Homework 1 (due Monday, Nov. 24)

There are 8 problems below, but most of them are quite long and divided into multiple parts. Hence, points are awarded for the different parts individually. The maximum number of points is 31. The total exam bonus will be calculated as $6x/31$, where x is the number of points obtained.

Some of the problems you might find more difficult than others. Some are the same as on last year's homework. Some others I had thought of during the last couple of weeks. A couple simply came to mind during class, for example as a result of questions from the audience !

Q.1 (5x1p) 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 $G(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$.

(iii) Write down a formula for the general solution of the Diophantine equation

$$7x + 19y + 23z = 11.$$

(iv) Calculate the Frobenius number $G(7, 19, 23)$. You may use a computer.

(v) Determine with proof all positive integers n for which there exist positive integers m_1, m_2 satisfying $m_1 < m_2 < 2m_1$ and $n = 3m_1 + 2m_2$.

Q.2 (5x1p) (i) If (x, y, z) is a Pythagorean triple, prove that xyz is divisible by 60.

(ii) Prove that, for any odd number t, the equation $x^4+y^4 = z^t$ has infinitely many solutions in positive integers x, y, z.

(iii) Let (a_1, b_1, c_1) and (a_2, b_2, c_2) be distinct primitve Pythagorean triples. Prove that $|\{a_1, b_1, c_1\} \cap \{a_2, b_2, c_2\}| \leq 1$.

(iv) Let p, q be relatively prime integers with $p > q$. Prove that $p^2 - q^2$ cannot divide $p^2 + q^2$.

(iv) Using the results of parts (iii) and (iv) or otherwise, prove that the equation $x^4 - y^4 = z^2$ has no solutions in positive integers.

Q.3 (2p+1p) (i) Let m, n be relatively prime positive integers. Prove that the equation $ax^n = by^m$ has an integer solution for any $a, b \in \mathbb{N}$.

(ii) Let $n \in \mathbb{N}$ be fixed. Describe a polynomial-time[1] algorithm for deciding whether or not the equation $ax^n = by^n$ has a positive integer solution and for finding this (unique) solution if it exists.

Q.4 (2p) 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 $d(r) < d(b)$.

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). One option is to first do this when b is a positive integer, using numerically least remainders (see the statement of Theorem 12.4 in the lecture notes). There is also a more purely geometric approach.).

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.5 (3x2p) (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. Roth's theorem (mentioned in class, and see Supplementary Lecture Notes for Week 51) 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

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

[1] that is, polynomial in the size of the inputs a, b.

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 $\sum_{i=1}^{n} a_i \neq 0$.

Q.6 (2x2p) With notation as in part **Q.5**, compute (with proof) $\lim_{n\to\infty} f(n)/n$ for each of the following variant equations :

(a) $2x = y$,

(b) $3x = y + z$.

OBS! One can generalise part (a) and determine explicitly, for every pair a, b of relatively prime positive integers, the maximum subset of $\mathbb{N}$ which contains no solutions to the equation $ax = by$. For extra credit (2p), do this instead of part (a).

Q.7 (2p) 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.8 (2p) Let $S = \{p/q : p \text{ and } q \text{ are primes}\}$. Prove that S is dense in $\mathbb{R}_+$.