Solutions to Exam 20-12-08

Q.1 All congruences below are modulo 31. $\mathbb{Z}_{31}^*$ is a cyclic group of order 30. Thus the possible orders of an element in this group are all the divisors of 30, namely 1,2,3,5,6,10,15 and 30. A primitive root has order 30. We first find one by brute force search. 2 doesn't work, since one can check that $2^{15} \equiv 1$. However, 3 works. One can check that

$$3^2 \equiv 9, \quad 3^3 \equiv -4, \quad 3^5 \equiv -5, \quad 3^6 \equiv 16, \quad 3^{10} \equiv -6, \quad 3^{15} \equiv -1. \qquad (1)$$

All the primitive roots are then given by

$$\{3^i \pmod{31} : 1 \leq i \leq 30 \text{ and } \mathrm{GCD}(i, 30) = 1\}. \qquad (2)$$

There are $\phi(30) = 8$ possible values for i, namely $i = 1, 7, 11, 13, 17, 19, 21, 23$. One then computes (with the help of the already computed (1) , for example)

$$3^7 \equiv 17, \quad 3^{11} \equiv 13, \quad 3^{13} \equiv 24, \quad 3^{17} \equiv 22,$$
$$3^{19} \equiv 12, \quad 3^{23} \equiv 11, \quad 3^{29} \equiv 21.$$

Thus the primitive roots modulo 31 are 3,11,12,13,17,21,22 and 24.

Q.2 Theorem 4.1 in the lecture notes.

Q.3 Theorem 12.4 in the lecture notes.

Q.4 The first part of Theorem 6.1 in the lecture notes (down as far as eq. (6.27)).

Q.5 (i) By squaring $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ and rearranging terms (valid when $\mathrm{Re}(s) > 1$), one directly obtains the relationship

$$[\zeta(s)]^2 = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}. \qquad (3)$$

(ii) We rewrite the sum, by considering the fact that a number $m \in \{1, ..., x\}$ appears once in the sum for each multiple of itself up to x, and hence appears $\lfloor x/m \rfloor$ times in all. Hence

$$\sum_{n=1}^{x} d(n) = \sum_{m=1}^{x} \lfloor x/m \rfloor. \qquad (4)$$

Now, trivially, $\lfloor x/m \rfloor = x/m + O(1)$ and thus

$$\sum_{m=1}^{x} \lfloor x/m \rfloor = \sum_{m=1}^{x} \left[\frac{x}{m} + O(1)\right] = x \cdot \sum_{m=1}^{x} \frac{1}{m} + O(x). \qquad (5)$$

The last sum is $\log x + O(1)$, by a simple comparison with $\int_1^x 1/m \; dm$. Thus

$$\sum_{n=1}^{x} d(n) = x \log x + O(x) \tag{6}$$

and dividing by x gives finally

$$\frac{1}{x} \sum_{n=1}^{x} d(n) = \log x + O(1) \sim \log x. \tag{7}$$

Q.6 Theorem 10.2 in the lecture notes (proven in Lecture 16).

Q.7 (i) A special case of Theorem 17.6 in the lecture notes (proven in Lecture 18).

(ii) Proposition 17.2 in the lecture notes.

Q.8 (i) An arithmetic progression is determined by its first term a and common difference d. So consider a k-term AP in $\{1, ..., n\}$. Obviously $a \in \{1, ..., n\}$ so there are no more than n choices for a. But also $a + (k-1)d \leq n$, hence $d < n/(k-1)$ and there are less than than $n/(k-1)$ choices for d. Thus, there are certainly no more than $n \cdot \frac{n}{k-1} = \frac{n^2}{k-1}$ choices for the pair (a, d), and hence for the k-term AP.

(ii) Consider a uniformly random l-coloring of $\{1, ..., n\}$, i.e.: each number is independently colored by tossing a fair l-sided die, so that the probability that any particular number receives any particular color is $1/l$.

Let A denote a generic k-term AP in $\{1, ..., n\}$. Let $\mathscr{E}_A$ be the event that A is colored monochromatically and let X_A be the indicator of the event $\mathscr{E}_A$. Let

$$X = \sum_{A} X_A. \tag{8}$$

For any A we have

$$\mathbb{E}(X_A) = \mathbb{P}(\mathscr{E}_A) = l \cdot \left(\frac{1}{l}\right)^k = l^{-(k-1)}. \tag{9}$$

Hence, by linearity of expectation and part **(i)** we have that

$$\mathbb{E}(X) \leq \left(\frac{n^2}{k-1}\right) \cdot l^{-(k-1)}. \tag{10}$$

Hence, if

$$n < \sqrt{k-1}\, l^{\frac{k-1}{2}} \tag{11}$$

then $\mathbb{E}(X) < 1$, which in turn implies that $\mathbb{P}(X = 0) > 0$, i.e.: that there exists an l-coloring of $\{1, ..., n\}$ which yields no monochromatic k-term AP:s. This immediately implies that

$$W(k, l) \geq \sqrt{k-1}\, l^{\frac{k-1}{2}}. \tag{12}$$