ITB8832 Mathematics for Computer Science
Third midterm test: 29 November 2024

Last modified: 2 December 2024

Exercise 1 (3 points)

Let m and n be positive integers such that $m \geq n$.

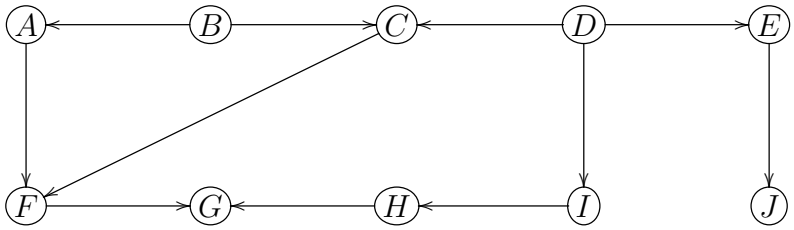
1. (1 point) Let q be a positive integer. Explain why $\gcd(5^n - 3^n, 5^{qn}) = 1$.
2. (2 points) Use the previous point to prove that if $5^m - 3^m$ is a multiple of $5^n - 3^n$, then m is a multiple of n. *Hint:* If $r, n \in \mathbb{N}$ and $r < n$, then $5^r - 3^r < 5^n - 3^n$.

Exercise 2 (3 points)

Use the Pulverizer to determine the private key d for the RSA public key $(e, n) = (227, 1247)$. *Hint:* $1247 = 29 \cdot 43$.

Exercise 3 (3 points)

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



Every task requires one time unit to be performed.

1. (1 point) Explain why D does *not* have a parallel schedule of minimum parallel time with only two processors.
2. (2 points) Determine a parallel schedule for D of minimum parallel time with three processors.

Exercise 4 (6 points total)

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

1. Which one of the following is an invariant for the Die Hard machine with jugs of $\ell = 15$ and $b = 21$ liters?

   (a) ℓ is a multiple of 3.

   (b) ℓ and b are both multiple of 3.

   (c) Neither *ell* nor b is a multiple of 3.

2. True or false: $a^{p-1} \equiv 1 \pmod{p}$ for every positive integer a and prime p.

3. Which one of the following pairs (e, n) is a valid RSA public key?

   (a) $(49, 289)$.

   (b) $(49, 707)$.

   (c) $(48, 707)$.

4. Which one of the following is true for every DAG D with 96 vertices?

   (a) D has an antichain of size 8.

   (b) D has either a chain of size 17, or an antichain of size 7, and possibly both.

   (c) D has either a chain of size 13, or an antichain of size 8, and possibly both.

5. Let A and B be sets. Which one of the following statements defines an equivalence relation on A?

   (a) xRy if and only if $f(x) = f(y)$, where $f : A \to B$ is a function.

   (b) xRy if and only if $f(x) = f(y)$, where $f : A \to B$ is a total function.

   (c) xRy if and only if $f(x) = f(y)$, where $f : B \to A$ is a total function.

6. True or false: Every relation which is both irreflexive and transitive is the positive walk relation of a DAG.

This page intentionally left blank.

This page too.

Solutions

Exercise 1

1. On the one hand, as q and n are positive, 5^{qn} is a power of the prime number 5; on the other hand, $5^n - 3^n$ is not a multiple of 5, so it is coprime with any power of 5.

2. Write $m = qn + r$ with $0 \leq r < n$. As we assume $m \geq n$, we have $q \geq 1$. Then:

$$\begin{aligned} 5^m - 3^m &= 5^{qn+r} - 3^{qn+r} \\ &= 5^{qn}5^r - 5^{qn}3^r + 5^{qn}3^r - 3^{qn}3^r \\ &= 5^{qn}(5^r - 3^r) + 3^r\left(5^{qn} - 3^{qn}\right) . \end{aligned}$$

On the right-hand side, we know from high school algebra that:

$$5^{qn} - 3^{qn} = (5^n)^q - (3^n)^q$$

is a multiple of $5^n - 3^n$. Assume that the left-hand side $5^m - 3^m$ is also a multiple of $5^n - 3^n$. Then their difference $5^{qn}(5^r - 3^r)$ must also be a multiple of $5^n - 3^n$. But as $\gcd(5^n - 3^n, 5^{qn}) = 1$, the other factor $5^r - 3^r$ must be a multiple of $5^n - 3^n$, and as the former is smaller than the latter, it must be $5^r - 3^r = 0$, which is only possible if $r = 0$.

Another argument, from the students' discussions, goes as follows. Rewrite the divisibility conditions as $5^{qn+r} \equiv 3^{qn+r} \pmod{5^n - 3^n}$ and $5^{qn} \equiv 3^{qn} \pmod{5^n - 3^n}$, respectively. Then:

$$5^{qn} \cdot 5^r \equiv 5^{qn} \cdot 3^r \pmod{5^n - 3^n} .$$

By the previous point, $\gcd(5^{qn}, 5^n - 3^n) = 1$, so 5^{qn} is cancellable modulo $5^n - 3^n$. The equality above is thus equivalent to $5^r \equiv 3^r \pmod{5^n - 3^n}$, which says that $5^r - 3^r$ is a multiple of $5^n - 3^n$. As $5^r - 3^r < 5^n - 3^n$, this is only possible if $5^r = 3^r$, so it must be $r = 0$.

Exercise 2

We have $\phi(1247) = 28 \cdot 42 = 1176$, so $d = 227^{-1} \pmod{1176}$. Using the Pulverizer:

a	b	$\mathrm{rem}(a,b)$	$= a - \mathrm{qcnt}(a,b) \cdot b$
1176	227	41	$= 1176 - 5 \cdot 227$
227	41	22	$= 227 - 5 \cdot 41$
			$= 227 - 5 \cdot (1176 - 5 \cdot 227)$
			$= -5 \cdot 1176 + 26 \cdot 227$
41	22	19	$= 41 - 22$
			$= (1176 - 5 \cdot 227) - (-5 \cdot 1176 + 26 \cdot 227)$
			$= 6 \cdot 1176 - 31 \cdot 227$
22	19	3	$= 22 - 19$
			$= (-5 \cdot 1176 + 26 \cdot 227) - (6 \cdot 1176 - 31 \cdot 227)$
			$= -11 \cdot 1176 + 57 \cdot 227$
19	3	1	$= 19 - 6 \cdot 3$
			$= (6 \cdot 1176 - 31 \cdot 227) - 6 \cdot (-11 \cdot 1176 + 57 \cdot 227)$
			$= 72 \cdot 1176 - 373 \cdot 227$

Then $d = \mathrm{rem}(-373, 1176) = 803$.

Exercise 3

1. By checking all the paths from the minimal vertices of D to the maximal ones, we see that the maximum chain size is 4; for example, $\{A, B, F, G\}$ is a chain of maximum size. But D has 10 vertices, so any parallel schedule with 2 processors requires at least $10/2 = 5$ time units.

2. The minimum parallel time obtained by partitioning $V(D)$ into blocks made of vertices with the same depth is:

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

   which requires 4 processors. However, the vertex J is maximal and is reachable only from D and E, so we can postpone the corresponding

tasks and obtain:

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

which uses three processors and runs in minimum parallel time.

Exercise 4

1. (a) **No:** from $(b, \ell) = (4, 3)$ we can reach $(b', \ell') = (0, 7)$.
   (b) **Yes:** $\gcd(15, 21) = 3$, so if at any point b and ℓ are multiples of 3, they will remain so after a transition of the Die Hard machine.
   (c) **No:** from $(b, \ell) = (4, 5)$ we can reach $(b', \ell') = (9, 0)$.
2. **False:** this happens if and only if a is not divisible by p.
3. (a) **No:** $289 = 17^2$ is not the product of two *distinct* primes.
   (b) **Yes:** $707 = 7 \cdot 101$ is a product of two distinct primes and $49 = 7^2$ is coprime with $\phi(707) = 600$.
   (c) **No:** if p and q are distinct primes, then $(p-1)(q-1)$ is even, so no pair $(2k, pq)$ can be a valid RSA public key.
4. (a) **No:** the DAG could be a single chain with 96 vertices.
   (b) **No:** the DAG could be made of 6 independent chains of size 16.
   (c) **Yes:** by Dilworth's lemma with $n = 96$ and $t = 12$, if D doesn't have a chain of size greater than 12, then it has an antichain of size at least $96/12 = 8$.
5. (a) **No:** if $f(x)$ is not defined for $x = a$, then $\mathbf{not}(aRa)$, and R is not reflexive.
   (b) **Yes:** f is "tricking" the equality relation of B into doing all the work R should be doing on A.
   (c) **No:** this defines an equivalence relation on B, not on A.
6. **True:** this is the "only if" part of Theorem 10.10.8.