



WIKIPEDIA  
The Free Encyclopedia

Main page  
Contents  
Featured content  
Current events  
Random article  
Donate to Wikipedia  
Wikipedia store

Interaction

Help  
About Wikipedia  
Community portal  
Recent changes  
Contact page

Tools

What links here  
Related changes  
Upload file  
Special pages  
Permanent link  
Page information  
Wikidata item  
Cite this page

Print/export

Create a book  
Download as PDF  
Printable version

Languages


Català  
Deutsch  
Français  
ไทย

 Edit links

[Create account](#) [Log in](#)

Article [Talk](#)

[Read](#) [Edit](#) [View history](#)



# Congruence of squares

From Wikipedia, the free encyclopedia



This article **does not cite any references or sources**. Please help [improve this article](#) by [adding citations to reliable sources](#). Unsourced material may be challenged and [removed](#). *(December 2009)*

In [number theory](#), a **congruence of squares** is a [congruence](#) commonly used in [integer factorization](#) algorithms.

**Contents** [\[hide\]](#)

- 1 Derivation
  - 1.1 Further generalizations
- 2 Examples
  - 2.1 Factorize 35
  - 2.2 Factorize 1649
- 3 See also

## Derivation [\[edit\]](#)

Given a positive [integer](#) *n*, [Fermat's factorization method](#) relies on finding numbers *x*, *y* satisfying the [equality](#)

$$x^2 - y^2 = n$$

We can then factor  $n = x^2 - y^2 = (x + y)(x - y)$ . This algorithm is slow in practice because we need to search many such numbers, and only a few satisfy the strict equation. However, *n* may also be factored if we can satisfy the weaker **congruence of squares** condition:

$$x^2 \equiv y^2 \pmod{n}, \quad x \not\equiv \pm y \pmod{n}.$$

From here we easily deduce

$$x^2 - y^2 \equiv 0 \pmod{n}, \quad (x + y)(x - y) \equiv 0 \pmod{n}$$

This means that *n* divides the product  $(x + y)(x - y)$ , but since we also require  $x \not\equiv \pm y \pmod{n}$ , *n* divides neither  $(x + y)$  nor  $(x - y)$  alone. Thus  $(x + y)$  and  $(x - y)$  each contain proper factors of *n*. Computing the [greatest common divisors](#) of  $(x + y, n)$  and of  $(x - y, n)$  will give us these factors; this can be done quickly using the [Euclidean algorithm](#).

Congruences of squares are extremely useful in integer factorization algorithms and are extensively used in, for example, the [quadratic sieve](#), [general number field sieve](#), [continued fraction factorization](#), and [Dixon's factorization](#). Conversely, because finding square roots modulo a composite number turns out to be probabilistic polynomial-time equivalent to factoring that number, any integer factorization algorithm can be used efficiently to identify a congruence of squares.

## Further generalizations [\[edit\]](#)

It is also possible to use [factor bases](#) to help find congruences of squares more quickly. Instead of looking for  $x^2 \equiv y^2 \pmod{n}$  from the outset, we find many  $x^2 \equiv y \pmod{n}$  where the *y* have small prime factors, and try to multiply a few of these together to get a square on the right-hand side.

## Examples [\[edit\]](#)

### Factorize 35 [\[edit\]](#)

We take ***n* = 35** and find that

$$6^2 = 36 \equiv 1 \equiv 1^2 \pmod{n}.$$

We thus factor as

$$(\gcd[6 - 1, 35]) \cdot (\gcd[6 + 1, 35]) = (5) \cdot (7) = 35.$$

## Factorize 1649 [[edit](#)]

Using  $n = 1649$ , as an example of finding a congruence of squares built up from the products of non-squares (see [Dixon's factorization method](#)), first we obtain several congruences

$$41^2 \equiv 32 : 42^2 \equiv 115 : 43^2 \equiv 200 \pmod{1649},$$

of these, two have only small primes as factors

$$32 = 2^5 : 200 = (2^3) \cdot (5^2),$$

and a combination of these has an even power of each small prime, and is therefore a square

$$(32) \cdot (200) = (2^{5+3}) \cdot (5^2) = ((2^4) \cdot (5))^2 = 80^2$$

yielding the congruence of squares

$$(32) \cdot (200) = 80^2 \equiv (41^2) \cdot (43^2) \equiv 114^2 \pmod{1649}$$

So using the values of 80 and 114 as our  $x$  and  $y$  gives factors

$$(\gcd[114 - 80, 1649]) \cdot (\gcd[114 + 80, 1649]) = (17) \cdot (97) = 1649.$$

## See also [[edit](#)]

- [Congruence relation](#)

Categories: [Modular arithmetic](#) | [Integer factorization algorithms](#)

This page was last modified on 18 December 2013, at 18:24.

Text is available under the [Creative Commons Attribution-ShareAlike License](#); additional terms may apply. By using this site, you agree to the [Terms of Use](#) and [Privacy Policy](#). Wikipedia® is a registered trademark of the [Wikimedia Foundation, Inc.](#), a non-profit organization.

[Privacy policy](#) [About Wikipedia](#) [Disclaimers](#) [Contact Wikipedia](#) [Developers](#) [Mobile view](#)

