1. Powers and congruence modulo \( m \), part III

These notes are written mostly by Sara

What about the converse of last time theorem: if there exists a \( k > 0 \) such that \( a^k \equiv 1 \mod m \) does this implies that \( \gcd(a, m) = 1 \)?

The answer is yes, and the proof is given below.

**Proof.** If \( a^k \equiv 1 \mod m \) then there exists an integer \( h \) such that \( a^k - 1 = hm \) or \( a(a^{k-1} + (-h)m = 1 \), which means that the equation \( aX + mY = 1 \) has integer solutions, which is equivalent to \( \gcd(a, m) = 1 \). \( \square \)

If the \( \gcd(a, m) = 1 \) what is the smallest \( k \) such that \( a^k \equiv 1 \mod m \)? It is not clear how to find such a smallest integer. We might give it a name in the following definition

(1.1) **Definition.** Let \( m \) and \( a \) be integers, if there exists an integer \( k \) such that \( a^k \equiv 1 \mod m \), then the smallest of such integers is called the order of \( a \) modulo \( m \) and it is defined by \( O_m(a) \).

By definition, if \( O_m(a) \) exists, then \( a^{O_m(a)} \equiv 1 \mod m \). If \( \gcd(a, m) = 1 \) then we know that there exists a \( k \) such that \( a^k \equiv 1 \mod m \) and therefore there is a minimum among such \( k \)'s.

What is \( O_m(a) \)? Can we compute it given \( m \) and \( a \)? We know that if \( m = p \), where \( p \) is a prime number, then \( a^{p-1} \equiv 1 \mod p \) (Fermat’s Theorem) and therefore \( O_m(a) \leq p - 1 \). Can we do anything better? We computed the following examples:

\[
\begin{align*}
O_5(1) &= 1 & O_5(2) &= 4 & O_5(3) &= 4 & O_5(4) &= 2 \\
O_7(1) &= 1 & O_7(2) &= 3 & O_7(3) &= 6 & O_7(4) &= 3 & O_7(5) &= 6 & O_7(6) &= 2
\end{align*}
\]

Several people noticed immediately that all the orders are factors of \( p - 1 \). We first conjectured and then proved the following

(1.2) **Theorem.** Let \( p \) be a prime and \( a \) be an integer which is not divisible by \( p \). Then \( O_p(a) \) divides \( p - 1 \).

**Proof.** Let \( k = O_p(a) \) and assume by way of contradiction that \( k \) does not divide \( p - 1 \) (we know that \( k \leq p - 1 \), as we observed above. By the division Theorem we can write \( p - 1 = kq + r \), where \( 0 \leq r < k \). We have the following equalities:

\[
1 \equiv a^{p-1} \equiv a^{kq+r} \equiv a^{kq}a^r \equiv (a^k)^qa^r \equiv a^r \mod p,
\]

where the first equality is Fermat’s Theorem, and the fifth is given because \( a^k \equiv 1 \mod p \), since \( k \) is the order of \( a \). This says that \( 1 \equiv a^r \mod p \), which is a contradiction since \( r < k \) and \( k \) is the smallest integer \( x \) such that \( a^x \equiv 1 \mod p \). \( \square \)

We worked on a generalization of this theorem to composite moduli:

(1.3) **Theorem.** Suppose \( \gcd(a, m) = 1 \). For any \( n \in \mathbb{Z} \), \( a^n \equiv 1 \) if and only if \( O_m(a) \) divides \( m \).
2. Inverses modulo \( m \)

If we want to find the solution \( x \) of the equation \( ax = b \), what we usually do is to multiply by the inverse of \( a \) both side of the equality.

\[
\begin{align*}
ax &= b \\
 a^{-1}(ax) &= a^{-1}b \\
(a^{-1}a)x &= a^{-1}b \\
x &= a^{-1}b
\end{align*}
\]

The inverse of 2 is \( \frac{1}{2} \), which is not an integer anymore. So equations like the one above do not have a solution among the integers in general. What happens in the “modular world”?

For \( m = 5, 6, 7, 8, 9, 10, \) and 11, which integers \( a \) with \( 1 \leq a \leq m - 1 \) does there exist an integer \( x \) such that \( ax \equiv 1 \mod m \)?

After looking over our modular multiplication tables, we were quickly able to identify which numbers mod \( m \) had such solutions:

<table>
<thead>
<tr>
<th>( m )</th>
<th>list of all ( a ) with ( 1 \leq a \leq m - 1 ) such that ( ax \equiv 1 \mod m ) for some ( x ) (the value of ( x ) is in parenthesis)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td>6</td>
<td>1, 5</td>
</tr>
<tr>
<td>7</td>
<td>1, 2, 3, 4, 5, 6</td>
</tr>
<tr>
<td>8</td>
<td>1, 3, 5, 7</td>
</tr>
<tr>
<td>9</td>
<td>1, 2, 4, 5, 7, 8</td>
</tr>
<tr>
<td>10</td>
<td>1, 3, 7, 9</td>
</tr>
<tr>
<td>11</td>
<td>1, 2, 3, 4, 5, 6, 7, 8, 9, 10</td>
</tr>
</tbody>
</table>

We then made a definition:

\[(2.1) \textbf{Definition.} \text{ Let } a, m \text{ be integers with } m > 0. \text{ We say } b \text{ is an inverse of } a \text{ modulo } m \text{ if } ab \equiv 1 \mod m. \text{ In this case, we write } b \equiv a^{-1} \mod m.\]

For example, from our multiplication tables we see that \( 3 \equiv 5^{-1} \mod 7 \) since \( 3 \cdot 5 \equiv 1 \mod 7 \). Similarly, and \( 3 \equiv 3^{-1} \mod 8 \).

We conjectured and then we proved the following:

\[(2.2) \textbf{Theorem.} \text{ Let } a \text{ and } m \text{ be integers with } m > 0. \text{ If } a \text{ has an inverse modulo } m \text{ if and only if } \gcd(a, m) = 1.\]

\[\textbf{Proof.} \text{ Suppose } a \text{ has an inverse modulo } m. \text{ Let } b \equiv a^{-1} \mod m. \text{ This means } ab \equiv 1 \mod m. \text{ Then } ab - 1 = mq \text{ for some } q, \text{ or } ab + m(-q) = 1. \text{ That is, } 1 \text{ is a linear combination of } a \text{ and } m. \text{ By a theorem we proved earlier this semester, this means } \gcd(a, m) \text{ divides } 1. \text{ Thus, } \gcd(a, m) = 1. \text{ For the converse, suppose } \gcd(a, m) = 1. \text{ Then we know that } 1 \text{ is a linear combination of } a \text{ and } m \text{ (again, by a theorem we proved early this semester). Thus, there exist integers } x \text{ and } y \text{ such that } ax + my = 1. \text{ Therefore, } ax + my \equiv 1 \mod m. \text{ But } m \equiv 0 \mod m, \text{ so we have } ax \equiv 1 \mod m. \text{ Hence } x \equiv a^{-1} \mod m. \]

For small moduli finding inverses can be done by a quick inspection. But let’s think a moment on how to find the inverse of 47 modulo 1000.

Several of us came up with the following solution.
(2.3) **Example.** Find $47^{-1} \mod 1000$.

Note that 47 is prime and does not divide 1000. Therefore, $\gcd(47, 1000) = 1$. Hence, 47 does indeed have an inverse modulo 1000. We want to find a solution to the equation $47x + 1000y = 1$. To do this, we implement the Euclidean algorithm:

$$
1000 = 47(21) + 13 \\
47 = 13(3) + 8 \\
13 = 8(1) + 5 \\
8 = 5(1) + 3 \\
5 = 3(1) + 2 \\
3 = 2(1) + 1
$$

For the back substitution, let $a = 1000$ and $b = 47$:

$$
a = b(21) + 13 \quad \implies \quad 13 = a - 21b \\
b = (a - 21b)(3) + 8 \quad \implies \quad 8 = 64b - 3a \\
a - 21b = (64b - 3a)(1) + 5 \quad \implies \quad 5 = 4a - 85b \\
64b - 3a = (4a - 85b)(1) + 3 \quad \implies \quad 3 = 67 = 149b - 7a \\
4a - 85b = (149b - 7a)(1) + 2 \quad \implies \quad 2 = 11a - 234b \\
149b - 7a = (11a - 234b)(1) + 1 \quad \implies \quad 1 = 383b - 18a
$$

Thus, $47(383) + 1000(-18) = 1$ which implies $(383)(47) \equiv 1 \mod 1000$. Hence, $47^{-1} \equiv 383 \mod 1000$. 
