Summary for "Elementary Number Theory: Second Edition by Underwood Dudley"

Agro Rachmatullah

2019-07-08

1 Integers

Definition 1.1 (Least-integer principle)**.** A nonempty set of integers that is bounded below contains a smallest element.

Example The set $\{4, 5, 6\}$ has 4 as the smallest element. The set $\{10, 12, 14, \dots\}$ has 10 as the smallest element.

Definition 1.2 (Greatest-integer principle)**.** A nonempty set of integers that is bounded above contains a largest element.

Example The set $\{4, 5, 6\}$ has 6 as the largest element. The set $\{1\}$ has 1 as the largest element.

Definition 1.3. a divides b (written $a \mid b$) if and only if there is an integer d such that $ad = b$.

Examples $3 \mid 6$, $15 \mid 60$, $9 \mid 9$, $-4 \mid 16$, and $2 \mid -100$.

Definition 1.4. If a does not divide b, we write $a \nmid b$.

Examples $10 \nmid 5$ and $3 \nmid 7$.

Lemma 1.1. If $d \mid a$ and $d \mid b$, then $d \mid (a + b)$.

Example $2 \mid 4$ and $2 \mid 10$, so $2 \mid 14$.

Proof. From the definition, we know that there are integers q and r such that

$$dq = a \quad \text{and} \quad dr = b$$

Thus

$$a + b = d(q + r)$$

so from the definition again, $d \mid (a + b)$. □

Lemma 1.2. If $d \mid a_1$, $d \mid a_2$, $\dots$ $d \mid a_n$, then $d \mid (c_1a_1 + c_2a_2 + \cdots + c_na_n)$ for any integers $c_1, c_2, \dots, c_n$

Example $2 \cdot 6 + 4 \cdot 9 = 12 + 36 = 48$. Because $3 \mid 6$ and $3 \mid 9$, we conclude that $3 \mid 48$.

Definition 1.5. d is the greatest common divisor of a and b (written $d = (a, b)$) if and only if

(i) $d \mid a$ and $d \mid b$, and

(ii) if $c \mid a$ and $c \mid b$, then $c \leqslant d$

Examples $(2, 6) = 2$ and $(5, 7) = 1$.

Theorem 1.1. If $(a, b) = d$, then $(a/d, b/d) = 1$.

Examples
$(16, 20) = 4$, so $(16/4, 20/4) = (4, 5) = 1$
$(12, 6) = 3$, so $(12/3, 6/3) = (4, 2) = 2$

Proof. Suppose that $c = (a/d, b/d)$. If follows that $c \mid (a/d)$ and $c \mid (b/d)$. Therefore there are integers q and r such that $cq = a/d$ and $cr = b/d$. That is,

$$(cd)q = a \text{ and } (cd)r = b$$

which means cd is a divisor of both a and b. Because $(a, b) = d$, it must be the case that $cd \leqslant d$. d is positive so $c \leqslant 1$.

Because $c = (a/d, b/d)$, it follows that $c \geqslant 1$. Therefore $c = 1$. □

Definition 1.6. If $(a, b) = 1$, then we will say that a and b are **relatively prime**.

Examples $(4, 5) = 1$, so 4 and 5 are relatively prime. 10 and 7 are also relatively prime.

Theorem 1.2 (The Division Algorithm)**.** Given positive integers a and b, $b \neq 0$, there exist unique integers q and r, with $0 \leqslant r < b$ such that

$$a = bq + r$$

Example With $a = 17$ and $b = 5$, we have $17 = 5 \cdot 3 + 2$

Proof. Consider the set of integers $\{a, a - b, a - 2b, a - 3b, \ldots, a - qb\}$ bounded below by 0. It contains members that are nonnegative and nonempty (because at least a is a member). From the least-integer principle, it contains a smallest element $a - qb$.

The smallest element must be less than b, because if not the smallest element in the set would have to be $a - (q + 1)b$.

Ler $r = a - qb$. It follows that $a = bq + r$ and we only have to show that q and r are unique.

Suppose that we have found q, r and q_1, r_1 such that $a = bq + r = bq_1 + r_1$ with $0 \leqslant r < b$ and $0 \leqslant r_1 < b$. Subtracting, we get

$$\begin{aligned} 0 &= b(q - q_1) + (r - r_1) \\ b(q_1 - q) &= r - r_1 \end{aligned}$$

Since b divides the left side of the equation, it follows that $b \mid r - r_1$.

Because $0 \leqslant r_1 < b$, we have $-b < -r_1 \leqslant 0$. We also have $0 \leqslant r < b$, so it follows that

$$-b < r - r_1 < b$$

Since the only number in that range divisible by b is 0, $r - r_1 = 0$ which implies $q - q_1 = 0$. Hence the numbers q and r in the theorem is unique. □

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

Proof. Let $d = (a, b)$. Because $d \mid a$ and $d \mid b$, we know from $a = bq + r$ that $d \mid r$. Therefore, d is a common divisor of b and r. It remains to show that d is not just any common divisor but in fact the greatest common divisor.

Now let us assume that c is a common divisor of b and r, so $c \mid b$ and $c \mid r$. From the equation $a = bq + r$, we know that $c \mid a$. So c is common divisor of both a and b. Because $(a, b) = d$, it must be the case that $c \leqslant d$.

Since d is a common divisor of b and r, and for any common divisor c we have $c \leqslant d$, we have proven that $(b, r) = d$. □

Theorem 1.3 (The Eucledian Algorithm)**.** If a and b are positive integers, $b \neq 0$, and

$$\begin{aligned}
a &= bq + r, & 0 &\leqslant r < b,\\
b &= rq_1 + r_1, & 0 &\leqslant r_1 < r,\\
r &= r_1q_2 + r_2, & 0 &\leqslant r_2 < r_1\\
&\cdot & &\cdot\\
&\cdot & &\cdot\\
&\cdot & &\cdot\\
r_k &= r_{k+1}q_{k+2} + r_{k+2}, & 0 &\leqslant r_{k+2} < r_{k+1}
\end{aligned}$$

then for k large enough, say $k = t - 1$, we have

$$r_{t-1} = r_tq_{t+1}$$

and $(a, b) = r_t$.

Proof. The sequence

$$b > r > r_1 > r_2 > \dots$$

is decreasing, and we know that they are nonnegative, so we will eventually reach 0. Suppose $r_{t+1} = 0$. Then we have $r_{t-1} = r_tq_{t+1}$. If we apply Lemma 3 over and over,

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

□

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

$$ax + by = d$$

Proof. Let us assume that a and b are positive integers with $a \geqslant b$ and $b \neq 0$. We can always switch the order of a and b, and if $b = 0$ then the proof is trivial.

If $(a, b) = b$, then $a \cdot 0 + b \cdot 1 = b$ so the equation is true with $x = 0$ and $y = 1$.

For $d < b$, then d will be one of the remainders in the set of equations from Theorem 3. If we call the remainders $r_0, r_1, \ldots$ then we can rewrite the equations as

$$\begin{aligned} r_0 &= a - bq \\ r_1 &= b - r_0 q_1 \\ r_2 &= r_0 - r_1 q_2 \\ &\ldots \\ r_n &= r_{n-2} - r_{n-1} q_n \end{aligned}$$

For the base case of r_0 and r_1, it is easy to confirm that they can be written as $ax + by$.

Now, assuming that $r_{n-2} = ax + by$ and $r_{n-1} = ax' + by'$, then

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1} q_n \\ &= ax + by - q_n(ax' + by') \\ &= a(x - q_n x') + b(y - q_n y') \end{aligned}$$

Because the base case and inductive case is proven, it is proved for all r_n.

If one or both of a and b are negative, we can use the property $(a, b) = (-a, b) = (a, -b) = (-a, -b)$. We can also switch the order such that $a \geqslant b$ as required by the beginning of the proof. □

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

Proof. Because d and a is relatively prime, we have

$$\begin{aligned} dx + ay &= 1 \\ d(bx) + (ab)y &= b \end{aligned}$$

Because the left side is divisible by d, we conclude that $d \mid b$. □

Corollary 1.2. Let $(a, b) = d$, and suppose that $c \mid a$ and $c \mid b$. Then $c \mid d$.

Examples $(18, 12) = 6$, and 3 is a common divisor of both 18 and 12. Thus by the corollary $3 \mid 6$.

Proof. We know that there are integers x and y such that

$$ax + by = d$$

Because $c \mid ax$ and $c \mid by$, c divides the right hand side too. □

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

Examples $3 \mid 30$, $5 \mid 30$, and $(3, 5) = 1$. Thus $3 \cdot 5 = 15 \mid 30$.

Proof. $b \mid m$ means there is an integer q such that $m = bq$. Since $a \mid m$, we have $a \mid bq$.

However since $(a, b) = 1$, from Corollary 1 we know that $a \mid q$. Therefore there is an integer r such that $q = ar$, so $m = bar = (ab)r$. Thus $ab \mid m$. □

2 Unique Factorization

Definition 2.1. A **prime** is an integer that is greater than 1 and has no positive divisors other than 1 and itself.

Examples 2, 3, 5, 7 and 11 are primes.

Definition 2.2. An integer that is greater than 1 but is not prime is called **composite**.

Examples 4 is a composite because it is divisible by 2. 10 is a composite because it has 2 and 5 as its divisor.

Definition 2.3. 1 is neither a prime nor composite. We will call 1 a **unit**.

Lemma 2.1. Every integer n, $n > 1$, is divisible by a prime.

Proof. Consider the set of all divisors of n larger than 1 and smaller than n itself. If it is empty, then n is a prime which means that it is divisible by a prime (namely itself).

If it is nonempty, then by the least integer principle it has a smallest divisor, say p. If p is not a prime, then it has divisor $q > 1$ but smaller than itself. However q must divide n which is a contradiction because p is supposed to be the smallest in the set. Therefore p is a prime, and n has a prime divisor which is p. □

Proof. (By induction) The lemma is true by inspection for $n = 2$. Suppose it is true for $n \leqslant k$. Then either $k + 1$ is prime, in which case we are done, or it is divisible by some number k_1 with $k_1 \leqslant k$. But from the induction assumption, k_1 is divisible by a prime, and this prime also divides $k + 1$. Again, we are done. □

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

Proof. From Lemma 1, we know that there is a prime p_1 such that $p_1 \mid n$. That is, $n = p_1 n_1$, where $1 \leqslant n_1 < n$. If $n_1 = 1$, then we are done: $n = p_1$ is an expression of n as a products of primes. If $n_1 > 1$, then from Lemma 1 again, there is a prime that divides n_1. That is, $n_1 = p_2 n_2$, where p_2 is a prime and $1 \leqslant n_2 < n_1$. If $n_2 = 1$, again we are done: $n = p_1 p_2$ is written as a product of primes. But if $n_2 > 1$, then Lemma 1 once again says that $n_2 = p_3 n_3$, with p_3 a prime and $1 \leqslant n_3 < n_2$. If $n_3 = 1$, we are done. If not we continue. We will sooner or later come to one of the n_i equal to 1, because $n > n_1 > n_2 > \ldots$ and each n, is positive; such a sequence cannot continue forever. For some k, we will have $n_k = 1$, in which case $n = p_1 p_2 \cdots p_k$ is the desired expression of n as a product of primes. Note that the same prime may occur several times in the product. □

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

Proof. Suppose not. Then there are only finitely many primes. Denote them by $p_1, p_2, \ldots, p_r$. Consider the integer

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

From Lemma 1, we see that n is divisible by a prime, and since there are only finitely many primes, it must be one of $p_1, p_2, \ldots, p_r$. Suppose that it is p_k. Then since

$$p_k \mid n \text{ and } p_k \mid p_1 p_2 \cdots p_r \,,$$

it divides two of the terms in (**??**). Consequently it divides the other term in (**??**); thus $p_k \mid 1$. This is nonsense: no primes divide 1 because all are greater than 1. This contradiction shows that we started with an incorrect assumption. Since there cannot be only finitely many primes, there are infinitely many. □

Lemma 2.3. If n is composite, then it has divisor d such that $1 < d \leqslant n^{\frac{1}{2}}$.

Proof. Since n is composite, there are integers d_1 and d_2 such that $d_1 d_2 = n$ and $1 < d_1 < n$, $1 < d_2 < n$. If d_1 and d_2 are both larger than $n^{\frac{1}{2}}$, then

$$n = d_1 d_2 > n^{\frac{1}{2}} n^{\frac{1}{2}} = n$$

□

which is impossible. Thus, one of d_1 and d_2 must be less than or equal to $n^{\frac{1}{2}}$.

Lemma 2.4. If n is composite, then it has a prime divisor less than or equal to $n^{\frac{1}{2}}$.

Proof. We know from Lemma **??** that n has a divisor—call it d—such that $1 < d \leqslant n^{\frac{1}{2}}$. From Lemma **??**, we know that d has a prime divisor p. Since $p \leqslant d \leqslant n^{\frac{1}{2}}$, the lemma is proved. □

Lemma 2.5. If p is a prime and $p \mid ab$, then $p \mid a$ or $b \mid b$.

Examples $2 \mid 4 \cdot 3$, so 2 must either divide 4 or 3. Indeed, $2 \mid 4$.

The same couldn't be said if the divisor is not a prime. For example, even though $4 \mid 2 \cdot 6$, 4 doesn't divide either 2 nor 6.

Proof. Since p is prime, its only positive divisors are 1 and p. Thus $(p, a) = p$ or $(p, a) = 1$. In the first case, $p \mid \boldsymbol{a}$, and we are done. In the second case, Corollary **??** tells us that $p \mid \boldsymbol{b}$, and again we are done. □

Lemma 2.6. If p is a prime and $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some i, $i = 1, 2, \ldots, k$.

Proof. Lemma **??** is true by inspection if $k = 1$, and Lemma **??** shows that it is true if $k = 2$. We will proceed by induction. Suppose that Lemma **??** is true for $k = r$. Suppose that $p \mid a_1 a_2 \cdots a_{r+1}$. The $p \mid a_1 a_2 \cdots a_r$ or $p \mid a_{r+1}$. In the first case, the induction assumption tells us that $p \mid a_i$ for some i, $i = 1, 2, \ldots, r$. In the second case, $p \mid a_i$ for $i = r + 1$. In either case, $p \mid a_i$ for some i, $i = 1, 2, \ldots, r + 1$. Thus, if the lemma is true for $k = r$, it is true for $k = r + 1$, and since it is true for $k = 1$ and $k = 2$, it is true for any positive integer k. □

Lemma 2.7. If $p, q_1, q_2, \ldots, q_n$ are primes, and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k.

Proof. From Lemma **??** we know that $p \mid q_k$ for some k. Since p and q_k are primes, $p = q_k$. (The only positive divisors of q_k are 1 and q_k, and p is not 1.) □

Theorem 2.2 (The Unique Factorization Theorem)**.** Any positive integer can be written as a product of primes in one and only one way.

Proof. Recall that we agreed to consider as identical all factorizations that differ only in the order of the factors.

We know already from Lemma **??** that any integer n, $n > 1$ can be written as a product of primes. Thus to complete the proof of the theorem, we need to show that n cannot have two such representations. That is, if

$$n = p_1 p_2 \cdots p_m \text{ and } n = q_1 q_2 \cdots q_r \tag{2}$$

then we must show that the same primes appear in each product, and the same number of times, though their order may be different. That is, we must show that the integer $p_1, p_2, \ldots, p_m$ are just a rearrangement of the integers $q_1 q_2, \ldots, q_r$. From (**??**) we see that since $p_1 \mid n$,

$$p_1 \mid q_1 q_2 \cdots q_r$$

From Lemma **??**, it follows that $p_1 = q_i$ for some i. If we divide

$$p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_r$$

by the common factor, we have

$$p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_r \ . \tag{3}$$

Because p_2 divides the left-hand side of this equation, it also divides the right-hand side. Applying Lemma **??** again, it follows that $p_2 = q_j$ for some j $(j = 1, 2, \ldots, i-1, i+1, \cdots n)$. Cancel this factor from both sides of (**??**), and continue the process. Eventually we will find that each p is a q. We cannot run out of q's before all the p's are gone, because we would then have a product of primes equal to 1, which is impossible. If we repeat the argument with the p's and q's interchanged, we see that each q is a p. Thus the numbers $p_1, p_2, \ldots, p_m$ are rearrangement of $q_1, q_2, \ldots q_r$ and the two factorizations differ only in the order of the factors. □

Proof. (Induction) The theorem is true, by inspection, for $n = 2$. Suppose that it is true for $n \leqslant k$. Suppose that $k+1$ has two representations:

$$k + 1 = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_r \ .$$

As in the last proof, $p_1 = q_i$ for some i, so

$$p_2 p_3 \cdots p_m = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_r \ .$$

But this number is less than or equal to k, and by the induction assumption, its prime decomposition is unique. Hence the integers $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_r$ are a rearrangement of $p_2, p_3, \ldots, p_m$, and since $p_1 = q_i$ the proof is complete. □

Definition 2.4. From the unique factorization theorem it follows that each positive integer can be written in exactly one way in the form

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $e_i \geqslant 1, i = 1, 2, \ldots, k$, each p_i is a prime, and $p_i \neq p_j$ for $i \neq j$. We call this representation the **prime-power decomposition** of n,

Theorem 2.3. If $e_1 \geqslant 0$, $f_1 \geqslant 0$, $(i = 1, 2, \ldots k)$,

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \ \text{ and } \ n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k} \ ,$$

then

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

where $g = \min(e_i, f_i)$, $i = 1, 2, \ldots k$

3 Linear Diophantine Equations

Definition 3.1. Equations in which we look for solutions in a restricted class of numbers—be they positive integers, negative integers, rational numbers, or whatever—are called **diophantine equations**.

Example $x^2 + y^2 = z^2$ where we look for solutions in integers. One such solution is $x = 3$, $y = 4$, $z = 5$.

Lemma 3.1. If x_0, y_0 is a solutions of $ax + by = c$, then so is

$$x_0 + bt, y_0 - at$$

for any integer t.

Example $x + 2y = 4$ has $x = 0, y = 2$ as one of its solution. If we set $t = 2$, then

$$x = 0 + 2 \cdot 2 = 4$$
$$y = 2 - 1 \cdot 2 = 0$$

is also a solution for the diophantine equation.

Proof. We are given that $ax_0 + by_0 = c$. Thus

$$\begin{aligned} a(x_0 + bt) + b(y_0 - at) &= ax_0 + abt + by_0 - bat \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

so $x_0 + bt, y_0 - at$ satisfies the equation too. □

Lemma 3.2. If $(a, b) \nmid c$. then $ax + by = c$ has no solutions, and if $(a, b) \mid c$, then $ax + by = c$ has a solution.

Example The equation $2x + 4y = 5$ has no solution because $(2, 4) = 2 \nmid 5$.

Proof. Suppose that there are integers x_0, y_0 such that $ax_0 + by_0 = c$, Since $(a, b) \mid ax_0$ and $(a, b) \mid by_0$, it follows that $(a, b) \mid c$. Conversely, suppose that $(a, b) \mid c$. Then $c = m(a, b)$ for some m. From Theorem **??**, we know that there are integers r and s such that

$$ar + bs = (a, b)$$

Then

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

and $x = rm, y = sm$ is a solution. □

Lemma 3.3. Suppose that $(a, b) = 1$ and x_0, y_0 is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by

$$x = x_0 + bt$$
$$y = y_0 - at$$

where t is an integer.

Proof. We see from Lemma 2 that the equation does have a solution, because $(a, b) = 1$ and $1 \mid c$ for all c. Then, let r, s be *any* solution of $ax + by = c$. We want to show that $r = x_0 + bt$ and $s = y_0 - at$ for some integer t. From $ax_0 + by_0 = c$ follows

$$c - c = (ax_0 + by_0) - (ar + bs)$$

or

$$a(x_0 - r) + b(y_0 - s) = 0 \tag{1}$$

Because $a \mid a(x_0 - r)$ and $a \mid 0$, we have $a \mid b(y_0 - s)$. But we have supposed that a and b are relatively prime. It follows from Corollary 1.1 that $a \mid y_0 - s$. That is, there is an integer t such that

$$at = y_0 - s \tag{2}$$

Substituting in (**??**), this gives

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

Because $a \neq 0$, we may cancel it to get

$$x_0 - r + bt = 0 \tag{3}$$

But (**??**) and (**??**) say that

$$s = y_0 - at$$
$$r = x_0 + bt$$

Since r, s was *any* solution, the lemma is proved. □

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

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

where r, s is any solution and t is an integer.

4 Congruences

Definition 4.1. We say that a is **congruent** to b modulo m (in symbols, $a \equiv b \pmod{m}$) if and only if $m \mid (a-b)$ and we will suppose always that $m > 0$.

Theorem 4.1. $a \equiv b \pmod{b}$ if and only if there is an integer k such that $a = b + km$.

Proof. Suppose that $a \equiv b \pmod{b}$. Then, from the definition of congruence, $m \mid (a-b)$. From the definition of divisibility, we know that since there is an integer k such that $km = a - b$, then $a = b + km$.

Conversely, suppose that $a = b + km$. Then $a - b = km$, which means that $(a-b)$ is divisible by m. But that is exactly the definition of $a \equiv b \pmod{b}$. □

Theorem 4.2. Every integer is congruent (mod m) to exactly one of $0, 1, \ldots, m-1$.

Proof. Write $a = qm+r$, with $0 \leqslant r < m$. We know from Theorem **??** that q and r are uniquely determined. Since $a \equiv r \pmod{m}$, the theorem is proved. □

Definition 4.2. The number r in the last theorem is called the **least residue** of $a \pmod{m}$.

Theorem 4.3. $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder on division by m.

Proof. If a and b leave the same remainder r when divided by m, then

$$a = q_1 m + r \text{ and } b = q_2 m + r$$

for some integers q_1 and q_2. It follows that

$$a - b = (q_1 m + r) - (q_2 m + r) = m(q_1 - q_2)$$

From the definition of divisibility, we have $m \mid (a-b)$. From the definition of congruence, we conclude that $a \equiv b \pmod{m}$. To prove the converse, suppose that $a \equiv b \pmod{m}$. Then $a \equiv b \equiv r \pmod{m}$, where r is a least residue modulo m. Then from Theorem 1,

$$a = q_1 m + r \text{ and } b = q_2 m + r$$

for some integers q_1 and q_2; since $0 \leqslant r < m$, the theorem is proved. □

Lemma 4.1. For integers a, b, c, and d

a) $a \equiv a \pmod{m}$.

b) If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

c) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

d) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

e) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. □

a) $a - a = 0 = m \cdot 0$, so $m \mid (a - a)$, which means $a \equiv a \pmod{m}$.

b) We are given $a - b = km$, so $b - a = (-k)m$, which means $b \equiv a \pmod{m}$.

c) The first condition means that a and b leaves the same remainder r_1 when divided by m. The second means that b and c leaves the same remainder r_2 when divided by m. Because both r_1 and r_2 are the remainders when b is divided by m, $r_1 = r_2$. Thus a and c has the same remainder when divided by m, or $a \equiv c \pmod{m}$.

d) We are given that $a - b = km$ and $c - d = jm$ for some integers k and j; thus

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= km - jm \\ &= m(k - j)\end{aligned}$$

from the definition of congruence, $a + c \equiv b + d \pmod{m}$.

e) We are given that $b - a = km$ and $d - c = jm$ for some integers k and j; thus

$$\begin{aligned}ac - bd &= ac - (a + km)(c + jm) \\ &= ac - ac - ajm - ckm - kjm^2 \\ &= m(-aj - ck - kjm)\end{aligned}$$

from the definition of congruence, $ac \equiv bd \pmod{m}$.

Theorem 4.4. If $ac \equiv bc \pmod{m}$ and $(c, m) = 1$, then $a \equiv b \pmod{m}$.

Proof. From the definition of congruence, $m \mid (ac - bc)$; consequently, $m \mid c(a - b)$. Because $(m, c) = 1$, we can conlude from Theorem 5 of Section 1 that $m \mid (a - b)$. That is, $a \equiv b \pmod{m}$. □

Theorem 4.5. If $ac \equiv bc \pmod{m}$ and $(c, m) = d$, then $a \equiv b \pmod{m/d}$.

Proof. If $ac \equiv bc \pmod{m}$, then $m \mid c(a - b)$ and $m/d \mid (c/d)(a - b)$. Since we know that $(m/d, c/d) = 1$, from Theorem 5 of Section 1 we get $m/d \mid (a - b)$, so $a \equiv b \pmod{m/d}$. □

Theorem 4.6. Every integer is congruent (mod 9) to the sum of its digits.

Proof. Take an integer n, and let its digital representation be

$$d_k d_{k-1} d_{k-2} \dots d_1 d_0$$

That is,

$$\begin{aligned} n &= d_k 10^k + d_{k-1} 10^{k-1} + d_{k-2} 10^{k-2} + \cdots + d_1 10^1 + d_0 10^0 \\ &\equiv d_k + d_{k-1} + d_{k-2} + \cdots + d_0 \pmod 9 \end{aligned}$$

□

5 Linear Congruences

Definition 5.1. A solution to $ax \equiv b \pmod m$ is a number r such that $ar \equiv b \pmod m$ and r is a least residue $\pmod m$. There might be no solutions, exactly one solution, or many solutions.

Lemma 5.1. If $(a, m) \nmid b$, then $ax \equiv b \pmod m$ has no solutions.

Proof. We will prove the contrapositive, which is logically the same thing: if $ax \equiv b \pmod m$ has a solution, then $(a, m) \mid b$. Suppose that r is a solution. Then $ar \equiv b \pmod m$, and from the definition of congruence, $m \mid (ar - b)$, or from the definition of divides, $ar - b = km$ for some k. Since $(a, m) \mid a$ and $(a,)m \mid km$, it follows that $(a, m) \mid b$. □

Lemma 5.2. If $(a, m) = 1$, then $ax \equiv b \pmod m$ has exactly one solution.

Proof. Since $(a, m) = 1$, we know that there are integers r and s such that $ar + ms = 1$. Multiplying by b gives

$$a(rb) + m(sb) = b$$

Which means

$$a(rb) \equiv b \pmod m$$

The least residue of rb modulo m is then a solution of the linear congruence.

It remains to show that there is not more than one solution. Suppose that both r and s are solutions. That is, since

$$ar \equiv b \pmod m \quad \text{and} \quad as \equiv b \pmod m$$

Then $ar \equiv as \pmod m$. Because $(a, m) = 1$, we can apply Theorem 4 of the last section, cancel the common factor, and get $r \equiv s \pmod m$. That is, $m \mid (r - s)$. But r and s are least residues $\pmod m$, so

$$0 \leqslant r < m \quad and \quad 0 \leqslant s < m$$

Thus $-m < r - s < m$; together with $m \mid (r - s)$, this gives $r - s = 0$, or $r = s$, and the solution is unique. □

Lemma 5.3. Let $d = (a, m)$. If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d solutions.

Proof. If we cancel the common factor, we get a congruence $(a/d)x \equiv (b/d) \pmod{m/d}$, which we know has exactly one solution, because $(a/d, m/d) = 1$. Call it r, and let s be any other solution of $ax \equiv b \pmod{m}$. Then $ar \equiv as \equiv b \pmod{m}$, and it follows from Theorem 5 of the last section that $r \equiv s \pmod{m/d}$. That is, $s - r = k(m/d)$ or $s = r + k(m/d)$ for some k. Putting $k = 0, 1, \ldots, d-1$, we get $0 \leqslant k(m/d) \leqslant (d-1)(m/d)$. Combined with $0 \leqslant r < m/d$, we conclude that s are numbers which are least residues (mod m), since

$$0 \leqslant r + k(m/d) < (m/d) + (d-1)(m/d) = m$$

and they all satisfy $ax \equiv b \pmod{m}$, because

$$(a/d)(r + k(m/d)) \equiv (a/d)r \equiv b/d \pmod{m/d}$$

and this implies (by definition of congruence and multiplying both sides by d)

$$a(r + k(m/d)) \equiv b \pmod{m}$$

□

Theorem 5.1. $ax \equiv b \pmod{m}$ has no solutions if $(a, m) \nmid b$. If $(a, m) \mid b$, then there are exactly (a, m) solutions.

Proof. This is just a summary of the previous three lemmas. □

Theorem 5.2 (The Chinese Remainder Theorem)**.** The system of congruences

$$x \equiv a_i \pmod{m_i}, i = 1, 2, \ldots, k \tag{1}$$

where $(m_i, m_j) = 1$ if $i \neq j$, has a unique solution modulo $m_1 m_2 \cdots m_k$.

Proof. We first show, by induction, that the system (**??**) has a solution. The result is obvious when $k = 1$. Let us consider the case $k = 2$. If $x \equiv a_1 \pmod{m_1}$, then $x = a_1 + k_1 m_1$ for some k_1. If in addition $x \equiv a_2 \pmod{m_2}$, then

$$a_1 + k_1 m_1 \equiv a_2 \pmod{m_2}$$

or

$$k_1 m_1 \equiv a_2 - a_1 \pmod{m_2}$$

Because $(m_2, m_1) = 1$, we know that this congruence, with k_1 as the unknown, has a unique solution modulo m_2. Call it t. Then $k_1 = t + k_2 m_2$ for some k_2, and

$$x = a_1 + (t + k_2 m_2)m_1 \equiv a_1 + t m_1 \pmod{m_1 m_2}$$

satisfies both congruences.

Suppose that system (**??**) has a solution (mod $m_1 m_2 \dots m_k$) for $k = r - 1$. Then there is a solution, s, to the system

$$x \equiv a_i \pmod{m_i}, i = 1, 2, \dots, r-1$$

But the system

$$x \equiv s \pmod{m_1 m_2 \cdots m_{r-1}}$$

$$x \equiv a_r \pmod{m_r}$$

has a solution modulo the product of the moduli, just as in the case $k = 2$, because $(m_1 m_2 \cdots m_{k-1}, m_k) = 1$. (This statement is true because no prime that divides $m_i, i = 1, 2, \dots, k-1$, can divide m_k)

It is easy to see that the solution is unique. If r and s are both solutions of the system, then

$$r \equiv s \equiv a_i \pmod{m_i}, i = 1, 2, \dots, k$$

So $m_i \mid (r-s), i = 1, 2, \dots, k$ Thus $r-s$ is a common multiple of $m_1, m_2, \dots, m_k$, and because the moduli are relatively prime in pairs, we have $m_1 m_2 \cdots m_k \mid (r - s)$. But since r and s are least residues modulo $m_1 m_2 \cdots m_k$,

$$-m_1 m_2 \cdots m_k < r - s < m_1 m_2 \cdots m_k$$

whence $r - s = 0$. □

6 Fermat's and Wilson's Theorems

Lemma 6.1. If $(a, m) = 1$, then the least residues of

$$a, 2a, 3a, \dots, (m-1)a \pmod{m} \tag{1}$$

are

$$1, 2, 3, \dots, m-1 \tag{2}$$

is some order.

Example For $m = 8$ and $a = 3$, the numbers in (1) are

$$3, 6, 9, 12, 15, 18, 21$$

and their least residues (mod 8) are

$$3, 6, 1, 4, 7, 2, 5$$

Proof. There are $m-1$ numbers in (1), none congruent to 0 (mod m). Hence each of them is congruent (mod m) to one of the numbers in (2). If we show that no two of the integers in (1) are congruent (mod m), then it follows that their least residues (mod m) are all different, and hence are a permutation of $1, 2, \ldots, m-1$.

Suppose that two of the integers in (1) are congruent (mod m): that is,

$$ra \equiv sa \pmod{m}$$

Because (a, m) = 1 we can cancel (Theorem 4.4) and get

$$r \equiv s \pmod{m}$$

But r and s are least residues modulo m; by argument we have used several times before, it follows that $r = s$. □

Theorem 6.1 (Fermat's Theorem)**.** If p is prime and $(a, p) = 1$,

$$a^{p-1} \equiv 1 \pmod{p}$$

Example For $p = 5$ and $a = 2$, we have $a^4 = 16 \equiv 1 \pmod{5}$.

Proof. Given any prime p, Lemma 1 says that if $(a, p) = 1$, then the least residues of

$$a, 2a, \ldots, (p-1)a \pmod{p}$$

are a permutation of

$$1, 2, \ldots, p-1.$$

Hence their products are congruent (mod p):

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

or

$$a^{p-1}(p-1)! = (p-1)! \pmod{p}$$

Since p and $(p-1)!$ are relatively prime, the last congruence gives

$$a^{p-1} \equiv 1 \pmod{p}$$

□

Corollary 6.1. If p is a prime, then

$$a^p \equiv a \pmod{p}$$

for all a.

Proof. If $(a, p) = 1$, this follows from Fermat's Theorem. If $(a, p) = p$, then the corollary says $0 = 0 \pmod{p}$, which is true. There are no other cases. □

Lemma 6.2. $x^2 \equiv 1 \pmod{p}$ has exactly two solutions: 1 and $p - 1$.

Proof. Let r be any solution of $x^2 \equiv 1 \pmod{p}$. By solution we mean, as we did for linear congruences, a least residue that satisfies the congruence. We have $r^2 - 1 \equiv 0 \pmod{p}$, so

$$p \mid (r + 1)(r - 1)$$

hence $p \mid (r + 1)$ or $p \mid (r - 1)$; otherwise expressed,

$$r + 1 \equiv 0 \text{ or } r - 1 \equiv 0 \pmod{p},$$

so $r \equiv p - 1$ or $1 \pmod{p}$. Since r is a least residue $(\text{mod } p)$, it follows that $r = p - 1$ or 1. It is easy to verify that both of these numbers actually satisfy $x^2 \equiv 1 \pmod{p}$. □

Lemma 6.3. Let p be an odd prime and let a' be the solution of $ax \equiv 1 \pmod{p}$, $a = 1, 2, \ldots, p - 1$. $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$. Furthermore, $a \equiv a' \pmod{p}$ if and only if $a = 1$ or $p - 1$.

Example For $p = 13$ we have

a	1	2	3	4	5	6	7	8	9	10	11	12
a'	1	7	9	10	8	11	2	5	3	4	6	12

Note that the bottom row does not have duplicate entries, which means $a' \equiv b' \pmod{p}$ if and only if $a \equiv b \pmod{p}$.

Proof. Suppose that $a' \equiv b' \pmod{p}$. Then

$$b \equiv aa'b \equiv ab'b \equiv a \pmod{p}$$

Conversely, suppose that $a \equiv b \pmod{p}$. Then

$$b' \equiv b'aa' \equiv b'ba' \equiv a' \pmod{p}.$$

For the second part of the proof, it follows from $1 \cdot 1 \equiv (p - 1)(p - 1) \equiv 1 \pmod{p}$ that $1' \equiv 1 \ (p)$ and $(p - 1)' \equiv p - 1 \pmod{p}$. Conversely, if $a \equiv a' \pmod{p}$, then $1 \equiv aa' \equiv a^2 \pmod{p}$, and from Lemma 2 we know that this is possible only if $a = 1$ or $p - 1$. □

Theorem 6.2 (Wilson's Theorem)**.** p is a prime if and only if

$$(p - 1)! \equiv -1 \pmod{p}$$

Example For the prime $p = 5$, we have

$$(p-1)! = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \equiv -1 \pmod{p}$$

Proof. From Lemma 3, we know that we can separate the numbers

$$2, 3, \ldots p-2$$

into $(p-3)/2$ pairs such that each pair consists of an integer a and its associated a', which is different from a. For example, for $p = 13$ the pairs are

$$(2,7), (3,9), (4,10), (5,8), (6,11)$$

The product of the two integers in each pair is congruent to 1 (mod p), so it follows that

$$2 \cdot 3 \cdot (p-2) \equiv 1 \pmod{p}.$$

Hence

$$(p-1)! \equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$$

and we have proved half of the theorem. It remains to prove the other half and show that if

$$(n-1)! \equiv -1 \pmod{n}, \tag{3}$$

then n is a prime. Suppose that $n = ab$ for some integers a and b, with $a \neq n$. From (3), we have

$$n \mid (n-1)! + 1,$$

and since $a \mid n$, we have

$$a \mid (n-1)! + 1 \tag{4}$$

But since $a \leqslant n-1$, it follows that one of the factors of $(n-1)!$ is a itself. Thus

$$a \mid (n-1)! \tag{5}$$

But (4) and (5) imply that $a \mid 1$. Hence the only positive divisors of n are 1 and n, and thus n is a prime. □

7 The Divisors of an Integer

TODO

8 Perfect Numbers

TODO

9 Euler's Theorem and Function

Definition 9.1. If m is a positive integer, let $\phi(m)$ denote the number of positive integers less than or equal to m and relatively prime to m. We will call ϕ **Euler's ϕ-function (totient function)**.

Example $\phi(6) = 2$ because 1 and 5 are the only two numbers less than or equal to 6 that are relatively prime to 6.

$\phi(10) = 4$ because 1, 3, 7, and 9 are the only four numbers less than or equal to 10 that are relatively prime to 10.

Lemma 9.1. If $(a, m) = 1$ and $r_1, r_2, \ldots, r_{\phi(m)}$ are the positive integers less than m and relatively prime to m, then the least residues (mod m) of

$$ar_1, ar_2, \ldots, ar_{\phi(m)} \tag{1}$$

are a permutation of

$$r_1, r_2, \ldots, r_{\phi(m)}$$

Example With $m = 10$ and $a = 3$, the least residues of $3 \cdot 1, 3 \cdot 3, 3 \cdot 7, 3 \cdot 9$ are $3, 9, 1, 7$ which is a permutation of $1, 3, 7, 9$.

Proof. Since there are exactly $\phi(m)$ numbers in the set (1), to prove that their least residues are a permutation of the $\phi(m)$ numbers $r_1, r_2, \ldots, r_{\phi(m)}$ we need to show that they are all different and that they are all relatively prime to m. To show that they are all different, suppose that

$$ar_i \equiv ar_j \pmod{m}$$

for some i and j ($1 \leqslant i \leqslant \phi(m)$, $1 \leqslant j \leqslant \phi(m)$). Since $(a, m) = 1$, we can cancel a from both sides of the congruence to get $r_i \equiv r_j \pmod{m}$. Since r_i and r_j are least residues (mod m), it follows that $r_i = r_j$. Hence $r_i \neq r_j$ implies $ar_i \not\equiv ar_j \pmod{m}$, so the numbers in (1) are all different.

To prove that all the number is (1) are relatively prime to m, suppose that p is a prime common divisor of ar_i and m for some i, $1 \leqslant i \leqslant \phi(m)$. Since p is prime, either $p \mid a$ or $p \mid r_i$. Thus either p is a common divisor of a and m or of r_i and m. But $(a, m) = (r_i, m) = 1$, so both cases are impossible. Therefore $(ar_i, m) = 1$ for each i, $i = 1, 2, \ldots, \phi(m)$. □

Theorem 9.1. Suppose that $m \geqslant 1$ and $(a, m) = 1$. Then $a^{\phi(m)} \equiv 1 \pmod{m}$.

Example $(3, 8) = 1$ and $\phi(8) = 4$, so $3^4 \equiv 9 \cdot 9 \equiv 1 \cdot 1 \equiv 1 \pmod 8$.

Proof. The theorem is true when $m = p$, a prime. Every positive integer less than p is relatively prime to it, so $\phi(p) = p - 1$, and by Fermat's Theorem $a^{p-1} \equiv 1 \pmod p$ when $(a, p) = 1$.

The theorem is also true for $m = 1$, since the definition of ϕ gives $\phi(1) = 1$, and $a^1 \equiv 1 \equiv 0 \pmod 1$ for any integer a.

More generally, for $m \neq 1$, we know from Lemma 1 that

$$\begin{aligned} r_1 r_2 \cdots r_{\phi(m)} &\equiv (ar_1)(ar_2) \cdots (ar_{\phi(m)}) \\ &\equiv a^{\phi(m)}(r_1 r_2 \cdots r_{\phi(m)}) \pmod m \end{aligned}$$

Because each of $r_1, r_2, \ldots, r_{\phi(m)}$ is relatively prime to m, their product is also. Thus that factor may be canceled in the last congruence, and we get

$$1 \equiv a^{\phi(m)} \pmod m$$

□

Lemma 9.2. $\phi(p^n) = p^{n-1}(p - 1)$ for all prime p and positive integers n.

Example $\phi(9) = \phi(3^2) = 3^1 \cdot (3 - 1) = 6$. Indeed there are 6 positive numbers less than or equal to 9 which are relatively prime to 9: 1, 2, 4, 5, 7, 8.

Proof. The positive integers less than or equal to p^n which are *not* relatively prime to p^n are exactly the multiples of p:

$$1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, (p^{n-1})p,$$

and there are p^{n-1} of them. Since there are in all p^n positive integers less than or equal to p^n, we have

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$$

□

Lemma 9.3. If $(a, m) = 1$ and $a \equiv b \pmod m$, then $(b, m) = 1$.

Example $(3, 4) = 1$ and $3 \equiv 11 \pmod m$, so $(11, 4) = 1$.

Proof. This follows from the fact that $b = a + km$ for some k, so $a = b - km$. If $(b, m) = d$ where $d > 1$, then because $d \mid b$ and $d \mid km$, it follows that $d \mid a$ which means $(a, m) = d$ which is a contradiction. □

Corollary 9.1. If the least residues (mod m) of

$$r_1, r_2, \ldots, r_m \tag{2}$$

are a permutation of 0, 1, . . . , m - 1, then (2) contains exactly $\phi(m)$ elements relatively prime to m.

Theorem 9.2. ϕ is multiplicative.

Example Because $(2,3) = 1$, $\phi(6) = \phi(2\dot{3}) = \phi(2)\phi(3) = 2$. Indeed the only two numbers less than or equal to 6 and is relatively prime to 6 are 1 and 5.

Proof. Suppose that $(m,n) = 1$ and write the numbers from 1 to mn as follows:

$$\begin{array}{ccccccc} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ & & \vdots & & \\ m & 2m & 3m & \dots & mn \end{array}$$

Suppose that $(m,r) = d$ and $d > 1$. Then we claim that no element in the r-th row of the array:

$$r \quad m+r \quad 2m+r \quad \dots \quad km+r \quad \dots \quad (n-1)m+r$$

is relatively prime to mn. This is so because if $d \mid m$ and $d \mid r$, then $d \mid (km+r)$ for any k. So, if we are looking for numbers that are relatively prime to mn, we will not find any except in those rows whose first element is relatively prime to m. There are $\phi(m)$ rows in total.

Suppose we can show that there are exactly $\phi(n)$ numbers relatively prime to mn in each of the rows that have first elements relatively prime to m. Since there are $\phi(m)$ such rows, it will follow that the number of integers in the whole array that are relatively prime to mn is $\phi(m)\phi(n)$: that is, $\phi(mn) = \phi(m)\phi(n)$, and the theorem will be proved. But the numbers in the r-th row (where r and m are relatively prime) are

$$r \quad m+r \quad 2m+r \quad \dots \quad km+r \quad \dots \quad (n-1)m+r \tag{3}$$

and we claim that their least residues (mod n) are a permutation of

$$0, 1, 2, \dots, (n-1) \tag{4}$$

To verify this claim, all we have to do is show that no two of the numbers in (3) are congruent (mod n), because (3) contains n elements, just as (4) does. This is easy. suppose that

$$km + r \equiv jm + r \pmod{n}$$

with $0 \leqslant k < n$ and $0 \leqslant j < n$. Then $km \equiv jm \pmod{n}$, and since $(m,n) = 1$, we have $k \equiv j \pmod{n}$. On account of the inequalities on k and j, it follows that $k = j$. Hence if $k \neq j$, then $km + r \not\equiv jm + r \pmod{n}$, and no two elements of (3) are congruent (mod n).

By the Corollary to Lemma 3, we have that (3) contains exactly $\phi(n)$ elements relatively prime to n. But from Lemma 3, every element in the r-th row of the array is relatively prime to m. It follows that the r-th row of the

array contains exactly $\phi(n)$ elements relatively prime to mn. As noted, this completes the proof. □

Theorem 9.3. If n has a prime-power decomposition given by

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

then

$$\phi(n) = p_1^{e_1-1}(p_1 - 1)p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1)$$

Example $\phi(72) = \phi(2^3 \cdot 3^2) = \phi(2^3)\phi(3^2) = 2^2 \cdot 1 \cdot 3^1 \cdot 2 = 24$

Proof. Because ϕ is multiplicative, Theorem 5 of Section 7 applies here to give

$$\phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$$

If we apply Lemma **??** to each term on the right, the theorem is proved. □

Corollary 9.2. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Example $\phi(72) = \phi(2^3 \cdot 3^2) = 72(1 - \frac{1}{2})(1 - \frac{1}{3}) = 72 \cdot \frac{1}{2} \cdot \frac{2}{3} = \frac{72}{6} = 12$

Proof.

$$\begin{aligned}
\phi(n) &= \left[p_1^{e_1-1}(p_1 - 1)\right]\left[p_2^{e_2-1}(p_2 - 1)\right] \cdots \left[p_k^{e_k-1}(p_k - 1)\right] \\
&= \left[p_1^{e_1}\left(1 - \frac{1}{p_1}\right)\right]\left[p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\right] \cdots \left[p_k^{e_k}\left(1 - \frac{1}{p_k}\right)\right] \\
&= p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

□

Theorem 9.4. If $n \geqslant 1$, then

$$\sum_{d \mid n} \phi(d) = n$$

Example The divisors of 8 are 1, 2, 4, and 8.

$$\sum_{d \mid 8} \phi(d) = \phi(1) + \phi(2) + \phi(4) + \phi(8) = 1 + 1 + 2 + 4 = 8$$

Proof. The proof is first thought by Gauss. Consider the integers 1, 2, ..., n. We will put one of these integers in class C_d if and only if its greatest common divisor with n is d. For example, if $n = 12$, we have

$$\begin{aligned} C_1 &= \{1, 5, 7, 11\}, & C_2 &= \{2, 10\}, \\ C_3 &= \{3, 9\}, & C_4 &= \{4, 8\}, \\ C_5 &= \{6\}, & C_6 &= \{12\}. \end{aligned}$$

We have m in C_d if and only if $(m, n) = d$. But $(m, n) = d$ if and only if $(m/d, n/d) = 1$. That is, an integer m is in class C_d if and only if m/d is relatively prime to n/d. The number of positive integers less than or equal to n/d and relatively prime to n/d is $\phi(n/d)$ by definition. Thus, the number of elements in class C_d is $\phi(n/d)$.

Since there is a class for each divisor of n, the total number of elements in all the classes C_d is

$$\sum_{d \mid n} \phi(n/d)$$

That is, $n = \sum_{d \mid n} \phi(n/d)$. But $\sum_{d \mid n} \phi(n/d)$ is the same as $\sum_{d \mid n} \phi(n)$, just with the terms in opposite order. Thus the theorem is proved. □

10 Primitive Roots

Definition 10.1. If $(a, m) = 1$, then the **order** of a modulo m is the smallest positive integer t such that $a^t \equiv 1 \pmod{m}$.

Example 10 has order of 2 (mod 11). On the other hand, 2 has order of 10 (mod 11).

Theorem 10.1. Suppose that $(a, m) = 1$ and a has order $t \pmod{m}$. Then $a^n = 1 \pmod{m}$ if and only if n is a multiple of t.

Example 10 has order of 2 (mod 11), so 10^4, 10^6, etc. are all congruent to 1 (mod 11). Also we can quickly know that 10^{13} is not congruent to 1 (mod 11) because 13 is not a multiple of 2.

Proof. Suppose that $n = tq$ for some integer q. Then $a^n \equiv a^{tq} \equiv (a^t)^q \equiv 1 \pmod{m}$ because $a^t \equiv 1 \pmod{m}$.

Conversely, suppose that $a^n \equiv 1 \pmod{m}$. Since t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, we have $n \geqslant t$ so we can divide n by t to get $n = tq + r$ with $q \geqslant 1$ and $0 \leqslant r < t$. Thus

$$1 \equiv a^n \equiv a^{tq+r} \equiv (a^t)^q a^r \equiv 1^q a^r \equiv a^r \pmod{m}$$

Since t is the smallest positive integer such that $a^t \equiv 1 \pmod{m}$, $a^r \equiv 1 \pmod{m}$ with $0 \leqslant r < t$ is possible only if $r = 0$. Thus $n = tq$ and the theorem is proved. □

Theorem 10.2. If $(a, m) = 1$ and a has order $t \pmod{m}$, then $t \mid \phi(m)$.

Example $\phi(11) = 10$, so an integer can have order of 1, 2, 5, or 10 (mod 11).

Proof. From Euler's extension of Fermat's Theorem we know that $a^{\Phi(m)} \equiv 1 \pmod{m}$. From Theorem 1, $\phi(m)$ is a multiple of t, which is what we wanted to prove. □

Theorem 10.3. If p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or $q = 2kp + 1$ for some integer k.

Proof. Since $q \mid a^p - 1$, we have $a^p \equiv 1 \pmod{q}$. So by Theorem 1, the order of $a \pmod{q}$ is a divisor of p. That is, a has order 1 or p. If the order of a is 1, then $a^1 \equiv 1 \pmod{q}$, so $q \mid a - 1$. If on the other had the order of a is p, then by Theorem 2, $p \mid \phi(q)$; that is, $p \mid q - 1$. So $q - 1 = rp$ for some integer r. Since p and q are odd, r must be even, and this completes the proof. □

Corollary 10.1. Any divisor of $2^p - 1$ (where p is a prime) is of the form $2kp + 1$.

Proof. $2^p - 1$ is odd, so any of its prime factor q must be odd which means the previous theorem apply. However $a = 2$ so $q \mid a - 1 = 1$ is nonsensical because q is a prime. Therefore $q = 2kp + 1$ for some integer k. If $2^p - 1$ has more than one factor (e.g., it is a composite number), then the product of any two factors q_1 and q_2 will be a divisor also. It is in fact

$$\begin{aligned} q_1 q_2 &= (2k_1 p + 1)(2k_2 p + 1) \\ &= 4k_1 k_2 p^2 + 2k_1 p + 2k_2 p + 1 \\ &= 2(2k_1 k_2 p + k_1 + k2_2)p + 1 \\ &= 2jp + 1 \end{aligned}$$

for some integer j. The same conclusion will hold for the product of more factors.

1 is the last divisor not covered by the cases above, but it can also be written as $2kp + 1$ with $k = 0$. Therefore the statement is proved. □

Theorem 10.4. If the order of $a \pmod{m}$ is t, then $a^r \equiv a^s \pmod{m}$ if and only if $r \equiv s \pmod{t}$.

Example The order of 2 is 3 (mod 7). Because $2 \equiv 8 \pmod 3$, $2^2 \equiv 2^8 \pmod 7$. Indeed, $2^8 \equiv 256 \equiv 256 - 210 \equiv 46 - 42 \equiv 4 \pmod 7$.

Proof. Suppose that $a^r \equiv a^s \pmod m$. We can suppose that $r \geqslant s$ with no loss of generality. Thus $a^{r-s} \equiv 1 \pmod m$, and from Theorem 1, $r - s$ is a multiple of t. That, by definition, says that $r \equiv s \pmod t$.

For the converse, suppose that $r \equiv s \pmod t$. Then $r = s + kt$ for some integer k, and

$$a^r = a^{s+kt} = a^s(a^t)^k \equiv a^s \pmod m$$

because $a^t \equiv 1 \pmod m$. □

Definition 10.2. If a is a least residue and the order of $a \pmod m$ is $\phi(m)$, then we will say that a is a primitive root of m.

Theorem 10.5. If g is a primitive root of m, then the least residues, modulo m, of

$$g, g^2, \ldots, g^{\Phi(m)}$$

are a permutation of the $\phi(m)$ positive integers less than m and relatively prime to it.

Example 2 is a primitive root of 9, and the powers

$$2, 2^2, 2^3, 2^4, 2^5, 2^6$$

are (mod 9),

$$2, 4, 8, 7, 5, 1$$

Which are exactly the residues relatively prime to 9.

Proof. Since $(g, m) = 1$, each power of g is relatively prime to m. Moreover, no two powers have the same residue, because if $g^j \equiv g^k \pmod m$, then from Theorem 4, $j \equiv k \pmod{\phi(m)}$. If $j \not\equiv k \pmod{\phi(m)}$, $g^j \not\equiv g^k \pmod m$. □

Lemma 10.1. Suppose that a has order $t \pmod m$. Then a^k has order $t \pmod m$ if and only if $(k, t) = 1$.

Example 2 has order 10 (mod 11), and the lemma says that 2^k has order 10 if and only if $(k, 10) = 1$; that is, for $k = 1, 3, 7, \text{and } 9$. The other primitive roots of 11 are thus $2^3, 2^7, \text{and } 2^9$, or 8, 7, and 6.

Proof. Suppose that $(k,t)=1$, and denote the order of a^k by s. We have

$$1 \equiv (a^t)^k \equiv (a^k)^t \pmod{m},$$

so from Theorem 1, $s \mid t$. Because s is the order of a^k,

$$(a^k)^s \equiv a^{ks} \equiv 1 \pmod{m},$$

so from Theorem 1 again, $t \mid ks$. Since $(k,t)=1$, it follows that $t \mid s$. This fact, combined with the fact that $s \mid t$, implies that $s=t$.

To prove the converse, suppose that a and a^k have order t and that $(k,t)=r$. Then

$$1 \equiv a^t \equiv (a^t)^{k/r} = (a^k)^{t/r} \pmod{m}$$

Because t is the order of a^k, Theorem 1 says that t/r is a multiple of t. This impies that $r=1$. □

Corollary 10.2. Suppose that g is a primitive root of a prime p. Then the least residue of g^k is a primitive root of p if and only if $(k,p-1)=1$.

Proof. Apply Lemma 1 with $t=p-1$. □

Lemma 10.2. If f is a polynomial of degree n and p is a prime, then

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

has at most n solutions.

Proof. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

have degree n; that is, $a_n \not\equiv 0 \pmod{p}$. We prove the lemma by induction. For $n=1$,

$$a_1 x + a_0 \equiv 0 \pmod{p}$$

has but one solution, since $(a_1,p)=1$. Suppose that the lemma is true for polynomials of degree $n-1$, and suppose that f has degree n. Either $f(x) \equiv 0 \pmod{p}$ has no solutions or it has at least one. In the first case, the lemma is true. In the second case, suppose that r is a solution. That is, $f(r) \equiv 0 \pmod{p}$ and r is a least residue $(\text{mod } p)$. Then because $x-r$ is a factor of $x^t - r^t$ for $t=0,1,\ldots,n$, we have

$$\begin{aligned} f(x) &\equiv f(x) - f(r) \\ &\equiv a_n(x^n - r^n) + a_{n-1}(x^{n-1} - r^{n-1}) + \cdots + a_1(x-r) \\ &\equiv (x-r)g(x) \pmod{p}, \end{aligned}$$

where g is a polynomial of degree $n-1$. Suppose that s is also a solution of (**??**). Thus

$$f(s) \equiv (s-r)g(s) \equiv 0 \pmod{p}$$

Because p is a prime it follows that

$$s \equiv r \pmod{p} \quad \text{or} \quad g(s) = 0 \pmod{p}$$

from the induction assumption, the second congruence has at most $n-1$ solutions. Since the first congruence has just one solution, the proof is complete. □

Lemma 10.3. If p is a prime and $d \mid p-1$, then $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Example With $p = 7$, we have $x^6 \equiv 1 \pmod{7}$ for $x = 1, 2, \ldots, 6$. The divisors of 6 are 1, 2, 3, and 6. The case 1 and 6 are trivial. For $x^2 \equiv 1 \pmod{7}$, the only solutions are 1 and 6. For $x^3 \equiv 1 \pmod{7}$, the solutions are 1, 2, and 4.

Proof. From Fermat's Theorem, the congruence $x^{p-1} \equiv 1 \pmod{p}$ has exactly $p-1$ solutions, namely $1, 2, ..., p-1$. Moreover,

$$\begin{aligned} x^{p-1} - 1 &= (x^d - 1)(x^{p-1-d} + x^{p-1-2d} + \cdots + x^d + 1) \\ &= (x^d - 1)h(x) \end{aligned}$$

From Lemma 2, we know that $h(x) \equiv 0 \pmod{p}$ has at most $p-1-d$ solutions. Hence $x^d \equiv 1 \pmod{p}$ has at least d solutions. Applying Lemma 2 again, $x^d \equiv 1 \pmod{p}$ has at most d solutions. Therefore it has exactly d solutions. □

Theorem 10.6. Every prime p has $\phi(p-1)$ primitive roots.

Proof. Theorem 2 says that each of the integers

$$1, 2, \ldots, p-1 \tag{2}$$

has an order that is a divisor of $p-1$. For each divisor t of $p-1$, let $\psi(t)$ denote the number of integers in (**??**) that have order t. Restating what we have just said:

$$\sum_{t \mid p-1} \psi(t) = p-1$$

From Theorem 4 of Section 9, we have

$$\sum_{t \mid p-1} \psi(t) = \sum_{t \mid p-1} \phi(t) \tag{3}$$

If we can show that $\psi(t) \leqslant \phi(t)$ for each t, it will follow from (**??**) that $\psi(t) = \phi(t)$ for each t. In particular, the number of primitive roots of p will be $\psi(p-1) = \phi(p-1)$.

Choose some t. If $\psi(t) = 0$, then $\psi(t) < \phi(t)$ and we are done. If $\psi(t) \neq 0$, then there is an integer with order t; call it a. The congruence

$$x^t \equiv 1 \pmod{p} \tag{4}$$

has, according to Lemma 3, exactly t solutions. Furthermore, (4) is satisfied by the t integers

$$a, a^2, a^3, \ldots, a^t \tag{5}$$

Why is this so? Note that a has order t, so $a, a^2, a^3, \ldots, a^{t-1}$ cannot be congruent to 1. And because a^t is congruent to 1, $a^{t+1} \equiv a^t a \equiv a \pmod{p}$ so the cycle will repeat again. Also note that no two of the numbers in (5) have the same least residue (mod p), because else the sequence will have repetition and it won't ever be congruent to 1.

From Lemma 1, the numbers in (5) that have order t are those powers a^k with $(k, t) = 1$. But there are $\phi(t)$ such numbers k. Hence $\psi(t) = \phi(t)$ in this case. As noted above, this completes the proof. □

Corollary 10.3. If p is a prime and $t \mid (p-1)$, then the number of least residues (mod p) with order t is $\phi(t)$.

Proof. This follows from $\psi(t) = \phi(t)$ on the previous proof. □

Theorem 10.7 (Wilson's Theorem, alternate proof)**.** If p is a prime, $(p-1)! \equiv -1 \pmod{p}$.

Proof. The case $p = 2$ can be confirmed by calculation. Now let g be a primitive root of the odd prime p. From Theorem 5, we know that the lest residues (mod p) of $g, g^2, \ldots, g^{p-1}$ are a permutation of $1, 2, \ldots, p-1$. Multiplying and using the fact that

$$1 + 2 + 3 + \cdots + (p-1) = (p-1)p/2,$$

we get

$$1 \cdot 2 \cdots (p-1) \equiv g \cdot g^2 \cdots g^{p-1} \pmod{p}$$

or

$$(p-1)! \equiv (g^p)^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}.$$

But $g^{(p-1)/2}$ satisfies $x^2 \equiv 1 \pmod{p}$, and we know that $g^{(p-1)/2} \equiv 1$ or -1 (mod p). But the first case is impossible, since g is a primitive root of p. Thus $(p-1)! \equiv -1 \pmod{p}$. □