**Licence 2 - 2018/2019**

**HLMA304 : Arithmétique**

Thierry Mignon

Octobre 2018

## Contrôle continu

*Durée : 1h15 – Documents, calculatrices et téléphones interdits*

**Exercice 1.** *(Cours)*

(1) Énoncer et démontrer le lemme de Gauss.

(2) Soit $p$ un nombre premier et $k$ un entier tel que $1 < k < p$. Montrer que $p$ divise le coefficient binomial $\binom{p}{k}$. Montrer que ce résultat est faux si $p$ n'est pas premier.

> CORRECTION : cf. cours

**Exercice 2.** Sachant que $12079233 = 75968 \times 159 + 321$ déterminer le reste de la division euclidienne de 12079233 par 159.

> CORRECTION : La division euclidienne de 321 par 159 s'écrit : $321 = 2 \times 159 + 3$, donc $12079233 = (75968 + 2) \times 159 + 3$, et puisque $0 \leq 3 < 21$, le reste recherché est 3.

**Exercice 3.**

(1) Calculer le pgcd, $d$, de 255 et 141 ; trouver deux entiers $u, v \in \mathbb{Z}$ tels que

$$255u + 141v = d$$

> CORRECTION : On applique l'algorithme d'Euclide étendu :
>
> $$\begin{aligned} 255 &= 1 \times 141 + 114 \\ 141 &= 1 \times 114 + 27 \\ 114 &= 4 \times 27 + 6 \\ 27 &= 4 \times 6 + 3 \end{aligned}$$
>
> Ce qui montre que $255 \wedge 141 = 3$. En remontant, on obtient :
>
> $$\begin{aligned} 3 &= 27 - 4 \times 6 = 27 - 4.(114 - 4 \times 27) = 17 \times 27 - 4 \times 114 \\ &= 17.(141 - 114) - 4.114 = 17 \times 141 - 21 \times 114 = 17.141 - 21.(255 - 141) \\ &= 38 \times 141 - 21 \times 255 \end{aligned}$$
>
> On peut donc prendre $(u, v) = (-21, 38)$, et on a $d = 3$.

(1) Soit $m$ et $n$ des entiers relatifs tels que $m$ divise à la fois $8n+7$ et $6n+5$. Montrer que $m = \pm 1$.

Correction : On observe que :

$$8n+7 = (6n+5) + (2n+2)$$
$$(6n+5) = 3.(2n+2) - 1$$

D'après un résultat du cours, on en déduit que :

$$(8n+7) \wedge (6n+5) = (6n+5) \wedge (2n+2) = (2n+2) \wedge (-1) = 1.$$

Donc $m$ divise 1, $m = \pm 1$.

(1) Soit $a$ un entier relatif. Déterminer le pgcd $d$ des entiers $m = 14a+3$ et $n = 21a+4$ ; trouver deux entiers $u$ et $v$ tels que

$$mu + nv = d.$$

Correction : On observe que :

$$21a+4 = (14a+3) + (7a+1)$$
$$14a+3 = 2 * (7a+1) + 1$$

D'après un résultat du cours, on en déduit que :

$$m \wedge n = (21a+4) \wedge (14a+3) = (14a+3) \wedge (7a+1) = (7a+1) \wedge 1 = 1$$

## Exercice 4.

(1) Montrer que si $n+m$ est pair, il en est de même pour $n-m$.

Correction : Écrivons $n+m = 2k$, où $k \in \mathbb{Z}$. Alors $n-m = (n+m) - 2m = 2(k-m)$ est pair aussi.

(1) Résoudre dans $\mathbb{Z}^2$ l'équation $n^2 - m^2 = 30$.

Correction : L'équation s'écrit : $(n-m).(n+m) = 30$.
Si $(n+m)$ est pair, $n-m$ l'est aussi, donc 4 divise 30, ce qui n'est pas le cas.
De la même façon (preuve similaire à celle ci-dessus) si $n-m$ est pair, $n+m$ l'est aussi et 4 divise 30 ce qui est impossible.
Ainsi, $(n+m)$ et $(n-m)$ sont tous les deux impairs, donc leur produit est impair, ce qui n'est pas possible puisque 30 est pair.
En conclusion, l'ensemble des solutions est vide.

**Exercice 5.**

(1) Soit $p$ un nombre premier, et $\alpha, \beta, \gamma \in \mathbb{N}$ trois entiers naturels tels que : $\alpha \leq \beta \leq \gamma$.
On pose :

$$a = p^{\alpha},\ b = p^{\beta},\ c = p^{\gamma}.$$

Déterminer $\mathrm{pgcd}(a, b, c)$ et $\mathrm{ppcm}(a, b, c)$. A quelle condition a-t-on :

$$\mathrm{pgcd}(a, b, c) \times \mathrm{ppcm}(a, b, c) = abc.$$

Correction : On sait que $\mathrm{pgcd}(a, b, c) = p^{\min(\alpha,\beta,\gamma)}$ et $\mathrm{ppcm}(a, b, c) = p^{\max(\alpha,\beta,\gamma)}$. L'équation s'écrit donc :

$$\begin{aligned} &\alpha + \beta + \gamma = \min(\alpha, \beta, \gamma) + \max(\alpha, \beta, \gamma) \\ \iff &\alpha + \beta + \gamma = \alpha + \gamma \\ \iff &\beta = 0 \end{aligned}$$

et puisque $0 \leq \alpha \leq \beta \leq \gamma$ la condition est : $\alpha = \beta = 0$, ou encore : deux des valuations $p$-adiques sont nulles.

(1) Soit maintenant $(a, b, c) \in (\mathbb{N}^*)^3$. Trouver une condition nécessaire et suffisante sur $\mathrm{pgcd}(a, b)$, $\mathrm{pgcd}(b, c)$ et $\mathrm{pgcd}(a, c)$ pour avoir :

$$\mathrm{pgcd}(a, b, c) \times \mathrm{ppcm}(a, b, c) = abc$$

Correction : Soit $p$ un nombre premier, et $\alpha_p, \beta_p, \gamma_p$ les valuations $p$-adiques de chacun des entiers $a, b, c$. On a la relation :

$$\alpha_p + \beta_p + \gamma_p = \min(\alpha_p, \beta_p, \gamma_p) + \max(\alpha_p, \beta_p, \gamma_p).$$

d'après la question précédente, ceci signifie que deux de ces trois valuations $p$-adiques sont nulles. On peut formuler cette condition de la façon suivante :

$$\min(\alpha_p, \beta_p) = 0 \text{ et } \ \min(\alpha_p, \gamma_p) = 0 \text{ et } \ \min(\beta_p, \gamma_p) = 0.$$

Puisque ces égalités sont vraies pour tous les nombres premiers $p$, elle se résume en :

$$a \wedge b = 1 \text{ et } a \wedge c = 1 \text{ et } b \wedge c = 1.$$