Selected Solutions to Homework 1

Tim Smits

1.2.30 If $a_1, a_2, \ldots, a_n$ are integers, not all zero, then their **greatest common divisor** is the largest integer d such that $d \mid a_i$ for all i. Prove that there exist integers u_i such that $d = a_1u_1 + \ldots + a_nu_n$.

Solution: We mimic the proof of Bezout's lemma. Let $S = \{a_1x_1 + \ldots + a_nx_n > 0 : x_i \in \mathbb{Z}\}$ be the set of positive linear combinations of a_i. Since not all $a_i = 0$, picking $x_i = a_i$ we see $a_1^2 + \ldots + a_n^2 > 0 \in S$. By the well-ordering principle, there is a minimal element of S, say d', and we may write $d' = a_1u_1 + \ldots + a_nu_n$ for some integers u_i. We will show that d' is the greatest common divisor of the a_i. By definition, $d = (a_1, \ldots, a_n)$ divides a_i for each i, so $d \mid a_1u_1 + \ldots + a_nu_n = d'$, which says that $d \leq d'$.

Now we show the other inequality. For any i, we may write $a_i = d'q + r$ for some integers q, r with $0 \leq r < d'$ by the division algorithm. We then see that $r = a_i - d'q = a_i - (a_1u_1 + \ldots + a_nu_n)q = a_1(-u_1) + \ldots + a_i(1 - u_iq) + \ldots + a_n(-u_nq)$. Since d' is the smallest element of S, necessarily we cannot have $r \in S$, so $r = 0$. This says $d' \mid a_i$ for all i, so it's a common divisor. Therefore $d' \leq d$, so $d' = d$ as desired.

1.3.30

(a) Prove there are no non-zero integers a, b such that $a^2 = 2b^2$.

(b) Prove that $\sqrt{2}$ is irrational.

Solution:

(a) By the fundamental theorem of arithmetic, we may write $a = 2^e m$ and $b = 2^f n$ for some integers e, f, m, n where m, n are odd and $e, f \geq 0$. We then have $a^2 = 2^{2e}m^2$ and $2b^2 = 2^{2f+1}n^2$. These cannot ever be equal, because the exponent of 2 in a^2 is even, while the exponent of 2 in $2b^2$ is odd.

(b) If $\sqrt{2}$ is rational, we can write $\sqrt{2} = \frac{a}{b}$ for some non-zero integers a, b. Squaring and rewriting says $2b^2 = a^2$, which by (a) has no solutions, a contradiction.

1.3.32 Prove there are infinitely many primes.

Solution: Suppose for sake of contradiction that there are only finitely many primes, say $p_1, \ldots, p_n$. Consider $p = p_1 \cdots p_n + 1$. We clearly have $p > 1$, and note that p is not divisible by p_i for any i (it has remainder 1 upon division by p_i). However, we know that every integer larger than 1 must have a prime divisor, but p is not divisible by any prime, a contradiction. Therefore, there must be infinitely many primes.