

Ex. We compute $\text{gcd}(2024, 748)$ using repeated division with remainder:

$$2024 = 748 \cdot 2 + 528$$

$$748 = 528 \cdot 1 + 220$$

$$528 = 220 \cdot 2 + 88$$

$$220 = 88 \cdot 2 + 44 \leftarrow \text{gcd} = 44$$

$$88 = 44 \cdot 2 + 0$$

Exercise: Compute the gcd of $\overset{a=}{1278}, \overset{b=}{234}$:

$$1278 = 234 \cdot 5 + 108$$

$$234 = 108 \cdot 2 + 18 \leftarrow \text{gcd} = 18.$$

$$108 = 18 \cdot 6 + 0$$

$$a = 5 \cdot b + 108 \Leftrightarrow 108 = a - 5b$$

$$b = 234 = (a - 5 \cdot b) \cdot 2 + 18$$

$$b = 2a - 10b + 18 \Leftrightarrow 18 = -2a + 11b$$

By ~~re-substituting~~ substitution, we get a linear combination of a and b which is equal to the gcd of a and b . This leads to the Extended Euclidean Algorithm (EEA).

Theorem 2.4 Let a, b be positive integers. Then the equation

$$a \cdot u + b \cdot v = \text{gcd}(a, b)$$

always has solutions in integers u and v .