18. More on Fermat’s Theorem and inverses modulo $m$

We began with the homework which was assigned last Thursday:

**Example:** Find $3^{31063} \% 17$.

**Answer:** By Fermat’s theorem, we have that $3^{16} \equiv 1 \pmod{17}$. Dividing 16 into 31063, we have $31063 = (1941)(16) + 7$. Hence

$$3^{31063} = 3^{(1941)(16)+7}$$

$$= (3^{16})^{1941} \cdot 3^7$$

$$\equiv (1)^{1941} \cdot 3^7 \pmod{17}$$

$$\equiv 3^7 \pmod{17}$$

$$\equiv 3^4 \cdot 3^3 \pmod{17}$$

$$\equiv 81 \cdot 27 \pmod{17}$$

$$\equiv 13 \cdot 10 \pmod{17}$$

$$\equiv 11 \pmod{17}$$

Since we will need the result of the second homework problem later, we state it as a theorem:

**Theorem:** Let $a, b, c$ be integers and suppose $a | c$ and $b | c$. Suppose $\gcd(a, b) = 1$. Then $ab | c$.

**Proof:** (Erica) We have $c = ad$ and $c = be$ for some integers $d$ and $e$. Since $\gcd(a, b) = 1$, we have that $1 = ax + by$. Multiplying by $c$, we obtain $c = axc + byc = axbe + byad = ab(xe + yd)$. Thus, $ab$ divides $c$. \(\square\)

We then moved on to a discussion of a new proof of Fermat’s Theorem.

First we introduce some notation. Let $p$ be a prime. Let

$$S_p = \{1, 2, 3, \ldots, p-1\}.$$

That is, $S_p$ is the set of all the numbers between 1 and $p - 1$. Given $a, b \in S_p$, note that $ab \% p$ is also in $S_p$. If not, then $ab \% p = 0$, which means $p$ divides $ab$. As $p$ is prime, this would mean that $p$ divides $a$ or $p$ divides $b$, contradicting that $a$ and $b$ are between 1 and $p - 1$. For $a \in S_p$ define a function $f : S_p \to S_p$ by $f_p^a(i) = ai \% p$ for each $i \in S_p$.

$$aS_p = \{a \% p, 2a \% p, \ldots, (p - 1)a \% p\}.$$

Let’s do an example with $p = 5$. We have $S_5 = \{1, 2, 3, 4\}$. Choose a random element in $S_5$, say 3. Then

$$f_5^3(1) = 3 \cdot 1 \% 5 = 3$$

$$f_5^3(2) = 3 \cdot 2 \% 5 = 1$$

$$f_5^3(3) = 3 \cdot 3 \% 5 = 4$$

$$f_5^3(4) = 3 \cdot 4 \% 5 = 5$$

Notice that every element in $S_5$ was ‘hit’; that is, the map is *onto*. We tried another example: say, $p = 7$ and $5 \in S_7$. We have
\[ f_5^7(1) = 5 \cdot 1 \mod 7 = 5 \]
\[ f_5^7(2) = 5 \cdot 2 \mod 7 = 3 \]
\[ f_5^7(3) = 5 \cdot 3 \mod 7 = 1 \]
\[ f_5^7(4) = 5 \cdot 4 \mod 7 = 6 \]
\[ f_5^7(3) = 5 \cdot 5 \mod 7 = 4 \]
\[ f_5^7(4) = 5 \cdot 6 \mod 7 = 2 \]

Again, we see that \( f_5^7 \) is onto.

Megan made the following conjecture:

**Conjecture:** Suppose \( p \) is prime and \( a \in S_p \). Then the map \( f_p^a : S_p \rightarrow S_p \) is onto.

To help prove this conjecture, we made the following observation:

**Observation:** Let \( f : S \rightarrow T \) be a function and suppose \( S \) and \( T \) have the same number of elements. If \( f \) is one-to-one then \( f \) is onto.

This observation follows from the **Pigeonhole Principle**, which says that if you have \( n + 1 \) pigeons to put into \( n \) holes, at least two pigeons have to go into the same hole. To see how this applies to the function \( f : S \rightarrow T \), let’s say that both \( S \) and \( T \) have \( n \) elements. If \( f \) is not onto, then the elements of \( S \) are being mapped by \( f \) into a subset of \( T \) consisting of at most \( n - 1 \) elements. Thus, at least two elements of \( S \) must be mapped to the same element, contradicting that \( f \) is one-to-one.

Now let’s prove Megan’s conjecture:

**Theorem:** Let \( p \) be prime and \( a \in S_p \). Then \( f_p^a : S_p \rightarrow S_p \) is onto.

**Proof:** By the observation, it suffices to prove that \( f_p^a \) is one-to-one. Suppose \( f_p^a(i) = f_p^a(j) \) for some elements \( i \neq j \) in \( S_p \). Then \( ai \equiv aj \mod p \), which means \( ai \equiv aj \mod p \). Since \( a \not\equiv 0 \mod p \), by cancellation we have that \( i \equiv j \mod p \). But, since \( i \) and \( j \) are between 1 and \( p - 1 \), this means that \( i = j \), a contradiction. Hence, \( f_p^a \) must be one-to-one (and thus onto). \( \square \)

We now are in a position to use Megan’s conjecture to give another proof of Fermat’s Theorem:

**Theorem:** Let \( p \) be a prime and \( a \) an integer such that \( a \not\equiv 0 \mod p \). Then \( a^{p-1} \equiv 1 \mod p \).

**Proof:** It is enough to prove this in the case \( a \in S_p \), since every integer not divisible by \( p \) is congruent to it’s remainder upon dividing by \( p \). By Megan’s conjecture, \( f_p^a : S_p \rightarrow S_p \) is one-to-one and onto, we have

\[
S_p = \{1, 2, \ldots, p - 1\} = \{f_p^a(1), f_p^a(2), \ldots, f_p^a(p - 1)\} = \{a \% p, 2a \% p, \ldots, (p - 1)a \% p\}.
\]
Since the elements in these sets are the same (with just the order scrambled), we get the following products are equal:

\[ 1 \cdot 2 \cdot \cdots \cdot (p - 1) = (a \% p) \cdot (2a \% p) \cdots ((p - 1)a \% p). \]

Going modulo \( p \), we have

\[ (p - 1) \equiv (p - 1)a^{p-1} \pmod{p}. \]

But since \( p \) is prime, \( p \) does not divide \((p - 1)\), so \((p - 1) \not\equiv 0 \pmod{p}\). By cancellation, we then have

\[ 1 \equiv a^{p-1} \pmod{p}. \]

\[ \square \]

We now make the following definition:

**Definition:** Let \( p \) be prime and \( a \) an integer not divisible by \( p \). The order of \( a \) modulo \( p \), denoted by \( o_p(a) \), is defined to be the smallest positive integer \( k \) such that \( a^k \equiv 1 \pmod{p} \).

By definition, \( o_p(a) \geq 1 \) for all \( a \not\equiv 0 \pmod{p} \). By Fermat’s Theorem, we also have \( o_p(a) \leq p - 1 \). However, it is possible for \( o_p(a) \) to be less than \( p - 1 \). For instance, \( o_p(1) = 1 \) no matter what \( p \) is. Here are some more examples:

**Example:** \( o_7(2) = 3 \), since \( 2^3 = 8 \equiv 1 \pmod{7} \) and \( 2^k \not\equiv 1 \pmod{7} \) for \( k = 1, 2 \).

**Example:** \( o_5(3) = 4 \), since \( 3^4 = 81 \equiv 1 \pmod{5} \) and \( 3^k \not\equiv 1 \pmod{5} \) for \( k = 1, 2, 3 \).

Here is your homework for Thursday:

**Homework:**

1. Find \( o_7(a) \) for \( 1 \leq a \leq 6 \).
2. Prove \( o_p(p - 1) = 2 \) if \( p \) is an odd prime.
3. Prove that \( o_p(a) \mid p - 1 \) for all \( 1 \leq a \leq p - 1 \)

On Thursday, we began by doing these homework problems:

**Example:** Find \( o_7(a) \) for \( 1 \leq a \leq 6 \).

The values are given in the following table:

<table>
<thead>
<tr>
<th>( a )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>( o_7(a) )</td>
<td>1</td>
<td>3</td>
<td>6</td>
<td>3</td>
<td>6</td>
<td>2</td>
</tr>
</tbody>
</table>

For the second homework problem, we noted that \( p - 1 \equiv -1 \pmod{p} \). Hence,

\[ (p - 1)^2 \equiv (-1)^2 \pmod{p} \]
\[ \equiv 1 \pmod{p}. \]

This says that \( o_p(p - 1) \leq 2 \). But if \( o(p - 1) = 1 \) then \( p - 1 \equiv 1 \pmod{p} \), which means \( p = 2 \), contradicting that \( p \) is odd.

**Theorem:** Let \( p \) be a prime and \( a \not\equiv 0 \pmod{p} \). Then \( o_p(a) \mid p - 1 \).
**Proof:** Let \( n = o_p(a) \). By the division theorem, we have that \( p - 1 = nq + r \) where \( 0 \leq r \leq n - 1 \). We want to show \( r = 0 \). Suppose \( r > 0 \). Then since \( a^n \equiv 1 \pmod{p} \) (by the definition of \( o_p(a) \) and \( a^{p-1} \equiv 1 \pmod{p} \) (by Fermat), we have

\[
1 \equiv a^{p-1} \pmod{p} \\
\equiv a^{nq+r} \pmod{p} \\
\equiv (a^n)^q \cdot a^r \pmod{p} \\
\equiv (1)^q \cdot a^r \pmod{p} \\
\equiv a^r \pmod{p}
\]

But this says that \( a^r \equiv 1 \pmod{p} \) and \( 1 \leq r \leq n - 1 \). But \( n = o_p(a) \), so \( n \) is the smallest positive integer such that \( a^n \equiv 1 \pmod{p} \). To avoid this contradiction, we must have \( r = 0 \). Hence, \( p - 1 = nq \) and so \( n \mid p - 1 \). \( \square \)

Next, we changed subjects and talked about multiplicative inverses. Recall that in the usual real number arithmetic to divide by a nonzero number \( a \) is the same as multiplying by \( \frac{1}{a} \) or \( a^{-1} \). The important property of \( a^{-1} \) is that \( a^{-1} \cdot a = 1 \). For example, to solve an equation of the form \( ax = b \), we just multiply both sides by \( a^{-1} \) to find the solution:

\[
ax = b \\
\Rightarrow a^{-1}(ax) = a^{-1}b \\
\Rightarrow (a^{-1}a)x = a^{-1}b \\
\Rightarrow 1 \cdot x = a^{-1}b \\
\Rightarrow x = a^{-1}b.
\]

The mathematical term for \( a^{-1} \) is the *multiplicative inverse*, or simply *inverse*, of \( a \).

This leads to the question of whether inverses exist in the “modular world.” We made the following definition:

**Definition:** Let \( a \) and \( m \) be integers with \( m > 1 \). We say that an integer \( b \) is an *inverse* for \( a \) modulo \( m \) if \( ba \equiv 1 \pmod{m} \). In this case, we write \( b \equiv a^{-1} \pmod{m} \).

**Example:** Note that 2 is an inverse for 6 modulo 11 since \( 2 \cdot 6 \equiv 1 \pmod{11} \).

**Example:** Note that 6 does not have an inverse modulo 4, since \( 6k \not\equiv 1 \pmod{4} \) for \( k = 0, 1, 2, 3 \).

This brings up the obvious question:

**Question:** When does an integer \( a \) have an inverse modulo \( m \)?

To answer this question, we looked at our multiplication tables modulo \( m \) for \( m = 3, 4, 5, 6, 7, 8, 9 \). The multiplication tables for \( 1 \leq m \leq 7 \) were listed on October 16th. Here are the tables for \( m = 8 \) and \( m = 9 \) (which we did in class):
An element has an inverse if and only if there is a 1 which appears in its row. For example, in the modulo 8 table, we see that 1, 3, 5, 7 have inverses, but 2, 4, 6 (and obviously 0) do not. Similarly, in the $m = 9$ table, we have 1, 2, 4, 5, 7, 8 have inverses while 3 and 6 do not. Based on this evidence (together with the evidence from the other tables), Lisa made the following conjecture:

**Conjecture:** (Lisa) Let $a, m$ be integers with $m \geq 2$. Then $a$ has an inverse modulo $m$ if and only if $\gcd(a, m) = 1$.

And actually, Lisa was able to come up with a proof of one direction of this conjecture:

**Theorem:** Let $a$ and $m$ be integers, with $m \geq 2$. Suppose $\gcd(a, m) = 1$. Then $a$ has an inverse modulo $m$.

**Proof:** (Lisa) Since $\gcd(a, m) = 1$ we have $ax + my = 1$ for some integers $x$ and $y$. Then $my = ax - 1$ so $m \mid (ax - 1)$. Hence, $ax \equiv 1 \pmod{m}$, which means $x$ is an inverse for $a$ modulo $m$. \hfill \Box

In fact, Lisa’s proof suggests a method for finding the inverse of $a$ modulo $m$ if $\gcd(a, m) = 1$. First, use the Euclidean Algorithm to find integers $x$ and $y$ such that $ax + my = 1$. Then the proof above shows that $x$ is an inverse for $a$ modulo $m$.

**Question:** What is $(13)^{-1} \pmod{1000}$?

**Answer:** (Mike) First, use the Euclidean algorithm to find $\gcd(13, 1000)$:

1. $1000 = 13(76) + 12$
2. $13 = 12(1) + 1$

So $1 = \gcd(13, 1000)$. For the back substitution, let $a = 1000$ and $b = 13$:

\[
\begin{align*}
    a &= b(76) + 12 \quad \Rightarrow \quad 12 = a - 76b \\
    b &= (a - 76b)(1) + 1 \quad \Rightarrow \quad 1 = 77b - a
\end{align*}
\]

Thus, $77(13) + 1000(-1) = 1$ which implies $(77)(13) \equiv 1 \pmod{1000}$. Hence, $13^{-1} \equiv 77 \pmod{1000}$.

**Example:** Let’s use the above inverse to solve the following equation for $x$:

$$13x + 88 \equiv 762 \pmod{1000}.$$ 

First, we subtract 762 from both sides to obtain:

$$13x \equiv 238 \pmod{1000}.$$
Now multiply both sides 77, which is the inverse of 13 modulo 1000:

\[
x \equiv (77)(13)x \pmod{1000}
\equiv (77)(236) \pmod{1000}
\equiv 18326 \pmod{1000}
\equiv 326 \pmod{1000}
\]

Hence, \( x \equiv 326 \pmod{1000} \) is the solution.

No homework for Tuesday except to work on Test # 5.