Université Paris 7 - Denis Diderot 2018-2019
UFR de Mathématiques M1 - Arithmétique

Feuille d'exercices 6

Test de primalité et polynômes cyclotomiques

Exercice 1 1. Montrer que $2^m + 1$ ne peut être premier que si $m = 2^n$.

2. Soit $n \geq 2$ et soit $F_n = 2^{2^n} + 1$ le n-ème nombre de Fermat. Démontrer que si p est un premier qui divise F_n alors p est de la forme $p = k2^{n+1} + 1$. En déduire que en effet p est de la forme $p = k2^{n+2} + 1$ et trouver un facteur de F_5.

Exercice 2 Soit $M = 85$, on définit les ensembles

$$G_0 = (\mathbb{Z}/M\mathbb{Z})^*,$$
$$G_1 = \{a \in G_0 \mid a^{M-1} = 1\},$$
$$G_2 = \{a \in G_0 \mid a^{\frac{M-1}{2}} = \pm 1\},$$
$$G_3 = \{a \in G_0 \mid a^{\frac{M-1}{2}} = \left(\frac{a}{M}\right)\},$$
$$S = \{a \in G_0 \mid a^{21} = 1 \text{ ou } a^{21} = -1 \text{ ou } a^{42} = -1\}.$$

1. Montrer que si $a \in S$ alors $-a \in S$, et en déduire que le cardinal de S est pair.
2. Calculer le cardinal de G_0, G_1, G_2 et S.
3. En déduire le cardinal de G_3.
4. L'ensemble S est-il un sous-groupe de G_0 ?

Exercice 3 Donner la factorisation de $x^{85} - 1$ dans $\mathbb{Q}[x]$. Donner le nombre et le degré de facteurs irréductibles de la décomposition de $x^{85} - 1$ dans $\mathbb{F}_2[x]$.

Exercice 4 1. Montrer les relations suivantes (on pourra comparer les degrés et les racines de chaque côté) :

$$\Phi_n(x^p) = \begin{cases} \Phi_{np}(x) \text{ si } p \mid n \\ \Phi_{np}(x)\Phi_n(x) \text{ si } p \nmid n. \end{cases}$$

2. Montrer que pour $r \geq 1$ et p premier on a

$$\Phi_{p^r}(x) = x^{p^{r-1}(p-1)} + x^{p^{r-1}(p-2)} + \cdots + x^{p^{r-1}} + 1.$$

3. Soit p un premier et soit $\mathbb{F}_q$ un corps fini de caractéristique p. Si $n = p^s m$ avec $p \nmid m$, on a, dans $\mathbb{F}_q[x]$,
$$\Phi_n(x) = \Phi_m(x)^{p^s - p^{s-1}}.$$

Exercice 5 1. Rappeler comment se décompose Φ_n dans $\mathbb{F}_p[x]$ pour $p \nmid n$.

2. Soit $a \in \mathbb{Z}$ et p premier ne divisant pas n et divisant $\Phi_n(a)$. Montrer que $p \equiv 1 \bmod n$ (on pourra observer que la classe de a modulo p est une racine de Φ_n).

3. Montrer que $\Phi_n(0) = 1$ et en déduire que, pour tout $m \geq 2$, on a que $\Phi_n(m)$ est premier avec m. Montrer aussi qu'il n'y a que un nombre fini de $a \in \mathbb{Z}$ tels que $\Phi_n(a) = \pm 1$.
4. En déduire l'existence d'une infinité de nombres premier $p \equiv 1 \bmod n$ (resp. l'existence d'une infinité de nombres premier $p \not\equiv -1 \bmod n$).

Exercice 6 Soit G un groupe abélien fini.

1. Montrer qu'il existe un entier N tel que G soit isomorphe à un sous-groupe (resp. un quotient) de $(\mathbb{Z}/N\mathbb{Z})^*$. (On peut se ramener au cas $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$; en choisissant des nombres premiers $p_i \equiv 1 \bmod n_i$, montrer que $N = p_1 \cdots p_s$ convient.)
2. Montrer qu'il existe une extension $K/\mathbb{Q}$ galoisienne telle que $\mathrm{Gal}(K/\mathbb{Q}) \cong G$.

Exercice 7 1. Pour $n \geq 3$ montrer qu'il existe un et un seul polynôme unitaire $\Phi_n^+(x) \in \mathbb{C}[x]$ tel que

$$(\Phi_n^+(x))^2 = \prod_{\zeta \in \mu_n^*} (x - \zeta - \zeta^{-1})$$

2. Calculer Φ_3^+, Φ_5^+ et Φ_7^+.
3. Monter que $\deg \Phi_n^+ = \varphi(n)/2$ et $\Phi_n(x) = x^{\varphi(n)/2}\Phi_n^+(x + x^{-1})$. En déduire que $\Phi_p^+(2) = \Phi_p(1) = p$.
4. Montrer que Φ_n^+ est dans $\mathbb{Z}[x]$ et est irréductible (en particulier, c'est le polynôme minimal de $2\cos(2\pi/n)$).

Exercice 8 Soit $M_n = 2^n - 1$ le n-ème nombre de Mersenne.

1. Monter que si $a^n - 1$ est premier alors $a = 2$ et n est premier. Vérifier que M_2, M_3, M_5 et M_7 sont premiers mais que M_{11} n'est pas premier.
2. Soit A un anneau et on considère la suite, à valeurs dans A, donnée par $V_0 = 2$, $V_1 = a \in A$ et $V_{n+1} - aV_n + V_{n-1} = 0$. Vérifier les formules suivantes : $V_{2n-1} = V_nV_{n-1} - a$, $V_{2n} = V_n^2 - 2$, ou encore $V_nV_m = V_{n+m} + V_{n-m}$.
3. Soit M impair, $a \in \mathbb{Z}$ tel que $\mathrm{pgcd}(a^2 - 4, M) = 1$ et V_n la suite définie précédemment. Si $V_{M+1} \equiv 2 \bmod M$ et si pour tout q premier divisant $M + 1$ on a $\mathrm{pgcd}(V_{\frac{M+1}{q}} - 2, M) = 1$, alors M est premier.
4. Soit L_i la suite définie par $L_1 = 4$ et $L_{i+1} = L_i^2 - 2$. Le nombre de Mersenne M_p est premier si et seulement si $L_{p-1} \equiv 0 \bmod M_p$.

Exercice 9 Un nombre est dit parfait si il est égal à la somme de se diviseurs propres.

1. Montrer que si $M_p = 2^p - 1$ est premier alors $P_p = 2^{p-1}M_p$ est parfait.
2. Montrer que un nombre parfait pair n est de la forme P_p. (Écrire $n = 2^m M$ avec M impair et $m \geq 1$; montrer que $2n = \sigma(2^m)\sigma(M)$ et en déduire que M doit être premier et conclure. Ici $\sigma(n) = \sum_{d|n} d$.)

Exercice 10 Soit $N \geq 2$. On suppose que $N - 1$ est partialement factorisé $N - 1 = p_1^{e_1} \cdots p_k^{e_k} M$, avec $M < \sqrt{N}$, et que, de plus, pour chaque p_i on dispose de a_i tel que

$$a_i^{N-1} \equiv 1 \bmod N \text{ et } \mathrm{pgcd}(a_i^{\frac{N-1}{p_i}} - 1, N) = 1.$$

En déduire que si q divise N alors $q \equiv 1 \bmod p_i^{e_i}$, puis que N est premier.