TMA 055 : Diskret matematik

Tentamen 171005

Lösningar

F.1 (i) Det är lätt att se att $\mathrm{SGD}(37, 98) = 1$ eftersom 37 är ett primtal. Därmed vet vi att inversen till 37 (mod 98) finns, dvs kongruensen HAR en lösning. Vi hittar inversen genom Euklides algoritm. Framåt får vi

$$\begin{aligned} 98 &= 2 \cdot 37 + 24, \\ 37 &= 1 \cdot 24 + 13, \\ 24 &= 1 \cdot 13 + 11, \\ 13 &= 1 \cdot 11 + 2, \\ 11 &= 5 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Bakåt får vi då

$$\begin{aligned} 1 &= 11 - 5 \cdot 2 \\ &= 11 - 5 \cdot (13 - 11) \\ &= 6 \cdot 11 - 5 \cdot 13 \\ &= 6 \cdot (24 - 13) - 5 \cdot 13 \\ &= 6 \cdot 24 - 11 \cdot 13 \\ &= 6 \cdot 24 - 11 \cdot (37 - 24) \\ &= 17 \cdot 24 - 11 \cdot 37 \\ &= 17 \cdot (98 - 2 \cdot 37) - 11 \cdot 37 \\ &= 17 \cdot 98 - 45 \cdot 37. \end{aligned}$$

Från den sista raden härleder vi att lösningen till kongruensen är $x \equiv -45 \pmod{98}$, eller om du föredrar positiva tal, $x \equiv 53 \pmod{98}$.

(ii) $98 = 2 \cdot 7^2$ so $\phi(98) = \phi(2) \cdot \phi(7^2) = (2-1)(7^2 - 7) = 1 \cdot 42 = 42$. Hence, Euler's Theorem states that, if n is an integer relatively prime to 98, then

$$n^{42} \equiv 1 \pmod{98}.$$

Note that both 3 and 5 are relatively prime to 98. Hence (all congruences are modulo 98)

$$3^{170} = (3^{42})^4 \cdot 3^2 \equiv 1^4 \cdot 9 \equiv 9,$$

and

$$5^{129} = (5^{42})^3 \cdot 5^3 \equiv 1^3 \cdot 125 \equiv 27.$$

Thus,

$$(3^{170} + 5^{129} + 1)^{83} \equiv (9 + 27 + 1)^{83} = 37^{83}.$$

Since 37 is a prime, it is also relatively prime to 98, so we can apply Euler's theorem again. Thus

$$37^{83} = \equiv (37^{42})^2 \cdot 37^{-1} \equiv 1^2 \cdot 37^{-1} \equiv 37^{-1}.$$

And in part **(i)** we have already computed that $37^{-1} \equiv 53 \pmod{98}$.

So the answer is 53.

(iii) 19 is a prime, so $\mathbf{Z}_{19}$ is a field, so all the usual manipulations of algebraic equations are valid here. In particular, we can use the formula for the roots of a quadratic equation to deduce that the solutions to the congruence are given by

$$x \equiv \frac{3 \pm \sqrt{3^2 - 4 \cdot 2 \cdot 10}}{2 \cdot 2} \pmod{19},$$

that is,

$$x \equiv 4^{-1} \left[3 \pm \sqrt{-71}\right] \pmod{19}.$$

Now one sees immediately that, modulo 19, $4^{-1} \equiv 5$ and $-71 \equiv 5$, so we can simplify to

$$x \equiv 5(3 \pm \sqrt{5}) \pmod{19}.$$

By exhaustive search, we find that $(\pm 9)^2 \equiv 5 \pmod{19}$. Hence, the solution becomes

$$x \equiv 5(3 \pm 9) \equiv 15 \pm 45 \equiv 15 \pm 7 \equiv 22 \text{ or } 8 \equiv 3 \text{ or } 8 \pmod{19}.$$

F.2 The homogeneous equation is

$$u_n - 6u_{n-1} + 9u_{n-2} = 0.$$

The characteristic equation for this is

$$x^2 - 6x + 9 = 0,$$

which factorises as

$$(x-3)^2 = 0,$$

and hence has the repeated root $x = 3$. Hence the general solution to the homogeneous equation is

$$u_n^h = (C_1 + C_2 \cdot n) \cdot 3^n.$$

Since 3^n and $n \cdot 3^n$ are already solutions to the homogeneous equation, our guess for a particular solution should have the form

$$u_n^p = A \cdot n^2 \cdot 3^n + B.$$

Substituting into the recurrence relation, the requirement on A is that

$$A \cdot \left[n^2 3^n - 6(n-1)^2 3^{n-1} + 9(n-2)^2 3^{n-2} \right] = 3^n, \tag{1}$$

whereas the requirement on B is that

$$B - 6B + 9B = 1. \tag{2}$$

From (1) we deduce that $A = 1/2$ and from (2) that $B = 1/4$. Hence the general solution to our recurrence relation is

$$u_n = \left(C_1 + C_2 n + \frac{n^2}{2} \right) \cdot 3^n + \frac{1}{4}.$$

It remains to insert the initial conditions :

$$n = 0 \Rightarrow u_0 = 1 = C_1 + \frac{1}{4},$$
$$n = 1 \Rightarrow u_1 = 1 = 3\left(C_1 + C_2 + \frac{1}{2} \right) + \frac{1}{4}.$$

Solving, we obtain $C_1 = 3/4$, $C_2 = -1$. Hence the final answer is

$$u_n = \left(\frac{3}{4} - n + \frac{n^2}{2}\right) \cdot 3^n + \frac{1}{4}.$$

F.3 (i) Clearly, $\chi(G) \geq 3$ since G contains many triangles. In fact, $\chi(G) \geq 4$ because the vertex h is at the centre of a wheel formed by d, g, i, f, h. This 5-cycle requires three colours, and then a fourth is needed for h. Similarly, b is at the centre of a 5-cycle formed by v, a, d, e, c. On the other hand, the graph is plane, hence $\chi(G) \leq 4$, by the Four-Colour Theorem. It follows that $\chi(G) = 4$.

If we apply the greedy algorithm with the nodes ordered so that v is first, and thereafter alphabetically, then we get a 4-coloring, namely (the colors are $1, 2, 3, 4$)

v	1	f	1
a	2	g	2
b	3	h	3
c	2	i	4
d	1	j	2
e	4	w	1

(ii) Apply Dijkstra's algorithm to build up the following tree

Step	Choice of edge	Labelling
1	$\{v, b\}$	$b := 3$
2	$\{v, a\}$	$a := 4$
3	$\{b, e\}$	$e := 4$
4	$\{e, h\}$	$h := 6$
5	$\{v, c\}$	$c := 7$
6	$\{e, d\}$	$d := 7$
7	$\{e, f\}$	$f := 8$
8	$\{d, g\}$	$g := 9$
9	$\{f, i\}$	$i := 11$
10	$\{f, j\}$	$j := 14$
11	$\{i, w\}$	$w := 17$

Hence the shortest path from v to w is the path $v \to b \to e \to f \to i \to w$ and has length 17.

F.4 (i) Firstly, one must decide in which of the four suits there are at least three cards (note that, since there are only 5 cards in total, there is no overlapping of these decisions). Then it reamins to decide whether the hand contains 3,4 or 5 cards in the chosen suit. This leads to the following formula for the total number of admissable hands :

$$4 \cdot \left[\binom{13}{3}\binom{39}{2} + \binom{13}{4}\binom{39}{1} + \binom{13}{5} \right].$$

(ii) Since p is a prime, each number amongst $1, 2, ..., p-1$ has an inverse modulo p. Which numbers are their own inverses ? Well, $x \equiv x^{-1} \pmod{p} \Leftrightarrow x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv \pm 1 \pmod{p}$, so only 1 and $p-1$ are their own inverses.

So now the idea is the following. The numbers in the product comprising $(p-1)!$, other than 1 and $p-1$, can be grouped in inverse-pairs, such that the product of each pair is congruent to 1 (mod p). It follows that

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}, \quad \text{v.s.v.}$$

(iii) Clearly, $D_1 = C_1 = 1$, since the only sequence of length 0 is the empty sequence, which satisfies any property you like. It now suffices to show that the numbers D_n satisfy the same recurrence relation as the Catalan numbers, i.e.: that, for every $n \geq 1$,

$$D_n = \sum_{m=1}^{n} D_{m-1} D_{n-m}, \tag{3}$$

where I define $D_0 = 1$ (note the $m = 1$ and $m = n$ terms), for the sake of consistency with the Catalan recurrence. It will be convenient to divide up the sum on the HL of (3) in the three intervals $m = 1$, $2 \leq m \leq n-1$ and $m = n$, and rewrite as

$$D_n = D_{n-1} + \sum_{m=2}^{n-1} D_{m-1} D_{n-m} + D_{n-1}. \tag{4}$$

To prove (4), consider an admissable sequence $a_1 \cdots a_{n-1}$ of length $n-1$. Suppose some partial sum equals zero, and if so let m tbe the first index such that

$$\sum_{i=1}^{m} a_i = 0. \tag{5}$$

Thus m can be any integer among $1, 2, ..., n-1$. Consider the two subsequences $a_1 \cdots a_m$ and $a_{m+1} \cdots a_{n-m}$. The latter must satisfy exactly the same conditions as the original sequence. Since it has length $n-1-m$, there are D_{n-m} choices for it. No partial sum of the subsequence $a_1 \cdots a_m$ can equal zero. Thus $a_1 = 1$ (no choice there !). If $m = 1$, this already gives as D_{n-1} the number of possibilites for the full sequence in this case, which is the first term on the HL of (4). If $2 \leq m \leq n-1$ then consider the subsequence $a_2 \cdots a_m$. By (5), a_m is uniquely determined by the previous terms. Since $a_1 = 1$ and m is minimal s.t. (5) is satisfied, we see that the subsequence $a_2 \cdots a_{m-1}$ must satisfy exactly the same conditions as at the outset. Since it has length $m-2$, there are D_{m-1} possibilities for it. By the MP, for each $m \in \{2, ..., n-1\}$, there are thus $D_{m-1}D_{n-m}$ possibilities for the full sequence. This gives the middle sum on the HL of (4).

Finally, the last term on the HL of (4) is just the number of length-$(n-1)$ sequences for which no partial sum equals zero (i.e.: (5) is not satisfied for any $m \in \{1, ..., n-1\}$). By the same argument as that just given, this forces $a_1 = 1$ and the sequence $a_2 \cdots a_{n-1}$, which has length $n-2$, to satisfy exactly the same conditions as the original sequence. Hence, there are D_{n-1} possibilities for it, as required.