

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

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

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

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

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

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) $1 \leq a \leq 5000$.

(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?

Euler's Phi Function and the Chinese Remainder Theorem

Euler's formula

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

is a beautiful and powerful result, but it won't be of much use to us unless we can find an efficient way to compute the value of $\phi(m)$. Clearly, we don't want to list all the numbers from 1 to $m - 1$ and check each to see if it is relatively prime to m . This would be very time consuming if $m \approx 1000$, for example, and it would be impossible for $m \approx 10^{100}$. One case where $\phi(m)$ is easy to compute is when $m = p$ is a prime, since then every integer $1 \leq a \leq p - 1$ is relatively prime to m . Thus, $\phi(p) = p - 1$.

We can easily derive a similar formula for $\phi(p^k)$ when $m = p^k$ is a power of a prime. Rather than trying to count the numbers between 1 and p^k that are relatively prime to p^k , we will instead start with all numbers $1 \leq a \leq p^k$, and then we will discard the ones that are not relatively prime to p^k .

When is a number a not relatively prime to p^k ? The only factors of p^k are powers of p , so a is not relatively prime to p^k exactly when it is divisible by p . In other words,

$$\phi(p^k) = p^k - \#\{a : 1 \leq a \leq p^k \text{ and } p \mid a\}.$$

So we have to count how many integers between 1 and p^k are divisible by p . That's easy, they are the multiples of p ,

$$p, 2p, 3p, 4p, \dots, (p^{k-1} - 2)p, (p^{k-1} - 1)p, p^k.$$

There are p^{k-1} of them, which gives us the formula

$$\phi(p^k) = p^k - p^{k-1}.$$

From Chapter 11 of *A Friendly Introduction to Number Theory*, Fourth Edition. Joseph H. Silverman.
Copyright © 2013 by Pearson Education, Inc. All rights reserved.

For example,

$$\phi(2401) = \phi(7^4) = 7^4 - 7^3 = 2058.$$

This means that there are 2058 integers between 1 and 2401 that are relatively prime to 2401.

We now know how to compute $\phi(m)$ when m is a power of a prime. Next suppose that m is the product of two primes powers, $m = p^j q^k$. To formulate a conjecture, we compute $\phi(p^j q^k)$ for some small values and compare it with the values of $\phi(p^j)$ and $\phi(q^k)$.

p^j	q^k	$p^j q^k$	$\phi(p^j)$	$\phi(q^k)$	$\phi(p^j q^k)$
2	3	6	1	2	2
4	5	20	2	4	8
3	7	21	2	6	12
8	9	72	4	6	24
9	25	225	6	20	120

This table suggests that $\phi(p^j q^k) = \phi(p^j)\phi(q^k)$. We can also try some examples with numbers that are not prime powers, such as

$$\phi(14) = 6, \quad \phi(15) = 8, \quad \phi(210) = \phi(14 \cdot 15) = 48.$$

all this leads us to guess that the following assertion is true:

$$\text{If } \gcd(m, n) = 1, \text{ then } \phi(mn) = \phi(m)\phi(n).$$

Before trying to prove this multiplication formula, we show how it can be used to easily compute $\phi(m)$ for any m or, more precisely, for any m that you are able to factor as a product of primes.

Suppose that we are given a number m , and suppose that we have factored m as a product of primes, say

$$m = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r},$$

where p_1, p_2, \dots, p_r are all different. First we use the multiplication formula to compute

$$\phi(m) = \phi(p_1^{k_1}) \cdot \phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}).$$

Then we use the prime power formula $\phi(p^k) = p^k - p^{k-1}$ to obtain

$$\phi(m) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}).$$

This formula may look complicated, but the procedure to compute $\phi(m)$ is really very simple. For example,

$$\begin{aligned}\phi(1512) &= \phi(2^3 \cdot 3^3 \cdot 7) = \phi(2^3) \cdot \phi(3^3) \cdot \phi(7) \\ &= (2^3 - 2^2) \cdot (3^3 - 3^2) \cdot (7 - 1) = 4 \cdot 18 \cdot 6 = 432.\end{aligned}$$

So there are 432 numbers between 1 and 1512 that are relatively prime to 1512.

We are now ready to prove the multiplication formula for Euler's phi function. We also restate the formula for prime powers so as to have both formulas conveniently listed together.

Theorem 1 (Phi Function Formulas). (a) *If p is a prime and $k \geq 1$, then*

$$\phi(p^k) = p^k - p^{k-1}.$$

(b) *If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

Proof. We verified the prime power formula (a) earlier in this chapter, so we need to check the product formula (b). We will do this by using one of the most powerful tools available in number theory:

COUNTING

You may wonder how counting can be so powerful. After all, it's one of the first things taught in kindergarten.¹ Briefly, we are going to find one set that contains $\phi(mn)$ elements and a second set that contains $\phi(m)\phi(n)$ elements. Then we will show that the two sets contain the same number of elements.

The first set is

$$\{a : 1 \leq a \leq mn \text{ and } \gcd(a, mn) = 1\}.$$

It is clear that this set contains $\phi(mn)$ elements, since that's just the definition of $\phi(mn)$. The second set is

$$\left\{ (b, c) : \begin{array}{l} 1 \leq b \leq m \text{ and } \gcd(b, m) = 1 \\ 1 \leq c \leq n \text{ and } \gcd(c, n) = 1 \end{array} \right\}.$$

How many pairs (b, c) are in this second set? Well, there are $\phi(m)$ choices for b , since that's the definition of $\phi(m)$, and there are $\phi(n)$ choices for c , since that's the definition of $\phi(n)$. So there are $\phi(m)\phi(n)$ choices for the first coordinate b and $\phi(n)$

¹Yet another illustration of the principle that *Everything I Ever Needed To Know I Learned in Kindergarten*, although proving theorems in number theory probably isn't one of the basic skills that Robert Fulghum had in mind when he wrote his book!

choices for the second coordinate c ; so there are a total of $\phi(m)\phi(n)$ choices for the pair (b, c) .

For example, suppose that we take $m = 4$ and $n = 5$. Then the first set consists of the numbers

$$\{1, 3, 7, 9, 11, 13, 17, 19\}$$

that are relatively prime to 20. The second set consists of the pairs

$$\{(1, 1), (1, 2), (1, 3), (1, 4), (3, 1), (3, 2), (3, 3), (3, 4)\}$$

where the first number in each pair is relatively prime to 4 and the second number in each pair is relatively prime to 5.

Going back to the general case, we are going to take each element in the first set and assign it to a pair in the second set in the following way:

$$\left\{ \begin{array}{l} a : 1 \leq a \leq mn \\ \gcd(a, mn) = 1 \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} (b, c) : 1 \leq b \leq m, \gcd(b, m) = 1 \\ 1 \leq c \leq n, \gcd(c, n) = 1 \end{array} \right\}$$

$$a \pmod{mn} \longmapsto (a \pmod{m}, a \pmod{n})$$

What this means is that we take the integer a in the first set and send it to the pair (b, c) with

$$a \equiv b \pmod{m} \quad \text{and} \quad a \equiv c \pmod{n}.$$

This is probably clearer if we look again at our example with $m = 4$ and $n = 5$. Then, for example, the number 13 in the first set gets sent to the pair $(1, 3)$ in the second set, since $13 \equiv 1 \pmod{4}$ and $13 \equiv 3 \pmod{5}$. We do the same for each of the other numbers in the first set.

$$\{1, 3, 7, 9, 11, 13, 17, 19\} \longrightarrow \left\{ \begin{array}{l} (1, 1), (1, 2), (1, 3), (1, 4), \\ (3, 1), (3, 2), (3, 3), (3, 4) \end{array} \right\}$$

$1 \mapsto (1, 1)$	$11 \mapsto (3, 1)$
$3 \mapsto (3, 3)$	$13 \mapsto (1, 3)$
$7 \mapsto (3, 2)$	$17 \mapsto (1, 2)$
$9 \mapsto (1, 4)$	$19 \mapsto (3, 4)$

In this example, you can see that each pair in the second set is matched with exactly one number in the first set. This means that the two sets have the same number of elements. We want to check that the same matching occurs in general.

We need to check that the following two statements are correct:

1. Different numbers in the first set get sent to different pairs in the second set.

2. Every pair in the second set is hit by some number in the first set.

Once we verify these two statements, we will know that the two sets have the same number of elements. But we know that the first set has $\phi(mn)$ elements and the second set has $\phi(m)\phi(n)$ elements. So in order to finish the proof that $\phi(mn) = \phi(m)\phi(n)$, we just need to verify (1) and (2).

To check (1), we take two numbers a_1 and a_2 in the first set, and we suppose that they have the same image in the second set. This means that

$$a_1 \equiv a_2 \pmod{m} \quad \text{and} \quad a_1 \equiv a_2 \pmod{n}.$$

Thus, $a_1 - a_2$ is divisible by both m and n . However, m and n are relatively prime, so $a_1 - a_2$ must be divisible by the product mn . In other words,

$$a_1 \equiv a_2 \pmod{mn},$$

which shows that a_1 and a_2 are the same element in the first set. This completes our proof of statement (1).

To check statement (2), we need to show that for any given values of b and c we can find at least one integer a satisfying

$$a \equiv b \pmod{m} \quad \text{and} \quad a \equiv c \pmod{n}.$$

The fact that these simultaneous congruences have a solution is of sufficient importance to warrant having its own name.

Theorem 2 (Chinese Remainder Theorem). *Let m and n be integers satisfying $\gcd(m, n) = 1$, and let b and c be any integers. Then the simultaneous congruences*

$$x \equiv b \pmod{m} \quad \text{and} \quad x \equiv c \pmod{n}$$

have exactly one solution with $0 \leq x < mn$.

Proof. Let's start, as usual, with an example. Suppose we want to solve

$$x \equiv 8 \pmod{11} \quad \text{and} \quad x \equiv 3 \pmod{19}.$$

The solution to the first congruence consists of all numbers that have the form $x = 11y + 8$. We substitute this into the second congruence, simplify, and try to solve. Thus,

$$\begin{aligned} 11y + 8 &\equiv 3 \pmod{19} \\ 11y &\equiv 14 \pmod{19}. \end{aligned}$$

We know how to solve linear congruences of this sort. The solution is $y_1 \equiv 3 \pmod{19}$, and then we can find the solution to the original congruences using $x_1 = 11y_1 + 8 = 11 \cdot 3 + 8 = 41$. Finally, we should check our answer: $(41 - 8)/11 = 3$ and $(41 - 3)/19 = 2$. ✓

For the general case, we again begin by solving the first congruence $x \equiv b \pmod{m}$. The solution consists of all numbers of the form $x = my + b$. We substitute this into the second congruence, which yields

$$my \equiv c - b \pmod{n}.$$

We are given that $\gcd(m, n) = 1$, so the Linear Congruence Theorem tells us that there is exactly one solution y_1 with $0 \leq y_1 < n$. Then the solution to the original pair of congruences is given by

$$x_1 = my_1 + b;$$

and this will be the only solution x_1 with $0 \leq x_1 < mn$, since there is only one y_1 between 0 and n , and we multiplied y_1 by m to get x_1 . This completes our proof of the Chinese Remainder Theorem and, with it, our proof of the formula $\phi(mn) = \phi(m)\phi(n)$. □

Historical Interlude. The first recorded instance of the Chinese Remainder Theorem appears in a Chinese mathematical work from the late third or early fourth century. Somewhat surprisingly, it deals with the harder problem of three simultaneous congruences.

“We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?”

Sun Tzu Suan Ching (Master Sun's Mathematical Manual)

Circa AD 300, volume 3, problem 26.

Exercises


- (a) Find the value of $\phi(97)$.
(b) Find the value of $\phi(8800)$.
- (a) If $m \geq 3$, explain why $\phi(m)$ is always even.

(b) $\phi(m)$ is "usually" divisible by 4. Describe all the m 's for which $\phi(m)$ is not divisible by 4.

3. Suppose that p_1, p_2, \dots, p_r are the distinct primes that divide m . Show that the following formula for $\phi(m)$ is correct.

$$\phi(m) = m \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Use this formula to compute $\phi(1000000)$.

4.  Write a program to compute $\phi(n)$, the value of Euler's phi function. You should compute $\phi(n)$ by using a factorization of n into primes, not by finding all the a 's between 1 and n that are relatively prime to n .

5. For each part, find an x that solves the given simultaneous congruences.


(a) $x \equiv 3 \pmod{7}$ and $x \equiv 5 \pmod{9}$

(b) $x \equiv 3 \pmod{37}$ and $x \equiv 1 \pmod{87}$

(c) $x \equiv 5 \pmod{7}$ and $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$

6. Solve the 1700-year-old Chinese remainder problem from the *Sun Tzu Suan Ching*.

7. A farmer is on the way to market to sell eggs when a meteorite hits his truck and destroys all of his produce. In order to file an insurance claim, he needs to know how many eggs were broken. He knows that when he counted the eggs by 2's, there was 1 left over, when he counted them by 3's, there was 1 left over, when he counted them by 4's, there was 1 left over, when he counted them by 5's, there was 1 left over, and when he counted them by 6's, there was 1 left over, but when he counted them by 7's, there were none left over. What is the smallest number of eggs that were in the truck?

8.  Write a program that takes as input four integers (b, m, c, n) with $\gcd(m, n) = 1$ and computes an integer x with $0 \leq x < mn$ satisfying

$$x \equiv b \pmod{m} \quad \text{and} \quad x \equiv c \pmod{n}.$$

9. In this exercise you will prove a version of the Chinese Remainder Theorem for three congruences. Let m_1, m_2, m_3 be positive integers such that each pair is relatively prime. That is,

$$\gcd(m_1, m_2) = 1 \quad \text{and} \quad \gcd(m_1, m_3) = 1 \quad \text{and} \quad \gcd(m_2, m_3) = 1.$$

Let a_1, a_2, a_3 be any three integers. Show that there is exactly one integer x in the interval $0 \leq x < m_1 m_2 m_3$ that simultaneously solves the three congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad x \equiv a_3 \pmod{m_3}.$$

Can you figure out how to generalize this problem to deal with lots of congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \dots, \quad x \equiv a_r \pmod{m_r}?$$

In particular, what conditions do the moduli m_1, m_2, \dots, m_r need to satisfy?