Key Lemma

Definition: Given $x, y \in \mathbb{Z}$, define the span of x and y to be $\text{span}\{x,y\} = \{ax+by : a,b \in \mathbb{Z}\}$

Key Lemma: $\forall x, y, c \in \mathbb{Z}$,

1) $\text{Span}\{x,y\} = \text{Span}\{x-cy, y\}$

2) $\text{Div}(x) \cap \text{Div}(y) = \text{Div}(x-cy) \cap \text{Div}(y)$

Proof:

1) If $z = ax+by$ then $z = a(x-cy) + (b+ac)y$.

   If $z = a(x-cy)+by$ then $z = ax + (b-ac)y$.

2) If $d \in \text{Div}(x) \cap \text{Div}(y)$ then $\exists q_1, q_2 \in \mathbb{Z}\ (x = q_1 d \wedge y = q_2 d)$

   $x - cy = q_1 d - c q_2 d = (q_1 - c q_2) d$ so $d \in \text{Div}(x-cy)$

   If $d \in \text{Div}(x-cy) \cap \text{Div}(y)$ then $\exists q_1, q_2 \in \mathbb{Z}\ (x-cy = q_1 d \wedge y = q_2 d)$

   $x = (x-cy) + cy = q_1 d + c q_2 d = (q_1 + c q_2) d$ so $d \in \text{Div}(x)$.

Explanation for Euclid's Algorithm

Recall Euclid's algorithm for finding $\gcd(x,y)$:

1. Start with $a=\max\{|x|,|y|\}$ and $b=\min\{|x|,|y|\}$.
2. While $b>0$:
   1. Divide a by b and let r be the remainder.
   2. Set $a=b$ and $b=r$.
3. When $b=0$, output a.

Q: Why does Euclid's algorithm succeed?

Idea: By the key lemma, $\mathrm{span}\{a,b\}$ and $\mathrm{Div}(a)\cap\mathrm{Div}(b)$ are <u>invariant</u> as the algorithm progresses.

Thus, letting a be the output of Euclid's algorithm,

1) $\mathrm{Div}(x)\cap\mathrm{Div}(y)=\mathrm{Div}(a)\cap\mathrm{Div}(0)=\mathrm{Div}(a)$ so $\gcd(x,y)=a$.

2) $\mathrm{span}\{x,y\}=\mathrm{span}\{a,0\}$ so $a=\gcd(x,y)\in\mathrm{span}\{x,y\}$

Corollaries:

1) $\mathrm{Div}(x)\cap\mathrm{Div}(y)=\mathrm{Div}(\gcd(x,y))$

2) Bézout's Identity: $\gcd(x,y)\in\mathrm{span}\{x,y\}$, i.e. $\exists a,b\in\mathbb{Z}\ (\gcd(x,y)=ax+by)$

Note: These corollaries can be proved more rigorously by induction.