+1/1/60+

EPFL

Prof. M. Gastpar

Quiz 4 (Homeworks 7, 8 & 9)

Due on Moodle

on Monday, April 28, 2024, at 23:59.

Quiz 4

SCIPER : **111111**

- This quiz is to be solved individually.
- Try not to use any of the course materials other than the formula collection on a first attempt.
- Once you are done, enter your answers into Moodle. Moodle will give you feedback. You can update your answers as many times as you want before the deadline.
- For each question there is **exactly one** correct answer. We assign **negative points** to the **wrong answers** in such a way that a person who chooses a wrong answer loses **25 %** of the points given for that question.

Respectez les consignes suivantes | Observe this guidelines | Beachten Sie bitte die unten stehenden Richtlinien

choisir une réponse | select an answer Antwort auswählen	ne PAS choisir une réponse | NOT select an answer NICHT Antwort auswählen	Corriger une réponse | Correct an answer Antwort korrigieren

ce qu'il ne faut **PAS** faire | what should **NOT** be done | was man **NICHT** tun sollte

For your examination, preferably print documents compiled from auto-multiple-choice.

Question 1

[2 points] Consider the group $(\mathbb{Z}/207\mathbb{Z}^*, \cdot)$. Find how many elements are in the group.

- ☐ 128
- ☐ 100
- ☐ 127
- ☐ 132

Solution: The number of elements in the group $\mathbb{Z}/m\mathbb{Z}^*$ is given by $\phi(m)$, where $\phi(.)$ is Euler's totient function. To find $\phi(207)$, we first need the prime factorization of 153. It is quick to see that 153 is divisible by 3, that is, $207 = 3 \times 69$. But $69 = 3 \times 23$, hence we can write $207 = 23 \times 3^2$. This is neither a prime power nor the product of two distinct primes, so the two basic formulas for $\phi(m)$ from the lecture notes will not work. To continue, we can leverage what we did in the homework. There, we saw that the CRT directly implies that if m and n are relatively prime, we have $\phi(mn) = \phi(m)\phi(n)$. Clearly, 23 and 9 are relatively prime, meaning that we have $\phi(207) = \phi(23)\phi(9)$. For any prime p and positive integer k, we know that $\phi(p^k) = p^k - p^{k-1}$, and thus $\phi(23) = 22, \phi(9) = 3^2 - 3 = 6$. Combining all of the above, we find that the number of elements in $(\mathbb{Z}/207\mathbb{Z}^*, \cdot)$ is $22 \times 6 = 132$.

Note that alternatively, we could have found the answer directly by starting from the full list $\{1, 2, \ldots, 207\}$ and removing all multiples of three and all multiples of seventeen. Specifically, start by removing the 69 multiples of 3. Also, there are 9 multiples of 23, but of these, 3 have already been removed since they are also multiples of 3. Hence, $\phi(m) = 207 - 69 - 9 + 3 = 132$.

Question 2

[3 points] Passing on secrets: Alice has posted her RSA credentials as (m, e), with m the modulus and e the encoding exponent. As required by RSA, she keeps her decoding exponent d preciously secret. Bob has a message t_1, RSA-encrypts it using (m, e_1) and passes the resulting cryptogram c_1 on to Carlos. Carlos has a message t_2, RSA-encrypts it using (m, e_2) to obtain the cryptogram c_2. Then, Carlos multiplies the two cryptograms, $(c_1 \cdot c_2) \mod m$, and passes this to Alice. Alice applies her regular RSA decryption to $(c_1 \cdot c_2) \mod m$. Under what condition is the result of this decryption exactly equal to the product $(t_1 \cdot t_2) \mod m$?

- ☐ If d is prime and $(e_1 + e_2) \mod m = 1$.
- ☐ If for some integer ℓ, we have $e_1 e_2 d = \ell\phi(m) + 1$, where $\phi(\cdot)$ denotes Euler's totient function.
- ☐ If $e_1 + e_2 = e$.
- ☐ If $e_1 = e_2 = e$.

Solution: The final cryptogram $c = (c_1 \cdot c_2) \mod m = (t_1^{e_1} \cdot t_2^{e_2}) \mod m$, and therefore, the decryption recovered by Alice is given as $(t_1^{e_1} \cdot t_2^{e_2})^d \mod m = (t_1^{e_1 d} \cdot t_2^{e_2 d}) \mod m$. This is exactly equal to $(t_1 \cdot t_2) \mod m$ when $e_1 = e_2 = e$.

Question 3

[6 points] *Note: This is an* **open** *question. In the real exam, we will grade your arguments. Here for the quiz, we do not have the capacity to do this. Therefore, you will merely enter your final answer into a*

multiple choice grid on Moodle. However, do make sure to carefully look at the solution and compare to your answer. How many points would you have given yourself?

Consider the source $S_1, S_2, \ldots$ such that S_1 is uniformly distributed on $\mathbb{Z}/10\mathbb{Z}^*$, and for every $n \geq 1$, S_{n+1} is distributed uniformly on $\mathbb{Z}/(S_n+1)\mathbb{Z}^*$. Answer the following questions.

(a) (3 pts) Calculate the marginal distribution of S_2.

(b) (1 pt) Is the source stationary? Fully justify your answer

(c) (2 pts) Show that $H(S_n|S_1,\ldots,S_{n-1}) \leq \big(p_{S_{n-1}}(3)+p_{S_{n-1}}(5)\big)\log 2 + \big(p_{S_{n-1}}(7)+p_{S_{n-1}}(9)\big)\log 4$.

(d) *[Difficult, and not graded on the Moodle interface]* Show that the probabilities in the right hand side of the above inequality converge to zero as n increases.

Solution: For (a), we need to find the marginal distribution of S_2. To do this, we first find the conditional distribution of S_2 given S_1. We know that $S_1 \in \{1,3,7,9\}$. When $S_1 = 1$, then S_2 is uniformly distributed on $\mathbb{Z}/2\mathbb{Z}^* = \{1\}$. Which is the same as saying that in that case, we must have $S_2 = 1$. Next, when $S_1 = 3$, then S_2 is uniformly distributed on $\mathbb{Z}/4\mathbb{Z}^* = \{1,3\}$. Next, when $S_1 = 7$, then S_2 is uniformly distributed on $\mathbb{Z}/8\mathbb{Z}^* = \{1,3,5,7\}$. Finally, when $S_1 = 9$, then S_2 is uniformly distributed on $\mathbb{Z}/10\mathbb{Z}^* = \{1,3,7,9\}$. Hence, the joint distribution of (S_1, S_2) can be expressed as

$$p_{S_1,S_2}(s_1,s_2) = p_{S_1}(s_1)p_{S_2|S_1}(s_2|s_1) = \begin{cases} \frac{1}{4}, & \text{if } s_1=1, s_2=1 \\ \frac{1}{4}\cdot\frac{1}{2}, & \text{if } s_1=3, s_2=1 \\ \frac{1}{4}\cdot\frac{1}{2}, & \text{if } s_1=3, s_2=3 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=7, s_2=1 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=7, s_2=3 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=7, s_2=5 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=7, s_2=7 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=9, s_2=1 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=9, s_2=3 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=9, s_2=7 \\ \frac{1}{4}\cdot\frac{1}{4}, & \text{if } s_1=9, s_2=9, \end{cases} \tag{1}$$

while all other choices for pairs (s_1, s_2) have probability zero. From the joint distribution, it is now a simple matter to find the marginal distribution of S_2 simply by summing over all values of S_1 (for a fixed values of S_2), hence,

$$p_{S_2}(s_2) = \begin{cases} \frac{1}{2}, & \text{if } s_2 = 1 \\ \frac{1}{4}, & \text{if } s_2 = 3 \\ \frac{1}{16}, & \text{if } s_2 = 5 \\ \frac{1}{8}, & \text{if } s_2 = 7 \\ \frac{1}{16}, & \text{if } s_2 = 9 \end{cases} \tag{2}$$

For (b), observe that the marginal distribution of S_2 is not the same as the marginal distribution of S_1. This already implies that the source cannot be stationary.

For (c), we may start by recalling that conditioning cannot increase entropy, hence

$$H(S_n|S_1,\ldots,S_{n-1}) \leq H(S_n|S_{n-1}). \tag{3}$$

(In fact, for the process at hand, you can even show that these two conditional entropies are equal, but this is not important for the property we are about to prove.) Next, let us write out the conditional entropy as we have done in class:

$$H(S_n|S_{n-1}) = \sum_{s_{n-1}} p_{S_{n-1}}(s_{n-1}) H(S_n|S_{n-1}=s_{n-1}). \tag{4}$$

From Part (a), extending to general S_n, we can see that $S_n \in \{1,3,5,7,9\}$. No other values can show up (since also $\mathbb{Z}/6\mathbb{Z}^* = \{1,5\}$). Moreover, $H(S_n|S_{n-1}=1) = 0$ since when $S_{n-1}=1$ we have $S_n = 1$ with probability one. Therefore,

$$\begin{aligned} H(S_n|S_1,\ldots,S_{n-1}) \leq\ & p_{S_{n-1}}(3)H(S_n|S_{n-1}=3) + p_{S_{n-1}}(5)H(S_n|S_{n-1}=5) \\ & + p_{S_{n-1}}(7)H(S_n|S_{n-1}=7) + p_{S_{n-1}}(9)H(S_n|S_{n-1}=9) && (5) \\ \leq\ & p_{S_{n-1}}(3)\log 2 + p_{S_{n-1}}(5)\log 2 + p_{S_{n-1}}(7)\log 4 + p_{S_{n-1}}(9)\log 4, && (6) \end{aligned}$$

where for the last inequality, we have used the fact that when $S_{n-1}=3$ or $S_{n-1}=5$, then S_n only has 2 possible values, and when $S_{n-1}=7$ or $S_{n-1}=9$, then S_n has 4 possible values.

For part (d), we have to study the conditional distribution $p_{S_n|S_1,\ldots,S_{n-1}}(s_n|s_1,\ldots,s_{n-1})$. To get there, let us imagine the process a bit further into the future. In particular, let us suppose that for some i, we end up with the sample $S_i = 1$. Then, we know that for all $n \geq i$, we must have $S_n = 1$ with probability one. That is, the process becomes fully deterministic. To be more formal, we have the following recursions:

$$\begin{aligned} p_{S_n}(9) =& \frac{1}{4} p_{S_{n-1}}(9) && (7) \\ p_{S_n}(7) =& \frac{1}{4} p_{S_{n-1}}(7) + \frac{1}{4} p_{S_{n-1}}(9) && (8) \\ p_{S_n}(5) =& \frac{1}{2} p_{S_{n-1}}(5) + \frac{1}{4} p_{S_{n-1}}(7) && (9) \\ p_{S_n}(3) =& \frac{1}{2} p_{S_{n-1}}(3) + \frac{1}{4}(p_{S_{n-1}}(7) + p_{S_{n-1}}(9)). && (10) \end{aligned}$$

Recall the distribution of S_1. From (7), we have

$$p_{S_n}(9) = \frac{1}{4^n}. \tag{11}$$

From (8), we have

$$\begin{aligned} p_{S_n}(7) =& \frac{1}{4} p_{S_{n-1}}(7) + \frac{1}{4^n} && (12) \\ =& \frac{1}{4^{n-1}} p_{S_1}(7) + (n-1)\frac{1}{4^n} \\ =& n\frac{1}{4^n}. && (13) \end{aligned}$$

From (9), we have

$$p_{S_n}(5) = \frac{1}{2} p_{S_{n-1}}(5) + (n-1)\frac{1}{4^n}. \tag{14}$$

This (roughly) tells us that $p_{S_n}(5)$ behaves similarly to $1/2^n$ asymptotically. Let $p_{S_n}(5) = f(n)/2^n$. Then we have

$$f(n) - f(n-1) = \frac{n-1}{2^n} \tag{15}$$

$$\implies f(n) = f(1) + \sum_{k=2}^{n} \frac{k-1}{2^k} \tag{16}$$

$$= 0 + \left(1 - \frac{n+1}{2^n}\right) = 1 - \frac{n+1}{2^n} \tag{17}$$

$$\implies p_{S_n}(5) = \left(1 - \frac{n+1}{2^n}\right)\frac{1}{2^n} \tag{18}$$

From (10), we have

$$p_{S_n}(3) = \frac{1}{2} p_{S_{n-1}}(3) + n\frac{1}{4^n} \tag{19}$$

Once again, letting $p_{S_n}(3) = g(n)/2^n$,

$$g(n) - g(n-1) = \frac{n}{2^n} \tag{20}$$

$$\implies g(n) = g(1) + \sum_{k'=2}^{n} \frac{k'}{2^{k'}} \tag{21}$$

$$= \frac{1}{2} + \sum_{k'=2}^{n} \frac{k'}{2^{k'}} \tag{22}$$

$$= \sum_{k'=1}^{n} \frac{k'}{2^{k'}} \tag{23}$$

$$= 2 - \frac{n+2}{2^n} \tag{24}$$

$$\implies p_{S_n}(3) = \left(2 - \frac{n+2}{2^n}\right)\frac{1}{2^n}. \tag{25}$$

Clearly, all of these probabilities converge to 0 as n grows large.

Grading Notes: For Part (a), 1 point for correctly identifying the support of S_2, 1 point for the right answer (the probabilities) and 1 point for the correct derivation logic. For Part (b), 1 point for the correct justification and answer. For Part (c), 1 point for the correct derivation of the conditional entropy, including dropping the conditioning and 1 point for the entropy upper bounds as logarithm of the alphabet size.

Question 4

[6 points] Consider an RSA encryption where the (p, q) are determined as $(67, 53)$. Check if the following encoding and decoding exponent pairs are valid.

(a) $(e, d) = (123, 79)$ are valid exponents.

☐ VRAI ☐ FAUX

(b) $(e, d) = (631, 223)$ are valid exponents.

☐ VRAI ☐ FAUX

(c) $(e, d) = (319, 23)$ are valid exponents.

☐ VRAI ☐ FAUX

Solution: As we have seen in class, the necessary and sufficient condition for (e, d) to be a valid pair is that we must have at the same time

$$ed = \ell_1(p-1) + 1 \tag{26}$$

$$ed = \ell_2(q-1) + 1 \tag{27}$$

for some positive integers ℓ_1 and ℓ_2. Of course, this is the same as asking $[ed]_{p-1} = [1]_{p-1}$ and $[ed]_{q-1} = [1]_{q-1}$.

(a) $[123 \cdot 79]_{66} = [15]_{66}$, which means game over: this cannot be a valid exponent pair. (No need to check $[123 \cdot 79]_{52}$.)

(b) $[631 \cdot 223]_{66} = [1]_{66}$ and $[631 \cdot 223]_{52} = [1]_{52}$, thus this is a valid exponent pair.

(c) $[319 \cdot 23]_{66} = [11]_{66}$, so again, game over: This cannot be a valid exponent pair.

Question 5

[3 Points] How many $x \in \{0, 1, 2, \ldots, 34\}$ satisfy the equation $x^2 - 5x + 4 \mod 35 = 0$?

☐ 2 ☐ 1

☐ 0 ☐ 4

Solution: Probably the fastest is to go via the Chinese Remainder Theorem. Write $35 = 5 \cdot 7$. Recall that $x^2 - 5x + 4 \mod 35 = 0$ if and only if $x^2 - 5x + 4 \mod 5 = 0$ and $x^2 - 5x + 4 \mod 7 = 0$.

The $\mod 5$ part is particularly easy: $x^2 - 5x + 4 \equiv x^2 + 4 \mod 5$. Moreover, $4 \equiv -1 \mod 5$. So, clearly, we have two solutions here: $x = 1$ and $x = 4$.

For the $\mod 7$ part, it is perhaps clever to observe that $x^2 - 5x + 4 = (x-1)(x-4)$. (This holds always, and of course also $\mod 7$.) So we can see that $x = 1$ and $x = 4$ both work.

To combine, thinking about the grid representation of the Chinese Remainder Theorem, we have 4 solutions (two choices for the row and two choices for the column in the grid representation). Namely, $(1, 1), (1, 4), (4, 1), (4, 4)$.

You are not asked to find the actual solutions. You could find those by the usual inversion formula for the Chinese Remainder Theorem. Numbers in this example are so small that we can probably guess the solutions... The first solution is a number x such that $x \mod 5 = 1$ and $x \mod 7 = 1$. This is simply $x = 1$. Next, we need a number x such that $x \mod 5 = 4$ and $x \mod 7 = 4$. This is simply $x = 4$. Now it gets more interesting: Another solution is x such that $x \mod 5 = 1$ and $x \mod 7 = 4$. A moment's reflection gets us to $x = 11$. And finally, we are looking for x such that $x \mod 5 = 4$ and $x \mod 7 = 4$. Here, we have to perhaps scratch our head a little longer (or actually draw up the Chinese Remainder Theorem table). Then, we find $x = 29$.

So, the four solutions are $x \in \{1, 4, 11, 29\}$. (It is not hard to verify that these four numbers are indeed solutions to the original equation.)