

MATHEMATIQUES POUR LA SECURITE INFORMATIQUE
FMSI

PARTIEL, EPITA_ING1_2021_S6
Mars / Avril 2019, Durée : 1h30 min

H. GROSCOT

Remarques : Le **support de cours** est autorisé.
Toutes les **calculatrices** sont autorisées.

Exercice 1 :

On se donne le nombre $n = 20705$.

Q1 – Le nombre de facteurs premiers de n vaut :

- A 2
- B 3
- C 4

Q2 – Le plus grand facteur premier de n est le suivant :

- A 97
- B 101
- C 103
- D 107
- E 109

Q3 – La somme des facteurs premiers de n vaut :

- A 135
- B 141
- C 147
- D 153
- E 159

Q4 - La valeur de $\varphi(n)$ est la suivante :

- A 14500
- B 15000
- C 15500
- D 16000
- E 16500

Q5 – Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique :

- A vrai
- B faux

Q6 – Le nombre de générateurs du groupe de la question Q5 vaut :

- A 10336
- B 12750
- C 14302
- D 16000
- E 20704

Q7 – $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps :

- A vrai
- B faux

Exercice 2 :

Nous avons vérifié avec une calculatrice l'identité suivante : $23507 \times 11 - 5387 \times 48 = 1$.

Q7 – Afin de vérifier avec une calculette que 5387 est premier, nous avons essayé de diviser 5387 par les nombres suivants (choisir la meilleure méthode si plusieurs fonctionnent) :

- A 2 ainsi que tous les nombres impairs jusqu'à 5386,
- B 2 ainsi que tous les nombres impairs jusqu'à 1000,
- C 2 ainsi que tous les nombres premiers impairs jusqu'à 101,
- D 2 ainsi que tous les nombres premiers impairs jusqu'à 73,
- E 2 ainsi que tous les nombres premiers impairs jusqu'à 71,

Q8 – $(\mathbb{Z}/5387\mathbb{Z}, +, \times)$ est un corps :

- A vrai
- B faux

Q9 – Le nombre de générateurs du groupe $(\mathbb{Z}/5387\mathbb{Z}, +)$ vaut :

- A 1344
- B 2692
- C 2693
- D 5386
- E 5387

Q10 – $(\mathbb{Z}/5387\mathbb{Z}^*, \times)$ est un groupe cyclique :

- A vrai
- B faux

Q11 – Le nombre de générateurs du groupe de la question Q10 est égal à :

- A 1344
- B 2692
- C 2693
- D 5386
- E 5387

Exercice 3 :

Nous avons calculé les puissances de **10** modulo le nombre premier **p = 17** dans le tableau suivant, où $p_{10}(k) = 10^k \pmod{17}$:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$p_{10}(k)$	1	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1

Q12 - Est-ce que **10** est un générateur de $\mathbb{Z}/17\mathbb{Z}^*$ (première réponse) ? Combien de générateurs y a-t-il dans $\mathbb{Z}/17\mathbb{Z}^*$ (deuxième réponse sur la même ligne) ?

- A oui et 16
- B non et 16
- C oui et 8
- D non et 8
- E oui et 15.

Q13 – Il est possible de trouver facilement $13^{31} \pmod{17}$. On trouve :

- A 2
- B 4
- C 7
- D 11
- E 15

Exercice 4 : Utilisation du RSA

Véronique envoie un message à Maurice qu'elle signe en utilisant le RSA. Le message est long, on l'appelle **M** et il occupe une place de 1,5 Mo en mémoire. Véronique utilise une fonction de hashage **H** connue de Maurice pour calculer :

$$m = H(M), \text{ où}$$

$$m = 4\ 071\ 055\ 667\ 727\ 926\ 747\ 805\ 540\ 511\ 627$$

Q14 - Dans l'optique d'une utilisation du RSA, Véronique a-t-elle vraiment besoin de la fonction **H** ?

- A oui
- B non

Pour signer, elle a besoin de fabriquer une clé. Véronique part du nombre suivant :

$$p = 79\ 792\ 756\ 297\ 612\ 087.$$

Véronique a utilisé un test de Miller-Rabin, avec 40 essais sur des témoins différents pris au hasard, pour en déduire que **p** est « probablement premier ».

Q15 - Quelle est une majoration de la probabilité pour que **p** ne soit pas premier :

- A 10^{-6}
- B 2×10^{-11}
- C 4×10^{-18}
- D 8×10^{-25}
- E 2×10^{-32}

Elle a fait de même avec le nombre **q** suivant :

$$q = 95\ 367\ 431\ 640\ 703$$

On pose :

$$\begin{aligned} n &= p \cdot q = 7\ 609\ 630\ 231\ 635\ 794\ 509\ 887\ 453\ 977\ 161 \\ f &= (p - 1)(q - 1) = 7\ 609\ 630\ 231\ 635\ 714\ 621\ 763\ 724\ 724\ 372 \\ e &= 34\ 348\ 917 \\ d &= 2\ 569\ 640\ 103\ 788\ 143\ 362\ 303\ 034\ 428\ 671 \\ w &= -11\ 599\ 034 \end{aligned}$$

Q16 - Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ vaut :

- A 2 569 640 103 788 143 362 303 034 428 671
- B 4 071 055 667 727 926 747 805 540 511 627
- C 7 609 630 231 635 714 621 763 724 724 372
- D 7 609 630 231 635 794 509 887 453 977 160

On a vérifié :

$$e \cdot d \equiv 1 \pmod{f}$$

Véronique a calculé le nombre **c** suivant :

$$c \equiv m^e \pmod{n}$$

ce qui a donné :

$$C = 2\ 969\ 387\ 768\ 310\ 818\ 749\ 865\ 678\ 669\ 300$$

Q17 - Dans un premier temps, Véronique a envoyé à Maurice sa clé publique. Elle est constituée des deux nombres :

- A n, e
- B n, c
- C n, f
- D f, e
- E f, c.

Q18 – Dans un deuxième temps, Véronique signe le message **M** avec une signature **s**. Ensuite, Maurice reçoit de Véronique le message **M**, accompagné de cette signature **s**. La valeur de **s** est la suivante :

- A **2 569 640 103 788 143 362 303 034 428 671**
- B **2 969 387 768 310 818 749 865 678 669 300**
- C **4 071 055 667 727 926 747 805 540 511 627**
- D **7 609 630 231 635 714 621 763 724 724 372**

Q19 – En recevant le message avec sa signature, Maurice a besoin de recalculer $H(M)$.

- A vrai
- B faux.

Q20 - Avec la clé publique de Véronique, Maurice pourrait effectuer les opérations suivantes :

- A Chiffrer un message M1 destiné à Véronique et signer un message M2 pour Véronique,
- B Chiffrer un message M1 destiné à Véronique mais non signer un message M2 pour Véronique,
- C Signer un message M2 pour Véronique mais pas chiffrer un message M1 destiné à Véronique,
- D Ni chiffrer un message M1 destiné à Véronique ni signer un message M2 pour Véronique.