109 - Anneaux Z/nZ. Applications.

I) Anneau (Z/nZ,+,x)

1) Définition

Attention, pas si évident.

Prop : A un anneau commutatif, R une relation d'équivalence sur A. On note A/R l'ensemble des classes d'équivalences. Alors A/R est un anneau ssi (xRy <=> x-y appartient à I), où I est un idéal de A. On note alors A/R=A/I.

Déf et prop : a congru à b ssi a-b appartient à nZ. nZ est un idéal de Z.

Csq : on peut définir l'anneau (Z/nZ,+,*).

Rq : les orbites de la relation de congruence sont les k+nZ (k compris entre 0 et n-1). On a donc Z/nZ={0 barre, 1 barre,.....n-1 barre}.

2) Propriétés

Th Chinois (équivalence) ; c'est un isomorphisme entre anneaux [Mat L2]

Systèmes de congruences [Mat L2]

Rq : en particulier, c'est un isomorphisme entre les groupes additifs et multiplicatifs.

Csq : identités concernant l'indicatrice d'Euler [Mat L2]

II) Le groupe (Z/nZ,+)

Groupe cyclique, sous groupes, générateurs

Th de Kronecker : tout groupe abélien fini est isomorphe à Z/d_1Z x ... x Z/d_rZ.

-> L'étude des (Z/nZ,+) nous permet de comprendre tous les groupes abéliens finis.

(Z/nZ,+) est un groupe cyclique. Pour tout diviseur d de n, il existe un sous groupe d'ordre d

III) Le groupe ((Z/nZ)*,x)

1) Premières propriétés

C'est l'anneau des inversibles de l'anneau Z/nZ.

Prop : a inversible ssi a générateur de (Z/nZ,+) ssi (a,n)=1

Csq 1 : il y a Phi(n) éléments dans le groupe multiplicatif Z/nZ

Csq 2 : théorème d'Euler, petit théorème de Fermat en corollaire.

Csq 3 : Z/nZ est un corps ssi n est premier.

Prop : si n est premier, (Z/nZ,x) est cyclique d'ordre n-1.

2) Structure

Par le théorème Chinois, il suffit d'étudier (Z/p^kZ,x).

Th : structure des Z/p^kZ (3 cas) ; attention : isomorphismes entre groupes additifs et multiplicatifs.

Prop : (Z/nZ,x) isomorphe à (Aut(Z/nZ,+),o).

Csq : |Aut(Z/nZ,+)|=Phi(n), et Aut(Z/nZ) est abélien.

IV) Applications en arithmétique

1) Premières propriétés [Comb] + [Zem]

Théorème (Fermat) : si p premier, pour tout entier on a x^p congru à x modulo p *(on regarde ça dans Fp)*

Th (Fermat Euler) : pour tout k entier premier avec n, k^{phi(n)} est congru à 1 modulo n *(regarder l'ordre de k dans (Z/nZ)*)*

Théorème (Wilson) : p est un nb premier ssi (p-1) ! congru à -1 modulo p *(supp p premier. Alors par Fermat, pour tout x dans Fp*, x^{p-1}=1. Donc X^(p-1)=(X-1)(X-2)…(X-p+1). On écrit l'égalité des termes constants de ces polynômes et c'est bon. Réciproquement, si (p-1) ! est congru à -1 modulo p, alors aucun entier plus petit que p-1 ne divise p donc p est premier)*

Appl : quel est le chiffre des unités de 27^1995 ? *(on veut connaître le reste de la DE de ce nb par 10. 27 est congru à 7 modulo 10. Phi(10)=4. 7 est premier avec 10 donc 7^4 est congru à 1 modulo 10. On divise 1995 par 4 : 1995=4q+3. Donc 27^1995=7^1995=7^(4q+3)=(7^4)^q*7^3=7^3=3. Le chiffre des unités est 3)*

2) Nombres premiers

Test de Fermat : on veut voir si n est premier. On choisit a au hasard. On calcul a^{n-1}. Si a{n-1} n'est pas congru à 1 modulo n, alors n n'est pas premier (th de Fermat). Sinon, on dit que p est pseudo premier en base a.

En pratique, ce test marche bien. Ceci dit, même si on l'applique pour un grand nb de bases différentes, on n'est pas sûr qu'un nombre vérifiant chaque test est premier. Il existe les nb de Carmichael qui vérifient le test pour tout a premier avec n, et qui ne sont pas premiers (il existe une infinité de nb de Carmichael, les premiers sont 561,1105, 1729…). Si ojn fait le test de Fermat avec un nb de Carmichael, le résultat de a^n-1 va nous donner 1 tout le temps, sauf quand a sera un diviseur de n.

Th : Dirichlet faible [Goz]

3) Une application : le cryptage RSA [Del]

Théorème : p, q deux nombres premiers. On pose n=pq. Si e est premier avec (p-1)(q-1), alors il existe d>0 tq ed=1 mod((p-1)(q-1)). Si on prend a premier avec n, on a a^ed=a (mod n) *(a^ed=a^[k*(p-1)(q-1)+1]=(a^(p-1)(q-1)]^k*a. Or Phi(n)=(p-1)(q-1), donc comme a et n sont pee, a^phi(n)=1 (mod n) par Fermat Euler. On a donc a^ed=a (mod n))*

Appl : le RSA. Je choisis p,q, puis e un nb premier avec (p-1)(q-1). On calcule l'inverse de e modulo (p-1)(q-1). On pose n=pq. Je rend public n et e, mais surtout pas p,q,d. L'expéditeur qui veut m'envoyer un message transforme son message en des nombres A plus petit que n. Il calcule ensuite B=A^e (mod n). Moi je reçois le message B et je calcule B^d, qui me fait retomber sur A d'après le th.

Précautions à prendre :
- p et q grands (sinon on peut les trouver en factorisant n)
- |p-q| grand sinon √n est proche de p et on peut trouver p.
- p-1 et q-1 ne doivent pas être trop friables
- e doit pas être trop petit

4) Equations diophantiennes

- ax+by=c
- $x^2+y^2=z^2$
- x^4+y^4=z^4

(Voir Madère p.47, qui renvoit à De Koninck et Mercier, introduction à la théorie des nombres)

5) Somme de deux carrés [Perr]

Déf : Σ l'ensemble des nombres somme de deux carrés. Z[i]. N la norme.

Prop : Σ stable par multiplication *(vient de l'identité de Lgrange, et faut passer par Z[i] en disant que $n \in \Sigma$ ssi $\exists z \in \mathbb{Z}[i]$ tq $n=N(z)$)*

Prop : $\mathbb{Z}[i]$ est euclidien *(on prend z et t dans Z[i], on défini le complexe z/t, et on prend l'élément q de Z[i] le plus proche de z/t. On mq $z=qt+(z-qt)$ avec $N(z-qt)<N(t)$ et c'est bon)*

Théorème : p nb premier. $p \in \Sigma$ ssi p=2 ou p congru à 1 modulo 4 *(un sens facile : si n est somme de deux carrés, alors n est congru à 0,1 ou 2 modulo 4. Comme p est premier il peut pas être congru à 0 ou 2, donc il est congru à 1. l'autre sens est balèze. Il faut mq $p \in \Sigma$ ssi p n'est pas irréductible dans Z[i], ça se fait bien. Z[i] principal donc p non irréductible ssi $\mathbb{Z}[i]/(p)$ non intègre. On mq $Z[i]/(p)=Fp[X]/(X^2+1)$. Du coup $Z[i]/(p)$ n'est pas intègre ssi X^2+1 est réductible dans Fp, ie si -1 est un carré modulo p, ie si p congru à 1 modulo 4)*

Théorème : $n \in \Sigma$ ssi vp(n) est pair pour p congru à 3 modulo 4 *(un sens clair avec la stabilité par multiplication. Pour l'autre, on fixe p congru à 3, et on montre par récurrence sur vp(n) que vp(n) est pair, en montrant que $vp(n/p^2)$ reste dans Σ)*

V) Anneaux Z/pZ

1) Corps finis

Définition, LRQ, équations

2) Réduction de polynômes

Eisenstein, modulo p

Développements :
1 - Théorème de Dirichlet faible [Goz 84] (* ou **)
2 – LRQ (* ou **)

Rapport jury 2005-2009 : *cette leçon classique demande toutefois une préparation minutieuse. Bien maîtriser le lemme chinois et sa réciproque. Distinguer clairement propriétés de groupes additifs et d'anneaux. Connaître les automorphismes, les nilpotents, les idempotents. Enfin, les candidats sont invités à rendre hommage à Gauss en présentant quelques applications arithmétiques des anneaux **Z**/n**Z**, telles l'étude de quelques équations diophantiennes bien choisies. Distinguer clairement propriétés de groupes additifs et d'anneaux. Connaître les automorphismes, les idempotents.*
On attend la description des sous-groupes additifs de Z/nZ. Attention en général si d|n, Z/dZ n'est pas un sous-ensemble de Z/nZ. La description des éléments inversibles pour la structure multiplicative doit être connue. La structure des groupes abéliens de type fini doit être connue, il y a deux présentations distinctes (diviseurs élémentaires ou via les p-Sylow) ; il faut savoir passer de l'une à l'autre.