**Prop. 2.29** Let $a, b \in \mathbb{Z}$.

Then, $\gcd(a, b) = d$ iff

(i) $d \geq 0$

(ii) $d|a$ and $d|b$

(iii) any common divisor $c$ of $a, b$ also divides $d$.

**Proof:**

[$\Rightarrow$]

If $\gcd(a, b) = d$

then by definition (i) $d \geq 0$ and (ii) $d|a$ and $d|b$

To prove (iii), use EEA, so that $\exists x, y, \in \mathbb{Z}$ s.t. $d = ax + by$.

If $c|a$ and $c|b$, then, by Prop. 2.11(ii), $c|ax + by$ which is $d$ thus (iii) above holds.

[$\Leftarrow$]

If (i)-(iii) holds, consider $d = 0$ and $d \neq 0$ cases separately.

If $d = 0$, then, by (ii) above, $a = b = 0$ thus $\gcd(a, b) = d$ by definition.

If $d \neq 0$, then, (ii) says that $d$ is a common divisor of $a, b$.

For any common divisor $c$ of $a, b$, <u>due to (iii) above and $d \neq 0$ and Prop. 2.11(iv)</u>, we have $c \leq |c| \leq |d|$.

So $d$ is the largest common divisor and so $\gcd(a, b) = d$.