of R. Then

$$\begin{aligned} \theta(0) &= 0, \\ \theta(x+y) &= \theta(x) + \theta(y) = 0, \\ \theta(-x) &= -\theta(x) = 0, \\ \theta(rx) &= \theta(r)\theta(x) = \theta(r)0 = 0, \\ \theta(xr) &= \theta(x)\theta(r) = 0\theta(r) = 0. \end{aligned}$$

It follows that 0, $x+y$, $-x$, rx and xr are elements of $\ker\theta$. Thus $\ker\theta$ is an ideal of R, as required. ∎

The image $\theta(R)$ of a ring homomorphism $\theta: R \to S$ is a subring of S; however it is not in general an ideal of S.

An ideal I of a ring R is the kernel of the quotient homomorphism that sends $x \in R$ to the coset $I + x$.

Definition. An isomorphism $\theta: R \to S$ between rings R and S is a homomorphism that is also a bijection between R and S. The inverse of an isomorphism is itself an isomorphism. Two rings are said to be *isomorphic* if there is an isomorphism between them.

Example. The function that sends a complex number to its conjugate is an isomorphism from the ring $\mathbb{C}$ of complex numbers to itself.

Proposition 7.8. *Let R and S be rings, let $\theta: R \to S$ be a homomorphism from R to S, and let I be a ideal of R. Suppose that $I \subset \ker\theta$. Then the homomorphism $\theta: R \to S$ induces a homomorphism $\hat{\theta}: R/I \to S$ sending $I + g \in R/I$ to $\theta(g)$. Moreover $\hat{\theta}: R/I \to S$ is injective if and only if $I = \ker\theta$.*

Proof. Let x and y be elements of R. Now $I + x = I + y$ if and only if $x - y \in I$. Also $\theta(x) = \theta(y)$ if and only if $x - y \in \ker\theta$. Thus if $I \subset \ker\theta$ then $\theta(x) = \theta(y)$ whenever $I + x = I + y$, and thus $\theta: R \to S$ induces a well-defined function $\hat{\theta}: R/I \to S$ sending $I + x \in R/I$ to $\theta(x)$. This function is a homomorphism since

$$\begin{aligned} \hat{\theta}((I+x)+(I+y)) &= \hat{\theta}(I+(x+y)) = \theta(x+y) = \theta(x) + \theta(y) = \hat{\theta}(I+x) + \hat{\theta}(I+y), \\ \hat{\theta}((I+x)(I+y)) &= \hat{\theta}(I+xy) = \theta(xy) = \theta(x)\theta(y) = \hat{\theta}(I+x)\hat{\theta}(I+y). \end{aligned}$$

Suppose now that $I = \ker\theta$. Then $\theta(x) = \theta(y)$ if and only if $I+x = I+y$. Thus the homomorphism $\hat{\theta}: R/I \to S$ is injective. Conversely if $\hat{\theta}: R/I \to S$ is injective then I must be the kernel of θ, as required. ∎

Corollary 7.9. *Let $\theta: R \to S$ be ring homomorphism. Then $\theta(R)$ is isomorphic to $R/\ker\theta$.*

Example. Let n be a non-negative integer. The function from the ring $\mathbb{Z}$ of integers to the ring $\mathbb{Z}_n$ of congruence classes of integers modulo n is a homomorphism whose kernel is the ideal $n\mathbb{Z}$ consisting of those integers which are multiples of n. This homomophism is surjective. It follows therefore that $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Example. The function $\theta: \mathbb{Z}_4 \to \mathbb{Z}_2$ that sends the congruence class of each integer x modulo 4 to the congruence class of x modulo 2 is a well-defined homomorphism. Its kernel is the ideal I of $\mathbb{Z}_4$ consisting of congrence classes of even integers modulo 4. This homomorphism is surjective. It follows therefore that $\mathbb{Z}_4/I \cong \mathbb{Z}_2$.

Unital Rings, Commutative Rings, and Integral Domains

A ring R is said to be *commutative* if $xy = yx$ for all $x, y \in R$. Not every ring is commutative: an example of a non-commutative ring is provided by the ring of $n \times n$ matrices with real or complex coefficients when $n > 1$.

A ring R is said to be *unital* if it possesses a (necessarily unique) non-zero multiplicative identity element 1 satisfying $1x = x = x1$ for all $x \in R$.

Lemma 7.10. *Let R be a unital commutative ring, and let X be a subset of R. Then the ideal generated by X coincides with the set of all elements of R that can be expressed as a finite sum of the form $r_1x_1 + r_2x_2 + \cdots + r_kx_k$, where $x_1, x_2, \ldots, x_k \in X$ and $r_1, r_2, \ldots, r_k \in R$.*

Proof. Let I be the subset of R consisting of all these finite sums. If J is any ideal of R which contains the set X then J must contain each of these finite sums, and thus $I \subset J$. Let a and b be elements of I. It follows immediately from the definition of I that $a + b \in I$, $-a \in I$, and $ra \in I$ for all $r \in R$. Also $ar = ra$, since R is commutative, and thus $ar \in I$. Thus I is an ideal of R. Moreover $X \subset I$, since the ring R is unital and $x = 1x$ for all $x \in X$. Thus I is the smallest ideal of R containing the set X, as required. ∎

Definition. A unital commutative ring R is said to be an *integral domain* if the product of any two non-zero elements of R is itself non-zero.

A non-zero element x of a unital commutative ring R is said to be a *zero divisor* if there exists some non-zero element y for which $xy = 0$. An integral domain is a unital commutative ring without zero divisors.

Example. There are no zero divisors in the ring $\mathbb{Z}_3$ of congruence classes of integers modulo 3. The non-zero elements of $\mathbb{Z}_3$ are the congruence classes [1] and [2] of the integers 1 and 2 respectively, and these satisfy $[1][1] = [2][2] = [1]$ and $[1][2] = [2][1] = [2]$. Thus the unital commutative ring $\mathbb{Z}_3$ is an integral domain.

Example. The congruence class [2] of 2 modulo 4 is a zero divisor in the ring $\mathbb{Z}_4$ of congruence classes of integers modulo 4, since $[2][2] = [4] = [0]$. Thus $\mathbb{Z}_4$ is not an integral domain.

We shall show that the ring $\mathbb{Z}_n$ of congruence classes of integers modulo some given integer n satisfying $n > 1$ is an integral domain if and only if n is a prime number. We recall that an integer p satisfying $p > 1$ is a prime number if and only if there do not exist integers r and s satisfying $rs = p$, $0 < r < p$ and $0 < s < p$.

Lemma 7.11. *Let p be a prime number, and let r and s be integers satisfying $0 < r < p$ and $0 < s < p$. Then rs is not divisible by p.*

Proof. Let I be the set of all integers x with the property that rx is divisible by p. Then I is an ideal of the ring $\mathbb{Z}$ of integers. It follows from Proposition 7.4 that there exists some non-negative integer d such that $I = d\mathbb{Z}$, where $d\mathbb{Z}$ is the set of all integer multiples of d. Now $p \in I$, since rp is obviously divisible by p. It follows that $d > 0$ and d divides p. Also $d > 1$, for if it were the case that $d = 1$ then r would be divisible by p, contradicting the requirement that $0 < r < p$. Now, since the divisor d of the prime number p cannot satisfy $1 < d < p$, we conclude that $d = p$, and thus the ideal I consists of all integer multiples of p. It follows that s cannot belong to I, since $0 < s < p$, and therefore rs is not divisible by p, as required. ∎

Theorem 7.12. *Let n be an integer satisfying $n > 1$. The ring $\mathbb{Z}_n$ of congruence classes of integers modulo n is an integral domain if and only if n is a prime number.*

Proof. First we show that $\mathbb{Z}_n$ is an integral domain only if n is a prime number. Suppose that n is not a prime number. Then $n = rs$, where r and s are integers satisfying $0 < r < n$ and $0 < s < n$. Let $[r]$ and $[s]$ denote the congruence classes of r and s modulo n. Then $[r]$ and $[s]$ are non-zero elements of $\mathbb{Z}_n$, and $[r][s] = [rs] = [n] = [0]$. It follows that if n is not a prime number then $\mathbb{Z}_n$ is not an integral domain.

We must show also that if n is a prime number then $\mathbb{Z}_n$ is an integral domain. Let α and β be elements of $\mathbb{Z}_n$. If $\alpha \neq [0]$ and $\beta \neq [0]$ then there exist integers r and s satisfying $0 < r < n$ and $0 < s < n$ such that $\alpha = [r]$ and $\beta = [s]$. It follows from Lemma 7.11 that rs is not divisible by p, and thus $\alpha\beta = [r][s] = [rs] \neq [0]$. We have thus shown that if n is a prime number then the product of any two non-zero elements of $\mathbb{Z}_n$ is non-zero. We conclude that if n is a prime number then $\mathbb{Z}_n$ is an integral domain, as required. ∎

Let R be a ring, and let $r \in R$. We may define $n.r$ for all natural numbers n by induction on $|n|$ so that $0.r = 0$, $n.r = (n-1).r + r$ for all $n > 0$, and $n.r = -((-n).r)$ for all $n < 0$. Then

$$(m+n).r = m.r + n.r, \qquad n.(r+s) = n.r + n.s,$$

$$(mn).r = m.(n.r), \qquad (m.r)(n.s) = (mn).(rs)$$

for all $m, n \in \mathbb{Z}$ and $r, s \in R$.

In particular, suppose that R is a unital ring. Then the set of all integers n satisfying $n.1 = 0$ is an ideal of $\mathbb{Z}$. Therefore there exists a unique non-negative integer p such that $p\mathbb{Z} = \{n \in \mathbb{Z} : n.1 = 0\}$ (see Proposition 7.4). This integer p is referred to as the *characteristic* of the ring R, and is denoted by $\mathrm{char}R$.

Lemma 7.13. *Let R be an integral domain. Then either* $\mathrm{char}R = 0$ *or else* $\mathrm{char}R$ *is a prime number.*

Proof. Let $p = \mathrm{char}R$. If $p \neq 0$ then $p > 1$, since the characteristic of a unital ring cannot be equal to 1. Let j and k be integers satisfying $0 < j < p$ and $0 < k < p$. Then $j.1$ and $k.1$ are are non-zero elements of R. It follows that $(j.1)(k.1)$ must be a non-zero element of R, since R is an integral domain. But $(j.1)(k.1) = (jk).1$. It follows that $jk \notin p\mathbb{Z}$, and thus jk is not equal to p. We conclude that p is a prime number, as required. ∎

Fields

Definition. A unital commutative ring R is said to be a *field* if, given any non-zero element x of R, there exists an element y of R such that $xy = 1$.

The following result follows immediately from the above definition.

Proposition 7.14. *A ring R is a field if and only if the non-zero elements of R constitute an Abelian group with respect to the operation of multiplication.*

The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of rational numbers, real numbers and complex numbers are fields.

Theorem 7.15. *A unital commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R.*

Proof. Suppose that R is a field. Let I be a non-zero ideal of R. Then there exists $x \in I$ satisfying $x \neq 0$. Moreover there exists $y \in R$ satisfying $xy = 1$. Therefore $1 \in I$. But then $r \in I$ for all $r \in R$, since $r = r1$. Thus if I is a non-zero ideal of R then $I = R$. This shows that of a field R are $\{0\}$ and R.

Conversely, suppose that R is a unital commutative ring with the property that the only ideals of R are $\{0\}$ and R. Let x be a non-zero element of R, and let xR denote the subset of R consisting of all elements of R that are of the form xr for some $r \in R$. Given that the ring R is commutative, it is easy to verify that xR is an ideal of R. Moreover $xR \neq \{0\}$, since $x \in xR$. We deduce that $xR = R$. Therefore $1 \in xR$, and hence there exists some element y of R satisfying $xy = 1$. This shows that R is a field. ∎

Every field is an integral domain. The converse is true for finite integral domains.

Theorem 7.16. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain, and let x be a non-zero element of R. We must show that there exists $y \in R$ satisfying $xy = 1$. Consider the function $\varphi: R \to R$ defined by $\varphi(r) = xr$. If r and s are elements of R satisfying $\varphi(r) = \varphi(s)$ then $xr = xs$, and hence $x(r - s) = 0$. But $x \neq 0$. It follows from the definition of integral domains that $r - s = 0$. Thus $r = s$. This shows that the function $\varphi: R \to R$ is injective. But R is finite. The function $\varphi: R \to R$ must therefore be surjective. Thus there exists $y \in R$ satisfying $\varphi(y) = 1$. Then $xy = 1$, as required. ∎

Example. The ring $\mathbb{Z}_n$ of congruence classes of integers modulo a given integer n greater than one is a field if and only if n is a prime number. This result follows directly from Theorem 7.12 and Theorem 7.16.

Polynomial Rings

Let R be a ring. A *polynomial* (in an *indeterminate* x) with coefficients in the ring R is an expression $f(x)$ of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m,$$

where a_k is an element of R for $i = 0, 1, 2, \ldots, m$. If $a_k = 0$ then the term $a_k x^k$ may be omitted when writing down the expression defining the polynomial. (Thus for example the polynomial $1 + 0x + 2x^2$ may be written as $1 + 2x^2$.) The elements a_k of R that determine the polynomial are referred to as *coefficients* of the polynomial. If $a_m \neq 0$, and if the polynomial contains no terms of the form $a_k x^k$

with $k > m$ and $a_k \neq 0$, then the non-negative integer m is referred to as the *degree* of the polynomial, and the coefficient a_m is referred to as the *leading coefficient* of the polynomial.

A polynomial determines and is determined by an infinite sequence $a_0, a_1, a_2, \ldots$ of elements of the ring R, where a_k is the coefficient of x^k in the polynomial. An infinite sequence $a_0, a_1, a_2, \ldots$ of elements of R determines a polynomial $a_0 + a_1x + a_2x^2 + \cdots$ if and only if the number of values of k for which $a_k \neq 0$ is finite. If the polynomial is non-zero then its degree is the largest value of m for which $a_m \neq 0$.

One can add and multiply polynomials in the usual fashion. Thus if

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m$$

and

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$$

then

$$f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_p + b_p)x^p,$$

where p is the maximum of m and n, and where $a_i = 0$ if $i > m$ and $b_i = 0$ if $i > n$. Also

$$f(x)g(x) = u_0 + u_1x + u_2x^2 + \cdots + u_{m+n}x^{m+n},$$

where, for each integer i between 0 and $m + n$, the coefficient u_i of x^i in $f(x)g(x)$ is the sum of those products a_jb_k for which $0 \leq j \leq m$, $0 \leq k \leq n$ and $j + k = i$. Straightforward calculations show that the set $R[x]$ of polynomials with coefficients in a ring R is itself a ring with these operations of addition and multiplication. The zero element of this ring is of course the polynomial whose coefficients are all equal to zero.

We obtain in this way rings $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$ of polynomials with coefficients in the rings of integers, rational numbers, real numbers and complex numbers respectively.

We now consider various properties of polynomials whose coefficients belong to a *field* K (such as the field of rational numbers, real numbers or complex mumbers).

Lemma 7.17. *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial with coefficients in K. Then, given any polynomial $h \in K[x]$, there exist unique polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$.*

Proof. If $\deg h < \deg f$ then we may take $q = 0$ and $r = h$. In general we prove the existence of q and r by induction on the degree $\deg h$ of h. Thus suppose that $\deg h \geq \deg f$ and that any polynomial of degree less than $\deg h$ can be expressed in the required form. Now there is some element c of K for which the polynomials $h(x)$ and $cf(x)$ have the same leading coefficient. Let $h_1(x) = h(x) - cx^m f(x)$, where $m = \deg h - \deg f$. Then either $h_1 = 0$ or $\deg h_1 < \deg h$. The inductive hypothesis then ensures the existence of polynomials q_1 and r such that $h_1 = fq_1 + r$ and either $r = 0$ or else $\deg r < \deg f$. But then $h = fq + r$, where $q(x) = cx^m + q_1(x)$. We now verify the uniqueness of q and r. Suppose that $fq + r = f\overline{q} + \overline{r}$, where $\overline{q}, \overline{r} \in K[x]$ and either $\overline{r} = 0$ or $\deg \overline{r} < \deg f$. Then $(q - \overline{q})f = r - \overline{r}$. But $\deg((q - \overline{q})f) \geq \deg f$ whenever $q \neq \overline{q}$, and $\deg(r - \overline{r}) < \deg f$ whenever $r \neq \overline{r}$. Therefore the equality $(q - \overline{q})f = r - \overline{r}$ cannot hold unless $q = \overline{q}$ and $r = \overline{r}$. This proves the uniqueness of q and r. ∎

Any polynomial f with coefficients in a field K generates an ideal (f) of the polynomial ring $K[x]$ consisting of all polynomials in $K[x]$ that are divisible by f.

Lemma 7.18. *Let K be a field, and let I be an ideal of the polynomial ring $K[x]$. Then there exists $f \in K[x]$ such that $I = (f)$, where (f) denotes the ideal of $K[x]$ generated by f.*

Proof. If $I = \{0\}$ then we can take $f = 0$. Otherwise choose $f \in I$ such that $f \neq 0$ and the degree of f does not exceed the degree of any non-zero polynomial in I. Then, for each $h \in I$, there exist polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$. (Lemma 7.17). But $r \in I$, since $r = h - fq$ and h and f both belong to I. The choice of f then ensures that $r = 0$ and $h = qf$. Thus $I = (f)$. ∎

Definition. Polynomials $f_1, f_2, \ldots, f_k$ with coefficients in some field K. are said to be *coprime* if there is no non-constant polynomial that divides all of them.

Theorem 7.19. *Let $f_1, f_2, \ldots, f_k$ be coprime polynomials with coefficients in some field K. Then there exist polynomials $g_1, g_2, \ldots, g_k$ with coefficients in K such that*

$$f_1(x)g_1(x) + f_2(x)g_2(x) + \cdots + f_k(x)g_k(x) = 1.$$

Proof. Let I be the ideal in $K[x]$ generated by $f_1, f_2, \ldots, f_k$. It follows from Lemma 7.18 that the ideal I is generated by some polynomial d. Then d divides all of $f_1, f_2, \ldots, f_k$ and is therefore a constant polynomial, since these polynomials are coprime. It follows that $I = K[x]$. The existence of the required polynomials $g_1, g_2, \ldots, g_k$ then follows using Lemma 7.10. ∎

Definition. A non-constant polynomial f with coefficients in a ring K is said to be *irreducible* over K if there does not exist any non-constant polynomial that divides f whose degree is less than that of f.

Proposition 7.20. *Let f, g and h be polynomials with coefficients in some field K. Suppose that f is irreducible over K and that f divides the product gh. Then either f divides g or else f divides h.*

Proof. Suppose that f does not divide g. We must show that f divides h. Now the only polynomials that divide f are constant polynomials and multiples of f. No multiple of f divides g. Therefore the only polynomials that divide both f and g are constant polynomials. Thus f and g are coprime. It follows from Proposition 7.19 that there exist polynomials u and v with coefficients in K such that $1 = ug + vf$. Then $h = ugh + vfh$. But f divides $ugh + vfh$, since f divides gh. It follows that f divides h, as required. ∎

8 Introduction to the Theory of Numbers

Greatest Common Divisors and the Euclidean Algorithm

Definition. Let $x_1, x_2, \ldots, x_k$ be integers that are not all zero. A positive integer d is said to be the *greatest common divisor* (or *highest common factor*) of $x_1, x_2, \ldots, x_k$ if the following conditions are satisfied:

- d divides each of $x_1, x_2, \ldots, x_k$;
- if e is any positive integer that divides each of $x_1, x_2, \ldots, x_k$ then e divides d.

Note that a positive integer d is the greatest common divisor of integers x and y if and only if it is the greatest common divisor of $|x|$ and $|y|$. This follows from the fact that a positive integer divides an integer x if and only if it divides $|x|$. If $y = 0$ then the greatest common divisor of x and y is clearly $|x|$.

We now describe a well-known algorithm, known as the *Euclidean algorithm* for computing the highest common divisor of two positive integers. The case where the two numbers are equal is of course trivial.

Let a_0 and a_1 be positive integers, where $a_0 > a_1$. We wish to compute the greatest common divisor of a_0 and a_1. If a_1 divides a_0 then a_1 is the greatest common divisor. Otherwise there exist positive integers q_1 and a_2 such that $0 < a_2 < a_1$ and $a_0 = q_1 a_1 + a_2$. If a_2 divides a_1 then a_2 divides both a_0 and a_1, and one can easily verify that a_2 is the greatest common divisor of a_0 and a_1. Otherwise there exist positive integers q_2 and a_3 such that $0 < a_3 < a_2$ and $a_1 = q_2 a_2 + a_3$. Continuing in this fashion, we construct positive integers $q_1, q_2, \ldots, q_{n-1}$ and $a_2, a_3, \ldots, a_n$ such that $0 < a_i < a_{i-1}$ for all i, $a_{i-2} = q_{i-1}a_{i-1} + a_i$ whenever $2 \leq i < n$, and $a_{n-1} = q_n a_n$. Note that the process of constructing the integers $a_2, a_3, \ldots, a_n$ must terminate after a finite number of steps, since $0 < a_n < a_{n-1} < \cdots < a_2 < a_1 < a_0$. Let $d = a_n$. We claim that d is the greatest common divisor of a_0 and a_1.

Now d divides both a_{n-1} and a_n, since $a_{n-1} = q_n a_n$ for some positive integer q_n. Also the identity $a_{i-2} = q_{i-1}a_{i-1} + a_i$ ensures that if d divides a_{i-1} and a_i for some i then d divides a_{i-2}. Repeated use of this result shows that d divides a_i for all i. In particular d divides a_0 and a_1.

Now let e be any positive integer which divides both a_0 and a_1. Successive applications of the identity $a_i = a_{i-2} - q_{i-1}a_{i-1}$ ensure that e divides $a_2, a_3, \ldots, a_n$. In particular e must divide d. We conclude therefore that d is the greatest common divisor of a_0 and a_1.

Finally we note that, for each integer i between 0 and n there exist integers u_i and v_i such that $a_i = u_i a_0 + v_i a_1$. We take $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ and $v_1 = 1$. When $i > 1$, u_i and v_i are determined from u_{i-2}, v_{i-2} and u_{i-1} and v_{i-1} by the formulae $u_i = u_{u-2} - q_{i-1}u_{u-1}$ and $v_i = v_{u-2} - q_{i-1}v_{u-1}$, since $a_i = a_{i-2} - q_{i-1}a_{i-1}$. In particular, we see that $d = ua_0 + va_1$, where $u = u_n$ and $v = v_n$. The Euclidean algorithm thus guarantees that if d is the greatest common divisor of two integers x and y, where x and y are not both zero, then there exist integers u and v such that $d = ux + vy$.

Example. We use the Euclidean algorithm to calculate the greatest common divisor of the numbers 272 and 119. Now

$$\begin{aligned} 272 &= 2 \times 119 + 34, \\ 119 &= 3 \times 34 + 17, \\ 34 &= 2 \times 17. \end{aligned}$$

It follows that 17 is the greatest common divisor of 272 and 119. We can now find integers u and v such that $272u + 119v = 17$.

$$\begin{aligned} 17 &= 119 - 3 \times 34 \\ &= 119 - 3 \times (272 - 2 \times 119) \\ &= 7 \times 119 - 3 \times 272. \end{aligned}$$

Thus $u = -3$ and $v = 7$.

Proposition 8.1. *Let $x_1, x_2, \ldots, x_k$ be integers, not all zero, and let d be the greatest common divisor of $x_1, x_2, \ldots, x_k$. Then there exist integers $u_1, u_2, \ldots, u_k$ such that*

$$d = u_1 x_1 + u_2 x_2 + \cdots + u_k x_k.$$

Proof. We recall that any ideal of the ring $\mathbb{Z}$ of integers is of the form $n\mathbb{Z}$ for some non-negative integer n, where $n\mathbb{Z}$ denotes the set of integer multiples of n (Proposition 7.4). Using the fact that

an integer n divides an integer x if and only if $x \in n\mathbb{Z}$, we see that a positive integer e divides each of $x_1, x_2, \ldots, x_k$ if and only if each of $x_1, x_2, \ldots, x_k$ belongs to the ideal $e\mathbb{Z}$ generated by e.

Let I be the ideal of $\mathbb{Z}$ generated by $x_1, x_2, \ldots, x_k$. Then $I = d\mathbb{Z}$ for some positive integer d. We claim that d is the greatest common divisor of $x_1, x_2, \ldots, x_k$. Now I is the set of multiples of d, and therefore d divides each of $x_1, x_2, \ldots, x_k$. Suppose that e is a positive integer that divides each of $x_1, x_2, \ldots, x_k$. Then each of $x_1, x_2, \ldots, x_k$ belongs to the ideal $e\mathbb{Z}$. But the ideal I generated by $x_1, x_2, \ldots, x_k$ is contained in every ideal of $\mathbb{Z}$ to which $x_1, x_2, \ldots, x_k$ belong. Thus $I \subset e\mathbb{Z}$. It follows that $d\mathbb{Z} \subset e\mathbb{Z}$, and thus $d \in e\mathbb{Z}$. But then e divides d. It follows from the definition of the greatest common divisor that d is the greatest common divisor of $x_1, x_2, \ldots, x_k$.

It follows from Lemma 7.10 that the ideal generated by $x_1, x_2, \ldots, x_k$ coincides with the set of all integers that can be expressed in the form $u_1x_1 + u_2x_2 + \cdots + u_kx_k$ for some integers $u_1, u_2, \ldots, u_k$. In particular the greatest common divisor d of $x_1, x_2, \ldots, x_k$ can be expressed as a sum of the required form. ∎

The Fundamental Theorem of Arithmetic

Proposition 8.2. *Let p be a prime number, and let r and s be integers. Suppose that p divides rs. Then either p divides r or else p divides s.*

Proof. Suppose that p does not divide r. We must show that p divides s. Now the greatest common divisor of p and r must be 1 since p is prime and p does not divide r. It follows from Proposition 8.1 that there exist integers u and v such that $1 = ur + vp$. Then $s = urs + vps$. But $urs + vps$ is divisible by p, since rs is divisible by p. It follows that s is divisible by p, as required. ∎

Corollary 8.3. *Let p be a prime number, and let $r_1, r_2, \ldots, r_n$ be integers. Suppose that p divides the product $r_1r_2 \cdots r_n$. Then p divides r_i for some i between 1 and n.*

Proof. The result follows easily by induction on n. The result has been verified when $n = 2$ (Proposition 8.2). Suppose that the result holds for all products of less than n integers and that the prime number p divides $r_1r_2 \cdots r_n$. Then p divides ar_n, where $a = r_1r_2 \cdots r_{n-1}$. It follows from Proposition 8.2 that either p divides r_n of else p divides a, in which case the induction hypothesis ensures that p divides r_i for some i between 1 and $n - 1$. The result follows. ∎

Theorem 8.4. (The Fundamental Theorem of Arithmetic) *Any integer greater than one is a prime number or can be expressed as a product of a finite number of prime numbers. The list of prime numbers whose product is a given integer is uniquely determined up to the order in which the factors are listed.*

Proof. Let A be the set of all integers greater than one that are not prime numbers and cannot be expressed as products of prime numbers. We must show that A is the empty set. Suppose that A were not empty. Then there would exist an integer n with the property that n is the smallest integer belonging to A. Then n would not be a prime number, and thus $n = rs$ for some positive integers r and s satisfying $1 < r < n$ and $1 < s < n$. Since r and s would be less than n they could not belong to the set A and therefore r and s would either be prime numbers or could be expressed as products of a finite number of prime numbers. It follows that n could be expressed as a product of a finite number of prime numbers, contradicting the requirement that n be an element of A. This contradiction shows that the set A must indeed be the empty set. Thus every integer greater than one that is not a prime number can be factored as a product of a finite number of prime numbers.

In order to show that, when any integer n greater than one is written as a product of primes, that list of primes is determined up to the order in which the primes are specified, it suffices to show that, when arranged in increasing order, the list of prime factors of n is uniquely determined. We show this by induction on n. The result clearly holds when $n = 2$, and indeed when n is any prime number.

Suppose then that all positive integers greater than one but less than some integer n have the property that, when factored as a product of prime numbers, the list of those prime numbers, when written in ascending order, is uniquely determined. We show that if n is then factored as a product of primes then the list of those prime numbers, when written in ascending order, is uniquely determined. The result is trivial when n is prime. Suppose then that n is not prime and that $n = p_1 p_2, \ldots, p_r = q_1 q_2 \ldots, q_s$, where $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ are prime numbers, $p_1 \leq p_2 \leq \cdots \leq p_r$ and $q_1 \leq q_2 \leq \cdots \leq q_s$. We must show that $r = s$ and $p_i = q_i$ for $i = 1, 2, \ldots, r$. Now if p is a prime number which divides n then p must divide p_i for some i between 1 and r (Corollary 8.3), and therefore $p = p_i$ for some integer i between 1 and s. It follows from this that $\{p_i : i = 1, 2, \ldots, r\}$ is the set of primes dividing n. Similarly $\{q_i : i = 1, 2, \ldots, s\}$ must be the set of prime numbers dividing n. It follows from this that $p_1 = q_1$, since both p_1 and q_1 must be equal to the smallest prime number that divides n. Let $m = n/p_1$. Then m is an integer greater than one but less than n. Our assumption ensures that, when factored as a product of prime numbers, the list of those prime numbers, when written in ascending order, is uniquely determined. Now $m = p_2, \ldots, p_r = q_2 \ldots, q_s$. It follows that $r = s$ and that $p_i = q_i$ for $i = 2, 3, \ldots, r$. Thus the prime factors $p_1, p_2, \ldots, p_r$, when written in ascending order, are uniquely determined.

It now follows by induction on n that, given any factorization of a number n greater than one as a product of prime numbers, the list of those prime numbers, when specified in ascending order, is uniquely determined, as required. ∎

The Theorems of Fermat, Wilson and Euler

Let p be a prime number. The ring $\mathbb{Z}_p$ of congruence classes of integers modulo p is then a field (see Theorem 7.12 Theorem 7.16). It follows that the set $\mathbb{Z}_p^*$ of non-zero congruence classes of integers modulo p is a group with respect to the operation of multiplication. This result can be used to prove a couple of theorems of number theory that are attributed to Pierre de Fermat (1601–1665) and John Wilson (1741–1793).

Theorem 8.5. (Fermat's Little Theorem) *Let p be a prime number. Then $x^p \equiv x \bmod p$ for all integers x.*

Proof. For each integer x let $[x]$ denote the congruence class of x modulo p. The group $\mathbb{Z}_p^*$ of non-zero congruence classes of integers modulo p is a group of order $p-1$. It follows from Lagrange's Theorem that the order of every element of $\mathbb{Z}_p^*$ divides $p-1$, and thus $[x]^{p-1} = [1]$ whenever $[x] \neq [0]$. But $[x]^{p-1} = [x^{p-1}]$. It follows that $x^{p-1} \equiv 1 \bmod p$ for all integers x that are not divisible by p.

Let x be an integer. If x is divisible by p then so is x^p, and therefore $x^p \equiv x \bmod p$ (since both x^p and x are congruent to zero modulo p). If x is not divisible by p then we have shown that $x^{p-1} \equiv 1 \bmod p$. It follows that $x^p \equiv x \bmod p$, as required. ∎

Theorem 8.6. (Wilson) *Let p be an prime number. Then $(p-1)! \equiv -1 \bmod p$.*

Proof. The result is true when $p = 2$. Suppose then that p is an odd prime. Let $\mathbb{Z}_p$ be the ring of congruence classes of integers modulo p, and let $\mathbb{Z}_p^*$ be the group of non-zero elements of $\mathbb{Z}_p$ with the operation of multiplication. For each integer x let $[x]$ denote the congruence class of x modulo p. Suppose that $\alpha \in \mathbb{Z}_p^*$ satisfies $\alpha^2 = [1]$. Then $(\alpha - [1])(\alpha + [1]) = [0]$. But then either $\alpha - [1] = [0]$,

in which case $\alpha = [1]$, or else $\alpha + [1] = [0]$, in which case $\alpha = -[1]$, since the ring $\mathbb{Z}_p$ is an integral domain. Now an element of $\mathbb{Z}_p^*$ is represented by a unique integer x satisfying $1 \leq x \leq p-1$, and the elements $[1]$ and $-[1]$ are represented by 1 and $p-1$ respectively. Thus if x is an integer which satisfies $1 < x < p-1$ then $[x]^2 \neq [1]$ and hence there exists exactly one integer y satisfying $1 < y < p-1$ which is not equal to x and which satisfies $[y] = [x]^{-1}$. Therefore the integers greater than 1 and less than $p-1$ can be listed as $x_1, y_1, x_2, y_2, \ldots, x_m, y_m$, where $m = \frac{1}{2}(p-3)$, so that $[x_j]^{-1} = [y_j]$ for $j = 1, 2, \ldots, m$. Then $[x_j][y_j] = [1]$ for $j = 1, 2, \ldots, m$. It follows that

$$[(p-1)!] = [1][2]\cdots[p-1] = [1][p-1][x_1][y_1][x_2][y_2]\cdots[x_m][y_m] = [1][p-1] = [-1],$$

and thus $(p-1)! \equiv -1 \bmod p$, as required. ∎

(A proof of Wilson's Theorem was given by Lagrange in 1773.)

Fermat's Little Theorem was generalized by Euler (1707–1783). Two integers m and n are said to be *coprime* if there is no prime number that divides both m and n. (Thus m and n are coprime if and only if the greatest common divisor of m and n is 1.) If m and n are coprime then we say that n is *coprime to* m (or that n is *relatively prime to* m. For each positive integer m, let $\varphi(m)$ denote the number of positive integers less than m that are coprime to m. If p is a prime number then all positive integers less than p are coprime to p. It follows that $\varphi(p) = p-1$ for all prime numbers p.

Theorem 8.7. (Euler) *Let m be a positive integer, and let x be a positive integer that is coprime to m. Then $x^{\varphi(m)} \equiv 1$ mod m, where $\varphi(m)$ is the number of positive integers less than m that are coprime to m.*

Proof. We say that the congruence class $[x]$ of an integer x modulo m is *invertible* if $[x][u] = [1]$ for some $[u] \in \mathbb{Z}_m$. Let us denote by G the set of all invertible elements of the ring $\mathbb{Z}_m$. We claim that G is a group with respect to the operation of multiplication. Let $[x]$ and $[y]$ be invertible congruence classes. Then there exist congruence classes $[u]$ and $[v]$ in $\mathbb{Z}_m$ such that $[x][u] = [1]$ and $[y][v] = [1]$. Then $[xy][uv] = [x][y][u][v] = [x][u][y][v] = [1][1] = [1]$. It follows that the product $[xy]$ of two invertible congruence classes $[x]$ and $[y]$ is invertible. Thus multiplication of invertible congruence classes is a binary operation on G. This operation is associative, and $[1]$ is the identity element of G. Moreover if $[x]$ is any congruence class of G then the inverse of $[x]$ in G exists and is the congruence class $[u]$ which satisfies $[x][u] = [1]$. Thus G is a group with respect to multiplication of congruence classes.

Let x be an integer. We claim that $[x] \in G$ if and only if x is coprime to m. Suppose that $[x] \in G$. Then there exists an integer u such that $[x][u] = [1]$ in $\mathbb{Z}_m$. Then $1 - xu$ is divisible by m, and therefore $1 = xu + mv$ for some integer v. It follows from this that x is coprime to m (since any prime number dividing both x and m would also have to divide 1).

Conversely let x be some integer that is coprime to m. Then 1 is the greatest common divisor of x and m. It follows from Proposition 8.1 that there exist integers u and v such that $1 = xu + mv$. But then $[1] = [xu + mv] = [x][u] + [m][v] = [x][u]$, since $[m] = [0]$. Thus $[x]$ is invertible.

We have shown that the group G consists of the congruence classes of those integers x that are coprime to m. Now for each congruence class in $\mathbb{Z}_m$ there is a unique non-negative integer less than m that belongs to the congruence class. It follows that the order of the group G is equal to the number $\varphi(m)$ of positive integers less than m that are coprime to m (since each element of G is the congruence class of exactly one such integer). It follows from Lagrange's Theorem that $[x]^{\varphi(m)} = [1]$ for each $[x] \in G$. Thus $x^{\varphi(m)} \equiv 1 \bmod m$ for all integers x that are coprime to m, as required. ∎

Problems

1. Calculate the Cayley table for the group of non-zero elements of $\mathbb{Z}_7$ with respect to multiplication, and show that this group is a cyclic group.

2. What are the zero divisors in $\mathbb{Z}_{12}$?

3. An element x of a unital ring R is said to be *invertible* if $xy = 1 = yx$ for some $y \in R$.

   (a) Let x, y and z be elements of a unital ring R. Suppose that $xy = 1 = yx$ and $xz = 1 = zx$. Prove that $y = z$.

   (b) Show that the set of invertible elements of a unital ring R is a group with respect to the operation of multiplication.

   (c) Let x be an element of a unital ring R. Suppose that $x^n = 0$ for some positive integer n (where x^n is defined for all positive integers n so that $x^1 = x$ and $x^n = x^{n-1}x$ for all $n > 1$). Prove that $1 - x$ is invertible.

4. An element x of a ring R is said to be an *idempotent* if $x^2 = x$ (where $x^2 = xx$).

   (a) Prove that an idempotent x satisfies $x^n = x$ for all $n > 0$,

   (b) What are the idempotents of the ring $\mathbb{Z}_6$ of congruence classes of integers modulo 6?

   (c) Prove that the only idempotents in an integral domain are 0 and 1.

   (d) Let x be an idempotent in a unital ring. Prove that $1 - x$ is also an idempotent.

   (e) Let x and y be idempotents in a unital ring R that satisfy $xy = yx$. Prove that xy and $x + y - xy$ are also idempotents.

   (f) Let f be a polynomial with coefficients in a unital commutative ring R. Prove that $f(x) = f(0)(1 - x) + f(1)x$ for any idempotent x of R. (Given $f \in R[t]$, the value $f(x)$ of f at x is calculated by substituting x for the indeterminant t in the expression $f(t)$. Thus if $f(t) = 1+t+t^2$ then $f(x) = 1 + x + x^2 = 1 + x + x = 1 + 2.x$ for any idempotent x.)

5. Use the Euclidean algorithm to calculate the greatest common divisor d of the numbers 391 and 276, and find integers u and v satisfying $391u + 276v = d$.

6. Let q be a quaternion q, given by $q = a + xi + yj + xk$. The *conjugate* $\overline{q}$ of the quaternion q is defined by $\overline{q} = a - xi - yj - xk$, and the norm $|q|$ of q is defined by $|q|^2 = a^2 + x^2 + y^2 + z^2$.

   (a) Verify that $q\overline{q} = \overline{q}q = |q|^2$ for all quaternions q.

   (b) Show that a quaternion q satisfies $q^2 = -1$ if and only if $q = xi + yj + zk$ for some real numbers x, y and z satisfying $x^2 + y^2 + z^2 = 1$.

   (c) Show that if a quaternion q satisfies $q^2 = -1$ and if $\varphi(s) = \cos s + (\sin s)q$ for all real numbers s then $\varphi(s + t) = \varphi(s)\varphi(t)$ for all real numbers s and t.