UGA-IUT2-Grenoble
Département Informatique

Année Universitaire 2021-2022

R1.06 Mathématiques discrètes
TD 4 : Congruence, théorème Chinois, Fermat et Euler

Calculs avec congruences

Exercice 1 Calculez :

- $-2 \times 5 \pmod 3$
- $13 \times 7 \pmod 9$
- $14 + 71 \pmod{83}$
- $14 + 82 \pmod{83}$
- $13 \times 29 - 7 \times 18 \pmod{11}$
- $7^3 \pmod{10}$
- $7^{401} \pmod{10}$
- $2^{1147} \pmod{17}$
- $18 \times 2^{17} \pmod 7$

Exercice 2 Traduire les phrases suivantes à l'aide de congruences.

1. n est un entier pair.
2. n est un entier impair.
3. les restes des divisions euclidiennes de a et de b par n sont identiques.
4. $n^7 + 2n^3$ est divisible par 3.
5. On dispose d'un nombre inconnu d'objets. Lorsqu'on les regroupe par 3 il en reste 2, lorsqu'on les regroupe par 5 il en reste 3 et lorsqu'on les regroupe par 7 il en reste 2.
6. Le chiffre des unités de l'entier n est 6.
7. Le reste de la division euclidienne par 8 du carré d'un entier impair est égal à 1.

Exercice 3 Tableaux de congruences.

1. Compléter la table de congruences modulo 5 suivante :

n	0	1	2	3	4
n^2					
n^3					
n^4					

2. Utiliser un tableau de congruence pour résoudre dans $\mathbb{Z}$, $3x \equiv 5 \pmod 7$.
3. Utiliser un tableau de congruence pour résoudre dans $\mathbb{Z}$, $4x \equiv 2 \pmod 6$.

Exercice 4 Calculs avec des congruences

1. Montrez que $34^{56} - 1$ est un multiple de 11.

2. Montrer que $9518^{42} - 4$ est divisible par 5.

3. Montrez que pour tout n entier naturel, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

4. Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est impair. Dans le cas où n est pair, donner le reste de la division de $7^n + 1$ par 8.

5. Soit n naturel impair.
   (a) Montrer que $(n-1)(n+1)$ est divisible par 4.
   (b) En déduire que $n^2 \equiv 1 \pmod 4$.
   (c) Que dire du carré de tout naturel pair?

Le théorème des restes chinois

Théorème 1 *des restes chinois*
Soient a_1 et a_2 deux entiers et n_1 et n_2 deux entiers premiers entre eux.
Alors les entiers relatifs x vérifiant le système suivant $\left\{ \begin{array}{ll} x \equiv a_1 & \pmod{n_1} \\ x \equiv a_2 & \pmod{n_2} \end{array} \right.$
s'écrivent $x \equiv a_1 \times un_2 + a_2 \times vn_1 \pmod{n_1 n_2}$
où u et v sont tels que $un_2 + vn_1 = 1$.

Application : Résoudre $\left\{ \begin{array}{l} x \equiv 3 (mod\ 5) \\ x \equiv 2 (mod\ 7) \end{array} \right.$

1. $pgcd(5,7) = 1$ donc on peut appliquer le théorème des restes chinois.

2. Le calcul des coefficients de Bézout donne $5 \times (-4) + 3 \times 7 = 1$

3. donc, $x \equiv 5 \times (-4) \times 2 + 3 \times 7 \times 3 (mod\ 35)$ d'où $x \equiv 23 (mod\ 35)$

Exercice 5 1. (a) Déterminer les coefficients u et v de l'égalité de Bezout : $3 \times u + 5 \times v = 1$.
(b) En utilisant ces coefficients, résoudre dans $\mathbb{Z}$ le systèmes suivant : $\left\{ \begin{array}{l} x \equiv 1\ (mod\ 3) \\ x \equiv 2\ (mod\ 5) \end{array} \right.$

(c) En déduire les solutions dans $\mathbb{Z}$ du système : $\left\{ \begin{array}{l} x \equiv 1\ (mod\ 3) \\ x \equiv 2\ (mod\ 5) \\ x \equiv 3\ (mod\ 7) \end{array} \right.$

2. (a) Pour tout $(p,q,r) \in \mathbb{Z}^* \times \mathbb{Z} \times \mathbb{Z}$, prouver que :
$$\forall x \in \mathbb{Z},\ p\,x \equiv p\,r\ (mod\ p\,q) \Leftrightarrow x \equiv r\ (mod\ q)$$
(b) En procédant à un changement de variable approprié, résoudre dans $\mathbb{Z}$ le système suivant : $\left\{ \begin{array}{l} x \equiv 4\ (mod\ 6) \\ x \equiv 0\ (mod\ 10) \end{array} \right.$

(c) Déduire de la question 2.(b), les solutions dans $\mathbb{Z}$ du système : $\left\{ \begin{array}{l} x \equiv 4\ (mod\ 6) \\ x \equiv 0\ (mod\ 10) \\ x \equiv 3\ (mod\ 7) \end{array} \right.$

Exercice 6 Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier chinois. Celui-ci recevrait alors trois pièces. Mais les pirates se querellent et sept d'entre eux sont tués. Le cuisinier recevrait alors quatres pièces après partage entre les pirates restants. Dans un naufrage ultérieur, seuls, le butin, six pirates et le cuisinier sont sauvés et le partage laisse toujours quatres pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates?

Exercice 7 Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$(a)\left\{\begin{array}{l} x \equiv 1\ (mod\ 3) \\ x \equiv 1\ (mod\ 5) \\ x \equiv 1\ (mod\ 7) \end{array}\right. \qquad (b)\left\{\begin{array}{l} x \equiv 3\ (mod\ 6) \\ x \equiv 1\ (mod\ 10) \end{array}\right. \qquad (c)\left\{\begin{array}{l} x \equiv 3\ (mod\ 6) \\ x \equiv 2\ (mod\ 10) \end{array}\right.$$

Le petit théorème de Fermat et le théorème d'Euler

Exercice 8 1. Utiliser le petit théorème de Fermat pour calculer :

- 27^{134} (mod 11)
- 31^{94} (mod 19)

2. Calculer $\varphi(97)$, $\varphi(24)$, $\varphi(1024)$, $\varphi(485)$.

3. Utiliser le théorème d'Euler pour calculer :

- 3^{121} (mod 77)
- 2^{1000} (mod 55)

Exercice 9 1. Calculer 2^{50} $(mod\ 45)$

2. Calculer 5^{145} $(mod\ 24)$

3. Calculer le reste de la division euclidienne de 3^{83} par 20.

4. Calculer le reste de la division euclidienne de $(18^{13})^{18}$ par 13.

Exercice 10 1. Quel est le dernier chiffre du nombre 3^{1998}?

2. donner les deux derniers chiffres de 7^{9^7}.

Exercice 11 En utilisant le petit théorème de Fermat, donner un multiple de 7 dont l'écriture en base dix est de la forme 99...9. (Un nombre de la forme 99...9, peut également s'écrire sous la forme $10^k - 1$)

Exercice 12 Soit $n \in \mathbb{N}$. Décomposer n en facteurs premiers, sachant que $\varphi(n) = (p_1^2 - p_1)(p_2 - 1)(p_3 - 1)$ et que p_1, p_2, p_3 sont des nombres premiers quelconques, distincts et différents de 2.

Exercice 13 Démontrer que chacune des relations suivantes est vraie pour tout $n \in \mathbb{N}$

- 5 divise $2^{2n+1} + 3^{2n+1}$
- 6 divise $5n^3 + n$
- 7 divise $3^{2n+1} + 2^{n+2}$
- 9 divise $4^n - 1 - 3n$
- 6 divise $n^3 - n$
- 6 divise $4(4^{2n} - 1)$
- 8 divise $5^n + 2 \times 3^{n-1} + 1$
- 11 divise $3^{n+3} - 4^{4n+2}$

Exercices supplémentaires

Exercice 14 *1. Quel est le reste de la division entière de* 55^{7975} *par 12?*

2. Montrer que $2^{100} + 3^{100}$ *est multiple de 97.*

Exercice 15 *1. Calculer le reste de 936 dans la division par 55, puis le reste de 496 dans la division par 55.*
2. Utiliser ces deux résultats pour en déduire le reste de $16^{15} \times 26^{17} \times 31^{15} \times 36^{18}$ *dans la division par 55.*

Exercice 16 *Démontrer que chacune des relations suivantes est vraie pour tout* $n \in \mathbb{N}$.

- 11 *divise* $2^{6n+3} + 3^{2n+1}$
- 17 *divise* $2^{6n+3} + 3^{4n+2}$
- 16 *divise* $5^n - 1 - 4n$