Divisibility and Euclidean Algorithm

Let a and b be integers such that $b \neq 0$. The a is *divisible* by b, denoted $b \mid a$, if and only if there exists integer k such that $a = bk$. In this case, b *divides* a.

Example 4.0.6. The integer 24 is divisible by 4 since 24 can be written as 4(6).

Example 4.0.7. Let $a \in \mathbb{Z}$ such that $a \neq 0$. Then $a^2 \mid a^5$ since $a^5 = a^2(a^3)$.

Theorem 4.0.8. *Let $a, b \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$, then $a \mid (-b)$ and $(-a) \mid b$.*

Proof. Suppose that $a \mid b$. By definition, there is an integer k such than $b = ak$. Hence $b = a(-1)(-k)$. Dividing by side by -1 gives $-b = a(-k)$. Therefore $a \mid -b$.

Now suppose $a \mid b$. Then for some integer k it is the case that $b = ak$. Hence $b = (-a)(-k)$. Therefore $b \mid -a$. □

Theorem 4.0.9. *For every integer n, $3|(n^3 - n)$.*

First note that $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. Since $n-1$, n, and $n+1$ are consecutive integers 3 must divide one of them.

Proof. By the Division Algorithm, $n = 3q + r$ where $0 \leq r < 3$. Hence $r \in \{0, 1, 2\}$. If $r = 0$ then we are done. If $r = 1$ then $n - 1 = 3q$. This shows that $3 \mid n - 1$. Similarly if $r = 2$, then $n + 1 = 3q$ which shows that $3 \mid n + 1$. □

Problem 4.0.10. Suppose a, b, and c are integers such that $c \mid a$ and $c \mid b$. Show that $c \mid (ax + yb)$ for any integers x and y.

Let $a, b \in \mathbb{Z}$ with $b \neq 0$ The *greatest common divisor*, denoted by $\gcd(a, b)$, is the largest common divisor of a and b.

Problem 4.0.11. What is the greatest common divisor of 4 and 16?

Example 4.0.12. The greatest common divisor of 4 and 16 is 4, since $4 \mid 4$, $4 \mid 16$, and if $c \mid 4$ and $c \mid 16$ then $c \leq 4$. Hence $\gcd(4, 16) = 4$.

Problem 4.0.13. What is the greatest common divisor of 70 and 42?

Theorem 4.0.14. *Euclidean Algorithm Let a and b be natural numbers with $b < a$. To find the greatest common divisor of a and b, write*

$$a = q_1 b + r_1 \qquad \textit{with} \qquad 0 < r_1 < b$$

then $b = q_2 r_1 + r_2$ and repeat until $r_{k+1} = 0$. Then $r_k = \gcd(a, b)$.

Note that the Euclidean Algorithm uses the Division Algorithm.

Example 4.0.15. Find $\gcd(630, 196)$. Using the

$$\begin{aligned}
630 &= 3(196) + 42 \\
192 &= 4(42) + 28 \\
42 &= 1(28) + 14 \\
28 &= 2(14) + 0
\end{aligned}$$

Problem 4.0.16. Use the Euclidean Algorithm to find the greatest common divisor of 70 and 42.

If the greatest common divisor of a and b is 1, then a and b are *relatively prime*.