Pepegproofs

July 2, 2024

0.1 Preface

I am usually alright not knowing how everything works. But when a statement is presented so simply in front of me and yet the answer is so unintuitive, I can't help but get sucked into a swirling black hole of wanting to understand why it is true. However, I am not very good at math, and I am lazy. The following are pepeg proofs to myself that I know why some things work.

0.2 Euclid's algorithm or something

This was not the first time. Euclid was dropped in SICP and CLRS, and in both times, I couldn't understand why the heck it worked, which entirely side-tracked any progress on them. Euclid's algorithm or something is a procedure to obtain the greatest common divisor (GCD) between 2 numbers. For example, $gcd(16, 28) = 4$.

The procedure is based on the observation that:

$$gcd(a, b) = gcd(b, r)$$

where $r = a\%b$, which is the remainder of a/b. This is useful as it lets us define a recurrence relation which breaks down the procedure's inputs smaller and smaller:

$$gcd(16, 28) = gcd(16, 12) = gcd(12, 4) = gcd(4, 0) = 4$$

I want to prove this somehow. Let's first prove to ourselves that there is some divisor of r which is a divisor of a. Basically, there exists some number d such that

$$a = t_1 d \tag{1}$$
$$b = t_2 d \tag{2}$$
$$r = t_3 d \tag{3}$$

If we assume that this is not true, we can say that:

$$r = t_3 d + c, 0 < c < d \tag{4}$$
$$r = a - qb \tag{5}$$
$$r = t_1 d - qb \tag{6}$$

Subtracting (4) from (6):

$$0 = t_4 d - qb - c \tag{7}$$
$$t_4 d = qb + c \tag{8}$$
$$t_4 d = q(t_2 d) + c \tag{9}$$

But since $0 < c < d$, there is a contradiction which means the previous statement is true. Now let's prove that this number d will be the GCD of a and b.

Let's say that d is *not* the GCD. This means that there is some other d' such that $d' > d$ but also this d' does not divide r.

$$a = k_1 d' \tag{10}$$
$$b = k_2 d' \tag{11}$$
$$r = k_3 d' + c, 0 < c < d' \tag{12}$$

Substituting these into (5):

$$k_3 d' + c = k_1 d' - q(k_2 d') \tag{13}$$
$$k_3 d' + c = k_4 d' \tag{14}$$
$$c = k_5 d' \tag{15}$$

However, $0 < c < d'$ so equation (15) cannot be true. With that we proved that a divisor of b and r is a divisor of a and b. We also proved that this divisor should be the greatest.