

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 $a^k \equiv 1 \pmod{m}$ does this implies that $\gcd(a, m) = 1$?

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

Proof. If $a^k \equiv 1 \pmod{m}$ then there exists an integer h such that $a^k - 1 = hm$ or $aa^{k-1} + (-h)m = 1$, 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 $a^k \equiv 1 \pmod{m}$? 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 $a^k \equiv 1 \pmod{m}$, then the smallest of such integers is called the order of a modulo m and it is defined by $\mathcal{O}_m(a)$.

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

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

$$\begin{array}{cccccc} \mathcal{O}_5(1) = 1 & \mathcal{O}_5(2) = 4 & \mathcal{O}_5(3) = 4 & \mathcal{O}_5(4) = 2 & & \\ \mathcal{O}_7(1) = 1 & \mathcal{O}_7(2) = 3 & \mathcal{O}_7(3) = 6 & \mathcal{O}_7(4) = 3 & \mathcal{O}_7(5) = 6 & \mathcal{O}_7(6) = 2 \end{array}$$

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 $\mathcal{O}_p(a)$ divides $p - 1$.

Proof. Let $k = \mathcal{O}_p(a)$ 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:

$$1 \equiv a^{p-1} \equiv a^{kq+r} \equiv a^{kq} a^r \equiv (a^k)^q a^r \equiv a^r \pmod{p},$$

where the first equality is Fermat's Theorem, and the fifth is given because $a^k \equiv 1 \pmod{p}$, since k is the order of a . This says that $1 \equiv a^r \pmod{p}$, which is a contradiction since $r < k$ and k is the smallest integer x such that $a^x \equiv 1 \pmod{p}$. \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 $\mathcal{O}_m(a)$ divides n .

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.

$$\begin{aligned} ax &= b \\ a^{-1}(ax) &= a^{-1}b \\ (a^{-1}a)x &= a^{-1}b \\ x &= a^{-1}b \end{aligned}$$

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 $ax \equiv 1 \pmod{m}$?

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

m	list of all a with $1 \leq a \leq m - 1$ such that $ax \equiv 1 \pmod{m}$ for some x (the value of x is in parenthesis)
5	1, 2, 3, 4
6	1, 5
7	1, 2, 3, 4, 5, 6
8	1, 3, 5, 7
9	1, 2, 4, 5, 7, 8
10	1, 3, 7, 9
11	1, 2, 3, 4, 5, 6, 7, 8, 9, 10

We then made a definition:

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

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

We conjectured and then we proved the following:

(2.2) **Theorem.** Let a and m be integers with $m > 0$. If a has an inverse modulo m if and only if $\gcd(a, m) = 1$.

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

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 $47^{-1} \% 1000$.

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 $b = 47$:

$$a = b(21) + 13 \implies 13 = a - 21b$$

$$b = (a - 21b)(3) + 8 \implies 8 = 64b - 3a$$

$$a - 21b = (64b - 3a)(1) + 5 \implies 5 = 4a - 85b$$

$$64b - 3a = (4a - 85b)(1) + 3 \implies 3 = 67 = 149b - 7a$$

$$4a - 85b = (149b - 7a)(1) + 2 \implies 2 = 11a - 234b$$

$$149b - 7a = (11a - 234b)(1) + 1 \implies 1 = 383b - 18a$$

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