Common Divisors

Reading

Section 3.3

Practice Problems

3.3 3, 4, 5, 6, 9, 10, 17, 18, 24
Challenge 3.3 (optional) 11, 15, 20, 21, 25

Notes

> The **greatest common divisor** of a and b is the largest natural number d such that d divides both a and b.
>
> We denote it as $d = \gcd(a, b)$
>
> Special case: a, b called **relatively prime**, if $\gcd(a, b) = 1$
>
> Similar definition: **least common multiple**

Work out some examples!

Most direct way: Find all divisors of each number, find the commons ones, pick largest.

Other option: Factor each number into primes, take the primes both numbers have in common.

For prime numbers, things are easier:

> If p is prime and n is any integer, then p does not divide n if and only if $\gcd(p, n) = 1$.

Proof:

- Forward direction:
  - The only possible common divisors are 1 and p.
  - Since p does not divide n, then 1 is the only common divisor.
  - So it must be the $\gcd(p, n)$.
- Backwards direction:
  - If $\gcd(p, n) = 1$, then there is no common divisor larger than 1.
  - In particular p is not a common divisor.
  - But p divides itself, so it must not divide n.

Another important result has to do with factoring out the greatest common divisor:

If $\gcd(a, b) = 1$ and x, y are such that $a = dx$ and $b = dy$, then $\gcd(x, y) = 1$.

Proof:

- Let $c = \gcd(x, y)$. We will show $c = 1$.
- $x = cr$, $y = cs$ for some integers r, s.
- Then $a = dcr$ and $b = dcs$.
- So dc is a common factor of a, b.
- By the definition of d, must have that $dc <= d$.
- So necessarily $dc = d$. Hence $c = 1$.