MA2C03 Mathematics
School of Mathematics, Trinity College
Hilary Term 2016
Lecture 56 (March 23, 2016)

David R. Wilkins

41. Elementary Number Theory

41.1. Subgroups of the Integers

A subset S of the set $\mathbb{Z}$ of integers is a *subgroup* of $\mathbb{Z}$ if $0 \in S$, $-x \in S$ and $x + y \in S$ for all $x \in S$ and $y \in S$.
It is easy to see that a non-empty subset S of $\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ if and only if $x - y \in S$ for all $x \in S$ and $y \in S$.
Let m be an integer, and let $m\mathbb{Z} = \{mn : n \in \mathbb{Z}\}$. Then $m\mathbb{Z}$ (the set of integer multiples of m) is a subgroup of $\mathbb{Z}$.

Theorem 41.1

Let S be a subgroup of $\mathbb{Z}$. Then $S = m\mathbb{Z}$ for some non-negative integer m.

Proof

If $S = \{0\}$ then $S = m\mathbb{Z}$ with $m = 0$. Suppose that $S \neq \{0\}$. Then S contains a non-zero integer, and therefore S contains a positive integer (since $-x \in S$ for all $x \in S$). Let m be the smallest positive integer belonging to S. A positive integer n belonging to S can be written in the form $n = qm + r$, where q is a positive integer and r is an integer satisfying $0 \leq r < m$. Then $qm \in S$ (because $qm = m + m + \cdots + m$). But then $r \in S$, since $r = n - qm$. It follows that $r = 0$, since m is the smallest positive integer in S. Therefore $n = qm$, and thus $n \in m\mathbb{Z}$. It follows that $S = m\mathbb{Z}$, as required. ∎

41.2. Greatest Common Divisors

Definition

Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. A *common divisor* of $a_1, a_2, \ldots, a_r$ is an integer that divides each of $a_1, a_2, \ldots, a_r$. The *greatest common divisor* of $a_1, a_2, \ldots, a_r$ is the greatest positive integer that divides each of $a_1, a_2, \ldots, a_r$. The greatest common divisor of $a_1, a_2, \ldots, a_r$ is denoted by $(a_1, a_2, \ldots, a_r)$.

Theorem 41.2

Let $a_1, a_2, \ldots, a_r$ be integers, not all zero. Then there exist integers $u_1, u_2, \ldots, u_r$ such that

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

where $(a_1, a_2, \ldots, a_r)$ is the greatest common divisor of $a_1, a_2, \ldots, a_r$.

Proof

Let S be the set of all integers that are of the form

$$n_1 a_1 + n_2 a_2 + \cdots + n_r a_r$$

for some $n_1, n_2, \ldots, n_r \in \mathbb{Z}$. Then S is a subgroup of $\mathbb{Z}$. It follows that $S = m\mathbb{Z}$ for some non-negative integer m (Theorem 41.1). Then m is a common divisor of $a_1, a_2, \ldots, a_r$, (since $a_i \in S$ for $i = 1, 2, \ldots, r$). Moreover any common divisor of $a_1, a_2, \ldots, a_r$ is a divisor of each element of S and is therefore a divisor of m. It follows that m is the greatest common divisor of $a_1, a_2, \ldots, a_r$. But $m \in S$, and therefore there exist integers $u_1, u_2, \ldots, u_r$ such that

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r,$$

as required. ∎

Definition

Let $a_1, a_2, \dots, a_r$ be integers, not all zero. If the greatest common divisor of $a_1, a_2, \dots, a_r$ is 1 then these integers are said to be *coprime*. If integers a and b are coprime then a is said to be coprime to b. (Thus a is coprime to b if and only if b is coprime to a.)

Corollary 41.3

Let $a_1, a_2, \ldots, a_r$ be integers that are not all zero. Then $a_1, a_2, \ldots, a_r$ are coprime if and only if there exist integers $u_1, u_2, \ldots, u_r$ such that

$$1 = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

Proof

If $a_1, a_2, \ldots, a_r$ are coprime then the existence of the required integers $u_1, u_2, \ldots, u_r$ follows from Theorem 41.2. On the other hand, if there exist integers $u_1, u_2, \ldots, u_r$ with the required property then any common divisor of $a_1, a_2, \ldots, a_r$ must be a divisor of 1, and therefore $a_1, a_2, \ldots, a_r$ must be coprime. ∎

41.3. The Euclidean Algorithm

Let a and b be positive integers with $a > b$. Let $r_0 = a$ and $r_1 = b$. If b does not divide a then let r_2 be the remainder on dividing a by b. Then $a = q_1 b + r_2$, where q_1 and r_2 are positive integers and $0 < r_2 < b$. If r_2 does not divide b then let r_3 be the remainder on dividing b by r_2. Then $b = q_2 r_2 + r_3$, where q_2 and r_3 are positive integers and $0 < r_3 < r_2$. If r_3 does not divide r_2 then let r_4 be the remainder on dividing r_2 by r_3. Then $r_2 = q_3 r_3 + r_4$, where q_3 and r_4 are positive integers and $0 < r_4 < r_3$. Continuing in this fashion, we construct positive integers $r_0, r_1, \ldots, r_n$ such that $r_0 = a$, $r_1 = b$ and r_i is the remainder on dividing r_{i-2} by r_{i-1} for $i = 2, 3, \ldots, n$. Then $r_{i-2} = q_{i-1} r_{i-1} + r_i$, where q_{i-1} and r_i are positive integers and $0 < r_i < r_{i-1}$. The algorithm for constructing the positive integers $r_0, r_1, \ldots, r_n$ terminates when r_n divides r_{n-1}. Then $r_{n-1} = q_n r_n$ for some positive integer q_n. (The algorithm must clearly terminate in a finite number of steps, since $r_0 > r_1 > r_2 > \cdots > r_n$.)

We claim that r_n is the greatest common divisor of a and b.
Any divisor of r_n is a divisor of r_{n-1}, because $r_{n-1} = q_n r_n$.
Moreover if $2 \leq i \leq n$ then any common divisor of r_i and r_{i-1} is a divisor of r_{i-2}, because $r_{i-2} = q_{i-1} r_{i-1} + r_i$. If follows that every divisor of r_n is a divisor of all the integers $r_0, r_1, \ldots, r_n$. In particular, any divisor of r_n is a common divisor of a and b. In particular, r_n is itself a common divisor of a and b.
If $2 \leq i \leq n$ then any common divisor of r_{i-2} and r_{i-1} is a divisor of r_i, because $r_i = r_{i-2} - q_{i-1} r_{i-1}$. It follows that every common divisor of a and b is a divisor of all the integers $r_0, r_1, \ldots, r_n$. In particular any common divisor of a and b is a divisor of r_n. It follows that r_n is the greatest common divisor of a and b.

There exist integers u_i and v_i such that $r_i = u_i a + v_i b$ for $i = 1, 2, \ldots, n$. Indeed $u_i = u_{i-2} - q_{i-1} u_{i-1}$ and $v_i = v_{i-2} - q_{i-1} v_{i-1}$ for each integer i between 2 and n, where $u_0 = 1$, $v_0 = 0$, $u_1 = 0$ and $v_1 = 1$. In particular $r_n = u_n a + v_n b$. The algorithm described above for calculating the greatest common divisor (a, b) of two positive integers a and b is referred to as the *Euclidean algorithm*. It also enables one to calculate integers u and v such that $(a, b) = ua + vb$.

Example

We calculate the greatest common divisor of 425 and 119. Now

$$\begin{aligned} 425 &= 3 \times 119 + 68 \\ 119 &= 68 + 51 \\ 68 &= 51 + 17 \\ 51 &= 3 \times 17. \end{aligned}$$

It follows that 17 is the greatest common divisor of 425 and 119. Moreover

$$\begin{aligned} 17 &= 68 - 51 = 68 - (119 - 68) \\ &= 2 \times 68 - 119 = 2 \times (425 - 3 \times 119) - 119 \\ &= 2 \times 425 - 7 \times 119. \end{aligned}$$

Example

We calculate the greatest common divisor of 90, 126, 210, and express it in the form $90u + 126v + 210w$ for appropriate integers u, v and w.

First we calculate the greatest common divisor of 90 and 126 using the Euclidean algorithm. Now

$$\begin{aligned} 126 &= 90 + 36 \\ 90 &= 2 \times 36 + 18 \\ 36 &= 2 \times 18. \end{aligned}$$

It follows that 18 is the greatest common divisor of 90 and 126. Moreover

$$\begin{aligned} 18 &= 90 - 2 \times 36 = 90 - 2 \times (126 - 90) \\ &= 3 \times 90 - 2 \times 126. \end{aligned}$$

Now any common divisor d of 90, 126 and 210 is a common divisor of 90 and 126, and therefore divides the greatest common divisor of 90 and 126. Thus d divides 18. But d also divides 210. It follows that any common divisor of 90, 126 and 210 is a common divisor of 18 and 210, and therefore divides the greatest common divisor of 18 and 210. We calculate this greatest common divisor using the Euclidean algorithm. Now

$$\begin{aligned} 210 &= 11 \times 18 + 12 \\ 18 &= 12 + 6 \\ 12 &= 2 \times 6. \end{aligned}$$

It follows that 6 is the greatest common divisor of 18 and 210. Moreover

$$\begin{aligned} 6 &= 18 - 12 = 18 - (210 - 11 \times 18) \\ &= 12 \times 18 - 210. \end{aligned}$$

But $18 = 3 \times 90 - 2 \times 126$. It follows that

$$6 = 36 \times 90 - 24 \times 126 - 210.$$

The number 6 divides 90, 126 and 210. Moreover any common divisor of 90, 126 and 210 must also divide 6. Therefore 6 is the greatest common divisor of 90, 126 and 210. Also
$6 = 90u + 126v + 210w$ where $u = 36$, $v = -24$ and $w = -1$.

Remark

Let $a_1, a_2, \ldots, a_r$ be non-zero integers, where $r > 2$. Suppose we wish to compute the greatest common divisor d of $a_1, a_2, \ldots, a_r$, and express it in the form

$$d = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r.$$

where $u_1, u_2, \ldots, u_r$ are integers.

Let d' be the greatest common divisor of $a_1, a_2, \ldots, a_{r-1}$. Then any common divisor of $a_1, a_2, \ldots, a_r$ divides both d' and a_r, and therefore divides the greatest common divisor (d', a_r) of d' and a_r. In particular d divides (d', a_r). But (d', a_r) divides a_i for $i = 1, 2, \ldots, r$. It follows that $d = (d', a_r)$. Thus

$$(a_1, a_2, \ldots, a_r) = ((a_1, a_2, \ldots, a_{r-1}), a_r).$$

for any non-zero integers $a_1, a_2, \ldots, a_r$. Moreover there exist integers p and q such that $d = pd' + qa_r$. These integers p and q may be computed using the Euclidean algorithm, given d' and a_r.

Let $v_1, v_2, \ldots, v_{r-1}$ be integers for which

$$d' = v_1 a_1 + v_2 a_2 + \cdots + v_{r-1} a_{r-1}.$$

Then

$$d = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r,$$

where $u_i = p v_i$ for $i = 1, 2, \ldots, r-1$ and $u_r = q$. Therefore successive applications of the Euclidean algorithm will enable us to compute the greatest common divisor $(a_1, a_2, \ldots, a_r)$ of $a_1, a_2, \ldots, a_r$ and express it in the form

$$(a_1, a_2, \ldots, a_r) = u_1 a_1 + u_2 a_2 + \cdots + u_r a_r$$

for appropriate integers $u_1, u_2, \ldots, u_r$.

Indeed we may proceed by computing successively the greatest common divisors

$$(a_1, a_2),\ \ (a_1, a_2, a_3),\ \ (a_1, a_2, a_3, a_4), \ldots,$$

representing each quantity $(a_1, a_2, \ldots, a_k)$ by an expression of the form

$$(a_1, a_2, \ldots, a_k) = \sum_{i=1}^{k} v_{ki} a_i,$$

where the quantities v_{ki} are integers.

41.4. Prime Numbers

Definition

A *prime number* is an integer p greater than one with the property that 1 and p are the only positive integers that divide p.

Let p be a prime number, and let x be an integer. Then the greatest common divisor (p, x) of p and x is a divisor of p, and therefore either $(p, x) = p$ or else $(p, x) = 1$. It follows that either x is divisible by p or else x is coprime to p.

Theorem 41.4

Let p be a prime number, and let x and y be integers. If p divides xy then either p divides x or else p divides y.

Proof

Suppose that p divides xy but p does not divide x. Then p and x are coprime, and hence there exist integers u and v such that $1 = up + vx$ (Corollary 41.3). Then $y = upy + vxy$. It then follows that p divides y, as required. ∎

Corollary 41.5

Let p be a prime number. If p divides a product of integers then p divides at least one of the factors of the product.

Proof

Let $a_1, a_2, \ldots, a_k$ be integers, where $k > 1$. Suppose that p divides $a_1 a_2 \cdots a_k$. Then either p divides a_k or else p divides $a_1 a_2 \cdots a_{k-1}$. The required result therefore follows by induction on the number k of factors in the product. ∎

41.5. The Fundamental Theorem of Arithmetic

Lemma 41.6

Every integer greater than one is a prime number or factors as a product of prime numbers.

Proof

Let n be an integer greater than one. Suppose that every integer m satisfying $1 < m < n$ is a prime number or factors as a product of prime numbers. If n is not a prime number then $n = ab$ for some integers a and b satisfying $1 < a < n$ and $1 < b < n$. Then a and b are prime numbers or products of prime numbers. Thus if n is not itself a prime number then n must be a product of prime numbers. The required result therefore follows by induction on n. ∎

An integer greater than one that is not a prime number is said to be a *composite number*.

Let n be an composite number. We say that n factors uniquely as a product of prime numbers if, given prime numbers $p_1, p_2, \ldots, p_r$ and $q_1, q_2, \ldots, q_s$ such that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots q_s,$$

the number of times a prime number occurs in the list $p_1, p_2, \ldots, p_r$ is equal to the number of times it occurs in the list $q_1, q_2, \ldots, q_s$. (Note that this implies that $r = s$.)

Theorem 41.7

(The Fundamental Theorem of Arithmetic) Every composite number greater than one factors uniquely as a product of prime numbers.

Proof

Let n be a composite number greater than one. Suppose that every composite number greater than one and less than n factors uniquely as a product of prime numbers. We show that n then factors uniquely as a product of prime numbers. Suppose therefore that

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \ldots, q_s,$$

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 prove that $r = s$ and $p_i = q_i$ for all integers i between 1 and r.

Let p be the smallest prime number that divides n. If a prime number divides a product of integers then it must divide at least one of the factors (Corollary 41.5). It follows that p must divide p_i and thus $p = p_i$ for some integer i between 1 and r. But then $p = p_1$, since p_1 is the smallest of the prime numbers $p_1, p_2, \ldots, p_r$. Similarly $p = q_1$. Therefore $p = p_1 = q_1$. Let $m = n/p$. Then

$$m = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

But then $r = s$ and $p_i = q_i$ for all integers i between 2 and r, because every composite number greater than one and less than n factors uniquely as a product of prime numbers. It follows that n factors uniquely as a product of prime numbers. The required result now follows by induction on n. (We have shown that if all composite numbers m satisfying $1 < m < n$ factor uniquely as a product of prime numbers, then so do all composite numbers m satisfying $1 < m < n + 1$.) ∎

41.6. The Infinitude of Primes

Theorem 41.8

(Euclid) The number of prime numbers is infinite.

Proof

Let $p_1, p_2, \ldots, p_r$ be prime numbers, let $m = p_1 p_2 \cdots p_r + 1$. Now p_i does not divide m for $i = 1, 2, \ldots, r$, since if p_i were to divide m then it would divide $m - p_1 p_2 \cdots p_r$ and thus would divide 1. Let p be a prime factor of m. Then p must be distinct from $p_1, p_2, \ldots, p_r$. Thus no finite set $\{p_1, p_2, \ldots, p_r\}$ of prime numbers can include all prime numbers. ∎

41.7. Congruences

Let m be a positive integer. Integers x and y are said to be *congruent* modulo m if $x - y$ is divisible by m. If x and y are congruent modulo m then we denote this by writing
$x \equiv y \pmod{m}$.
The *congruence class* of an integer x modulo m is the set of all integers that are congruent to x modulo m.
Let x, y and z be integers. Then $x \equiv x \pmod{m}$. Also $x \equiv y \pmod{m}$ if and only if $y \equiv x \pmod{m}$. If $x \equiv y \pmod{m}$ and $y \equiv z \pmod{m}$ then $x \equiv z \pmod{m}$. Thus congruence modulo m is an equivalence relation on the set of integers.

Lemma 41.9

Let m be a positive integer, and let x, x', y and y' be integers. Suppose that $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$. Then $x + y \equiv x' + y' \pmod{m}$ and $xy \equiv x'y' \pmod{m}$.

Proof

The result follows immediately from the identities

$$\begin{aligned} (x+y) - (x'+y') &= (x - x') + (y - y'), \\ xy - x'y' &= (x - x')y + x'(y - y'). \end{aligned}$$

∎

Lemma 41.10

Let x, y and m be integers with $m \neq 0$. Suppose that m divides xy and that m and x are coprime. Then m divides y.

Proof

There exist integers a and b such that $1 = am + bx$, since m and x are coprime (Corollary 41.3). Then $y = amy + bxy$, and m divides xy, and therefore m divides y, as required. ∎

Lemma 41.11

Let m be a positive integer, and let a, x and y be integers with $ax \equiv ay \pmod{m}$. Suppose that m and a are coprime. Then $x \equiv y \pmod{m}$.

Proof

If $ax \equiv ay \pmod{m}$ then $a(x - y)$ is divisible by m. But m and a are coprime. It therefore follows from Lemma 41.10 that $x - y$ is divisible by m, and thus $x \equiv y \pmod{m}$, as required. ∎

Lemma 41.12

Let x and m be non-zero integers. Suppose that x is coprime to m. Then there exists an integer y such that $xy \equiv 1 \pmod{m}$. Moreover y is coprime to m.

Proof

There exist integers y and k such that $xy + mk = 1$, since x and m are coprime (Corollary 41.3). Then $xy \equiv 1 \pmod{m}$. Moreover any common divisor of y and m must divide xy and therefore must divide 1. Thus y is coprime to m, as required. ∎

Lemma 41.13

Let m be a positive integer, and let a and b be integers, where a is coprime to m. Then there exist integers x that satisfy the congruence $ax \equiv b \pmod{m}$. Moreover if x and x' are integers such that $ax \equiv b \pmod{m}$ and $ax' \equiv b \pmod{m}$ then $x \equiv x' \pmod{m}$.

Proof

There exists an integer c such that $ac \equiv 1 \pmod{m}$, since a is coprime to m (Lemma 41.12). Then $ax \equiv b \pmod{m}$ if and only if $x \equiv cb \pmod{m}$. The result follows. ∎

Lemma 41.14

Let $a_1, a_2, \ldots, a_r$ be integers, and let x be an integer that is coprime to a_i for $i = 1, 2, \ldots, r$. Then x is coprime to the product $a_1 a_2 \cdots a_r$ of the integers $a_1, a_2, \ldots, a_r$.

Proof

Let p be a prime number which divides the product $a_1 a_2 \cdots a_r$. Then p divides one of the factors $a_1, a_2, \ldots, a_r$ (Corollary 41.5). It follows that p cannot divide x, since x and a_i are coprime for $i = 1, 2, \ldots, r$. Thus no prime number is a common divisor of x and the product $a_1 a_2 \cdots a_r$. It follows that the greatest common divisor of x and $a_1 a_2 \cdots a_r$ is 1, since this greatest common divisor cannot have any prime factors. Thus x and $a_1 a_2 \cdots a_r$ are coprime, as required. ∎

Let m be a positive integer. For each integer x, let $[x]$ denote the congruence class of x modulo m. If x, x', y and y' are integers and if $x \equiv x' \pmod{m}$ and $y \equiv y' \pmod{m}$ then $xy \equiv x'y' \pmod{m}$. It follows that there is a well-defined operation of multiplication defined on congruence classes of integers modulo m, where $[x][y] = [xy]$ for all integers x and y. This operation is commutative and associative, and $[x][1] = [x]$ for all integers x. If x is an integer coprime to m, then it follows from Lemma 41.12 that there exists an integer y coprime to m such that $xy \equiv 1 \pmod{m}$. Then $[x][y] = [1]$. Therefore the set $\mathbb{Z}_m^*$ of congruence classes modulo m of integers coprime to m is an Abelian group (with multiplication of congruence classes defined as above).