Well Ordering, Division, and the Euclidean Algorithm

Let us explore some basic properties of the integers: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. We can add, subtract, and multiply integers, but that is not all. One important property of the set of integers is its well ordering principle.

Definition: [Well Ordering Principle (WOP)] Let X be a non-empty subset of $\mathbb{Z}$ such that X is bounded below (there exists some $M \in \mathbb{Z}$ such that $x \geq M$ for all $x \in X$). Then X has a minimal element – that is – there exists some $m \in X$ such that $m \leq x$ for all $x \in X$. When such an element exists, it is unique. We denote this element by $\min(X) = m$.

Notice that if X is bounded below by M, then $-M + X = \{-M + x \mid x \in X\}$ is bounded below by 0. If m is the minimum of $-M + X$ then $m + M$ is the minimum of X. Likewise, if m is the minimum of X, then $m - M$ is the minimum of $-M + X$. This means that if we wish to establish the WOP, we can just focus on sets of non-negative integers and the general case will follow.

It turns out that the WOP is logically equivalent to the Principle of Mathematical Induction (PMI).

Theorem: PMI $\Longrightarrow$ WOP

proof: Let X be a non-empty set of non-negative integers. For sake of contradiction, suppose that X has no minimum. Let $S = \{n \in \mathbb{Z}_{\geq 0} \mid n \text{ is a lower bound for } X\}$. Notice that $0 \in S$ since X is clearly bounded below by 0.

Our inductive hypothesis is that for some $n \geq 0$ we have $n \in S$. Well, this means that n is a lower bound. Thus $n \leq x$ for all $x \in X$. Notice that $n+1$ must be a lower bound as well. If not, $x_0 < n+1$ for some $x_0 \in X$. But $n \leq x_0$. Thus $n = x_0$. So x_0 is a lower bound and $x_0 \in X$. This means x_0 is the minimum of X (contradiction since we assumed X has no minimum). Thus $n+1$ must also be a lower bound, so $n+1 \in S$.

So we have shown that $0 \in S$ and if $n \geq 0$ and $n \in S$, then $n+1 \in S$. By induction we can conclude that $S = \mathbb{Z}_{\geq 0}$. This means that any element of X must be greater than all non-negative integers! Therefore, X must be empty (contradiction since we assumed X was non-empty).

We have reached our final contradiction, so we must conclude that X *does* have a minimum. $\square$

Theorem: WOP $\Longrightarrow$ PMI

proof: Let us suppose that $\varphi(n)$ is some statement such that $\varphi(0)$ is true and whenever $n \geq 0$ and $\varphi(n)$ holds, $\varphi(n+1)$ also holds. We wish to show that $\varphi(n)$ holds for all $n \geq 0$.

Consider $X = \{m \in \mathbb{Z}_{\geq 0} \mid \varphi(m) \text{ does not hold }\}$. If $\varphi(n)$ is true for all $n \geq 0$, then X is empty. For sake of contradiction, let us assume that X is non-empty. So by the WOP, X must have a minimal element, say $m \in X$. Now $m \neq 0$ since $0 \notin X$ because $\varphi(0)$ holds. Therefore, $m > 0$ and so $m = n+1$ for some $n \geq 0$. Next, $n \notin X$ (otherwise, $n \in X$ so m isn't the minimum since $n < n+1 = m$). Thus since $n \notin X$, $\varphi(n)$ holds. Therefore, by assumption, $\varphi(n+1) = \varphi(m)$ also holds. But then $m \notin X$ (contradiction).

Therefore, X must be empty. Thus $\varphi(n)$ holds for all $n \geq 0$. $\square$

We will accept that the PMI is true and so the WOP must hold as well. It turns out that a familiar result from grade school follows immediately from the WOP.

Theorem: [Division Algorithm] Let $a, b \in \mathbb{Z}$ and suppose $b \neq 0$. Then there exists unique integers $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < |b|$. We call q the *quotient* and r the *remainder*.

This is nothing more than division with remainder. One first computes quotients and remainders using repeated subtraction. This gives us a glimpse of how to prove this *very important* result.

proof: Let $X = \{a - qb \mid q \in \mathbb{Z} \text{ such that } a - qb \geq 0\}$ (we repeatedly subtract b from a). Notice that if $a \geq 0$, then $a - 0b \in X$ ($q = 0$ and $a - 0q \geq 0$). Now if $a < 0$, then, noting that $b^2 > 0$ since $b \neq 0$, we have $-ab^2 \geq -a = |a|$ so $a - ab^2 \geq 0$ thus $a - qb = a - (ab)b \in X$ (where $q = ab$ and we have that $a - (ab)b \geq 0$). All of this to say, X is non-empty.

Since X is a non-empty set of non-negative integers, by the WOP, it has a minimal element. Let's call this element r. Thus $r = a - qb \geq 0$ for some $q \in \mathbb{Z}$. It looks like we're nearly done since $a = bq + r$ and $r \geq 0$. Now suppose that $r \geq |b|$. Then notice that $0 \leq r - |b| = a - bq - |b| = q - b(q \pm 1)$ ($+$ if $b > 0$ and $-$ if $b < 0$). Thus $r - |b| \in X$ and so r is not the minimum (contradiction). Therefore, $r < |b|$ and we are done (except for uniqueness).

As is usually the case with uniqueness proofs, we assume that there are two solutions and show they are equal. Suppose $a = bq + r$ and $a = bq' + r'$ where $q, r, q', r' \in \mathbb{Z}$ and $0 \leq r, r' < |b|$. Without loss of generality, let us assume that $r \leq r'$. Notice that $0 = a - a = (bq' + r') - (bq + r) = b(q' - q) + (r' - r)$. Therefore, $b(q - q') = r' - r$. If $q - q' \neq 0$, then $b(q - q')$ must have an absolute value of at least $|b|$. But this cannot happen since $b(q - q') = r' - r < |b|$. Therefore, $q - q' = 0$ so $q = q'$. This then implies that $r' - r = b(q - q') = b(0) = 0$ so $r = r'$ as well. Thus we have shown that any pair of valid quotients and remainders must match (i.e. they're unique). $\square$

Next, we will turn our attention to greatest common divisors (and to a lesser extent, least common multiples).

Definition: Let $a, b \in \mathbb{Z}$. We say that a *divides* b, denoted $a \Big| b$, if there exists some $k \in \mathbb{Z}$ such that $ak = b$ (i.e. b is an integer multiple of a). Next, if for some $c \in \mathbb{Z}$, we have $c \Big| a$ and $c \Big| b$, then c is called a *common divisor* of a and b. Likewise, if $a \Big| c$ and $b \Big| c$, then c is a *common multiple* of a and b.

When either a or b is non-zero, the set of common divisors are bounded above by $\max\{|a|, |b|\}$, so in this case a *greatest common divisor (gcd)*, denoted $\gcd(a, b)$, exists. Likewise, when both a and b are non-zero, the set of (positive) common multiples is bounded below by $\max\{|a|, |b|\}$, so in this case a *least common multiple (lcm)*, denoted $\text{lcm}(a, b)$, exists. If either a or b is zero, define $\text{lcm}(a, b) = 0$.

Note: Sometimes books write (a, b) for $\gcd(a, b)$ and $[a, b]$ for $\text{lcm}(a, b)$.

Example: As we learn in grade school, the divisors of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$. The divisors of 15 are $\pm 1, \pm 3, \pm 5, \pm 15$. The common divisors of 12 and 15 are $\pm 1, \pm 3$. Therefore, $\gcd(12, 15) = 3$. To find the least common multiple, notice that any multiple of 12 needs two 2 factors and one 3 factor. Likewise multiples of 15 need a 3 and a 5. Thus common multiples need at least $2^2 \cdot 3 \cdot 5 = 60$. Therefore, $\text{lcm}(12, 15) = 60$. Notice that $12 \cdot 15 = \gcd(12, 15) \cdot \text{lcm}(12, 15) = 3 \cdot 60 = 180$.

Theorem: Suppose that $a, b, c \in \mathbb{Z}$ and that $a \Big| b$ and $a \Big| c$. Then a divides any integral linear combination of b and c. This means that $a \Big| mb + nc$ for any integers $m, n \in \mathbb{Z}$. In particular, $a \Big| |b|$ $\quad$ ($|b| = b$ or $(-1)b$).

proof: There exists some $k, \ell \in \mathbb{Z}$ such that $ak = b$ and $a\ell = c$. Thus $mb + nc = mak + na\ell = a(mk + n\ell)$. Since $k, \ell, m, n \in \mathbb{Z}$ we have $mk + n\ell \in \mathbb{Z}$. Thus $a \Big| mb + nc$. $\square$

Theorem: Suppose $a, b, q, r \in \mathbb{Z}$ and that $a = bq + r$. Then a, b and b, r have the same common divisors.

proof: Suppose that c is a common divisor of a and b, so $c \Big| a$ and $c \Big| b$. Then $c \Big| (1)a + (-q)b = r$ (since $r = (1)a + (-q)b$ is a integral linear combination of a and b). Thus c is a common divisor of both b and r. Likewise, if $c \Big| b$ and $c \Big| r$, then $c \Big| bq + r = a$. Thus c is a common divisor of both a and b. $\square$

As a consequence of this theorem, we have that whenever $a = bq + r$, if $\gcd(a, b)$ and $\gcd(b, r)$ exist, then $\gcd(a, b) = \gcd(b, r)$. Why? Well, a, b and b, r have the same common divisors, so they must share the same greatest common divisor.

This the key to establishing an ancient, extremely important algorithm:

Theorem: [**Extended Euclidean Algorithm**] Let $a, b \in \mathbb{Z}$ where $b \neq 0$. Set $r_0 = |b|$. Use the division algorithm to find $q_1, r_1 \in \mathbb{Z}$ such that $a = r_0 q_1 + r_1$ (where $0 \leq r_1 < r_0$). In general, if $r_n \neq 0$, divide r_{n-1} by r_n and get $q_{n+1}, r_{n+1} \in \mathbb{Z}$ such that $r_{n-1} = r_n q_{n+1} + r_{n+1}$ (where $0 \leq r_{n+1} < r_n$).

Then there exists some $N \geq 0$ such that $r_{N+1} = 0$ and the last non-zero remainder: $r_N = \gcd(a, b)$. Moreover, using the quotients and remainders from this procedure, we can find $x, y \in \mathbb{Z}$ such that $ax+by = \gcd(a, b)$.

Note: Using repeated divisions to find the greatest common divisor is known as the *Euclidean algorithm*. The process of combining the results of these divisions to build up the greatest common divisor as an integral linear combination gives us the "*extended*" part of the algorithm.

proof: Notice our remainders: $|b| = r_0 > r_1 > \cdots > r_{n-1} > r_n \geq 0$. Each remainder is smaller than the previous one. So we cannot divide more than $|b|$ times. This implies that our procedure must eventually terminate. Moreover, we must eventually get a reminader of zero. Why? If not, the set of remainders is a non-empty set of non-negative integers which must, by the WOP, have a minimal element. If this element is $r_N > 0$, we could just divide again (by r_N) and get $r_{N+1} < r_N$ so that r_N isn't actually the minimum (contradiction).

Now that we know that our algorithm terminates, seeing that it actually computes the greastest common divisor is simple. So far we have some $N \geq 0$ such that $r_N > 0$ and $r_{N+1} = 0$.

First, notice that everything divides zero: $x0 = 0$ so $x \Big| 0$. Therefore, the greatest common divisor of 0 and r_N is actually just r_N (every divisor of $r_N > 0$ must be smaller than r_N). Therefore, $\gcd(r_N, 0) = r_N$. Also, notice that b and $-b$ have the same divisors so

$$\gcd(a, b) = \gcd(a, |b|) = \gcd(a, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{N-1}, r_N) = \gcd(r_N, r_{N+1}) = \gcd(r_N, 0) = r_N$$

Finally, let $d = \gcd(a, b) = r_N$. Also, let $r_{-1} = a$ (to make our notation consistent). Then we have $r_{n-1} = r_n q_{n+1} + r_{n+1}$ for all $0 \leq n \leq N$. Therefore, $r_{n+1} = (1)r_{n-1} + (-q_{n+1})r_n$.

Set $x_N = 1$ and $y_N = -q_N$. Then $d = r_N = (1)r_{N-2} + (-q_N)r_{N-1} = x_N r_{N-2} + y_N r_{N-1}$. Now since $r_{n+1} = (1)r_{n-1} + (-q_{n+1})r_n$, we can replace r_{N-1} with $(1)r_{N-3} + (-q_{N-1})r_{N-2}$. This gives us $d = x_N r_{N-2} + y_N[(1)r_{N-3} + (-q_{N-1})r_{N-2}]$. Letting $x_{N-1} = y_N$ and $y_{N-1} = x_N - q_{N-1}y_N$, we have $d = x_{N-1}r_{N-3} + y_{N-1}r_{N-2}$. Continuing in this fashion we end up with $d = x_1 r_{-1} + y_1 r_0 = xa + yb$ letting $x = x_1$ and $y = \pm y_1$ ($r_0 = |b| = \pm b$). $\square$

Example: Consider 246 and 50. Divide 246 by 50 and get $246 = (4)50 + 46$. Now divide 50 by 46 and get $50 = (1)46 + 4$. Next, divide 46 by 4 and get $46 = (11)4 + 2$. Finally, divide 4 by 2 and get $4 = (2)2 + 0$. The last non-zero remainder is 2. Therefore, $\gcd(246, 50) = 2$.

Next, let's run backwards through our divisions. We have $2 = (1)46 + (-11)4$. Subbing in $4 = (1)50 + (-1)46$, we get $2 = (1)46+(-11)[(1)50+(-1)46] = (-11)50+(12)46$. Now subbing in $46 = (1)246+(-4)50$, we get $2 = (-11)(50) + (12)[(1)246 + (-4)50] = (12)246 + (-59)50$. Therefore, $(12)246 + (-59)50 = 2$.

Theorem: Let $a, b \in \mathbb{Z}$ not both zero. Let $d = \gcd(a, b)$. If c is a common divisor of a and b, then $c \Big| d$.

proof: By the extended Euclidean algorithm there exists some $x, y \in \mathbb{Z}$ such that $ax + by = d$. Now $c \Big| a$ and $c \Big| b$, so $c \Big| ax + by = d$ (an integral linear combination of a and b). $\square$

Theorem: Let $a, b \in \mathbb{Z}$ where both a and b are non-zero. Let $\ell = \operatorname{lcm}(a, b)$. If c is a common multiple of a and b, then $\ell \Big| c$.

proof: Note $\ell \geq \max\{|a|, |b|\} > 0$ since ℓ is a positive multiple of both a and b. Thus, using the division algorithm, we can divide c by ℓ. There exists some $q, r \in \mathbb{Z}$ such that $c = \ell q + r$ where $0 \leq r < \ell$.

Now c and ℓ are common multiples of a and b. Since $a \Big| c$ and $a \Big| \ell$, we have $a \Big| c - \ell q = r$ (an integral linear combination of c and ℓ). Likewise, $b \Big| r$. Therefore, r is a common multiple of a and b. But $0 \leq r < \ell$ and ℓ is the *least* common multiple. Therefore, r cannot be a positive common multiple. This means $r = 0$, so $c = \ell q$ which means $\ell \Big| c$. $\square$

A very useful characterization of greatest common divisors comes from their description in terms of linear combinations.

Theorem: Let $a, b \in \mathbb{Z}$ not both zero, and let $d = \gcd(a, b)$. Then $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, that is:

$$\{kd \mid k \in \mathbb{Z}\} = \{ax + by \mid x, y \in \mathbb{Z}\}$$

In other words, integral linear combinations of a and b are multiples of $\gcd(a, b)$ and conversely any multiple of $\gcd(a, b)$ is an integral linear combination of a and b. As an immediate consequence, $\gcd(a, b)$ *is the smallest positive integral linear combination of a and b.*

proof: By the extended Euclidean algorithm there exists $m, n \in \mathbb{Z}$ such that $am + bn = d$.

Let $x \in d\mathbb{Z}$. There exists some $k \in \mathbb{Z}$ such that $x = dk$. But then $x = dk = (am + bn)k = a(mk) + b(nk) \in a\mathbb{Z} + b\mathbb{Z}$. Therefore, $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.

Conversely, suppose that $x \in a\mathbb{Z}+b\mathbb{Z}$. There exists some $m, n \in \mathbb{Z}$ such that $x = am+bn$. By definition $d \Big| a$ and $d \Big| b$ (d is a common divisor). It then follows that $d \Big| am + bn = x$. Thus there is some $k \in \mathbb{Z}$ such that $x = dk$ so $x \in d\mathbb{Z}$. Therefore, $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$.

We have shown that $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$ and $a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$. Therefore, $d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$. $\square$

Example: Suppose that for some $a, b, x, y \in \mathbb{Z}$, we have $ax + by = 6$. What can we conclude about $d = \gcd(a, b)$?

We cannot conclude that $\gcd(a, b) = 6$. However, $6 = ax + by \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Therefore, $d \Big| 6$. This means that $d = 1, 2, 3$, or 6.

On the other hand if $ax + by = 1$, we can conclude that $d = \gcd(a, b) \Big| 1$ and so $\gcd(a, b) = 1$!

Definition: Let $a, b \in \mathbb{Z}$. We say that a and b are *relatively prime* if $\gcd(a, b) = 1$. The above discussion shows that a and b are relatively prime if and only if there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

Recall that if $p \in \mathbb{Z}$ and $p > 1$, then p is *prime* if its only positive divisors are 1 and p.

Theorem: [**Euclid's Lemma**] Let $a, b \in \mathbb{Z}$ and p be a prime. If $p \Big| ab$, then either $p \Big| a$ or $p \Big| b$.

proof: Suppose that $p \not\Big| a$. We need to show that $p \Big| b$.

The only positive divisors of p are 1 and p, this means that $\gcd(p, n) = 1$ or p for any $n \in \mathbb{Z}$. Since $p \not\Big| a$, $\gcd(p, a) = 1$. Therefore, a and p are relatively prime and so there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. But then $b = b(ax + py) = (ab)x + (p)by$. Now $p \Big| ab$ and, of course, $p \Big| p$, so $p \Big| (ab)x + (p)by = b$. $\square$

This leads us to the fundamental theorem of arithmetic.

Theorem: [Fundamental Theorem of Arithmetic] Let $n \in \mathbb{Z}_{>1}$. There exists primes $p_1 < \cdots < p_\ell$ and positive integers $k_1, \dots, k_\ell \in \mathbb{Z}_{>0}$ such that $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$. Moreoever, this factorization is unique.

proof: (sketch) Consider $n = 2$. Since 2 is prime, it is already factored. Let us proceed using induction.

Suppose that all integers x such that $2 \leq x < n$ have factorizations. Either n is prime (it is already factored) or n is not prime. If n isn't prime there exists some $a \in \mathbb{Z}_{>0}$ such that $a \Big| n$ and $a \neq 1$ or n. Thus there is some $b \in \mathbb{Z}_{>0}$ so that $ab = n$. Now since $a \neq 1$ or n, we have $b \neq n$ or 1.

Thus $1 < a, b < n$. By our inductive hypothesis a and b can be factored into primes. Multiplying these factorizations together yields a factorization for $n = ab$. Therefore, by induction, all $n \geq 2$ have factorizations.

Next, suppose $n = p_1^{k_1} \cdots p_\ell^{k_\ell} = q_1^{m_1} \cdots q_r^{m_r}$ are two factorizations. Then since p_ℓ clearly divides $n = p_1^{k_1} \cdots p_\ell^{k_\ell}$, it divides $q_1^{m_1} \cdots q_r^{m_r}$. Thus by Euclid's lemma p_ℓ either divides $q_1^{m_1} \cdots q_{r-1}^{m_{r-1}} q_r^{m_r - 1}$ or q_r. If it divides $q_1^{m_1} \cdots q_{r-1}^{m_{r-1}} q_r^{m_r-1}$, then it must either divide $q_1^{m_1} \cdots q_{r-1}^{m_{r-1}} q_r^{m_r-2}$ or q_r. Continuing in this fashion, we see that p_ℓ either divides $q_1^{m_1} \cdots q_{r-1}^{m_{r-1}}$ or q_r. Continuing further, we see that p_ℓ must divide one of the $q_1, \dots, q_r$. But q_i's are primes (the only divisors of q_i are 1 and q_i itself). Therefore $p_\ell = q_i$ for some i. Thus p_ℓ can be canceled off from both sides of: $p_1^{k_1} \cdots p_\ell^{k_\ell} = q_1^{m_1} \cdots q_r^{m_r}$.

Continuing in this fashion we can cancel off all of the p_i's. This leaves us with 1 on the left hand side and potentially some q_i's on the right hand side. Since any product of primes is bigger than 1, we must have canceled off all of the q_i's and so the factorizations must have matched exactly (we canceled everything in pairs)!

Note: I labeled this proof as a "sketch" since I have left out some details. For example, each time I wrote "continuing in this fashion" I should (in a more formal setting) have set up an inductive argument. Also, if we allow prime exponents to be zero, we can give 1 a "factorization" as well: $1 = 2^0$. $\square$

Theorem: Let $a = p_1^{k_1} \cdots p_\ell^{k_\ell}$ and $b = p_1^{s_1} \cdots p_\ell^{s_\ell}$ be factorizations of postive integers a and b. [Here we allow k_i's and s_j's to be zero if the corresponding prime doesn't appear in a or b's factorization.] Then $\gcd(a,b) = p_1^{m_1} \cdots p_\ell^{m_\ell}$ and $\mathrm{lcm}(a,b) = p_1^{M_1} \cdots p_\ell^{M_\ell}$ where $m_j = \min\{k_j, s_j\}$ and $M_j = \max\{k_j, s_j\}$.

proof: Let $d = \gcd(a,b)$. Then d factors into primes, say $d = p_1^{r_1} \cdots p_\ell^{r_\ell}$. Since $d \Big| a$ and $d \Big| b$, we must have at least r_j copies of p_j in the factorizations of both a and b. Thus $r_j \leq \min\{k_j, s_j\} = m_j$. But $c = p_1^{m_1} \cdots p_\ell^{m_\ell}$ is a common divisor of a and b since at least m_j copies of p_j appear in the factorizations of a and b. Since c is a common divisor, $d \Big| c$. Thus $r_j \geq m_j$ for each j. This establishes that $r_j = m_j$ for all $j = 1, \dots, \ell$. This implies that $d = p_1^{m_1} \cdots p_\ell^{m_\ell}$.

A very similar argument will establish the corresponding formula for the least common multiple. $\square$

Theorem: Let $a, b \in \mathbb{Z}$ be non-negative integers and not both zero. Then $\gcd(a,b) \cdot \mathrm{lcm}(a,b) = ab$.

proof: Notice that $x + y = \min\{x,y\} + \max\{x,y\}$. Referring to the notation established in the last theorem, we have $k_j + s_j = m_j + M_j$. The result follows. $\square$

We already know how to add, subtract, and multiply mod n. Really, these operations are essentially the same as adding, subtracting, and multiplying integers. We just need to remember to "reduce mod n" at the end.

Division is a little trickier. The reason for this is that we can't typically divide integers by integers and get back integers (Example: $6/3 = 2$, but $4/3$ isn't an integer). When we move over to modular arithmetic, sometimes division works in cases it didn't before.

Theorem: Let $a \in \mathbb{Z}$ and n be some fixed positive integer. $ax \equiv 1 \pmod{n}$ for some $x \in \mathbb{Z}$ if and only if a and n are relatively prime.

proof: Suppose $ax \equiv 1 \pmod{n}$ for some $x \in \mathbb{Z}$. Then ax and 1 are off by a multiple of n. Therefore, there exists some $y \in \mathbb{Z}$ such that $ax + ny = 1$. This implies that a and n are relatively prime.

Next, suppose that a and n are relatively prime. This implies that there are $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Therefore, $ax \equiv 1 \pmod{n}$. $\square$

Thus $x = a^{-1}$ exists mod n if and only if a and n are relatively prime. Notice that computing such an inverse is equivalent to finding $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. This can be done using the extended Euclidean algorithm.

Example: Does 50^{-1} exist mod 246? No. We saw in a previous example that $\gcd(50, 246) = 2 \neq 1$, so no (multiplicative) inverse exists.

Example: Does 50^{-1} exist mod 997? Let's run the Euclidean algorithm.

997 divided by 50 gives $997 = 50(19) + 47$. Now divide 50 by 47 and get $50 = 47(1) + 3$. Next, 47 by 3 yields $47 = 3(15) + 2$. Then, 3 by 2 gives $3 = 2(1) + 1$. Finally, 2 divided by 1 gives $2 = 1(2) + 0$. The last non-zero divisor was 1. Therefore, $\gcd(997, 50) = 1$. This means 997 and 50 are relatively prime, so 50^{-1} (mod 997) does exist.

To find the inverse we need run the Euclidean algorithm backwards. $1 = (1)3 + (-1)2$. Then $2 = (1)47 + (-15)3$ so $1 = (1)3 + (-1)[(1)47 + (-15)3]$ thus $1 = (-1)47 + (16)3$. Next, $3 = (1)50 + (-1)47$ so $1 = (-1)47 + (16)[(1)50 + (-1)47]$ thus $1 = (16)50 + (-17)47$. Finally, $47 = (1)997 + (-19)50$ so $1 = (16)50 + (-17)[(1)997 + (-19)50]$ thus $1 = (-17)997 + (339)50$.

Thus $50 \cdot 339 \equiv 1 \pmod{997}$. This means that $\boxed{50^{-1} = 339}$ (mod 997).

Example: Consider the equation: $6x + 1 \equiv 8 \pmod{10}$. This is equivalent to trying to find $x, y \in \mathbb{Z}$ such that $6x + 1 = 8 + 10y$. Thus $6x - 10y = 7$.

Now obviously $\gcd(6, -10) = 2$, but then any integral linear combination of 6 and -10 must be a multiple of 2. Since 2 does not divide $7 = 6x - 10y$, finding x and y is impossible. Therefore, our equation has no solution!

Example: Consider the equation: $6x + 1 \equiv 8 \pmod{11}$. As above, to solve this equation we need $x, y \in \mathbb{Z}$ such that $6x - 11y = 7$. But this time $\gcd(6, -11) = 1$ and 1 does divide $7 = 6x - 11y$. Thus there is a solution. We could find such a solution by running the extended Euclidean algorithm, but let's try a different way.

Note that 6 and 11 are relatively prime so 6^{-1} exists mod 11. Therefore, $x \equiv 6^{-1}(8 - 1) = 6^{-1} \cdot 7 \pmod{11}$. Now 6 and 11 are small enough that we can "guess" at 6's inverse.

6^{-1} has 6 itself as its inverse, so 6^{-1} must be relative prime to 11. This $6^{-1} \in \{1, 2, \ldots, 10\}$. We can just try these one at a time: $6 \cdot 1 = 6 \not\equiv 1$, $6 \cdot 2 = 12 \equiv 1$. We got lucky (on our second try)! $6^{-1} = 2 \pmod{11}$.

Therefore, $x \equiv 6^{-1} \cdot 7 = 2 \cdot 7 = 14 \equiv \boxed{3} \pmod{11}$. This means that the complete set of solutions of $6x + 1 \equiv 8 \pmod{11}$ is $\boxed{3 + 11\mathbb{Z} = \{3 + 11k \mid k \in \mathbb{Z}\}}$.