Euclid's Lemma Revisited

Marc Bezem

Department of Informatics, University of Bergen
P.O. Box 7803, N-5020 Bergen, Norway
bezem@ii.uib.no

In [2], Peter Walker rightly underlines the importance of a self-contained proof of Euclid's lemma [1], which states that a prime divides at least one of two integers when dividing their product. Walker proposes an inductive proof of Euclid's lemma, not using Bezout's identity. Walker's proof is interesting since it uses induction on the prime. His proof actually contains several other inductions, namely the induction behind division with remainder, behind existence of factorisation and behind cancellation of an unknown number of common factors.

Here we take a further step by giving an inductive argument that bypasses all of the above inductions and auxiliary results. Our proof only uses elementary arithmetic and logic, in addition to one main induction in the natural numbers, based on a seemingly original induction value. The base case holds vacuously.

Let $p \mid ab$ with p a prime and a, b positive integers. We will call the value of the expression $pab + \min(a, b)$ the *induction value* of $p \mid ab$, or i-value for short. We will prove by well-founded induction on the i-value that $p \mid ab$ implies $p \mid a$ or $p \mid b$. Let $p \mid ab$ with p prime and assume Euclid's lemma holds for all $p' \mid a'b'$, p' prime, with i-value smaller than that of $p \mid ab$. Without loss of generality we can assume that $1 < a \leq b$, as both Euclid's lemma and the i-value are symmetric in a and b. If $a > p$ we are done since $p \mid (a - p)b$ has smaller i-value than $p \mid ab$, and $p \mid a - p$ implies $p \mid a$. The case $p = a$ is trivial, so assume $1 < a \leq p - 1$. We distinguish two cases: a is composite and a is prime. If a is composite, that is, $a = a_1 a_2$ with $1 < a_1, a_2 < a$, then $p \mid a_1(a_2 b)$ has a smaller i-value than $p \mid ab$, since $\min(a_1, a_2 b) < \min(a, b)$. If $p \mid a_1$, then $p \mid a$ and we are done, so assume $p \mid a_2 b$. In turn, $p \mid a_2 b$ has a smaller i-value than $p \mid ab$. In both cases, $p \mid a_2$ (which implies $p \mid a$) or $p \mid b$, we are done. It remains to treat the case that a is prime. Let q be such that $pq = ab$ and assume $a \leq p - 1$ is prime. Then we have $a \mid pq$, with i-value $apq + \min(p, q) \leq (p-1)pq + \min(p, q) = ppq - pq + \min(p, q) \leq pab < pab + \min(a, b)$. It follows that $a \mid q$ since $a \mid p$ is impossible. Let q' be such that $q = aq'$, then we have $paq' = pq = ab$, so $pq' = b$, which means $p \mid b$.

References

[1] Euklid, *The Elements*. Book VII, Proposition 30, `http://aleph0.clarku.edu/~djoyce/java/elements/bookVII/propVII30.html`

[2] Peter Walker, A Lemma on Divisibility. *American Mathematical Monthly* **115**(4):338.