Solutions to Exam 27-08-15

Q.1 (a) Theorem 3.8 in the lecture notes.
(b) Theorem 4.1 in the lecture notes.

Q.2 (a) $(a_1, b_1) = (2, 1)$ is one solution. For any $k \in \mathbb{N}$ define the positive integers a_k, b_k by

$$a_k + \sqrt{3}\, b_k = (a_1 + \sqrt{3}\, b_1)^k.$$

It is clear that the sequences (a_k) and (b_k) are both strictly increasing. Moreover, (a_k, b_k) is a solution for every k since

$$a_k^2 - 3b_k^2 = (a_k + \sqrt{3}\, b_k)(a_k - \sqrt{3}\, b_k) =$$
$$= (a_1 + \sqrt{3}\, b_1)^k (a_1 - \sqrt{3}\, b_1)^k = (a_1^2 - 3b_1^2)^k = 1.$$

(b) For any integers a, b, if we set

$$x = a(a^2 - 3b^2), \quad y = b(3a^2 - b^2), \quad z = a^2 + b^2, \tag{1}$$

then one checks directly that (x, y, z) is a solution. It is also easy to check that we get a primitive solution whenever GCD$(a, b) = 1$ and a and b have opposite parity. Thus there are infinitely many primitive solutions. To see where this idea "comes from", one factorises the equation as $(x + iy)(x - iy) = z^3$. If GCD$(x, y) = 1$, one checks that $x \pm iy$ are relatively prime in $\mathbb{Z}[i]$ hence, by the unique factorisation property, there must exist integers a, b such that $x \pm iy = (a \pm ib)^3$, which leads to (1).

Q.3 (a) Theorem 12.4 in the lecture notes.
(b) Theorem 11.7 in the lecture notes.

Q.4 If $p = 2$ or $p = 7$, then $x = 0$ is a solution. Now suppose $p \notin \{2, 7\}$. We seek all p for which $\left(\frac{14}{p}\right) = +1$. We have $\left(\frac{14}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{7}{p}\right)$, so there are two cases to consider.

CASE 1: $\left(\frac{2}{p}\right) = \left(\frac{7}{p}\right) = +1$.

If $\left(\frac{2}{p}\right) = +1$, then it follows from Gauss Lemma that $p \equiv \pm 1 \pmod 8$.

Subcase 1(a): $p \equiv 1 \pmod 8$. In particular, $p \equiv 1 \pmod 4$ so, by quadratic reciprocity, $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$. Thus $\left(\frac{p}{7}\right) = +1$, which is the case if and only if $p \equiv 1, 2, 4 \pmod 7$. By the Chinese Remainder Theorem, there are thus three possibilities for p mod 56, namely $p \equiv 1, 9, 25 \pmod{56}$.

Subcase 1(b): $p \equiv 7 \pmod 8$. In particular, $p \equiv 3 \pmod 4$ so, by quadratic reciprocity, $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$. Thus $\left(\frac{p}{7}\right) = -1$, which is the case if and only if $p \equiv 3,\ 5,\ 6 \pmod 7$. By the Chinese Remainder Theorem, there are thus three possibilities for p mod 56, namely $p \equiv 31,\ 47,\ 55 \pmod{56}$.

In total, from Case 1 we get six possibilities for $p \pmod{56}$, namely

$$p \equiv \pm 1,\ \pm 9,\ \pm 25 \pmod{56}.$$

CASE 2: $\left(\frac{2}{p}\right) = \left(\frac{7}{p}\right) = -1$.

A similar analysis to Case 1 (details left to reader) leads to a further six possibilities for $p \pmod{56}$, namely

$$p \equiv \pm 5,\ \pm 11,\ \pm 13 \pmod{56}.$$

FINAL ANSWER: $p = 2, p = 7$ or $p \equiv \pm 1,\ \pm 5,\ \pm 9,\ \pm 11,\ \pm 13,\ \pm 25 \pmod{56}$.

Q.5 Theorem 1.7 in the supplementary lecture notes to Week 47, plus Exercise 1 on Homework 2.

Q.6 (a) (i) Since n is always a divisor of itself, the quotient $\frac{\sigma(n)}{n}$ is always at least one. If n is prime, then $\sigma(n) = n + 1$ and, since there are infinitely many primes, it follows that

$$\liminf_{n \to \infty} \frac{\sigma(n)}{n} = 1.$$

(ii) Suppose n is the product of the first k primes, which we denote $p_1, \ldots, p_k$. Then n/p_i is a divisor of n for each i and so

$$\frac{\sigma(n)}{n} \geq \sum_{i=1}^{k} \frac{1}{p_i}.$$

We know that the right-hand sum diverges as $k \to \infty$ (Corollary 5.5 in the lecture notes), hence

$$\limsup_{n \to \infty} \frac{\sigma(n)}{n} = \infty.$$

(iii) A priori,

$$\sigma(n) \leq n + \frac{n}{2} + \frac{n}{3} + \cdots = n \cdot \left(\sum_{k=1}^{n} \frac{1}{k} \right) = (1 + o(1))(n \log n).$$

It follows that, for any $\varepsilon > 0$,

$$\lim_{n \to \infty} \frac{\sigma(n)}{n^{1+\varepsilon}} = 0.$$

(b) If Re$(s) > 1$ then we have the Euler product formula for the zeta function (Theorem 5.3 in the lecture notes), thus

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

and

$$\zeta(2s) = \prod_p \left(1 - \frac{1}{p^{2s}}\right)^{-1}.$$

Using the fact that $1 - t^2 = (1+t)(1-t)$, it follows that

$$\frac{\zeta(s)}{\zeta(2s)} = \prod_p \left(1 + \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s},$$

where $a(n) = 1$ if n is squarefree and $a(n) = 0$ otherwise. In other words, $a(n) = |\mu(n)|$, v.s.v.

Q.7 (a) Proposition 1.6 in Supplement 2 to Week 50.
(b) See Theorem 1.7 and preceeding text in Supplement 2 to Week 50.

Q.8 We can construct a 3-AP avoiding subset of $\{1, 2, \ldots, n\}$ using the same idea as for constructing the usual Cantor set, namely as follows: Divide the interval $\{1, \ldots, n\}$ into three subintervals $A_1 \sqcup B_1 \sqcup C_1$, whose lengths are as close to equal as possible and such that, if (a, b, c) is any 3-term AP with $a \in A_1$ and $c \in C_1$, then one must have $b \in B_1$. Remove B_1 and repeat the above procedure for both A_1 and C_1. Iterate as far as possible.

By construction, the resulting subset $X \subseteq \{1, \ldots, n\}$ will contain no 3-APs and it is easy to show that $|X| = \Omega(n^{2/3})$.