First practice exam

Solutions

1. If you choose 1002 of the numbers from 1 to 2003 then either
(i) you choose all the odd numbers or,
(ii) (at least) two of the numbers you choose are consecutive.

In case (i), you choose in particular the number 1, and this is relatively prime with any other number you choose.
In case (ii), well we know that any two consecutive numbers are relatively prime.

2 (i) For $m = 1, ..., n$ let us consider the number of such paths which first meet the x-axis at $(2m, 0)$. Then there is only one choice for that part of the path from $(0, 0)$ to $(2n, 0)$, namely : the first step is up, the last step down, and in-between it zig zags with alternating up- and down-steps. There are D_{n-m} choices for the part of the path from $(2m, 0)$ to $(2n, 0)$. Hence we may conclude that

$$D_n = \sum_{m=1}^{n} D_{n-m} = \sum_{m=0}^{n-1} D_m, \quad \text{v.s.v.}$$

(ii) If you compute the first few values of D_n, it's easy to spot the pattern. I claim that $D_n = 2^{n-1}$ for all $n \geq 1$. We may prove this, for example, by strong induction[1] on n. For $n = 1$, it's clear that $D_1 = 2^0 = 1$. So suppose $D_k = 2^{k-1}$ for $k = 1, ..., n$. We must deduce that $D_{n+1} = 2^n$. Simply use the recurrence relation. Noting that $D_0 = 1$, we have

$$\begin{aligned} D_{n+1} &= \sum_{m=0}^{n} D_m \\ &= D_0 + \sum_{m=1}^{n} D_m \\ &= 1 + \sum_{m=1}^{n} 2^{m-1} \end{aligned}$$

[1] This means the following : to prove that a proposition $P(n)$ holds for all $n \geq n_0$, you first verify the base case $n = n_0$. Then, for any given $n > n_0$, you assume that $P(k)$ holds for all $n_0 \leq k \leq n$, and thereby deduce that $P(n + 1)$ holds.

$$= 1 + \sum_{m=0}^{n-1} 2^m$$
$$= 1 + (2^n - 1) = 2^n, \quad \text{v.s.v.}$$

3. Clearly $q_0 = 1$, since the empty word works, and $q_1 = 4$ since each of the one-letter words a, b, c, d work. Now let $n \geq 2$. Divide the q_n allowed words of length n into two types :

(i) those that begin with a b. Then the second letter must be a, c or d (i.e.: 3 choices), and there are q_{n-2} choices for the remaining letters. So there are $3q_{n-2}$ words of this type.

(ii) those that don't begin with a b. Then the first letter can be a, c or d (3 choices) and there are q_{n-1} choices for the remaining letters. There are thus $3q_{n-1}$ choices for the remaining letters.

From the above analysis we deduce the following recurrence relation for the q_n :

$$\begin{aligned} q_0 = 1, \quad q_1 = 4, \\ q_n = 3q_{n-1} + 3q_{n-2}, \quad \forall\, n \geq 2. \end{aligned} \tag{1}$$

Eq. (1) is a standard (second order, linear, homogeneous) recurrence relation. The general solution is

$$q_n = C_1 \alpha^n + C_2 \beta^n,$$

where α, β are the two roots of the quadratic equation

$$x^2 - 3x - 3 = 0.$$

Hence

$$q_n = C_1 \left(\frac{3 + \sqrt{21}}{2} \right)^n + C_2 \left(\frac{3 - \sqrt{21}}{2} \right)^n.$$

Inserting the initial conditions $q_0 = 1$, $q_1 = 3$ we get the following two equations for C_1 and C_2 :

$$\begin{aligned} C_1 + C_2 = 1, \\ \left(\frac{3 + \sqrt{21}}{2} \right) C_1 + \left(\frac{3 - \sqrt{21}}{2} \right) C_2 = 4. \end{aligned}$$

After a little algebra we get the solution

$$C_1 = \frac{5+\sqrt{21}}{2\sqrt{21}}, \quad C_2 = \frac{\sqrt{21}-5}{2\sqrt{21}}$$

and hence

$$q_n = \frac{1}{2\sqrt{21}}\left[(5+\sqrt{21})\left(\frac{3+\sqrt{21}}{2}\right)^n - (5-\sqrt{21})\left(\frac{3-\sqrt{21}}{2}\right)^n\right].$$

4. First note that $240 = 16 \cdot 3 \cdot 5$ so it suffices to prove divisibility by each of $16, 3$ and 5.

First, let's take 3. We have the factorisation

$$n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = n(n-1)(n+1)(n^2+1). \quad (2)$$

Hence $n^5 - n$ is divisible by $n(n-1)(n+1)$, which is a product of 3 consecutive numbers, hence divisible by 3. Hence $n^5 - n$ is also divisible by 3.

Next, consider 5. Here we can simply refer to Fermat's Theorem which, for the prime 5, states that $n^5 \equiv n \pmod 5$ for ALL integers n and hence a fortiori for all odd integers n.

Finally, we take care of 16. We use the factorisation (2) again. Note that, since n is odd, each of $n-1$, $n+1$ and n^2+1 is even. Hence we have at least divisibility by 8. But one of $n \pm 1$ must in fact be divisible by 4, and so we get divisibility by 16.

5. This is a real 'typtal'.

Step 1 : We compute the inverse of $11 \cdot 13 = 143$ modulo 7. Since $143 \equiv 3 \pmod 7$, we seek a solution to

$$3a_1 \equiv 1 \pmod 7.$$

You can run Euclid's algorithm back-and-forth if you like, but it's probably easier just to search for a solution directly. Anyway, a solution is $a_1 = 5$.

Step 2 : Compute the inverse of $7 \cdot 13 = 91$ modulo 11. Since $91 \equiv 3 \pmod{11}$, we must solve

$$3a_2 \equiv 1 \pmod{11}.$$

A solution is $a_2 = 4$.

Step 3 : Compute the inverse of $7 \cdot 11 = 77$ modulo 13. Since $77 \equiv -1 \pmod{13}$, we see immediately that an inverse is given by $a_3 = -1$.

Step 4 : A solution to the three congruences is given by

$$\begin{aligned} x &= 2 \cdot a_1 \cdot (11 \cdot 13) + 3 \cdot a_2 \cdot (7 \cdot 13) + 4 \cdot a_3 \cdot (7 \cdot 11) \\ &= 2 \cdot 5 \cdot 11 \cdot 13 + 3 \cdot 4 \cdot 7 \cdot 13 + 4 \cdot (-1) \cdot 7 \cdot 11 \\ &= 2214. \end{aligned}$$

Step 5 : The general solution is

$$x = 2214 + (7 \cdot 11 \cdot 13) \cdot n = 2214 + 1001n,$$

where n is an arbitrary integer.

(NOTE : the smallest positive solution is $x = 212$, got by taking $n = -2$.)

6 (i) We may compute the prime factorisation

$$7000 = 2^3 \cdot 5^3 \cdot 7.$$

Hence

$$\begin{aligned} \phi(7000) &= \phi(2^3) \cdot \phi(5^3) \cdot \phi(7) \\ &= (2^3 - 2^2) \cdot (5^3 - 5^2) \cdot (7 - 1) \\ &= 4 \cdot 100 \cdot 6 = 2400. \end{aligned}$$

(ii) Euler's theorem states that

$$a^{\phi(n)} \equiv 1 \pmod{n}, \quad \text{whenever SGD}(a, n) = 1.$$

We have that $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$ and hence it is required to prove that

$$a^{(p-1)(q-1)} \equiv 1 \pmod{n}, \quad \text{whenever SGD}(a, n) = 1.$$

Henceforth, let a denote an integer satisfying $\text{SGD}(a, n) = 1$. We must show that $a^{(p-1)(q-1)} - 1$ is divisible by n. Since $\text{SGD}(p, q) = 1$, it suffices to show divisiblity by both p and q. In other words, it suffices to prove that both

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p} \tag{3}$$

and

$$a^{(p-1)(q-1)} \equiv 1 \pmod{q}. \tag{4}$$

I'll demonstrate the proof of (3). That for (4) is identical.

Note that $\mathrm{SGD}(a, n) = 1 \Rightarrow \mathrm{SGD}(a, p) = 1$. Hence, Fermat's theorem implies that

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

But then

$$a^{(p-1)(q-1)} = (a^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p}, \quad \text{v.s.v.}$$