Division Algorithm.

Given integers a and b, with $b > 0$, there exist unique integers q and r satisfying $a = qb + r$ $0 \le r < b$

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

Proof:

Let $S = \{a - xb \mid x \text{ an integer}; a - xb \ge 0\}$

Claim: S is nonempty.

Infact, the integer $b \ge 1 \Rightarrow |a|b \ge |a|$

$\Rightarrow a - (-|a|)b = a + |a|b \ge a + |a| \ge 0$

For the choice $x = -|a|$, then, $a - xb$ lies in S.

=> S is nonempty.

By Well-Ordering Principle, from which we infer that the set S contains a smallest integer; call it r.

By the definition of S, there exists an integer q satisfying $r = a - qb$ $0 \le r$

Claim: $r < b$.

Otherwise, if $r \ge b$ then,

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

=> the integer $a - (q + 1)b$ has the proper form to belong to the set S.

But $a - (q + 1)b = r - b < r$, a contradiction, r is the smallest member of S.

Hence, $r < b$ as claimed.

Uniqueness:

Suppose that a has two representations of the desired form, say, $a = qb + r = q'b + r'$ where $0 \le r < b$, $0 \le r' < b$.

Then $r' - r = b(q - q')$

$\Rightarrow |r' - r| = b\,|q - q'|$

Adding the two inequalities, $-b < -r \le 0$ and $0 \le r' < b$,

$\Rightarrow -b < r' - r < b$

$\Rightarrow |r' - r| < b.$

$\Rightarrow b\,|q - q'| < b,$

$\Rightarrow 0 \le |q - q'| < 1$

Because $|q - q'|$ is a nonnegative integer, the only possibility is that $|q - q'| = 0$,

$\Rightarrow q = q'$

$\Rightarrow r = r'$

$\Rightarrow$ Uniqueness.

Example

Let $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59,

$$\Rightarrow \quad 1 = 0(-7) + 1$$
$$-2 = 1(-7) + 5$$
$$61 = (-8)(-7) + 5$$
$$-59 = 9(-7) + 4$$

Remark:

If a and b are integers, with $b = 0$, then there exist unique integers q and r such that

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

Proof. It is enough to consider the case in which b is negative. Then $|b| > 0$,
=> there are unique integers q and r for which
$a = q|b| + r, \quad 0 \le r < |b|$.

Noting that $|b| = -b$, we may take $q = -q$ to arrive at $a = qb + r$, with $0 \le r < |b|$.

Let $b = -7$. Then, for the choices of $a = 1, -2, 61$, and -59,

$$
\begin{aligned}
1 &= 0(-7) + 1 \\
-2 &= 1(-7) + 5 \\
61 &= (-8)(-7) + 5 \\
-59 &= 9(-7) + 4
\end{aligned}
$$

Divisibility

An integer b is said to be divisible by a non-zero integer a, denoted by $a \mid b$, if there exists some integer c such that $b = ac$.

Properties

For integers a, b, c, the following hold:
(a) $a \mid 0$, $1 \mid a$, $a \mid a$.
(b) $a \mid 1$ if and only if $a = \pm 1$.
(c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.
(d) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(e) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.
(f) If $a \mid b$ and $b = 0$, then $|a| \leq |b|$.
(g) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.

Greatest Common Divisor (gcd)

Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following:
(a) $d \mid a$ and $d \mid b$.
(b) If $c \mid a$ and $c \mid b$, then $c \leq d$.

Example: $\gcd(-5, 5) = 5$
$\gcd(8, 17) = 1$
$\gcd(-8, -36) = 4$

Theorem:
Given integers a and b, not both of which are zero, there exist integers x and y such that $\gcd(a, b) = ax + by$

Proof.

Let $S = \{au + bv \mid au + bv > 0;\ u, v \text{ integers}\}$
Claim: S is not empty.
Infact, if $a = 0$, then the integer $|a| = au + b \cdot 0$ which lies in
We take $u = 1$ or $u = -1$ according as a is positive or negative.

By Well-Ordering Principle, S must contain a smallest element d.
=> there exist integers x and y for which $d = ax + by$.

Claim: $d = \gcd(a, b)$.

By Division Algorithm, there exists integers q and r such that $a = qd + r$, where $0 \leq r < d$.
Then r can be written in the form
$r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$.

If r were positive, then this representation would imply that r is a member of S, contradicting the fact that d is the least integer in S (recall that $r < d$).
Therefore, $r = 0$, and so $a = qd$, or equivalently $d \mid a$.
Similarly , $d \mid b$.
=> d is a common divisor of a and b.

Now if c is an arbitrary positive common divisor of the integers a and b, then $c \mid (ax + by)$;
=> $c \mid d$.
=> $c = |c| \leq |d| = d$,
=> $d = \gcd(a, b)$, as claimed.

Example: If a and b are given integers, not both zero, then prove that the set $T = \{ax + by \mid x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = \gcd(a, b)$.
(Hint: use the definition of g.c.d.)

Relatively Prime integers:

Two integers a and b, not both of which are zero, are said to be relatively prime whenever $\gcd(a, b) = 1$.

Example: 13 and 25 are relatively primes.
Theorem:
Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.
(Proof: simple one)

Note: If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.

Example:
$\gcd(-12, 30) = 6$ and $\gcd(-12/6, 30/6) = \gcd(-2, 5) = 1$

Example: If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then prove that $ab \mid c$.

Answer: As $a \mid c$ and $b \mid c$, integers r and s can be found such that $c = ar = bs$.
Now $\gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y.
Multiplying the last equation by c,
$\Rightarrow c = c \cdot 1 = c(ax + by) = acx + bcy$
$\Rightarrow c = a(bs)x + b(ar)y = ab(sx + r y)$
$\Rightarrow ab \mid c$, as desired.

Note: The condition that $\gcd(a, b)=1$ in the above example is necessary in the above example, as we can see that 6|24 and 8|24, but 6x8=48 cannot divide 24.

Euclid's lemma.

If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.

Proof:

$\gcd(a, b) = 1 \implies 1 = ax + by$, where x and y are integers.

Multiplication of this equation by c,

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

Now. $a \mid ac$ and $a \mid bc$, $\implies a \mid (acx + bcy)$

$\implies a \mid c$.

Euclidean Algorithm:

The Euclidean Algorithm may be described as follows: Let a and b be two integers whose greatest common divisor is desired. Because $\gcd(|a|, |b|) = \gcd(a, b)$, there is no harm in assuming that $a \geq b > 0$. The first step is to apply the Division Algorithm to a and b to get

$$a = q_1 b + r_1 \qquad 0 \leq r_1 < b$$

If it happens that $r_1 = 0$, then $b \mid a$ and $\gcd(a, b) = b$. When $r_1 \neq 0$, divide b by r_1 to produce integers q_2 and r_2 satisfying

$$b = q_2 r_1 + r_2 \qquad 0 \leq r_2 < r_1$$

If $r_2 = 0$, then we stop; otherwise, proceed as before to obtain

$$r_1 = q_3 r_2 + r_3 \qquad 0 \leq r_3 < r_2$$

This division process continues until some zero remainder appears, say, at the $(n+1)$th stage where r_{n-1} is divided by r_n (a zero remainder occurs sooner or later because the decreasing sequence $b > r_1 > r_2 > \cdots \geq 0$ cannot contain more than b integers).

The result is the following system of equations:

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

We argue that r_n, the last nonzero remainder that appears in this manner, is equal to $\gcd(a, b)$. Our proof is based on the lemma below.

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

Proof. If $d = \gcd(a, b)$, then the relations $d \mid a$ and $d \mid b$ together imply that $d \mid (a - qb)$, or $d \mid r$. Thus, d is a common divisor of both b and r. On the other hand, if c is an arbitrary common divisor of b and r, then $c \mid (qb + r)$, whence $c \mid a$. This makes c a common divisor of a and b, so that $c \leq d$. It now follows from the definition of $\gcd(b, r)$ that $d = \gcd(b, r)$.

Using the result of this lemma, we simply work down the displayed system of equations, obtaining
gcd(a, b) = ... = the last non-zero remainder.

Let a=12378, and b= 3054

$12378 = 4 \cdot 3054 + 162$
$3054 = 18 \cdot 162 + 138$
$162 = 1 \cdot 138 + 24$
$138 = 5 \cdot 24 + 18$
$24 = 1 \cdot 18 + 6$
$18 = 3 \cdot 6 + 0$

=> $6 = \gcd(12378, 3054)$

Substituting from back,

$$\begin{aligned}
6 &= 24 - 18 \\
&= 24 - (138 - 5 \cdot 24) \\
&= 6 \cdot 24 - 138 \\
&= 6(162 - 138) - 138 \\
&= 6 \cdot 162 - 7 \cdot 138 \\
&= 6 \cdot 162 - 7(3054 - 18 \cdot 162) \\
&= 132 \cdot 162 - 7 \cdot 3054 \\
&= 132(12378 - 4 \cdot 3054) - 7 \cdot 3054 \\
&= 132 \cdot 12378 + (-535)3054
\end{aligned}$$

Thus $6 = \gcd(12378, 3054) = 12378x + 3054y$ where $x= 132$ and $y=-535$.