Solutions to Homework 1

Q.1 (i) Let $u_1, ..., u_n$ be any integers, positive or negative, satisfying

$$a_1u_1 + \cdots + a_nu_n = 1.$$

We know from the lectures that such integers exist. Now let

$$m := \min\{a_1, ..., a_n\}, \tag{1}$$
$$M := \max\{|u_1|, ..., |u_n|\}, \tag{2}$$
$$s := \sum_{i=1}^{n} a_i.$$

Let $r_0 := smM$. I claim that $G(a_1, ..., a_n) < r_0$. Clearly, there is a non-negative solution to $\sum a_i x_i = r_0$, namely $x_i = mM$ for all i. Now let $\delta \in \{0, 1, ..., m-1\}$. Then a solution to $\sum a_i x_i = r_0 + \delta$ is given by

$$x_i = mM + \delta u_i, \quad i = 1, ..., n. \tag{3}$$

By (1) and (2), we see that each x_i in (3) is non-negative. Thus we have shown that there is a non-neagative solution to $\sum a_i x_i = r$, for each of a sequence of m integers starting at $r_0 = smM$. But from this it follows easily that there is a non-negative solution for any $r \geq r_0$. For suppose $a_j = m$. Then given a non-negative solution to $\sum a_i x_i = r$, for some r, a non-negative solution to $\sum a_i x_i' = r + m$ is given by

$$x_i' = x_i, \ \text{if } i \neq j, \quad x_j' = x_j + 1.$$

(ii) If $a_1 = a_2 = 1$ then the theorem states that $G(1, 1) = -1$, in other words that every non-negative integer can be written as $x + y$, for some $x, y \geq 0$. This is clear. So we may henceforth assume, without loss of generality, that $a_1 > a_2 \geq 1$. We shall show two things :

CLAIM 1 : There is no non-negative integer solution to

$$a_1x + a_2y = (a_1 - 1)(a_2 - 1) - 1 = a_1a_2 - a_1 - a_2. \tag{4}$$

CLAIM 2 : There is a non-negative solution to

$$a_1x + a_2y = (a_1 - 1)(a_2 - 1) + \delta,$$

for every $\delta \in \{0, 1, ..., a_2 - 1\}$. The fact that these claims in turn suffice to establish that $G(a_1, a_2) = (a_1 - 1)(a_2 - 1) - 1$ is then argued in a manner similar to that given in part **(i)** above.

PROOF OF CLAIM 1 : Assume the contrary, and let (x, y) be a non-negative solution. First look at (4) modulo a_1. It reads

$$a_2(y + 1) \equiv 0 \ (\text{mod } a_1).$$

Since GCD$(a_1, a_2) = 1$ it follows from FTA that $a_1 | y + 1$. Since y is non-negative, this means that $y \geq a_1 - 1$. Similarly, by looking at (4) modulo a_2 we find that $x \geq a_2 - 1$. But then

$$a_1 x + a_2 y \geq a_1(a_2 - 1) + a_2(a_1 - 1) = 2a_1 a_2 - a_1 - a_2 > a_1 a_2 - a_1 - a_2,$$

a contradiction.

PROOF OF CLAIM 2 : The equation we want to solve can be rewritten as

$$a_1(x + 1) + a_2(y + 1) = a_1 a_2 + \delta', \tag{5}$$

where $\delta' \in \{1, 2, ..., a_2\}$. Since GCD$(a_1, a_2) = 1$, the integers $a_1, 2a_1, ..., a_2 a_1$ represent, in some order, all congruence classes modulo a_2 exactly once. In particular, there is some $\xi \in \{1, 2, ..., a_2\}$ such that

$$a_1 \xi \equiv \delta' \text{ (mod } a_2).$$

In other words, there exists an integer $\eta \geq 0$ such that

$$a_1 \xi = \delta + a_2 \eta \;\Rightarrow\; a_1 \xi - a_2 \eta = \delta.$$

Note that, since $\xi \leq a_2$, we also have $\eta < a_1$. Then a non-negative solution to (5) is given by $x + 1 = \xi$, $y + 1 = \eta + a_1$.

(iii) Note that GCD$(7, 19) = 1$. Let

$$w := 7x + 19y. \tag{6}$$

Thus, in terms of w and z, the equation reads

$$w + 23z = 11. \tag{7}$$

One solution to () is clearly $w = 34$, $z = -1$. Since GCD$(1, 23) = 1$, by Euclid the general solution to () is thus

$$w = 34 + 23n, \quad z = -1 - n, \quad n \in \mathbb{Z}.$$

Euclid also tells us that the general solution to (6) is

$$x = x_0 w + 19m, \quad y = y_0 w - 7m, \quad m \in \mathbb{Z},$$

where $7x_0 + 19y_0 = 1$. Clearly we can take, for example, $x_0 = 11$, $y_0 = -4$. Substituting in everything, we find that the general solution to the original Diophantine equation is

$$x = 11(34 + 23n) + 19m = 19m + 253n + 374,$$
$$y = -4(34 + 23n) - 7m = -7m - 92n - 136,$$
$$z = -1 - n, \quad m, n \in \mathbb{Z}.$$

(iv) There seems to be a general agreement among those who did the homework that $G(7, 19, 23) = 62$. Note that $(3, 1, 1)$ is a solution to the equation

$7x + 19y + 23z = 63$.

(v) There is a solution if and only if $n \geq 12$ and $n \notin \{13, 14, 15, 16, 18, 20, 21, 23, 25, 28, 30, 35\}$. To see where the hell this problem came from, go to page 7 of the article
`http://www.math.chalmers.se/~hegarty/HK_circle_oct26.pdf`

Q.2 (i) Clearly, it suffices to prove the result for all primitive triples. Let (x, y, z) be any such triple. By Theorem 3.8 in the lecture notes we have, without loss of generality,

$$x = 2ab, \quad y = b^2 - a^2, \quad z = b^2 + a^2,$$

for some relatively prime integers $a < b$ of opposite parity. Since one of a and b is thus even, it follows that $4|x$. If either a or b is divisible by 3, then so is x. Otherwise, $b^2 \equiv a^2 \equiv 1 \pmod 3$, so $3|y$. In either case, $3|xy$. Since already $4|x$, FTA implies that $12|xy$. Finally, it suffices to show that at least one of x, y, z is divisible by 5. If either a or b is divisible by 5, then so is x. Otherwise, each of a^2 and b^2 must be congruent to either $+1$ or -1 (mod 5). In particular, $b^2 \equiv \pm a^2 \pmod 5$, hence $5|(b^2 \mp a^2)$, i.e.: $5|y$ or $5|z$, as required.

(ii) Since t is odd, there exist positive integers i, j such that $ti - 4j = 1$. Now let $m \in \mathbb{N}$ and take $x = y = 2^{tm+j}$, $z = 2^{4m+i}$. Check that $x^4 + y^4 = z^t$. This gives an infinite family of solutions.

(iii) The exercise is easily reduced to proving that there are no 4-tuples $(a, b, c, d) \in \mathbb{N}^4$ satisfying the pair of equations

$$a^2 + b^2 = c^2, \qquad a^2 + d^2 = b^2. \tag{8}$$

We will use an infinite decscent argument - assuming a solution exists to (8), we will construct a “smaller” one, in a sense which will become evident as the argument unfolds. This will yield a contradiction.

We can assume both Pythagorean triples are primitive, because if a prime p divides any two of a, b, c, d, then it is easily seen to divide all four, and hence $(a/p, b/p, c/p, d/p)$ will be a smaller 4-tuple satisfying (8). Since both triples are primitive, b must be odd, hence a must be even. By Theorem 3.8 in the lecture notes, there exist integers positive integers x_1, y_1, x_2, y_2, with GCD$(x_i, y_i) = 1$, x_i and y_i of opposite parity, such that

$$a = 2x_1y_1 = 2x_2y_2, \quad b = y_1^2 - x_1^2 = y_2^2 + x_2^2, \quad c = y_1^2 + x_1^2, \quad d = y_2^2 - x_2^2. \tag{9}$$

Note that the equations for b lead to

$$y_1^2 = x_1^2 + x_2^2 + y_2^2, \tag{10}$$

which forces y_1 to be odd and x_1 even, as vice versa would lead to the contradiction $0 \equiv 2 \pmod 4$. Let

$$g_1 := \text{GCD}(x_1, x_2), \quad g_2 := \text{GCD}(y_1, y_2), \quad g_3 := \text{GCD}(x_1, y_2), \quad g_4 := \text{GCD}(x_2, y_1).$$

Since $\text{GCD}(x_1, y_1) = \text{GCD}(x_2, y_2) = 1$, it is easily seen that the g_i are pairwise relatively prime. Moreoever, the equations for a in (9) imply that $x_1 y_1 = x_2 y_2$, from which it then follows that

$$x_1 = g_1 g_3, \quad x_2 = g_1 g_4, \quad y_1 = g_2 g_4, \quad y_2 = g_2 g_3. \tag{11}$$

Since y_1 is odd and x_1 even and the g_i are pairwise relatively prime, we deduce that g_2 and g_4 are both odd, and exactly one of g_1 and g_3 is even. If g_1 is even and g_3 odd, then substituting (11) into (10) leads to

$$g_2^2 \left(\frac{g_4^2 - g_3^2}{2} \right) = g_1^2 \left(\frac{g_4^2 + g_3^2}{2} \right).$$

The terms on the left and right are relatively prime in pairs, so it must be the case (by FTA) that

$$g_2^2 = \frac{g_4^2 + g_3^2}{2}, \quad g_1^2 = \frac{g_4^2 - g_3^2}{2},$$

which implies that the 4-tuple (g_1, g_2, g_4, g_3) also satisfies (8). But $g_1 \leq g_1 g_2 g_3 g_4 = x_1 y_1 < 2x_1 y_1 = a$, so this new 4-tuple is indeed "smaller".

If instead g_3 is even and g_1 odd, a similar argument leads to the contradiction that (g_3, g_1, g_2, g_4) is a "smaller" 4-tuple. This completes the proof.

(iv) Let $d = \text{GCD}(p^2 - q^2, p^2 + q^2)$. Then d divides $(p^2 - q^2) \pm (p^2 + q^2)$, i.e.: d divides both $2p^2$ and $2q^2$. Hence d divides $\text{GCD}(2p^2, 2q^2) = 2$, since $\text{GCD}(p, q) = 1$. Hence if $p^2 - q^2$ were to divide $p^2 + q^2$, then $p^2 - q^2$ would have to divide 2, in other words, since $p > q$, either $p^2 - q^2 = 1$ or $p^2 - q^2 = 2$. It is easily checked that the latter equation has no integer solution, and the only solutions to the former are $p = \pm 1$, $q = 0$. But p and q are assumed positive, contradiction.

(v) Suppose by way of contradiction that we have a solution $x^4 - y^4 = z^2$. If $d \mid x$ and $d \mid y$, then $d^2 \mid z$ and so $(x/d, y/d, z/d^2)$ is another solution. We may thus suppose x, y, z are pairwise relatively prime. The equation factorises as $z^2 = (x^2 - y^2)(x^2 + y^2)$. Since $\text{GCD}(x, y) = 1$ it follows easily (see part **(iv)**) that $\text{GCD}(x^2 - y^2, x^2 + y^2) \in \{1, 2\}$. If the GCD is 1, then FTA implies that each of $x^2 - y^2$ and $x^2 + y^2$ is a square, i.e.: there exists integers a, b such that $x^2 - y^2 = a^2$ and $x^2 + y^2 = b^2$. But then the

4-tuple (y, x, b, a) would satisfy (8), contradicting the fact that the latter system has no integer solutions. Similarly, if the GCD is 2, then we can write $\left(\frac{z}{2}\right)^2 = \left(\frac{x^2-y^2}{2}\right)\left(\frac{x^2+y^2}{2}\right)$, and now each factor on the right must be a square. So in this case, there exists integers a, b such that $x^2 - y^2 = 2a^2$ and $x^2 + y^2 = 2b^2$. But then the 4-tuple (a, b, x, y) satisfies (8), again a contradiction.

Q.3 (i) Let $p_1, p_2, \dots, p_k$ be the set of all primes appearing in the factorisations of either a or b. Let

$$a = \prod_{i=1}^{k} p_i^{\alpha_i}, \quad b = \prod_{i=1}^{k} p_i^{\beta_i}, \quad \alpha_i, \beta_i \geq 0.$$

We seek a solution of the form

$$x = \prod_{i=1}^{k} p_i^{\gamma_i}, \quad y = \prod_{i=1}^{k} p_i^{\delta_i}, \quad \gamma_i, \delta_i \geq 0.$$

One readily checks that $ax^n = by^m$ is satisfied if and only if, for each $i = 1, \dots, k$,

$$n\gamma_i - m\delta_i = \beta_i - \alpha_i. \tag{12}$$

But since GCD$(m, n) = 1$, (12) will always have a solution in non-negative integers.

(ii) Write the equation as $x/y = \sqrt[n]{b/a}$. First, compute $d =$ GCD(a, b) using Euclid's algorithm. Then divide out d from both a and b, to get new numbers a_1, b_1. So far, this runs in polynomial time. Since GCD$(b_1, a_1) = 1$, the quotient b_1/a_1 is the n:th power of a rational number if and only if each of a_1 and b_1 is the n:th power of an integer (this follows easily from FTA). Thus we just need to approximate $\sqrt[n]{b_1}$ and $\sqrt[n]{a_1}$. Clearly, an approximation to the nearest integer can be obtained in polynomial time (by some kind of divide-and-conquer procedure, in other words, something which uses the Intermediate Value Theorem), and hence we can also determine in polynomial time if the n:th roots are in fact integers and, if so, which ones.

Q.4 The first two properties are easy to verify, so I will concentrate on the third. To simplify notation, put $\xi := \sqrt{-2}$. Let a, b be two non-zero elements of R. First suppose b is a positive integer and let $a = x + y\xi$, where $x, y \in \mathbb{Z}$. Let r_1, r_2 be the numerically least residues of x resp. y modulo b, i.e.: the unique numbers $r_1, r_2 \in (-b/2, b/2]$ such that $x = q_1 b + r_1$ and $y = q_2 b + r_2$ for some $q_1, q_2 \in \mathbb{Z}$. Let $q := q_1 + q_2\xi$ and $r := r_1 + r_2\xi$. Then

$a = qb + r$ and

$$d(r) = r_1^2 + 2r_2^2 \leq 3\left(\frac{b}{2}\right)^2 < b^2 = d(b),$$

which proves property (iii) of a Euclidean domain in the case where $b \in \mathbb{N}$. Now consider a general $b \in R$. Set $u := a\bar{b}$, $v := b\bar{b} = d(b) \in \mathbb{N}$. By the above, there exist $q, r \in R$ such that

$$u = qv + r \text{ and } 0 < d(r) < d(v).$$

Dividing across by $\bar{b}$ we have that $a = qb + r_0$, where $r_0 = r/\bar{b}$. But the function d is clearly multiplicative, so $d(v) = d(b)d(\bar{b})$ and $d(r) = d(r_0)d(\bar{b})$ and hence $0 < d(r) < d(v)$ implies that $0 < d(r_0) < d(b)$, so we are done.

REMARK : One may give a geometric decription of the above argument, which is probably more enlightening than the 'algebraic' presentation given above. $R = \mathbb{Z}[\sqrt{-2}]$ is a rectangular lattice in the complex plane generated by 1 and $\sqrt{-2}$. A rectangle with vertices at $(0,0), (1,0), (1,2)$ and $(0,2)$ forms a fundamental domain for this lattice (once one removes an appropriate part of the boundary). The set $\{qb : q \in R\}$ is an ideal in the ring and corresponds geoemtrically to a sublattice generated by the orthogonal vectors b and $\sqrt{-2}\ b$. These two vectors span a rectangular fundamental domain $\mathcal{F}$ for the sublattice. The point $a \in \mathcal{C}$ must lie in some translate of $\mathcal{F}$, and hence there must be a point in the lattice whose distance to a is certainly no more than half the diameter of $\mathcal{F}$, i.e.: there exists $q \in R$ such that

$$|a - qb| \leq \frac{1}{2}\text{diam}(\mathcal{F}) = \frac{1}{2}\sqrt{d(b)^2 + d(\sqrt{-2}\ b)^2} = \frac{\sqrt{3}}{2}d(b) < d(b), \quad \text{v.s.v..}$$

Q.5 (i) Since every $a_n \geq 0$, the limit, if it exists, must be non-negative. Subadditivity implies that $a_n \leq na_1$, hence $a_n/n \leq a_1$ for any n. Hence the sequence (a_n/n) is bounded and must have a convergent subsequence. Suppose there is a subsequence (a_{n_i}/n_i) converging to a limit L, say. If L is not the limit of the entire sequence then we can find $\epsilon > 0$ and another subsequence (a_{m_i}/m_i), such that, for all $i \geq i_0$,

$$\left|\frac{a_{n_i}}{n_i} - L\right| < \frac{\epsilon}{2}, \quad \left|\frac{a_{m_i}}{m_i} - L\right| > \epsilon. \tag{13}$$

Let's suppose that, for all $i \geq i_0$, $a_{m_i}/m_i > a_{n_i}/n_i$ - a similar argument works in the case of the reverse inequality holding. Thus, by (13), for all $i_1, i_2 \geq i_0$ we have that

$$\frac{a_{m_{i_1}}}{m_{i_1}} - \frac{a_{n_{i_2}}}{n_{i_2}} > \frac{\epsilon}{2}.$$

In particular, for all $i \geq i_0$ one has that

$$\frac{a_{m_i}}{m_i} - \frac{a_{n_{i_0}}}{n_{i_0}} > \frac{\epsilon}{2}. \tag{14}$$

Let $S := \max\{a_s : 1 \leq s < n_{i_0}\}$. For each i, there exist integers q_i, r_i such that $m_i = q_i n_{i_0} + r_i$, where $0 \leq r_i < n_{i_0}$. By subadditivity, we have that $a_{m_i} \leq q_i a_{n_{i_0}} + a_{r_i}$ and hence that

$$\frac{a_{m_i}}{m_i} \leq \frac{q_i a_{n_{i_0}} + a_{r_i}}{m_i} \leq \frac{a_{n_{i_0}}}{n_{i_0}} + \frac{S}{m_i}. \tag{15}$$

Now S is a fixed number and thus $S/m_i \to 0$ as $i \to \infty$. Hence (15) will contradict (14) for all sufficiently large i. This completes the proof.

(REMARK : The result proven above is known in the literature as *Fakete's Lemma*).

(ii) Let $m, n \in \mathbb{N}$. If A is a subset of $\{1, 2, ..., m+n\}$ which is free of 3-term arithmetic progressions, then both A_1 and A_2 are also free of 3-APs, where $A_1 := A \cap \{1, ..., m\}$ and $A_2 := A \cap \{m+1, ..., m+n\}$. This and the fact that a translate of an AP is still an AP easily lead to the conclusion that the function $f(n)$ in this exercise is sub-additive. Then the result follows immediately from part (i).

(iii) First suppose $a_0 \neq 0$. Let p be any prime which does not divide a_0 and let the set A consist of all multiples of p. Then A contains no solutions to the equation $\mathcal{L}$, as it doesn't even contain any solutions modulo p. Hence, in this case,

$$\liminf_{n \to \infty} \frac{f(n)}{n} \geq \liminf_{n \to \infty} \frac{|A \cap \{1, ..., n\}|}{n} = \frac{1}{p} > 0.$$

Next, suppose $\sum_{i=1}^{n} a_i \neq 0$. Let $s := \sum_{i=1}^{n} a_i$, let k be the smallest positive integer such that $ks \neq a_0$ and let p be any prime satisfying $p > \max\{k|s|, |a_0|\}$. Now let $A = \{n \in \mathbb{Z} : n \equiv k \pmod{p}\}$. It is easy to see that A contains no solutions to the equation $\mathcal{L}$, simply because it doesn't even contain any solutions modulo p. Hence, as above, $\liminf f(n)/n \geq 1/p > 0$.

Q.6 (i) In general, one can construct a subset of $\mathbb{N}$ containing no solutions to some fixed equation by means of a *greedy choice procedure*, i.e.: go through the natural numbers in increasing order and, at each step, add the number to the set A if it doesn't create any solutions. For some equations (though by no means all !), this turns out to give an optimal construction. An example is just the equation $2x = y$. It is easy to check that the set A

obtained by this greedy choice is the set

$$A = \{n \in \mathbb{N} : 2^{2k} \mid\mid n \text{ for some } k \geq 0\}. \tag{16}$$

In other words, A consists of all those number which are divisible by an even power of 2. This set has an asymptotic density given by

$$d(A) = \frac{1}{2}\left(\sum_{k=0}^{\infty}\frac{1}{4^k}\right) = \frac{2}{3}.$$

No set avoiding solutions to $2x = y$ can have a higher asymptotic upper density. For if B is such a set, then $B \cap 2B = \phi$, where $2B = \{2b : b \in B\}$. Thus $1 \geq \overline{d}(B \cup 2B) = \overline{d}(B) + \overline{d}(2B) = \frac{3}{2}\overline{d}(B)$, which implies that $\overline{d}(B) \leq 2/3$.

From the above reasoning, it is easy to deduce that $\lim_{n\to\infty} f(n)/n = 2/3$. In fact, if one argues more carefully, one can in fact show that, for every $n \in \mathbb{N}$, the set $A \cap \{1, ..., n\}$, where A is given by (16), is a subset of $\{1, ..., n\}$ of largest possible size containing no solutions to $2x = y$.

(ii) The limit is at least $1/2$, because the set of odd numbers avoids solutions to $3x = y + z$. In fact, the limit is $1/2$. See the 3-page supplementary document on the homepage for a proof of a more precise result. For generalisations of the result, see Papers No. 25 and 29 on my research page.

Q.7 Factorise an integer n as

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Then

$$d(n) = \prod_{i=1}^{k}(\alpha_i + 1),$$

and hence

$$\frac{d(n)}{n^\epsilon} = \prod_{i=1}^{k}\frac{\alpha_i + 1}{p_i^{\epsilon\alpha_i}}.$$

Fix $\epsilon > 0$. For a prime p and a positive integer α, let $f_\epsilon(p, \alpha) := \frac{\alpha+1}{p^{\epsilon\alpha}}$. For fixed ϵ, it is clear that $f_\epsilon(p, \alpha) \to 0$ as long as any one of p and α goes to infinity, even if the other is held fixed. In particular, there will be only a finite number (depending on ϵ) of pairs (p, α) such that $f_\epsilon(p, \alpha) > 1/2$. It follows easily that $d(n)/n^\epsilon \to 0$ as $n \to \infty$.

(NOTE : You can replace $1/2$ by any number strictly less than one and the argument will work).

Q.8 It suffices to show that, for any $r > 1$ and $\varepsilon > 0$ sufficiently small, there exist primes p, q such that $(1-2\varepsilon)r < p/q < (1+3\varepsilon)r$. By the prime number theorem,

$$\pi((1-\varepsilon)x) \sim \frac{(1-\varepsilon)x}{\log(1-\varepsilon)x}, \qquad \pi((1+\varepsilon)x) \sim \frac{(1+\varepsilon)x}{\log(1+\varepsilon)x},$$
$$\pi((1-\varepsilon)rx) \sim \frac{(1-\varepsilon)rx}{\log(1-\varepsilon)rx}, \qquad \pi((1+\varepsilon)rx)) \sim \frac{(1+\varepsilon)rx)}{\log(1+\varepsilon)rx)}.$$

It follows that, for x sufficiently large and ε sufficiently small, there exist distinct primes p, q such that $(1-\varepsilon)x < q < (1+\varepsilon)x$ and $(1-\varepsilon)rx < p < (1+\varepsilon)rx$. Thus $r\left(\frac{1-\varepsilon}{1+\varepsilon}\right) < p/q < r\left(\frac{1+\varepsilon}{1-\varepsilon}\right)$, which in turn implies that $r(1-2\varepsilon) < p/q < (1+3\varepsilon)r$, for sufficiently small ε.