2.2 Inverses and GCDs

Solutions to Equations and Inverses mod n

In the last section we explored multiplication in Z_n. We saw in the special case with $n = 12$ and $a = 4$ that if we used multiplication by a in Z_n to encrypt a message, then our receiver would need to be able to solve, for x, the equation $4 \cdot_n x = b$ in order to decode a received message b. We saw that if the encrypted message was 0, then there were four possible values for x. More generally, Exercise 2.2-6 and some of the problems in the last section show that for certain values of n, a, and b, equations of the form $a \cdot_n x = b$ have a unique solution, while for other values of n, a, and b, the equation could have no solutions, or more than one solution.

To decide whether an equation of the form $a \cdot_n x = b$ has a unique solution in Z_n, it helps know whether a has a *multiplicative inverse* in Z_n, that is, whether there is another number a' such that $a' \cdot_n a = 1$. For example, in Z_9, the inverse of 2 is 5 because $2 \cdot_9 5 = 1$. On the other hand, 3 does not have an inverse in Z_9, because the equation $3 \cdot_9 x = 1$ does not have a solution. (This can be verified by checking the 9 possible values for x.) If a does have an inverse a', then we can find a solution to the equation

$$a \cdot_n x = b \ .$$

To do so, we multiply both sides of the equation by a', obtaining

$$a' \cdot_n (a \cdot_n x) = a' \cdot_n b.$$

By the associative law, this gives us

$$(a' \cdot_n a) \cdot_n x = b.$$

But $a' \cdot_n a = 1$ by definition so we have that

$$x = a' \cdot_n b \ .$$

Since this computation is valid for any x that satisfies the equation, we conclude that the only x that satisfies the equation is $a' \cdot_n b$. We summarize this discussion in the following lemma.

Lemma 2.5 *Suppose a has a multiplicative inverse a' in Z_n. Then for any $b \in Z_n$, the equation*

$$a \cdot_n x = b$$

has the unique solution

$$x = a' \cdot_n b \ .$$

Note that this lemma holds for *any* value of $b \in Z_n$.

This lemma tells us that whether or not a number has an inverse mod n is important for the solution of modular equations. We therefore wish to understand exactly when a member of Z_n has an inverse.

Inverses mod n

We will consider some of the examples related to Problem 9 of the last section.

Exercise 2.2-1 Determine whether every element a of Z_n has an inverse for n= 5, 6, 7, 8, and 9.

Exercise 2.2-2 If an element of Z_n has a multiplicative inverse, can it have two different multiplicative inverses?

For Z_5, we can determine by multiplying each pair of nonzero members of Z_5 that the following table gives multiplicative inverses for each element a of Z_5. For example, the products $2 \cdot_5 1 = 2$, $2 \cdot_5 2 = 4$, $2 \cdot_5 3 = 1$, and $2 \cdot_5 4 = 3$ tell us that 3 is the unique multiplicative inverse for 2 in Z_5. This is the reason we put 3 below 2 in the table. One can make the same kinds of computations with 3 or 4 instead of 2 on the left side of the products to get the rest of the table.

a	1	2	3	4
a'	1	3	2	4

For Z_7, we have similarly the table

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

.

For Z_9, we have already said that $3 \cdot_9 x = 1$ does not have a solution, so by Lemma 2.5, 3 does not have an inverse. (Notice how we are using the Lemma. The Lemma says that if 3 had an inverse, then the equation $3 \cdot_9 x = 1$ *would* have a solution, and this would contradict the fact that $3 \cdot_9 x = 1$ does not have a solution. Thus assuming that 3 had an inverse would lead us to a contradiction. Therefore 3 has no multiplicative inverse.)

This computation is a special case of the following corollary to Lemma 2.5.

Corollary 2.6 *Suppose there is a b in Z_n such that the equation*

$$a \cdot_n x = b$$

does not have a solution. Then a does not have a multiplicative inverse in Z_n.

Proof: Suppose that $a \cdot_n x = b$ has no solution. Suppose further that a does have a multiplicative inverse a' in Z_n. Then by Lemma 2.5, $x = a'b$ is a solution to the equation $a \cdot_n x = b$. This contradicts the hypothesis given in the corollary that the equation does not have a solution. Thus some supposition we made above must be incorrect. One of the assumptions, namely that $a \cdot_n x = b$ has no solution was the hypothesis given to us in the statement of the corollary. The only other supposition we made was that a has an inverse a' in Z_n. Thus this supposition must be incorrect as it led to the contradiction. Therefore, it must be case that a does not have a multiplicative inverse in Z_n. ■

Our proof of the corollary is a classical example of the use of contradiction in a proof. The principle of *proof by contradiction* is the following.

Principle 2.1 (Proof by contradiction) *If by assuming a statement we want to prove is false, we are lead to a contradiction, then the statement we are trying to prove must be true.*

We can actually give more information than Exercise 1 asks for. You can check that the table below shows an X for the elements of Z_9 that do not have inverses and gives an inverse for each element that has one

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

.

In Z_6, 1 has an inverse, namely 1, but the equations

$$2 \cdot_6 1 = 2, \quad 2 \cdot_6 2 = 4, \quad 2 \cdot_6 3 = 0, \quad 2 \cdot_6 4 = 2, \quad 2 \cdot_6 5 = 4$$

tell us that 2 does not have an inverse. Less directly, but with less work, we see that the equation $2 \cdot_6 x = 3$ has no solution because $2x$ will always be even, so $2x \bmod 6$ will always be even. Then Corollary 2.6 tells us that 2 has no inverse. Once again, we give a table that shows exactly which elements of Z_6 have inverses.

a	1	2	3	4	5
a'	1	X	X	X	5

A similar set of equations shows that 2 does not have an inverse in Z_8. The following table shows which elements of Z_8 have inverses.

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

.

We see that every nonzero element in Z_5 and Z_7 does have a multiplicative inverse, but in Z_6, Z_8, and Z_9, some elements do not have a multiplicative inverse. Notice that 5 and 7 are prime, while 6, 8, and 9 are not. Further notice that the elements in Z_n that do not have a multiplicative inverse are exactly those that share a common factor with n.

We showed that 2 has exactly one inverse in Z_5 by checking each multiple of 2 in Z_5 and showing that exactly one multiple of 2 equals 1. In fact, for any element that has an inverse in Z_5, Z_6, Z_7, Z_8, and Z_9, you can check in the same way that it has exactly one inverse. We explain why in a theorem.

Theorem 2.7 *If an element of Z_n has a multiplicative inverse, then it has exactly one inverse.*

Proof: Suppose that an element a of Z_n has an inverse a'. Suppose that a^* is also an inverse of a. Then a' is a solution to $a \cdot_n x = 1$ and a^* is a solution to $a \cdot_n x = 1$. But by Lemma 2.5, the equation $a \cdot_n x = 1$ has a unique solution. Therefore $a' = a^*$. ■

Just as we use a^{-1} to denote the inverse of a in the real numbers, we use a^{-1} to denote the unique inverse of a in Z_n when a has an inverse. Now we can say precisely what we mean by division in Z_n. We will define what we mean by *dividing* a member of Z_n by a if and only if a has an inverse $a^{-1} \bmod n$; in this case dividing b by $a \bmod n$ is defined to be same as multiplying b by $a^{-1} \bmod n$. We were led to our discussion of inverses because of their role in solving equations. We observed that in our examples, an element of Z_n that has an inverse mod n has no factors greater than 1 in common with n. This is a statement about a and n as integers with ordinary multiplication rather than multiplication mod n. Thus to prove that a has an inverse mod n if and only if a and n have no common factors other than 1 and -1, we have to convert the equation $a \cdot_n x = 1$ into an equation involving ordinary multiplication.

Converting Modular Equations to Normal Equations

We can re-express the equation

$$a \cdot_n x = 1$$

as

$$ax \bmod n = 1.$$

But the definition of $ax \bmod n$ is that it is the remainder r we get when we write $ax = qn + r$, with $0 \leq r < n$. This means that $ax \bmod n = 1$ if and only if there is an integer q with $ax = qn + 1$, or

$$ax - qn = 1. \tag{2.8}$$

Thus we have shown

Lemma 2.8 *The equation*

$$a \cdot_n x = 1$$

has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1.$$

Proof: We simply take $y = -q$. ■

We make the change from $-q$ to y for two reasons. First, if you read a number theory book, you are more likely to see the equation with y in this context. Second, to solve this equation, we must find both x and y, and so using a letter near the end of the alphabet in place of $-q$ emphasizes that this is a variable for which we need to solve.

It appears that we have made our work harder, not easier, as we have converted the problem of solving (in Z_n) the equation $a \cdot_n x = 1$, an equation with just one variable x (that could only have $n-1$ different values), to a problem of solving Equation 2.8, which has two variables, x and y. Further, in this second equation, x and y can take on any integer values, even negative values.

However, this equation will prove to be exactly what we need to prove that a has an inverse mod n if and only if a and n have no common factors larger than one.

Greatest Common Divisors (GCD)

Exercise 2.2-3 Suppose that a and n are integers such that $ax + ny = 1$, for some integers x and y. What does that tell us about being able to find a (multiplicative) inverse for $a \pmod n$? In this situation, if a has an inverse in Z_n, what is it?

Exercise 2.2-4 If $ax + ny = 1$ for integers x and y, can a and n have any common divisors other than 1 and -1?

In Exercise 2.2-3, since by Lemma 2.8, the equation $a \cdot_n x = 1$ has a solution in Z_n if and only if there exist integers x and y such that $ax + ny = 1$, we can can conclude that

Theorem 2.9 *A number a has a multiplicative inverse in Z_n if and only if there are integers x and y such that $ax + ny = 1$.*

We answer the rest of Exercise 2.2-3 with a corollary.

Corollary 2.10 *If $a \in Z_n$ and x and y are integers such that $ax+ny = 1$, then the multiplicative inverse of a in Z_n is $x \bmod n$.*

Proof: Since $n \cdot_n y = 0$ in Z_n, we have $a \cdot_n x = 1$ in Z_n and therefore x is the inverse of a in Z_n. ■

Now let's consider Exercise 2.2-4. If a and n have a common divisor k, then there must exist integers s and q such that

$$a = sk$$

and

$$n = qk \ .$$

Substituting these into $ax + ny = 1$, we obtain

$$\begin{aligned} 1 &= ax + ny \\ &= skx + qky \\ &= k(sx + qy). \end{aligned}$$

But then k is a divisor of 1. Since the only integer divisors of 1 are ± 1, we must have $k = \pm 1$. Therefore a and n can have no common divisors other than 1 and -1.

In general, the **greatest common divisor** of two numbers j and k is the largest number d that is a factor of both j and k.[4] We denote the greatest common divisor of j and k by $\gcd(j, k)$.

We can now restate Exercise 2.2-4 as follows:

Lemma 2.11 *Given a and n, if there exist integers x and y such that $ax + ny = 1$ then $\gcd(a, n) = 1$.*

If we combine Theorem 2.9 and Lemma 2.11, we see that that if a has a multiplicative inverse mod n, then $\gcd(a, n) = 1$. It is natural to ask whether the statement that "if $\gcd a, n = 1$, then a has a multiplicative inverse" is true as well.[5] If so, this would give us a way to test whether a has a multiplicative inverse mod n by computing the greatest common divisor of a and n. For this purpose we would need an algorithm to find $\gcd(a, n)$. It turns out that there is such an algorithm, and a byproduct of the algorithm is a proof of our conjectured converse statement! When two integers j and k have $\gcd(j, k) = 1$, we say that j and k are *relatively prime*.

Euclid's Division Theorem

One of the important tools in understanding greatest common divisors is Euclid's Division Theorem, a result which has already been important to us in defining what we mean by $m \bmod n$. While it appears obvious, as do many theorems in number theory, it follows from simpler principles of number theory, and the proof helps us understand how the greatest common divisor

[4] There is one common factor of j and k for sure, namely 1. No common factor can be larger than the smaller of j and k in absolute value, and so there must be a largest common factor.

[5] Notice that this statement is *not* equivalent to the statement in the lemma. This statement is what is called the "converse" of the lemma; we will explain the idea of converse statements more in Chapter 3.

algorithm works. Thus we restate it and present a proof here. Our proof uses the method of proof by contradiction, which you first saw in Corollary 2.6. Notice that we are assuming m is nonnegative which we didn't assume in our earlier statement of Euclid's Division Theorem, Theorem 2.1. In Problem 16 we will explore how we can remove this additional assumption.

Theorem 2.12 (Euclid's Division Theorem, restricted version) *For every nonnegative integer m and positive integer n, there exist unique integers q and r such that $m = nq + r$ and $0 \leq r < n$. By definition, r is equal to $m \bmod n$.*

Proof: To prove this theorem, assume instead, for purposes of contradiction, that it is false. Among all pairs (m, n) that make it false, choose the smallest m that makes it false. We cannot have $m < n$ because then the statement would be true with $q = 0$ and $r = m$, and we cannot have $m = n$ because then the statement is true with $q = 1$ and $r = 0$. This means $m - n$ is a positive number smaller than m. We assumed that m was the smallest value that made the lemma false, and so the theorem must be true for the pair $(m-n, n)$. Therefore, there must exist a q' and r' such that

$$m - n = q'n + r', \text{ with } 0 \leq r' < n.$$

Thus $m = (q' + 1)n + r'$, and by setting $q = q' + 1$ and $r = r'$, we can satisfy the theorem for the pair (m, n), contradicting the assumption that the statement is false. Thus the only possibility is that the statement is true. ■

We call the proof technique used here *proof by smallest counterexample*. In this method, we assume, as in all proofs by contradiction, that the theorem is false. This implies that there must be a *counterexample* which does not satisfy the conditions of the theorem. In this case that counterexample consists of numbers m and n such that *no* integers q and r exist which satisfy $m = qn + r$. Further, if there are counterexamples, then there must be one that is smallest in some sense. (Here being smallest means having the smallest m.) We choose such a smallest one, and then reason that if it exists, then every smaller example is true. If we can then use a smaller true example to show that our supposedly false example is true as well, we have created a contradiction. The only thing this can contradict is our assumption that the theorem was false. Therefore this assumption has to be invalid, and the theorem has to be true. As we will see in Chapter **??**, this method is closely related to a proof method called *proof by induction* and to recursive algorithms. In essence, the proof of Theorem 2.1 describes a recursive program to find q and r in the theorem above so that $0 \leq r < n$.

Exercise 2.2-5 Suppose that $k = jq + r$ as in Euclid's Division Theorem. Is there a relationship between $\gcd(j, k)$ and $\gcd(r, j)$?

In this exercise, if $r = 0$, then $\gcd(r, j)$ is j, because any number is a divisor of zero. But this is the GCD of k and j as well since in this case $k = jq$. The answer to the remainder of Exercise 2.2-5 appears in the following lemma.

Lemma 2.13 *If j, k, q, and r are positive integers such that $k = jq + r$ then*

$$\gcd(j, k) = \gcd(r, j). \tag{2.9}$$

Proof: In order to prove that both sides of Equation 2.9 are equal, we will show that they have exactly the same set of factors. That is, we will first show that if d is a factor of the left-hand side, then it is a factor of the right-hand side. Second, we will show that if d is a factor of the right-hand side, then it is a factor of the left-hand side.

If d is a factor of $\gcd(j,k)$ then it is a factor of both j and k. There must be integers i_1 and i_2 so that $k = i_1 d$ and $j = i_2 d$. Thus d is also a factor of

$$\begin{aligned} r &= k - jq \\ &= i_1 d - i_2 dq \\ &= (i_1 - i_2 q)d \ . \end{aligned}$$

Since d is a factor of j (by supposition) and r (by the equation above), it must be a factor of $\gcd(r,j)$.

Similarly, if d is a factor of $\gcd(r,j)$, it is a factor of j and r, and we can write $j = i_3 d$ and $r = i_4 d$. Therefore,

$$\begin{aligned} k &= jq + r \\ &= i_3 dq + i_4 d \\ &= (i_3 q + i_4)d \ , \end{aligned}$$

and d is a factor of k and therefore of $\gcd(j,k)$.

Since $\gcd(j,k)$ has the same factors as $\gcd(r,j)$ they must be equal. ■

While we did not need to assume $r < j$ in order to prove the lemma, Theorem 2.1 tells us we may assume $r < j$. The assumption in the lemma that j, q and r are positive implies that $j < k$. Thus this lemma reduces our problem of finding $\gcd(j,k)$ to the simpler (in a recursive sense) problem of finding $\gcd(r,j)$.

The GCD Algorithm

Exercise 2.2-6 Using Lemma 2.13, write a recursive algorithm to find $\gcd(j,k)$, given that $j \leq k$. Use it (by hand) to find the GCD of 24 and 14 and the GCD of 252 and 189.

Our algorithm for Exercise 2.2-6 is based on Lemma 2.13 and the observation that if $k = jq$, for any q, then $j = \gcd(j,k)$. We first write $k = jq + r$ in the usual way. If $r = 0$, then we return j as the greatest common divisor. Otherwise, we apply our algorithm to find the greatest common divisor of j and r. Finally, we return the result as the greatest common divisor of j and k.

To find

$$\gcd(14, 24)$$

we write

$$24 = 14(1) + 10.$$

In this case $k = 24$, $j = 14$, $q = 1$ and $r = 10$. Thus we can apply Lemma 2.13 and conclude that

$$\gcd(14, 24) = \gcd(10, 14).$$

We therefore continue our computation of $\gcd(10, 14)$, by writing $14 = 10 \cdot 1 + 4$, and have that

$$\gcd(10, 14) = \gcd(4, 10).$$

Now,

$$10 = 4 \cdot 2 + 2,$$

and so

$$\gcd(4, 10) = \gcd(2, 4).$$

Now

$$4 = 2 \cdot 2 + 0,$$

so that now $k = 4$, $j = 2$, $q = 2$, and $r = 0$. In this case our algorithm tells us that our current value of j is the GCD of the original j and k. This step is the base case of our recursive algorithm. Thus we have that

$$\gcd(14, 24) = \gcd(2, 4) = 2.$$

While the numbers are larger, it turns out to be even easier to find the GCD of 252 and 189. We write

$$252 = 189 \cdot 1 + 63,$$

so that $\gcd(189, 252) = \gcd(63, 189)$, and

$$189 = 63 \cdot 3 + 0.$$

This tells us that $\gcd(189, 252) = \gcd(189, 63) = 63$.

Extended GCD algorithm

By analyzing our process in a bit more detail, we will be able to return not only the greatest common divisor, but also numbers x and y such that $\gcd(j, k) = jx + ky$. This will solve the problem we have been working on, because it will prove that if $\gcd(a, n) = 1$, then there are integers x and y such that $ax + ny = 1$. Further it will tell us how to find x, and therefore the multiplicative inverse of a.

In the case that $k = jq$ and we want to return j as our greatest common divisor, we also want to return 1 for the value of x and 0 for the value of y. Suppose we are now in the case that that $k = jq + r$ with $0 < r < j$ (that is, the case that $k \neq jq$). Then we recursively compute $\gcd(r, j)$ and in the process get an x' and a y' such that $\gcd(r, j) = rx' + jy'$. Since $r = k - jq$, we get by substitution that

$$\gcd(r, j) = (k - jq)x' + jy' = kx' + j(y' - qx').$$

Thus when we return $\gcd(r, j)$ as $\gcd(j, k)$, we want to return the value of x' as y and and the value of $y' - qx'$ as x.

We will refer to the process we just described as "Euclid's extended GCD algorithm."

Exercise 2.2-7 Apply Euclid's extended GCD algorithm to find numbers x and y such that the GCD of 14 and 24 is $14x + 24y$.

For our discussion of Exercise 2.2-7 we give pseudocode for the extended GCD algorithm. While we expressed the algorithm more concisely earlier by using recursion, we will give an iterative version that is longer but can make the computational process clearer. Instead of using the variables q, j, k, r, x and y, we will use six arrays, where $q[i]$ is the value of q computed on the ith iteration, and so forth. We will use the index zero for the input values, that is $j[0]$ and $k[0]$ will be the numbers whose gcd we wish to compute . Eventually $x[0]$ and $y[0]$ will become the x and y we want.

```
gcd(j, k)
// assume that j < k
(1)  i = 0; k[i] = k; j[i] = j
(2)  Repeat
(3)        q[i] = ⌊k[i]/j[i]⌋
(4)        r[i] = k[i] − q[i]j[i]
(5)        k[i + 1] = j[i]; j[i + 1] = r[i]
(6)        i = i + 1
(7)  Until  (r[i − 1] = 0)
// we have found the value of the gcd, now we compute the x and y
(8)  i = i − 1
(9)  gcd = j[i]
(10) y[i] = 0; x[i] = 1
(11) i = i − 1
(12) While (i ≥ 0)
(13)       y[i] = x[i + 1]
(14)       x[i] = y[i + 1] − q[i]x[i + 1]
(15)       i = i − 1
(16) Return gcd
(17) Return x
(18) Return y
```

(In Line 3 we are using the notation $\lfloor x \rfloor$ to stand for the floor of x, the largest integer less than or equal to x.)

We show the details of how this algorithm applies to $\gcd(24, 14)$ in Table 2.1. In a row, the $q[i]$ and $r[i]$ values are computed from the $j[i]$ and $k[i]$ values. Then the $j[i]$ and $r[i]$ are passed down to the next row as $k[i+1]$ and $j[i+1]$ respectively. This process continues until we finally reach a case where $k[i] = q[i]j[i]$ and we can answer $j[i]$ for the gcd. We can then begin computing $x[i]$ and $y[i]$. In the row with $i = 3$, we have that $x[i] = 0$ and $y[i] = 1$. Then, as i decreases, we compute $x[i]$ and $y[i]$ for a row by setting $y[i]$ to $x[i+1]$ and $x[i]$ to $y[i+1] - q[i]x[i+1]$. We note that in every row, we have the property that $j[i]x[i] + k[i]y[i] = \gcd(j, k)$.

We summarize Euclid's extended GCD algorithm in the following theorem:

Theorem 2.14 *Given two integers j and k, Euclid's extended GCD algorithm computes* $\gcd(j, k)$ *and two integers x and y such that* $\gcd(j, k) = jx + ky$.

We now use Eculid's extended GCD algorithm to extend Lemma 2.11.

$\underline{i}$	$\underline{j[i]}$	$\underline{k[i]}$	$\underline{q[i]}$	$\underline{r[i]}$	$\underline{x[i]}$	$\underline{y[i]}$
0	14	24	1	10		
1	10	14	1	4		
2	4	10	2	2		
3	2	4	2	0	1	0
2	4	10	2	2	-2	1
1	10	14	1	4	3	-2
0	14	24	1	10	-5	3
$\gcd = 2$						
$x = -5$						
$y = 3$						

Table 2.1: The computation of $\gcd(14, 24)$ by algorithm $\gcd(j, k)$.

Theorem 2.15 *Two positive integers j and k have greatest common divisor 1 (and thus are relatively prime) if and only if there are integers x and y such that $jx + ky$=1.*

Proof: The statement that if there are integers x and y such that $jx+ky = 1$, then $\gcd(j, k) = 1$ is proved in Lemma 2.11. In other words, $\gcd(j, k) = 1$ if there are integers x and y such that $jx + ky = 1$.

On the other hand, we just showed, by Euclid's extended GCD algorithm, that given positive integers j and k, there are integers x and y such that $\gcd(j, k) = jx+ky$. Therefore, $\gcd(j, k) = 1$ only if there are integers x and y such that $jx + ky = 1$. ■

Combining Lemma 2.8 and Theorem 2.15, we obtain:

Corollary 2.16 *For any positive integer n, an element a of Z_n has a multiplicative inverse if and only if* $\gcd(a, n) = 1$.

Using the fact that if n is prime, $\gcd(a, n) = 1$ for all non-zero $a \in Z_n$, we obtain

Corollary 2.17 *For any prime p, every non-zero element a of Z_p has an inverse.*

Computing Inverses

Not only does Euclid's extended GCD algorithm tell us if an inverse exists, but, just as we saw in Exercise 2.2-3 it computes it for us. Combining Exercise 2.2-3 with Theorem 2.15, we get

Corollary 2.18 *If an element a of Z_n has an inverse, we can compute it by running Euclid's extended GCD algorithm to determine integers x and y so that $ax + ny = 1$; then the inverse of a is $x \bmod n$.*

For completeness, we now give pseudocode which determines whether an element a in Z_n has an inverse and computes the inverse if it exists:

```
inverse(a, n)
(1)  Run procedure gcd(a, n) to obtain gcd(a, n), x and y
(2)  if gcd(a, n) = 1
(3)       return x
(4)  else
(5)       print ‘‘no inverse exists’’
```

The correctness of the algorithm follows immediately from the fact that $\gcd(a, n) = ax + ny$, so if $\gcd(a, n) = 1$, $ax \bmod n$ must be equal to 1.

Important Concepts, Formulas, and Theorems

1. *Multiplicative inverse.* a' is a multiplicative inverse of a in Z_n if $a \cdot_n a' = 1$. If a has a multiplicative inverse, then it has a unique multiplicative inverse which we denote by a^{-1}.

2. *An important way to solve modular equations.* Suppose a has a multiplicative inverse mod n, and this inverse is a^{-1}. Then for any $b \in Z_n$, the unique solution to the equation

$$a \cdot_n x = b$$

   is

$$x = a^{-1} \cdot_n b \ .$$

3. *Converting modular to regular equations.* The equation

$$a \cdot_n x = 1$$

   has a solution in Z_n if and only if there exist integers x and y such that

$$ax + ny = 1 \ .$$

4. *When do inverses exist in Z_n?* A number a has a multiplicative inverse in Z_n if and only if there are integers x and y such that $ax + ny = 1$.

5. *Greatest common divisor (GCD).* The *greatest common divisor* of two numbers j and k is the largest number d that is a factor of both j and k.

6. *Relatively prime.* When two numbers, j and k have $\gcd(j, k) = 1$, we say that j and k are relatively prime.

7. *Connecting inverses to GCD.* Given a and n, if there exist integers x and y such that $ax + ny = 1$ then $\gcd(a, n) = 1$.

8. *GCD recursion lemma.* If j, k, q, and r are positive integers such that $k = jq + r$ then $\gcd(j, k) = \gcd(r, j)$.

9. *Euclid's GCD algorithm.* Given two numbers j and k, this algorithm returns $\gcd(j, k)$.

10. *Euclid's extended GCD algorithm.* Given two numbers j and k, this algorithm returns $\gcd(j, k)$, and two integers x and y such that $\gcd(j, k) = jx + ky$.

11. *Relating GCD of 1 to Euclid's extended GCD algorithm.* Two positive integers j and k have greatest common divisor 1 if and only if there are integers x and y such that $jx + ky$=1. One of the integers x and y could be negative.

12. *Restatement for Z_n.* $\gcd(a, n) = 1$ if and only if there are integers x and y such that $ax + ny = 1$.

13. *Condition for multiplicative inverse in Z_n* For any positive integer n, an element a of Z_n has an inverse if and only if $\gcd(a, n) = 1$.

14. *Multiplicative inverses in Z_p, p prime* For any prime p, every non-zero element a of Z_p has a multiplicative inverse.

15. *A way to solve some modular equations $a \cdot_n x = b$.* Use Euclid's extended GCD algorithm to compute a^{-1} (if it exists), and multiply both sides of the equation by a^{-1}. (If a has no inverse, the equation might or might not have a solution.)

Problems

1. If $a \cdot 133 - m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

2. If $a \cdot 133 - 2m \cdot 277 = 1$, does this guarantee that a has an inverse mod m? If so, what is it? If not, why not?

3. Determine whether every nonzero element of Z_n has a multiplicative inverse for $n = 10$ and $n = 11$.

4. How many elements a are there such that $a \cdot_{31} 22 = 1$? How many elements a are there such that $a \cdot_{10} 2 = 1$?

5. Given an element b in Z_n, what can you say in general about the possible number of elements a such that $a \cdot_n b = 1$ in Z_n?

6. If $a \cdot 133 - m \cdot 277 = 1$, what can you say about all possible common divisors of a and m?

7. Compute the GCD of 210 and 126 by using Euclid's GCD algorithm.

8. If $k = jq + r$ as in Euclid's Division Theorem, is there a relationship between $\gcd(q, k)$ and $\gcd(r, q)$. If so, what is it?

9. Bob and Alice want to choose a key they can use for cryptography, but all they have to communicate is a bugged phone line. Bob proposes that they each choose a secret number, a for Alice and b for Bob. They also choose, over the phone, a prime number p with more digits than any key they want to use, and one more number q. Bob will send Alice bq mod p, and Alice will send Bob aq mod p. Their key (which they will keep secret) will then be abq mod p. (Here we don't worry about the details of how they use their key, only with how they choose it.) As Bob explains, their wire tapper will know p, q, aq mod p, and bq mod p, but will not know a or b, so their key should be safe.

   Is this scheme safe, that is can the wiretapper compute abq mod p? If so, how does she do it?

Alice says "You know, the scheme sounds good, but wouldn't it be more complicated for the wire tapper if I send you $q^a \bmod p$, you send me $q^b \pmod p$ and we use $q^{ab} \bmod p$ as our key?" In this case can you think of a way for the wire tapper to compute $q^{ab} \bmod p$? If so, how can you do it? If not, what is the stumbling block? (It is fine for the stumbling block to be that you don't know how to compute something, you don't need to prove that you can't compute it.)

10. Write pseudocode for a recursive version of the extended GCD algorithm.

11. Run Euclid's extended GCD algorithm to compute $\gcd(576, 486)$. Show all the steps.

12. Use Euclid's extended GCD algorithm to compute the multiplicative inverse of 16 modulo 103.

13. Solve the equation $16 \cdot_{103} x = 21$ in Z_{103}.

14. Which elements of Z_{35} do not have multiplicative inverses in Z_{35}?

15. If $k = jq + r$ as in Euclid's Division Theorem, is there a relationship between $\gcd(j, k)$ and $\gcd(r, k)$. If so, what is it?

16. Notice that if m is negative, then $-m$ is positive, so that by Theorem 2.12 $-m = qn + r$, where $0 \leq r < n$. This gives us $m = -qn - r$. If $r = 0$, then we have written $m = q'n + r'$, where $0 \leq r' \leq n$ and $q' = -q$. However if $r > 0$, we cannot take $r' = -r$ and have $0 \leq r' < n$. Notice, though, that since since we have already finished the case $r = 0$ we may assume that $0 \leq n - r < n$. This suggests that if we were to take r' to be $n - r$, we might be able to find a q' so that $m = q'n + r'$ with $0 \leq r' \leq n$, which would let us conclude that Euclid's Division Theorem is valid for negative values m as well as nonnegative values m. Find a q' that works and explain how you have extended Euclid's Division Theorem from the version in Theorem 2.12 to the version in Theorem 2.1.

17. The Fibonacci numbers F_i are defined as follows:

$$F_i = \begin{cases} 1 & \text{if } i \text{ is 1 or 2} \\ F_{i-1} + F_{i-2} & \text{otherwise.} \end{cases}$$

What happens when you run Euclid's extended GCD algorithm on F_i and F_{i-1}? (We are asking about the execution of the algorithm, not just the answer.)

18. Write (and run on several different inputs) a program to implement Euclid's extended GCD algorithm. Be sure to return x and y in addition to the GCD. About how many times does your program have to make a recursive call to itself? What does that say about how long we should expect it to run as we increase the size of the j and k whose GCD we are computing?

19. The least common multiple of two positive integers x and y is the smallest positive integer z such that z is an integer multiple of both x and y. Give a formula for the least common multiple that involves the GCD.

20. Write pseudocode that given integers a, b and n in Z_n, either computes an x such that $a \cdot_n x = b$ or concludes that no such x exists.

21. Give an example of an equation of the form $a \cdot_n x = b$ that has a solution even though a and n are not relatively prime, or show that no such equation exists.