Week 2

1.5 The Euclidean Algorithm

(Named after the Greek mathematician Euclid, c. 350 BC, who published the algorithm in his book *Elements*.)

Lemma 1.3 *If $a = bq + r$, then $(a, b) = (b, r)$.*

Proof.
Let $d = (a, b)$. Then $d|a$ and $d|b$, and since $a = bq + r$, it follows that $d|r$. Therefore d is a common divisor of b and r. Suppose c is any common divisor of b and r. Then again from $a = bq + r$ we have that $c|a$, so c is a common divisor of a and b and thus $c \leq d$. Therefore any common divisor of b and r is less than or equal to d and so, by definition of greatest common divisor, $d = (b, r)$. ■

Theorem 1.3 (The Euclidean Algorithm) *If a and b are positive integers and*

$$\begin{array}{ll} a = bq + r, & 0 \leq r < b, \\ b = rq_1 + r_1, & 0 \leq r_1 < r, \\ r = r_1 q_2 + r_2, & 0 \leq r_2 < r_1, \\ \vdots & \vdots \\ r_{k-1} = r_k q_{k+1} + r_{k+1}, & 0 \leq r_{k+1} < r_k, \end{array}$$

then for k large enough, say $k = t$, we have

$$r_{t-1} = r_t q_{t+1} \quad \text{and} \quad (a, b) = r_t.$$

Proof. By the Well-Ordering Principle, the sequence of nonnegative integers

$$b > r > r_1 > \cdots$$

ends. Thus eventually one of the remainders is zero. Suppose $r_{t+1} = 0$. Then $r_{t-1} = r_t q_{t+1}$. Applying Lemma 1.3 several times we get

$$(a, b) = (b, r) = (r, r_1) = (r_1, r_2) = \cdots = (r_{t-1}, r_t) = (r_t, 0) = r_t.$$

■

Example: Determine $(986, 391)$.

$$\overset{a}{986} = \overset{b}{391} \cdot \overset{q}{2} + \overset{r}{204} \tag{1.8}$$

$$\overset{b}{391} = \overset{r}{204} \cdot \overset{q_1}{1} + \overset{r_1}{187} \tag{1.9}$$

$$\overset{r}{204} = \overset{r_1}{187} \cdot \overset{q_2}{1} + \overset{r_2}{17} \tag{1.10}$$

$$\overset{r_1}{187} = \overset{r_2}{17} \cdot \overset{q_3}{11}$$

Hence $(986, 391) = 17$.

Now work this backwards: From (1.10),

$$17 = 204 - 187 \tag{1.11}$$

and from (1.9), $187 = 391 - 204$, so (1.11) becomes

$$17 = 204 - (391 - 204) = -391 + 2 \cdot 204. \tag{1.12}$$

But from (1.8), $204 = 986 - 2 \cdot 391$, and substitution in (1.12) gives

$$\begin{aligned} 17 &= -391 + 2(986 - 2 \cdot 391) \\ &= 2 \cdot 986 - 5 \cdot 391. \end{aligned}$$

So we have written $(986, 391)$ as $x \cdot 986 + y \cdot 391$, where $x = 2$ and $y = -5$. This is always possible:

Theorem 1.4 *If $(a, b) = d$, then there exist integers x and y such that*

$$ax + by = d.$$

(These numbers x and y are not unique – there are infinitely many that will work.) Moreover, if x', y' are integers such that $ax' + by' = c$, then c is a multiple of d.

The Euclidean algorithm computes the greatest common divisor of large numbers efficiently: it never requires more division steps than five times the number of digits of the smaller integer.

The following three frequently used corollaries to Theorem 1.4 are mentioned without proof; work through the proofs on your own.

Corollary 1.1 *If $d|ab$ and $(d, a) = 1$, then $d|b$.*

Corollary 1.2 *If $(a, b) = d$, and $c|a$, $c|b$, then $c|d$.*

Corollary 1.3 *If $a|m$, $b|m$, and $(a, b) = 1$, then $ab|m$.*

Section 2

Unique Factorization

The aim here is to prove that every positive integer can be written as a product of prime numbers in one and only one way – the **Unique Factorization Theorem**.

2.1 Prime Numbers

Definitions

A **non-trivial (positive) divisor** of an integer n is any divisor d of n such that $d \notin \{1, n\}$.

A **prime number** is an integer $n \geq 2$ without non-trivial divisors.

A **composite number** is a positive integer with at least one non-trivial divisor.

Note that 1 is neither a prime nor a composite number, but a **unit**.

Example: 1,000,000,000,000,066,600,000,000,000,001 is prime and is called *Belphegor's prime*.

Lemma 2.1 *Every integer n with $n \geq 2$ is divisible by a prime.*

Proof.
Let S be the set of non-trivial positive divisors of n. If $S = \varnothing$, then n is prime by definition and $n|n$, so the lemma follows.
If $S \neq \varnothing$, then (by the Well-Ordering Principle) it has a smallest element, say d. If d has a non-trivial positive divisor c, then $c < d$ and $c|n$ (since $c|d$ and $d|n$), which is impossible by the choice of d as the smallest non-trivial positive divisor of n. Thus d is prime and a divisor of n. ■

Lemma 2.2 *Every integer n with $n > 1$ can be written as a product of primes.*

Proof (Induction – strong form).
For $n \geq 2$, let $\mathrm{P}(n)$ be the statement

$$\mathrm{P}(n)\text{: } n \text{ can be written as a product of primes.}$$

P(2) is true: Clearly, since 2 is prime, 2 can be written as a (trivial) product of primes.

Induction hypothesis: For an arbitrary integer $k \geq 2$, suppose $\mathrm{P}(r)$ is true for each $r \in \{2, 3, 4, ..., k\}$, that is, for each such r, suppose r can be written as a product of primes.

To prove: $\mathrm{P}(k+1)$ holds, that is, $k+1$ can be written as a product of primes.

By Lemma 2.1, $k+1$ is divisible by a prime, say c. If $c = k+1$, then $k+1$ is prime and we are done, because then $k+1$ is a trivial product of primes. If $c \neq k+1$, then $c < k+1$. Consider the integer $(k+1)/c$. Since $c > 1$ (because c is prime) and $c < k+1$, we have

$$1 < (k+1)/c \leq k$$

and we may apply the induction hypothesis to $(k+1)/c$. Thus assume $(k+1)/c$ can be written as a product of primes, say

$$(k+1)/c = p_1 p_2 ... p_s.$$

Now

$$k + 1 = ((k+1)/c) \cdot c = (p_1 p_2 ... p_s) \cdot c,$$

where each number p_i and c in the product on the right hand side is prime. Thus $\mathrm{P}(k+1)$ holds, and by the Principle of Induction, $\mathrm{P}(n)$ is true for all $n \geq 2$. ■

Alternative Proof. If the statement is false, then

$$S = \{x \in \mathbb{Z},\ x \geq 2 : x \text{ cannot be written as a product of primes}\} \neq \varnothing.$$

By the Well Ordering Principle, S has a smallest element m. Then m is not prime, otherwise m is a trivial product of primes. Since m is composite, $m = ab$, where $1 < a, b < m$. By the minimality of m, each of a and b is a product of primes, hence m is a product of primes, a contradiction. ■

Theorem 2.1 (Euclid) *There are infinitely many primes.*

Proof.
Suppose not. Then there are only finitely many primes $p_1, p_2, ..., p_r$. Consider the integer

$$n = p_1 p_2 ... p_r + 1. \tag{2.1}$$

By Lemma 2.1 n is divisible by a prime and so n is divisible by one of the integers $p_1, p_2, ..., p_r$. Suppose $p_k | n$ for some $k = 1, ..., r$. Obviously $p_k | p_1 p_2 ... p_r$. Now p_k divides the left-hand side and the first term on the right-hand side of (2.1), hence it also divides the second term on the right-hand side, i.e. $p_k | 1$. This is impossible because all primes are greater than 1. Therefore the original assumption that there are only finitely many primes is incorrect and the theorem follows. ■

Lemma 2.3 *If n is composite, then it has a divisor d such that $1 < d \leq \sqrt{n}$.*

Proof. Since n is composite, there are integers d_1 and d_2 such that $1 < d_1 < n$, $1 < d_2 < n$, and $d_1 d_2 = n$. If $d_1 > \sqrt{n}$ and $d_2 > \sqrt{n}$, then

$$n = d_1 d_2 > \sqrt{n}\sqrt{n} = n,$$

which is impossible. Thus one of d_1 and d_2 is less than or equal to $\sqrt{n}$, as required. ■

The above result can be strengthened as follows.

Lemma 2.4 *If n is composite, then it has a prime divisor less than or equal to $\sqrt{n}$.*

Proof omitted – try it on your own.

The following simple lemma will be used very often. Note that this result holds only if p is prime; if p is not prime, the conclusion may be false. (E.g., take $p = 6$, $a = 3$, $b = 4$.)

Lemma 2.5 *If p is prime and $p | ab$, then $p | a$ or $p | b$.*

Proof.
Since p is prime, its only positive divisors are 1 and p. Thus

$$(p, a) = p \quad \text{or} \quad (p, a) = 1.$$

If $(p, a) = p$, then $p | a$ and we are done.
If $(p, a) = 1$, then by Corollary 1.1, $p | b$ and again we are done. ■

More generally:

Lemma 2.6 *If p is prime and $p|a_1a_2...a_k$, then $p|a_i$ for some $i \in \{1, 2, ..., k\}$.*

Proof. (By induction)
The result is obviously true if $k = 1$, and Lemma 2.5 shows that it is true if $k = 2$.

Suppose the result is true if $k = r$, that is, assume that if p is prime and $p|a_1a_2...a_r$, then $p|a_i$ for some $i \in \{1, 2, ..., r\}$.

Now assume $p|a_1a_2...a_ra_{r+1}$. Then $p|(a_1a_2...a_r)a_{r+1}$. By Lemma 2.5, $p|a_1a_2...a_r$ or $p|a_{r+1}$.

In the first case, $p|a_i$ for some $i \in \{1, 2, ..., r\}$, by the induction hypothesis. In the second case, $p|a_i$ for $i = r + 1$. In either case $p|a_i$ for some $i \in \{1, 2, ..., r + 1\}$ and the result follows by the principle of induction. ■

Lemma 2.7 *If p and q_1, q_2, ..., q_n are prime and $p|q_1q_2...q_n$, then $p = q_i$ for some $i \in \{1, 2, ..., n\}$.*

Proof omitted – try it on your own.

2.2 The Unique Factorization Theorem

also known as

The Fundamental Theorem of Arithmetic

Theorem 2.2 *Every integer $n \geq 2$ can be written as a product of primes in one and only one way.*

Proof (Induction – strong form).
By Lemma 2.2, every integer $n > 1$ can be written as a product of primes, and we only have to prove that this can be done in a unique way (except for the order of the primes).

Clearly, 2 can be written in only one way as a product of primes.

For a given integer $k \geq 2$, suppose every integer $r \in \{2, 3, ..., k\}$ can be written in only one way as a product of primes, and consider $k + 1$.

Say

$$k + 1 = p_1 p_2 ... p_s \ \text{ and } \ k + 1 = q_1 q_2 ... q_t,$$

where each p_i, $i = 1, 2, ..., s$, and each q_j, $j = 1, 2, ..., t$ is prime. Clearly, $p_1 | p_1 p_2 ... p_s$ and so $p_1 | q_1 q_2 ... q_t$. By Lemma 2.7, $p_1 = q_j$ for some index j. Dividing by p_1, we get

$$(k + 1)/p_1 = p_2 ... p_s = q_1 q_2 ... q_{j-1} q_{j+1} ... q_t.$$

But $p_2 ... p_s < k+1$ and by the induction hypothesis, its prime decomposition is unique. Thus the factors $q_1, q_2, ..., q_{j-1}, q_{j+1}, ..., q_t$ are just a rearrangement of $p_2, ..., p_s$. Since $p_1 = q_j$, the integers $q_1, q_2, ..., q_t$ are just a rearrangement of $p_1, p_2, ..., p_s$ and the proof that $k + 1$ can be written in only one way as a product of primes is complete.

By the principle of induction, any integer $n > 1$ can be written uniquely as a product of primes. ■

Alternative Proof. Suppose the result is not true. By the Well Ordering Principle there exists a smallest integer n for which it is false. Then n can be factored as

$$n = p_1 p_2 ... p_k = q_1 q_2 ... q_m,$$

where all the p_i's are primes such that $p_1 \leq p_2 \leq \cdots \leq p_k$, and all the q_j's are primes such that $q_1 \leq q_2 \leq \cdots \leq q_m$, and either $k \neq m$, or $k = m$ but $p_i \neq q_i$ for some $i \in \{1, 2, ..., m\}$. After cancelling all equal factors on both sides of the equation, we either have an equation saying that the product of some primes is equal to 1, which is impossible, or an equation of the form

$$r_1 r_2 ... r_{k'} = s_1 s_2 ... s_{m'},$$

where $\{r_1, r_2, ..., r_{k'}\} \cap \{s_1, s_2, ..., s_{m'}\} = \varnothing$. Then $r_1 | r_1 r_2 ... r_{k'}$ and thus $r_1 | s_1 s_2 ... s_{m'}$. By Lemma 2.7, $r_1 = s_i$, a contradiction. ■

We call the product $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$, where each p_i is prime, all the p_i's are distinct and (usually) each e_i is positive, the **prime-power decomposition** of n. If in addition $p_1 < p_2 < ... < p_k$, we call $n = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}$ the **canonical form** or **standard form** of n.

This gives another way of determining the greatest common divisor of two integers:

Theorem 2.3 *If $e_i \geq 0$, $f_i \geq 0$ $(i \in \{1, 2, ..., k\})$, and*

$$m = p_1^{e_1} p_2^{e_2} ... p_k^{e_k}, \qquad n = p_1^{f_1} p_2^{f_2} ... p_k^{f_k},$$

then

$$(m, n) = p_1^{g_1} p_2^{g_2} ... p_k^{g_k},$$

where $g_i = \min(e_i, f_i)$, $i \in \{1, 2, ..., k\}$.

Although there are infinitely many primes, little is known about their distribution within the positive integers. The difference between two consecutive odd primes can be as small as 2, like between 3 and 5, 5 and 7, 11 and 13, 1,000,000,000,061 and 1,000,000,000,063.

- Two primes p and q such that $|p - q| = 2$ are called **twin primes**.

It is unknown whether there are infinitely many pairs of twin primes. The general guess is that there are, but it also looks as if they become more scarce as the integers increase. At present it can be proved that there are infinitely many prime pairs whose difference is no greater than 246. The largest known twin primes are

$$2996863034895.21290000 \pm\ 1;$$

they have 388, 342 decimal digits and were discovered in September 2016 by Tom Greer, a contributor to PrimeGrid, a massive online project that allows anyone with a computer to join the search for large prime numbers. See https://www.sciencenewsforstudents.org/article/two-numbers-set-record-and-not-just-being-book-length.

There also exist arbitrary long intervals in the sequence of integers without any primes. More precisely, given any positive integer n, there exist n consecutive integers, all of which are composite:

$$(n + 1)! + 2, \quad (n + 1)! + 3, \quad ..., \quad (n + 1)! + (n + 1).$$

The largest confirmed gap (number of composite numbers) between *known* consecutive prime numbers is 1, 113, 106, and falls between two primes with 18, 662 digits. It was discovered by P. Cami, M. Jansen and J. K. Andersen in 2013. The largest known prime gap with identified *probable* prime gap ends has length 4, 680, 156, with 99, 750-digit probable primes found by M. Raab in 2016.

Another famous unsolved problem concerning prime numbers is the

Goldbach Conjecture: Any even integer bigger than 2 can be written as the sum of two primes.

This has been verified for a large number of even integers; certainly for every even integer up to $4 \cdot 10^{14}$. For large even integers amongst these there are *thousands* of ways of writing them as a sum of two primes, but a general proof remains elusive.

It has also been proved that every even integer can be written as a sum $p + m$, where p is prime and m is either prime or the product of two prime numbers.

A good web site for primes: www.utm.edu/research/primes.

Section 3

Linear Diophantine Equations

Diophantine equations are equations where the solutions must come from a restricted class of numbers. They are named after the Greek mathematician Diophantus, c. 250, who wrote the *Arithmetica*, the earliest known book on algebra.

A **linear Diophantine equation** is an equation of the form

$$ax + by = c,$$

where a, b and c are known, fixed integers, and we want solutions where x and y are integers.

Lemma 3.1 *If $(x, y) = (x_0, y_0)$ is a solution of $ax+by = c$, then so is $(x, y) = (x_0+bt, y_0-at)$ for any integer t.*

Proof.
Since (x_0, y_0) is a solution of $ax + by = c$, we have

$$ax_0 + by_0 = c. \tag{3.1}$$

Now,

$$\begin{aligned} a(x_0 + bt) + b(y_0 - at) &= ax_0 + abt + by_0 - abt \\ &= ax_0 + by_0 \\ &= c \qquad\qquad \text{by (3.1)}, \end{aligned}$$

so $x = x_0 + bt$ and $y = y_0 - at$ also satisfy $ax + by = c$. ■

Lemma 3.2 *Let $d = (a, b)$. The equation $ax + by = c$ has integer solutions if and only if $d|c$.*

Proof.
Suppose there are integers x_0 and y_0 such that $ax_0 + by_0 = c$. Since $d|a$ and $d|b$, d divides the left hand side of $ax_0 + by_0 = c$ and thus d also divides c.
Conversely, suppose $d|c$. Then $c = dm$ for some $m \in \mathbb{Z}$. By Theorem 1.4 there are integers r, s such that

$$ar + bs = d.$$

Multiply both sides by m:

$$a(rm) + b(sm) = dm = c,$$

so $x = rm$ and $y = sm$ is a solution. ■

Lemma 3.3 *Suppose $a, b \neq 0$, $\underline{(a, b) = 1}$ and $(x, y) = (x_0, y_0)$ is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by*

$$\left.\begin{array}{l} x = x_0 + bt \\ y = y_0 - at \end{array}\right\}, \text{ where } t \in \mathbb{Z}.$$

Proof. By Lemma 3.2 the equation does have a solution because $(a, b) = 1$ and $1|c$ for all c. We also know by Lemma 3.1 that if $(x, y) = (x_0, y_0)$ is a solution, then $(x, y) = (x_0 + bt, y_0 - at)$ is a solution for any $t \in \mathbb{Z}$.
Consider any solution $(x, y) = (r, s)$ of $ax + by = c$, thus

$$ar + bs = c. \tag{3.2}$$

Also, since (x_0, y_0) is a solution, we have

$$ax_0 + by_0 = c. \tag{3.3}$$

We must prove that $r = x_0 + bt$ and $s = y_0 - at$ for some integer t. Now, from (3.2) and (3.3),

$$0 = a(x_0 - r) + b(y_0 - s). \tag{3.4}$$

Because $a|0$ and $a|a(x_0 - r)$, it follows that $a|b(y_0 - s)$. But $(a, b) = 1$, so by Corollary 1.1, $a|(y_0 - s)$ and so there is an integer t such that

$$at = y_0 - s. \tag{3.5}$$

Substitution in (3.4) gives

$$a(x_0 - r) + bat = 0$$

$$\text{i.e.} \qquad x_0 - r + bt = 0. \tag{3.6}$$

Hence from (3.5) and (3.6),

$$s = y_0 - at \qquad \text{and} \qquad r = x_0 + bt$$

as required. ■

Lemmas 3.1 – 3.3 can be summarized as follows:

Theorem 3.1 *The linear diophantine equation $ax + by = c$ has no solution if $(a, b) \nmid c$. If $(a, b)|c$, there are infinitely many solutions,*

$$x = r + \frac{b}{(a,b)}t, \quad y = s - \frac{a}{(a,b)}t,$$

where $(x, y) = (r, s)$ is any solution and t is an integer.

Example Find all the solutions in positive integers to $6x + 15y = 51$.

Solution This is equivalent to finding the solutions of $2x + 5y = 17$. (Always divide both sides of the equation by (a, b) if $(a, b) > 1$.) We have

$$x = \frac{17 - 5y}{2}.$$

We want x to be an integer, so $5y$ must be odd, that is, y is odd. Choose $y = 1$. Then $x = 6$, so one solution is $(x, y) = (6, 1)$. In general $(x, y) = (6 + 5t, 1 - 2t)$, where t is an integer such that $6 + 5t > 0$ and $1 - 2t > 0$, that is, $t \geq -1$ and $t \leq 0$. Thus the only other solution in positive integers is $(x, y) = (1, 3)$.