Homework 1 (due Friday, Nov. 16)

There are 9 problems below, but Q.7 is quite long and counts as two problems. Hence 10 problems. A total of at least 8 correct solutions gives 5 bonus points on the exam. Problems marked with a * are considered more difficult and these count double. So, for example, if you solve 4 non-starred problems, including Q.7, plus one starred problem, then you have solved 7 problems. Clear ?? :)

Q.1 (i) Complete the induction step of the proof of Theorem 3.4 in the notes, i.e.: the proof that

$$a_1 x_1 + \cdots + a_n x_n = a_0 \tag{1}$$

has a solution if and only if GCD$(a_1, ..., a_n)$ divides a_0.
(ii) Find any solution of the equation

$$49x + 63y + 85z = 1,$$

and write down a formula for the general solution.

Q.2 Let $a_1, ..., a_n$ be positive integers with GCD$(a_1, ..., a_n) = 1$. Let $G(a_1, ..., a_n)$ denote their *Frobenius number*, i.e.: the largest positive integer a_0 such that (1) above has no solution in non-negative integers $x_1, ..., x_n$.
(i) Prove that $G(a_1, ..., a_n) < \infty$ always.
(ii) Prove that $G(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$.

Q.3 If (x, y, z) is a Pythagorean triple, prove that xyz is divisible by 60.

Q.4 A *k-term arithmetic progression* is a k-tuple $(a_1, ..., a_k)$ of distinct integers such that the differences $a_i - a_{i-1}$ are all equal, for $i = 2, ..., k$.
(i) Prove that there are infinitely many primitive[1] 3-term arithmetic progressions each of whose terms is a perfect square.
***(ii)** Prove that it is impossible to find a 4-term arithmetic progression consisting entirely of perfect squares.

Q.5 Let $(R, +, \cdot)$ be a commutative ring. A function $d : R \to \mathbb{Z}_+$ is said to be *Euclidean* if the following three properties are satisfied :
(i) $d(a) = 0 \Leftrightarrow a = 0$.
(ii) For all $a, b \neq 0$, $d(a) \leq d(ab)$.
(iii) For all $a, b \neq 0$, there exist $q, r \in R$ such that $a = qb + r$ and either $r = 0$ or $d(r) < d(b)$.

[1] i.e.: GCD$(a_1, a_2, a_3) = 1$.

Now let $R = \mathbb{Z}[\sqrt{-2}]$. Prove that the function

$$d(z) = |z|^2, \text{ i.e.: } d(x + y\sqrt{-2}) = x^2 + 2y^2,$$

is a Euclidean function on R.

(HINT : The hard part is to verify property (iii). First do this when b is a positive integer, using numerically least remainders (see the statement of Theorem 12.4 in the lecture notes)).

Remark : An integral domain equipped with a Euclidean function is called a *Euclidean ring*. As I have said on multiple occasions in class, it can be shown that a Euclidean ring is a principal ideal domain and satisfies a unique factorisation property. We may discuss this in class later. This is one way of proving that one has unique factorisation in $\mathbb{Z}[\sqrt{-2}]$, which we used in Theorem 4.2.

Q.6 Let $\mathscr{A}_1 = (a_{1,n})_{n=1}^{\infty}$, $\mathscr{A}_2 = (a_{2,n})_{n=1}^{\infty}, \cdots, \mathscr{A}_k = (a_{k,n})_{n=1}^{\infty}$ be a family of sequences of positive integers. We say that the family $\{\mathscr{A}_1, ..., \mathscr{A}_k\}$ is *complementary* if every positive integer appears exactly once and in exactly one of the sequences.

(i) Now let α, β be positive real numbers. Prove that the sequences $([n\alpha])_{n=1}^{\infty}$ and $([n\beta])_{n=1}^{\infty}$ are complementary if and only if α and β are both irrational and satisfy

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1.$$

***(ii)** Prove that it is impossible to find three positive real numbers α, β, γ such that the sequences $([n\alpha]), ([n\beta])$ and $([n\gamma])$ are complementary.

Q.7 (i) A sequence $(a_n)_{n=1}^{\infty}$ of real numbers is said to be *subadditive* if, for every $m, n \in \mathbb{N}$, $a_{m+n} \leq a_m + a_n$. Let $(a_n)_{n=1}^{\infty}$ be a subadditive sequence of non-negative integers. Prove that $\lim_{n\to\infty} a_n/n$ exists and is a non-negative real number.
(ii) For $n \in \mathbb{N}$, let $f(n)$ be the largest size of a subset of $\{1, ..., n\}$ containing no three-term arithmetic progressions. A famous theorem of Roth (see Supplementary Lecture Notes for Week 50) states that $\lim_{n\to\infty} f(n)/n = 0$. Without using this, prove that $\lim_{n\to\infty} f(n)/n$ actually exists at least.
(iii) Let $\mathscr{L}$ be any linear Diophantine equation, say

$$\mathscr{L} : \quad a_1x_1 + \cdots + a_nx_n = a_0, \quad a_i \in \mathbb{Z}.$$

Let $f(n)$ be the largest size of a subset of $\{1, ..., n\}$ which contains no non-trivial solutions to $\mathscr{L}$. In general, it is not known whether $\lim_{n\to\infty} f(n)/n$ exists. Prove, however, that $\liminf_{n\to\infty} f(n)/n > 0$ whenever the equation

is *variant*, .i.e.: whenever either $a_0 \neq 0$ or $\sum_{i=1}^{n} a_i \neq 0$.
(iv), (v) With notation as in part **(iii)**, compute (with proof) $\lim_{n\to\infty} f(n)/n$ for each of the following variant equations :

(a) $2x = y$,
(b) $3x = y + z$.

Q.8 For $n \in \mathbb{N}$ define $\tau(n)$ to be the number of positive integers which divide n, including both 1 and n itself. Prove that, for any $\epsilon > 0$,

$$\lim_{n\to\infty} \frac{\tau(n)}{n^{\epsilon}} = 0.$$

(You can get partial credit for proving the result just for $\epsilon = 1$).

***Q.9** Let

$$S_{2,3} := \{n \in \mathbb{Z} : n = 3^x - 2^y \text{ for some } x, y \in \mathbb{N}_0\}.$$

Prove any non-trivial statement about this set.