Chapter 1 Preliminaries

Section 1.1. Mathematical Induction

The Well-Ordering Principle: Every nonempty set S of non-negative integers contains a least element. That is, there is some $a \in S$ such that $a \leq b$ for all $b \in S$.

We will assume ~~that~~ the Well-ordering Principle is true: That is, it is an axiom.

Theorem 1.1. (The Archimedean Property). If a and b are positive integers, then there exists a positive integer n such that $na \geq b$.

Proof. We proceed by contradiction, and so assume there are positive integers a and b such that $na < b$ for every positive integer n. Then

$$S = \{ b - na : n \text{ is a positive integer} \}$$

consists of positive integers. By the Well-Ordering Principle, S has a least element, say $b - ma$. Then $b - (m+1)a$ is also in S as S contains all integers of the form $b - na$. Then

$$b - (m+1)a = b - ma - a < b - ma$$

which contradicts $b - ma$ being the smallest integer in S. □

This property is named for Archimedes, who stated it in one of his books. Marcus Claudius Marcellus

Theorem 1.2. (First Principle of Finite Induction AKA Weak Induction). Let S be a set of positive integers such that

a) $1 \in S$

b) Whenever $k \in S$, then $k+1 \in S$.

Then S is the set of all positive integers.

Proof. Let T be the set of all positive integers not in S, and assume $T \neq \emptyset$. By the Well-Ordering Principle, T has a least element, say a. As $1 \in S$, $a > 1$ and so $0 < a-1 < a$. By choice of a, $a - 1 \in S$. But then $a - 1 + 1 = a \in S$, a contradiction. □

Example. Show $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Proof. We use strong induction. First if $n=1$, the

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$$

so the formula holds for $n=1$. Assume $\underbrace{\sum_{i=1}^{n} i = \frac{n(n+1)}{2}}^{\text{induction hypothesis}}$. The

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + n+1 = \underbrace{\frac{n(n+1)}{2}}_{\text{by induction hypothesis}} + n+1 = \frac{n(n+1)+2(n+1)}{2} = \frac{n^2+n+2n+2}{2} = \frac{n^2+3n+2}{2} = \underbrace{\frac{(n+1)(n+2)}{2}}_{\text{formula when } n \text{ is replaced by } n+1}$$

□.

So the formula is true for all positive integers n.

Second Principle of Induction or Strong Induction.

Let S be a set of positive integers such that

a) $1 \in S$

b) If k is a positive integer such that $1, 2, \ldots, k$ is in S, then $k+1 \in S$.

Then S is the set of all positive integers.

Example 1.1 Consider the Lucas sequence $1, 3, 4, 7, 11, 18, 29, 47, 76, \ldots$. These can be defined inductively by setting $a_1 = 1, a_2 = 3$, and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$.

We will show that $a_n < \left(\frac{7}{4}\right)^n$. For $n = 1, 2$ we have

$$1 < \left(\frac{7}{4}\right)^1 \text{ and } 2 < \left(\frac{7}{4}\right)^2 = \frac{49}{16}.$$

For the induction hypothesis, assume $a_i < \left(\frac{7}{4}\right)^i$ for all $1 \leq i \leq n$. The

$$\begin{aligned} a_{n+1} &= a_n + a_{n-1} \\ &< \left(\frac{7}{4}\right)^n + \left(\frac{7}{4}\right)^{n-1} \\ &= \left(\frac{7}{4}\right)^{n-1}\left[\frac{7}{4}+1\right] \\ &= \left(\frac{7}{4}\right)^{n-1}\left(\frac{11}{4}\right) \\ &< \left(\frac{7}{4}\right)^{n-1}\left(\frac{7}{4}\right)^2 = \left(\frac{7}{4}\right)^{n+1}. \end{aligned}$$

□

By weak induction the inequality holds for all positive integers.

Example Show $1+4+7+\ldots+3n-2 = \frac{n(3n-1)}{2}$.

For $n=1$, $\frac{1(3(1)-1)}{2} = \frac{1 \cdot 2}{2} = 1$, so the formula holds for $n=1$. Assume

$\underbrace{1+4+7+\ldots+3n-2 = n\frac{(3n-1)}{2}}_{\text{Induction hypothesis}}$, and consider $1+4+7+\ldots+3n-2+3(n+1)-2$.

By the induction hypothesis, this is

$$\frac{n(3n-1)}{2} + 3(n+1) - 2 = \frac{n(3n-1)}{2} + 3n + 1$$

$$= \frac{3n^2 - n}{2} + \frac{6n+2}{2}$$

$$= \frac{3n^2+5n+2}{2} = \frac{(n+1)(3n+2)}{2} = \frac{(n+1)(3(n+1)-1)}{2},$$

and the formula holds for all positive integers n by induction. ☐.

§1.2. The Binomial Theorem

Recall that for a positive integer n, $n! = 1\cdot 2\cdot 3\cdot \ldots \cdot n$, and we define $0! = 1$.
So $5! = 5\cdot 4\cdot 3\cdot 2\cdot 1 = 120$, $6! = 6\cdot 5! = 6\cdot 120 = 720$, etc.

Definition. A binomial coefficient is defined as

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!} \qquad \text{(read "n choose k")}$$

where $0 \le k \le n$. Note

$$\binom{n}{k} = \frac{n(n-1)\ldots(k+1)}{(n-k)!} = \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k!},$$

by cancelling a term in the denominator.

Example $\binom{9}{5} = \dfrac{9!}{5!\,(9-5)!} = \dfrac{9!}{5!\,4!} = \dfrac{9\cdot 8\cdot 7\cdot 6\cdot 5!}{5!\,4!} = \dfrac{9\cdot \cancel{8}^{2}\cdot \cancel{7}\cdot \cancel{6}}{\cancel{4}\cdot\cancel{3}\cdot\cancel{2}\cdot 1} = 126.$

Pascal's Rule: $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}, \quad 1 \le k \le n.$

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-(k-1))!}$$

$$= \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!}$$

$$= \frac{n!\,(n-k+1)}{k!\,(n-k+1)!} + \frac{n!\cdot k}{k!\,(n-k+1)!}$$

$$= \frac{n!\,(n+1-k) + n!\,k}{k!\,(n-k+1)!} = \frac{(n+1)! - n!\,k + n!\,k}{k!\,(n-k+1)!}$$

$$= \frac{(n+1)!}{k!\,(n+1-k)!} = \binom{n+1}{k}.$$

This gives Pascal's Triangle:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \vdots & & & & &
\end{array}$$

Note

$$\left.\begin{aligned}(a+b)^0 &= 1\\ (a+b)^1 &= a+b\\ (a+b)^2 &= a^2+2ab+b^2\\ (a+b)^3 &= a^3+3a^2b+3ab^2+b^3\\ (a+b)^4 &= a^4+4a^3b+6a^2b^2+4ab^3+b^3\end{aligned}\right\}$$ Coefficients are the same as in Pascal's triangle.

etc.

We will show $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$ by induction. When $n=1$, our formula is $(a+b)^1 = \sum_{k=0}^{1} \binom{1}{k} a^{1-k} b^k = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1 = a+b$ is true.

So we assume $\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = (a+b)^n$, and consider

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k+1} b^k + \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^{k+1}$$

$$= \binom{n}{0} a^{n+1} + \binom{n}{1} a^n b + \binom{n}{2} a^{n-1} b^2 + \dots + \binom{n}{n-1} a^2 b^{n-1} + \binom{n}{n} a b^n$$
$$+ \binom{n}{0} a^n b + \binom{n}{1} a^{n-1} b^2 + \dots + \binom{n}{n-2} a^2 b^{n-1} + \binom{n}{n-1} a b^n + \binom{n}{n} b^{n+1}$$

$$= \binom{n}{0} a^{n+1} + \left[\binom{n}{1}+\binom{n}{0}\right] a^n b + \left[\binom{n}{2}+\binom{n}{1}\right] a^{n-1} b^2 + \dots + \left[\binom{n}{n-1}+\binom{n}{n-2}\right] a^2 b^{n-1} + \left[\binom{n}{n}+\binom{n}{n-1}\right] a b^n + b^{n+1}$$

Apply Pascal's Rule $$= a^{n+1} + \binom{n+1}{1} a^n b + \binom{n+1}{2} a^{n-1} b^2 + \dots + \binom{n+1}{n-1} a^2 b^{n-1} + \binom{n+1}{n} a b^n + b^{n+1}$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{n+1-k} b^k.$$

So the binomial Theorem is true by induction.

Example $(x+2y)^4 = \binom{4}{0} x^4 + \binom{4}{1} x^3 (2y)^1 + \binom{4}{2} x^2 (2y)^2 + \binom{4}{3} x (2y)^3 + \binom{4}{4} (2y)^4$

$$= x^4 + 4x^3(2y) + 6x^2 \cdot 4y^2 + 4x \cdot 8y^3 + 16y^4$$

$$= x^4 + 8x^3y + 24x^2y^2 + 32xy^3 + 16y^4.$$

What is sum along a row?

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
\qquad
\begin{array}{l}
= 1 = 2^0 \\
= 2 = 2^1 \\
= 4 = 2^2 \\
= 8 = 2^3 \\
= 16 = 2^4 \\
= 32 = 2^5.
\end{array}
$$

How to prove? What is $(1+1)^n$? It is

$$\sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k = \sum_{k=0}^{n} \binom{n}{k} = 2^n!$$

Many, many, binomial identities!

Chapter 2.

Divisibility Theory in the Integers

§2.2 The Division Algorithm.

Theorem 2.1. (The Division Algorithm) Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying

$$a = qb + r \qquad 0 \leq r < b.$$

The integers q and r are the quotient and remainder in the division of a by b.

Proof. We first show $S = \{a - xb : x \text{ is an integer and } a - xb \geq 0\} \neq \emptyset$. It suffices to give a value of x where $a - xb \geq 0$. As $b > 0$, $|a| b \geq |a|$ so

$$a - (-|a| b) = a + |a| b \geq a + |a| \geq 0.$$

So, for $x = -|a|$, $a - xb \in S$. By the Well-Ordering Principle, S contains a smallest positive integer r. By definition, there is an integer q such that

$$r = a - qb, \quad 0 \leq r.$$

We next show $r < b$. If not, then $r \geq b$ and

$$a - (q+1)b = (a - qb) - b = r - b \geq 0.$$

But $a - (q+1)b$ is of the form to be in S, contradicting our choice of r as the smallest element in S. So $r < b$.

To show uniqueness of q and r, we use the standard way of assuming there are two then showing they are equal. So suppose

$$a = qb + r = q'b + r'$$

where $0 \leq r < b$, $0 \leq r' < b$. Then $r' - r = b(q - q')$ and

$$|r' - r| = b|q - q'|.$$

Adding the two inequalities $-b < -r \leq 0$ and $0 \leq r' < b$, we get $-b < r' - r < b$ or $|r' - r| < b$. So $b|q - q'| < b$ or $0 \leq |q - q'| < 1$. The only way this can happen is if $q = q'$. This gives $r = r'$. $\square$

Corollary. If a and b are integers with $b \neq 0$, then there exist unique integers q and r such that

$$a = qb + r, \quad 0 \le r < |b|.$$

Proof. This is true by the Division Algorithm if $b > 0$ so we need only consider when $b < 0$. Then $|b| > 0$ and by the Division Algorithm there are unique integers q' and r for which

$$a = q'|b| + r, \quad 0 \le r < |b|.$$

As $|b| = -b$, let $q = -q'$ to get $a = qb + r$ with $0 \le r < |b|$. $\square$

Examples. Let $a = -17$, $b = 5$. Then $-17 = (-4)(5) + 3$.

$a = 23$, $b = 4$. Then $23 = 5(4) + 3$

$a = 41$, $b = 8$. Then $41 = 5 \cdot 8 + 1$

$a = 17$, $b = -6$. Then $17 = -3(-6) - 1$

$a = 24$, $b = -7$. Then $24 = -3(-7) + 3$.

Example The square of an integer has remainder 0 or 1 after division by 4.

· If $a = 2q$ then $a^2 = 4q^2$ and so has remainder 0 after division by 4.

If $a = 2q+1$ then $a^2 = (2q+1)^2 = 4q^2 + 4q + 1 = 4(q^2+q) + 1$ and has remainder 1 after division by 4.

Example. The square of an odd integer is of the form $8k+1$.

By the Division algorithm, any integer can be written as $4q$, $4q+1$, $4q+2$, or $4q+3$. Only $4q+1$ and $4q+3$ are odd. Their squares are

$$(4q+1)^2 = 16q^2 + 8q + 1 = 8(2q^2+q) + 1$$

$$(4q+3)^2 = 16q^2 + 24q + 9 = 16q^2 + 24q + 8 + 1 = 8(2q^2+3q+1) + 1.$$

Example 2.1. For $a \ge 1$, $a(a^2+2)/3$ is an integer.

Every integer is of the form $3q$, $3q+1$, or $3q+2$. Considering each case seperately, we see

If $a = 3q$ then

$$\frac{a(a^2+2)}{3} = \frac{3q(9q+2)}{3} = q(9q+2)$$

if $a = 3q+1$ then

$$\frac{a(a^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3} = \frac{(3q+1)(9q^2+6q+1+2)}{3}$$

$$= \frac{(3q+1)\cdot 3(3q^2+2q+1)}{3} = (3q+1)(3q^2+2q+1).$$

if $a = 3q+2$, then

$$\frac{a(a^2+2)}{3} = \frac{(3q+2)((3q+2)^2+2)}{3} = \frac{(3q+2)(9q^2+12q+4+2)}{3}$$

$$= \frac{(3q+2)\cdot 3(3q^2+4q+2)}{3} = (3q+2)(3q^2+4q+2).$$

Moral: For certain questions we can answer questions about all integers by only considering a finite number of cases!

§2.3 The Greatest Common Divisor

Definition 2.1. An integer b is divisible by an integer $a \neq 0$, written $a|b$, if there exists an integer c such that $b = ac$. We write $a \nmid b$ if b is not divisible by a.

Ex. $4 | (-20)$ as $4(-5) = -20$ while $5 \nmid 17$.

We also say a is a divisor of b, or a is a factor of b, or b is a multiple of a.

Note that if $a|b$ then $-a | b$ as if $b = ac$ then $b = (-a)(-c)$. So we usually only discuss the positive divisors of b.

Theorem 2.2. For integers a, b, c the following hold:

a) $a|0$, $1|a$, $a|a$

b) $a|1$ iff $a = \pm 1$

c) If $a|b$ and $c|d$ then $ac | bd$

d) If $a|b$ and $b|c$ then $a|c$.

e) $a|b$ and $b|a$ iff $a = \pm b$

f) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$

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

Proof. We only show f) and g).

f) If $a|b$ then there is $c \in \mathbb{Z}$ with $b = ac$. As $b \neq 0$, $c \neq 0$. Then

$$|b| = |ac| = |a||c|.$$

As $c \neq 0$, $|c| \geq 1$, whence $|b| = |a||c| \geq |a|$.

g) As $a|b$ and $a|c$ we have $b = ar$ and $c = as$ for $r, s \in \mathbb{Z}$. But then

$$bx + cy = arx + asy = a(rx + sy)$$

and as $rx + sy \in \mathbb{Z}$, $a | (bx+cy)$. ◻.

Of course, we could use induction to show if $a | b_k$, $k = 1, \dots, n$, then

$$a | (b_1 x_1 + \dots + b_n x_n).$$

Let's not, but say we did.

Defin. If $a, b \in \mathbb{Z}$ then d is a common divisor of a and b if $d \mid a$ and $b \mid d$.

As $1 \mid d$, 1 is a common divisor of a and b for every $a, b \in \mathbb{Z}$. So the set of positive common divisors of a and b is never empty. If $a = b = 0$, then this set is $\mathbb{Z}$! However, if $a \neq 0$ or $b \neq 0$, this set is finite, and so there is a greatest such integer.

Definition 2.7. Let $a, b \in \mathbb{Z}$ with $ab \neq 0$. The greatest common divisor of a and b, denoted $\gcd(a,b)$, is the positive integer d satisfying

a) $d \mid a$ and $d \mid b$

b) If $c \mid a$ and $c \mid b$, then $c \leq d$.

Example. The positive divisors of 18 are $1, 2, 3, 6, 9, 18$ and the positive divisors of -42 are $1, 2, 3, 6, 7, 14, 21, 42$. So $\gcd(18, -42) = 6$.

Note that $(-1)(-42) + (-2)18 = 6$.

Defin. For $a, b \in \mathbb{Z}$, an expression of the form $ax + by$, x, y, is called a linear combination of x and y.

Theorem 2.3. Let $a, b \in \mathbb{Z}$ with $ab \neq 0$. Then there exists $x, y \in \mathbb{Z}$ such that

$$\gcd(a,b) = ax + by.$$

Proof. Let

$$S = \{au + bv : au + bv > 0,\ u, v \in \mathbb{Z}\}.$$

Note $S \neq \emptyset$ as if $a \neq 0$ then $|a| = au + b \cdot 0 \in S$ with $u = \pm 1$ depending on whether $a > 0$ or $a < 0$. By the Well-Ordering Principle, S contains a smallest element d. So there exist $x, y \in S$ with $ax + by = d$. We claim $d = \gcd(a,b)$.

By the Division Algorithm for $\mathbb{Z}$ there are integers q, r such that $a = qd + r$, $0 \leq r < d$. Then

$$r = a - qd = a - q(ax + by)$$

$$= a(1 - qx) + b(-qy).$$

If $r > 0$, then $r \in S$ and $r < d$, a contradiction to our choice of d. So $r = 0$.

So $a = qd$, and $d \mid a$. Similarly, $d \mid b$, so d is a common divisor of a and b.

Let c be a positive common divisor of a and b. By Theorem 2.2. (g), $c \mid (ax+by)$ or $c \mid d$. By Theorem 2.2. (f) $c = |c| \leq |d| = d$, so d is d is at least every common divisor of a and b. ∎

We will see an algorithm to calculate $\gcd(a,b)$ later.

<u>Corollary</u>. If a and $b \in \mathbb{Z}$, $ab \neq 0$, then

$$T = \{ax+by : x, y \in \mathbb{Z}\}$$

is the set of all multiples of $d = \gcd(a,b)$.

<u>Proof</u>. As $d \mid a$ and $d \mid b$, $d \mid (ax+by)$ for all $x, y \in \mathbb{Z}$. So every element of T is a multiple of d. Conversely, write $d = ax_0 + by_0$, so that any multiple of d is of the form

$$nd = n(ax_0+by_0) = a(nx_0) + b(ny_0).$$

So nd is a linear combination of a and b, and so in T. ∎

<u>Definition 2.3</u>. Let $a, b \in \mathbb{Z}$, $ab \neq 0$. Then a and b are relatively prime, or coprime, if $\gcd(a,b) = 1$.

<u>Theorem 2.4</u>. Let $a, b \in \mathbb{Z}$, with $ab \neq 0$. Then a and b are relatively prime iff there are $x, y \in \mathbb{Z}$ such that $1 = ax + by$.

<u>Proof</u>. If $\gcd(a,b) = 1$, then there are $x, y \in \mathbb{Z}$ with $ax+by = 1$ by Theorem 2.3.
Conversely, suppose $ax+by = 1$, and set $d = \gcd(a,b)$. As $d \mid a$, $d \mid b$, by Theorem 2.2, $d \mid (ax+by)$ or $d \mid 1$. So $d = \pm 1$ and as $d > 0$, $d = 1$. ∎

<u>Corollary 1</u>. If $\gcd(a,b) = d$ then $\gcd(a/d, b/d) = 1$.

<u>Proof</u>. Of course, $a/d, b/d \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$ with $\gcd(a,b) = d = ax+by$. Then

$$1 = \frac{a}{d}x + \frac{b}{d}y$$

As a/d and b/d are integers, the rest follows by Theorem 2.4. ∎

Corollary 2. If $a|c$ and $b|c$ with $\gcd(a,b)=1$, then $ab|c$.

Proof. As $a|c$ and $b|c$, there are integers r,s such that $c=ar=bs$. As $\gcd(a,b)=1$, there are integers x,y such that $1=ax+by$. So

$$c=c\cdot 1=c(ax+by)=acx+bcy$$

$\therefore\ c=a(bs)x+b(ar)y=ab(sx+ry)$.

$\therefore\ ab|c$.

Theorem 2.5. (Euclid's Lemma) If $a|bc$ and $\gcd(a,b)=1$, then $a|c$.

Proof. Write $1=ax+by$ for $x,y\in\mathbb{Z}$. Then

$$c=(ax+by)c=acx+bcx.$$

As $a|ac$ and $a|bc$, $a\,|\,(acx+bcx)$ or $a|c$. $\square$

Theorem 2.6. Let $a,b\in\mathbb{Z}$, $ab\neq 0$. For a positive integer d, $d=\gcd(a,b)$ iff

(a) $d|a$, $d|b$

(b) Whenever $c|a$ and $c|a$, then $c|d$.

Proof. Suppose $d=\gcd(a,b)$. Then $d|a$, $d|b$. By Theorem 2.3, $d=ax+by$ for some $x,y\in\mathbb{Z}$. So, if $c|a$ and $c|b$ then $c|(ax+by)$ or $c|d$.

Conversely, let d satisfy a) and b). Let c be a common divisor of a and b. Then $c|d$ by (b). Then $d\geq c$ and $g=\gcd(a,b)$ $\square$.

This statement is often taken as the definition of $\gcd(a,b)$.

§2.4. The Euclidean Algorithm.

Let $a, b \in \mathbb{Z}$. As $\gcd(|a|,|b|) = \gcd(a,b)$, we may assume $a \geq b > 0$. Apply the Division Algorithm to obtain

$$a = q_1 b + r_1, \quad 0 \leq r_1 < b.$$

If $r_1 = 0$, then $b \mid a$ and $\gcd(a,b) = b$. If $r_1 \neq 0$ divide b by r_1 to obtain q_2, r_2 such that

$$b = q_2 r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

If $r_2 = 0$, then we are finished (and $r_1 = \gcd(a,b)$). The division process continues until some nonzero remainder is obtained (which will happen as the remainders are a strictly decreasing sequence of positive integers). The result is the system of equations

$$\begin{aligned}
a &= q_1 b + r_1 & 0 &< r_1 < b \\
b &= q_2 r_1 + r_2 & 0 &< r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 & 0 &< r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

and $r_n = \gcd(a,b)$.

<u>Lemma</u>. If $a = qb + r$, then $\gcd(a,b) = \gcd(b,r)$.

<u>Proof</u>. Set $d = \gcd(a,b)$. Then $d \mid a$ and $d \mid b$ give $d \mid (a - qb)$ or $d \mid r$. So d is a common divisor of b and r. If c is a common divisor of b and r, then $c \mid (qb + r)$, so $c \mid a$. So c is a common divisor of a and b so $c \leq d$. $\square$

The Euclidean algorithm then works as

$$\gcd(a,b) = \gcd(b,r_1) = \gcd(r_1,r_2) = \ldots = \gcd(r_{n-1},r_n) = \gcd(r_n,0) = r_n$$

Example 2.3. Find gcd (12,378, 3054)

$12378 = 4 \cdot 3054 + 162$

$3054 = 18 \cdot 162 + 138$

$162 = 1 \cdot 138 + 24$

$138 = 5 \cdot 24 + 18$

$24 = 1 \cdot 18 + 6$

$18 = 3 \cdot 6 + 0$

$$\begin{array}{r} 4 \\ 3054\overline{)12378} \\ 12216 \\ \hline 162 \end{array} \qquad \begin{array}{r} 18 \\ 162\overline{)3054} \\ 162 \\ \hline 1434 \\ 1296 \\ \hline 138 \end{array} \qquad \begin{array}{r} 1 \\ 138\overline{)162} \\ 138 \\ \hline 24 \end{array} \qquad \begin{array}{r} 5 \\ 24\overline{)138} \\ 120 \\ \hline 18 \end{array} \qquad \begin{array}{r} 1 \\ 18\overline{)24} \\ 18 \\ \hline 6 \end{array} \qquad \begin{array}{r} 3 \\ 6\overline{)18} \\ 18 \\ \hline 0 \end{array}$$

$18 = 130 - 5 \cdot 24$

$24 = 162 - 1 \cdot 138$

$138 = 3054 - 18 \cdot 162$

$162 = 12378 - 4 \cdot 3054$

So gcd (12,378, 3054) = 6. Also

$$\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (130 - 5 \cdot 24) \\
&= -138 + 6 \cdot 24 \\
&= -138 + 6(162 - 1 \cdot 138) \\
&= -138 + 6 \cdot 162 - 6 \cdot 138 \\
&= -7 \cdot 138 + 6 \cdot 162 \\
&= -7(3054 - 18 \cdot 162) + 6 \cdot 162 \\
&= -7 \cdot 3054 + 126 \cdot 162 + 6 \cdot 162 \\
&= -7 \cdot 3054 + 132 \cdot 162 \\
&= -7 \cdot 3054 + 132(12{,}378 - 4 \cdot 3054) \\
&= 132 \cdot 12{,}378 - 7 \cdot 3054 - 528 \cdot 3054 \\
&= 132 \cdot 12378 - 535 \cdot 3054
\end{aligned}$$

$\therefore 6 = \gcd(12378, 3054) = 132 \cdot 12378 - 535 \cdot 3054.$

There are other possibilities though for the linear combination. Gabriel Lamé (1795-1870) proved that the number of steps in the Euclidean Algorithm is at most 5 times the number of digits in the smaller number. So for our example this gives 20

The Euclidean Algorithm works faster if the remainder is chosen so that it is at most $n/2$ (after being made positive, if necessary. For example

$$12378 = 4\cdot 3054 + 162$$
$$3054 = 18\cdot 162 + 138 = 19\cdot 162 - 24$$
$$162 = 7\cdot 24 - 6$$
$$24 = (-4)(-6) + 0$$

It may though produce a negative gcd (so just make it positive).

Theorem 2.7. If $k>0$ then $\gcd(ka, kb) = k\gcd(a,b)$.

Proof. In each equation for the Euclidean algorithm for a,b, multiply both sides by k to obtain:

$$\begin{aligned} ak &= q_1(bk) + r_1k & 0 < r_1k < bk \\ bk &= q_2(r_1k) + r_2k & 0 < r_2k < r_1k \\ &\vdots & \vdots \\ r_{n-2}k &= q_n(r_{n-1}k) + r_nk & 0 < r_nk < r_{n-1}k \\ r_{n-1}k &= q_{n+1}(r_nk) + 0. \end{aligned}$$

But this is the Euclidean Algorithm applied to ak and bk, so $\gcd(ak, bk) = k\gcd(a,b)$. $\square$

Corollary. For $k \neq 0$, $\gcd(ka, kb) = |k|\gcd(a,b)$.

Proof. We need only consider when $k<0$. Then $-k = |k| > 0$ and by Theorem 2.7

$$\begin{aligned} \gcd(ak, bk) &= \gcd(-ak, -bk) \\ &= \gcd(a|k|, b|k|) \\ &= |k|\gcd(a,b). \end{aligned}$$ $\square$

Def. An integer c is a common multiple of two nonzero integers a and b whenever $a|c$ and $b|c$.

Of course, 0 is a common multiple of a and b, as are ab and $-(ab)$ – and one of these last two is positive! By the Well-Ordering Principal, there is a smallest common multiple that is positive. It is the least common multiple of a and b

Definition 2.4. The least common multiple of two nonzero integers a and b, denoted $\mathrm{lcm}(a,b)$, is the positive integer m satisfying:

a) $a \mid m$ and $b \mid m$
b) if $a \mid c$ and $b \mid c$ with $c > 0$, then $m \leq c$.

Theorem 2.8. For positive integers a and b,

$$\gcd(a,b) \cdot \mathrm{lcm}(a,b) = ab.$$

Proof. Set $d = \gcd(a,b)$ and write $a = dr$, $b = ds$, for $r, s \in \mathbb{N}$. Set $m = ab/d$, so $m = as = rb$, so m is a positive common multiple of a and b.

Let c be a positive integer that is a common multiple of a and b. Set $c = au = bv$. There exists integers x, y such that $d = ax + by$. So

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx + uy$$

This gives $m \mid c$ so $m \leq c$. So $m = \mathrm{lcm}(a,b)$.

$\therefore \quad \mathrm{lcm}(a,b) = \dfrac{ab}{d} = \dfrac{ab}{\gcd(a,b)}$, and we are finished. $\square$

Corollary. For any positive integers a and b, $\mathrm{lcm}(a,b) = ab$ iff $\gcd(a,b) = 1$.

We may now calculate $\mathrm{lcm}(a,b)$ using the Euclidean algorithm! For example, we have seen $\gcd(3054, 12378) = 6$, so

$$\mathrm{lcm}(3054, 12378) = \frac{3054 \cdot 12378}{6} = 6300402.$$

§2.5 The Diophantine Equation $ax+by=c$.

Def. A Diophantine Equation is a equation of the form $ax+by=c$ where $a,b,c \in \mathbb{Z}$ and x,y are variables. A solution is a pair of integers x_0, y_0 such that $ax_0+by_0=c$.

Example The pairs $4,1$ and $-6,6$ and $10,-2$ are solutions of $3x+6y=18$ as

$$3 \cdot 4 + 6(1) = 18$$
$$3(-6) + 6(6) = 18$$
$$3(10) + 6(-2) = 18.$$

Example. $2x+10y=17$ has no solution as the left-hand side is even and the right hand side is 17.

Theorem 2.9. The linear Diophantine equation $ax+by=c$ has a solution if and only if $d \mid c$, where $d = \gcd(a,b)$. If (x_0,y_0) is any particular solution of the equation, then all others are given by

$$x = x_0 + \left(\frac{b}{d}\right)t \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

Proof. Suppose a solution of $ax+by=c$ exists with $ax_0+by_0=c$ for some $x_0,y_0 \in \mathbb{Z}$. As $d=\gcd(a,b)$, there are integers r,s for which $a=dr$ and $b=ds$. Then

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0+sy_0).$$

so $d \mid c$.

Conversely, assume $d \mid c$ with say $c=dt$. By Theorem 2.3, there are integers x_0,y_0 such that $d = ax_0+by_0$. Multiplying both sides by t we have

$$c = dt = (ax_0+by_0)t = a(tx_0) + b(ty_0)$$

So $ax+by=c$ has $x=tx_0$ and $y=ty_0$ as particular solutions.

For the second part of the Theorem, suppose x_0,y_0 is a solution of $ax+by=c$. If x', y' is another solution, then

$$ax_0 + by_0 = c = ax' + by'$$

or

$$a(x' - x_0) = b(y_0 - y').$$

By a corollary of Theorem 2.4, there are relatively prime integers r, s such that $a = dr$, $b = ds$. So

$$dr(x' - x_0) = ds(y_0 - y') \text{ or } r(x' - x_0) = s(y_0 - y').$$

Hence $r \mid s(y_0 - y')$ with $\gcd(r,s) = 1$. By Euclid's Lemma, $r \mid (y_0 - y')$ or $y_0 - y' = rt$ for some integer t. So

$$r(x' - x_0) = s(y_0 - y') = srt.$$

$$\therefore \quad x' - x_0 = st.$$

$$\therefore \quad x' = x_0 + st = x_0 + \left(\frac{b}{d}\right)t$$

and

$$y' = y_0 - rt = y_0 - \left(\frac{a}{d}\right)t.$$

Finally, substituting x' and y' into $ax + by = c$ we have

$$a\left(x_0 + \frac{b}{d}\right)t + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + \frac{abt}{d} + by_0 - \frac{abt}{d}$$

$$= ax_0 + by_0 = c. \qquad \blacksquare.$$

Example 2.4. Consider $172x + 20y = 200$. We apply the Euclidean algorithm to find $\gcd(172, 20)$.

$$\begin{array}{r} 8 \\ 20\overline{)172} \\ \underline{160} \\ 12 \end{array} \qquad \begin{array}{r} 1 \\ 12\overline{)20} \\ \underline{12} \\ 8 \end{array}$$

$172 = 8 \cdot 20 + 12$

$20 = 1 \cdot 12 + 8$

$12 = 1 \cdot 8 + 4$

$8 = 2 \cdot 4$

So $\gcd(172, 20) = 4$. As $4 \mid 200$, there is a solution!

We work backwards and express 4 as a linear combination of 172 and 20:

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2(172 - 8 \cdot 20) - 20 \end{aligned}$$

$8 = 20 - 12$

$12 = 172 - 8 \cdot 20$

$$= 2\cdot 172 - 17\cdot 20$$

We multiply both sides by 50 to obtain

$$200 = 100\cdot 172 - 850(20)$$

So $x=100$ and $y=-850$ are solutions. The other solutions are

$$x = 100 + \frac{20}{4}t \quad , \quad y = -850 - \frac{172}{4}t$$

$$x = 100 + 5t, \quad y = -850 - 43t$$

To find all positive solutions, we want

$$100 + 5t > 0 \qquad -850 - 43t > 0$$

$$5t > -100 \qquad -43t > 850$$

$$t > -20 \qquad t < \frac{850}{-43}$$

$$-20 < t < \frac{850}{-43} \quad \text{but } -\frac{850}{43} < -20 \text{ so none!}$$

Corollary. If $\gcd(a,b)=1$ and x_0, y_0 a particular solution of $ax+by=c$, then all solutions are given by

$$x = x_0 + bt, \quad y = y_0 - at.$$

Example (From 6^{th} Century China) If a cock is worth 5 coins, a hen 3 coins, and 3 chicks together one coin, how many cocks, hens, and chicks can be bought for 100 coins?

Let x = # of cocks
y = # of hens
z = # of chicks.

We have

$$5x + 3y + \frac{1}{3}z = 100$$

$$x + y + z = 100$$

$$z = 100 - x - y$$

$$5x + 3y + \frac{1}{3}(100 - x - y) = 100$$

$$15x + 9y + 100 - x - y = 300$$

$$14x + 8y = 200$$

$$7x + 4y = 100$$

This has particular solution $x=0$ and $y=25$ so

$$x = 4t \qquad y = 25-7t \quad \text{and} \quad z = 100-x-y$$
$$= 100-4t-(25-7t)$$
$$= 75+3t.$$

In order to have $x>0, y>0, z>0$, we have

$$4t>0 \qquad 25-7t>0 \qquad 75+3t>0$$
$$t>0 \qquad \frac{25}{7}>t \qquad t>-25$$

or $0<t<\frac{25}{7}$. As t is an integer, the solutions are $t=1,2,3$. Or,

$$x=4 \qquad y=18 \qquad z=78$$
$$x=8 \qquad y=11 \qquad z=81$$
$$x=12 \qquad y=4 \qquad z=84.$$

These are the solutions give by the Chinese.