Some Baby Number Theory

* mainly divisibility-related

Notation

- $a|b$ $(a,b \in \mathbb{Z})$ means that "a" is a factor of "b" (mostly >0)
  - ie: $b = ak$ for some $k \in \mathbb{Z}$

Question: Given a & b, how do we test if $a|b$?

* in practice, given $a<b$, we can find a unique q & r such that: $b = qa + r$ & $0 \le r < a$
  - if $r=0$ then $a|b$
  - $\gcd(a,b) | r$

Definition

- Given $a,b \in \mathbb{Z}^+$, the greatest common divisor of a & b is $d = \gcd(a,b)$
  - where if $n|a$ & $n|b \Rightarrow n|d$
  - example: $\gcd(432, 278)$

$432 = 1 \cdot 278 + 154$

$\Rightarrow = \gcd(278, 154)$

$278 = 1(154) + 124$

$\Rightarrow = \gcd(154, 124)$

$154 = 1(124) + 30$

$\Rightarrow = \gcd(124, 30)$

$124 = 4(30) + 4$

$\Rightarrow = \gcd(30, 4)$

$30 = 7(4) + 2$

$\Rightarrow = \gcd(4, 2)$

$4 = 2(2) + 0$

this is called The Euclidean Algorithm

  - $\gcd(a,b)$ $(0<a<b)$

$b = q_1 a + r_0 \quad 0 \le r_0 < a$

$a = q_1 r_0 + r_1 \quad 0 \le r_1 < r_0$

$r_0 = q_2 r_1 + r_2 \quad 0 \le r_2 < r_1$

$\vdots$

$r_{k-1} \Rightarrow \gcd(a,b) = r_k$

  - The Euclidean Algorithm terminates after finitely many steps because $r_0 > r_1 > r_2 > \dots$ is a strictly decreasing sequence of non-negative integers
    - has a max length $r_0 + 1$ before hitting 0

2. $p > 1$ is <u>prime</u> if p is only divisible by 1 and itself
   - ie: $\gcd(1,p) = 1$, $\gcd(2,p) = 1$, $\gcd(3,p) = 1$ ... $\gcd(p-1, p) = 1$

Proposition:

- If p is prime & $p | ab$ then $p|a$ or $p|b$
- <u>Proof</u>: Assume p is prime & $p|ab$ but $p \nmid a$ (to show $p|b$)

ie $b = pk$ for $k \in \mathbb{Z}$)

$p \nmid a \Rightarrow \gcd(p,a) = 1$

$\Rightarrow$ there are $x,y \in \mathbb{Z}$ such that $ax + py = 1$

$\Rightarrow abx + pby = b$

$\Rightarrow p|b$ because $p|abx$ & $p|pby$ ∎

Lemma: If $\gcd(n,k) = d$ then there are $x,y \in \mathbb{Z}$ such that $d = xn + yk$

- proof $n = q_0 k + r_0$

$k = q_1 r_0 + r_1$

$\vdots$

$r_m = d$

$r_{m+1} = 0$

$r_{m-2} = q_m r_{m-1} + r_m \Rightarrow r_m = r_{m-2} - q_m r_{m-1}$

$\vdots$

$r_m = ?k - n$

$\uparrow$

y

∎