Solutions to Exam 19-12-12

Q.1 The usual formula would give as solutions

$$x \equiv \frac{-9 \pm \sqrt{21}}{6} \pmod{p}. \tag{1}$$

The formula makes no sense if $p|6$, i.e.: if $p = 2$ or 3. We first treat these as special cases. If $p = 2$ then the congruence becomes $x^2 + x + 1 \equiv 0$, which has no solutions modulo 2. If $p = 3$, then the congruence becomes $5 \equiv 0$, which also has no solutions modulo 3.

So now assume $p > 3$. Then (1) says that we have solution(s) if and only if 21 is a quadratic residue modulo p. This will be true if $p = 7$. Otherwise, we require that

$$\left(\frac{21}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{7}{p}\right) = 1. \tag{2}$$

We have two cases, depending on whether p is congruent to 1 or 3 (modulo 4).

CASE 1: $p \equiv 1 \pmod{4}$.

By quadratic reciprocity, one has $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$ and $\left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)$. Hence, by (2), we require in this case that

$$\left(\frac{p}{3}\right)\left(\frac{p}{7}\right) = 1. \tag{3}$$

This gives two options, namely

$$\left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = +1 \text{ or } \left(\frac{p}{3}\right) = \left(\frac{p}{7}\right) = -1. \tag{4}$$

CASE 2: $p \equiv 3 \pmod{4}$.

By quadratic reciprocity, one has $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$ and $\left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right)$. Hence, by (2), we also require in this case that (3) be satisfied and thus get the same two options as in (4). Overall, then, the condition modulo 4 disappears, and we are left with (4).

On the one hand, if both symbols in (4) equal +1, then $p \equiv 1 \pmod{3}$ and $p \equiv 1, 2 \vee 4 \pmod{7}$. By the Chinese Remainder Theorem, we thus have three options modulo 21, namely $p \equiv 1, 4 \vee 16 \pmod{21}$.

On the other hand, if both symbols in (4) equal -1, then $p \equiv 2 \pmod{3}$ and $p \equiv 3, 5 \vee 6 \pmod{7}$. By the Chinese Remainder Theorem, we thus have three more options modulo 21, namely $p \equiv 5, 17 \vee 20 \pmod{21}$.

We conclude that the primes for which the original congruence is solvable are $p = 7$ together with all odd primes satisfying

$$p \equiv \pm 1, \pm 4, \pm 5 \pmod{21}. \tag{5}$$

(ii) The primes in part **(i)**, other than $p = 7$, fall into 6 congruence classes modulo 21. One has $\phi(21) = \phi(3 \cdot 7) = 2 \cdot 6 = 12$, so there are 12 congruence classes modulo 21 containing infinitely many primes. By the strong form of Dirichlet's theorem, the primes are equidistributed in all 12 classes. It follows that

$$\lim_{x \to \infty} \frac{\pi_S(x)}{\pi(x)} = \frac{1}{2}. \tag{6}$$

Q.2 See Theorem 9.6 in the notes.

Q.3 See Theorem 4 in the lecture notes from 2004.

Q.4 See Theorem 6.1 in the notes.

Q.5 If $A \subseteq \mathbb{Z}_p$ then, by the Cauchy-Davenport theorem,

$$|A + A| \geq \min\{p, 2|A| - 1\}. \tag{7}$$

If A is sum-free, it follows that $3|A| - 1 \leq p$, hence that $|A| \leq (p+1)/3$. Conversely, suppose $p = 3k+i$, where $i \in \{0, 1, 2\}$. If $i \in \{0, 1\}$, then $A = \{k+1, k+2, ..., 2k\}$ is sum-free. If $i = 2$, then $A = \{k+1, k+2, ..., 2k+1\}$ is sum-free.

CONCLUSION: The maximum size of a sum-free subset of $\mathbb{Z}_p$ is $\lfloor \frac{p+1}{3} \rfloor$.

Q.6 See Theorem 17.6 in the notes. The definition of the representation function $r_h(A, n)$ is given earlier in that lecture.

Q.7 (i) $W(k, l)$ is the least positive integer n such that any l-coloring of the set $\{1, 2, ..., n\}$ must yield a monochromatic k-term arithmetic progression.

(ii) Consider a uniformly random l-coloring of $\{1, 2, ..., n\}$. The probability that any given k-term AP will be monochromatic is $l \cdot l^{-k} = l^{-(k-1)}$, since there are l possibilities for the color, and given the color, each of the k terms gets that color with probability l^{-1}. Let $f_k(n)$ be the number of k-term APs in $\{1, ..., n\}$. By Linearity of Expectation, the expected number of monochromatic k-APs in a uniform coloring is $f_k(n) \cdot l^{-(k-1)}$. Hence, if $f_k(n) \cdot l^{-(k-1)} < 1$, then $W(k, l) > n$.

Now an AP is completely determined by its first term and common difference. If the first term is x, and the AP lies enitrely inside $\{1, ..., n\}$ and contains k terms in all, then the common difference cannot exceed $\frac{n-x}{k-1}$. It follows that

$$f_k(n) \leq \sum_{x=1}^{n} \frac{n-x}{k-1} = \frac{n(n-1)}{2(k-1)}, \tag{8}$$

and hence that $W(k,l) > n$ provided

$$\frac{n(n-1)}{2(k-1)l^{k-1}} < 1. \tag{9}$$

Since $n(n-1) < n^2$, it follows that

$$W(k,l) > \sqrt{2(k-1)}l^{(k-1)/2}, \quad \text{Q.E.D.} \tag{10}$$

Q.8 (i) See the handout from Diestel's book.
(ii) See the Supplementary Notes for Week 50.