Extraits (avec légères modifications) de deux lettres à Julien :

Attention à l'énoncé à la fin de votre leçon, un énoncé important qui n'est pas facile

Déjà il faut se convaincre que les groupes multiplicatifs (Z/pZ)* lorsque p est premier sont cycliques, il y a un argument spécial pour cela et bien connu (il est dans ma fiche sur les corps de Galois)

pris de cette fameuse fiche :

Rappelons qu'un groupe cyclique est un groupe isomorphe au groupe additif $\mathbf{Z}/N\mathbf{Z}$ (cardinalité finie si $N \geq 1$). Notons d'une manière générale $\langle x \rangle$ le groupe engendré par un élément x d'un groupe quelconque. Pour $\mathbf{Z}/N\mathbf{Z}$ on a $\langle x \rangle = \mathbf{Z}/N\mathbf{Z}$ si et seulement si il existe $a \in \mathbf{Z}$ avec $ax = 1$ si et seulement si x est premier à N. Le nombre de générateurs est donc $\phi(N)$ (fonction d'Euler). Comptons les éléments x d'ordre d où d est un diviseur de N. L'équation $dx = 0 \pmod N$ signifie $x = 0 \pmod{\frac{N}{d}}$, donc x est parmi les multiples de $\frac{N}{d}$, $x = k\frac{N}{d}$, $0 \leq k < d$, et $\langle x \rangle \subset < \frac{N}{d} >$. Pour que $\#\langle x \rangle = d$ il est nécessaire et suffisant qu'il existe j avec $jx = \frac{N}{d}$, soit $jk\frac{N}{d} = \frac{N}{d} \pmod N$ soit (puisque $\frac{N}{d}$ divise N), $jk = 1 \pmod d$. Il y a donc précisément $\phi(d)$ éléments d'ordre d dans $\mathbf{Z}/N\mathbf{Z}$ et on obtient en particulier l'identité :

Ce premier paragraphe vise uniquement à justifier l'équation (1); il existe d'autres façons de le faire, et de plus souvent les gens démontrent le Théorème sur k^* en utilisant la formule (1) sans la redémontrer.

$$(1) \qquad N = \sum_{d|N} \phi(d)$$

Faisons le même genre de décompte directement dans le groupe multiplicatif k^* d'un corps k de cardinalité $q = p^n$. Soit $N = q - 1 = p^n - 1$. Prenons $x \in k^*$ et considérons le groupe cyclique $\langle x \rangle$ qu'il engendre. Il a cardinalité d avec $d|N$ et $x^d - 1 = 0$. On peut factoriser le polynôme $t^d - 1$ dans $k[t]$ en $\prod_{0 \leq j < d}(t - x^j)$ puisque $1, x, \ldots, x^{d-1}$ en sont déjà d racines distinctes dans k. Tout autre $y \in k^*$ d'ordre d vérifie $y^d = 1$, donc est racine de ce polynôme et par conséquent de la forme x^j. Or x^j est d'ordre d si et seulement si j est premier à d (on a un isomorphisme $\langle x \rangle \simeq \mathbf{Z}/d\mathbf{Z}$ qui fait correspondre $j \pmod d$ à x^j). Il y a donc précisément $\phi(d)$ éléments y dans k^* d'ordre d dès qu'il y en a au moins un. Notons $\mathcal{D}$ l'ensemble des diviseurs d de $N = q - 1$ pour lesquels on peut trouver un élément d'ordre d. On a donc :

(2) $$N = \sum_{d \in \mathcal{D}} \phi(d)$$

La comparaison de (1) et (2) impose la conclusion que $\mathcal{D}$ contient tous les diviseurs de N, en particulier N lui-même. Par conséquent :

Théorème. *Le groupe multiplicatif k* d'un corps fini est cyclique.*

Ensuite pour gérer les $(Z/p^nZ)^*$, n au moins 2, on montre que (**attention p>2, n>1**) :

$$(1+p)^{p^{n-2}} = 1 + p^{n-1} \pmod{p^n},$$

(il faut utiliser que les coefficients du binôme dans $(a+b)^p$ sont divisibles par p sauf le premier et le dernier et faire une récurrence ; *cf.* le **Lemme** plus bas), et

$$(1+p)^{p^{n-1}} = 1 \pmod{p^n},$$

donc 1+p a un ordre qui divise p^{n-1}, mais pas p^{n-2} il est donc d'ordre exactement p^{n-1} (**p>2**)

Si l'entier x engendre $(Z/p\,Z)^*$ alors son ordre dans $(Z/p^nZ)^*$ est un multiple de p-1

Supposons qu'il soit d'ordre (p-1) a, alors x^a est d'ordre p-1

Donc x^a fois (1+p) est d'ordre (p-1) fois p^{n-1} (**ordres premiers entre eux**)

Ainsi $(Z/p^nZ)^*$ est aussi cyclique (engendré par $(1+p)\omega$ avec $\omega = x^a$ d'ordre p - 1, x choisi parmi les générateurs de $(Z/pZ)^*$; il est aussi possible que x convienne directement)

Pour p=2, 3 = 1+2 ne marche pas, il faut 5 = 1+4, qui sera d'ordre 2^{n-2}

Bon le lemme qui autorise une récurrence c'est :

Lemme. *si p premier est au moins 3, et n entier au moins 2, ou si p =2 et n est au moins 3 : si u est divisible par p à la puissance n-1 alors* $(1+u)^p = 1+pu \pmod{p^{n+1}}$

Ensuite on prend : - soit p>2 et alors u=p et n=2 et par récurrence on en déduit que (1+p) à la puissance p^{n-2} vaut $1+p^{n-1}$ (mod p^n) pour n au moins égal à 2
- soit p=2 et alors au départ u = 4 = 2^2 et n=3 et par récurrence on montre que 5 à la puissance 2^{n-3} vaut $1+2^{n-1} \pmod{2^n}$

Donc 5 est d'ordre 2^{n-2} ensuite supposons qu'une puissance (positive ou négative) de 5 donne -1 modulo 2^n en réduisant modulo 4 on obtient une contradiction, donc les puissances de 5 ne sont jamais égales à -1, par conséquent les éléments $(-1)^a 5^b$ avec a=0 ou 1 et b =0, 1, . . ., 2^{n-2} - 1 sont tous distincts modulo 2^n, et forment donc un système complet de représentants du groupes multiplicatif de $Z/2^nZ$ qui contient 2^{n-1} éléments. Ainsi ce groupe multiplicatif est isomorphe au produit de Z/2Z et de $Z/2^{n-2}Z$ (pour n au moins égal à 3)

Cordialement

JF Burnol, 8 novembre 2010

deuxième lettre

La différence entre p=2 et p $\geq$ 3 (p premier) est donc que dans Z/p^nZ l'équation $x^2 = 1$ n'a que les solutions x= 1 et x=-1, lorsque p est au moins 3

Par contre dans $Z/2^nZ$ et pour n au moins 3 l'équation $x^2 = 1$ a 4 solutions, qui sont
x=1
x=-1
$x = 5^{2^{n-3}} = 1+2^{n-1}$
$x = -5^{2^{n-3}} = -1+2^{n-1}$
Par exemple pour n=5, on travaille modulo 32 et on a les solutions x=1, x=-1, $x = 5^4 = 17$ et x= -17 = 15 à l'équation $x^2 = 1$

Dans un groupe cyclique G d'ordre d, l'équation $x^2 = e$ a 1 ou 2 solutions suivant la parité de d : soit a un générateur, $x = a^k$, k=0, 1, ..., d-1 $x^2 = e$ signifie que 2k est divisible par d, donc 2k = 0 ou 2k = d

Donc si d est impair 1 seule solution k=0, x=e si d est pair il a deux solutions x = e et $x = a^{d/2}$

Lorsque l'on parle de $(Z/p^nZ)^*$ son ordre $d = (p - 1)p^n$ est toujours pair (sauf si p=2 et n=1)

Le groupe est cyclique pour p>2 ou pour p=2, n=1, n=2, tandis que pour p=2, n>2 il est isomorphe au produit de Z/2Z par un groupe cyclique

Cordialement

JF Burnol, 8 novembre 2010

Extraits légèrement modifiés de mes lettres plus récentes aux agrégatifs :

On s'intéresse aux congruences modulo 1000 ; par le théorème des restes chinois $Z/1000Z \simeq Z/8Z \times Z/125Z$, donc déjà on va déterminer le groupe muliplicatif $(Z/125Z)^*$, dont on sait par ce qui précède qu'il est cyclique avec $\phi(125) = 125(1 - 1/5) = 100$ éléments. On essaie avec 2. Comme 100 = 4x 25, l'ordre de 2 est un diviseur de 100, donc s'il n'est pas 100 il est soit diviseur de 100/2 =50 soit diviseur de 100/5 = 20 donc on calcule 2^{50} et 2^{20} pour voir si ça vaut 1. Si par malheur c'était le cas :

- ou on réessaierait avec 3,
- ou on appliquerait la méthode générale et on remplacerait 2 par la puissance $\omega = 2^a$ qui est précisément d'ordre 4 = 5 - 1. Ensuite on aurait la garantie que 6ω est un générateur (car on sait par notre théorème général que 6 est exactement d'ordre 25 = 100/4 dans le groupe $(Z/125Z)^*$.)

Pour calculer les 2^n il suffit de le faire avec n des puissances de 2 car ensuite on écrit n en base 2 donc on commence par faire

$2 = 2$
$2^2 \equiv 4$
$2^4 \equiv 16$
$2^8 \equiv 16^2 \equiv 256 \equiv 6$
$2^{16} \equiv 6^2 \equiv 36$
$2^{32} \equiv 36^2 \equiv 900 + 2*30*6 + 36 \equiv 1296 \equiv 46$
donc $2^{50} \equiv 2^{32+16+2} \equiv 46*36*4 \equiv 46*19 \equiv 920 - 46 \equiv -80 - 46 \equiv -126 \equiv -1$
et $2^{20} \equiv 2^{16+4} \equiv 36*16 \equiv 576 \equiv 76$

Ceci prouve que (Z/125Z)* est un groupe cyclique avec 2 comme générateur. On va maintenant résoudre le problème suivant :

Exercice. *Déterminer les racines cinquièmes de* 701 *modulo* 1000*.*

Par le théorème des restes chinois, il faut d'une part le faire modulo 8, d'autre part le faire modulo 125. On a $701 \equiv 5 \pmod 8$. Les puissances cinquièmes modulo 8 de $0, \ldots, 7$ sont $0, 1, 0, 3, 0, 5, 0, 7$. Donc si $m^5 \equiv 701 \pmod{1000}$ alors $m \equiv 5 \pmod 8$.

Passons au module 125, on a $701 \equiv -49 \equiv 76$

Il faut déterminer a tel que $76 \equiv 2^a$. Par chance, on avait justement obtenu $2^{20} \equiv 76$. Donc a = 20 convient. Par chance ce a est divisible par 5. Donc il y a 5 racines cinquième de 76 ce sont 2^b avec b=4,24,44,64,84. 0n sait déjà que $2^{20} \equiv 76$, donc les racines cinquièmes sont

$2^4 = 16$, puis $16*76$, $16*76^2$, $16*76^3$, $16*76^4$
On calcule successivement modulo 125 :
$76^2 \equiv 26$
$76^3 \equiv 101$
$76^4 \equiv 51$

Nos solutions sont donc y= 16, 16*76, 16*26, 16*101, 16*51 ok c'est un peu calculatoire on trouve 16, 91, 41, 116, 66 modulo 125

Finalement 701 est une puissance cinquième modulo 1000 et il a cinq racines

cinquièmes modulo 1000 qui s'obtiennent en résolvant les congruences

$m \equiv 5 \pmod 8$
$m \equiv 16, 91, 41, 116, \text{ou } 66 \pmod{125}$

Pour résoudre $m \equiv w \pmod 8$ et $m \equiv z \pmod{125}$ on commence par trouver un Bezout $47*8 - 3*125 = 1$, puis on cherche m sous la forme $125\,u + 8\,v$. La première équation devient

$$125u \equiv w \pmod 8 \text{ donc } u \equiv -3w \pmod 8 ,$$

et la deuxième équation devient :

$$8v \equiv z \pmod{125} \text{ donc } v \equiv 47z \pmod{125} ,$$

donc la solution est :

$$m \equiv -375w + 376z \pmod{1000} .$$

Ok ok c'est un peu calculatoire il reste à remplacer w par 5 et z par 16, 91, 41, 116, ou 66

$m \equiv -1875 + 376*(16 \text{ ou } 91 \text{ ou } 41 \text{ ou } 116 \text{ ou } 66) \pmod{1000}$

Voici le résultat : m vaut 141 ou 341 ou 541 ou 741 ou 941

La forme du résultat est surprenante et pas du tout prévue ! les racines cinquièmes de 701 forment une progression arithmétique... il nous faut une explication !

C'est très simple les coefficients du binôme sont 1, 5, 10, 10, 5, 1, donc (en observant aussi que $1000 | 200^5$) :

$$(x + 200)^5 \equiv x^5 \pmod{1000}$$

Ainsi on a fait beaucoup de calculs superflus, il suffisait de s'occuper plus haut de résoudre $m \equiv 5 \pmod 8$ et $m \equiv 2^4 \equiv 16 \pmod{125}$, cela nous aurait donné une première solution et les quatre autres auraient été obtenues en ajoutant des multiples de 200. . .