Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Fiche TD 5

Le théorème de progression arithmétique de Dirichlet

Exercice 1 *La preuve d'Euclide ou Dirichlet pour $2n+1$*
Montrer qu'il existe un nombre infini de nombres premiers.
Par l'absurde, on suppose que l'ensemble $\mathcal{P}$ des nombres premiers est fini, et on considère les diviseurs premiers de $1+\prod_{p\in\mathcal{P}} p$.

Exercice 2 *Dirichlet pour $4n-1$*
Montrer qu'il existe un nombre infini de nombres premiers de la forme $4n-1$ (ou $4n+3$ si on préfère), avec n entier.
Par l'absurde, on suppose que l'ensemble $\mathcal{P}_{4,3}$ des nombres premiers de cette forme est fini, et on considère les diviseurs premiers de $-1+4\prod_{p\in\mathcal{P}_{4,3}} p$.

Exercice 3 *Dirichlet pour $6n-1$*
Montrer qu'il existe un nombre infini de nombres premiers de la forme $6n+5$ (ou $6n-1$ si on préfère), avec n entier.
Par l'absurde, on suppose que l'ensemble $\mathcal{P}_{6,5}$ des nombres premiers de cette forme est fini, et on considère les diviseurs premiers de $-1+6\prod_{p\in\mathcal{P}_{6,5}} p$.
La méthode des deux derniers exercices s'épuise ici car $\varphi(n)=2$ implique $n=3,4,6$.

Exercice 4 *Dirichlet pour $4n+1$*
Montrer qu'il existe un nombre infini de nombres premiers de la forme $4n+1$, avec n entier.
Par l'absurde, on suppose que l'ensemble $\mathcal{P}_{4,1}$ des nombres premiers de cette forme est fini, et on considère les diviseurs premiers de $1+4\prod_{p\in\mathcal{P}_{4,1}} p^2$. On dégaine alors le symbole de Legendre.

Exercice 5 *Dirichlet pour $6n+1$*
Montrer qu'il existe un nombre infini de nombres premiers de la forme $6n+1$, avec n entier.
On montre, en s'aidant de Lagrange et de la formule

$$(x^2-x+1)(x+1)(x^2+x+1)(x-1)=x^6-1,$$

que x^2-x+1, avec x entier, n'a pour diviseurs premiers que 3, ou p congru à 1 modulo

6. *Par l'absurde, on suppose que l'ensemble $\mathcal{P}_{6,1}$ des nombres premiers de cette forme est fini, et on considère les diviseurs premiers de* $1 - 6\prod_{p\in\mathcal{P}_{6,1}} p + 6^2\prod_{p\in\mathcal{P}_{6,1}} p^2$.

Rappel pour la suite : le polynôme ϕ_n est le polynôme unitaire ayant pour racines les racines primitives de l'unité. Voici quelques propriétés fondamentales :

• $X^n - 1 = \prod_{d|n} \phi_d$

• $\phi_n \in \mathbb{Z}[X]$, en particulier $\phi_n(0)$ est entier, et comme il est de module 1 (c'est le produit des racines), il vient $\phi_n(0) = \pm 1$.

• ϕ_n est irréductible sur $\mathbb{Q}$ (plus difficile, mais ce ne sera pas utilisé par la suite)

Exercice 6 *Version faible du théorème de progression arithmétique de Dirichlet [Algèbre 1, Francinou Gianella Nicolas]*
Soit n dans $\mathbb{N}^*$. On veut montrer qu'il existe une infinité de nombres premiers p congrus à 1 modulo n.

1. Mise en jambe. Calculer les 12 premiers polynômes cyclotomiques ϕ_k, $1 \leq k \leq 12$.
   Tout provient d'une récurrence sur n qui utilise la formule $\prod_{d|n} \phi_d = X^n - 1$.
2. Soit a dans $\mathbb{N}^*$ et p premier, tels que p divise $\phi_n(a)$ et ne divise pas $\phi_d(a)$ pour d divisant strictement n. Montrer que p est congru à 1 modulo n.
   Quotienter par p et utiliser Lagrange.
3. On prend $N > \mathrm{Max}\{3, n\}$, et $a = N!$.
   (a) Montrer que $|\phi_n(a)| \geq 2$.
   On pourra utiliser l'inégalité triangulaire.
   (b) Montrer que si p divise $\phi_n(a)$, alors $p > N$.
   On pourra montrer que si $p \leq N$, alors p divise a et donc, p divise le terme constant de ϕ_n, c'est-à-dire ± 1.
   (c) Montrer que p ne divise pas $\phi_d(a)$ pour d divisant strictement n.
   On aurait une racine double pour $X^n - 1$.
4. Conclure.

Exercice 7 *Version faible du théorème de progression arithmétique [Variante perso]*
Soit n dans $\mathbb{N}^*$. On veut montrer qu'il existe une infinité de nombres premiers p congrus à 1 modulo n. On suppose dans la suite $n \geq 3$, les cas $n = 1$ et 2 étant déjà clairs.

1. On suppose p premier ne divisant pas n. Montrer
$$\exists \overline{x} \in \mathbb{F}_p,\ \phi_n(\overline{x}) = \overline{0} \Rightarrow n \text{ divise } p - 1$$
   Les hypothèses assurent que $X^n - 1$ n'a pas de racine multiple. Ceci implique que $\overline{x}$ est d'ordre n dans un groupe d'ordre $p - 1$.
2. On suppose par l'absurde que l'ensemble $\mathcal{P}_{n,1}$ des nombres p premiers, congrus à 1 modulo n est fini. Soit $a := n\prod_{p\in\mathcal{P}_{n,1}} p$.

(a) Montrer que $|\phi_n(a)| \geq 2$.

On a $a \geq n \geq 3$. Donc, l'inégalité provient de l'inégalité triangulaire quand on scinde ϕ_n en facteurs de degré 1.

(b) Montrer que si q premier divise $\phi_n(a)$, alors n divise $q-1$, et aboutir à une contradiction.

Comme q divise $\phi_n(a)$ et a, on aurait que q divise le terme constant $\phi_n(0) = \pm 1$.

Remarque historique ! On notera que la preuve originale que l'ensemble des nombres premiers (pour $n = 2$, donc) est infini, utilise le polynôme cyclotomique $\phi_2 = X + 1$ et $a = 2 \prod_{p \in \mathcal{P}_{2,1}} p$. Cette méthode est une généralisation dans le respect d'une preuve plusieurs fois millénaire !

Exercice 8 *Application : Tout groupe abélien fini s'injecte dans $(\mathbb{Z}/n\mathbb{Z})^*$ pour un n*

Montrer que, pour tout groupe abélien fini G, il existe n tel que le groupe G s'injecte dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$.

On commence par un groupe cyclique : $\mathbb{Z}/a\mathbb{Z}$ s'injecte dans $\mathbb{Z}/p\mathbb{Z}^*$, dès que p est un nombre premier tel que a divise $p-1$. Le cas général utilise le théorème de structure des groupes abéliens finis, mais il faut faire attention à bien choisir des p distincts pour chaque groupe cyclique de la décomposition, et c'est là que l'on se sert du fait que l'ensemble des nombres premiers congrus à 1 modulo a est infini.