**Fermat’s theorem**, also known as **Fermat’s little theorem** and **Fermat’s primality test**, in [number theory](https://www.britannica.com/science/number-theory), the statement, first given in 1640 by French mathematician [Pierre de Fermat](https://www.britannica.com/biography/Pierre-de-Fermat), that for any [prime](https://www.britannica.com/science/prime-number) number p and any [integer](https://www.britannica.com/science/integer) a such that p does not divide a (the pair are relatively prime), p divides exactly into ap − a. Although a number n that does not divide exactly into an − a for some a must be a composite number, the converse is not necessarily true. For example, let a = 2 and n = 341, then a and n are relatively prime and 341 divides exactly into 2341 − 2. However, 341 = 11 × 31, so it is a composite number (a special type of composite number known as a [pseudoprime](https://www.britannica.com/science/pseudoprime)). Thus, Fermat’s theorem gives a test that is necessary but not sufficient for primality.

**Fermat's little theorem** states that if *p* is a [prime number](https://en.wikipedia.org/wiki/Prime_number), then for any [integer](https://en.wikipedia.org/wiki/Integer) *a*, the number *ap* − *a* is an integer multiple of *p*. In the notation of [modular arithmetic](https://en.wikipedia.org/wiki/Modular_arithmetic), this is expressed as

{\displaystyle a^{p}\equiv a{\pmod {p}}.}

For example, if *a* = 2 and *p* = 7, then 27 = 128, and 128 − 2 = 126 = 7 × 18 is an integer multiple of 7.

If *a* is not divisible by *p*, Fermat's little theorem is equivalent to the statement that *ap*− 1 − 1 is an integer multiple of *p*, or in symbols:[[1]](https://en.wikipedia.org/wiki/Fermat%27s_little_theorem#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Fermat%27s_little_theorem#cite_note-2)

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

For example, if *a* = 2 and *p* = 7, then 26 = 64, and 64 − 1 = 63 = 7 × 9 is thus a multiple of 7.

Fermat's little theorem is the basis for the [Fermat primality test](https://en.wikipedia.org/wiki/Fermat_primality_test) and is one of the fundamental results of [elementary number theory](https://en.wikipedia.org/wiki/Elementary_number_theory). The theorem is named after [Pierre de Fermat](https://en.wikipedia.org/wiki/Pierre_de_Fermat), who stated it in 1640. It is called the "little theorem" to distinguish it from [Fermat's last theorem](https://en.wikipedia.org/wiki/Fermat%27s_last_theorem)

Proofs

Several proofs of Fermat's little theorem are known. It is frequently proved as a corollary of [Euler's theorem](https://en.wikipedia.org/wiki/Euler%27s_theorem).

# **Euler's theorem**

In [number theory](https://en.wikipedia.org/wiki/Number_theory), **Euler's theorem** (also known as the **Fermat–Euler theorem** or **Euler's totient theorem**) states that if *n* and *a* are [coprime](https://en.wikipedia.org/wiki/Coprime) positive integers, then *a* raised to the power of the [totient](https://en.wikipedia.org/wiki/Totient) of *n* is congruent to one, [modulo](https://en.wikipedia.org/wiki/Modular_arithmetic) *n*, or:

{\displaystyle a^{\varphi (n)}\equiv 1{\pmod {n}}}

where {\displaystyle \varphi (n)} is [Euler's totient function](https://en.wikipedia.org/wiki/Euler%27s_totient_function). In 1736, [Leonhard Euler](https://en.wikipedia.org/wiki/Leonhard_Euler) published his proof of [Fermat's little theorem](https://en.wikipedia.org/wiki/Fermat%27s_little_theorem),[[1]](https://en.wikipedia.org/wiki/Euler%27s_theorem#cite_note-1) which [Fermat](https://en.wikipedia.org/wiki/Pierre_de_Fermat) had presented without proof. Subsequently, Euler presented other proofs of the theorem, culminating with "Euler's theorem" in his paper of 1763, in which he attempted to find the smallest exponent for which Fermat's little theorem was always true.[[2]](https://en.wikipedia.org/wiki/Euler%27s_theorem#cite_note-2)

The converse of Euler's theorem is also true: if the above congruence is true, then {\displaystyle a} and {\displaystyle n} must be coprime.

The theorem is a generalization of [Fermat's little theorem](https://en.wikipedia.org/wiki/Fermat%27s_little_theorem), and is further generalized by [Carmichael's theorem](https://en.wikipedia.org/wiki/Carmichael_function).

The theorem may be used to easily reduce large powers modulo {\displaystyle n}. For example, consider finding the ones place decimal digit of {\displaystyle 7^{222}}, i.e. {\displaystyle 7^{222}{\pmod {10}}}. The integers 7 and 10 are coprime, and {\displaystyle \varphi (10)=4}. So Euler's theorem yields {\displaystyle 7^{4}\equiv 1{\pmod {10}}}, and we get {\displaystyle 7^{222}\equiv 7^{4\times 55+2}\equiv (7^{4})^{55}\times 7^{2}\equiv 1^{55}\times 7^{2}\equiv 49\equiv 9{\pmod {10}}}.

In general, when reducing a power of {\displaystyle a} modulo {\displaystyle n} (where {\displaystyle a} and {\displaystyle n} are coprime), one needs to work modulo {\displaystyle \varphi (n)} in the exponent of {\displaystyle a}:

if {\displaystyle x\equiv y{\pmod {\varphi (n)}}}, then {\displaystyle a^{x}\equiv a^{y}{\pmod {n}}}.

Euler's theorem underlies [RSA cryptosystem](https://en.wikipedia.org/wiki/RSA_(cryptosystem)), which is widely used in [Internet](https://en.wikipedia.org/wiki/Internet) communications. In this cryptosystem, Euler's theorem is used with *n* being a product of two large [prime numbers](https://en.wikipedia.org/wiki/Prime_number), and the security of the system is based on the difficulty of [factoring](https://en.wikipedia.org/wiki/Integer_factorization) such an integer.

**Proofs**

 Euler's theorem can be proven using concepts from the [theory of groups](https://en.wikipedia.org/wiki/Group_(mathematics)):[[3]](https://en.wikipedia.org/wiki/Euler%27s_theorem#cite_note-3) The residue classes modulo *n* that are coprime to *n* form a group under multiplication (see the article [Multiplicative group of integers modulo *n*](https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n) for details). The [order](https://en.wikipedia.org/wiki/Order_(group_theory)) of that group is *φ*(*n*). [Lagrange's theorem](https://en.wikipedia.org/wiki/Lagrange%27s_theorem_(group_theory)) states that the order of any subgroup of a [finite group](https://en.wikipedia.org/wiki/Finite_group) divides the order of the entire group, in this case *φ*(*n*). If *a* is any number [coprime](https://en.wikipedia.org/wiki/Coprime) to *n* then *a* is in one of these residue classes, and its powers *a*, *a*2, ... , *ak* modulo *n* form a subgroup of the group of residue classes, with *ak* ≡ 1 (mod *n*). Lagrange's theorem says *k* must divide *φ*(*n*), i.e. there is an integer *M* such that *kM* = *φ*(*n*). This then implies,

{\displaystyle a^{\varphi (n)}=a^{kM}=(a^{k})^{M}\equiv 1^{M}=1\equiv 1{\pmod {n}}.}

2. There is also a direct proof:[[4]](https://en.wikipedia.org/wiki/Euler%27s_theorem#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Euler%27s_theorem#cite_note-5) Let *R* = {*x*1, *x*2, ... , *xφ*(*n*)} be a [reduced residue system](https://en.wikipedia.org/wiki/Reduced_residue_system) (mod *n*) and let *a* be any integer coprime to *n*. The proof hinges on the fundamental fact that multiplication by *a* permutes the *xi*: in other words if *axj* ≡ *axk* (mod *n*) then *j* = *k*. (This law of cancellation is proved in the article [Multiplicative group of integers modulo *n*](https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n#Group_axioms).[[6]](https://en.wikipedia.org/wiki/Euler%27s_theorem#cite_note-6)) That is, the sets *R* and *aR* = {*ax*1, *ax*2, ... , *axφ*(*n*)}, considered as sets of congruence classes (mod *n*), are identical (as sets—they may be listed in different orders), so the product of all the numbers in *R* is congruent (mod *n*) to the product of all the numbers in *aR*:

{\displaystyle \prod \_{i=1}^{\varphi (n)}x\_{i}\equiv \prod \_{i=1}^{\varphi (n)}ax\_{i}=a^{\varphi (n)}\prod \_{i=1}^{\varphi (n)}x\_{i}{\pmod {n}},} and using the cancellation law to cancel each *xi* gives Euler's theorem:

{\displaystyle a^{\varphi (n)}\equiv 1{\pmod {n}}.}

**Euler’s Quotient:**

The **Euler quotient** of an integer *a* with respect to *n* is defined as:

{\displaystyle q\_{n}(a)={\frac {a^{\varphi (n)}-1}{n}}}

The special case of an Euler quotient when *n* is prime is called a [Fermat quotient](https://en.wikipedia.org/wiki/Fermat_quotient).

Any odd number *n* that divides {\displaystyle q\_{n}(2)} is called a [Wieferich number](https://en.wikipedia.org/wiki/Wieferich_number). This is equivalent to saying that 2*φ*(*n*) ≡ 1 (mod *n*2). As a generalization, any number *n* that is coprime to a positive integer *a*, and such that *n* divides {\displaystyle q\_{n}(a)}, is called a (generalized) Wieferich number to base *a*. This is equivalent to saying that a*φ*(*n*) ≡ 1 (mod *n*2).

**Second Explanation of Euler’s & Fermat’s**

**FERMAT’S AND EULER’S THEOREMS**

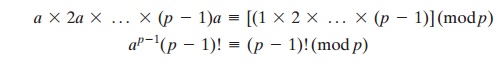
Two theorems that play important roles in public-key cryptography are Fermat’s theorem and Euler’s theorem.

Fermat’s Theorem

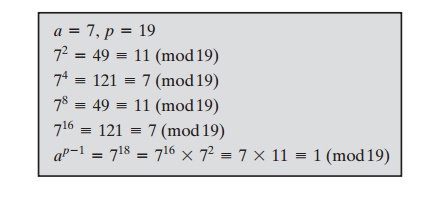
Fermat’s theorem states the following: If *p*is prime and *a*is a positive integer not divisible by *p*, then



Proof: Consider the set of positive integers less than p: {1, 2,  ......., p  -   1}  and multiply   each   element  by a,  modulo p,   to   get   the  set X = {a mod p,  2a mod p, ..... , (p - 1)a mod p}. None of the elements of X is equal to zero because *p*does not divide *a*. Furthermore, no two of the integers in *X*are equal. To see this, assume that *ja*== *ka*(mod *p*)), where 1 <= *j*< *k*<= *p*- 1. Because *a*is relatively prime5 to *p*, we can eliminate *a*from both sides of the equation [see Equation (4.3)] resulting in *j*=== *k*(mod *p*). This last equality is impossible, because *j*and *k*are both positive integers less than *p*. Therefore, we know that the (*p*- 1) elements of *X*are all positive integers with no two elements equal. We can conclude the *X*consists of the set of integers {1, 2, ...., *p*- 1} in some order. Multiplying the numbers in both sets (*p*and *X*) and taking the result mod *p*yields



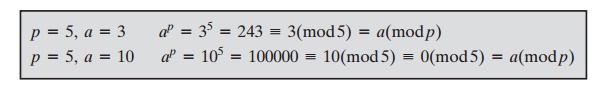
We can cancel the ((*p*- 1)! term because it is relatively prime to *p*[see Equation (4.5)]. This yields Equation (8.2), which completes the proof.



An alternative form of Fermat’s theorem is also useful: If *p*is prime and *a*is a positive  integer, then



Note that the first form of the theorem [Equation (8.2)] requires that *a*be relatively prime to *p*, but this form does not.



Euler’s Totient Function

Before presenting Euler’s theorem, we need to introduce an important quantity in number theory, referred to as **Euler’s totient function**, written ϕ(*n*), and defined as the number of positive integers less than *n*and relatively prime to *n*. By convention, ϕ(1)   =   1.

**DETERMINE**ϕ**(37) AND**ϕ**(35).**

**Because 37 is prime, all of the positive integers from 1 through 36 are rela- tively prime to 37. Thus**ϕ**(37)   =   36.**

**To determine**ϕ**(35), we list all of the positive integers less than 35 that are rela- tively prime to it:**

**1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18**

**19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34**

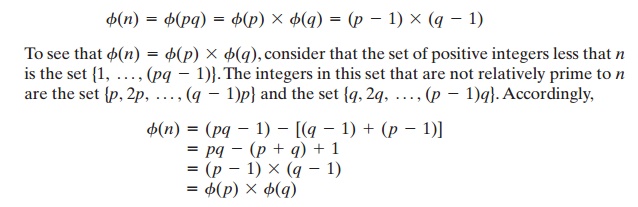
**There are 24 numbers on the list, so**ϕ**(35)  =  24.**

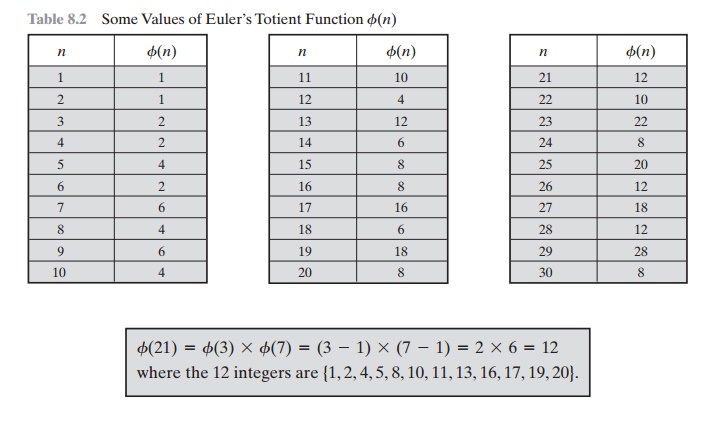
Table 8.2 lists the first 30 values of ϕ(*n*). The value ϕ(1) is without meaning but is defined to have the value 1.

It should be clear that, for a prime number *p*,

ϕ(*p*)  =  *p*-  1

Now suppose that we have two prime numbers *p*and *q*with *p*!= *q*. Then we can show that, for *n*= *pq*,





Euler’s Theorem

Euler’s theorem states that for every *a*and *n*that are relatively   prime:



***Proof:***Equation (8.4) is true if *n*is prime, because in that case, ϕ(*n*)  =  (*n*-  1) and Fermat’s theorem holds. However, it also holds for any integer *n*. Recall that *f*(*n*) is the number of positive integers less than *n*that are relatively prime to *n*. Consider the set of such integers, labeled as

*R*=  {*x*1, *x*2,  ...... , *x*ϕ(*n*)}

That  is,  each  element *xi*is  a  unique  positive  integer  less  than  *n*with gcd(*xi*, *n*)  = 1. Now multiply each element by *a*, modulo *n*:

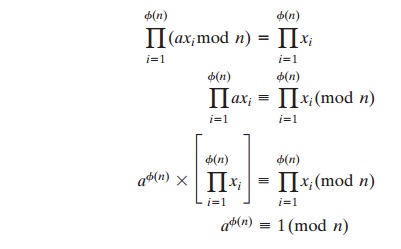
*S*=  {(*ax*1 mod *n*), (*ax*2 mod *n*),  ....., (*ax*ϕ(*n*) mod *n*)}

The set *S*is a permutation6 of *R*, by the following line of reasoning:

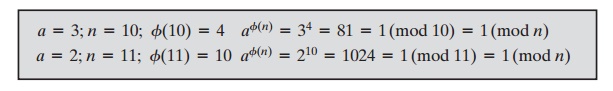
**1.**                                                                                  Because *a*is relatively prime to *n*and *xi*is relatively prime to *n*, *axi*must also be relatively prime to *n*. Thus, all the members of *S*are integers that are less than *n*and that are relatively prime to  *n*.

1. There are no duplicates in S. Refer to Equation (4.5). If axi mod n = axj mod n, then xi = xj.

Therefore,



which completes the proof. This is the same line of reasoning applied to the proof of Fermat’s theorem.



As is the case for Fermat’s theorem, an alternative form of the theorem is also useful:



Again, similar to the case with Fermat’s theorem, the first form of Euler’s theorem [Equation (8.4)] requires that *a*be relatively prime to *n*, but this form does   not.

**Euler’s Totient Function**

In [number theory](https://en.wikipedia.org/wiki/Number_theory), **Euler's totient function** counts the positive integers up to a given integer *n* that are [relatively prime](https://en.wikipedia.org/wiki/Relatively_prime) to *n*. It is written using the Greek letter [phi](https://en.wikipedia.org/wiki/Phi) as *φ*(*n*) or *ϕ*(*n*), and may also be called **Euler's phi function**. In other words, it is the number of integers *k* in the range 1 ≤ *k* ≤ *n* for which the [greatest common divisor](https://en.wikipedia.org/wiki/Greatest_common_divisor) gcd(*n*, *k*) is equal to 1.[[2]](https://en.wikipedia.org/wiki/Euler%27s_totient_function#cite_note-2)[[3]](https://en.wikipedia.org/wiki/Euler%27s_totient_function#cite_note-3) The integers *k* of this form are sometimes referred to as [totatives](https://en.wikipedia.org/wiki/Totative) of *n*.

For example, the totatives of *n* = 9 are the six numbers 1, 2, 4, 5, 7 and 8. They are all relatively prime to 9, but the other three numbers in this range, 3, 6, and 9 are not, since gcd(9, 3) = gcd(9, 6) = 3 and gcd(9, 9) = 9. Therefore, *φ*(9) = 6. As another example, *φ*(1) = 1 since for *n* = 1 the only integer in the range from 1 to *n* is 1 itself, and gcd(1, 1) = 1.

Euler's totient function is a [multiplicative function](https://en.wikipedia.org/wiki/Multiplicative_function), meaning that if two numbers *m* and *n* are relatively prime, then *φ*(*mn*) = *φ*(*m*)*φ*(*n*).[[4]](https://en.wikipedia.org/wiki/Euler%27s_totient_function#cite_note-4)[[5]](https://en.wikipedia.org/wiki/Euler%27s_totient_function#cite_note-5) This function gives the [order](https://en.wikipedia.org/wiki/Order_(group_theory)) of the [multiplicative group of integers modulo *n*](https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n) (the [group](https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n) of [units](https://en.wikipedia.org/wiki/Unit_(ring_theory)) of the [ring](https://en.wikipedia.org/wiki/Ring_(algebra)) **ℤ**/*n***ℤ**).[[6]](https://en.wikipedia.org/wiki/Euler%27s_totient_function#cite_note-6) It is also used for defining the [RSA encryption system](https://en.wikipedia.org/wiki/RSA_(cryptosystem)).

**Euler's Totient Function and Euler's Theorem**

The Euler's totient function, or phi (φ) function is a very important number theoretic function having a deep relationship to prime numbers and the so-called order of integers. The totient φ(*n*) of a positive integer *n* greater than 1 is defined to be the number of positive integers less than *n* that are coprime to *n*. φ(*1*) is defined to be 1. The following table shows the function values for the first several natural numbers:

| **n** | **φ(*n*)** | **numbers coprime to n** |
| --- | --- | --- |
| 1 | 1 | 1 |
| 2 | 1 | 1 |
| 3 | 2 | 1, 2 |
| 4 | 2 | 1,3 |
| 5 | 4 | 1,2,3,4 |
| 6 | 2 | 1,5 |
| 7 | 6 | 1,2,3,4,5,6 |
| 8 | 4 | 1,3,5,7 |
| 9 | 6 | 1,2,4,5,7,8 |
| 10 | 4 | 1,3,7,9 |
| 11 | 10 | 1,2,3,4,5,6,7,8,9,10 |
| 12 | 4 | 1,5,7,11 |
| 13 | 12 | 1,2,3,4,5,6,7,8,9,10,11,12 |
| 14 | 6 | 1,3,5,9,11,13 |
| 15 | 8 | 1,2,4,7,8,11,13,14 |

Can you find some relationships between *n* and φ(*n*)? One thing you may have noticed is that:

**when *n* is a prime number** (e.g. 2, 3, 5, 7, 11, 13), **φ(*n*) = *n*-1**.

But how about the composite numbers? You may also have noticed that, for example, 15 = 3\*5 and φ(*15*) = φ(*3*)\*φ(*5*) = 2\*4 = 8. This is also true for 14,12,10 and 6. However, it does not hold for 4, 8, 9. For example, 9 = 3\*3 , but φ(*9*) = 6 ≠ φ(3)\*φ(*3*) = 2\*2 =4. In fact, this multiplicative relationship is conditional:

**when *m* and *n* are coprime, φ(*m\*n*) = φ(*m*)\*φ(*n*)**.

The general formula to compute φ(n) is the following:

I**f the prime factorisation of n is given by n =p1e1\*...\*pnen, then φ(n) = n \*(1 - 1/p1)\* ... (1 - 1/pn)**.

For example:

* 9 = 32, φ(*9*) = 9\* (1-1/3) = 6
* 4 =22, φ(*4*) = 4\* (1-1/2) = 2
* 15 = 3\*5, φ(*15*) = 15\* (1-1/3)\*(1-1/5) = 15\*(2/3)\*(4/5) =8

Euler’s theorem generalises Fermat’s theorem to the case where the modulus is not prime. It says that:

if *n* is a positive integer and a, n are coprime, then *a*φ(n) ≡ 1 mod *n* where φ(n) is the Euler's totient function.

Let's see some examples:

* 165 = 15\*11, φ(165) = φ(15)\*φ(11) = 80. 880 ≡ 1 mod 165
* 1716 = 11\*12\*13, φ(1716) = φ(11)\*φ(12)\*φ(13) = 480. 7480 ≡ 1 mod 1716
* φ(13) = 12, 912 ≡ 1 mod 13

We can see that Fermat's little theorem is a special case of Euler's Theorem: for any prime *n*, φ(n) = *n*-1 and any number a 0< a <n is coprime to *n*. From Euler's Theorem, we can easily get several useful corollaries. First:

if *n* is a positive integer and *a, n* are coprime, then *a*φ(n)+1 ≡ a mod *n*.

This is because *a*φ(n)+1 = *a*φ(n)\*a, *a*φ(n) ≡ 1 mod *n* and *a ≡ a*mod *n*, so *a*φ(n)+1 ≡ *a* mod *n*. From here, we can go even further:

if *n* is a positive integer and *a, n* are coprime, b ≡ 1 mod φ(n), then *a*b ≡ *a* mod *n*.

If b ≡ 1 mod φ(n), then it can be written as *b = k\*φ(n)*+1 for some *k*. Then *a*b = ak\*φ(n)+1 = (aφ(n))k\*a. Since *a*φ(n) ≡ 1 mod *n*, (*a*φ(n))k ≡ 1k ≡ 1 mod *n*. Then (aφ(n))k\*a ≡ *a* mod *n.*This is why RSA works.

REFERENCES

<http://www.brainkart.com/article/Classical-Encryption-Techniques_8339/>

<https://www.tutorialspoint.com/cryptography/index.htm>

<https://www.geeksforgeeks.org/cryptography-introduction/>

[https://www.techopedia.com/definition/1770/cryptography#:~:text=Cryptography%20involves%20creating%20written%20or,information%20to%20be%20kept%20secret.&text=Information%20security%20uses%20cryptography%20on,transit%20and%20while%20being%20stored](https://www.techopedia.com/definition/1770/cryptography).

<https://www2.slideshare.net/lineking/classical-encryption-techniques-in-network-security?qid=e388c29f-793d-4f2b-bcaf-9d22e9ca07b5&v=&b=&from_search=1>

<https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography>

<https://www.academia.edu/Documents/in/Cryptography>