Congruences, Powers, and Fermat's Little Theorem

Take a number a and consider its powers $a, a^2, a^3, \ldots$ modulo m. Is there any pattern to these powers? We will start by looking at a prime modulus $m = p$, since the pattern is easier to spot. This is a common situation in the theory of numbers, especially when working with congruences. So whenever you're faced with discovering a congruence pattern, it's usually a good idea to begin with a prime modulus.

For each of the primes $p = 3$, $p = 5$, and $p = 7$, we have listed integers $a = 0, 1, 2, \ldots$ and some of their powers modulo p. Before reading further, you should stop, examine these tables, and try to formulate some conjectural patterns. Then test your conjectures by creating a similar table for $p = 11$ and seeing if your patterns are still true.

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	1	2	1

a^k modulo 3

a	a^2	a^3	a^4	a^5	a^6
0	0	0	0	0	0
1	1	1	1	1	1
2	4	3	1	2	4
3	4	2	1	3	4
4	1	4	1	4	1

a^k modulo 5

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
2	4	1	2	4	1	2	4
3	2	6	4	5	1	3	2
4	2	1	4	2	1	4	2
5	4	6	2	3	1	5	4
6	1	6	1	6	1	6	1

a^k modulo 7

Many interesting patterns are visible in these tables. The one that we will be

concerned with in this chapter can be seen in the columns

$$a^2 \pmod 3, \qquad a^4 \pmod 5, \qquad \text{and} \qquad a^6 \pmod 7.$$

Every entry in these columns, aside from the top one, is equal to 1. Does this pattern continue to hold for larger primes? You can check the table you made for $p = 11$, and you will find that

$$1^{10} \equiv 1 \pmod{11}, \quad 2^{10} \equiv 1 \pmod{11}, \quad 3^{10} \equiv 1 \pmod{11} \ldots$$
$$9^{10} \equiv 1 \pmod{11}, \quad \text{and} \quad 10^{10} \equiv 1 \pmod{11}.$$

This leads us to make the following conjecture:

$$a^{p-1} \equiv 1 \pmod p \qquad \text{for every integer } 1 \le a < p.$$

Of course, we don't really need to restrict a to be between 1 and $p - 1$. If a_1 and a_2 differ by a multiple of p, then their powers will be the same modulo p. So the real condition on a is that it not be a multiple of p. This result was first stated by Pierre de Fermat in a letter to Frénicle de Bessy dated 1640, but Fermat gave no indication of his proof. The first known proof appears to be due to Gottfried Leibniz.[1]

Theorem 1 (Fermat's Little Theorem)**.** *Let p be a prime number, and let a be any number with $a \not\equiv 0 \pmod p$. Then*

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

Before giving the proof of Fermat's Little Theorem, we want to indicate its power and show how it can be used to simplify computations. As a particular example, consider the congruence

$$6^{22} \equiv 1 \pmod{23}.$$

This says that the number $6^{22} - 1$ is a multiple of 23. If we wanted to check this fact without using Fermat's Little Theorem, we would have to multiply out 6^{22}, subtract 1, and divide by 23. Here's what we get:

$$6^{22} - 1 = 23 \cdot 5722682775750745.$$

[1] Gottfried Leibniz (1646–1716) is best known as one of the discoverers of the calculus. He and Isaac Newton worked out the main theorems of the calculus independently and at about the same time. The German and English mathematical communities spent the next two centuries arguing over who deserved priority. The current consensus is that both Leibniz and Newton should be given joint credit as the (independent) discoverers of the calculus.

Similarly, in order to verify directly that $73^{100} \equiv 1 \pmod{101}$, we would have to compute $73^{100} - 1$. Unfortunately, $73^{100} - 1$ has 187 digits! And notice that this example only uses $p = 101$, which is a comparatively small prime. Fermat's Little Theorem thus describes a very surprising fact about extremely large numbers.

We can use Fermat's Little Theorem to simplify computations. For example, in order to compute $2^{35} \pmod 7$, we can use the fact that $2^6 \equiv 1 \pmod 7$. So we write $35 = 6 \cdot 5 + 5$ and use the law of exponents to compute

$$2^{35} = 2^{6\cdot 5+5} = (2^6)^5 \cdot 2^5 \equiv 1^5 \cdot 2^5 \equiv 32 \equiv 4 \pmod 7.$$

Similarly, suppose that we want to solve the congruence $x^{103} \equiv 4 \pmod{11}$. Certainly, $x \not\equiv 0 \pmod{11}$, so Fermat's Little Theorem tells us that

$$x^{10} \equiv 1 \pmod{11}.$$

Raising both sides to the 10^{th} power gives $x^{100} \equiv 1 \pmod{11}$, and then multiplying by x^3 gives $x^{103} \equiv x^3 \pmod{11}$. So, to solve the original congruence, we just need to solve $x^3 \equiv 4 \pmod{11}$. This can be solved by trying successively $x = 1$, $x = 2, \ldots$. Thus,

$x \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$x^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

So the congruence $x^{103} \equiv 4 \pmod{11}$ has the solution $x \equiv 5 \pmod{11}$.

We are now ready to prove Fermat's Little Theorem. In order to illustrate the method of proof, we will first prove that $3^6 \equiv 1 \pmod 7$. Of course, there is no need to give a fancy proof of this fact, since $3^6 - 1 = 728 = 7 \cdot 104$. Nevertheless, when attempting to understand a proof or when attempting to construct a proof, it is often worthwhile using specific numbers. Of course, the idea is to devise a proof that doesn't really use the fact that we are considering specific numbers and then hope that the proof can be made to work in general.

To prove that $3^6 \equiv 1 \pmod 7$, we start with the numbers

$$1, 2, 3, 4, 5, 6,$$

multiply each of them by 3, and reduce modulo 7. The results are listed in the following table:

$x \pmod 7$	1	2	3	4	5	6
$3x \pmod 7$	3	6	2	5	1	4

Notice that each of the numbers $1, 2, 3, 4, 5, 6$ reappears exactly once in the second row. So if we multiply together all the numbers in the second row, we get the same

result as multiplying together all the numbers in the first row. Of course, we must work modulo 7. Thus,

$$\underbrace{(3\cdot 1)(3\cdot 2)(3\cdot 3)(3\cdot 4)(3\cdot 5)(3\cdot 6)}_{\text{numbers in second row}} \equiv \underbrace{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}_{\text{numbers in first row}} \pmod 7.$$

To save space, we use the standard symbol $n!$ for the number n *factorial*, which is the product of $1, 2, \ldots, n$. In other words,

$$n! = 1\cdot 2\cdot 3\cdots(n-1)\cdot n.$$

Factoring out the six factors of 3 on the left-hand side of our congruence gives

$$3^6\cdot 6! \equiv 6! \pmod 7.$$

Notice that $6!$ is relatively prime to 7, so we can cancel the $6!$ from both sides. This gives $3^6 \equiv 1 \pmod 7$, which is exactly Fermat's Little Theorem.

We are now ready to prove Fermat's Little Theorem in general. The key observation in our proof for $3^6 \pmod 7$ was that multiplication by 3 rearranged the numbers $1, 2, 3, 4, 5, 6 \pmod 7$. So first we are going to verify the following claim:

Lemma 2. *Let p be a prime number and let a be a number with $a \not\equiv 0 \pmod p$. Then the numbers*

$$a, 2a, 3a, \ldots, (p-1)a \pmod p$$

are the same as the numbers

$$1, 2, 3, \ldots, (p-1) \pmod p,$$

although they may be in a different order.

Proof. The list $a, 2a, 3a, \ldots, (p-1)a$ contains $p-1$ numbers, and clearly none of them are divisible by p. Suppose that we take two numbers ja and ka in this list, and suppose that they happen to be congruent,

$$ja \equiv ka \pmod p.$$

Then $p \mid (j-k)a$, so $p \mid (j-k)$, since we are assuming that p does not divide a. Notice that we are using the Prime Divisibility Property, which says that if a prime divides a product then it divides one of the factors. On the other hand, we know that $1 \le j, k \le p-1$, so $|j-k| < p-1$. There is only one number with absolute value less than $p-1$ that is divisible by p and that number is zero. Hence, $j = k$. This shows that different multiples in the list $a, 2a, 3a, \ldots, (p-1)a$ are distinct modulo p.

So we now know that the list $a, 2a, 3a, \ldots, (p-1)a$ contains $p-1$ distinct nonzero values modulo p. But there are only $p-1$ distinct nonzero values modulo p, that is, the numbers $1, 2, 3, \ldots, (p-1)$. Hence, the list $a, 2a, 3a, \ldots, (p-1)a$ and the list $1, 2, 3, \ldots, (p-1)$ must contain the same numbers modulo p, although the numbers may appear in a different order. This finishes the proof of the lemma.

Using the lemma, it is easy to finish the proof of Fermat's Little Theorem. The lemma says that the lists of numbers

$$a, 2a, 3a, \ldots, (p-1)a \pmod{p} \quad \text{and} \quad 1, 2, 3, \ldots, (p-1) \pmod{p}$$

are the same, so the product of the numbers in the first list is equal to the product of the numbers in the second list:

$$a \cdot (2a) \cdot (3a) \cdots ((p-1)a) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

Next we factor our $p-1$ copies of a from the left-hand side to obtain

$$a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}.$$

Finally, we observe that $(p-1)!$ is relatively prime to p, so we may cancel it from both sides to obtain Fermat's Little Theorem,

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

Fermat's Little Theorem can be used to show that a number is not a prime without actually factoring it. For example, it turns out that

$$2^{1234566} \equiv 899557 \pmod{1234567}.$$

This means that 1234567 cannot be a prime, since if it were, Fermat's Little Theorem would tell us that $2^{1234566}$ must be congruent to 1 modulo 1234567. It turns out that $1234567 = 127 \cdot 9721$, so in this case we can actually find a factor. But consider the number

$$m = 10^{100} + 37.$$

When we compute $2^{m-1} \pmod{m}$, we get

$$\begin{aligned} 2^{m-1} \equiv\ & 362636032754586106248776019963358391083687325301915138012832082409112485946357945905973007023184439 \\ & \pmod{m}. \end{aligned}$$

Again we deduce from Fermat's Little Theorem that $10^{100} + 37$ is not prime, but it is not at all clear how to find a factor. A quick check on a desktop computer reveals no prime factors less than 200,000. It is somewhat surprising that we can easily write down numbers that we know are composite, yet for which we are unable to find any factors.

Exercises

1. Use Fermat's Little Theorem to perform the following tasks.

(a) Find a number $0 \leq a < 73$ with $a \equiv 9^{794} \pmod{73}$.

(b) Solve $x^{86} \equiv 6 \pmod{29}$.

(c) Solve $x^{39} \equiv 3 \pmod{13}$.

2. The quantity $(p-1)! \pmod{p}$ appeared in our proof of Fermat's Little Theorem, although we didn't need to know its value.

(a) Compute $(p-1)! \pmod{p}$ for some small values of p, find a pattern, and make a conjecture.

(b) Prove that your conjecture is correct. [Try to discover why $(p-1)! \pmod{p}$ has the value it does for small values of p, and then generalize your observation to prove the formula for all values of p.]

3. Exercise 2 asked you to determine the value of $(p-1)! \pmod{p}$ when p is a prime number.

(a) Compute the value of $(m-1)! \pmod{m}$ for some small values of m that are not prime. Do you find the same pattern as you found for primes?

(b) If you know the value of $(n-1)! \pmod{n}$, how can you use the value to definitely distinguish whether n is prime or composite?

4. If p is a prime number and if $a \not\equiv 0 \pmod{p}$, then Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$.

(a) The congruence $7^{1734250} \equiv 1660565 \pmod{1734251}$ is true. Can you conclude that 1734251 is a composite number?

(b) The congruence $129^{64026} \equiv 15179 \pmod{64027}$ is true. Can you conclude that 64027 is a composite number?

(c) The congruence $2^{52632} \equiv 1 \pmod{52633}$ is true. Can you conclude that 52633 is a prime number?