Chapter 1. Number Theory

§ 1. Modular Arithmetic

Let m be any positive integer and consider any pair of integers a and b. We say that $a \equiv b \bmod m$ when a and b differ by a multiple of m.

Example: $5 \equiv 29 \bmod 3$ since 29 - 5 = 24 and 24 is a multiple of 3.

Example: What are all the integers a such that $a \equiv 3 \bmod 5$?

We need all the integers a that differ from 3 by a multiple of 5:

$$\ldots, -17, -12, -7, -2, 3, 8, 13, 18, \ldots$$

So $a \equiv 3 \bmod 5$ is just a compact way to describe this arithmetic progression.

Example: What does it mean about the integers a and b to say that $a \equiv b \bmod 2$?

By definition it means that a and b differ by a multiple of 2. There are two possibilities. Either a and b both lie in the arithmetic progression

$$\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots$$

and $a \equiv b \equiv 0 \mod 2$ or they both lie in

$$\ldots, -5, -3, -1, 1, 3, 5, \ldots$$

and $a \equiv b \equiv 1 \bmod 2$.

Example: Every pair of integers a and b satisfies the congruence $a \equiv b \bmod 1$ since any two integers differ by an integer multiple of 1.

We have seen in the examples above that every integer is congruent to either 0 or to 1 modulo 2. If we work modulo 3 we find that there are 3 possibilites. Every integer a lies in *exactly one* of the arithmetic progressions

$$\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots (a \equiv 0 \bmod 3)$$
$$\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots (a \equiv 1 \bmod 3)$$
$$\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots (a \equiv 2 \bmod 3)$$

In general, if we work mod m, then every integer will be congruent to exactly one of the numbers $\{0, 1, 2, \ldots m-1\}$. We will refer to this set of integers as *the* *standard set of representatives* modulo m. Each number a here *represents* an arithmetic progression:

$$\ldots, a-2m, a-m, a, a+m, a+2m, \ldots$$

This is true because of the division algorithm. Given an integer x and a modulus m, we can find integers q and r so that

$$x = q \cdot m + r \text{ where } 0 \leq r < m$$

Since x and r differ by a multiple of m, we have $x \equiv r \bmod m$ amd r is in the set $\{0, 1, 2, 3, 4\}$.

Example: Find the standard representatives for 97 mod 5, 97 mod 7, 97 mod 6, 97 mod 12, and 97 mod 35.

In each case apply the division algorithm:

$$\begin{aligned}
97 = 5 \cdot 19 + 2 &\Rightarrow 97 \equiv 2 \bmod 5 \\
97 = 7 \cdot 13 + 6 &\Rightarrow 97 \equiv 6 \bmod 7 \\
97 = 6 \cdot 16 + 1 &\Rightarrow 97 \equiv 1 \bmod 6 \\
97 = 1 + 12 \cdot 8 &\Rightarrow 97 \equiv 1 \bmod 12 \\
97 = 27 + 2 \cdot 35 &\Rightarrow 97 \equiv 27 \bmod 35
\end{aligned}$$

It turns out that we can do arithmetic modulo m in much the same way that we do arithmetic with integers. Suppose we want to add 25 and 37 modulo 12. There are two natural approaches to this problem:

$$25 + 37 = 62 = 2 + 60 \equiv 2 \bmod 12$$

or

$$\begin{aligned}
25 &\equiv 1 \bmod 12 \\
37 &\equiv 1 \bmod 12 \\
\Rightarrow 25 + 37 &\equiv 2 \bmod 12
\end{aligned}$$

In our example it did not matter which method we used. Both gave the same result for 25 + 37 mod 12. This will always be the case:

Proposition: If $a \equiv \alpha \bmod m$ and $b \equiv \beta \bmod m$ then $a + b \equiv \alpha + \beta \bmod m$.

Proof: Since $a \equiv \alpha \bmod m$, we can find an integer j such that $a = \alpha + j \cdot m$. Similarly, we can find an integer k with the property that $b = \beta + k \cdot m$. Hence

$$a + b = \alpha + j \cdot m + \beta + k \cdot m = \alpha + \beta + (j + k) \cdot m$$

and therefore $a + b \equiv \alpha + \beta \bmod m$. Similarly $a - b \equiv \alpha - \beta \bmod m$ and

Proposition: If $a \equiv \alpha \bmod m$ and $b \equiv \beta \bmod m$ then $a \cdot b \equiv \alpha \cdot \beta \bmod m$.

Proof: As above we can find integers j and k such that $a = \alpha + j \cdot m$ and $b = \beta + k \cdot m$. So multiplying gives

$$a \cdot b = (\alpha + j \cdot m)(\beta + k \cdot m) = \alpha \cdot \beta + (j\beta + k\alpha + jkm)m$$

Example: Compute $150(25^8 + 37^5 - 99^2) \bmod 12$.

Solution: Since $150 \equiv 6 \bmod 12$, $25 \equiv 1 \bmod 12$, $37 \equiv 1 \bmod 12$ and $99 \equiv 3 \bmod 12$ we find

$$\begin{aligned} 150(25^8 + 37^5 - 99^2) &\equiv 6(1^8 + 1^5 + 3^2) \bmod 12 \\ &\equiv 6(1 + 1 + 9) \bmod 12 \\ &\equiv 6 \bmod 12. \end{aligned}$$

In many ways modular arithmetic behaves like ordinary arithmetic, but there are important differences. For example, recall the cancellation law for integers:

$$ax = ay \Rightarrow x = y \text{ provided that } a \neq 0.$$

This law does not hold for modular arithmetic. Consider the congruence $2x \equiv 4 \bmod 6$. Both sides contain a factor of 2, but we would be wrong to conclude that $x \equiv 2 \bmod 6$ since $2 \cdot 5 \equiv 4 \bmod 6$ and thus $x \equiv 5 \bmod 6$ is another solution.

Another difference between integer arithmetic and modular arithmetic, closely related to the failure of the cancellation law, is the existence of zero divisors. In the integers if $ab = 0$, then we can conclude that either $a = 0$ or $b = 0$. This is not true when we work mod m, as the example $2 \cdot 3 \equiv 0 \bmod 6$ illustrates.

§ 2. Division mod m

Consider the problem of finding all solutions to the linear congruence

$$ax \equiv b \bmod m.$$

If we were solving the equation $ax = b$, we would multiply both sides by the multiplicative inverse of a, provided it exists. That is, can we divide by a when we do arithmetic mod m?

Example: Find all integers x so that $3x \equiv 2 \bmod 5$.

Solution: We need to "divide" by 3 mod 5. Can we find an integer a so that $a \cdot 3 \equiv 1 \bmod 5$? Obviously we can: $2 \cdot 3 = 6 \equiv 1 \bmod 5$. Thus 2 is a multiplicative inverse for 3 mod 5.

So to solve the congruence, we just multiply through by 2 to get rid of the coefficient 3:

$$2 \cdot 3 \cdot x \equiv 2 \cdot 2 \bmod 5 \quad \Rightarrow \quad 1 \cdot x \equiv 4 \bmod 5$$

This shows that if $3x \equiv 2 \bmod 5$ then $x \equiv 4 \bmod 5$. It is also clear that if $x \equiv 4 \bmod 5$ then $3x \equiv 12 \equiv 2 \bmod 5$ so $x \equiv 4 \bmod 5$ is our solution.

Example: The example above showed that $2^{-1} \equiv 3 \bmod 5$ and $3^{-1} \equiv 2 \bmod 5$. Clearly 1 is its own inverse. What about the multiplicative inverse of 4 mod 5?

$$4 \cdot 4 = 16 \equiv 1 \bmod 5 \Rightarrow 4^{-1} \equiv 4 \bmod 5.$$

Example: Find all integers x so that $3x \equiv 2 \bmod 12$.

Solution: Before we search for a multiplicative inverse for 3 mod 12, notice what the congruence above becomes when we translate it into a statement about integers.

$$\begin{gathered} 3x \equiv 2 \bmod 12 \text{ is satisfied by an integer } x \\ \Updownarrow \\ \text{there is an integer k such that } 3x = 2 + 12 \cdot k \end{gathered}$$

Clearly, no such integers x and k can be found, because if they did exist we could write $2 = 3x - 12k$ and this would mean that 2 is an integer multiple of 3.

So $3x \equiv 2 \bmod 12$ has *no solutions*. We conclude that 3 is not invertible mod 12.

Example: Find all the invertible elements mod 12.

Solution: Let a be any integer. By definition a is invertible mod 12 if and only if there is an integer b such that

$$ab \equiv 1 \bmod 12.$$

Translating this into a statement about integers, we can say that a is invertible mod 12 if and only if there are integers b and k so that

$$ab = 1 + 12k.$$

Thus a is invertible mod 12 if and only if

$$\text{There are integers b and k so that } 1 = ab - 12k.$$

This cannot happen if a and 12 have a common divisor $d > 1$ because then d would be a divisor of $ab - 12k$, hence a divisor of 1.

We conclude that if a is congruent to $0, 2, 3, 4, 6, 8, 9$ or 10 modulo 12 then a is not invertible mod 12 (because all these numbers have a common divisor with

12). What about the numbers that are relatively prime to 12? We can easily check that 1, 5, 7, and 11 are all invertible mod 12:

$$\begin{aligned}
1 \cdot 1 &\equiv 1 \bmod 12 \Rightarrow 1^{-1} \equiv 1 \bmod 12 \\
5 \cdot 5 &\equiv 1 \bmod 12 \Rightarrow 5^{-1} \equiv 5 \bmod 12 \\
7 \cdot 7 &\equiv 1 \bmod 12 \Rightarrow 7^{-1} \equiv 7 \bmod 12 \\
11 \cdot 11 &\equiv 1 \bmod 12 \Rightarrow 11^{-1} \equiv 11 \bmod 12
\end{aligned}$$

Example: Find all the invertible elements modulo 15.

Solution: As we saw in the previous example, if a and 15 have a common divisor, then a will not be invertible modulo 15. So any integer that is congruent to $0, 3, 5, 6, 9, 10$ or 12 mod 15 will not be invertible. Every other integer is congruent to $1, 2, 4, 7, 8, 11, 13$ or 14. Again we can "guess" an inverse for each of these:

$$\begin{aligned}
1 \cdot 1 &\equiv 1 \bmod 15 \Rightarrow 1^{-1} \equiv 1 \bmod 15 \\
2 \cdot 8 &\equiv 1 \bmod 15 \Rightarrow 2^{-1} \equiv 8 \bmod 15 \text{ and } 8^{-1} \equiv 2 \bmod 15 \\
4 \cdot 4 &\equiv 1 \bmod 15 \Rightarrow 4^{-1} \equiv 4 \bmod 15 \\
7 \cdot 13 &\equiv 1 \bmod 15 \Rightarrow 7^{-1} \equiv 13 \bmod 15 \text{ and } 13^{-1} \equiv 7 \bmod 15 \\
11 \cdot 11 &\equiv 1 \bmod 15 \Rightarrow 11^{-1} \equiv 11 \bmod 15 \\
14 \cdot 14 &\equiv 1 \bmod 15 \Rightarrow 14^{-1} \equiv 14 \bmod 15.
\end{aligned}$$

§ 3. The Euclidean Algorithm

The discussion of divisibility mod m in the previous section suggests the following

Theorem: An integer a is invertible mod m if and only if a and m are relatively prime. In other words, a is invertible mod m if and only if the greatest common divisor d of a and m is 1.

Proof: As we saw above, if a and m have a common divisor $d > 1$ then it is impossible to find integers b and k so that $ab = 1 + mk$ since then d would be a divisor of 1. So if a is invertible mod m, then a and m are relatively prime.

Conversely, suppose that a and m are relatively prime. We must show that a is invertible mod m. In other words, we must show that it is possible to find integers b and k such that $ab = 1 + m \cdot k$. In our examples above, we did this by "guessing" or by trial-and-error. It turns out that there is a systematic approach, called the *Euclidean Algorithm* that gives us exactly what we need. Rather than give a formal proof we state the Euclidean algorithm and give some examples showing how it is used to find the inverse of a mod m in the case where a and m are relatively prime.

The Euclidean Algorithm

Given two integers a and b where $a < b$, carry out the following sequence of divisions:

$$\begin{aligned} a &= q_1 b + r_1 \text{ where } 0 \le r_1 < b \\ b &= q_2 r_1 + r_2 \text{ where } 0 \le r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 \text{ where } 0 \le r_3 < r_2 \\ r_2 &= q_4 r_3 + r_4 \text{ where } 0 \le r_4 < r_3 \\ &\dots \end{aligned}$$

This process must terminate after finitely many steps since at each step the new remainder is a positive integer that is *smaller than* the remainder at the previous step.

Example: Run the Euclidean algorithm on the numbers $a = 97$ and $b = 13$. Then find 13^{-1} mod 97.

Solution: The Euclidean algorithm gives the sequence

$$\begin{aligned} 97 &= 7 \cdot 13 + 6 \\ 13 &= 2 \cdot 6 + 1 \\ 6 &= 6 \cdot 1 + 0 \end{aligned}$$

To find 13^{-1} mod 97 we need to write 1 as an integer linear combination of 13 and 97. Solve the second equation above for 1 and substitute the first equation into it to get:

$$1 = 13 - 2 \cdot 6 = 13 - 2(97 - 7 \cdot 13) = 13 \cdot 15 - 2 \cdot 97$$

Hence $13 \cdot 15 \equiv 1 \bmod 97$ and $13^{-1} \equiv 15 \bmod 97$.

Example: Run the Euclidean algorithm on $a = 97$ and $b = 23$. Find 23^{-1} mod 97.

Solution: The Euclidean algorithm gives:

$$\begin{aligned} 97 &= 4 \cdot 23 + 5 \\ 23 &= 4 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

To find $23^{-1} \bmod 97$, we solve the next-to-last equation for 1 and then substitute to eventually eliminate all the remainders and write 1 as an integer linear combination of 23 and 97:

$$\begin{aligned}
1 &= 3 - 2 \\
&= 3 - (5 - 3) = 2 \cdot 3 - 5 \\
&= 2(23 - 4 \cdot 5) - 5 = 2 \cdot 23 - 9 \cdot 5 \\
&= 2 \cdot 23 - 9 \cdot (97 - 4 \cdot 23) = 23 \cdot 38 - 9 \cdot 97
\end{aligned}$$

Thus $23 \cdot 38 \equiv 1 \bmod 97$ and $23^{-1} \equiv 38 \bmod 97$.

It is important to understand what the Euclidean algorithm tells us about the greatest common divisor of a and b. The first step of the Euclidean algorithm looks like $a = q_1 \cdot b + r_1$. So if d divides a and d divides b then d must also divide r_1 and similarly if d divides b and d divides r_1 then d must also divide a. In other words, the first step of the Euclidean algorithm tells us that

$$\{ \text{ common divisors of } a \text{ and } b\} = \{ \text{ common divisors of } b \text{ and } r_1\}$$

and similarly, the next steps allow us to continue all the way through the steps of the Euclidean algorithm. After finitely many steps we get a remainder of 0:

$$\begin{aligned}
a &= q_1 \cdot b + r_1 \\
&\dots \\
r_{i-2} &= q_i \cdot r_{i-1} + r_i \\
r_{i-1} &= q_{i+1} \cdot r_i + 0
\end{aligned}$$

and so we conclude that

$$\begin{aligned}
\{ \text{ common divisors of } a \text{ and } b \ \} &= \{ \text{ common divisors of } b \text{ and } r_1 \ \} \\
&= \{ \text{ common divisors of } r_1 \text{ and } r_2 \ \} \\
&\dots \\
&= \{ \text{ common divisors of } r_{i-1} \text{ and } r_i \ \} \\
&= \{ \text{ common divisors of } r_i \text{ and } 0 \ \} \\
&= \{ \text{ divisors of } r_i \ \}
\end{aligned}$$

In other words, the common divisors of the original integers a and b are precisely the divisors of the last nonzero remainder in the Euclidean algorithm. Thus, the last nonzero remainder is the greatest common divisor of the integers a and b.

Example: Find the greatest common divisor of the integers 3800 and 8740.

Method 1: Find the greatest common divisor by factoring.

$$3800 = 2^3 \cdot 5^2 \cdot 19 \text{ and } 8740 = 2^2 \cdot 5 \cdot 19 \cdot 23$$

So the greatest common divisor, the largest number that divides both 3800 and 8740 is just the "intersection" of these two prime factorizations, in this case $2^2 \cdot 5 \cdot 19 = 380$.

Method 2: Find the greatest common divisor using the Euclidean algorithm.

$$\begin{aligned} 8740 &= 2 \cdot 3800 + 1140 \\ 3800 &= 3 \cdot 1140 + 380 \\ 1140 &= 3 \cdot 380 + 0 \end{aligned}$$

The last nonzero remainder, 380, is the greatest common divisor of 8740 and 3800.

Now go back to the question of finding $a^{-1} \bmod m$. If a and m have a common divisor $d > 1$, then a is not invertible mod m. On the other hand, suppose that a and m are relatively prime. When we apply the Euclidean algorithm to a and m,

$$\begin{aligned} m &= q_1 \cdot a + r_1 \\ a &= q_2 \cdot r_1 + r_2 \\ &\cdots \\ r_{i-2} &= q_i \cdot r_{i-1} + r_i \\ r_{i-1} &= q_{i+1} \cdot r_i + 0 \end{aligned}$$

and the last nonzero remainder r_i will equal 1. As illustrated in the example, we can then solve the next-to-last equation for 1 in terms of the previous remainders r_{i-2} and r_{i-1}. Working our way backwards through these equations, we eventually eliminate all the intermediate remainders and get 1 as an integer linear combination of the original numbers a and m. Thus we can not only see that a^{-1} exists mod m, but this process also finds a^{-1} mod m for us.

§ 4. Powers mod m

Let a be any integer and consider the (positive) integer powers of a mod m. For each power of a, reduce to the standard representatives mod m.

Example: Look at sequences of powers mod 6. The powers of 0 and of 1 are not too interesting. What about the powers of $2, 3, 4$ and 5? For example, the sequence of powers of 2

$$2, 4, 8, 16, 32, 64, \ldots$$

reduces mod 6 to the standard representatives

$$2, 4, 2, 4, 2, 4, \ldots$$

Similarly,

powers of 3:	$3, 3, 3, 3, 3, 3, \ldots$
powers of 4:	$4, 4, 4, 4, 4, 4, \ldots$
powers of 5:	$5, 1, 5, 1, 5, 1, \ldots$

Example: If we work mod 7 (again, ignoring 0) we get:

powers of 1:	$1, 1, 1, 1, 1, 1, \ldots$
powers of 2:	$2, 4, 1, 2, 4, 1, \ldots$
powers of 3:	$3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, 1, \ldots$
powers of 4:	$4, 2, 1, 4, 2, 1, \ldots$
powers of 5:	$5, 4, 6, 2, 3, 1, 5, 4, 6, 2, 3, 1, \ldots$
powers of 6:	$6, 1, 6, 1, 6, 1, \ldots$

Example: If we work mod 9 (again, ignoring 0) we get:

powers of 1:	$1, 1, 1, 1, 1, 1, 1, 1, \ldots$
powers of 2:	$2, 4, 8, 7, 5, 1, 2, 4, 8, 7, 5, 1, \ldots$
powers of 3:	$3, 0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots$
powers of 4:	$4, 7, 1, 4, 7, 1, 4, 7, 1, \ldots$
powers of 5:	$5, 7, 8, 4, 2, 1, 5, 7, 8, 4, 2, 1, \ldots$
powers of 6:	$6, 0, 0, 0, 0, 0, 0, 0, 0, \ldots$
powers of 7:	$7, 4, 1, 7, 4, 1, 7, 4, 1, \ldots$
powers of 8:	$8, 1, 8, 1, 8, 1, 8, 1, \ldots$

Example: If we work mod 11 (again, ignoring 0) we get:

powers of 1:	$1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \ldots$
powers of 2:	$2, 4, 8, 5, 10, 9, 7, 3, 6, 1, \ldots$
powers of 3:	$3, 9, 5, 4, 1, 3, 9, 5, 4, 1, \ldots$
powers of 4:	$4, 5, 9, 3, 1, 4, 5, 9, 3, 1, \ldots$
powers of 5:	$5, 3, 4, 9, 1, 5, 3, 4, 9, 1, \ldots$
powers of 6:	$6, 3, 7, 9, 10, 5, 8, 4, 2, 1, \ldots$
powers of 7:	$7, 5, 2, 3, 10, 4, 6, 9, 8, 1, \ldots$
powers of 8:	$8, 9, 6, 4, 10, 3, 2, 5, 7, 1, \ldots$
powers of 9:	$9, 4, 3, 5, 1, 9, 4, 3, 5, 1, \ldots$
powers of 10:	$10, 1, 10, 1, 10, 1, 10, 1, 10, 1, \ldots$

In all our examples, the sequence of powers reduced mod m to standard representatives in the set $\{0, 1, 2, \ldots m-1\}$ eventually starts to repeat since there are only finitely many possible reductions. If we examine the examples above (among others), we see that the sequences of powers behave differently for prime moduli like 7 or 11 than they do for composite moduli like 6 or 9. These sequences will be important for us because they give the starting point for a prime-testing method that does not involve factoring. Consider first the case where the modulus is prime.

Theorem(Fermat): If p is a prime and if a is any integer not divisible by p, then

$$a^{p-1} \equiv 1 \bmod p.$$

Proof: Let p be any prime. The invertible elements mod p are all the nonzero elements, namely $\{1, 2, \ldots, p-1\}$. Let a be any integer not divisible by p and consider the sequence

$$a, 2a, 3a, \ldots, (p-1)a$$

There are exactly $p-1$ numbers on this list and none of them can be congruent to any other mod p. Suppose that $ax \equiv ay \bmod p$ where x and y both belong to $\{1, 2, \ldots, p-1\}$. Since a is invertible mod p, we conclude that $x \equiv y \bmod p$ and hence we must have $x = y$. So

$$\{a, 2a, \ldots, (p-1)a\} \text{ is just a permuation of } \{1, 2, \ldots, p-1\}$$

and therefore

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p.$$

Multiply through by 2^{-1}, 3^{-1}, up through $(p-1)^{-1}$, and we get

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

and the theorem is proved.

We have a similar theorem in the case where the modulus is composite, but first we need a definition.

Definition (Euler's ϕ-function) Let m be any positive integer and let $\phi(m)$ denote the number of integers between 0 and m that are invertible mod m. In other words $\phi(m)$ is the number of integers in $\{1, 2, \ldots, m-1\}$ that are relatively prime to m. .

Example: To compute $\phi(6)$ we must count the number of elements in $\{1, 2, 3, 4, 5\}$ that are relatively prime to 6. Only 1 and 5 have this property, so $\phi(6) = 2$.

Example: To compute $\phi(9)$ we count the number of elements between 1 and 8 that are relatively prime to 9. We have to throw out all the multiples of 3 in this range and we are left with $\{1, 2, 4, 5, 7, 8\}$. Thus $\phi(9) = 6$.

Example: $\phi(12) = 4$ since the only invertible elements mod 12 are $1, 5, 7$ and 11. $\phi(15) = 8$ since the only invertible elements mod 15 are $1, 2, 4, 7, 8, 11, 13$ and 14.

Theorem: (Euler) If a is any invertible integer mod m then

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

Note that Fermat's theorem is a special case of Euler's theorem. For any prime p, $\phi(p) = p - 1$ and any integer a that is not divisible by p is invertible mod p. The proof of Fermat's theorem works for Euler's theorem as well. Simply replace the set $\{1, 2, \ldots, p-1\}$ by the set of invertible elements mod m.

§ 5. Prime Testing and Pseudoprimes

Suppose we are given an odd number m and we want to know if it is prime or composite. Fermat's theorem suggests that we might decide this by computing powers mod m. For example, if m is prime, then $2^{m-1} \equiv 1 \bmod m$. So if we compute $2^{m-1} \bmod m$ and we get anything other than 1, we will know that m is composite.

On the other hand, if m is composite then $\phi(m)$ will be less than $m - 1$ and so we have no reason to expect that 2^{m-1} will reduce to 1 mod m. However, this can happen. So if $2^{m-1} \equiv 1 \bmod m$ then m can be prime or composite. Further testing is needed before we can decide for sure.

Definition: We say that m is a pseudoprime to the base b if

$$b^{m-1} \equiv 1 \bmod m \text{ and } m \text{ is composite.}$$

So if we are looking for primes we can sort through a list of (odd) integers m and compute the quantity $2^{m-1} \bmod m$. If we get something different from 1 we will know that m is composite and we will delete it from our list. If we get 1, then we know that m is probably prime. When we finish we will have all the primes that were on the original list, but a few composite numbers will have sneaked by our test. How can we eliminate them?

One method would be to try a different base. Take our list of probable primes and go through it again, this time computing $3^{m-1} \bmod m$. Again, if we get something different from 1, we will know that m is composite and we can delete it from our list of probable primes. If we do this for enough different bases, we can eventually eliminate all the composites from our list.

We have made a good start on developing a fool-proof primality test, but to finish, we would need to understand just how hard it is to be a pseudoprime. How often will it happen that a composite number passes Fermat's test for several bases? How many bases do we need to check to be sure that we have eliminated all the composites from our list? The answer to this question is beyond the scope of this course, but we can look at it experimentally in the homework.

We were after a prime-testing algorithm that is more efficient than trial division. It is not clear yet that we have made any progress toward that goal. To check that m is prime using trial division we check that no (odd) number d smaller than $\sqrt{m}$ is a divisor of m. Thus it takes $\sqrt{m}/2$ divisions to show that m is prime.

How does this compare to the work of computing $b^{m-1} \bmod m$? At first glance, computing $b^{m-1} \bmod m$ seems like much more work. It takes about $2(m-1)$ multiplications to compute this power since we must not only multiply by b, but we must also reduce mod m, requiring another division. So without a more efficient way to compute $b^{m-1} \bmod m$, trial division looks more promising. A very efficient algorithm for computing powers mod m is illustrated in the following example.

Compute $999^{179} \bmod 1763$ using Fast Exponentiation:

First note that $179 = 1 + 2 + 2^4 + 2^5 + 2^7$ so

$$999^{179} = (999)^{1+2+2^4+2^5+2^7}$$

$$= 999 \cdot 999^2 \cdot 999^{16} \cdot 999^{32} \cdot 999^{128}$$

To compute these powers of 999 we simply square repeatedly:

$$\begin{aligned}
999^2 &\equiv 143 \bmod 1763 \\
999^4 &\equiv 143^2 \equiv 1056 \bmod 1763 \\
999^8 &\equiv 1056^2 \equiv 920 \bmod 1763 \\
999^{16} &\equiv 920^2 \equiv 160 \bmod 1763 \\
999^{32} &\equiv 160^2 \equiv 918 \bmod 1763 \\
999^{64} &\equiv 918^2 \equiv 10 \bmod 1763 \\
999^{128} &\equiv 10^2 \equiv 100 \bmod 1763
\end{aligned}$$

and thus

$$\begin{aligned}
999^{179} &\equiv 999 \cdot 143 \cdot 160 \cdot 918 \cdot 100 \bmod 1763 \\
&\equiv 54 \cdot 160 \cdot 918 \cdot 100 \bmod 1763 \\
&\equiv 1588 \cdot 918 \cdot 100 \bmod 1763 \\
&\equiv 1546\dot{1}00 \bmod 1763 \\
&\equiv 1219 \bmod 1763
\end{aligned}$$

If we want to program this process, then we can refine the algorithm to make it more efficient by computing the binary expansion of the exponent and form the product as we go:

Algorithm to compute a^k mod m

Step 1: $x \leftarrow 1$

Step 2: while $k > 0$

(a) If k is even then leave x alone. If k is odd, then replace a by ax and reduce mod m.

(b) Replace a by a^2 and reduce mod m.

(c) Replace k by $k/2$ if k is even. Replace k by $(k-1)/2$ if k is odd.

Claim: When this process finishes, $x \equiv a^k$ mod m. To see this, trace it out for our example 999^{179} mod 1763.

$$\begin{aligned}
&x = 1, a = 999, k = 179, m = 1763 \\
\text{k is odd: }&x \leftarrow 999, a \leftarrow 999^2 \equiv 143, k \leftarrow 178/2 = 89 \\
\text{k is odd: }&x \leftarrow 999 \cdot 143 \equiv 54, a \leftarrow 143^2 \equiv 1056, k \leftarrow 88/2 = 44 \\
\text{k is even: }&x = 54, a \leftarrow 1056^2 \equiv 920, k \leftarrow 44/2 = 22 \\
\text{k is even: }&x = 54, a \leftarrow 920^2 \equiv 160, k \leftarrow 22/2 = 11 \\
\text{k is odd: }&x = 54 \cdot 160 \equiv 1588, a \leftarrow 160^2 \equiv 918, k \leftarrow 10/2 = 5 \\
\text{k is odd: }&x = 1588 \cdot 918 \equiv 1546, a \leftarrow 918^2 \equiv 10, k \leftarrow 4/2 = 2 \\
\text{k is even: }&x = 1546, a \leftarrow 10^2 \equiv 100, k \leftarrow 2/2 = 1 \\
\text{k is odd: }&x = 1546 * 100 \equiv 1219, a \leftarrow 100^2 \equiv ??, k \leftarrow 0/2 = 0
\end{aligned}$$

We exit the loop when k reaches 0 and x is $1219 \equiv 999^{179}$ mod 1763.