Démonstration kholle 16

I Théorème de la division euclidienne (cas $(a,b) \in \mathbb{N} \times \mathbb{N}^*$)

Théorème :
soit $(a,b) \in \mathbb{Z}^2$ avec $b \neq 0$:
$\exists!(q,r) \in \mathbb{Z}^2, (a = bq + r$ et $0 \leq r < |b|$)
C'est la division euclidienne de a par b avec a le dividende, q quotient, r reste
Démonstration :
Unicité : si (q,r) et (q',r') conviennent :
$a = bq + r$ et $a = bq' + r'$, ainsi que $0 \leq r < |b|$ et $0 \leq r' < |b|$
on a : $bq + r = bq' + r'$
$r - r' = b(q' - q)$ or :
$0 \leq r < |b|$ et $-|b| < -r' \leq 0$
$-|b| < r - r' < |b|$
Or si $q \neq q'$:
$|q' - q| \geq 1$ et $|r - r'| = |b||q - q'| \geq |b|$
incompatible avec $-|b| < r - r' < |b|$ donc $q = q'$ par conséquent :
$r - r' = b(q - q') = 0, r = r'$
Existence : distinguons trois cas:
Cas 1 : $a \in \mathbb{N}, b \in \mathbb{N}^*$
Posons $E = \{k \in \mathbb{N}, bk \leq a\}$
On a : $E \subset \mathbb{N}$, $E \neq \emptyset$ car $0 \in E$
E est majorée par a : pour $k \in E$ on a :
$k \leq \underbrace{b}_{\in \mathbb{N}^*} k \leq a$
Ainsi, E possède un maximum q : On a $q \in E$ donc $bq \leq a$
On a $(q + 1) \notin E$ car $q + 1 > max(E)$
Comme $(q + 1) \in \mathbb{N}$, on a donc $b(q + 1) > a$
ainsi : $bq \leq a < bq + b$
Posons $r = a - bq \in \mathbb{Z}$
$a = bq + r$ et $0 \leq r < b = |b|$ car $b \in \mathbb{N}^*$
Cas 2 : $a \leq 0$, $b > 0$: on applique le premier cas à $(-a,b)$, il existe $(q,r) \in \mathbb{Z}^2$ tel que :
$-a = bq + r$ et $0 \leq r < |b|$ alors:
$a = -bq - r$ si r=0 $(-q,0)$ convient
sinon : $b(-q - 1) + (b - r)$ $0 < b - r < b$ car $r > 0$, $(-q - 1,b - r)$ convient
Cas 3 : a quelconque, b<0
avec a et b : $\exists(q,r) \in \mathbb{Z}^2, a = (-b)q + r$ et $0 \leq r < -b$
$a = b(-q) + r$ le couple $(-q,r)$ convient car $0 \leq r < |b|$

II Sous-groupes de $(\mathbb{Z},+)$

Théorème :
1) Pour $n \in \mathbb{Z}$, $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ est un sous groupe de $(\mathbb{Z},+)$
2) Tout sous-groupe de $(\mathbb{Z},+)$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ unique
Démonstration :
1) Soit $n \in \mathbb{Z}$

a) $n\mathbb{Z} \subset \mathbb{Z}$ par définition
b) $0 = n \times 0 \in n\mathbb{Z}$ donc $n\mathbb{Z} \neq \emptyset$
c) Soit $(x,y) \in (n\mathbb{Z})$:
$\exists (k,l) \in \mathbb{Z}^2, x = nk$ et $y = nl$ alors :
$x - y = n\underbrace{(k-l)}_{\in \mathbb{Z}}$
$x - y \in n\mathbb{Z}$
2) Soit H un sous-groupe de $(\mathbb{Z},+)$
cas 1 : $H = \{0\}$, on prend $n = 0$
cas 2 : $H \neq \{0\}$ comme $H \neq \emptyset$
$\exists h \in H, h \neq 0$ H est stable par opposé : $-h \in H$
Ainsi : $\underbrace{(h, -h)}_{h>0 \quad ou \quad -h>0} \in H^2$ donc :
$H \cap \mathbb{N}^* \neq \emptyset$ posons donc :
$n = min(H \cap \mathbb{N}^*)$ et montrons que $H = n\mathbb{Z}$
$\underline{n\mathbb{Z} \subset H}$: soit $k \in \mathbb{Z}$
Si $k = 0$ $n0 = 0 \in H$
Si $k \geq 0$: $nk = \underbrace{n + .. + n}_{k \quad termes}$
Or $n \in H$ (car $n \in H \cap \mathbb{N}^*$) et H stable par + donc $nk \in H$
Si $k \leq -1$, $nk = (-n)(-k)$
Or $-k \in \mathbb{N}^*$ donc $n(-k) \in H$ (propriété précédente).
Or H stable par opposé donc $nk \in H$
$\underline{H \subset n\mathbb{Z}}$: soit $h \in H$
On a $n \in H \cap \mathbb{N}^* \subset \mathbb{N}^*$
Soit la division euclidienne de h par n :
$b = nq + r$, $q \in \mathbb{Z}$, $0 \leq r < n$
On a $h \in H$ et $nq \in H$ car $n\mathbb{Z} \subset H$
donc $r = k - nq \in H$ car H sous-groupe de $(\mathbb{Z},+)$
Si on avait $r > 0$, on aurait :
$r \in H \cap \mathbb{N}^*$ or $r < n = min(H \cap \mathbb{N}^*)$ contradiction
donc r=0 : $h = nq \in n\mathbb{Z}$

III Existence du PGCD et relation de Bézout + lemme de Gauss

Théorème :
Soit $(a,b) \in \mathbb{Z}^2$
Il existe un unique $d \in \mathbb{N}$ tel que :
$d|a,d|b$ et pour tout $c \in \mathbb{Z}$ tel que $c|a$ et $c|b$ alors $c|d$
C'est le pgcd de a et b, noté pgcd(a,b) ou $a \wedge b$ de plus :
$\exists (u,v) \in \mathbb{Z}^2, au + bv = d$ (Relation de Bézout)
Démonstration :
Unicité : si d_1 et d_2 conviennent on a :
$d_1|a$ et $d_1|b$ donc $d_1|d_2$
De même, $d_2|d_1$ or d_1 et $d_2 \geq 0$ donc $d_1 = d_2$
Existence : posons l'ensemble $a\mathbb{Z} + b\mathbb{Z} = \{au + bv : (u,v) \in \mathbb{Z}\}$
Il s'agit d'un sous-groupe de $(\mathbb{Z},+)$. En effet :
1) $0 = a \times 0 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z}$ donc $a\mathbb{Z} + b\mathbb{Z} \neq \emptyset$
2) Soit $(x_1,x_2) \in (a\mathbb{Z} + b\mathbb{Z})^2$:
$\exists (u_1,v_1,u_2,v_2) \in \mathbb{Z}^4, x_1 = au_1 + bv_1$ et $x_2 = au_2 + bv_2$
$x_1 - x_2 = a\underbrace{(u_1 - u_2)}_{\in \mathbb{Z}} + \underbrace{b(v_1 - v_2)}_{\in \mathbb{Z}}$ donc $x_1 - x_2 \in a\mathbb{Z} + b\mathbb{Z}$
Ainsi, il existe $d \in \mathbb{N}$ tel que :
$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$
Vérifions que d convient :

On a: $d = d_1 \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$ donc :
$\exists(u,v) \in \mathbb{Z}, d = au + bv$
De plus : $a = a \times 1 + b \times 0 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ donc $d|a$
$b = a \times 0 + b \times 1 \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ donc $d|b$
Enfin, soit $c \in \mathbb{Z}$ tel que $c|a$ et $c|b$
Par combinaison linéaire : $c|(au + bv)$ et $c|d$
Théorème :
Lemme de Gauss :
Soit $(a,b,c) \in \mathbb{Z}^3$ tel que $a|bc$ et $a \wedge b = 1$ alors $a|c$.
Démonstration :
Soit $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$:
$a \times cu + bc \times v = c$
Or : $a|a$(refléxivité) et $a|bc$(hypothèse) donc par combinaison linéaire:
$a|(a \times uc + bc \times v)$ c'est-à-dire $a|c$

IV Algorithme d'Euclide (avec le lemme)

Lemme :
Soit $(a,b,q,r) \in \mathbb{Z}^4$ tel que $a = bq + r$ alors $a \wedge b = b \wedge r$.
C'est en particulier vrai si on a une division euclidienne
Démonstration :
D'une part : $(b \wedge r)|b$ et $(b \wedge r)|r$
donc par combinaison linéaire : $(b \wedge r)|(bq + r)$ donc$(b \wedge r)|a$
ainsi $b \wedge r$ divise a et b donc $(b \wedge r)|(a \wedge b)$
D'autre part : $r = b(-q) + a$
donc par le point précédent : $(b \wedge a)|(r \wedge b)$ et $(a \wedge b)|(b \wedge r)$
Ainsi $a \wedge b$ et $b \wedge r$ sont associés or ils sont ≥ 0 donc $a \wedge b = b \wedge r$
Algorithme :

```
def pgcd(a,b) :
    x,y = a,b
    while y!=0 :
        x,y=y,x%y
    return x
```

Démonstration : Notons x_k et y_k les valeurs de x et y après k itérations
Invariant: $\underline{x_k \wedge y_k = a \wedge b}$
$k = 0, x = a \quad y = b$
Soit $k \geq 1$ tel que $x_{k-1} \wedge y_{k-1} = a \wedge b$
Si on effectue une k-ième itérations :$y_{k-1} \neq 0$
Le corps de la boucle vérifie : $x_k = y_{k-1}$
$y_k =$ reste de la division euclidienne de x_{k-1} et y_{k-1}
Donc par le lemme : $x_k \wedge y_k = x_{k-1} \wedge y_{k-1} = a \wedge b$
Terminaison : Si $b \geq 0$, les valeurs y_k est une suite décroissante de $\mathbb{N}$ elle est donc finie.
Si $b < 0$ à partir du rang 1 car reste ≥ 0
Correction : notons k_0 le nombre d'itérations effectuées.
La condition de la boucle montre que $y_{k_0} = 0$
Mais $a \wedge b = x_{k_0} \wedge \underbrace{y_{k_0}}_{=0}$ (invariant)
$a \wedge b = x_{k_0}$ on renvoie bien $a \wedge b$ (au signe près)

V $(a \wedge b)(a \vee b) = |ab|$

Propriété :
$\forall(a,b) \in \mathbb{Z}^2, (a \wedge b)(a \vee b) = |ab|$

Démonstration :
Si $a = b = 0$: $a \wedge b = 0$
Si $(a,b) \neq (0,0)$ notons $d = a \wedge b \neq 0$ et $m = a \vee b$
posons $\mu = \frac{ab}{d}$
On a $\mu = a \times \underbrace{(\frac{b}{d})}_{\in \mathbb{Z}} \in \mathbb{Z}$ donc $a|\mu$
De même : $\mu = b \underbrace{(\frac{a}{d})}_{\in \mathbb{Z}}$ donc $b|\mu$
Ainsi : $m|\mu$
D'autre part :
$\exists (u,v) \in \mathbb{Z}^2, au + bv = d$ puis :
$amu + bmv = dm$
Or : $b|m$ donc $ab|am$ et $a|m$ donc $ab|bm$
donc par combinaison linéaire :
$ab|(amu + bmv)$ c'est-à-dire $ab|dm$
donc : $d\mu|dm$ enfin $d \neq 0$ donc $\mu|m$
Conclusion : $|\mu| = |m|$ donc $dm = |ab|$

VI Tout entier ≥ 2 possède un diviseur premier + infinité de l'ensemble des nombres premiers

Propriété :
Tout entier ≥ 2 possède un diviseur premier.
Démonstration : Soit $n \geq 2$
Soit $D = \{d \in \mathbb{N}^* : d \geq 2$ et $d|n\}$
On a $D \subset \mathbb{N}$ par définition et $n \in D \neq \emptyset$
Posons donc $p = min(D)$:
On a $p \in D$ donc $p|n$ mais aussi $p \geq 2$.
Soit $d \in \mathbb{N}^*$ tel que $d|p$:
Comme $p|n$, on a donc $d|n$ si $d \neq 1$, on a donc : $d \in D$ donc $d \geq p$
Or $d|p$, d'où $d = p$
Ainsi $p \geq 2$ est divisible seulement par 1 et p donc p est premier.
Propriété :
L'ensemble des nombres premier est infini.
Démonstration :
S'il existaient qu'un nombre fini de nombres premiers $p_1,...,p_r$:
Prenons $N = p_1..p_r + 1 \geq 2$
On a montré que N possédait un diviseur premier :
$\exists i \in [[1,r]], p_i|N$
Or $p_i|p_1...p_r$ donc par combinaison linéaire :
$p_i|(N - p_1...p_r)$ donc $p_i|1$
Absurde car $p_i \geq 1$

VII Tout entier ≥ 2 possède un diviseur premier + existence de la décomposition en facteurs premiers

Propriété :
Tout entier ≥ 2 possède un diviseur premier.
Démonstration : Soit $n \geq 2$
Soit $D = \{d \in \mathbb{N}^* : d \geq 2$ et $d|n\}$
On a $D \subset \mathbb{N}$ par définition et $n \in D \neq \emptyset$
Posons donc $p = min(D)$:

On a $p \in D$ donc $p|n$ mais aussi $p \geq 2$.
Soit $d \in \mathbb{N}^*$ tel que $d|p$:
Comme $p|n$, on a donc $d|n$ si $d \neq 1$, on a donc : $d \in D$ donc $d \geq p$
Or $d|p$, d'où $d = p$
Ainsi $p \geq 2$ est divisible seulement par 1 et p donc p est premier.
Théorème :
Tout entier ≥ 1 s'écrit de façon unique (à l'ordre des facteurs près) comme produit de nombres premiers.
Démonstration :
Existence : Récurrence forte
Initialisation : $n = 1$, produit nulle
Hérédité : soit $n \geq 2$ tel que tout entier ≥ 1 et $< n$ soit produit de nombres de premiers :
soit p premier tel que $p|n$ soit $k = \frac{n}{p} \in \mathbb{N}$:
$1 \leq k < n$
donc k est produit de nombres premiers donc $n = p \times k$ l'est aussi
Unicité : Récurrence forte
Initialisation : $n = 1$ seul le produit vide convient
Hérédité : soit $n \geq 2$ tel que l'unicité soit vraie pour tout k avec $1 \leq k < n$
Supposons : $n = p_1...p_r$ et $n = q_1..q_s$ avec $(r,q) \in \mathbb{N^*}^2$
p_i,q_j premiers et $p_1 \leq ... \leq p_r$ ainsi que $q_1 \leq ... \leq q_s$
L'ensemble des diviseurs premiers de n est une partie non vide (car $n \geq 2$).
Il possède donc un minimum p :
On a $p|n$, c'est-à-dire $p|p_1...p_r$ et p premier donc (lemme de Gauss) :
$\exists i \in [[1,r]], p|p_i$
Or p et p_i premier donc $p = p_i$
De plus : $p_1 \leq ... \leq p_i$
D'où comme $p = p_i$:
$p = p_1 = ... = p_i$
De même $p = q_1$
Posons $k = \frac{n}{p} = p_2...p_r = q_2...q_s$
On a $1 \leq k < n$ donc par hypothèse de récurrence :
$r = s$ et $p_2 = q_2,...,p_r = q_r$

VIII Petit théorème de Fermat (avec le lemme)

Lemme :
Soit p premier et $k \in [[1,p-1]]$ alors $p|\binom{p}{k}$
Démonstration :
$p\binom{p-1}{k-1} = k\binom{p}{k}$
Comme p est premier on a par le lemme d'Euclide
$p|k$ ou $p|\binom{p}{k}$
Les deux premiers multiples ≥ 0 de p sont 0 et p or $0 < k < p$ donc p ne divise pas k
Conclusion : $p|\binom{p}{k}$
Théorème :
Soit p un nombre premier :
1) $\forall n \in \mathbb{Z}, n^p \equiv n[p]$
2) Pour $n \in \mathbb{Z}$ non multiple de p :
$n^{p+1} \equiv 1[p]$
Démonstration :
1) **a)**Pour $n \in \mathbb{N}$ récurrence
Initialisation : $n = 0$ $0^p \equiv 0[p]$
Hérédité : Soit $n \in \mathbb{N}$ tel que $n^p \equiv n[p]$
alors : $(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$
$(n+1)^p \equiv n^p + 1[p]$ car pour $0 < k < p$
$\binom{p}{k} n^k \equiv 0[p]$ par le lemme
Donc par hypothèse de récurrence :

$(n+1)^p \equiv (n+1)[p]$
b)Soit $n \in \mathbb{N}^*$ et montrons que $(-n)^p \equiv -n[p]$
On a : $(-n)^p = (-1)^p n^p$
$(-n)^p = -(n^p)$ si p impaire, c'est-à-dire $p \geq 3$
$(-n)^p \equiv -n[p]$ par **a**
Si $p = 2$:
$(-n) = n^2$
$(-n) \equiv n[2]$
$(-n) \equiv -n[2]$ car $-1 \equiv 1[2]$
2) On a $n^p \equiv n[p]$ et de plus $non(p|n)$
Comme p est premier : $p \wedge n = 1$. Or p divise $n^p - n = n(n^{p-1} - 1)$
donc par le lemme de Gauss : $p|(n^{p-1} - 1)$
c'est-à-dire $n^{p-1} \equiv 1[p]$