Examen de session 2 du jeudi 15 juin 2023 - Durée 2h00

L'usage de tout document ou appareil électronique (y compris calculatrice) est prohibé. Les réponses aux questions doivent être justifiées faute de quoi elles ne rapporteront aucun point, même si elles sont justes.

Exercice 1.

1) Donner les solutions des deux systèmes d'équations suivants :

$$a) \begin{cases} x \equiv 1[3] \\ x \equiv 3[4] \end{cases} \qquad b) \begin{cases} x \equiv 2[3] \\ x \equiv 1[4] \end{cases}$$

2) Considérons le système :

$$(S) : \begin{cases} x \equiv 3[4] \\ x \equiv 1[6] \end{cases}$$

Parmi les propositions suivantes, laquelle est équivalente au système (S) ? (justifiez votre réponse)

$$(i)\ x \equiv 7[24], \quad (ii)\ x \equiv 7[12], \quad (iii)\ x \equiv 4[24], \quad (iv)\ x \equiv 4[12], \quad (v)\ x \equiv -1[12].$$

Exercice 2.

1) Déterminer le PGCD de 1004 et 768 et trouver $u, v \in \mathbb{Z}$ tels que $1004u + 768v = \text{pgcd}(1004, 768)$.
2) En déduire la fraction continue de $\frac{1004}{768}$.
3) Donner la décomposition en fraction continue de $\sqrt{5}$.

Exercice 3.

1) Quelles sont les solutions de $x^2 \equiv 1[n]$ quand $n \in \mathbb{N}^*$ est premier ?
2) Montrer que si $n \in \mathbb{N}^*$ est premier, alors $(n-1)! \equiv -1[n]$.
3) Soit n un entier non premier. Montrer que $(n-1)! \equiv 0[n]$ si $n \neq 4$ et $(n-1)! \equiv 2[n]$ si $n = 4$.
4) En déduire le théorème de Wilson : un entier $n \geq 2$ est premier si et seulement si $(n-1)! \equiv -1[n]$.

Exercice 4. On cherche à calculer 51447^{12} modulo 17 par exponentiation rapide.

1) Montrer que $51447 \equiv 5[17]$.
2) Décomposer 12 en binaire.
3) Calculer $\{5^{2^i} \bmod 17\}$ pour $i = 0, 1, 2, 3$.
4) En déduire la valeur de 51447^{12} modulo 17.
5) Soient n et m deux entiers. Montrer que pour calculer n^m, la complexité (nombre de multiplications) de l'exponentiation naïve est en $O(m)$, tandis que la complexité de l'exponentiation rapide est en $O(2\ln(m))$.

Exercice 5. Soient $n := 35$ et $c = 5$.

1) Calculer $\varphi(n)$.
2) Calculer l'inverse de c modulo $\varphi(n)$.
3) Décoder le message $C = 10$ qui a été crypté avec le protocole RSA, via la clé publique (n, e).