PRES Sorbonne-Paris Cité.
Université Paris 13
Institut Galilée
Licence Informatique Semestre 4 **feuille TD n° 4**

Congruences

Exercice 1.

(*i*) Démontrer que pour tout $n \in \mathbb{N}$, $n^2 + 4n + 7 \equiv 3 \quad (n+2)$.

(*ii*) En déduire le reste r dans la division euclidienne du nombre $n^2 + 4n + 7$ par le nombre $n + 2$.

Exercice 2. Quel est le reste de la division euclidienne de 2^{342} par 5.

Exercice 3. Montrer que $\forall n \in \mathbb{N}_*$, $(n+1)^n \equiv 1 \quad (n^2)$.

Exercice 4.

(*i*) Quel est le reste de la division euclidienne de 3^n par 5 ?

(*ii*) En déduire le reste de la division par 5 de 3^{3012}.

(*iii*) Montrer que $\forall n \in \mathbb{N}$, $3^{2n} \equiv (-1)^n \quad (5)$

(*iv*) En déduire que

  (*i*) $3^{2n} + 3^{2n+2} \equiv 0 \quad (5)$. Montrer que ce résultat peut être obtenu plus directement.

  (*ii*) Pour quelles valeurs de $a \in \mathbb{N}$ la somme

$$\sum_{k=a}^{2a+1} 3^{2k} \quad \text{est-elle divisible par 5 ?}$$

Exercice 5. Le numéro d'INSEE d'une personne est un nombre de 15 chiffres $c_1c_2 \cdots c_{13}c_{14}c_{15}$. Il se compose de plusieurs parties. $c_1 = 1ou2$ suivant le sexe ; c_2c_3 sont les deux derniers chiffres de l'année de naissance ; c_4c_5 code le mois de naissance ; c_6c_7 le département de naissance ; $c_8c_9c_{10}$ la commune de naissance ; $c_{11}c_{12}c_{13}$ le numéro d'inscription sur le registre d'état civil. Le nombre N représenté par ces 13 chiffres est divisé par 97 et son reste r permet de déterminer $K = c_{14}c_{15} = 97 - r$, appelé clé de contrôle.

(*i*) Comment déterminer cette clé avec une calculatrice qui n'effectue pas de calculs exacts sur des nombres à 13 chiffres ?

(*ii*) Déterminer les entiers a et b tels que $N = a.10^6 + b$.

(*iii*) Déterminer le reste de la division euclidienne de 10^6 par 97 (On pourra utiliser une puissance plus petite).

(*iv*) En déduire que $K \equiv_{97} 97 - 27a - b$.

(*v*) Vous trouvez la carte vitale suivante dont le nom du propriétaire et les deux derniers chiffres sont effacés. Les 13 premiers chiffres sont 1540454208091. Que savez-vous de son propriétaire. Restaurer les deux derniers chiffres.

(*vi*) Si vous inversez c_{12} et c_{13}, l'erreur sera-t-elle détectée ?

(*vii*) Si l'on change le code commune en 305, l'erreur sera-t-elle détectée ?

Exercice 6. On considère un polynôme P à coefficients entiers relatifs $a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$.

(i) Montrer que si $x \in \mathbb{Z}$ est une racine entière de P, alors $x|a_0$.
(ii) Que peut-on dire du polynôme $X^4 - 3X^3 + 2X^2 - 3X + 21$?

Exercice 7. On considère la suite (u_n) d'entiers naturels définie par $u_0 = 14$ et $u_{n+1} = 5u_n - 6$
(i) Quelle conjecture peut-on faire sur les deux derniers chiffres de u_n ?
(ii) Montrer que $\forall n \in \mathbb{N}$, $u_{n+2} \equiv_4 u_n$
(iii) En déduire que pour tout $k \in \mathbb{N}$, $u_{2k} \equiv_4 2$ et $u_{2k+1} \equiv_4 0$
(iv) Montrer que $\forall n \in \mathbb{N}$, $2u_n = 5^{n+2} + 3$
(v) En déduire que $\forall n \in \mathbb{N}$, $2u_n \equiv_{100} 28$
(vi) Déterminer les deux derniers chiffres de l'écriture en base 10 de u_n.

Exercice 8. Soit p un nombre premier plus grand que 10 et l entier tel que $10^l < p < 10^{l+1}$
(i) Montrer que si $1 \leq a \leq 9$ et si n est un entier, les nombres $a10^n$ et p sont premiers entre eux.
(ii) Montrer que si $n = (a_k \cdots a_4a_3a_2a_1a_0)_{10}$ la représentation de n en base 10, alors il existe des entiers uniques $b_{l+1}, \cdots b_k$ strictement plus petits que p tels que :
$n \equiv a_0 + 10a_1 + \cdots + a_l10^l + b_{l+1}a_{l+1} + \cdots b_ka_k$ modulo p
(iii) appliquer à $p = 7$ et $k = 4$

Exercice 9. Quel est le dernier chiffre dans l'écriture décimale de 7777^{7777} ?

Exercice 10. (i) Soit $n \in \mathbb{N}$. Montrer que n^3 est congru à $0, 1, 8$ modulo 9.
(ii) En déduire que l'équation $x^3 + y^3 = z^3 + 4$ n'a pas de solutions entières.
(iii) Montrer en utilisant une congruence à trouver que l'équation $x^2 - 5y^2 = 3$ n'a pas de solutions entières.

Exercice 11. Simplifier les expressions suivantes :
(i) $1000^{10000} \pmod{11}$.
(ii) $25^{15} \pmod{31}$.
(iii) $27^9 \pmod{20}$.

Exercice 12. Résoudre $ax \equiv_n 1$ selon les valeurs de a et n.

Exercice 13. On va déterminer tous les entiers premiers p et q tels que $pq \mid (5^p - 2^p)(5^q - 2^q)$.
(i) Montrer que 3 est le seul entier premier p tel que $p \mid (5^p - 2^p)$.
(ii) Montrer que, si (p, q) est une solution, alors $p = 3$ ou $q = 3$.
(iii) Si $(3, q)$ est une solution, déterminer toutes les valeurs possibles de q.

Exercice 14. Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par trois colonnes, il reste deux soldats, rangés par cinq colonnes, il reste trois soldats et, rangés par sept colonnes, il reste deux soldats ?

Exercice 15. Solutions du système de Scaliger, qui détermine le cycle calendaire julien. Le cycle de 15 ans est celui de l'addiction romaine (cycle d'imposition), celui de 19 ans le cycle de Méton correspondance approximative solaire-lunaire, celui de 28 le cycle année/semaine.
Montrer que le système de Scaliger $\begin{cases} 532\,x \equiv 1 \pmod{15} \\ 285x \equiv 1 \pmod{28} \\ 420x \equiv 1 \pmod{19} \end{cases}$ équivaut à $\begin{cases} 7\,x \equiv 1 \pmod{15} \\ 5x \equiv 1 \pmod{28} \\ 2x \equiv 1 \pmod{19} \end{cases}$ puis le résoudre.

Exercice 16. Le magicien dit : « Choisissez, sans me le dire, un nombre entier entre 1 et 500. Je vais seulement vous demander trois nombres construits à l'aide de celui-ci et je retrouverais sans trop de difficulté le nombre que vous aviez choisi.
Pour cela, diviser votre nombre par 5 et donner moi le reste obtenu. Faites de même avec la division par 7 et celle par 19. Ces trois restes me suffisent pour retrouver votre nombre. »
(i) Expliquer pourquoi le magicien trouve toujours le bon nombre.
(ii) Amusez-vous bien.