Parimaths-Mathematical Olympiads Club
Arithmétique

Séance du 4 janvier 2014

Ippolyti Dellatolas & Louis Mutricy

1 Rappels

Le but de cette séance est d'approfondir les résultats vus précédemment en **arithmétique** (cf. séance du 30 novembre 2013). On rappelle les résultats suivants :

- ☞ Un entier naturel est dit **premier** si ses seuls diviseurs positifs sont 1 et lui même. L'ensemble des nombres premiers est infini.
- ☞ Soit a, b et c trois entiers tels que a divise b. Alors a divise c si et seulement si a divise $b+c$, si et seulement si a divise $b-c$.
- ☞ **Propriété de Bézout** : Soit a et b deux entiers, et d leur PGCD ; il existe deux entiers u et v tels que $au+bv=d$. En particulier, a et b sont premiers entre eux si et seulement si il existe des entiers $u$et v tels que $au+bv=1$.
- ☞ **Lemme de Gauss** : Soit a, b et c trois entiers tels que a divise bc ; si $PGCD(a,b)=1$, alors a divise c.
- ☞ **Théorème fondamental de l'arithmétique** : Tout entier naturel non nul admet une unique décomposition en facteurs premiers.

2 Congruence

2.1 Définitions et premières propriétés

Définition 1 *Soit $n>1$ un entier. Deux entiers a et b sont dits* congrus modulo n *si n divise $a-b$. On écrit alors $a \equiv b[n]$.*

Propriétés immédiates : Pour tout a et $n>1$ entiers, on vérifie que :

- ✏ $a \equiv 0[n]$ si et seulement si n divise a
- ✏ Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$
- ✏ Il existe un unique entier $b \in \{0,1,...n-1\}$ tel que $a \equiv b[n]$

Propriétés calculatoires : Montrer que la relation de congruence est compatible avec l'addition et la multiplication. En d'autres termes que montrer que si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors :

- ✏ $a + b \equiv a' + b'[n]$
- ✏ $ab \equiv a'b'[n]$
- ✏ $a^n \equiv a'^n[n]$

Les congruences ont de nombreux usages. Elles sont en particulier très utiles pour résoudre des équations à variables entières (aussi appelées équations diophantiennes). A titre d'exemple on peut citer :

Exercice 1 Touver tous les entiers x et y strictement positifs tel que $3x^2 + 2x + 2 = y^2$.
Indication Quelles valeurs peuvent prendre x^2 et y^2 modulo 4 ?

Exercice 2 Montrer que la somme de 5 carrés d'entiers consécutifs n'est pas un carré parfait.

Attention. Si la relation de congruence est compatible avec la multiplication et l'addition, elle n'est **pas** compatible avec la division. On ne doit **jamais** diviser une congruence. Dans certains cas, il est toutefois possible d'effectuer des opérations similaires en utilisant les inverses modulo n. C'est l'objet de la rubrique suivante.

2.2 Éléments inversibles

Définition 2 *Soit $n > 1$ un entier. On dit qu'un entier u est inversible modulo n si et seulement si il existe un entier v tel que $uv \equiv 1[n]$.*

Proposition 1 *Un entier u est inversible modulo n si et seulement si $PGCD(u; n) = 1$.*

En particulier, si n est premier, tous les élements non nuls modulo n sont inversibles.

Exercice 3 (*Théorème de Wilson*) Soit $p > 1$ un entier. Montrer que p est premier si et seulement si $(p-1)! \equiv -1[p]$

Proposition 2 *Soit a,b,c et $n > 1$ des entiers. On suppose $ab \equiv ac[n]$. Si a est premier avec n alors $b \equiv c[n]$.*

3 Ordre modulo n

Les résultats suivants découlent essentiellement du fait que a^k ne peut prendre qu'un nombre fini de valeurs modulo n.

Proposition 3 *Soit $n > 1$ un entier, et a premier avec n. Il existe un entier m tel que $a^m \equiv 1[n]$*

Corollaire : La suite définie par $u_k \equiv a^k[n]$ est périodique.

Exercice 4 Calculer le reste de la division euclidienne de $2013^{2013^{2014^{2014}}}$ par 7.

Définition 3 *Soit $n > 1$ un entier, et a premier avec n. On appelle ordre de a modulo n le plus petit entier ω tel que $a^\omega \equiv 1[n]$*

Proposition 4 *Soit $n > 1$ un entier, et a premier avec n d'ordre ω et k un entier positif. Si $a^k \equiv 1[n]$ alors ω divise k*

Proposition 5 (Petit théorème de Fermat) *Soit p un nombre premier et a un entier. Alors $a^p \equiv a[p]$. En particulier si a n'est pas divisible par p : $a^{p-1} \equiv 1[p]$*

Exercice 5 Soit p un nombre premier, et a, n deux entiers naturels. Montrer que p disvise $a^{n+p} - a^{n+1}$.

Exercice 6 Trouver tous les entiers p premiers tels que p divise $2^p + 1$

En particulier, si p est premier l'ordre de tout élément non divisible par p divise $p - 1$.

4 Exercices

Exercice 7 Montrer que pour tout entier n :

1. 7 divise $3^{2n+1} + 2^{n+2}$
2. 111 divise $10^{6n+2} + 10^{3n+1} + 1$

Exercice 8 Montrer que si $2^n + 1$ est premier alors n est une puissance de 2.

Exercice 9 Montrer que l'ensemble des nombres premiers congrus à -1 modulo 4 est infini.

Exercice 10

1. Montrer que tout entier est congru à la somme de ses chiffres modulo 9.
2. Soit S la somme des chiffres de 4444^{4444} et S' la somme des chiffres de S. Déterminer la somme des chiffres de S'.

Exercice 11 Trouver les deux derniers chiffres de $7^{9^{9^9}}$

Exercice 12 Soit p un nombre premier impair tel que p divise $x^2 + 1$ (avec x un entier). Montrer que $p \equiv 1[4]$. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.