
Definition:

Given two integers b and c at least one of which is not 0,
we say a is the **greatest common divisor** of b and c
if a is the greatest among all common divisors of b and c.

The greatest common divisor of b and c is denoted by $\gcd(b, c)$ or simply (b, c).

- Why do we require that "at least one of b and c be nonzero"?
- Could we make sense of $\gcd(0, 0)$?

EX. Find

1. $\gcd(24, 36)$
2. $\gcd(22, 35)$

Theorem 1. For any integers a and b, the followng properties hold:

1. $\gcd(a, b) = \gcd(b, a)$,
2. $\gcd(a, b) \geq 1$,
3. $\gcd(a, b) = \gcd(|a|, |b|)$,
4. $\gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$,

Theorem. If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for all integers m and n.

Use the previous theorem to prove the following :

5. $\gcd(a, b) = \gcd(a + nb, b)$, $\forall n \in \mathbb{Z}$.

Use the Fundamental Theorem of Algebra to prove the following.

Theorem 2. For all $m, n \in \mathbb{Z}$, if $m^2 \mid n^2$, then $m \mid n$.

Note: Is it true that if $a \mid n^2$, then $a \mid n$, $\forall a, n \in \mathbb{Z}$?

Theorem 3. A natural number is divisible by 2 if and only if its last digit is divisible by 2.

Theorem 4. A natural number is divisible by 4 if and only if the number formed by its last two digits is divisible by 4. *(27.23 (ix-b))*

Carefully read the proof of the Division Algorithm (Division Lemma) - Chapter 28, pp 196-199 and be ready to discuss it next class. Briefly write down your answers for the following questions and turn them in with the previous questions.

1. What are the main stages in the proof?
2. What is the main idea in proving existence of q and r?
3. How are q and r defined?
4. How is uniqueness of q and r proved?
5. Why is there a need for a more general version of the Division Algorithm Theorem?
6. What is the statement of the more general Division Theorem?
7. What is the main idea in its proof?