Chapitre A5 : NOMBRES PREMIERS et DPFP

Objectif : retour sur un point basique de l'arithmétique, comme quoi les pb les plus simples ...

I. NB PREMIERS ; NB premiers entre eux

1. nb premier

th il existe une infinité de nombres premiers.

Dem : lecture et analyse de la démonstration page 47 (prop2 et prop1 qu'elle utilise

par l'absurde

2. ; nombres premiers entre eux ; th gauss

rappel th Gauss *a, b et c entiers non nuls.*

Si a divise le produit bc et si a est premier avec b, alors a divise c.

prop n est divisible par a et b premiers entre eux si , et ssi, n est divisible par le produit ab.

Exemple : n est divisible par 2 et par 3, si et ssi il est divisible par 6

Démonstration

** si n est divisible par a et b, alors n=ak = bk' a divise le produit bk' et a premier avec b donc (th Gauss) a divise k' càd k' = ak » et donc n=bak » est bien divisible par ab.*

** récip : si n est div par ab alors n = abk ce qui montre qu' il est divisible par a et par b*

prop Soit p un nb premier alors « n est premier avec p » si et ssi « n n'est pas divisible par p»

→ si n est div par p ; comme p est aussi div par p, ils ont un div commun qui est p , donc ne sont pas premiers entre eux

→ si n n'est pas premier avec p, leur pgcd d est supérieur à 1, ils ont un diviseur commun d>1, or le seul diviseur de p supérieur à 1 est p lui-même, donc p divise n càd n est divisible par p

II. DÉCOMPOSITION EN PFP

1. existence page 47

lecture et analyse de dem p47

2. unicité :

unicité admise é mais on peut aller y voir de plus près : revenons sur Gauss et certaines conséquences :

* Vrai ou faux : si deux entiers a et b divisent un entier c alors leur produit divise c

faux : vrai si a et b premiers entre eux

* Vrai ou faux : si un nb premier p divise un produit ab alors il divise a ou b

vrai : si p ne divise pas a, a non div par p, a premier avec p, p premier avec a et divise ab donc th gauss p divise b)

* si un entier premier p divise un produit de nb premiers alors *p égale l'un d'entre eux*

* si un entier p est premier avec certains entiers alors il est premier avec leur produit

Ÿ l'unicité découle de tout ça !--> voir Math'x page 172

3. conséquence pour le pgdc et le ppcm

pour le pgcd : *prendre les facteurs communs et les affecter du plus petit exposant → intersection des DPFP*

pour le ppcm : *prendre tous les facteurs , et les affecter de l'exposant le plus grand → Union des DPFP*
rappel : **prop : pgcd * ppcm = ab.**

III. RECHERCHE DE DIVISEUR PREMIER : Fermat

rappel : Comment savoir si un nb est divisible par un nb p ?
N div par p ssi N multiple de p ssi Ek tq N=pk ssi N==0(modp) (et pour p premier : ssi pgcd(n,p) = p)

1. petit th de Fermat

Soit p un nb premier.

th1 : *p un nb premier, alors pour tout entier n : n^p = n modulo p*
exemple : p=3 alors pour tout n, n^3 – n est divisible par 3.
exemple : 2^3 – 2 = 8-2=6 OK ;
rq : si n est divisible par p, c'est évident, c'est pour n premier avec p que c'est intéressant : 5^3 – 5 = 125-5 = 120 OK !

Preuve
voir manuel Pixel page 51

Th2 (autre formulation)
p un nb premier, alors pour tout entier n non divisible par p: n^(p-1) = 1 modulo p
preuve :
n^p-n = n(n^(p-1)-1)
p premier divise ce produit n(n^(p-1)-1) (th 1) donc (csq gauss) il divise soit n soit ...
soit p divise n,
sinon p ne divise pas n alors n premier avec p (hypothèse)→ th Gauss p divise n^(p-1)-1
CQFD.
Rq : il ne peut pas diviser les deux facteurs car sinon il diviserait 1...

Exemples :
** pour tout n non div par 3, n²-1 est divisible par 3 (vérif orale avec n = 5, 10, 11, ...*
** pour tout n non div par 2, n-1 est divisible par 2 (évident : n non div par 2 est un nb impair n=2k+1 et n-1 = 2k est div par 2 !*
** pour tout n non div par 5, n^4-1 est divisible par 5 (vérif avec n = 2, 3, 4, 9, 12, ...)*

exercice : mq que pour tout entier n, n^5-n est divisible par 30.
** Fermat pour div par 5 ;*
** n5-n = n(n4-1) = n(n²-1)(n²+1)=n(n-1)(n+1)(n²+1)*
→ n5-n est divisible par 2 car soit n soit n+1 l'est
et par 3 car soit n-1,; soit n, soit n+1 l'est
*→ (csq th Gauss) n5-n est div par 2*3*5 = 30.*

2. . APPLICATION A LA CRYPTO : le système RSA *Voir exercices…..*