Specimen exam paper

1 (a) If the most frequently occurring letter in the ciphertext is M then we guess that E → M. Since this is a Caesar cipher we guess that the encoding key is 8.

Ciphertext	O	W	W	L
numerical equivalent a	14	22	22	11
a − 8	6	14	14	3
Cleartext	G	O	O	D

(b) We first calculate $\begin{vmatrix} 2 & 23 \\ 3 & 1 \end{vmatrix} \bmod 26$

$= 2 - 3\times 23 = -67 \equiv 11 \pmod{26}$.

We now need to calculate $11^{-1} \bmod 26$.

$26 = 2\times 11 + 4$
$11 = 2\times 4 + 3$
$4 = 1\times 3 + 1$
$3 = 3\times 1 + 0$

$$\left(\begin{array}{cc|c} 1 & 0 & 11 \\ 0 & 1 & 26 \end{array}\right) \to \left(\begin{array}{cc|c} 1 & 0 & 11 \\ -2 & 1 & 4 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} 5 & -2 & 3 \\ -2 & 1 & 4 \end{array}\right) \to \left(\begin{array}{cc|c} 5 & -2 & 3 \\ -7 & 3 & 1 \end{array}\right)$$

$$\to \left(\begin{array}{cc|c} -7 & 3 & 1 \end{array}\right)$$

$(-7)\ 11 + 3(26) = 1$

$\therefore\ -7\times 11 \equiv 1 \bmod 26$

$\therefore\ \boxed{11^{-1} = 19 \bmod 26}$

The decryption matrix is therefore

$$19\begin{pmatrix}1 & -23\\ -3 & 2\end{pmatrix} = 19\begin{pmatrix}1 & 3\\ 23 & 2\end{pmatrix} = \begin{pmatrix}19 & 57\\ 437 & 38\end{pmatrix}$$

$$= \begin{pmatrix}19 & 5\\ 21 & 12\end{pmatrix}$$

Check $\begin{pmatrix}2 & 23\\ 3 & 1\end{pmatrix}\begin{pmatrix}19 & 5\\ 21 & 12\end{pmatrix} = \begin{pmatrix}2\times19+23\times21 & 2\times5+23\times12\\ 3\times19+1\times21 & 3\times5+1\times12\end{pmatrix}$

$$= \begin{pmatrix}521 & 286\\ 78 & 27\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

The ciphertext is WGTT. The numerical equivalent is

22 6 19 19. We calculate

$$\begin{pmatrix}19 & 5\\ 21 & 12\end{pmatrix}\begin{pmatrix}22\\ 6\end{pmatrix} = \begin{pmatrix}448\\ 534\end{pmatrix} = \begin{pmatrix}6\\ 14\end{pmatrix} = \begin{pmatrix}G\\ O\end{pmatrix}$$

$$\begin{pmatrix}19 & 5\\ 21 & 12\end{pmatrix}\begin{pmatrix}19\\ 19\end{pmatrix} = \begin{pmatrix}456\\ 627\end{pmatrix} = \begin{pmatrix}14\\ 3\end{pmatrix} = \begin{pmatrix}O\\ D\end{pmatrix}$$

GOOD

(c)

We have to calculate 2415^{29} mod 2701.

$29 = 16 + 13 = 16 + 8 + 5 = 16 + 8 + 4 + 1$

2415^1 *	mod 2701
2415^2	766
2415^4	639 *
2415^8	470 *
2415^{16}	2119 *

$2119 \times 470 \times 639 \times 2415$

$= 1962 \times 639 \times 2415$

$= 454 \times 2415$

$= 2505$

2 (a) $C \subseteq \mathbb{Z}_2^n$ is a <u>linear code</u> if

$\underline{u}, \underline{v} \in C \Rightarrow \underline{u} + \underline{v} \in C$ and $\underline{0} \in C$.

The minimum distance d of a code = minimum non-zero weight in a linear code.

If t is the maximum number of errors that the code can correct then

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

Suppose that the code has minimum distance d.

Then by the above there is a codeword $\underline{u}$ of weight d.

By the definition of the parity check matrix $H\underline{u}^T = \underline{0}$

Let the non-zero entries of $\underline{u}$ be $i_1, i_2, \ldots, i_d$.

Let the corresponding columns of H be $\underline{h}_{i_1}, \ldots \underline{h}_{i_d}$.

Then $\underline{h}_{i_1} + \underline{h}_{i_2} + \ldots + \underline{h}_{i_d} = \underline{0}$.

Thus we have shown that d columns of H are linearly dependent.

To prove the second assertion, suppose that any $d-1$ columns of H were linearly dependent. Say $\underline{h}_{j_1} + \ldots \underline{h}_{j_{d-1}} = \underline{0}$.

Let $\underline{v}$ be the vector whose only non-zero entries are at $j_1, \ldots, j_{d-1}$.

Then $H\underline{v}^T = \underline{0}$. This implies that $\underline{v}$ is in the code and its weight is $d-1$.

This contradicts the fact that the minimum weight is d.

(b) We find a basis for the nullspace of the given matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} t \\ u \\ v \\ w \\ x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$\Rightarrow$

$$\begin{aligned} t + y + z &= 0 \\ u + x + z &= 0 \\ v + x + y &= 0 \\ w + x + y + z &= 0 \end{aligned}$$

$x = \alpha$, $y = \beta$, $z = \gamma$

$$\begin{aligned} t &= \beta + \gamma \\ u &= \alpha + \gamma \\ v &= \alpha + \beta \\ w &= \alpha + \beta + \gamma \end{aligned} \Rightarrow \begin{pmatrix} \beta+\gamma \\ \alpha+\gamma \\ \alpha+\beta \\ \alpha+\beta+\gamma \\ \alpha \\ \beta \\ \gamma \end{pmatrix}$$

$$\left\{ \alpha \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} : \alpha, \beta, \gamma \in \mathbb{Z}_2 \right\}$$

Thus

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Observe that $\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$

Thus some 3 columns are linearly dependent.

But 2 columns can't be linearly dependent ($\Leftrightarrow$ they are equal and all columns are distinct.

Thus the min. distance is 3.

3(a)

Base step: $f_3 = 3$, $\phi^{3-2} = \phi = \frac{1}{2}(1+\sqrt{5}) \approx 1.62$

$\therefore f_3 > \phi$.

$f_4 = 5$, $\phi^{4-2} = \phi^2 = \phi + 1 \simeq 2.62$

$\therefore f_4 > \phi^2$.

IH Formula holds for $n-1$ and n.

We now prove it holds for $n+1$:

$f_{n+1} = f_n + f_{n-1} > \phi^{n-2} + \phi^{n-3} = \phi^{n-3}(\phi+1) = \phi^{n-3}\phi^2 = \phi^{n-1}$.

as required — using the fact that $\phi^2 = \phi + 1$.

We have that $b \geq f_{n+1}$ and so by the above $b > \phi^{n-1}$.

Take $\log_{10}$'s of both sides to get

$$\log_{10}(b) > (n-1)\log_{10}(\phi)$$

But $\log_{10}(\phi) > 1/5$. Thus $\log_{10}(b) > \frac{1}{5}(n-1)$.

We have that $k = \lfloor \log_{10}(b) \rfloor + 1$.

Thus $k > \log_{10}(b)$. It follows that $k > \frac{1}{5}(n-1)$.

Thus $5k \geq n$.

3(b) We have that

$$\phi(n) = \phi(p_1^{e_1}) \dots \phi(p_m^{e_m}).$$

We claim that $\phi(p^e) = p^e - p^{e-1}$.

Let a be $1 \le a \le p^e$ and not coprime to p^e.
Then $p \mid a$. Thus $a = pb$ where $1 \le b \le p^{e-1}$.
It follows that $\phi(p^e) = p^e - p^{e-1} - p^{e-1}(p-1)$

$$\therefore \phi(n) = p_1^{e_1-1}(p_1-1) \dots\dots p_m^{e_m-1}(p_m-1)$$

$$= p_1^{e_1-1} \dots p_m^{e_m-1}(p_1-1)\dots(p_m-1)$$

$$= \frac{n}{p_1 \dots p_m}(p_1-1)\dots(p_m-1)$$

$$= n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_m}\right).$$

$n = pq = \underline{198,931}$.

$\phi(n) = (p-1)(q-1) = 198,000$

$\therefore pq - p - q + 1 = 198,000$

$\therefore -p-q+1 = 198,000 - 198,931$

$\therefore p+q-1 = 198,931 - 198,000 = 931$

$\therefore \underline{p+q = 932}$

$$(x-p)(x-q) = x^2 - xq - px + pq$$
$$= x^2 - (p+q)x + pq$$

∴ Our p and q are roots of

$$x^2 - 932x + 198,931 = 0$$

$$(x - 466)^2 - 466^2 = x^2 - 932x$$

$$\therefore (x-466)^2 - 466^2 + 198,931 = 0$$

$$(x-466)^2 - 18225 = 0$$

$$(x-466)^2 = 18,225$$

$$x - 466 = \pm 135$$

$$\therefore x = 466 + 135, \quad 466 - 135$$
$$= 601, 331$$

3 (i) Assume only finitely many $p_1, \ldots, p_n$.

Put $N = p_1 \cdots p_n + 1$.

Smallest no ≥ 2 dividing N is a prime but it cannot be any of the primes in the above list. Contradiction.

PNT:

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

$$\therefore \pi(x) \simeq \frac{x}{\ln(x)}$$

Let p be a prime with 150 digits.

Then $10^{149} < p < 10^{150}$

$$\therefore \#\text{primes} = \frac{10^{150}}{\ln(10^{150})} - \frac{10^{149}}{\ln(10^{149})}$$

$$= 10^{149}\left(\frac{10}{150\ln(10)} - \frac{1}{149\ln(10)}\right)$$

$$= \underline{1.38 \times 10^{148} \text{ primes}}$$

4. Lagrange's theorem states that if G is a finite group and $H \leq G$ then $|H| \mid |G|$. [4]

We shall work with right cosets Hg of H in G.

Two key facts need to be proved:

(1) $|Hg| = |H| \quad \forall g \in G$. This is proved by means of the bijection $H \xrightarrow{\alpha} Hg$ given by $\alpha(h) = hg$. [4]

(2) $Hg_1 \cap Hg_2 \neq \emptyset \Rightarrow Hg_1 = Hg_2$.
This is proved by taking $a = h_1 g_1 = h_2 g_2 \in Hg_1 \cap Hg_2$ and rewriting to get $g_1 = (h_1^{-1} h_2) g_2$ where $h_1^{-1} h_2 \in H$ because $H \leq G$. This shows that $Hg_1 \subseteq Hg_2$ and the reverse inclusion follows by symmetry. [4]

It then follows that $G/H = \{Hg : g \in G\}$ is a partition of G and that all the blocks have the same size. [2]

The order of $g = |\langle g \rangle|$. If G is finite then $\exists m \neq n$; $g^m = g^n$. Deduce that $\exists d > 0$ s.t. $g^d = 1$. Choose smallest such no. For any n $n = qd + r$ where $0 \leq r < d$ we have $g^n = g^{qd+r} = (g^d)^q g^r = g^r$.
$\therefore \langle g \rangle = \langle g^0, \ldots g^{d-1} \rangle$.

Let G be a finite group and let $g \in G$. Then

$$g^{|G|} = 1.$$

Let $\langle g \rangle$ be the cyclic subgroup generated by g.

Then the order of g is $|\langle g \rangle|$ - smallest non-zero d s.t. $g^d = 1$.

It follows that $d \mid |G|$.

$\therefore |G| = de$

so $g^{|G|} = g^{de} = (g^d)^e = 1$.

FLT states that if p is a prime and $p \nmid a$

then

$$a^{p-1} \equiv 1 \pmod{p}.$$

We work in the group U_p which has order $p-1$

$\therefore p \nmid a \iff [a]$ is invertible

$\therefore$ By the above $[a]^{p-1} = [1]$

then $a^{p-1} \equiv 1 \pmod{p}$.

5(a) Let $C \subseteq A^*$ be a code where $|A| = a$.

The parameters of C is the set of numbers

$(n_1, n_2, \ldots, n_M)$ such that

n_i = # codewords in C of length i

(thus M is the max. length of a codeword in C).

We put

$$K = \sum_{i=1}^{M} \frac{n_i}{a^i}$$

, the Kraft-McMillan number of the code

Claim:

If $K \leq 1$ then there is a prefix a-ary code with these parameters

Proof

$$\sum_{i=1}^{M} \frac{n_i}{a^i} = \frac{n_1}{a^1} + \frac{n_2}{a^2} + \frac{n_3}{a^3} + \ldots + \frac{n_M}{a^M} \leq 1$$

$$\Rightarrow \quad \frac{n_1}{a} < 1, \quad \frac{n_1}{a} + \frac{n_2}{a^2} < 1,$$

$$\frac{n_1}{a} + \frac{n_2}{a^2} + \frac{n_3}{a^3} < 1, \quad \ldots\ldots$$

$$\Rightarrow \quad \underline{n_1 < a}, \quad a n_1 + n_2 < a^2 \quad n_3 < a(a^2 - n_1 a - n_2)$$

$$n_2 < a^2 - a n_1,$$

$$\underline{n_2 < a(a - n_1)} \qquad \text{etc}$$

We now construct a prefix code with these parameters

- Since $n_1 < a$ we may choose n_1 letters for a. This leaves $a - n_1$ letters unused.
- There are now $a(a-n_1)$ strings of length 2 we may use and since $n_2 < a(a-n_1)$ we may choose n_2 of them. This leaves $a(a-n_1) - n_2 = a^2 - an_1 - n_2$.
- There are now $a(a^2 - an_1 - n_2)$ strings of length 3 we may use and since $n_3 < a(a^2 - an_1 - n_2)$ we may choose n_3 of them.

etc

5(b)

letter	probability (f)
a	$\frac{2}{52}$
b	$\frac{3}{52}$
c	$\frac{5}{52}$
d	$\frac{8}{52}$
e	$\frac{13}{52}$
f	$\frac{21}{52}$

N.B. In this course, we shall only be interested in base 2 entropy

$2 + 3 + 5 + 8 + 13 + 21 = \underline{\underline{52}}$

$$H_2(f) = \sum_{i=1}^{m} p_i \log_2 (1/p_i)$$

$$= \frac{1}{\log_{10}(2)} \sum_{i=1}^{m} p_i \log_{10} (1/p_i)$$

$2^{\log_2(x)} = x$

$\log_{10}(x) = \log_2(x) \log_{10}(2)$

$\therefore \log_2(x) = \frac{\log_{10}(x)}{\log_{10}(2)}$

$$= \frac{1}{\log_{10}(2)} \left[\frac{2}{52} \log_{10}\left(\frac{52}{2}\right) + \frac{3}{52} \log_{10}\left(\frac{52}{3}\right) + \frac{5}{52} \log_{10}\left(\frac{52}{5}\right) + \frac{8}{52} \log_{10}\left(\frac{52}{8}\right) + \frac{13}{52} \log_{10}\left(\frac{52}{13}\right) + \frac{21}{52} \log_{10}\left(\frac{52}{21}\right) \right]$$

$$= \frac{1}{52 \log_{10}(2)} \left[2(\log 52 - \log 2) + 3(\log 52 - \log 3) + 5(\log 52 - \log 5) + 8(\log 52 - \log 8) + 13(\log 52 - \log 13) + 21(\log 52 - \log 21) \right]$$

$$= \frac{1}{52 \log_{10}(2)} \Big[(2+3+5+8+13+21) \log 52 - (2\log 2 + 3\log 3 + 5\log 5 + 8\log 8 + 13\log 13 + 21\log 21) \Big]$$

$$= \frac{1}{52 \log_{10}(2)} \Big[52 \log 52 - 55.000862\ldots \Big]$$

$$= \frac{1}{52 \log_{10}(2)} \Big[89.23217387 - 55.000862\ldots \Big]$$

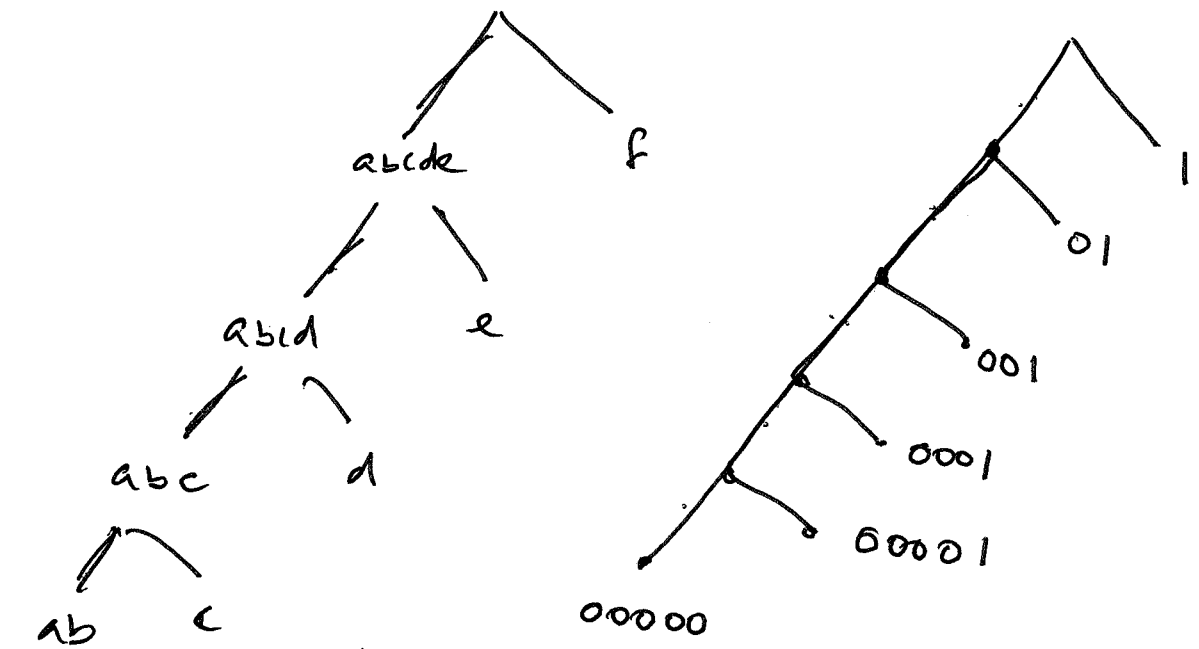
$$= \frac{1}{52 \log_{10}(2)} \; 34.23131143$$

$$= \underline{\underline{2.18681}}$$

a 2
b 3
c 5
d 8
e 13
f 21

→ ab 5, c 5 → abc 10, d 8 → abcd 18, e 13, f 21

→ abcde 31, f 21 → abcdef 52



letter	code
a	00000
b	00001
c	0001
d	001
e	01
f	1

We now Compute the averge word length

$$= 5 \times \frac{2}{52} + 5 \times \frac{3}{52} + 4 \times \frac{5}{52} + 3 \times \frac{8}{52}$$

$$+ 2 \times \frac{13}{52} + 1 \times \frac{21}{52}$$

$$= \frac{1}{52}(10 + 15 + 20 + 24 + 26 + 21)$$

$$= \frac{116}{52} = \underline{\underline{2.2308}}$$

$$2.2308 \geq 2.18681$$

Which is true in general

– final part of the question