



Exercise 1. Let $a, b, c, x, y \in \mathbb{Z}$. Prove that if $c|a$ and $c|b$, then $c|ax + by$.

Exercise 2. Let $a, b \in \mathbb{Z}$, not both zero. The *greatest common divisor* of a and b , denoted $\gcd(a, b)$, is the largest $c \in \mathbb{N}$ so that $c|a$ and $c|b$.

- a. Explain why $\gcd(a, b)$ exists.
- b. Prove that $\gcd(a, b) = \gcd(a, a + b) = \gcd(a + b, b)$. [*Suggestion:* Show that the common (positive) divisors of a and b are the same as those of a and $a + b$.]

Exercise 3. Prove that the equation $x^2 = 4y + 2$ has no integer solutions.

Exercise 4. Let $a \in \mathbb{N}$, $a > 1$. Suppose that a has the following property: if $b, c \in \mathbb{N}$ and $a|bc$, then $a|b$ or $a|c$. Prove that a is prime.¹

¹The converse is also true, although it's substantially harder to prove.