FEUILLE DE TRAVAUX DIRIGÉS

ARITHMÉTIQUE

Exercice 1 (Carrés de $\mathbb{Z}/p\mathbb{Z}$)**.**
Soit p un nombre premier impair.

(1) Montrer qu'il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

(2) ....

Exercice 2 (Groupe cyclique des unités)**.**
Soient un nombre entier $m \geq 1$ et un nombre premier p impair. On considère et $q = p^\nu$, avec $\nu \in \mathbb{N}$.

(1) Montrer que
$$\mathrm{Card}\{x \in {\mathbb{F}_q}^\times \mid x^m = 1\} = \mathrm{pgcd}(m, q-1) \ .$$

(2) Montrer que
$$\mathrm{Card}\{x \in (\mathbb{Z}/p^\nu\mathbb{Z})^\times \mid x^m = 1\} = \mathrm{pgcd}(m, p^{\nu-1}(p-1)) \ .$$

Plus généralement, soit $n = p_1^{\nu_1} \dots p_r^{\nu_r}$ impair.

(3) Montrer que
$$\mathrm{Card}\{x \in (\mathbb{Z}/n\mathbb{Z})^\times \mid x^m = 1\} = \prod_{i=1}^{r} \mathrm{pgcd}(m, p_i^{\nu_i-1}(p_i-1)) \ .$$

(4) En déduire que
$$\mathrm{Card}({\mathbb{F}_q}^\times)^m = \mathrm{Card}\{x \in {\mathbb{F}_q}^\times \mid \exists\, y \in {\mathbb{F}_q}^\times,\ x = y^m\} = \frac{q-1}{\mathrm{pgcd}(m, q-1)} \ .$$

(5) En conclure que l'indice du sous-groupe $({\mathbb{F}_q}^\times)^2$ de ${\mathbb{F}_q}^\times$ est
$$[{\mathbb{F}_q}^\times : ({\mathbb{F}_q}^\times)^2] \ .$$

Exercice 3 (Petit théorème de Fermat, nombres pseudo-premiers et nombres de Carmichael)**.**

(1) [*Petit théorème de Fermat*] Montrer que pour p un nombre premier et a un nombre premier avec p
$$a^{p-1} \equiv 1_{[p]} \ .$$

Soit un nombre entier $a \geq 2$. Un nombre entier n est dit *pseudo-premier en base* a si n n'est pas premier et s'il vérifie
$$a^{n-1} \equiv 1_{[n]} \ .$$

(2) Soit p un nombre premier impair qui ne divise pas $a(a^2-1)$. Montrer que
$$n := (a^{2p}-1)/(a^2-1)$$
est un nombre pseudo-premier en base a.

(3) En déduire que pour tout $a \geq 2$, il existe une infinit de nombres pseudo-premiers en base a.

Un *nombre de Carmichael* est un entier $n \geq 2$, qui n'est pas un nombre premier et qui vérifie

$$a^{n-1} \equiv 1_{[n]} \ ,$$

pour tout entier a premier avec n. (Dit autrement, n est un nombre pseudo-premier en base a, pour tout entier a premier avec n).

(4) Soit $n = p_1 \dots p_k$, avec les p_i premiers et distincts. Montrer que si $p_i - 1 | n - 1$, pour tout $1 \leq i \leq k$, alors n est un nombre de Carmichael.

(5) Réciproquement, montrer que tout nombre de Carmichael est de la forme $n = p_1 \dots p_k$ où les p_i sont premiers et distincts et où $p_i - 1 | n - 1$, pour tout $1 \leq i \leq k$.

(6) Montrer qu'un nombre de Carmichael a au moins 3 facteurs premiers.

(7) Donner le plus petit nombre de Carmichael.

(8) Soit $n = pqr$ un nombre de Carmichael à 3 fracteurs premiers $p < q < r$. Si p est fixé, montrer que q et r sont bornés.

Remarque : Il existe une infinité de nombres de Carmichael [AGP94].

Exercice 4 (Cryptograhpie : le système RSA, Rivest-Shamir-Adelman 1978)**.**
Soient p et q deux nombres premiers distincts ; on pose $n = pq$. Soient c et d deux entiers tels que $cd \equiv 1_{[\varphi(n)]}$.

(1) Montrer que $t^{cd} \equiv t_{[n]}$.

Supposons que n et c soient connus (*clef publique*). Tout le monde peut alors coder un message $t \in \mathbb{Z}$ en appliquant la fonction $t \mapsto t^c \in \mathbb{Z}/n\mathbb{Z}$.

(2) Expliquer comment on décode ce message.

(3) Expliquer en quoi ce système de cryptage est particulièrement difficile à attaquer.

(4) Peut-on coder tous les messages $t \in \mathbb{Z}$?

(5) Est-ce que la contrainte "t premier avec n" est très génante ? (Pour cela calculer la proportion de nombres inférieurs à n et premiers avec n).

Exercice 5 (Repartition des nombres premiers)**.**
On note p_n le n-ième nombre premier et $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x.

(1) Montrer que $p_{n+1} \leq p_1 \dots p_n + 1$ et que $p_n < 2^n$.

(2) En déduire que, pour x assez grand, on a $\log \log x \leq \pi(x) \leq x$.

Remarque : Cet encadrement est très grossier. Le *théorème des nombres premiers* [Hadamard et de la Valle Poussin, 1896] affirme que

$$\pi(x) \sim \frac{x}{\log x} \ .$$

(3) Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 1$. (Utiliser l'exercice **??**).

(4) Montrer qu'il existe une infinité de nombres premiers de la forme $6k + 1$.

(5) Montrer qu'il existe une infinité de nombres premiers de la forme $4k + 3$.

(6) Montrer qu'il existe une infinité de nombres premiers de la forme $6k + 5$.

Soit p un nombre premier impair divisant $a^2 + b^2$, où $a \wedge b = 1$.

(7) Montrer que $p \equiv 1_{[4]}$.

(8) En déduire qu'il existe une infinité de nombres premiers de la forme $8k + 5$.

Remarque : Tous ces exemples se généralise dans le *théorème de Dirichlet* [1838] : Pour toute paire $n \wedge m = 1$ de nombres entiers premiers entre eux, il existe infinité de nombres premiers de la forme $n + km$, où k est un entier positif.

Ajouter un exercice sur les symboles de Legendre

Cours et TDs : Bruno Vallette (brunov@unice.fr)

Page web du cours : http ://math.unice.fr/∼brunov/Cours-Agregation(2011-2012).html