

Euclid's lemma

In number theory, **Euclid's lemma** is a lemma that captures a fundamental property of prime numbers, namely:^[note 1]

Euclid's lemma— If a prime p divides the product ab of two integers a and b , then p must divide at least one of those integers a and b .

For example, if $p = 19$, $a = 133$, $b = 143$, then $ab = 133 \times 143 = 19019$, and since this is divisible by 19, the lemma implies that one or both of 133 or 143 must be as well. In fact $133 = 19 \times 7$.

The lemma is not true when p is a composite number. For example, in the case of $p = 10$, $a = 4$, $b = 15$, composite number 10 divides $ab = 4 \times 15 = 60$, but 10 divides neither 4 nor 15.

This property is the key in the proof of the fundamental theorem of arithmetic.^[note 2] It is used to define prime elements, a generalization of prime numbers to arbitrary commutative rings. Euclid's Lemma shows that in the integers irreducible elements are also prime elements. The proof uses induction so it does not apply to all integral domains.

Contents

Formulations
History
Proof
Proof using Bézout's lemma Proof of Elements
See also
Footnotes
Notes Citations
References
External links

Formulations

Let p be a prime number, and assume p divides the product of two integers a and b . (In symbols this is written $p|ab$. Its negation, p does not divide ab is written $p \nmid ab$.) Then $p|a$ or $p|b$ (or both). Equivalent statements are:

- If $p \nmid a$ and $p \nmid b$, then $p \nmid ab$.
- If $p \nmid a$ and $p|ab$, then $p|b$.

Euclid's lemma can be generalized from prime numbers to any integers:

Theorem — If $n|ab$, and n is relatively prime to a , then $n|b$.

This is a generalization because if n is prime, either

- $n|a$ or
- n is relatively prime to a . In this second possibility $n \nmid a$ so $n|b$.

History

The lemma first appears as proposition 30 in Book VII of [Euclid's *Elements*](#). It is included in practically every book that covers elementary number theory^{[4][5][6][7][8]}

The generalization of the lemma to integers appeared in [Jean Prestet's](#) textbook *Nouveaux Elémens de Mathématiques* in 1681.^[9]

In [Carl Friedrich Gauss's](#) treatise *Disquisitiones Arithmeticae*, the statement of the lemma is Euclid's Proposition 14 (Section 2), which he uses to prove the uniqueness of the decomposition product of prime factors of an integer (Theorem 16), admitting the existence as "obvious." From this existence and uniqueness he then deduces the generalization of prime numbers to integers.^[10] For this reason, the generalization of Euclid's lemma is sometimes referred to as Gauss's lemma, but some believe this usage is incorrect^[11] due to confusion with [Gauss's lemma on quadratic residues](#)

Proof

Proof using Bézout's lemma

The usual proof involves another lemma called [Bézout's identity](#).^[12] This states that if x and y are [relatively prime integers](#) (i.e. they share no common divisors other than 1) there exist integers r and s such that

$$rx + sy = 1.$$

Let a and n be relatively prime, and assume that $n|ab$. By Bézout's identity there are r and s making

$$rn + sa = 1.$$

Multiply both sides by b :

$$rnb + sab = b.$$

The first term on the left is divisible by n , and the second term is divisible by ab , which by hypothesis is divisible by n . Therefore their sum, b , is also divisible by n . This is the generalization of Euclid's lemma mentioned above.

Proof of Elements

Euclid's lemma is proved at the Proposition 30 in Book VII of *Elements*. The original proof is difficult to understand as is, so we quote the commentary from [Euclid & Heath \(1956 pp. 319-332\)](#).

Proposition 19

If four numbers be proportional, the number produced from the first and fourth is equal to the number produced from the second and third; and, if the number produced from the first and fourth be equal to that produced from the second and third, the four numbers are proportional. ^[note 3]

Proposition 20

The least numbers of those that have the same ratio with them measures those that have the same ratio the same number of times—the greater the greater and the less the less. ^[note 4]

Proposition 21

Numbers prime to one another are the least of those that have the same ratio with them. ^[note 5]

Proposition 29

Any prime number is prime to any number it does not measure. ^[note 6]

Proposition 30

If two numbers, by multiplying one another, make the same number, and any prime number measures the product, it also measures one of the original numbers. ^[note 7]

Proof

If c , a prime number, measure ab , c measures either a or b .

Suppose c does not measure a .

Therefore c , a are prime to one another.

[VII. 29]

Suppose $ab = mc$.

Therefore $c : a = b : m$.

[VII. 19]

Hence [VII. 20, 21] $b = nc$, where n is some integer.

Therefore c measures b .

Similarly, if c does not measure b , c measures a .

Therefore c measures one or other of the two numbers a , b .

Q.E.D. ^[18]

See also

- | | |
|---|---------------------------------------|
| ▪ Bézout's identity | ▪ Irreducible element |
| ▪ Euclidean algorithm | ▪ Prime element |
| ▪ Fundamental theorem of arithmetic | ▪ Prime number |

Footnotes

Notes

1. It is also called **Euclid's first theorem**^{[1][2]} although that name more properly belongs to the side-angle-side condition for showing that triangles are congruent^[3]
2. In general, to show that a domain is a unique factorization domain it suffices to prove Euclid's lemma and the ascending chain condition on principal ideals (ACCP)
3. If $a : b = c : d$, then $ad = bc$; and conversely. ^[13]
4. If $a : b = c : d$, and a , b are the least numbers among those that have the same ratio, then $a = na$, $d = nb$, where n is some integer. ^[14]
5. If $a : b = c : d$, and a , b are prime to one another, then a , b are the least numbers among those that have the same ratio. ^[15]
6. If a is prime and does not measure b , then a , b are prime to one another ^[16]
7. If c , a prime number, measure ab , c measures either a or b . ^[17]

Citations

1. [Bajnok 2013](#), Theorem 14.5
2. [Joyner, Kreminski & Turisco 2004](#), Proposition 1.5.8, p. 25
3. [Martin 2012](#), p. 125
4. [Gauss & Clarke 2001](#), p. 14
5. [Hardy, Wright & Wiles 2008](#), Theorem 3
6. [Ireland & Rosen 2010](#), Proposition 1.1.1
7. [Landau & Goodman 1999](#), Theorem 15
8. [Riesel 1994](#), Theorem A2.1
9. [Euclid & Vitrac 1994](#), pp. 338–339
10. [Gauss & Clarke 2001](#), Article 19

11. [Weisstein, Eric W. "Euclid's Lemma" \(http://mathworld.wolfram.com/EuclidsLemma.html\)](http://mathworld.wolfram.com/EuclidsLemma.html) *MathWorld*.
12. [Hardy, Wright & Wiles 2008](#) §2.10
13. [Euclid & Heath 1956](#) p. 319
14. [Euclid & Heath 1956](#) p. 321
15. [Euclid & Heath 1956](#) p. 323
16. [Euclid & Heath 1956](#) p. 331
17. [Euclid & Heath 1956](#) p. 332
18. [Euclid & Heath 1956](#) pp. 331–332

References

- [Bajnok, Béla \(2013\), *An Invitation to Abstract Mathematics* Undergraduate Texts in Mathematics Springer, ISBN 978-1-4614-6636-9](#)
- [Euclid; Heath, Thomas Little \(translator into English\) \(1956\), *The Thirteen Books of the Elements* Vol. 2 \(Books III-IX\), Dover Publications, ISBN 978-0-486-60089-5 vol. 2](#)
- [Euclid; Vitrac, Bernard \(translator into French\) \(1999\), *Les Éléments, traduction, commentaires et notes* \(in French\), 2, pp. 338–339, ISBN 2-13-045568-9](#)
- [Gauss, Carl Friedrich; Clarke, Arthur A. \(translator into English\) \(2001\) *Disquisitiones Arithmeticae* \(Second, corrected ed.\), New Haven, CT Yale University Press, ISBN 978-0-300-09473-2](#)
- [Gauss, Carl Friedrich; Maser, H. \(translator into German\) \(1981\), *Untersuchungen über höhere Arithmetik \(Disquisitiones Arithmeticae & other papers on number theory\)* \(Second ed.\), New York: Chelsea, ISBN 978-0-8284-0191-3](#)
- [Hardy, G. H.; Wright, E. M.; Wiles, A. J. \(2008-09-15\), *An Introduction to the Theory of Numbers* \(6th ed.\), Oxford: Oxford University Press ISBN 978-0-19-921986-5](#)
- [Ireland, Kenneth; Rosen, Michael \(2010\) *A Classical Introduction to Modern Number Theory* \(Second ed.\), New York: Springer, ISBN 978-1-4419-3094-1](#)
- [Joyner, David; Kreminski, Richard; Trisco, Joann \(2004\), *Applied Abstract Algebra*, JHU Press, ISBN 978-0-8018-7822-0.](#)
- [Landau, Edmund; Goodman, J. E. \(translator into English\) \(1999\) *Elementary Number Theory* \(2nd ed.\), Providence, Rhode Island: American Mathematical Society ISBN 978-0-821-82004-9](#)
- [Martin, G. E. \(2012\), *The Foundations of Geometry and the Non-Euclidean Plane* Undergraduate Texts in Mathematics, Springer ISBN 978-1-4612-5725-7.](#)
- [Riesel, Hans \(1994\), *Prime Numbers and Computer Methods for Factorization* \(2nd ed.\), Boston: Birkhäuser ISBN 978-0-8176-3743-9](#)

External links

- [Weisstein, Eric W. "Euclid's Lemma". *MathWorld*.](#)

Retrieved from 'https://en.wikipedia.org/w/index.php?title=Euclid%27s_lemma&oldid=826518218

This page was last edited on 19 February 2018, at 16:07.

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.