Solutions to Exam 16-01-15

Q.1 (i) $66 = 2 \times 3 \times 11$ and $\phi(66) = 1 \cdot 2 \cdot 10 = 20$ so there are 20 primitive roots modulo 67. If a is any such primitive root, then the full list is given by $\{a^k : 1 \leq k \leq 66,\ (k,\, 66) = 1\}$, i.e.:

$k \in \{1,\, 5,\, 7,\, 13,\, 17,\, 19,\, 23,\, 25,\, 29,\, 31,\, 35,\, 37,\, 41,\, 43,\, 47,\, 49,\, 53,\, 59,\, 61,\, 65\}.$

I claim that $a = 2$ is a primitive root. The proper divisors of 66 are $1,\, 2,\, 3,\, 6,\, 11,\, 22,\, 33$ and one can check that, modulo 67,

$$\begin{gathered} 2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^6 \equiv -3, \\ 2^{11} \equiv -29, \quad 2^{22} \equiv -30, \quad 2^{33} \equiv -1. \end{gathered} \tag{1}$$

(ii) Yes. This can in fact be seen from (1), namely that $-29 \equiv 2^{11}$. This is an element of order $66/11 = 6$ in $\mathbb{Z}_{67}^{\times}$, hence not a square, since the subgroup of squares has order $66/2 = 33$, which is not a multiple of 6. Hence, -29 is a quadratic non-residue. So is -1, since $67 \equiv 3 \pmod 4$. Thus $+29 = (-29)(-1)$ is a quadratic residue.

Alternatively, one can use quadratic reciprocity. Since $29 \equiv 1 \pmod 4$ and $67 = 2 \cdot 29 + 9$, it follows that

$$\left(\frac{29}{67}\right) = \left(\frac{67}{29}\right) = \left(\frac{9}{29}\right) = \left(\frac{3}{29}\right)^2 = +1.$$

Q.2 See Theorem 9.6 in the notes. For full points, proofs need to be included of Proposition 9.1, Theorem 9.3 and Lemma 9.5.

Q.3 If $d = e^2$ then $x = e$ gives a solution to the congruence for any p. Conversely, suppose d is a non-square. We need to prove the existence of a prime p such that the congruence has no solution. It suffices to find a prime p such that $\left(\frac{d}{p}\right) = -1$.

Now, since d is not a square, there is at least one prime q such that the highest power of q dividing d is odd. Let $q_1,\, \dots,\, q_k$ be the full list of such primes. Then, for any prime $p > d$,

$$\left(\frac{d}{p}\right) = \prod_{i=1}^{k} \left(\frac{q_i}{p}\right). \tag{2}$$

CASE 1: $k = 1$ and $q_1 = 2$. Choose $p > d$ such that $p \equiv 3 \pmod 8$. Dirichlet's theorem guarantees the existence of such a prime. By Gauss Lemma, $\left(\frac{2}{p}\right) = -1$ and hence $\left(\frac{d}{p}\right) = -1$, by (2).

CASE 2: $k > 1$. Then we may assume $q_1 > 2$. If $p \equiv 1 \pmod 4$, then by quadratic reciprocity,

$$\left(\frac{d}{p}\right) = \prod_{i=1}^{k} \left(\frac{p}{q_i}\right).$$

Let r_1 be any quadratic non-residue mod q_1 and, for each $i = 2, \ldots, k$, let r_i be a quadratic residue mod q_i, where we choose $r_i = 1$ if $q_i = 2$. The Chinese Remainder Theorem plus Dirichlet's theorem guarantee the existence of a prime $p > d$ satisfying all the congruences

$$p \equiv 1 \pmod 4, \quad p \equiv r_i \pmod{q_i},\ i = 1, \ldots, k.$$

For any such prime we will have $\left(\frac{d}{p}\right) = -1$, by (2).

Q.4 Theorem 6.4 in the lecture notes.

Q.5 Call a subset S of $\{1, 2, \ldots, n\}$ *primitive* if no element of S is an integer multiple of any other. The set

$$S_1 = \left\{ \lceil \frac{n}{2} \rceil, \lceil \frac{n}{2} \rceil + 1, \ldots, n \right\}$$

is clearly primitve, thus $g_2(n) \geq \lfloor \frac{n+1}{2} \rfloor$. Conversely, let S be any primitive set. Each element of S can be written uniquely in the form $s = 2^{k(s)} a(s)$, where $k(s) \in \mathbb{N}_0$ and $a(s)$ is an odd integer in $\{1, 2, \ldots, n\}$. If $a(s_1) = a(s_2)$ with $s_1 < s_2$, then s_1 divides s_2. Hence, the cardinality of S does not exceed that of the subset of odd numbers in $\{1, 2, \ldots, n\}$, and so $g_2(n) \leq \lfloor \frac{n+1}{2} \rfloor$.

Q.6 (i) Theorem 20.2 in the lecture notes.
(ii) Lemma 20.3 in the lecture notes.
(iii) Theorem 18.2 in the lecture notes. The proof is in Lecture 21.

Q.7 This proof will be a little sketchy. There are $\Theta(n^2)$ 3-term APs in total in $\mathbb{Z}_n$. List them in any fixed order, and let A_i denote the event that the i:th AP is contained in our random set $A = A(n, p)$. Let X_i be the indicator of the event A_i and let $X = \sum X_i$ be the random variable which counts the total number of APs in A. It is clear that, for each i, $\mathbb{E}[X_i] = \mathbb{P}(A_i) = p^3$ and hence, by linearity of expectation,

$$\mathbb{E}[X] = \Theta(n^2 p^3). \tag{3}$$

Since $n^{-2/3} = o(p(n))$, it follows that $\mathbb{E}[X] \to \infty$ as $n \to \infty$. We want to prove that $\mathbb{P}(X > 0) \to 1$. It follows from Chebyshev's inequality (Theorem 20.1 in the notes) that, whenever $\mathbb{E}[X] \to \infty$, a sufficient condition for

$\mathbb{P}(X > 0) \to 1$ is that Var$(X) = o((\mathbb{E}[X])^2)$. Hence, by (3), it suffices to prove that

$$\text{Var}(X) = o(n^4 p^6). \tag{4}$$

From the general second moment method, we have

$$\text{Var}(X) = \sum_i \text{Var}(X_i) + \sum_{i \neq j} \text{Cov}(X_i,\, X_j). \tag{5}$$

Since X_i is an indicator, Var$(X_i) \leq \mathbb{E}[X_i]$ and so the first sum is at most $\mathbb{E}[X] = \Theta(n^2p^3)$. The only pairs $(i,\, j)$ that contribute to the second sum are those such that the events A_i and A_j are dependent, which is the case if and only if the i:th and j:th APs share at least one common element.

CASE 1: Pairs of APs sharing one term.

It is clear that the number of such pairs is $\Theta(n^3)$, since there are $\Theta(n)$ choices for the common element, and $\Theta(n)$ choices for the common difference in each AP. Any such pair contains a total of 5 distinct elements of $\mathbb{Z}_n$, hence $\mathbb{P}(A_i \wedge A_j) = p^5$. Thus the contribution to (5) from such pairs is $\Theta(n^3p^5)$.

CASE 2: Pairs of APs sharing two terms.

The number of such pairs is $\Theta(n^2)$. For there are so many choices for the first AP in the pair, and then only $O(1)$ choices for the second AP, since a 3-term AP is completely determined by specifying two of its terms and their positions (1st, 2nd or 3rd). In any such pair there are a total of 4 distinct elements of $\mathbb{Z}_n$, hence the contribution of these pairs to (5) is $\Theta(n^2p^4)$.

Summarising, we have

$$\text{Var}(X) = \Theta(n^2p^3) + \Theta(n^2p^4) + \Theta(n^3p^5) = \begin{cases} \Theta(n^3p^5), & \text{if } \frac{p(n)}{n^{-1/2}} \to \infty, \\ \Theta(n^2p^3), & \text{otherwise}. \end{cases}$$

In any case, since $n^2p^3 \to \infty$, one easily checks that (4) holds, and we are done.

Q.8 (i) See the handout from Diestel's book.
(ii), (iii) See the Supplementary Lecture Notes for Week 51.