Solutions to Exam 18-12-10

Q.1 Three squares is not enough, because a sum of three suqares cannot be congruent to 7 (mod 8). Now see Theorem 10.2 in the lecture notes, or Theorem 7.3 in the handout from Stewart and Tall.

Q.2 If $a, b \in \mathbb{Z}$ and $z := a + b\sqrt{2}$, then define

$$z^* := a - b\sqrt{2}, \quad N(z) := zz^* = a^2 - 2b^2.$$

Let $R := \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. For any $z_1, z_2 \in R$, it is easily checked that

$$(z_1 z_2)^* = z_1^* z_2^*$$

and hence that

$$N(z_1 z_2) = N(z_1)N(z_2).$$

From this we can deduce the following algebraic identity : if $a, b, c, d \in \mathbb{Z}$, then

$$(a^2 - 2b^2)(c^2 - 2d^2) = (ac + 2bd)^2 - 2(ad + bc)^2. \tag{1}$$

This is what is meant by being able to 'multiply' integer solutions to the equation

$$x^2 - 2y^2 = 1. \tag{2}$$

In particular, taking $a = c$, $b = d$ in (1) we find that if (a, b) is any solution to (2) then $(a^2 + 2b^2, 2ab)$ is another solution. Now if a, b are positive integers, then clearly

$$\min\{a^2 + 2b^2, 2ab\} > \max\{a, b\}.$$

Hence, starting from any solution whatsoever to (2) in positive integers, iteration of the map

$$(a, b) \mapsto (a^2 + 2b^2, 2ab)$$

produces an infinity of solutions. Since, for example, $(3, 2)$ is a solution to (2), this proves that (2) has infinitely many integer solutions.

Q.3 (i) Theorem 12.4 in the lecture notes.
(ii) Theorem 11.7 in the lecture notes.

Q.4 The presumtive solutions would be given by the usual quadratic formula

$$x \equiv \frac{3 \pm \sqrt{3^2 - 4 \cdot 9 \cdot 11}}{2(9)} = (18)^{-1}[3 \pm \sqrt{-387}] \pmod{1237}.$$

Hence solutions exist if and only if

$$\left(\frac{-387}{1237}\right) = +1.$$

Since $1237 \equiv 1 \pmod 4$, we first have

$$\left(\frac{-387}{1237}\right) = \left(\frac{-1}{1237}\right)\left(\frac{387}{1237}\right) = \left(\frac{387}{1237}\right).$$

Next, since $387 = 3^2 \cdot 43$, we have

$$\left(\frac{387}{1237}\right) = \left(\frac{3}{1237}\right)^2\left(\frac{43}{1237}\right) = \left(\frac{43}{1237}\right).$$

Since $1237 \equiv 1 \pmod 4$, quadratic reciprocity implies that

$$\left(\frac{43}{1237}\right) = \left(\frac{1237}{43}\right).$$

Since $1237 = 28 \cdot 43 + 33$, it follows that

$$\left(\frac{1237}{43}\right) = \left(\frac{33}{43}\right).$$

Since $33 \equiv 1 \pmod 4$, Jacobi reciprocity implies that

$$\left(\frac{33}{43}\right) = \left(\frac{43}{33}\right) = \left(\frac{10}{33}\right).$$

Next, since $33 \equiv 1 \pmod 8$, one has

$$\left(\frac{10}{33}\right) = \left(\frac{2}{33}\right)\left(\frac{5}{33}\right) = \left(\frac{5}{33}\right).$$

Finally, Jacobi reciprocity yields

$$\left(\frac{5}{33}\right) = \left(\frac{33}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Hence, the original congruence has no solution.

Q.5 (i) $r_{A,h}(n)$ is the number of unordered h-tuples $\{a_1, ..., a_h\}$ of elements of A which satisfy $a_1 + \cdots + a_h = n$. We say that A is an *asymptotic basis* if, for some positive integer h, one has $r_{A,h}(n) > 0$ for all $n \gg 0$. The least such h is then called the ***(exact) order*** of the asymptotic basis.
(ii) See Theorem 17.6 in the lecture notes.

Q.6 A cannot be an asymptotic basis of order 1 since $\underline{d}(A) < 1$. Now it remains to show that every sufficiently large $n \in \mathbb{N}$ can be written as a sum of two elements of A. Since $\underline{d}(A) > 1/2$, one has for all $n \gg 0$ that

$$|A \cap \{1, ..., n\}| > cn,$$

for some fixed $c > 1/2$. Now fix such an n, and let

$$A_1 := A \cap \{1, ..., n\}, \quad A_2 := \{n - a : a \in A_1\}.$$

On the one hand, $|A_1| = |A_2| > cn$, so $|A_1| + |A_2| > 2cn$. On the other hand, $A_1 \cup A_2 \subseteq \{0, 1, ..., n\}$, so $|A_1 \cup A_2| \leq n + 1$. This implies that $A_1 \cap A_2$ must be non-empty. Let $a_1 \in A_1 \cap A_2$. Then $a_1 \in A$ and there exists $a_2 \in A$ such that $n - a_2 = a_1$, in other words $n = a_1 + a_2$. Hence $n \in 2A$, as required.

Q.7 (i) See the handout from Diestel's book. The Regularity Lemma is stated as Lemma 7.2.1.
(ii) Theorem 1.2 in the supplementary lecture notes for week 49.
(iii) The result follows immediately from Theorem 1.3 in the supplementary lecture notes for week 49.

Q.8 This is a special case of *Rado's regularity theorem* which states that a homogeneous linear equation

$$\mathcal{L} : a_1x_1 + \cdots + a_nx_n = 0, \quad a_i \in \mathbb{Z},$$

is irregular if and only if the following condition holds :

(*) For every non-empty subset $S \subseteq \{1, ..., n\}$, one has $\sum_{i \in S} a_i \neq 0$.

Here I prove the sufficiency of the irregularity condition (*), which is all we need to solve the problem at hand. So let $\mathcal{L}$ be an equation for which (*) is satisfied. Let p be a prime which does not divide any of the subset-sums $\sum_{i \in S} a_i$. Then there exists a $(p-1)$-coloring $\chi : \mathbb{Z} \to \{1, ..., p-1\}$ which avoids monochromatic solutions to $\mathcal{L}$. Namely, every $x \in \mathbb{Z}$ can be written uniquely as $x = p^{k_x}x_0$, where x_0 is not divisible by p. Then there is a unique $x_1 \in \{1, ..., p-1\}$ such that $x_0 \equiv x_1 \pmod{p}$. We define $\chi(x) = x_1$.

It is easy to check that condition (*) guarantees the absence of monochromatic solutions to $\mathcal{L}$.

Note that, for the equation $x + y = 5z$, the coefficients are $a_1 = a_2 = 1$, $a_3 = -5$, and so the set of subset sums of coefficients is $\{1, -5, 2, -4, -3\}$. So the smallest prime which works in the construction aboce is $p = 7$, so we can color the integers with at most 6 colors and avoid monochromatic solutions to $x + y = 5z$.

REMARK : The reader who is also interested in a proof of the necessity of Rado's condition can check, for example, the following sources :

1. http://www.math.uga.edu/$\sim$lyall/REU/rado.pdf
2. The book *Ramsey Theory*, by Graham, Rothschild and Spencer.