Partiel Mat309, 9 novembre 2022, 11h30-13h

Calculatrices interdites.
Une feuille manuscrite A4 recto-verso autorisée.
Les réponses doivent être justifiées.

Exercice 1. (~ 6 points)

1. Calculer $8 \cdot 9 \cdot 10 + 3^4 \pmod{89}$.
2. Calculer $8! \pmod{17}$ et $(8!)^2 \pmod{17}$.
3. Montrer $(((n-1)/2)!)^2 \equiv (-1)^{(n-1)/2}(n-1)! \pmod{n}$ si n est impair.
4. Vérifier la valeur obtenue pour $(8!)^2 \pmod{17}$ en utilisant l'identité de la question 3 et l'identité (admise) $(p-1)! \equiv -1 \pmod{p}$ si p est premier.
5. Utiliser le fait que x^{-1} est différent de x dans $(\mathbb{Z}/(p\mathbb{Z}))^*$ pour $x \not\equiv \pm 1 \pmod{p}$ pour montrer l'identité $(p-1)! \equiv -1 \pmod{p}$ si p est premier.

Exercice 2. (~ 4 points) 1. Trouver le plus petit entier naturel x tel que

$$\begin{cases} x & \equiv 2004 \pmod{19}, \\ x & \equiv 2004 \pmod{11}. \end{cases}$$

2. Les comètes P/2004 V3 et P/2004 FY ont étés vues toutes les deux durant l'année 2004 et elles sont visibles tous les 19, respectivement tous les 11 ans.

(a) Quelle est la prochaine année durant laquelle on pourra voir les deux comètes?

(b) La comète P/2011 C2 a été vue en 2011 et elle est visible tous les 20 ans. Combien de temps s'écoule entre deux apparitions simultanées (dans la même année) des trois comètes P/2004 V3 et P/2004 FY et P/2011 C2?

Exercice 3. (~ 6 points)

1. Sachant que $2^{1022} \equiv 4 \pmod{1023}$, que peut-on en déduire (sans s'intéresser aux diviseurs de 1023) sur la primalité de l'entier 1023?

Dans la suite de cet exercice on se propose de vérifier indépendamment que 2^{1022} est effectivement congru à 4 modulo 1023.

2. Donner l'écriture binaire (écriture en base 2) de 1022.
3. Calculer $2^{1022} \pmod{11}$ en utilisant l'algorithme de l'exponentiation rapide et en détaillant les calculs.
4. Calculer $2^{1022} \pmod{31}$ en utilisant le théorème de Lagrange: $a^{\phi(n)} \equiv 1 \pmod{n}$ si a et n sont premiers entre eux. (Indication: $\phi(p) = p-1$ si p est premier.)
5. Calculer $2^{1022} \pmod{3}$ par la méthode de votre choix.
6. Utiliser les résultats des questions 2-4 pour vérifier que 2^{1022} est bien congru à 4 modulo 1023. (Indication: Combien vaut le produit $3 \cdot 11 \cdot 31$?)

Exercice 4. (~ 5 points)

1. Calculer les indicatrices d'Euler $\phi(8)$ et $\phi(12)$ de 8 et de 12.
2. Écrire la table du groupe multiplicatif $(\mathbb{Z}/8\mathbb{Z})^*$.
3. Écrire la table du groupe multiplicatif $(\mathbb{Z}/12\mathbb{Z})^*$.
4. Exhiber une bijection σ de $(\mathbb{Z}/8\mathbb{Z})^*$ dans $(\mathbb{Z}/12\mathbb{Z})^*$ qui vérifie $\sigma(ab) = \sigma(a)\sigma(b)$ pour tous les a, b dans $(\mathbb{Z}/8\mathbb{Z})^*$.