

THE JOY OF NUMBERS

1. POWERS AND CONGRUENCE II

We started class by proving a simple result which is a consequence of the “pigeonhole principle.” The Pigeonhole Principle says that if you have $n + 1$ ‘pigeons’ to put into n ‘pigeonholes’, there will have to be at least 2 pigeons in at least one hole. One application of the Pigeonhole Principle is that at least two people in Nebraska have the same number of hairs on their heads. (A reasonable upper bound on the number of hairs on any person’s head is about 1 million and the population of Nebraska is over a million.)

(1.1) **Lemma.** *Let $a, m \in \mathbb{Z}$ with $m > 0$. Then there exist integers k, ℓ , $0 \leq k < \ell \leq m$ such that $a^k \equiv a^\ell \pmod{m}$.*

Proof. Given a and m , consider the first $m + 1$ powers of a : $a^0, a^1, a^2, \dots, a^m$. Now take the remainders modulo m of each of these numbers:

$$a^0 \% m, a^1 \% m, \dots, a^m \% m.$$

Each remainder must be between 0 and $m - 1$, a total of m different possibilities. But there are $m + 1$ numbers in the above list. By the Pigeonhole Principle, two of the remainders must be the same! That is, there exist integers $k < \ell$ between 0 and m such that $a^k \equiv a^\ell$. \square

Notice that since $k < \ell$ in the above equation, we could write it as

$$a^k \equiv a^k \cdot a^{\ell-k} \pmod{m}.$$

If we could cancel modulo m , then we could cancel a^k from both sides and get $1 \equiv a^{\ell-k} \pmod{m}$, where $\ell - k > 0$. However, we know we can’t cancel arbitrarily. For one thing, if $a \equiv 0 \pmod{m}$ then we certainly could never have $a^i \equiv 1 \pmod{m}$ for any $i > 0$. Even if $a \not\equiv 0 \pmod{m}$ cancellation sometimes doesn’t hold. However, one of your test problems is to show that cancellation does hold modulo a prime. That is, if $ab \equiv ac \pmod{p}$ where p is prime and $a \not\equiv 0 \pmod{p}$, then $b \equiv c \pmod{p}$. We will use this result in the proof of the following theorem:

(1.2) **Theorem.** *Let p be prime and $a \in \mathbb{Z}$ such that p does not divide a . Then there exists an integer s with $1 \leq s \leq p$ such that $a^s \equiv 1 \pmod{p}$.*

Proof. By the lemma, there exists integers $k < \ell$ between 0 and p such that $a^k \cdot a^\ell \equiv a^k \cdot a^\ell \pmod{p}$. Then $a^k \equiv a^k \cdot a^{\ell-k} \pmod{p}$. Since p does not divide a , p does not divide a^k . (Note we are using prime here!) Since cancellation holds modulo p , we can cancel a^k in this situation. This gives us $a^{\ell-k} \equiv 1 \pmod{p}$. Note that $1 \leq \ell - k \leq p$. \square

Now we focused our attention on the exponents.

Date: December 25, 2007.

(1.3) **Question.** Given a prime p , is there an exponent $k > 0$ such that for all $a \in \mathbb{Z}$ such that $a \not\equiv 0 \pmod{p}$ we have $a^k \equiv 1 \pmod{p}$? In other words, is there a single exponent which works for all a not divisible by p ? If so, what is the smallest such exponent?

To try to get a handle on this question, we looked at the first few primes and found that there is indeed a common exponent which works:

value of p :	2	3	5	7	11
smallest k :	1	2	4	6	10

This led us to make the following conjecture:

(1.4) **Conjecture.** Let p be a prime. Then $p - 1$ works for all a not divisible by p . That is, $a^{p-1} \equiv 1 \pmod{p}$ for all $1 \leq a \leq p - 1$.

Actually, this conjecture has a name: *Fermat's Theorem*. This is the same Fermat of Fermat's Last Theorem fame (see page 35), so some people prefer to call this Fermat's *Little* Theorem to distinguish it from his "big" theorem (which he probably never proved).

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

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

That is, S_p is the set of all the numbers between 1 and $p - 1$. Given $a \in S_p$, let

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

That is, multiply each number in S_p by a and take remainder modulo 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

$$3S_5 = \{3, 1, 4, 2\}.$$

Here, we multiplied 3 by 1, 2, 3, and 4 and took remainders modulo 5. Notice the resulting set is the same set we began with — only the order of the numbers was changed. Let's try another example: Let $p = 7$ and $5 \in S_7$. Then

$$5S_7 = \{5, 3, 1, 6, 4, 2\},$$

which again is the set S_7 . (The numbers are scrambled, but they're all there.) Let's try to prove this always happens:

(1.5) **Theorem.** Let p be prime and $a \in S_p$. Then $aS_p = S_p$.

Proof. The first step is to show that no number appears twice in aS_p ; i.e., aS_p contains $p - 1$ distinct elements. We will use that cancellation holds modulo p , since p is prime. Suppose $i, j \in S_p$, $i \neq j$, and $ai \% p = aj \% p$. Then $ai \equiv aj \pmod{p}$. Since $a \in S_p$ then $a \not\equiv 0 \pmod{p}$. Cancelling, we get $i \equiv j \pmod{p}$. But this is a contradiction, as i and j are less than p .

The next step is to show that $0 \notin S_p$. Suppose $ai \% p = 0$ for some $i \in S_p$. Then $ai \equiv 0 \pmod{p}$. But this means p divides ai , so p divides a or p divides i . This is a contradiction as $a, i \in S_p$.

Combining these two results, we see that aS_p consists of $p - 1$ different numbers between 1 and $p - 1$. Therefore, every remainder between 1 and $p - 1$ occurs in aS_p once and only once. Hence, $aS_p = S_p$. \square

We now use this to prove Fermat's Theorem:

(1.6) **Theorem.** (*Fermat's Theorem*) Let p be a prime and $a \in \mathbb{Z}$ such that p does not divide a . Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. First, by replacing a by its remainder modulo p , we can assume a is between 1 and $p-1$. (If $r = a \% p$ then $r \equiv a \pmod{p}$. Hence, $a^{p-1} \equiv r^{p-1} \pmod{p}$.) Consider the following:

$$\begin{aligned} a^{p-1}(1)(2)(3) \cdots (p-1) &= (a)(2a)(3a) \cdots (p-1)a \\ &\equiv (a \% p)(2a \% p)(3a \% p) \cdots ((p-1)a \% p) \pmod{p} \end{aligned}$$

In the first equality, we just rearranged the multiplication by putting an a next to each term in the product. In the next step we replaced each number in the product by its remainder modulo p . Now, the last number is just the product of all the numbers in the set aS_p . By the previous theorem, this is the same as the product of the numbers in S_p . (The two sets S_p and aS_p consist of the same numbers but rearranged. Of course, it doesn't matter which order you multiply numbers.) Hence,

$$\begin{aligned} a^{p-1}(1)(2)(3) \cdots (p-1) &\equiv (a \% p)(2a \% p)(3a \% p) \cdots ((p-1)a \% p) \pmod{p} \\ &\equiv (1)(2)(3) \cdots (p-1) \pmod{p}. \end{aligned}$$

Now just cancel 1, 2, 3, etc. from each side of the equation (again, this is possible since p is prime), we get

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

□

One application of this theorem is that it simplifies our successive squaring technique for finding large powers modulo a prime.

(1.7) **Example.** Find $5^{101} \% 11$. By Fermat, $5^{10} \equiv 1 \pmod{11}$. Using that $101 = (10)(10) + 1$, we have

$$\begin{aligned} 5^{101} &= 5^{(10)(10)+1} = (5^{10})^{10} \cdot 5^1 \\ &\equiv (1)^{10} \pmod{11} \cdot 5 \\ &\equiv 5 \pmod{11}. \end{aligned}$$

(1.8) **Example.** Find $(81)^{69} \% 23$. Since 23 is prime $81^{22} \equiv 1 \pmod{23}$ by Fermat. Now, $69 = (3)(22) + 3$. Therefore,

$$\begin{aligned} (81)^{69} &= (81^{22})^3 \cdot 81^3 \\ &\equiv (1)^3 \cdot (12)^3 \pmod{23} \\ &\equiv 3 \pmod{23}. \end{aligned}$$

by giving another proof of Fermat's Theorem. The new proof uses induction and the Freshman's Dream, which some of you proved on Test 4. The Freshman's Dream says that if p is prime then $(a+b)^p \equiv a^p + b^p \pmod{p}$ for all integers a, b . This is a consequence of the binomial theorem and that $\binom{p}{i} \equiv 0 \pmod{p}$ for $1 \leq i \leq p-1$.

(1.9) **Theorem.** (*Fermat's Theorem, Version II*) Let p be a prime. Then $a^p \equiv a \pmod{p}$ for all integers a .

Proof. We first prove this for all integers $a \geq 0$ using induction. Certainly when $a = 0$ the equation is true, since $0^p \equiv 0 \pmod{p}$. Suppose now that $a > 0$ and we know that statement is true for all integers less than or equal to a . In particular, we assume that $a^p \equiv a \pmod{p}$. We need to prove that the equation is true for $a + 1$, i.e., $(a + 1)^p \equiv a + 1 \pmod{p}$. Using the result of the test problem mentioned above, we have

$$\begin{aligned} (a + 1)^p &\equiv a^p + 1^p \pmod{p} \\ &\equiv a^p + 1 \pmod{p} \\ &\equiv a + 1 \pmod{p} \quad (\text{since } a^p \equiv a \pmod{p}). \end{aligned}$$

Hence, $(a + 1)^p \equiv a + 1 \pmod{p}$. Thus, we know the theorem is true for all $a \geq 0$. It was left to you to show this holds for negative values of a as well. \square

Note that new version of Fermat's theorem recovers our original version of Fermat's Theorem. For, if p does not divide a then we can cancel a from both sides of the equation $a^p \equiv a \pmod{p}$ to get $a^{p-1} \equiv 1 \pmod{p}$.

Next, we proved the following cancellation theorem. This is a generalization of the cancellation theorem we have been using when the modulus is prime.

(1.10) **Theorem.** Let a, b, c , and m be integers with $m > 0$. Suppose $ab \equiv ac \pmod{m}$ and $\gcd(a, m) = 1$. Then $b \equiv c \pmod{m}$.

Proof. Translating our assumption, we have m divides $a(b - c)$. But as $\gcd(a, m) = 1$, we must have m divides $b - c$. (See page 21 of your notes.) Therefore, $b \equiv c \pmod{m}$. \square

We can now give a proof of Conjecture of the last section.

(1.11) **Theorem.** Let $a, m \in \mathbb{Z}$ with $m > 0$ and $\gcd(a, m) = 1$. Then there exists an integer k with $1 \leq k \leq m$ such that

$$a^k \equiv 1 \pmod{m}.$$

Proof. There exists integers k, ℓ with $0 \leq k < \ell \leq m$ such that

$$a^k \equiv a^\ell \pmod{m}.$$

Since $\gcd(a, m) = 1$ we can cancel a from each side of the congruence to get $a^{k-1} \equiv a^{\ell-1} \pmod{m}$. Cancelling $k - 1$ more times, we get $1 \equiv a^{\ell-k} \pmod{m}$. Note that $1 \leq \ell - k \leq m$. \square