Bezout's Identity

Theorem 1 (Bezout's Identity)**.** *If a and b are integers, then there exist integers u and v such that* $\mathsf{gcd}(a, b) = ua + vb$

Proof. We start with the case $b \geq 0$, proceeding by strong induction.

- **Base Case** ($b = 0$): Note that $\mathsf{gcd}(a, 0) = a = a \cdot 1 + 0 \cdot 0$ as needed. That is, the result holds with $u = 1$ and $v = 0$.
- **Base Case** ($b = 1$): Note that $\mathsf{gcd}(a, 1) = 1 = a \cdot 0 + 1 \cdot 1$ as needed. That is, the result holds with $u = 0$ and $v = 1$.
- **Inductive Step**: Suppose the result holds for all integers b' with $0 \leq b' < b$, where $b > 1$. That is, for all such b' and all integers a there exist integers u and v such that $\mathsf{gcd}(a, b') = au + b'v$. Now consider b. By the division algorithm we have integers q and r such that $a = qb + r$ and $0 \leq r < b$. We have two possibilities to consider.
  - If $r = 0$, then in fact $b|a$, since $a = qb$. So $\mathsf{gcd}(a, b) = b = a \cdot 0 + q \cdot b$. That is, the result holds with $u = 0$ and $v = 1$.
  - If $r > 0$, then by the induction hypothesis there exist integers u' and v' such that $\mathsf{gcd}(b, r) = bu' + rv'$. By the euclidean algorithm, we have

$$\begin{aligned} \mathsf{gcd}(a, b) &= \mathsf{gcd}(b, r) \\ &= bu' + rv' \\ &= bu' + (a - qb)v' \\ &= av' + b(u' - qv'). \end{aligned}$$

    That is, the result holds with $u = v'$ and $v = u' - qv'$.

By Strong Induction, for all $b \geq 0$ and all integers a there exist integers u and v such that $\mathsf{gcd}(a, b) = au + bv$.

Now suppose $b < 0$, so that $-b > 0$. By the previous discussion, there exist integers u' and v' such that $\mathsf{gcd}(a, -b) = au' + (-b)v'$. Now

$$\mathsf{gcd}(a, b) = \mathsf{gcd}(a, -b) = au' + (-b)v' = au' + b(-v').$$

That is, the result holds with $u = u'$ and $v = -v'$. $\square$

Similar to the Euclidean Algorithm, this proof of Bezout's Identity provides us with a strategy for actually finding the coefficients u and v recursively.

Definition 1 (Relatively Prime)**.** *We say that integers a and b are* relatively prime *if* $\mathsf{gcd}(a, b) = 1$.

Theorem 2 (Euclid's Lemma)**.** *If a and b are relatively prime integers and c an integer such that $a|bc$, then $a|c$.*

Proof. By Bezout's Identity, we have $1 = au + bv$ for some integers u and v; so $c = auc + bvc$. Since $a|bc$, we have $bc = at$ for some integer t. Thus

$$c = auc + bvc = auc + atv = a(uc + tv),$$

and so $a|c$ as claimed. $\square$