Universite Paris Diderot — MI4{ Annee 2014/15
Departement de Sciences Exactes — L2 Info

Partiel du 21 mars 2015

Les exercices sont indépendants. On peut apporter un page A4 et écrire les formules et théorèmes de mon cours. MAIS il n'y a pas d'autres documents autorisés, ni ploy, ni TD, ni notes de cours. Les calculatrices ne sont pas autorisées. On rappelle que $\varphi(n)$ désigne l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et que « résoudre »une équation signifie trouver toutes ses solutions.

Exercice 1 Resoudre en nombres entiers l'equation :

$$924x + 469y = 15. \tag{1}$$

Même question avec l'equation :

$$924x + 469y = 21. \tag{2}$$

On commence par calculer avec l'algorithme d'Euclide $d := pgcd(924; 469)$ Comme $924 = 1\times469+455$ et $469 = 1\times455+14$, $455 = 32\times14+7$, $14 = 2\times7+0$, on trouve $d = 7$.

De plus le calcul donne $7 = 455 - 32 \times (469 - 455) = 33 \times 455 - 32 \times 469 = 33 \times (924 - 469) - 32 \times 469 = 33 \times 924 - 65 \times 469$.

La premiere equation n'a pas de solution entieres puisque 7 ne divise pas 15.

On observe que $d = 7$ divise 21 donc l'equation possede des solutions. Par $7 = 33 \times 924 - 65 \times 469$, on trouve $7 = (3 \times 33) \times 924 + (3 \times (-65)) \times 469$, i.e. $(x_0, y_0) = (99, -195)$. Les autres solutions s'obtiennent en ecrivant $132(x - x_0) + 67(y - y_0) = 0$ et donc $x = x_0 + 67l$, $y = y_0 - 132l$ d'ou l'ensemble des solutions

$$S = \{(x; y) = (99 + 67l, -195 - 133l) | l \in \mathbb{Z}\}.$$

On peut appliquer aussi ce qu'on a fait dans le cours. On a calcule $q_2 = 1, r_3 = 455$, $q_3 = 1, r_4 = 14$, $q_4 = 32, r_5 = 7$, $q_5 = 2, r_6 = 0$. Donc $x_1 = 1, y_1 = 0$, $x_2 = 0, y_2 = 1$, $x_3 = x_1 - q_2x_2 = 1$, $y_3 = y_1 - q_2y_2 = -1$, $x_4 = x_2 - q_3x_3 = -1$, $y_4 = y_2 - q_3y_3 = 2$, $x_5 = x_3 - q_4x_4 = 33$, $y_5 = y_3 - q_4y_4 = -65$. Donc par le theoreme de cours, $x = \frac{21}{d}x_4 + \frac{469}{d}l = 99 + 67l$, $y = \frac{21}{d}y_4 + \frac{931}{d}l = -195 + 133l$, $l \in \mathbb{Z}$ sont les solutions de (2).

Exercice 2 Montrer que les nombres 23 et 34 sont premiers entre eux et trouver deux entiers u, v, tels que $23u + 34v = 1$.

En deduire la resolution dans $\mathbb{Z}$ du systeme d'equations suivant

$$\begin{cases} x \equiv 4 \mod 23 \\ x \equiv 5 \mod 34. \end{cases} \tag{3}$$

On applique le theoreme chinois : on calcule d'abord d = $pgcd$(23; 34) qui vaut 1 et on en deduit une identite de Bezout, ici 1 = $3 \times 23 - 2 \times 34$. Comme le pgcd est 1, les solutions existent et forment une classe de congruence modulo 23.34.

Par le theoreme chinois, l'ensemble des solutions du systeme est l'ensemble des entiers x = $4(-2\times34)+5(3\times23) mod$(23.34). Comme $4(-2\times34)+5(3\times23)$ = -272 + 345 = 73, les solutions sont x = $73 mod$(23.34).

Exercice 3 Determiner le reste de la division par 23 de 1891^{2004} puis le reste de la division par 47 de $4756^{1891^{2004}}$.

On a 1891 = 5 mod 23, de plus le petit theoreeme de Fermat nous garantit que 5^{22} = 1 mod 23, et 2004 = 22.91 + 2 donc

$$1891^{2004} \equiv 5^{2004} \equiv 5^2 \equiv 2 \mod 23$$

Le reste de la division par 23 est donc 2.

On a 4756 $\equiv$ 9 mod 47. Le petit theoreme de Fermat nous garantit que $9^{23} = 3^{46} \equiv 1$ mod 47 donc

$$4756^{1891^{2004}} \equiv 9^{1891^{2004}} \equiv 9^{23.q+2} \equiv 9^2 \equiv 34 \mod 47.$$

Le reste de la division par 47 est donc 34.

Exercice 4 Soit n = 1368 = $8 \times 9 \times 19$

1. Calculer $\varphi(n)$ (sous forme factorisee).
2. Montrer que si pgcd(a, n) = 1 alors $a^{18} \equiv 1$ mod 19 et etablir un resultat similaire modulo 8 et modulo 9.
3. En deduire que si pgcd(a, n) = 1 alors $a^{36} \equiv 1$ mod n.
4. Ecrire precisement la de nition d'un groupe, et un isomorphisme de groupes.
5. Est ce qu'il existe $a \in (\mathbb{Z}/n\mathbb{Z})^*$ telle que $(\mathbb{Z}/n\mathbb{Z})^* = \{a^j | j \in \mathbb{N}\}$? Quels sont les elements de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre 1 ?
6. Determiner tous les couples de groupes isomorphes parmi

$$A = \mathbb{Z}/8\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z},\ B = \mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/15\mathbb{Z},\ C = \mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/20\mathbb{Z},\ D = \mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/20\mathbb{Z}.$$

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

$$\phi(n) = \phi(2^3)\phi(3^2)\phi(19) = 2^2(2-1)3(3-1)(19-1) = 2^4 3^3.$$

D'apres le theoreme d'Euler (de Fermat pour un module premier) on sait $a^{18} \equiv 1$ mod 19, $a^4 \equiv 1$ mod 8, $a^6 \equiv 1$ mod 9 des que a est premier avec le module de congruence. En notant que $ppcm(18; 4; 6)$ = 36 on voit que pour a premier avec n, on aura $a^{36} \equiv 1$ mod 19, mod 8, mod 9, donc $a^{36} \equiv 1$ mod n.

4. Un groupe est un couple $(G, *)$, G un ensemble et la loi de groupe $*$: $G \times G \to G$ telle que a) associative $(x * y) * z = x * (y * z)$, b) un element neutre

$e \in G$, i.e., $x*e = e*x = x$ pour $x/in G$. c) inverse : pour $x \in G$, il existe $x' \in G$ telle que $x * x' = x' * x = e$.

Une application $f : G \to H$ de deux groupes est un isomorphisme de groupes si $f(x*y) = f(x) *_H f(y)$ pour tout $x, y \in G$ et f est bijiective.

Par 3, le cardinal de $\{a^j | j \in \mathbb{N}\}$ est ≤ 36 si $a \in (\mathbb{Z}/n\mathbb{Z})^*$, mais le cardinal de $(\mathbb{Z}/n\mathbb{Z})^*$ est $\phi(n) = 2^4.3^3 > 36$, donc il n'existe pas de $a \in (\mathbb{Z}/n\mathbb{Z})^*$ telle que $(\mathbb{Z}/n\mathbb{Z})^* = \{a^j | j \in \mathbb{N}\}$.

g a d'ordre 1 ssi $g = g^1 = e$. Les elements de $(\mathbb{Z}/n\mathbb{Z})^*$ d'ordre 1 est $\overline{1}$.

6. Par le lemme chinois en terme d'anneaux residuels, $A = \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, $B = \mathbb{Z}/4\mathbb{Z} \oplus \oplus\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, $C = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$, $D = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. Donc B et D sont isomorphe.

Exercice 5 La lettre p designe un nombre premier impair (di erent de 2), on etudie l'equation suivante dans $\mathbb{Z}/p\mathbb{Z}$:

$$x^4 + 1 = 0. \tag{4}$$

1. Montrer qu'une solution de l'equation (4) est un element d'ordre huit dans $(\mathbb{Z}/p\mathbb{Z})^*$. En deduire que si $p \equiv 3 \mod 8$ alors l'equation (4) n'a pas de solution.
2. Resoudre l'equation pour $p = 11$ puis $p = 19$.
3. Soit $p \equiv 1 \mod 8$, soit a un element d'ordre $p-1$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer que $a^{\frac{p-1}{2}} \equiv -1(p)$. Determiner les entiers k tels que $x = a^k$ soit solution de (4).

Comme $x^8 = (x^4)^2 = (-1)^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$, et $x^4 \neq 1, 4$ est le diviseur maximal de 8, donc par le lemme de Chap 12, on sait que l'ordre de x est 8.

Si $p \equiv 3 \mod 8$, alors $|(\mathbb{Z}/p\mathbb{Z})^*| = p - 1 \equiv 2 \mod 8$, et par le theoreme Lagrange, pour $a \in (\mathbb{Z}/p\mathbb{Z})^*$, $ord(a)$ divise $p - 1$. Donc il n'exste pas d'element d'ordre 8 dans $(\mathbb{Z}/p\mathbb{Z})^*$, et donc l'equation (4) n'est pas de solution.

2. Car $11 = 3 \mod 8$, $19 = 3 \mod 8$, l'equation (4) n'est pas de solution.

3. Si $ord(a) = p-1$, alors $(\mathbb{Z}/p\mathbb{Z})^* = \{\overline{a}^j | j \in \mathbb{N}\}$. Donc il existe $0 < m < p-1$ telle que $a^m \equiv -1(p)$ car $a^{p-1} \equiv 1(p)$. Donc $a^{2m} \equiv 1(p)$, et ca implique $p - 1$ divise $2m$, et $0 < 2m < 2(p - 1)$, donc $m = \frac{p-1}{2}$. I.e.,

$$a^{\frac{p-1}{2}} \equiv -1(p). \tag{5}$$

Pour $0 \leq k \leq p - 1$, alors $a^{4k} \equiv -1(p)$ implique $a^{8k} \equiv 1(p)$, et donc $p - 1$ divise $8k$, et $p-1$ ne divise pas $4k$. Donc les possibles k est $\frac{p-1}{8}, 3\frac{p-1}{8}, 5\frac{p-1}{8}, 7\frac{p-1}{8}$. Par (5), les k tels que $x = a^k$ soit solution de (4) sont $\frac{p-1}{8}, 3\frac{p-1}{8}, 5\frac{p-1}{8}, 7\frac{p-1}{8}$.