2M220 – Arithmétique, 2014-2015
Université Pierre et Marie Curie

François Lê
francois.le@imj-prg.fr

TD n° 5 – $(\mathbf{Z}/n\mathbf{Z})^\times$, fonction d'Euler et RSA

Exercice 1

1. Rappeler la définition de la fonction φ d'Euler et l'expression de $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n.
2. Calculer $\varphi(12)$, $\varphi(100)$, $\varphi(108)$.
3. Montrer que si n est impair, alors $\varphi(2n) = \varphi(n)$.
4. Montrer que si n est pair, alors $\varphi(2n) = 2\varphi(n)$.
5. Montrer que $\varphi(3n) = 3\varphi(n)$ si et seulement si $n \equiv 0 \mod 3$, et que dans la négative, on a $\varphi(3n) = 2\varphi(n)$.
6. Montrer que $\varphi(n) = n/2$ si et seulement si n est une puissance de 2.
7. Montrer que $\varphi(n)$ divise $n!$.

Exercice 2
Le but de l'exercice est de montrer que pour tout $n \in \mathbf{N}^*$, on a

$$\sum_{d|n,\, d>0} \varphi(d) = n.$$

1. Si $d > 0$ est un diviseur de n, on pose $E_d = \{x \in [\![1, n]\!] \mid x \wedge n = d\}$. Montrer que si d_1 et d_2 sont deux diviseurs distincts de n, alors $E_{d_1} \cap E_{d_2} = \varnothing$.
2. Montrer que $[\![1, n]\!]$ est la réunion de tous les E_d, avec $d < 0$ diviseur positif de n.
3. Montrer que $\operatorname{Card} E_d = \varphi(n/d)$.
4. Conclure.

Exercice 3

1. Rappeler le lien entre $\varphi(n)$ et l'anneau $\mathbf{Z}/n\mathbf{Z}$. Rappeler le théorème d'Euler et l'interpréter en termes de théorie des groupes.
2. Soient a et n premiers entre eux. Montrer que pour tout $m \in \mathbf{N}$, on a $a^m \equiv a^r \mod n$, où r est le reste dans la division euclidienne de m par $\varphi(n)$.

Exercice 4

1. Trouver le reste dans la division euclidienne de 2^{52} par 11.
2. Montrer que $2^{70} + 3^{70}$ est divisible par 13.
3. Trouver le reste dans la division euclidienne de 100^{1000} par 13.
4. Trouver le reste dans la division euclidienne de $3^{115} + 5^{115}$ par 13.
5. Montrer que pour tout entier naturel n, le nombre $2^{2^{6n+2}}$ est divisible par 19.

Exercice 5

1. Montrer que pour tout $a \in \mathbf{Z}$, on a $a^{13} \equiv a \mod 2730$. *Indication :* $2730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$.
2. Montrer que pour tout entier impair a, on a $a^{33} \equiv a \mod 4080$. *Indication :* $4080 = 15 \cdot 16 \cdot 17$.

Exercice 6

1. Soit p un nombre premier. Montrer que $(p-1)! \equiv -1 \mod p$. *Indication : montrer que* $x^2 \equiv 1 \mod p \iff x \equiv 1 \quad ou \quad x \equiv -1 \mod p$.
2. Réciproquement, soit n un entier positif tel quel $(n-1)! \equiv -1 \mod n$. Montrer que n est un nombre premier.
3. Soit p un nombre premier impair. Montrer que l'équation $x^2 \equiv -1 \mod p$ admet une solution si et seulement si $p \equiv 1 \mod 4$.

Exercice 7

1. Soit $a \in \mathbf{Z}$. Montrer que $\overline{a}$ est d'ordre 16 dans $\mathbf{Z}/17\mathbf{Z}$ si et seulement si $a^8 \not\equiv 1 \mod 17$.
2. En déduire que $\overline{3}$ engendre $(\mathbf{Z}/17\mathbf{Z})^*$.
3. De la même façon, trouver un générateur de $(\mathbf{Z}/27\mathbf{Z})^*$.

Exercice 8

Soit p un nombre premier et soit $\overline{a}$ un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$.

1. Soit d l'ordre de a modulo p^2. Montrer que $d = p-1$ ou $d = p(p-1)$.
2. On suppose que $d = p-1$. Montrer que l'ordre de $b = a+p$ est $p(p-1)$.
3. Trouver en fonction de $\overline{a}$ un générateur de $(\mathbf{Z}/p^2\mathbf{Z})^*$.

Exercice 9

Dans un cryptosystème utilisant la méthode RSA, déterminer la clé secrète $(d, (p-1)(q-1))$ et le message envoyé $M \in \mathbf{Z}/n\mathbf{Z}$ pour les clés publiques (e, n) et les messages reçus $C = M^e$ suivants :

1. $n = 35$, $e = 5$, $C = 10$.
2. $n = 265$, $e = 139$, $C = 10$.

Exercice 10

Alice et Bob communiquent en utilisant la méthode RSA. Bob cherche donc deux nombres premiers p et q puis calcule leur produit $n = 253$. Il rend public le couple $(13, n)$.

1. Quelle est la clé secrète de Bob ?
2. Alice veut transmettre le message $M = 2$ à Bob. Quel message C ce dernier va-t-il recevoir ?
3. Bob a reçu $C = 22$. Quel est le message M que Alice lui a envoyé ?