# Congruences, Powers, and Euler's Formula

Here is Fermat's Little Theorem: If $p$ is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. This formula is certainly not true if we replace $p$ by a composite number. For example, $5^5 \equiv 5 \pmod{6}$ and $2^8 \equiv 4 \pmod{9}$. So we ask whether there is some power, depending on the modulus $m$, such that

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

Our first observation is that this is impossible if $\gcd(a, m) > 1$. To see why, suppose that $a^k \equiv 1 \pmod{m}$. Then $a^k = 1 + my$ for some integer $y$, so $\gcd(a, m)$ divides $a^k - my = 1$. In other words, if some power of $a$ is congruent to 1 modulo $m$, then we must have $\gcd(a, m) = 1$. This suggests that we look at the set of numbers that are relatively prime to $m$,

$$\big\{a \,:\, 1 \le a \le m \text{ and } \gcd(a, m) = 1\big\}.$$

For example,

| $m$ | $\{a : 1 \le a \le m \text{ and } \gcd(a, m) = 1\}$ |
|---|---|
| 1 | $\{1\}$ |
| 2 | $\{1\}$ |
| 3 | $\{1, 2\}$ |
| 4 | $\{1, 3\}$ |
| 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 | $\{1, 3, 7, 9\}$ |

From Chapter 10 of *A Friendly Introduction to Number Theory*, Fourth Edition. Joseph H. Silverman.

The number of integers between 1 and $m$ that are relatively prime to $m$ is an important quantity, so we give this quantity a name:

$$\phi(m) = \#\big\{a \,:\, 1 \le a \le m \text{ and } \gcd(a,m) = 1\big\}.$$

The function $\phi$ is called *Euler's phi function*. From the preceding table, we can read off the value of $\phi(m)$ for $1 \le m \le 10$. Thus

| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $\phi(m)$ | 1 | 1 | 2 | 2 | 4 | 2 | 6 | 4 | 6 | 4 |

Notice that if $p$ is a prime number then every integer $1 \le a < p$ is relatively prime to $p$. So for prime numbers we have the formula

$$\phi(p) = p - 1.$$

We are going to try to mimic a proof of Fermat's Little Theorem. Suppose, for example, that we want to find a power of 7 that is congruent to 1 modulo 10. Rather than taking all the numbers $1 \le a < 10$, we will just take the numbers that are relatively prime to 10. They are

$$1,\ 3,\ 7,\ 9 \pmod{10}.$$

If we multiply each of them by 7, we get

$$\begin{aligned} 7 \cdot 1 &\equiv 7 \pmod{10}, & 7 \cdot 3 &\equiv 1 \pmod{10}, \\ 7 \cdot 7 &\equiv 9 \pmod{10}, & 7 \cdot 9 &\equiv 3 \pmod{10}. \end{aligned}$$

Notice that we get back the same numbers, but rearranged. So if we multiply them together, we get the same product,

$$\begin{aligned} (7 \cdot 1)(7 \cdot 3)(7 \cdot 7)(7 \cdot 9) &\equiv 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10} \\ 7^4(1 \cdot 3 \cdot 7 \cdot 9) &\equiv 1 \cdot 3 \cdot 7 \cdot 9 \pmod{10}. \end{aligned}$$

Now we can cancel $1 \cdot 3 \cdot 7 \cdot 9$ to get $7^4 \equiv 1 \pmod{10}$.

Where does the exponent 4 come from? It's equal to the number of integers between 0 and 10 that are relatively prime to 10; that is, the exponent is 4 because $\phi(10) = 4$. This suggests the truth of the following formula.

**Theorem 1** (Euler's Formula)**.** *If* $\gcd(a,m) = 1$*, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

*Proof.* Now that we have identified the correct set of numbers to consider, the proof of Euler's formula is almost identical to the proof of Fermat's Little Theorem. So we let

$$1 \leq b_1 < b_2 < \cdots < b_{\phi(m)} < m$$

be the $\phi(m)$ numbers between 0 and $m$ that are relatively prime to $m$.

**Lemma 2.** *If* $\gcd(a, m) = 1$*, then the numbers*

$$b_1 a,\ b_2 a,\ b_3 a,\ \ldots,\ b_{\phi(m)} a \pmod{m}$$

*are the same as the numbers*

$$b_1,\ b_2,\ b_3,\ \ldots,\ b_{\phi(m)} \pmod{m},$$

*although they may be in a different order.*

*Proof of the lemma.* We note that if $b$ is relatively prime to $m$, then $ab$ is also relatively prime to $m$. Hence, each of the numbers in the list

$$b_1 a, b_2 a, b_3 a, \ldots, b_{\phi(m)} a \pmod{m}$$

is congruent to one number in the list

$$b_1, b_2, b_3, \ldots, b_{\phi(m)} \pmod{m}.$$

Furthermore, there are $\phi(m)$ numbers in each list. So if we can show that the numbers in the first list are distinct modulo $m$, it will follow that the two lists are the same (after rearranging).

Suppose that we take two numbers $b_j a$ and $b_k a$ from the first list, and suppose that they are congruent,

$$b_j a \equiv b_k a \pmod{m}.$$

Then $m|(b_j - b_k)a$. But $m$ and $a$ are relatively prime, so we find that $m|b_j - b_k$. On the other hand, $b_j$ and $b_k$ are between 1 and $m$, which implies $|b_j - b_k| \leq m - 1$. There is only one number with absolute value strictly less than $m$ that is divisible by $m$ and that number is zero. Hence, $b_j = b_k$. This shows that the numbers in the list

$$b_1 a, b_2 a, b_3 a, \ldots, b_{\phi(m)} a \pmod{m}$$

are all distinct modulo $m$, which completes the proof that the lemma is true.

Using the lemma, we can easily finish the proof of Euler's formula. The lemma says that the lists of numbers

$$b_1 a, b_2 a, b_3 a, \ldots, b_{\phi(m)} a \pmod{m}$$

and

$$b_1, b_2, b_3, \ldots, b_{\phi(m)} \pmod{m}$$

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:

$$(b_1 a) \cdot (b_2 a) \cdot (b_3 a) \cdots (b_{\phi(m)} a) \equiv b_1 \cdot b_2 \cdot b_3 \cdots b_{\phi(m)} \pmod{m}.$$

We can factor out $\phi(m)$ copies of $a$ from the left-hand side to obtain

$$a^{\phi(m)} B \equiv B \pmod{m}, \qquad \text{where } B = b_1 b_2 b_3 \cdots b_{\phi(m)}.$$

Finally, we observe that $B$ is relatively prime to $m$, since each of the $b_i$'s is relatively prime to $m$. This means we may cancel $B$ from both sides to obtain Euler's formula

$$a^{\phi(m)} \equiv 1 \pmod{m}. \qquad \square$$

## Exercises

**1.** Let $b_1 < b_2 < \cdots < b_{\phi(m)}$ be the integers between 1 and $m$ that are relatively prime to $m$ (including 1), and let $B = b_1 b_2 b_3 \cdots b_{\phi(m)}$ be their product. The quantity $B$ came up during the proof of Euler's formula.

**(a)** Show that either $B \equiv 1 \pmod{m}$ or $B \equiv -1 \pmod{m}$.

**(b)** Compute $B$ for some small values of $m$ and try to find a pattern for when it is equal to $+1 \pmod{m}$ and when it is equal to $-1 \pmod{m}$.

**2.** The number 3750 satisfies $\phi(3750) = 1000$. Find a number $a$ that has the following three properties:

(i) $a \equiv 7^{3003} \pmod{3750}$.

(ii) $1 \le a \le 5000$.

(iii) $a$ is not divisible by 7.

**3.** A composite number $m$ is called a *Carmichael number* if the congruence $a^{m-1} \equiv 1 \pmod{m}$ is true for every number $a$ with $\gcd(a, m) = 1$.

**(a)** Verify that $m = 561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. [*Hint*. It is not necessary to actually compute $a^{m-1} \pmod{m}$ for all 320 values of $a$. Instead, use Fermat's Little Theorem to check that $a^{m-1} \equiv 1 \pmod{p}$ for each prime $p$ dividing $m$, and then explain why this implies that $a^{m-1} \equiv 1 \pmod{m}$.]

**(b)** Try to find another Carmichael number. Do you think that there are infinitely many of them?