Examen du vendredi 01 juillet 2022, de 8h à 10h.

Sont autorisés : une calculatrice et une feuille manuscrite format A4 recto-verso. Autres documents et portables interdits.

Le sujet comporte 2 pages. Le barême est indicatif.

1. RESTES CHINOIS (6 POINTS)

Les écuries royales peuvent héberger au plus 150 chevaux.

Quand le roi sort avec toutes ses calèches d'apparat tirées par huit chevaux chacune, il reste 9 chevaux dans les écuries.

Quand tous les nobles de la Cour sortent par groupe de trois cavaliers pour une chasse royale, il reste 16 chevaux dans les écuries.

Durant une nuit sombre, sept voleurs font plusieurs aller-retours et emmènent chaque fois 7 chevaux. Au matin il ne reste que 48 chevaux dans les écuries.

Combien de chevaux ont été volés au roi ?

On pourra répondre aux questions suivantes

(1) Soit n le nombre de chevaux dans les écuries avant le vol. Quel est le reste de la division de n par 3 ? par 7 ? par 8 ? Écrire le systeme de congruences vérifié par n.

(2) Trouver les solutions dans $\mathbb{Z}$ au système de la question (1).

(3) On rappelle que les écuries peuvent héberger au plus 150 chevaux, peut-on déterminer le nombre de chevaux royaux avant le vol ? le nombre de chevaux volés ?

2. ÉVITONS LES DIVISIONS EUCLIDIENNES.

Soit p un entier, on représente un élément $\overline{a}$ de $\mathbb{Z}/p\mathbb{Z}$ par le reste de la division de a par p. Pour faire le produit $\overline{a}\times\overline{b}$ dans $\mathbb{Z}/p\mathbb{Z}$, on doit calculer le reste de la division par p du produit $a\times b$ de deux entiers $a,b\in[0,p[$. On va étudier une méthode qui permet pour certaines valeurs de p d'accélérer l'étape de calcul du reste de la division par p.

La troisième partie est indépendante des deux premières.

2.1. $p=11$ **(3 points).** Les humains travaillent habituellement en base 10. On va voir qu'on peut éviter de diviser lorsqu'on écrit les entiers en base 10 et que $p=10+1$.
On suppose aux trois premières questions que $a\times b$ s'écrit en base 10 avec 2 chiffres $\alpha\beta$.

(1) Déterminer en fonction de α et β le quotient et le reste de la division par 10 de $a\times b$.

(2) Quel est le quotient et le reste de la division par 11 de 67 ? Même question pour 65.

(3) Soient q et r le quotient et le reste de la division de $a\times b$ par 11. Lorsque $\alpha>\beta$, montrer que $q=\alpha-1$ et déterminer r. Que se passe-t-il si $\alpha\leq\beta$?

(4) Quelle est la valeur maximale possible pour $a\times b$ lorsque $a,b\in[0,p[$? Quelle est alors la valeur de $\overline{a\times b}$?

(5) Décrire une méthode permettant de calculer le produit de deux éléments de $\mathbb{Z}/11\mathbb{Z}$ sans effectuer de divisions.

2.2. $p = 17$ **(6 points).** Les ordinateurs travaillent habituellement en base une puissance de 2, par exemple en base 16=`0x10` (N.B. : le préfixe `0x` indique un nombre écrit en base 16). On va voir qu'on peut éviter de diviser lorsqu'on écrit les entiers en base `0x10` et que `p=0x11` ($p = 17$ en base 10).
On suppose aux trois premières questions que $a \times b$ s'écrit en base `0x10` avec 2 chiffres $\alpha\beta$.

(1) Déterminer en fonction de α et β le quotient et le reste de la division par `0x10` de $a \times b$.

(2) Quel est le quotient et le reste de la division par `0x11` de `0x67` ? Même question pour `0x65`.

(3) Soient q et r le quotient et le reste de la division de $a \times b$ par `0x11`. Lorsque $\alpha > \beta$, montrer que $q = \alpha - 1$ et déterminer r. Que se passe-t-il si $\alpha \leq \beta$?

(4) Quelle est la valeur maximale possible pour $a \times b$ lorsque $a, b \in [0, p[$? Quelle est alors la valeur de $\overline{a \times b}$?

(5) Décrire une méthode permettant de calculer le produit de deux éléments de $\mathbb{Z}/$`0x11`$\mathbb{Z}$ sans effectuer de divisions.

(6) Donner un algorithme en langage naturel ou C ou Python implémentant cette méthode. On pourra utiliser `(n >> 4)` et `(n & 0xf)` pour obtenir le quotient et le reste de `n` par `0x10`.

2.3. $p = 19$ **(6 points).** Principe : pour p premier, soit g un générateur de $\mathbb{Z}/p\mathbb{Z}^*$. Si a ou b est nul alors leur produit est nul. Si a et b sont non nuls, alors il existe α tel que $a = g^\alpha$ et $b = g^\beta$, donc $a \times b = g^{\alpha+\beta}$, on a transformé un produit en addition.

(1) Comment vérifie-t-on que 2 est un générateur de $\mathbb{Z}/19\mathbb{Z}$ en utilisant l'algorithme de la puissance rapide ?

(2) Déterminer la table des puissances de 2 modulo 19.

(3) Déterminer α et β pour $a = 11$ et $b = 10$.
En déduire $\gamma = \alpha + \beta \pmod{18}$, puis la valeur de 2^γ avec la table.
Vérifier en calculant $a \times b \pmod{19}$.

(4) Expliquer comment on peut calculer le produit de deux élément de $\mathbb{Z}/19\mathbb{Z}$ sans effectuer de division euclidienne.

(5) Peut-on généraliser cette méthode à d'autres valeurs de p ?