Sample GCHQ Mathematics Aptitude Test

This is a sample of the GCHQ Mathematics Aptitude Test given to candidates applying for our Mathematics & Cryptography roles[1].

There will be more questions on the paper than you could expect to answer in the time limit of 90 minutes. Therefore, you are advised to read the whole paper before starting and to then focus on questions that you feel most confident on. More credit will be given for complete answers to a relatively small number of questions than for a larger number of partial attempts. All questions are weighted equally.

While this sample bears a resemblence to the test given to applicants, the subject areas covered by the two may differ substantially.

[1] https://www.gchq-careers.co.uk/departments/mathematics-and-cryptography.html

Questions

1. For a sequence $s_1, s_2, \ldots$ with entries in $\mathbb{Z}$, we say that s has the divisibility property if: for every positive $a \in \mathbb{Z}$, there exists a positive $b \in \mathbb{Z}$ such that $a|s_n$ whenever $b|n$. Let R be the set of all integer sequences having the divisibility property.

   (a) Give an example of an element of R.

   (b) Does any element of R have infinitely many terms equal to 1?

   (c) Let $s, t \in R$ and define a sequence u by

   $$u_n = s_{t_n} \text{ for all } n.$$

   Prove that the sequence u is an element of R.

2. Suppose a Knight sits on the origin $(0, 0)$ of a Cartesian plane. The Knight can move in two ways:

   - Two places right and one place up
   - One place right and two places up

   The Knight may perform these multiple times and in any order and no other moves are available. Find the smallest distance the Knight can be from the following points:

   - $P_1 = (40, 30)$.
   - $P_2 = (19, 63)$.

   Justify your reasoning.

3. A paper cup company produces conical paper cups in the following way

   - Start with a circular piece of paper of radius R.
   - Make two radial cuts to remove a sector of paper, with internal angle θ.
   - Glue together the two edges of the remaining piece formed by the cutting.

   The company produces cones that maximise the volume of liquid they contain.

   (a) Show that the volume of the cone can be expressed as

   $$V(\gamma) = \frac{1}{3}\pi R^3 (1-\gamma)^2 \sqrt{2\gamma - \gamma^2}, \text{ where } \gamma = \frac{\theta}{2\pi}$$

   (b) By finding this γ or otherwise, find the maximised volume.

   Recall that the volume of a cone with base radius r and perpendicular height h is $\frac{1}{3}\pi r^2 h$.

4. Given sets of integers X and Y, both of size n, we define the sum-set

   $$X + Y = \{x + y : x \in X, y \in Y\}$$

   (a) Prove by induction or otherwise that the smallest possible size of $X + Y$ is $2n - 1$.

   (b) Find the maximum size of $X + Y$.

5. Let $G = (V, E)$ be a connected directed graph. A directed graph is *strongly connected* if every vertex is reachable from every other vertex. That is, given any pair of vertices s, t there is a sequence of edges that may be followed starting at s and ending at t.

   (a) Let C_1 be the condition that for every vertex $v \in V$ there is at least one edge in and at least one edge out of v. Give an example to show that C_1 is not a sufficient condition for G to be strongly connected.

   (b) Let C_2 be the condition that $\forall A \subset V$, there exists some $u \in A$ and some $v \notin A$ and $(u, v) \in E$. Prove that C_2 is necessary and sufficient for G to be strongly connected.

6. Let X_i be independent continuous uniform random variables on $[0, 1]$ for $i = 1, \ldots, k$. Now let $Y = \max\{X_1, X_2, \ldots, X_k\}$

   (a) Find the cumulative distribution function for the random variable Y.

   (b) Suppose we don't know the value k but observe Y as some value α. Show that the maximum likelihood estimate for k is approximately:

$$\frac{1}{\log \frac{1}{\alpha}}$$

   Recall the cumulative distribution function is defined by $F_Y(t) = \mathbb{P}(Y \leq t)$.

7. Let $f(x) = x^6 + x^4 - 4x^2 - 4$.

   (a) Show that $f(x) = 0$ has no roots over the integers.

   (b) Show that for every prime p, $f(x) = 0$ has a solution mod p.

   You may use the fact that given prime p, Legendre symbols satisfy $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, where

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p|a \\ +1, & \text{if } a \text{ is a non-zero square modulo } p \\ -1, & \text{if } a \text{ is not a square modulo } p \end{cases}$$

8. I have a bucket of n balls, labelled 1 to n. I reach in and grab a handful of k of them at random. I do the following n times:

   - Discard the lowest-numbered ball in my hand.
   - Grab a new ball from the bucket (if there are any) at random.

   (a) What is the probability that I discard the balls in strictly increasing order?

   (b) Describe the set of possible discard sequences produced by this process for general n and k. Use this to state what possible values of k could produce the discard sequence

$$5, 1, 3, 4, 2, 6, 7, 8, 9, 10$$