Université Paris Diderot
Département de Sciences Exactes

MI4– Année 2009/10
L2 Info

Un corrigé du partiel du 20 mars 2010 :

Les exercices sont indépendants. Les documents autorisés sont le polycopié, les notes de cours et TD. Les calculatrices ne sont pas autorisées. On rappelle que $\phi(n)$ désigne l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1 *Résoudre en nombres entiers les équations*

$$1263x + 421y = 4 \tag{1}$$

$$1263x + 420y = 21 \tag{2}$$

On commence par calculer avec l'algorithme d'Euclide $d := \text{pgcd}(1263, 421)$ Comme $1263 = 3.421 + 0$ on trouve $d = 421$. La première équation n'a pas de solutions entières puisque 421 ne divise pas 4.

Pour la deuxième équation, on commence par calculer avec l'algorithme d'Euclide $d := \text{pgcd}(1263, 420)$. Comme $1263 = 3.420 + 3$ et $420 = 3.140 + 0$, on trouve $d = 3$. De plus le calcul donne $3 = 1263 - 3.420$. On observe que $d = 3$ divise 21 donc l'équation possède des solutions qui sont les mêmes que $421x + 140y = 7$. De l'identité de Bézout $1 = 421 - 3.140$ on tire une première solution $7 = 421.7 - 140.21$ i.e. $(x_0, y_0) = (7, -21)$. Les autres solutions s'obtiennent en écrivant $421(x - x_0) + 140(y - y_0) = 0$ et donc $x = x_0 + 140m$, $y = y_0 - 421m$ d'où l'ensemble des solutions

$$S = \{(x, y) = (7 + 140m, -21 - 421m) \mid m \in \mathbb{Z}\}$$

[NOTA. Dans l'examen distribué le "420" de la seconde l'équation avait été accidentellement remplacé par "421", ce qui simplifiait la résolution puisqu'il n'y avait aucune solution.]

Exercice 2 *Résoudre en nombres entiers les systèmes d'équations suivantes*

$$\begin{cases} x & \equiv & 2 & \mod 17 \\ x & \equiv & 3 & \mod 33 \end{cases} \tag{3}$$

$$\begin{cases} x & \equiv & 5 & \mod 35 \\ x & \equiv & 8 & \mod 133 \end{cases} \tag{4}$$

$$\begin{cases} x & \equiv & 2 & \mod 17 \\ x & \equiv & 3 & \mod 33 \\ x & \equiv & 1 & \mod 28 \end{cases} \tag{5}$$

On applique le théorème chinois : on calcule d'abord $d = \text{pgcd}(33, 17)$ qui vaut 1 et on en déduit une identité de Bézout, ici $1 = 2.17 - 33$. Comme le pgcd

est 1, les solutions existent et forment une classe de congruence modulo 17.33. Pour calculer une solution écrivons $x = 2+17.h = 3+33.k$ donc $1 = 17.h-33.k$, cette équation possède une solution $(h, k) = (2, 1)$ qui correpond à $x_0 = 36$. L'ensemble des solutions du premier système est l'ensemble des entiers $x \equiv 36 \mod 17.33$.

Pour le deuxième système, on calcule d'abord $d = \text{pgcd}(35, 133)$ qui vaut 7. La condition pour l'existence de solution s'écrit donc 7 divise $8 - 5$, qui n'est pas vérifiée ; il n'y a donc aucune solution.

Pour le troisième système, on peut remplacer les deux première congruences par $x \equiv 36 \mod 33.17$ et résoudre le système :

$$\begin{cases} x & \equiv & 36 & \mod 33.17 \\ x & \equiv & 1 & \mod 28 \end{cases}$$

On calcule donc $\text{pgcd}(33.17, 28)$ qui vaut 1 et conclut que l'ensemble des solutions est une classe de congruence modulo $33.17.28 = 15708$. L'algorithme d'Euclide-Bézout donne $33.17 = 561 = 20.28 + 1$ donc $\text{pgcd}(561, 28) = 1 = 561-20.28$. On cherche une solution sous la forme $x_0 = 36+561k = 1+28h$ donc $35 = -561k + 28h$; une solution est donnée par $k = -35$ (et $h = -20.35$) soit encore $x_0 = 36 - 35.561 = -19599$ ou, si l'on veut une solution dans $[0, 16708]$, $x_1 = 11817$. L'ensemble des solutions du premier système est l'ensemble des entiers $x \equiv 11817 \mod 17.33.28$.

Exercice 3 *Déterminer le reste de la division par* 11 *de* 2205^{2302} *puis le reste de la division par* 23 *de* $2304^{2205^{2302}}$.

On a $2205 \equiv 5 \mod 11$, de plus le petit théorème de Fermat nous garantit que $5^{10} \equiv 1 \mod 11$ donc

$$2205^{2302} \equiv 5^{2302} \equiv (5^{10})^{230}5^2 \equiv 5^2 \equiv 3 \mod 11.$$

Le reste de la division par 11 est donc 3.

On a $2304 \equiv 4 \mod 23$. Le petit théorème de Fermat nous garantit que $4^{11} = 2^{22} \equiv 1 \mod 23$ donc

$$2304^{2205^{2302}} \equiv 4^{2205^{2302}} \equiv 4^{11.r+3} \equiv 4^3 \equiv 18 \mod 23.$$

Le reste de la division par 23 est donc 18.

Exercice 4 *Soit* $n = 6188 = 4.7.13.17$

1. *Calculer* $\phi(n)$ *(sous forme factorisée).*
2. *Montrer que si* $\text{pgcd}(a, n) = 1$ *alors* $a^{16} \equiv 1 \mod 17$ *et établir un résultat similaire mod* 4, *mod* 7 *et mod* 13
3. *En déduire que si* $\text{pgcd}(a, n) = 1$ *alors* $a^{48} \equiv 1 \mod n$.

On utilise les deux règles $\phi(nm) = \phi(n)\phi(m)$ [si $\text{pgcd}(m,n) = 1$] et $\phi(p^r) = p^r - p^{r-1}$ [si p premier] pour obtenir :

$$\phi(n) = \phi(4)\phi(7)\phi(13)\phi(17) = (4-2)(7-1)(13-1)(17-1) = 2.6.12.16 = 2^8 3^2.$$

D'après le théorème d'Euler (de Fermat pour un module premier) on sait $a^{16} \equiv 1 \mod 17$, $a^2 \equiv 1 \mod 4$, $a^6 \equiv 1 \mod 7$ et $a^{12} \equiv 1 \mod 13$ dès que a est premier avec le module de congruence. En notant que $\text{ppcm}(16,2,6,12) = 48$ on voit que pour a premier avec n, on aura $a^{48} \equiv 1 \mod 17, \mod 4, \mod 7$ et $\mod 13$ donc $a^{48} \equiv 1 \mod n$.

Exercice 5 *La lettre p désigne un nombre premier différent de 3, on étudie l'équation suivante dans $\mathbb{Z}/p\mathbb{Z}$:*

$$x^2 + x + 1 = 0. \tag{6}$$

1. *Montrer qu'une solution de l'équation (6) est un élément d'ordre trois dans $(\mathbb{Z}/p\mathbb{Z})^*$. En déduire que si $p \equiv 2 \mod 3$ alors l'équation (6) n'a pas de solution.*
2. *Résoudre l'équation pour $p = 7$ puis $p = 13$.*
3. *Soit $p \equiv 1 \mod 3$, soit a un élément générateur du groupe $(\mathbb{Z}/p\mathbb{Z})^*$, déterminer les entiers k tels que $x = a^k$ soit solution de (6).*

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps l'équation (6) possède au plus deux solutions.

En utilisant l'identité $x^3 - 1 = (x^2 + x + 1)(x - 1)$ on voit qu'une racine de l'équation (6) vérifie $x^3 = 1$ de plus elle ne peut être égale à 1 car sinon on aurait $3 = 1^2 + 1 + 1 = 0$ et donc $p = 3$, ce que l'énoncé exclut. Une racine est donc un élément d'ordre trois dans $(\mathbb{Z}/p\mathbb{Z})^*$. S'il existe une racine on peut en déduire que 3 divise le cardinal de $(\mathbb{Z}/p\mathbb{Z})^*$, c'est-à-dire $p \equiv 1 \mod 3$. Il ne peut donc y avoir de solution si $p \equiv 2 \mod 3$.

Si $p = 7$, on trouve une première solution $x_1 = 2$ car $2^3 \equiv 1 \mod 7$ et la deuxième est $x_2 = x_1^2 = 4$. Si $p = 13$, on trouve une première solution $x_1 = 3$ car $3^3 \equiv 1 \mod 13$ et la deuxième est $x_2 = x_1^2 = 9$.

L'élément $x = a^k$ est solution de (6) si et seulement si $x \neq 1$ et $x^3 = 1$ donc si et seulement si k n'est pas divisible par $p-1$ mais $3k$ est divisible par $p-1$; on peut en déduire que (modulo $p-1$) on a $k = \frac{p-1}{3}$ ou $k = 2\frac{p-1}{3}$ ainsi l'ensemble des solutions est

$$S = \left\{ a^{\frac{p-1}{3}} \, , \, a^{2\frac{p-1}{3}} \right\}.$$