DIVISIBILITY WITHOUT BEZOUT'S IDENTITY

KEITH CONRAD

The key result used in proofs of most basic theorems about divisibility and greatest common divisors is Bezout's identity: if a and b are in $\mathbf{Z}^+$, then

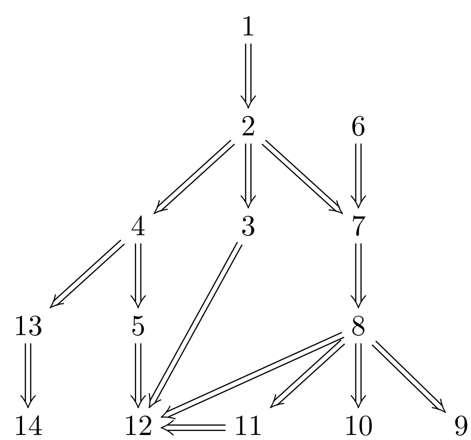
$$(a, b) = ax + by$$

for some integers x and y. Consequences of Bezout's identity include

- $d \mid a, d \mid b \Rightarrow d \mid (a, b)$,
- $a \mid bc, (a, b) = 1 \Rightarrow a \mid c$,
- $(a, b) = 1, (a, c) = 1 \Rightarrow (a, bc) = 1$.

Here we will show a way to derive these *without* Bezout's identity (Theorem 9 and Corollaries 4 and 5 below). The main tool will be the least common multiple $[a, b]$, which often plays a minimal (if not nonexistent) role in treatments of divisibility. Our arguments are adapted from or inspired by [1, pp. 14, 42].

The diagram below indicates the logical dependencies of the results we will show.



All variables are in $\mathbf{Z}^+$ unless said otherwise.

Theorem 1. *If $a \mid m$ and $b \mid m$ then $[a, b] \mid m$.*

Proof. Write

$$m = [a, b]q + r, \text{ such that } 0 \leq r < [a, b].$$

Since m and $[a, b]$ are both multiples of a, also $r = m - [a, b]q$ is a multiple of a. Similarly, r is a multiple of b. So r is a common multiple of $[a, b]$. If $r > 0$, then $r \geq [a, b]$ by the definition of the least common multiple. But $r < [a, b]$, so we must have $r = 0$, so $[a, b] \mid m$. $\square$

This is the last time you will see addition being used to prove results about divisibility (until the very end when we come back to Bezout's identity). From now on, proofs are purely multiplicative.

Theorem 2. *For all a and b, $(a,b) = 1 \Longleftrightarrow [a,b] = ab$.*

Proof. ($\Rightarrow$) By Theorem 1, $[a,b] \mid ab$ since ab is a common multiple of a and b. To get the reverse inclusion, write $ab = [a,b]c$. We want to show $c = 1$.

Let $[a,b] = ak$ and $[a,b] = b\ell$. Then $ab = (ak)c$ and $ab = (b\ell)c$, so

$$b = kc, \quad a = \ell c.$$

Thus c is a common divisor of a and b. Since a and b are relatively prime, $c = 1$.

($\Leftarrow$) Set $d = (a,b)$. We want to show $d = 1$ if $[a,b] = ab$. Write $a = da'$ and $b = db'$. Then $da'b'$ is a common multiple of a and b:

$$da'b' = ab' = ba'.$$

Thus $[a,b] \leq da'b'$, from the definition of the least common multiple, so $ab \leq da'b'$ because we're assuming $[a,b] = ab$. Since $ab = (da')(db') = d^2a'b'$, we get

$$d^2a'b' \leq da'b'.$$

Cancelling common terms, $d \leq 1$, so $d = 1$. □

We will generally use only the direction ($\Rightarrow$) of Theorem 2.

Corollary 3. *If $a \mid c$, $b \mid c$, and $(a,b) = 1$ then $ab \mid c$.*

Proof. By Theorem 1, $[a,b] \mid c$. By Theorem 2, $[a,b] = ab$, so $ab \mid c$. □

Corollary 4. *If $a \mid bc$ and $(a,b) = 1$ then $a \mid c$.*

Proof. Since $a \mid bc$ (by hypothesis) and $b \mid bc$, from Theorem 1 we get $[a,b] \mid bc$. Then $ab \mid bc$ by Theorem 2, so $a \mid c$. □

Corollary 4 implies that for any prime p, if $p \mid mn$ then $p \mid m$ or $p \mid n$, and that is the key result behind the uniqueness of prime factorization in $\mathbf{Z}^+$.

Corollary 5. *If $(a,b) = 1$ and $(a,c) = 1$ then $(a,bc) = 1$.*

Proof. We will show $[a,bc] = abc$. Then the direction ($\Leftarrow$) of Theorem 2 implies $(a,bc) = 1$.

Write $[a,bc] = bck$. Then $a \mid bck$ (since $[a,bc]$ is a multiple of a) and $(a,b) = 1$, so $a \mid ck$ by Corollary 4. From $a \mid ck$ and $(a,c) = 1$, we get $a \mid k$ by Corollary 4. Hence $a \leq k$, so

$$[a,bc] = bck \geq bca = abc. \tag{1}$$

Since abc is a common multiple of a and bc, (1) tells us $abc = [a,bc]$, so we're done by Theorem 2. □

Theorem 6. *For all a, b, and c, $[ca,cb] = c[a,b]$.*

Proof. This result will not rely on anything done above.

Certainly $c[a,b]$ is a common multiple of ca and cb. Now let m be any common multiple of ca and cb. We want to show $m \geq c[a,b]$, which would make $c[a,b]$ the least common multiple of ca and cb.

From either $ca \mid m$ or $cb \mid m$ we have $c \mid m$. Write $m = cm'$. Then $ca \mid cm'$, so $a \mid m'$, and $cb \mid cm'$, so $b \mid m'$. Thus m' is a common multiple of a and b, so $[a,b] \leq m'$, so $c[a,b] \leq cm' = m$. □

Theorem 7. *For all a and b, $ab = [a,b](a,b)$.*

Proof. Let $d = (a, b)$ and write $a = da'$ and $b = db'$. Then $(a', b') = 1$ (if a' and b' had a common divisor greater than 1 then we could get a common divisor of a and b larger than d), so

$$\begin{aligned} [a, b] &= [da', db'] \\ &= d[a', b'] \text{ by Theorem 6} \\ &= da'b' \text{ by Theorem 2.} \end{aligned}$$

Therefore $[a, b](a, b) = (da'b')d = da' \cdot db' = ab$. □

Corollary 8. *For all a, b, and c, $(ca, cb) = c(a, b)$.*

Proof. By Theorem 7,

$$[ca, cb](ca, cb) = ca \cdot cb.$$

By Theorem 6, this can be rewritten as

$$c[a, b](ca, cb) = c^2ab,$$

so

$$[a, b](ca, cb) = cab.$$

By Theorem 7 again, $cab = c[a, b](a, b)$, and substituting this into the above equation gives us

$$[a, b](ca, cb) = c[a, b](a, b).$$

Now cancel $[a, b]$ on both sides. □

Theorem 9. *If $d \mid a$ and $d \mid b$ then $d \mid (a, b)$.*

Proof. Write $a = dm$ and $b = dn$. Then $(a, b) = (dm, dn) = d(m, n)$ by Corollary 8, so $d \mid (a, b)$. □

In Theorem 9, that d is a common divisor of a and b certainly forces $d \le (a, b)$ by the definition of the greatest common divisor. In order to refine this inequality to the divisibility relation $d \mid (a, b)$, you might consider writing $(a, b) = dq + r$ with $0 \le r < d$ and trying to show $r = 0$. Unfortunately, d doesn't have any convenient property that makes it easy to show $r = 0$.

Corollary 10. *If $a \mid bc$, $a \mid bd$, and $(c, d) = 1$ then $a \mid b$.*

Proof. Write $bc = ak$ and $bd = a\ell$. Then $(bc, bd) = (ak, a\ell)$, so by Corollary 8 we get

$$b(c, d) = a(k, \ell).$$

Therefore $b = a(k, \ell)$ since $(c, d) = 1$, so $a \mid b$. □

Lemma 11. *If $d = (a, b)$ and we write $a = da'$ and $b = db'$, then $(a', b') = 1$.*

Proof. Using Corollary 8, $(a, b) = (da', db') = d(a', b')$. Therefore $(a, b) = (a, b)(a', b')$, so $(a', b') = 1$. □

Theorem 12. *If $(b, c) = 1$ then for all a, $(a, bc) = (a, b)(a, c)$.*

Proof. Since $(a, b) \mid b$ and $(a, c) \mid c$, we can write

$$b = (a, b)b', \qquad c = (a, c)c'.$$

The numbers (a, b) and (a, c) are both factors of a, and they are relatively prime since they are respective factors of b and c, which are relatively prime. Therefore Corollary 3 tells us $(a, b)(a, c) \mid a$. Write

$$a = (a, b)(a, c)a'.$$

Since $(a, b)(a, c)$ is a common factor of a and $bc = (a, b)(a, c)b'c'$, Corollary 8 tells us

$$(a, bc) = ((a, b)(a, c)a', (a, b)b'(a, c)c') = (a, b)(a, c)(a', b'c').$$

It remains to show $(a', b'c') = 1$.

From $a = (a, b)((a, c)a')$ and $b = (a, b)b'$, Lemma 11 tells us $((a, c)a', b') = 1$, so $(a', b') = 1$. Similarly, $(a', c') = 1$. Then Corollary 5 implies $(a', b'c') = 1$. $\square$

Finally we derive the result we have avoided using all along, Bezout's identity. It will follow from Corollary 4 (whose usual proof involves Bezout's identity).

Theorem 13. *If $(a, b) = 1$ then $ax + by = 1$ for some x and y in $\mathbf{Z}$.*

Proof. Consider the function $f \colon \mathbf{Z}/(a) \to \mathbf{Z}/(a)$ given by $f(y) = by \bmod a$. This is one-to-one: if $f(y_1) \equiv f(y_2) \bmod a$ then $by_1 \equiv by_2 \bmod a$, so $a \mid b(y_1 - y_2)$ in $\mathbf{Z}$. Therefore $a \mid (y_1 - y_2)$ in $\mathbf{Z}$ by Corollary 4, so $y_1 \equiv y_2 \bmod a$.

Since f is a one-to-one function of $\mathbf{Z}/(a)$ with itself, and $\mathbf{Z}/(a)$ is finite, f is onto as well. In particular, 1 is a value: $1 \equiv by \bmod a$ for some $y \in \mathbf{Z}$, so $1 = by + ax$ for some x and y in $\mathbf{Z}$. $\square$

Corollary 14. *For all a and b, $(a, b) = ax + by$ for some x and y in $\mathbf{Z}$.*

Proof. Let $d = (a, b)$. Write $a = da'$ and $b = db'$, so $(a', b') = 1$. Then by Theorem 13, $a'x + b'y = 1$ for some x and y in $\mathbf{Z}$. Multiply through this equation by d to get $da'x + db'y = d$, so $ax + by = d$. $\square$

References

[1] N. N. Vorob'ev, "Criteria for Divisibility," Univ. of Chicago Press, Chicago, 1980.