Divisibility and GCD

Definition 1 (Divides)**.** *Given integers a and b, we say that a* divides *b, written $a|b$, if there is an integer c such that $ac = b$. In this case we say that a is a* divisor *of b.*

Proposition 1.

- *$a|0$ for all integers a.*
- *$1|a$ for all integers a.*
- *$a|a$ for all integers a.*
- *If $a|b$, then $(-a)|b$ and $a|(-b)$.*
- *If $a|b$ and $b \neq 0$, then $0 < |a| \leq |b|$.*

Definition 2. *Let a and b be integers.*

- *We say that an integer c is a* common divisor *of a and b if $c|a$ and $c|b$.*
- *We say that an integer d is a* greatest common divisor *of a and b if d is a common divisor, and if c is another common divisor, then $c \leq d$.*

Proposition 2. *Any two integers (not both zero) have a unique greatest common divisor, which we denote $\mathsf{gcd}(a, b)$. We also define $\mathsf{gcd}(0, 0) = 0$ as a special case.*

Proposition 3.

- *$\mathsf{gcd}(a, b) = \mathsf{gcd}(b, a)$ for all integers a and b.*
- *$\mathsf{gcd}(a, a) = |a|$ for all integers a.*
- *If a and b are integers with $b|a$, then $\mathsf{gcd}(a, b) = |b|$.*
- *$\mathsf{gcd}(a, 1) = 1$ for all integers a.*
- *$\mathsf{gcd}(a, 0) = |a|$ for all integers a.*

Proposition 4 (Euclidean Algorithm)**.** *If a and b are integers with $b > 0$, and if $a = qb + r$ where $0 \leq r < b$, then $\mathsf{gcd}(a, b) = \mathsf{gcd}(b, r)$.*

Proof. Let $d = \mathsf{gcd}(a, b)$ and $e = \mathsf{gcd}(b, r)$. We need to show that $d = e$; to do this, we will show that $d \leq e$ and $e \leq d$.

- By definition we have $d|a$ and $d|b$; that is, $a = da'$ and $b = db'$ for some integers a' and b'. Now

  $$r = a - qb = da' - qdb' = d(a' - qb'),$$

  so that $d|r$. In particular, d is a common divisor of b and r, and so $d \leq e$.

- Similarly, we have $e|b$ and $e|r$, so that $e|a$, and thus $e \leq d$. $\square$

The Euclidean Algorithm gives us a way to explicitly compute the GCD of two integers *as long as* we can compute quotients and remainders as in the Division Algorithm; in fact, it is quite fast. Note that since r is strictly less than b, this recursion must eventually terminate with a statement of the form $\mathsf{gcd}(a, 0)$.