One of the fundamental tools of number theory is the congruence. This idea will be critical to most of what we do the rest of the term. This set of notes partially follows the book’s treatment. I will not use the language of abstract algebra, however, to the extent that the book does. In addition, I will present some results of historical importance, which are not in the book.

**Definition 1** We say \( a \equiv b \pmod{m} \) (read \( a \) is congruent to \( b \) modulo \( m \)) if \( a - b \) is divisible by \( m \).

If \( a = qm + r \), where \( 0 \leq r < m \), then \( a \equiv r \pmod{m} \). We refer to \( r \) as the least residue of \( a \) modulo \( m \) and say that \( a \) belongs to the residue class of \( r \). The book denotes this \( a \in \mathbb{Z}_m \), where \( \mathbb{Z}_m \) is the set \( \{\ldots, r - 2m, r - m, r, r + m, r + 2m, \ldots\} \). I will not refer much to residue classes.

**Theorem 1** Let \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \). Then

1) \( a + c \equiv b + d \pmod{m} \)
2) \( ac \equiv bd \pmod{m} \)
3) for any \( n > 0 \), \( a^n \equiv b^n \pmod{m} \)

**Proof:** I will leave you to prove (1). You should try to do this to get used to working with congruences. (3) follows by induction from (2) (with \( c = a \) and \( d = b \)). Here is a verification of (2): if \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \), then for some integers \( k_1 \) and \( k_2 \), \( a - b = k_1 m \) and \( c - d = k_2 m \). Writing this as \( a = b + k_1 m \) and \( c = d + k_2 m \), we have \( ac = (b + k_1 m)(d + k_2 m) = bd + m(k_1 d + k_2 b + k_1 k_2 m) \). Thus, \( ac - bd \) is a multiple of \( m \), so \( ac \equiv bd \pmod{m} \), as desired.

Division is not possible in general with congruences. For example, \( 24 \equiv 84 \pmod{15} \) but if we divide both sides by 6, we get \( 4 \equiv 14 \pmod{15} \), which is not correct. However, we do have the following:

**Theorem 2** If \( ac \equiv bc \pmod{m} \) and \( \gcd(c, m) = 1 \), then \( a \equiv b \pmod{m} \).

More generally, if \( ac \equiv bc \pmod{m} \) and \( \gcd(c, m) = d \), then \( a \equiv b \pmod{m/d} \).

**Proof:** If \( ac \equiv bc \pmod{m} \), then for some integer, \( k \), \( ac - bc = km \), or \( (a - b)c = km \). If \( \gcd(c, m) = d \), then for some integers \( x \) and \( y \), \( cx + my = d \). Now \( (a - b)cx = kmx \) and \( cx = d - my \) so \( (a - b)(d - my) = kmx \). Dividing by \( d \) gives \( (a - b)\left(1 - \frac{my}{d}\right) = \frac{kmx}{d} \).

Thus, \( a - b = \frac{m}{d}(kx + (a - b)y) \), which means that \( a \equiv b \pmod{m/d} \). If \( d = 1 \), we get the first assertion.

The idea of a congruence goes back many centuries, but Gauss made the notation and its properties explicit. When we talk about theorems of Euler and Fermat that apply to congruences, they did not use congruence notation. For example, Fermat made two observations of some importance to us here. First, he noticed that if \( p \) is prime and \( q \) is a divisor of the Mersenne number \( 2^p - 1 \), then \( q \equiv 1 \pmod{p} \). Fermat would have phrased this as \( q - 1 \) is divisible by \( p \). Second, and more important to us in this course, is one of the most fundamental results in computational number theory.
Theorem 3 (Fermat’s Little Theorem) If $p$ is prime and $a$ is any integer, then 

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

Proof: Our book derives this theorem as a corollary to Euler’s theorem, which we state in a little bit. Here is an alternative proof by induction. First, for odd primes, $p$, $(-a)^p = -a^p$, so if we can establish the result for nonnegative $a$, we will get the negative values as well. Inducting on $a$, the result is obviously true when $a = 0$. Supposing we have established the result for $a$, we must show that $p^a \equiv 1 \pmod{p}$.

Using the Binomial Theorem,

$$(a + 1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1.$$ 

Now \( \binom{p}{k} = \frac{p!}{k!(p-k)!} \), and this will be divisible by $p$ if there is no factor involving $p$ in the denominator. This is the case whenever $1 \leq k \leq p-1$, so all the middle binomial coefficients are divisible by $p$. This means

$$a^p + 0 + \cdots + 0 + 1 \equiv a + 1 \pmod{p},$$

establishing the inductive step.

Corollary 1 (Also called Fermat’s Little Theorem) If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

This follows by the cancellation theorem since if $p \nmid a$ then $\gcd(a,p) = 1$.

If $n$ is not prime, then usually $a^{n-1} \not\equiv 1 \pmod{n}$. As we will see shortly, this gives a quick way to determine that most composite numbers are not prime. For example, $2^{14} = 16384 \equiv 4 \pmod{15}$. Thus, 15 can’t be prime. We say it violates Fermat’s Little Theorem, or fails the Fermat Test. Unfortunately, this is not a fool proof approach. It turns out that $2^{340} \equiv 1 \pmod{341}$ even though $341 = 11 \times 31$. A composite number $n$ that has the property that $2^{n-1} \equiv 1 \pmod{n}$ is called a base 2 pseudoprime. These numbers are rare: there are 245 pseudoprimes under 1,000,000 while there are 78,498 primes less than 1,000,000. So if a number, $n < 1,000,000$ is selected at random and $2^{n-1} \equiv 1 \pmod{n}$, then the probability that $n$ is prime is $\frac{78,498}{245 + 78,498} \approx .997$, pretty good odds.

Let’s show that 341 is a base 2 pseudoprime. By Fermat’s Little Theorem, $2^{11} \equiv 2 \pmod{11}$, or $2^{10} \equiv 1 \pmod{11}$. In fact, $2^{10} - 1 = 1023$, which is $93 \times 11$. Noticing that 31 is a divisor of 93, we see that 31 $| 1023$ as well. In fact, $1023 = 3 \times 341$. This means $341 \mid 2^{10} - 1$. But $2^{10} - 1$ is a divisor of $2^{340} - 1$ (since 10 is a divisor of 340) so $341 \mid 2^{340} - 1$, or $2^{340} \equiv 1 \pmod{341}$.
Now even though 341 is a base 2 pseudoprime, it is not a base 3 pseudoprime. That is, \(3^{340} \equiv 56 \not\equiv 1 \pmod{341}\). We say that 341 fails a base 3 Fermat test. Unfortunately, there are very rare numbers that are pseudoprimes to infinitely many bases. A number \(n\) for which \(a^n \equiv a \pmod{n}\) for all integers \(a\) is called a \textbf{Carmichael number}. Carmichael was a mathematician trying to prove that such numbers could not exist. While studying properties such numbers would have to possess, he discovered, in 1910, that 561 had those properties. Of course Carmichael numbers are much rarer than pseudoprimes. Of the 245 base 2 pseudoprimes under 1,000,000, only 43 of them are Carmichael numbers. Even so, it was proved in 1993 that there are infinitely many Carmichael numbers.

**Euler’s \(\phi\) function**

A useful number theoretic function is \textbf{Euler’s \(\phi\) function} \(\phi(n)\) = the number of positive integers less than \(n\) which are relatively prime to \(n\). For example, the numbers prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14. There are 8 of them so \(\phi(15) = 8\). The following is a generalization of Fermat’s Little Theorem.

**Theorem 4 (Euler’s Theorem)** If \(\gcd(a, n) = 1\), then \(a^{\phi(n)} \equiv 1 \pmod{n}\).

**Proof:** Let \(\phi(n) = k\) and suppose that \(x_1, x_2, x_3, \ldots, x_k\) are the numbers less than, but prime to \(n\). As mentioned before, since \(\gcd(a, n) = 1\), if \(ax \equiv ay \pmod{n}\) then \(x \equiv y \pmod{n}\). Because of this, the numbers \(ax_1, ax_2, ax_3, \ldots, ax_k\) must all be distinct modulo \(n\). That is, for all \(i \neq j\), \(ax_i \neq ax_j \pmod{n}\). These numbers are also relatively prime to \(n\), so modulo \(n\) they must be a reordering of the numbers \(x_1, x_2, x_3, \ldots, x_k\). This means that they must have the same product modulo \(n\). That is, \(x_1x_2\cdots x_k \equiv (ax_1)(ax_2)\cdots(ax_k) \pmod{n}\), so \(x_1x_2\cdots x_k \equiv a^kx_1x_2\cdots x_k \pmod{n}\). Since \(x_1x_2\cdots x_k\) is relatively prime to \(n\), we may cancel it out to get \(a^k \equiv 1 \pmod{n}\), as desired.

For an example of the proof, using \(n = 15\), and \(x_1, \ldots, x_8\) being 1, 2, 4, 7, 8, 11, 13, 14, if we were to pick \(a = 7\) then multiplying each of these numbers by 7 would give the list 7, 14, 28, 49, 56, 77, 91, 98. Reducing these modulo 15 would give the list 7, 14, 13, 4, 11, 2, 1, 8, a reordering of the original list. This means that

\[
7 \cdot 14 \cdot 28 \cdot 49 \cdot 56 \cdot 77 \cdot 91 \cdot 98 \equiv 7 \cdot 14 \cdot 13 \cdot 4 \cdot 11 \cdot 2 \cdot 1 \cdot 8 \equiv 1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14 \equiv 1 \pmod{15},
\]

modulo 15. That is,

\[
7^8 \equiv 1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14 \equiv 1 \cdot 2 \cdot 4 \cdot 7 \cdot 8 \cdot 11 \cdot 13 \cdot 14 \pmod{15},
\]

so \(7^8 \equiv 1 \pmod{15}\). In fact, \(7^8 = 5764801 = 15 \times 384320 + 1\).

I mentioned that Fermat made two observations about primes, most easily understood in terms of congruences. One was Fermat’s Little Theorem. The other was that if \(p\) is prime and \(q\) is any divisor of the Mersenne number \(2^p - 1\) then \(q \equiv 1 \pmod{p}\). For example, in the previous set of notes, we commented that \(2^{11} - 1\) is not prime, it has prime divisors 23 and 89. Indeed, \(23 \equiv 1 \pmod{11}\) and \(89 \equiv 1 \pmod{11}\). We now turn our attention to this second observation of Fermat’s. We need one more fact.
Lemma 1 For positive integers m and n, \( \gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1 \).

Proof: We may assume \( m \geq n \). We have

\[
\gcd(a^m - 1, a^n - 1) = \gcd(a^m - a^n, a^n - 1) = \gcd(a^n(a^{m-n} - 1), a^n - 1).
\]

Since \( a^n \) is prime to \( a^n - 1 \), we can deduce that \( \gcd(a^m - 1, a^n - 1) = \gcd(a^{m-n} - 1, a^n - 1) \).

Now suppose that \( m = qn + r \). Then \( m - n = (q-1)n + r \), and if we repeat the calculation above \( q \) times, we end with \( \gcd(a^m - 1, a^n - 1) = \gcd(a^n - 1, a^r - 1) \). This completely mimics the gcd calculation \( \gcd(m, n) = \gcd(n, r) \). Consequently, after some number of steps, we obtain \( \gcd(a^m - 1, a^n - 1) = \gcd(a^{\gcd(m,n)} - 1, a^0 - 1) \). But \( a^0 - 1 = 0 \), and \( \gcd(k, 0) = k \), so \( \gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1 \).

For example, suppose we had \( m = 84, n = 35 \). We have

\[
\gcd(a^{84} - 1, a^{35} - 1) = \gcd(a^{84} - a^{35}, a^{35} - 1) = \gcd(a^{35}(a^{49} - 1), a^{35} - 1) = \gcd(a^{49} - 1, a^{35} - 1) = \gcd(a^{35}(a^{14} - 1), a^{35} - 1) = \gcd(a^{14} - 1, a^{35} - 1) = \gcd(a^{35} - 1, a^{14} - 1) = \gcd(a^{14} - 1, a^{7} - 1) = \gcd(a^{7} - 1, a^{7} - 1) = \gcd(a^{7} - 1, 0) = a^{7} - 1.
\]

In abbreviated form, this would read

\[
\gcd(a^{49} - 1, a^{35} - 1) = \gcd(a^{35} - 1, a^{14} - 1) = \gcd(a^{14} - 1, a^{7} - 1) = \gcd(a^{7} - 1, 0),
\]

which we contrast with \( \gcd(84, 35) = \gcd(35, 14) = \gcd(14, 7) = \gcd(7, 0) = 7 \).

Theorem 5 (Fermat’s second observation) If \( d \mid 2^p - 1 \) then \( d \equiv 1 \) (mod \( p \)).

Proof: First, consider the case where \( d = q \), a prime. By Fermat’s Little Theorem, 
\( 2^{q-1} \equiv 1 \) (mod \( q \)). This means that \( q \mid 2^{q-1} - 1 \) and \( q \mid 2^p - 1 \). Since \( q \) is a common divisor of these two numbers, it must be that \( q \mid \gcd(2^{q-1} - 1, 2^p - 1) \). By the previous lemma, \( \gcd(2^{q-1} - 1, 2^p - 1) = 2^{\gcd(q-1,p)} - 1 \), and this number must be divisible by \( q \). If \( \gcd(q-1,p) = 1 \), then \( 2^{\gcd(q-1,p)} - 1 = 1 \), which is not divisible by \( q \) so \( \gcd(q-1,p) > 1 \). But \( p \) is a prime so if \( \gcd(q-1,p) > 1 \), then \( \gcd(q-1,p) = p \), meaning that \( p \mid q - 1 \), or \( q \equiv 1 \) (mod \( p \)).

To finish the proof, if \( d \) is not prime, then \( d \) can be factored into primes: \( d = q_1 q_2 \cdots q_k \), and if \( d \mid 2^p - 1 \), then each prime divisor has the same property: \( q_i \mid 2^p - 1 \). By the first part of the proof, each \( q_i \equiv 1 \) (mod \( p \)), and so their product will also be congruent to 1.

The point of this observation is the following: Suppose we wish to try to factor a Mersenne number, say \( 2^{29} - 1 \). By Fermat’s observation, if \( p \mid 2^{29} - 1 \), then \( p \equiv 1 \) (mod \( 29 \)), meaning that for some integer, \( k, p = 29k + 1 \). Since \( p \) must be odd, we can throw in a factor of 2:
As mentioned earlier, since $2^{15} \neq 2 \pmod{15}$, we know, by Fermat’s Little Theorem, that 15 is not prime without actually factoring the number. This might be a little more impressive if we didn’t know what the factors of 15 were. If we want to use Fermat’s Little Theorem as a way to prove numbers are composite without actually factoring them, we must be able to calculate $2^n \pmod{n}$ or more generally, $a^n \pmod{n}$ relatively quickly. There is a way to do this, based on the fact that $a^{2^k} = (a^{2^k-1})^2$. We will show the method with an example. Suppose we wish to verify that 341 is not a base 3 pseudoprime. That is, we wish to show that $3^{240} \equiv 1 \pmod{341}$. We do the following.

Step 1 Write 340 as a sum of powers of 2: $340 = 256 + 64 + 16 + 4$. From this, it follows that $3^{340} = 3^{256}3^{64}3^{16}3^4$.

Step 2 Construct a table of powers $3^{2^k} \pmod{341}$ by repeatedly squaring previous entries.

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2^n$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>64</td>
<td>128</td>
<td>256</td>
</tr>
<tr>
<td>$3^{2^n} \pmod{341}$</td>
<td>3</td>
<td>9</td>
<td>81</td>
<td>82</td>
<td>245</td>
<td>9</td>
<td>81</td>
<td>82</td>
<td>245</td>
</tr>
</tbody>
</table>

Step 3 Use the table to find $3^{340}$: $3^{340} \equiv 245 \times 9 \times 245 \times 81 \equiv 56 \pmod{341}$.

This is called the **Binary Squaring Algorithm**. How good is it? The naive algorithm to calculate $a^k \pmod{n}$ might consist of $k-1$ multiplications and $k-1$ divisions by $n$ (to keep the number from growing too big) for a total of $2k - 2$ multiplications/divisions. For our problem above, $3^{340} \pmod{341}$, this would be a total of 678 multiplications/divisions. For the binary squaring algorithm, the number of multiplications/divisions depends on the highest power of 2 less than $k$, $\lfloor \log_2 k \rfloor$. If we call this number $m$, for now, then we must calculate $a^{2^j}$ for each $j < m$, by squaring the previous entry, for a total of $m$ squaring and $m$ divisions by $n$. Then, we multiply as many terms as needed, which could be as large as $m$ again, giving $2m$ more multiplications/divisions. This gives an upper bound of $4\lfloor \log_2 k \rfloor$ multiplications/divisions. For 340, this would be $4\log_2 340 \approx 34$ such operations. For large numbers, if we had an exponent $k$ with, say 100 digits, so $k \approx 10^{99}$, then on the fastest computer it would take more than the lifetime of the universe to use the naive approach. With the binary squaring algorithm, at most $4\log_2(10^{99})$ steps, or about 1315 multiplications/divisions are required. This algorithm makes Fermat’s Little Theorem practical.
Both Maple and Mathematica know about the binary squaring algorithm to calculate $a^k \mod n$. In Maple, one uses the command “$a \&^k k \mod n$,” in Mathematica, “PowerMod[$a, k, n$].”

**Terms used in this set of notes**

Here are the major terms introduced above.

The **Binary Squaring Algorithm** is a fast way to calculate $a^n$ or $a^n \mod m$ based on writing $n$ as a sum of powers of 2.

A **base a pseudoprime** is a number $n > a$ which we know to be composite and for which $a^n \equiv a \mod n$. Most books say $a$ must be relatively prime to $n$ as well, in which case we can use the congruence $a^{n-1} \equiv 1 \mod n$ instead.

In contrast with a pseudoprime, a **probable prime** is a number $n$ which we DON’T know to be prime or composite, for which there is an $a$ with $1 < a < n-1$ and $a^n \equiv a \mod n$. Again, we sometimes use the condition $a^{n-1} \equiv 1 \mod n$ instead.

We say a number $n$ passes a **Fermat test** if $a^{n-1} \equiv 1 \mod n$ (or if $a^n \equiv a \mod n$) where $1 < a < n-1$. That is, if we don’t know if $n$ is prime, but $n$ passes a Fermat test, then $n$ is a probable prime.

Finally, a **Carmichael number** is a composite number $n$ which is a pseudoprime for every possible base. That is, $n$ is a Carmichael number if $a^n \equiv a \mod n$ for every $a$, even though $n$ is not prime.