ITB8832 Mathematics for Computer Science
Third midterm test: 1st December 2023

Last modified: 30 November 2023

Exercise 1 (3 points)

Prove that

$$m = n^{21} - 2n^{20} + n^{19} - n^5 + 2n^4 - n^3$$

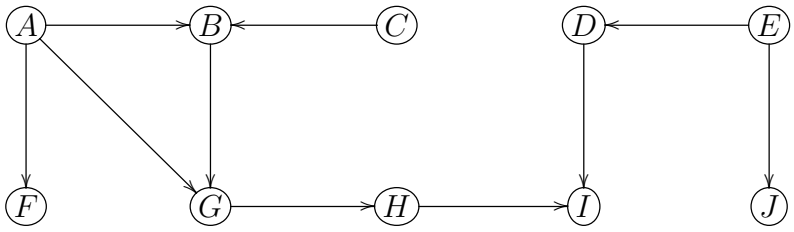
is divisible by 68 for every $n \in \mathbb{Z}^+$. *Hint:* Find suitable factorizations of m and 68 and apply Fermat's little theorem.

Exercise 2 (3 points)

Use the Pulverizer to determine the private key d for the RSA public key $(e, n) = (175, 481)$. *Hint:* $481 = 13 \cdot 37$.

Exercise 3 (3 points)

The following DAG represents a set of tasks together with their priorities:



1. (2 points) Determine a parallel schedule of minimum time.
2. (1 point) Does this set of tasks admit a parallel schedule of minimum time with only two processors? If yes, why? If not, why not?

Important: Point 2 will be considered as correctly answered if the schedule from point 1 uses only two processors.

Exercise 4 (6 points total)

For each of the following questions, mark the only correct answer.

1. What is the remainder of 10^{512} in the division by 17?

   (a) 0.

   (b) 1.

   (c) 16.

2. True or false: $(3, 0)$ is not reachable from $(0, 0)$ for the Die Hard machine with jugs of 10 and 14 liters.

3. Let (e, n) be an RSA public key. Which one of these values would allow you to recover the private key d?

   (a) $d^e \pmod{n}$.

   (b) $\phi(n)$.

   (c) $e^{\phi(n)} \pmod{n}$.

4. Which of the following is true for every DAG D with 120 vertices?

   (a) D has a chain of size 12.

   (b) D has either a chain of size 12, or an antichain of size 11, and possibly both.

   (c) D has either a chain of size 12, or an antichain of size 12, and possibly both.

5. Let R be a binary relation on a nonempty set. Which one of the following is equivalent to R being a strict partial order?

   (a) $R = G^*$ for a suitable DAG G.

   (b) $R = G^+$ for a suitable digraph G.

   (c) $R = G^+$ for a suitable DAG G.

6. True or false: every irreflexive relation is asymmetric.

This page intentionally left blank.

This page too.

Solutions

Exercise 1

We rewrite:

$$\begin{aligned} n^{21} - 2n^{20} + n^{19} - n^5 + 2n^4 - n^3 &= n^3 \cdot (n^{18} - 2n^{17} + n^{16} - n^2 + 2n - 1) \\ &= n^3(n^2 - 2n + 1)(n^{16} - 1) \\ &= n^2(n-1)^2(n^{17} - n)\,. \end{aligned}$$

The first two factors are the square of an even number and the square of an odd number, so their product is divisible by 4. The third factor is divisible by 17 by Fermat's little theorem, because 17 is prime. Then the product m of the three factors is divisible by $\operatorname{lcm}(4, 17) = 68$, as required.

Exercise 2

We have $\phi(481) = 12 \cdot 36 = 432$, so $d = 175^{-1} \pmod{432}$. Using the Pulverizer:

a	b	$\operatorname{rem}(a,b)$	$= a - \operatorname{qcnt}(a,b) \cdot b$
432	175	82	$= 432 - 2 \cdot 175$
175	82	11	$= 175 - 2 \cdot 82$
			$= 175 - 2 \cdot (432 - 2 \cdot 175)$
			$= -2 \cdot 432 + 5 \cdot 175$
82	11	5	$= 82 - 7 \cdot 11$
			$= (432 - 2 \cdot 175) - 7 \cdot (-2 \cdot 432 + 5 \cdot 175)$
			$= 15 \cdot 432 - 37 \cdot 175$
11	5	1	$= 11 - 2 \cdot 5$
			$= (-2 \cdot 432 + 5 \cdot 175) - 2 \cdot (15 \cdot 432 - 37 \cdot 175)$
			$= -32 \cdot 432 + 79 \cdot 175$

Then $d = 79$.

Exercise 3

1. A parallel schedule of minimum time can be obtained by performing at each time k all and only the tasks of depth k:

$$\begin{aligned} A_0 &= \{A, C, E\} \\ A_1 &= \{B, D, F, J\} \\ A_2 &= \{G\} \\ A_3 &= \{H\} \\ A_4 &= \{I\} \end{aligned}$$

2. This set of tasks does admit a schedule of minimum time with only two processors. We can obtain one from that of the previous point by observing that the tasks F and J are maximal vertices in the DAG, so we could run them at any time greater than their own depth and still obtain a parallel schedule. For example, we could do:

$$\begin{aligned} B_0 &= \{A, C\} \\ B_1 &= \{B, E\} \\ B_2 &= \{D, G\} \\ B_3 &= \{H, J\} \\ B_4 &= \{F, I\} \end{aligned}$$

Exercise 4

1. (a) **No:** 7 is a prime which doesn't divide 10, so the remainder cannot be zero.

   (b) **Yes:** $\phi(17) = 16$ and $512 = 16 \cdot 32$, and as 17 is a prime larger than 10, $10^{512} = (10^{16})^{32} \equiv 1^{32} = 1 \pmod{17}$.

   (c) **No:** see above.

2. **True:** $\gcd(10, 14) = 2$, so in any state reachable from $(0, 0)$, the number of liters of water in each jug must be even.

3. (a) **No:** this is simply the encryption of the private key with the public key.

   (b) **Yes:** then $d = e^{-1} \pmod{\phi(n)}$.

(c) **No:** for most values of e, this is simply 1.

4. (a) **No:** the DAG could be made of 120 isolated vertices.

   (b) **Yes:** by Dilworth's lemma with $d = 11$, if D doesn't have a chain of size greater than 11, then it has an antichain of size at least $\lceil 120/11 \rceil = 11$.

   (c) **No:** the DAG could be made of ten chains of size 11 and an eleventh chain of size 12.

5. (a) **No:** this is equivalent to R being a *weak* partial order.

   (b) **No:** if G has a cycle, then some elements are related to themselves by G^+.

   (c) **Yes.**

6. **False:** the binary relation R on $\mathbb{N}$ defined by $a \, R \, b$ **iff** $a \neq b$ is irreflexive, but not asymmetric.