

## Inlämningsuppgift 2 : Lösningar

**Q.1** The homogeneous equation is

$$2a_n - 9a_{n-1} + 4a_{n-2} = 0.$$

The characteristic equation for this is

$$2x^2 - 9x + 4 = 0,$$

which factorises as

$$(2x - 1)(x - 4) = 0,$$

and hence has the two roots  $x = 1/2$ ,  $x = 4$ . Hence the general solution to the homogeneous equation is

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

Since  $4^n$  is already a solution to the homogeneous equation, our guess for a particular solution should have the form

$$a_n^p = A \cdot n \cdot 4^n + Bn + C.$$

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

$$A \cdot [2n4^n - 9(n-1)4^{n-1} + 4(n-2)4^{n-2}] = 4^n, \quad (1)$$

whereas the requirement on  $B$  and  $C$  is that

$$2[Bn + C] - 9[B(n-1) + C] + 4[B(n-2) + C] = n. \quad (2)$$

From (1) we deduce that  $A = 4/7$ . From (2) we deduce that  $B = -1/3$ ,  $C = -1/9$ . Hence the general solution to our recurrence relation is

$$a_n = C_1 \cdot \left(\frac{1}{2}\right)^n + C_2 \cdot 4^n + \frac{n}{7} \cdot 4^{n+1} - \frac{n}{3} - \frac{1}{9}.$$

It remains to insert the initial conditions :

$$\begin{aligned} n = 0 &\Rightarrow a_0 = 1 = C_1 + C_2 - \frac{1}{9}, \\ n = 1 &\Rightarrow a_1 = 1 = \frac{1}{2}C_1 + 4C_2 + \frac{16}{7} - \frac{1}{3} - \frac{1}{9}. \end{aligned}$$

Solving, we obtain  $C_1 = 74/49$ ,  $C_2 = -176/441$ . Hence the final answer is

$$a_n = \frac{74}{49} \cdot \left(\frac{1}{2}\right)^n - \frac{176}{441} \cdot 4^n + \frac{n}{7} \cdot 4^{n+1} - \frac{n}{3} - \frac{1}{9}.$$

**Q.2** Fix  $n \geq 0$ . We describe an explicit 1-1 mapping from the set of all Dyck paths of length  $2n$  to the set of Dyck paths of length  $2n + 2$  which contain no peaks of height two. Let  $\mathcal{P}$  be a Dyck path of length  $2n$ . We map  $\mathcal{P}$  to the path  $\mathcal{P}^*$  of length  $2n + 2$  as follows :

STEP 1 : Let  $\mathcal{P}_1$  be the path of length  $2n + 2$  whose first two steps are up-down, and whose remaining  $2n$  steps coincide with those of  $\mathcal{P}$ .

STEP 2 : The path  $\mathcal{P}_1$  has at least one peak of height one, by construction. Let there be  $k$  peaks of height one. These divide the remainder of the path into  $k$  pieces, one between each pair of consecutive height-one peaks, and one after the last such peak. Note that some of the pieces could be empty (happens if two height-one peaks immediately follow one another). Call the pieces  $\mathcal{P}_{1,1}, \dots, \mathcal{P}_{1,k}$ . Now replace each piece  $\mathcal{P}_{1,i}$  by a path  $\mathcal{P}_i^*$ , which consists of an up-step, followed by the steps of  $\mathcal{P}_{1,i}$ , followed by a down-step. The path  $\mathcal{P}^*$  is now just the concatenation of the  $\mathcal{P}_i^*$ . Note that, by definition, each segment  $\mathcal{P}_{1,i}$  has no peaks at height one, hence no segment  $\mathcal{P}_i^*$  has any peaks at height two, and thus the same is true of the path  $\mathcal{P}^*$ .

**Q.3** We show that the  $E_n$  satisfy the same recurrence relation as the Catalan numbers, namely that  $E_0 = 1$  and that,

$$\forall n \geq 1, \quad E_n = \sum_{m=1}^n E_{m-1} E_{n-m}. \quad (3)$$

That  $E_0 = 1$  is obvious, so it remains to prove (3). Call the  $2n$  points  $p_1, \dots, p_{2n}$ , ordered from left to right. Suppose  $p_1$  is joined to  $p_t$ . That no arcs can cross means that the points  $p_2, \dots, p_{t-1}$  have to be paired off amongst themselves, and not with any of the points  $p_{t+1}, \dots, p_{2n}$ . In particular, this means that  $t$  is even, hence  $t = 2m$  for some  $1 \leq m \leq n$ .

Fix a choice of  $m$ . Then  $p_2, \dots, p_{2m-1}$  constitute  $2m - 2$  points, which must be paired off according to the same rules as at the outset so, by definition, there are  $E_{m-1}$  ways to do this. Similarly, the points  $p_{2m+1}, \dots, p_{2n}$  must be paired off, and this can be done in  $E_{n-m}$  ways. Hence, by the

multiplication principle there are, for a fixed  $m$ ,  $E_{m-1}E_{n-m}$  possible configurations, and this proves (3).

**Q.4** The given number has prime factorisation

$$97111014 = 2 \times 3 \times 7 \times 11 \times 13 \times 19 \times 23 \times 37.$$

The important point is that no prime factor is repeated. There are 8 of them in total. Hence, the number of ways of writing 97111014 as a product of four numbers greater than one is just the number of ways of grouping these 8 primes into 4 groups. By definition, this is just the Stirling number  $S(8, 4)$  (the primes are ‘not identical’, as the way in which they’re grouped determines what the 4 factors are, whereas the groups ARE ‘identical’, since the ordering of the 4 factors is being ignored).

Stirling numbers can be computed by repeated use of the recurrence relation for them, which you recall is

$$S(n, k) = S(n - 1, k - 1) + k \cdot S(n - 1, k), \quad (4)$$

with initial condition  $S(1, 1) = 1$ . Now one just needs to compute. If one cheats a little (!) one can look at Table 12.1.1 in Biggs, which gives the seventh row of the Stirling triangle ( $n = 7$ ) as

$$1 \quad 63 \quad 301 \quad 350 \quad 140 \quad 21 \quad 1$$

By (4) we then have

$$S(8, 4) = S(7, 3) + 4 \cdot S(7, 4) = 301 + 4 \cdot 350 = 1701.$$

**Q.5** Konstatera att  $\text{SGD}(18, 47) = 1$  eftersom 47 är ett primtal. Därför vet vi att det finns heltal  $x_0, y_0$  så att

$$18x_0 + 47y_0 = 1. \quad (5)$$

Vi hittar först en lösning till (5) genom att köra Euklides algoritm fram och tillbaka. Framåt får vi

$$\begin{aligned} 47 &= 2 \cdot 18 + 11, \\ 18 &= 1 \cdot 11 + 7, \\ 11 &= 1 \cdot 7 + 4, \\ 7 &= 1 \cdot 4 + 3, \\ 4 &= 1 \cdot 3 + 1. \end{aligned}$$

Bakåt får vi då

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) \\ &= 2 \cdot 4 - 7 \\ &= 2 \cdot (11 - 7) - 7 \\ &= 2 \cdot 11 - 3 \cdot 7 \\ &= 2 \cdot 11 - 3 \cdot (18 - 11) \\ &= 5 \cdot 11 - 3 \cdot 18 \\ &= 5 \cdot (47 - 2 \cdot 18) - 3 \cdot 18 \\ &= 5 \cdot 47 - 13 \cdot 18. \end{aligned}$$

Därmed har vi hittat lösningen  $x_0 = -13$ ,  $y_0 = 5$ . Genom att multiplicera dessa med 3000 så får vi en lösning  $(x_1, y_1)$  till

$$18x + 47y = 3000, \quad (6)$$

nämligen  $x_1 = -39000$ ,  $y_1 = 15000$ . Den allmänna lösningen till (6) ges då av

$$x = -39000 + 47n, \quad (7)$$

$$y = 15000 - 18n \quad (8)$$

där  $n$  är ett godtyckligt heltal. Vi är nu intresserade av lösningar för vilka både  $x > 0$  och  $y > 0$ .

Å ena sidan

$$x > 0 \Leftrightarrow -39000 + 47n > 0 \Leftrightarrow 47n > 39000 \Leftrightarrow n \geq 830. \quad (9)$$

Å andra sidan

$$y > 0 \Leftrightarrow 15000 - 18n > 0 \Leftrightarrow 18n < 15000 \Leftrightarrow n \leq 833. \quad (10)$$

Från (9) och (10) får vi fyra möjligheter för  $n$ , nämligen  $n = 830, 831, 832, 833$ . Till sist sätter vi in dessa fyra värden i (7) och (8) så får vi fyra lösningar :

$$x = 10, y = 60 \quad x = 53, y = 42 \quad x = 100, y = 24, \quad x = 147, y = 6.$$

**Q.6** Fix  $n$ . Let  $d$  be a positive integer which divides both  $n! + 1$  and  $(n + 1)! + 1$ . We must show that  $d = 1$ . Since  $d$  divides  $n! + 1$ , it also

divides  $(n + 1)$ -times this number, which is just  $(n + 1)! + (n + 1)$ . It also divides  $(n + 1)! + 1$ , so it divides the difference between these latter two, namely  $n$ . But  $n!$  is a multiple of  $n$ , so  $d$  also divides  $n!$ . But now we have that  $d$  divides both  $n!$  and  $n! + 1$ , from which it follows that it divides their difference, namely 1. Thus  $d = 1$ , v.s.v.

**Q.7** The point is that the expression  $n^4 + n^2 + 1$  can be factorised. Namely, we have that

$$n^4 + n^2 + 1 = (n^4 + 2n^2 + 1) - n^2 = (n^2 + 1)^2 - n^2 = (n^2 + 1 - n)(n^2 + 1 + n).$$

Hence if  $n^4 + n^2 + 1$  is to be prime, then one of these factors must equal  $\pm 1$ . But both factors are positive for all  $n$ , the first one equals 1 for  $n = 0, \pm 1$  and the second one equals 1 only for  $n = 0$ . Thus  $n^4 + n^2 + 1$  is prime if and only if  $n = \pm 1$ .

**Q.8** Let

$$\begin{aligned} a &= p_1^{\alpha_1} \cdots p_k^{\alpha_k}, \\ b &= p_1^{\beta_1} \cdots p_k^{\beta_k}, \end{aligned}$$

where each  $\alpha_i \geq 0$  and  $\beta_i \geq 0$ . In other words, we have factorised each of  $a$  and  $b$  into its' prime factors and added on to each factorisation the prime factors of the other which do not already appear, but raised to the zeroeth power so as not to change anything. For example, if  $a = 36$  and  $b = 45$  we would write

$$a = 2^2 \cdot 3^2 \cdot 5^0, \quad b = 2^0 \cdot 3^2 \cdot 5^1.$$

Then, with this notation, and by the Fundamental Theorem of Arithmetic, we have that

$$\begin{aligned} a \cdot b &= \prod_{i=1}^k p_i^{\alpha_i + \beta_i}, \\ \text{LCM}(a, b) &= \prod_{i=1}^k p_i^{\max\{\alpha_i, \beta_i\}}, \\ \text{GCD}(a, b) &= \prod_{i=1}^k p_i^{\min\{\alpha_i, \beta_i\}}. \end{aligned}$$

Hence the desired equality follows if we can just verify that, for any two (real) numbers  $x$  and  $y$ ,

$$x + y = \max\{x, y\} + \min\{x, y\}.$$

But this is obvious.

**Q.9** An example which shows that the result need not hold if  $p$  is not a prime is  $p = 4$ ,  $i = 2$ . We have that  $C(4, 2) = 6$  which is not a multiple of 4.

So now let  $p$  be prime and fix  $i \in \{1, \dots, p - 1\}$ . A priori, we know that  $C(p, i)$  is an integer (since it is the number of ways to do something). Call this integer  $m$ . Thus we have that

$$\frac{p!}{i!(p-i)!} = m,$$

from which we deduce that

$$p! = m \times i! \times (p-i)!.$$

The prime  $p$  obviously divides the left-hand side, so it must also do so for the right-hand side. But recall that Euklides lemma says that if a prime divides a product of integers, then it must divide one of them. But both  $i$  and  $(p-i)!$  are products of integers all less than  $p$ , hence none of these is divisible by  $p$ . Thus  $m$  must be so, which is what we wanted to prove.

**Q.10** Recall that if  $p(x)$  is any non-constant polynomial then  $p(x) \rightarrow \pm\infty$  as  $x \rightarrow \infty$ . First choose any  $x_0$  such that  $|p(x_0)| > 1$ . Let  $p$  be any prime divisor of  $p(x_0)$ . Now, by the usual rules for congruences, if  $l$  is any integer, then

$$p(x_0 + lp) \equiv p(x_0) \equiv 0 \pmod{p}.$$

Thus  $p(x_0 + lp)$  is a multiple of  $p$  for any  $l$ , so is either composite or equal to  $p$  itself. But as  $l \rightarrow \infty$  then so does  $p(x_0 + lp)$ , hence  $p(x_0 + lp)$  cannot equal  $p$  for all sufficiently large  $l$ , and is therefore composite for all such  $l$ , as required.