UNIVERSITÉ DE RENNES 1
UFR Mathématiques

Licence-portail MIPE

NOMBRES ENTIERS ET RATIONNELS,
CONGRUENCES, PERMUTATIONS(A02)

Proposition de corrigé pour l'examen du Mardi 9 mai 2006

EXERCICE 1

1. **Montrer, par récurrence sur n, que pour tout entier $n \geq 1$, 4^n+5 est multiple de 3.**

   Soit pour n entier ≥ 1 la propriété $\mathcal{P}(n)$: "4^n+5 multiple de 3".
   La propriété $\mathcal{P}(1)$ s'écrit "$4+5$ multiple de 3", ce qui est vrai.
   Soit n entier ≥ 1. Supposons $\mathcal{P}(n)$ vraie. Alors il existe k dans $\mathbb{Z}$ tel que $4^n+5=3\,k$.
   Fixons un tel k.

   $$\begin{aligned} 4^{n+1}+5 &= 4\times 4^n+5 \\ &= 4\times(4^n+5)-15 \\ &= 4\times 3\,k-5\times 3 \\ &= 3\times(4\,k-5) \end{aligned}$$

   donc $4^{n+1}+5$ est multiple de 3 et $\mathcal{P}(n+1)$ est vraie.
   Conclusion : $\mathcal{P}(n)$ est vraie pour tout entier $n \geq 1$.

2. **Proposer une démonstration de ce résultat qui n'utilise pas le principe du raisonnement par récurrence.**

   Soit n un entier ≥ 1.

   $$\begin{aligned} 4^n+5 &\equiv 1^n+5 \pmod 3 \quad \text{car } 4\equiv 1 \pmod 3 \\ &\equiv 0 \pmod 3 \end{aligned}$$

   donc, par définition de la congruence modulo 3, 4^n+5 est multiple de 3.

EXERCICE 2

1. **Calculer le reste de la division euclidienne de 2^{11} par 23.**

   On a : $11=1+2+2^3$. On en déduit $2^{11}=2\times 2^2\times 2^8$. De plus

   $$\begin{cases} 2\equiv 2 \pmod{23} \\ 2^2\equiv 4 \pmod{23} \\ 2^4\equiv 16 \pmod{23} \equiv -7 \pmod{23} \\ 2^8\equiv 49 \pmod{23} \equiv 3 \pmod{23} \end{cases}$$

   Donc $2^{11}\equiv 2\times 4\times 3 \pmod{23} \equiv 1 \pmod{23}$.
   Le reste de la division euclidienne de 2^{11} par 23 est égal à 1.

2. **En déduire l'ordre multiplicatif modulo 23 de 2.**

   Comme 23 est un nombre premier, les ordres multiplicatifs modulo 23 sont des diviseurs de 22. Ce sont donc 1, 2, 11 ou 22. D'après les calculs précédents, 2^1 et 2^2 ne sont pas congrus à 1 modulo 23 et $2^{11}\equiv 1 \pmod{23}$ donc 11 est le plus petit entier non nul k vérifiant $2^k\equiv 1 \pmod{23}$. L'ordre multiplicatif modulo 23 de 2 est égal à 11.
   Bonus : 2 est-il un générateur multiplicatif modulo 23 ?
   Un entier w non multiple de 23 est un générateur multiplicatif modulo 23 si, et seulement si, son ordre multiplicatif est égal à 22. Comme l'ordre multiplicatif modulo 23 de 2 est égal à 11, 2 n'est pas un générateur multiplicatif modulo 23.

EXERCICE 3

1. **Résoudre dans $\mathbb{Z}$ l'équation $5\,x\equiv 1 \pmod{13}$.**

   Comme 5 et 13 sont premiers, ils sont premiers entre eux donc 5 est inversible modulo 13. Calculons son inverse par l'algorithme d'Euclide étendu.

   $$\begin{array}{lrcl} & 13 &=& 13\times 1 + 5\times 0 \quad \text{initialisation} \\ (\times 2) & 5 &=& 13\times 0 + 5\times 1 \quad \text{initialisation} \\ (\times 1) & 3 &=& 13\times 1 + 5\times(-2) \\ (\times 1) & 2 &=& 13\times(-1) + 5\times 3 \\ (\times 1) & 1 &=& 13\times 2 + 5\times(-5) \end{array}$$

   Donc $5\,x\equiv 1 \pmod{13} \Leftrightarrow x\equiv -5 \pmod{13} \equiv 8 \pmod{13}$.
   L'ensemble des solutions de l'équation est donc $S=\{8+13\,k, k\in\mathbb{Z}\}$.

2. **Calculer 3^6 modulo 13. En déduire si 10 est un carré ou non modulo 13.**

   $3^6=3^2\times 3^4$ et $3^2\equiv -4 \pmod{13}$, $3^4\equiv 3 \pmod{13}$,
   donc $3^6\equiv -4\times 3 \pmod{13} \equiv 1 \pmod{13}$.
   Comme 13 est un nombre premier et 10 n'est pas multiple de 13, 10 est un carré modulo 13 si, et seulement si, $10^{\frac{13-1}{2}}\equiv 1 \pmod{13}$.
   Or $10^6\equiv(-3)^6 \pmod{13} \equiv 3^6 \pmod{13}$ donc $10\equiv 1 \pmod{13}$ et 10 est un carré modulo 13.

3. **Résoudre dans $\mathbb{Z}$ l'équation $5x^2-2x+10\equiv 0 \pmod{13}$.**

   D'après la question 1, 5 est inversible modulo 13 et possède pour inverse 8 donc

   $$5x^2-2x+10\equiv 0 \pmod{13} \Leftrightarrow 8\,(5x^2-2x+10)\equiv 0 \pmod{13}$$

   Après simplification, on fait apparaître le début d'un carré :

   $$\begin{aligned} 5x^2-2x+10\equiv 0 \pmod{13} &\Leftrightarrow x^2-16x+80\equiv 0 \pmod{13} \\ &\Leftrightarrow x^2-2\times 8\,x+2\equiv 0 \pmod{13} \\ &\Leftrightarrow (x-8)^2-64+2\equiv 0 \pmod{13} \quad \text{(on a reconnu le début d'un carré)} \\ &\Leftrightarrow (x-8)^2\equiv 10 \pmod{13} \end{aligned}$$

   D'après la question précédente, 10 est un carré modulo 13, donc l'équation a deux solutions modulo 13. Pour les déterminer, on cherche a entier tel que $a^2\equiv 10 \pmod{13}$.

$2^2 = 4, 3^2 = 9, 4^2 = 16 \equiv 3 \pmod{13}, 5^2 = 25 \equiv 12 \pmod{13}, 6^2 = 36 \equiv 10 \pmod{13}$.

$$\begin{aligned} 5x^2 - 2x + 10 \equiv 0 \pmod{13} &\Leftrightarrow (x-8)^2 \equiv 6^2 \pmod{13} \\ &\Leftrightarrow (x-8-6)(x-8+6) \equiv 0 \pmod{13} \\ &\Leftrightarrow x \equiv 1 \pmod{13} \text{ ou } x \equiv 2 \pmod{13} \quad \text{(lemme d'Euclide)} \end{aligned}$$

EXERCICE 4

1. 5 **est-il inversible modulo** 22 **? Si oui, quel est son inverse ?**

   5 est premier et ne divise pas 22 donc les deux entiers sont premiers entre eux. Pour calculer l'inverse de 5 modulo 22 on applique l'algorithme d'Euclide étendu à 22 et 5.

   $$\begin{array}{rrcl} & 22 & = & 22 \times 1 + 5 \times 0 \quad \text{initialisation} \\ (\times 4) & 5 & = & 22 \times 0 + 5 \times 1 \quad \text{initialisation} \\ (\times 2) & 2 & = & 22 \times 1 + 5 \times (-4) \\ & 1 & = & 22 \times (-2) + 5 \times (9) \end{array}$$

   Donc l'inverse de 5 modulo 22 est égal à 9.

2. 110 **est-il inversible modulo** 63 **? Si oui, quel est son inverse ?**

   Les décompositions de 110 et de 63 en produits de facteurs premiers sont : $110 = 2 \times 5 \times 11$ et $63 = 3^2 \times 7$. Les deux entiers n'ont pas de facteurs premiers communs, donc ils sont premiers entre eux et 110 est bien inversible modulo 63.
   On remarque que $110 \equiv 47 \pmod{63}$ donc pour calculer l'inverse de 110 modulo 63, on applique l'algorithme d'Euclide étendu à 63 et à 47.

   $$\begin{array}{rrcl} & 63 & = & 63 \times 1 + 47 \times 0 \quad \text{initialisation} \\ (\times 1) & 47 & = & 63 \times 0 + 47 \times 1 \quad \text{initialisation} \\ (\times 2) & 16 & = & 63 \times 1 + 47 \times (-1) \\ (\times 1) & 15 & = & 63 \times (-2) + 47 \times 3 \\ & 1 & = & 63 \times 3 + 47 \times (-4) \end{array}$$

   L'inverse de 110 modulo 63 est donc -4 ou 59.

3. **Trouver le plus petit entier** x **positif vérifiant**

   $$\begin{cases} x \equiv 2 \pmod{5} & (1) \\ x \equiv 12 \pmod{22} & (2) \\ x \equiv 18 \pmod{63} & (3) \end{cases}$$

   Comme les entiers 5, 22 et 63 sont premiers entre eux *deux à deux*, d'après le théorème chinois, ce système possède une solution unique modulo $5 \times 22 \times 63 = 6930$.
   On écrit

   $$x = a_1 + 5 \times a_2 + 5 \times 22 \times a_3 + 5 \times 22 \times 63 \times k$$

   avec $0 \leq a_1 < 5$, $0 \leq a_2 < 22$, $0 \leq a_3 < 63$ et $k \in \mathbb{Z}$.
   – D'après (1), $a_1 \equiv 2 \pmod{5}$. On pose $a_1 = 2$.
   – D'après (2), $2 + 5\,a_2 \equiv 12 \pmod{22}$ soit $5 \times a_2 \equiv 10 \pmod{22}$. D'après la question 1., l'inverse de 5 modulo 22 est égal à 9 donc on obtient : $a_2 \equiv 90 \pmod{22}$. On pose $a_2 = 2$.

   – D'après (3), $2 + 5 \times 2 + 110 \times a_3 \equiv 18 \pmod{63}$ soit $110 \times a_3 \equiv 6 \pmod{63}$. D'après la question 2., l'inverse de 110 modulo 63 est égal à -4 donc on obtient $a_3 \equiv -4 \times 6 \pmod{63} \equiv 39 \pmod{63}$. On pose $a_3 = 39$.
   Les solutions sont donc les $2 + 5 \times 2 + 110 \times 39 + 6930 \times k = 4302 + 6930 \times k$ où k décrit $\mathbb{Z}$. La plus petite des solutions positives est 4302.

EXERCICE 5

Dans tout l'exercice n **désignera l'entier** 133**.**

1. **Factoriser** n **et calculer** $\varphi(n)$**.**

   $n = 7 \times 19$ avec 7 et 19 nombres premiers distincts donc $\varphi(n) = (7-1) \times (19-1) = 108$.

2. **Montrer que l'ordre multiplicatif modulo** n **de** 12 **est égal à** 6**.**

   L'ordre multiplicatif modulo n de 12 est le plus petit entier k non nul tel que $12^k \equiv 1 \pmod{n}$.
   Or

   $$\begin{aligned} &12^1 \equiv 12 \pmod{133} \\ &12^2 \equiv 144 \pmod{133} \equiv 11 \pmod{133} \\ &12^3 \equiv 12^2 \times 12 \pmod{133} \equiv 132 \pmod{133} \equiv -1 \pmod{133} \\ &12^4 \equiv -12 \pmod{133} \\ &12^5 \equiv -11 \pmod{133} \\ &12^6 \equiv (12^3)^2 \pmod{133} \equiv 1 \pmod{133} \end{aligned}$$

   L'ordre multiplicatif modulo n de 12 est donc bien égal à 6.

3. **Quel est l'inverse de** 5 **modulo** 108 **?**

   On applique l'algorithme d'Euclide étendu à 108 et à 5.

   $$\begin{array}{rrcl} & 108 & = & 108 \times 1 + 5 \times 0 \quad \text{initialisation} \\ (\times 21) & 5 & = & 108 \times 0 + 5 \times 1 \quad \text{initialisation} \\ (\times 1) & 3 & = & 108 \times 1 + 5 \times (-21) \\ (\times 1) & 2 & = & 108 \times (-1) + 5 \times 22 \\ & 1 & = & 108 \times 2 + 5 \times (-43) \end{array}$$

   L'inverse de 5 modulo 108 est égal à -43 ou 65.

4. **Dans le cryptosystème RSA, vous choisissez la clé publique** $(133, 5)$**. Le secrétariat veut vous transmettre un message** $m \in \{0, \ldots, 132\}$**. Il chiffre** m **en** $M = 12$ **en utilisant le chiffrement RSA et vous transmet** M**.**
   Vous recevez M**. Que vaut** m **?**

   Pour retrouver m, on calcule le reste de la division euclidienne de M^d par 133 où d est l'inverse modulo $\varphi(133)$ de 5.
   Or d'après la question 1., $\varphi(133) = 108$ et d'après la question 3., l'inverse de 5 modulo 108 est égal à 65, donc $d = 65$.
   De plus, d'après la question 2., l'ordre multiplicatif modulo 133 de 12 est égal à 6, donc $M^d \equiv 12^{6 \times 10 + 5} \pmod{133} \equiv (12^6)^{10}\, 12^5 \pmod{133} \equiv 12^5 \pmod{133} \equiv -11 \pmod{133} \equiv 122 \pmod{133}$.
   Le message initial était donc $m = 122$.