More number theory review

Thm: Let $a, b \in \mathbb{Z}$. Then $\gcd(a,b)$ exists and is unique.

Specifically,

- $\gcd(0,0) = 0$;
- if a and b are not both 0, then $\gcd(a,b)$ is the smallest positive integer of the form $ax+by$ for $x, y \in \mathbb{Z}$.

Ex: $a = 6, \quad b = 15$

x	y	$6x + 15y$
1	0	6
-1	1	9
2	-1	$\cancel{-3}$
3	-1	3
-2	1	3
⋮	⋮	⋮

Proof: For all $n \in \mathbb{Z}$, $n \mid 0$ is true $(0 = n \cdot 0)$. Moreover, 0 is the only integer divisible by all other integers. Hence, $\gcd(0,0) = 0$.

When a and b are not both 0, consider the set

$$S = \{ n \in \mathbb{N} \mid n = ax + by \text{ for some } x, y \in \mathbb{Z} \}$$

Since $S \neq \emptyset$ (Why?), S has a smallest element. Call it d.

Since $d \in S$, $d = ax + by$ for some $x, y \in \mathbb{Z}$.

Divide a by d to get

$$a = dq + r$$

for $q, r \in \mathbb{Z}$ with $0 \leq r \leq d - 1$.

If $r > 0$, then

$$\begin{aligned} r &= a - dq \\ &= a - (ax + by)q \\ &= a(1 - qx) + b(-qy), \end{aligned}$$

so $r \in S$. But $r < d$, contradicting the minimality of d.

Hence, $r = 0$ and $d \mid a$.
Similarly, $d \mid b$.

Now, suppose $d' \in \mathbb{Z}$ is a common divisor of a and b, i.e., $d' \mid a$ and $d' \mid b$.

Then $a = d'k$ and $b = d'l$ for some $k, l \in \mathbb{Z}$. Thus,

$$d = ax + by = d'(kx + ly)$$

so that $d' | d$.

Therefore, $d = \gcd(a,b)$. $\blacksquare$

<u>Cor</u>: Let $a, b \in \mathbb{Z}$. Then $\gcd(a,b) = 1$ if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.

The proof above is constructive! It yields the

Euclidean Algorithm

INPUT: $a, b \in \mathbb{N}$
OUTPUT: $\gcd(a,b)$.

Set $r_{-1} = a$, $r_0 = b$, and $n = 0$.

While $r_n \neq 0$:

- Divide r_{n-1} by r_n to get

$$r_{n-1} = r_n q_{n+1} + r_{n+1}$$

- If $r_{n+1} = 0$, OUTPUT r_n and STOP.

- Else, increment $n \mapsto n+1$.

Why does this work?

Initially, $r_{-1} = a$ and $r_0 = b$ are in

$$S = \{n \in \mathbb{N} \mid n = ax + by \text{ for some } x, y \in \mathbb{Z}\}.$$

since $a = a(1) + b(0)$ and $b = a(0) + b(1)$.

When we divide $r_{n-1} \in S$ by $r_n \in S$, the new remainder r_{n+1} is also in S, and $0 \leq r_{n+1} \leq r_n - 1$.

Thus, we get

$$b = r_0 > r_1 > r_2 > \cdots \geq 0.$$

This cannot go on forever, so eventually we arrive at the smallest element in S, which is $\gcd(a, b)$.

Ex: $a=270$, $b=192$

$r_{-1}=270$

$r_0=192$

$$270 = 192(1) + 78 \qquad r_1 = 78$$
$$192 = 78(2) + 36 \qquad r_2 = 36$$
$$78 = 36(2) + 6 \qquad r_3 = 6$$
$$36 = 6(6) + 0 \qquad r_4 = 0$$

So $\gcd(270, 192) = 6$.

We can also work backwards to get

$$\begin{aligned}
6 &= 78 - 36\cdot 2 \\
&= 78 - (192 - 78\cdot 2)\cdot 2 \\
&= 78\cdot 5 + 192(-2) \\
&= (270-192)\cdot 5 + 192(-2) \\
&= 270(5) + 192(-7).
\end{aligned}$$

Note: $\gcd(a,b) = \gcd(|a|,|b|)$ and $\gcd(a,0) = |a|$, so we lose nothing by assuming $a, b \in \mathbb{N}$.

Primes

Def: An integer p is prime if

① $p \geq 2$

and

② if $d \in \mathbb{N}$ and $d \mid p$, then $d = 1$ or $d = p$.

Thm: There are infinitely many primes.

Proof: Math 3345 or see text.

Thm: Let $p \in \mathbb{Z}$ with $p \geq 2$. Then p is prime if and only if for all $a, b \in \mathbb{Z}$, $p \mid ab$ implies $p \mid a$ or $p \mid b$.

Proof: $(\Rightarrow)$ [Euclid's Lemma]

Suppose $a, b \in \mathbb{Z}$ with $p \mid ab$.

If $p \mid a$, then we are done. So assume $p \nmid a$. Then $\gcd(a, p) = 1$ (Why?).

Thus, $1 = ax + py$ for some $x, y \in \mathbb{Z}$. Now,

$$b = b \cdot 1 = b(ax + py) = (ab)x + p(by).$$

Since $p \mid ab$ and $p \mid p$, p divides the left-hand side, i.e., $p \mid b$.

($\Leftarrow$) Conversely, suppose the implication

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$$

is true for all $a, b \in \mathbb{Z}$.

Let $d \in \mathbb{N}$ be a divisor of p. We wish to show $d = 1$ or $d = p$.

Since $d \mid p$, we have $p = dk$ for some $k \in \mathbb{N}$. Since $p \mid p$, we have $p \mid d$ or $p \mid k$.

<u>Case 1</u>: $p \mid d$. Since $d \mid p$ also, we have $d = p$.

<u>Case 2</u>: $p \mid k$. Since $k \mid p$ also, we have $k = p$ and $d = 1$.

Thus, p is prime. $\blacksquare$

Thm (Fundamental Theorem of Arithmetic):

Every integer $n \geq 2$ can be expressed uniquely as a product of primes.

↳ up to reordering the factors

Proof: Math 3345 or see text.