Université Paris Diderot
Département de Sciences Exactes

MI4– Année 2013/14
L2 MI4

Feuille d'exercices n°3

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 [calculs de $\phi(n)$ pour certaines valeurs de n]

1. Calculer $\phi(n)$ pour $n \in \{5, 8, 13, 18, 19, 21, 25, 27, 33, 36\}$.
2. Pour quelles valeurs de n, parmi ceux de la question 1, le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est-il cyclique ?

Exercice 2 Pour quels entiers n a-t-on $\phi(n) = \frac{n}{3}$?

Exercice 3

1. Existe-t-il un entier $n > 1$ tel que $x^n \equiv 1 \mod 15$ pour tout $x \in \mathbb{Z}$?
2. Trouver un entier $n > 1$ tel que $x^n \equiv 1 \mod 15$ pour tout entier $x \in \mathbb{Z}$ premier avec 15.

Exercice 4

1. Soit $n = p_1 \dots p_r$ un produit de nombres premiers distincts deux à deux, et soit :
$$a = 1 + (p_1 - 1) \times \dots \times (p_r - 1).$$
Montrer qu'on a $x^a \equiv x \mod n$ pour tout $x \in \mathbb{Z}$.
2. Soit $n = p^k q$ où p est premier, $k \geq 2$, et p ne divise pas q. Montrer qu'il existe $x \in \mathbb{Z}$ tel que $x \equiv p^{k-1} \mod p^k$ et $x \equiv 0 \mod q$. Montrer que pour tout $a > 1$, $x^a \not\equiv x \mod n$.

Exercice 5 [une autre démonstration du théorème de Fermat] Soit p un nombre premier. Pour $k \in \mathbb{Z}/p\mathbb{Z}$, $k \neq 0$, on définit une application $f_k : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ par $f_k(x) = kx$.

1. En observant que f_k est bijective, vérifier l'égalité suivante dans $\mathbb{Z}/p\mathbb{Z}$:
$$\prod_{x=1}^{p-1} f_k(x) = (p-1)!$$
2. En déduire une démonstration du petit théorème de Fermat, $a^{p-1} \equiv 1 \mod p$ pour tout entier a premier avec p.

Exercice 6 Déterminer les entiers $x \in \mathbb{N}$ tels que $3^x \equiv 11 \mod 14$.

Exercice 7 [fonction puissance modulaire] Déterminer les entiers $n \geq 1$ tels que le morphisme $\varphi : x \mapsto x^n$ de $(\mathbb{Z}/35\mathbb{Z})^*$ dans lui-même soit bijectif.

Exercice 8 [racines de -1 modulo p] Soit p un nombre premier différent de 2.

1. Montrer que p est de la forme $4k+1$ ou $4k+3$.
2. Vérifier que l'équation
$$x^2 + 1 \equiv 0 \mod p \tag{1}$$
n'a pas de solution si p est de la forme $4k+3$. *Indication :* déterminer l'ordre de x.
3. Si $p = 4k+1$, vérifier que $x = (2k)!$ est solution de l'équation (1). *Indication :* utiliser le théorème de Wilson, $(p-1)! \equiv -1 \mod p$.
4. Exemple : donner les solutions de l'équation $x^2 + 1 \equiv 0 \mod 13$.

Exercice 9 Soit $f(x,y) = x^3 - y^3 + 2xy + x - 2$; notons $G(m)$ le nombre de solutions modulo m de la congruence $f(x,y) \equiv 0 \mod m$. C'est-à-dire

$$G(m) = \operatorname{card}\{(x,y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \mid f(x,y) \equiv 0 \mod m\}.$$

Montrer que si m et n sont premiers entre eux alors $G(mn) = G(m)G(n)$. [*Indication* : utiliser le théorème des restes chinois, l'énoncé vaut pour tout polynôme à coefficients dans $\mathbb{Z}$.]

Nombres pseudo-premiers

Dans la suite, on appelle base *d'un entier $n > 1$ tout entier $b \geq 1$ premier avec n. On dit qu'un nombre $n > 1$ est* pseudo-premier *pour une de ses bases b si n n'est pas premier et si $b^{n-1} \equiv 1 \mod n$.*

Exercice 10 [exemples de nombres pseudo-premiers]

1. Montrer que $2^{10} \equiv 1 \mod 341$. En déduire que $n = 341$ est pseudo-premier pour la base 2.
2. Montrer que 3^{10} n'est pas congru à 1 modulo 341. Montrer que 3 est inversible modulo 341, et calculer l'ordre du groupe $(\mathbb{Z}/341\mathbb{Z})^*$. Déterminer l'ordre de 3 dans $(\mathbb{Z}/341\mathbb{Z})^*$, et en déduire que 341 n'est pas pseudo-premier pour la base 3.
3. Soit n un nombre pseudo-premier pour la base 2 et soit $n' = 2^n - 1$. Montrer que $n | n' - 1$. Montrer que n' est pseudo-premier pour la base 2 (utiliser $a \mid b \Rightarrow 2^a - 1 \mid 2^b - 1$). En déduire qu'il existe une infinité de nombres pseudo-premiers pour la base 2.

Exercice 11 Trouver toutes les bases pour lesquelles 15 est pseudo-premier.

Exercice 12 [carrés pseudo-premiers] Soit p un nombre premier. Montrer que p^2 est pseudo-premier pour la base b si et seulement si $b^{p-1} \equiv 1 \mod p^2$.

Exercice 13 Soit $n = pq$ avec p et q deux nombres premiers distincts. On pose $d = \text{pgcd}(p-1, q-1)$. Montrer que n est pseudo-premier pour la base b si et seulement si $b^d \equiv 1 \mod n$. *Indication :* utiliser le théorème chinois. Calculer en fonction de d le nombre de bases pour lesquelles le nombre n est pseudo-premier.

Exercice 14 [nombres de Mersenne et de Fermat pseudo-premiers pour la base 2]

1. Montrer qu'un nombre de Mersenne $M_p = 2^p - 1$ non premier est pseudo-premier pour la base 2.
2. Même question pour les nombres de Fermat non premiers $F_n = 2^{2^n} + 1$.

Nombres de Carmichaël

On dit qu'un entier $n > 1$ est un *nombre de Carmichaël* si n est pseudo-premier pour toutes ses bases. D'après un théorème du cours, un nombre $n > 1$ non premier est de Carmichaël si et seulement si, pour tout diviseur p premier de n, on a $p - 1 | n - 1$ et $p^2 \not| n$.

Exercice 15 [exemples numériques] Vérifier que 1729, 6601 et 278545 sont des nombres de Carmichaël. [Indication : $1729 = 7.13.19$, $6601 = 7.23.41$ et $278\,545 = 5.17.29.113$.]

Exercice 16 [exemples de nombres de Carmichaël] Montrer que si $6m + 1$, $12m + 1$ et $18m + 1$ sont tous trois premiers, alors leur produit $n = (6m + 1)(12m + 1)(18m + 1)$ est un nombre de Carmichaël. Exemple : $m = 1$ fournit $n = 7.13.19 = 1729$.

Exercice 17 [une caractérisation des nombres de Carmichaël] Montrer qu'un entier non premier $n > 1$ est un nombre de Carmichaël si et seulement si $a^n \equiv a \mod n$ pour tout entier $a \in \mathbb{Z}$.

Exercice 18 [nombres de Carmichaël avec 3 diviseurs premiers]

1. Montrer que tout nombre de Carmichaël a au moins 3 diviseurs premiers. *Indication :* par l'absurde, écrire $n = pq$ avec $p < q$, p et q premiers.
2. Montrer que pour r premier fixé, il n'existe qu'un nombre fini de nombres de Carmichaël de la forme $n = rpq$ avec p et q premiers. *Indication : on peut supposer que $p > q$ et il y aura deux cas possible $r > q$ et $r < q$, montrer que pour chaque cas il n'y a qu'un nombre fini de (p, q) possible.*
3. Trouver tous les nombres de Carmichaël de la forme précédente pour $r = 3$ et pour $r = 5$.

Note : *il existe une infinité de nombre de Carmichaël ; la démonstration (difficile) date de 1994 et est due à Alford, Granville et Pomerance.*