Bézout's identity

Bézout's identity (also called **Bézout's lemma**) is a theorem in elementary number theory: let a and b be nonzero integers and let d be their greatest common divisor. Then there exist integers x and y such that

$$ax + by = d.$$

In addition,

- the greatest common divisor d is the smallest positive integer that can be written as $ax + by$
- every integer of the form $ax + by$ is a multiple of the greatest common divisor d.

The integers x and y are called **Bézout coefficients** for (a, b); they are not unique. A pair of Bézout coefficients can be computed by the extended Euclidean algorithm. If both a and b are nonzero, the extended Euclidean algorithm produces one of the two pairs such that $|x| \leq \left|\frac{b}{d}\right|$ and $|y| \leq \left|\frac{a}{d}\right|$ (equality may occur only if one of a and b is a multiple of the other).

Many theorems of elementary theory of numbers, such as Euclid's lemma or Chinese remainder theorem, result from Bézout's identity.

A Bézout domain is an integral domain in which Bézout's identity holds. In particular, Bézout's identity holds in principal ideal domains. Every theorem that results from Bézout's identity is thus true in all these domains.

1 Structure of solutions

When one pair of Bézout coefficients (x, y) has been computed (e.g., using extended Euclidean algorithm), all pairs can be represented in the form

$$\left(x + k\frac{b}{\gcd(a,b)},\ y - k\frac{a}{\gcd(a,b)}\right),$$

where k is an arbitrary integer and the fractions simplify to integers.

Among these pairs of Bézout coefficients, exactly two of them satisfy

$$|x| \leq \left|\frac{b}{\gcd(a,b)}\right| \quad \text{and} \quad |y| \leq \left|\frac{a}{\gcd(a,b)}\right|,$$

and equality may occur only if one of a and b divides the other. This relies on a property of Euclidean division: given two integers c and d, if d does not divide c, there is exactly one pair (q,r) such that $c = dq + r$ and $0 < r < |d|$, and another one such that $c = dq + r$ and $0 < -r < |d|$. The two pairs of small Bézout's coefficients are obtained by choosing k in the above formula for getting either remainder of the division of x by $b/\gcd(a,b)$.

The Extended Euclidean algorithm always produces one of these two minimal pairs.

1.1 Example

Let $a = 12$ and $b = 42$, $\gcd(12, 42) = 6$. Then we have the following Bézout's identities, with the Bézout coefficients written in red for the minimal pairs and in blue for the other ones.

$$\begin{aligned}
&\vdots \\
12 \times -10 \ &+ \ 42 \times 3 \ &= 6 \\
12 \times -3 \ &+ \ 42 \times 1 \ &= 6 \\
12 \times 4 \ &+ \ 42 \times -1 \ &= 6 \\
12 \times 11 \ &+ \ 42 \times -3 \ &= 6 \\
12 \times 18 \ &+ \ 42 \times -5 \ &= 6 \\
&\vdots
\end{aligned}$$

2 Proof

(proof adapted from 'proofwiki.org'[1])

Bézout's lemma is a consequence of the defining property of Euclidean division, namely: that dividing a positive integer p by a positive integer q yields a remainder greater than or equal to zero and strictly less than q .

i.e. $p = nq + r, \quad 0 \leq r < q$

To begin the proof of Bézout's lemma, let d be the smallest positive integer of the form $ax + by$. Specifically,

let $d = as + bt$

let $n = ax + by, \quad n > d$

If n is not divisible by d, then according to Euclidean division,

$$
\begin{aligned}
& & r &= n - qd \\
n = qd + r, \quad 0 < r < d & & &= ax + by - q(as + bt) \\
& & &= a(x - qs) + b(y - qt)
\end{aligned}
$$

which of course is of the form $ax + by$

But $r < d$ which violates the original premise that d is the smallest number in that form, *therefore* $r = 0$ and

n **is divisible by** d

Since n can be any number of the form $ax + by$ lets look at the following specific examples:

$n = 1 \cdot a + 0 \cdot b = a$

$n = 0 \cdot a + 1 \cdot b = b$

Therefore, d is a common divisor to both a and b

If there exists another common divisor (c) of a and b , then it also divides d

$a = pc$

$b = qc$

$d = as + bt$

$= (pc)s + (qc)t$

$= c(ps + qt)$

If c divides d, then $c \leq d$

Therefore, (finally) d is the greatest common divisor.

This proof does not provide a method for computing Bézout's coefficients. However, Bézout's lemma is also a corollary of the proof of the Extended Euclidean algorithm and this algorithm does provide an efficient method of computing these coefficients. This algorithm and the associated proof may also be extended to any Euclidean domain.

3 Generalizations

3.1 For three or more integers

Bézout's identity can be extended to more than two integers: if

$$\gcd(a_1, a_2, \ldots, a_n) = d$$

then there are integers $x_1, x_2, \ldots, x_n$ such that

$$d = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

has the following properties:

- d is the smallest positive integer of this form
- every number of this form is a multiple of d

3.2 For polynomials

Main article: Polynomial greatest common divisor § Bézout's identity and extended GCD algorithm

Bézout's identity works for univariate polynomials over a field exactly in the same ways as for integers. In particular the Bézout's coefficients and the greatest common divisor may be computed with the Extended Euclidean algorithm.

As the common roots of two polynomials are the roots of their greatest common divisor, Bézout's identity and fundamental theorem of algebra imply the following result:

> For univariate polynomials f and g with coefficients in a field, there exist polynomials a and b such that $af + bg = 1$ if and only if f and g have no common root in any algebraically closed field (commonly the field of complex numbers).

The generalization of this result to any number of polynomials and indeterminates is Hilbert's Nullstellensatz.

3.3 For principal ideal domains

As noted in the introduction, Bézout's identity works not only in the ring of integers, but also in any other principal ideal domain (PID). That is, if R is a PID, and a and b are elements of R, and d is a greatest common divisor of a and b, then there are elements x and y in R such that $ax + by = d$. The reason: the ideal $Ra+Rb$ is principal and indeed is equal to Rd.

An integral domain in which Bézout's identity holds is called a Bézout domain.

4 History

French mathematician Étienne Bézout (1730–1783) proved this identity for polynomials.[2] However, this statement for integers can be found already in the work of another French mathematician, Claude Gaspard Bachet de Méziriac (1581–1638).[3][4][5]

5 See also

- AF+BG theorem, an analogue of Bézout's identity for homogeneous polynomials in three indeterminates
- Fundamental theorem of arithmetic
- Euclid's lemma

6 Notes

[1] https://proofwiki.org/wiki/B%C3%A9zout%27s_Lemma

[2] Bézout, É. (1779). *Théorie générale des équations algébriques*. Paris, France: Ph.-D. Pierres.

[3] Tignol, Jean-Pierre (2001). *Galois' Theory of Algebraic Equations*. Singapore: World Scientific. ISBN 981-02-4541-6.

[4] Claude Gaspard Bachet (sieur de Méziriac) (1624). *Problèmes plaisants & délectables qui se font par les nombres* (2nd ed.). Lyons, France: Pierre Rigaud & Associates. pp. 18–33. On these pages, Bachet proves (without equations) "Proposition XVIII. Deux nombres premiers entre eux estant donnez, treuver le moindre multiple de chascun d'iceux, surpassant de l'unité un multiple de l'autre." (Given two numbers [which are] relatively prime, find the lowest multiple of each of them [such that] one multiple exceeds the other by unity (1).) This problem (namely, ax - by = 1) is a special case of Bézout's equation and was used by Bachet to solve the problems appearing on pages 199 ff.

[5] See also: Maarten Bullynck (February 2009). "Modular arithmetic before C.F. Gauss: Systematizations and discussions on remainder problems in 18th-century Germany" (PDF). *Historia Mathematica*. **36** (1): 48–72. doi:10.1016/j.hm.2008.08.009.

7 External links

- Online calculator for Bézout's identity.
- Weisstein, Eric W. "Bézout's Identity". *MathWorld*.

8 Text and image sources, contributors, and licenses

8.1 Text

- **Bézout's identity** *Source:* https://en.wikipedia.org/wiki/B%C3%A9zout'{}s_identity?oldid=757381267 *Contributors:* AxelBoldt, Bryan Derksen, Zundark, Heron, Nd12345, Michael Hardy, Oliver Pereira, Charles Matthews, Timwi, Jitse Niesen, Robbot, Gandalf61, Math-Martin, Merovingian, Giftlite, Wmahan, Azuredu, Xmlizer, Blokhead, Rich Farmbrough, Guanabot, Bender235, Spoon!, Keenan Pepper, Burn, Gene Nygaard, Oleg Alexandrov, JanKG, Shreevatsa, David Haslam, Ohanian, FlaBot, VKokielov, Maxal, Bgwhite, Bota47, Kompik, Anghammarad, Kier07, Zvika, SmackBot, Grover cleveland, Michael Ross, Sadeq, CmdrObot, Philiprbrenan, Banedon, Myasuda, Ntsimp, Hanche, Thijs!bot, Konradek, JAnDbot, Stdazi, David Eppstein, JadeNB, CarlFriedrich~enwiki, Fruits Monster, Sanderling, Ilya Voyager, TXiKiBoT, A4bot, Wtt, AlleborgoBot, Caarecengi, SieBot, Cwkmail, Oxymoron83, Stfg, Tuntable, Justin W Smith, BOTarate, Marc van Leeuwen, Virginia-American, MystBot, Legobot, Rick Ballan, LGB, Calle, AnomieBOT, Materialscientist, Omnipaedista, FrescoBot, RedAcer, DixonDBot, RjwilmsiBot, Dupuju, Garfieldnate, Dcirovic, ZéroBot, Peterepeat11, D.Lazard, CocuBot, Kerkeslager, יהודה שמחה ולדמן, Swunggyro, TheKing44, William2001, Stephenamills, Ramanujan srinivasa, Differintegral, Loraof, Ankiitt, Bender the Bot, Sandybultena, CryptoDiophantus and Anonymous: 49

8.2 Images

8.3 Content license