Correction du devoir maison 19
Calcul de PGCD - Théoreme de Bezout

Exercice 1. On rappelle que 2003 est un nombre premier.

1. (a) Déterminer deux entiers relatifs u et v tels que :

$$123u + 2003v = 1$$

Puisque 2003 est un nombre premier, il suit que PGCD$(123;2003) = 1$ et d'après le théorème de Bezout il existe deux entiers relatifs u et v tels que $123u + 2003v = 1$.
Déterminons les en remontant l'algorithme d'Euclide :

$$2003 = 123 \times 16 + 35 \Longrightarrow 35 = 2003 - 123 \times 16$$

$$123 = 35 \times 3 + 18 \Longrightarrow 18 = 123 - 3 \times 35$$

$$35 = 18 \times 1 + 17 \Longrightarrow 17 = 35 - 18$$

$$18 = 17 \times 1 + 1 \Longrightarrow 1 = 18 - 17$$

Donc

$$1 = 18 - 17 = 18 - 35 + 18 = 18 \times 2 - 35 = 123 \times 2 - 6 \times 35 - 35 = 2 \times 123 - 7 \times 35$$

Puis :

$$1 = 2 \times 123 - 7 \times (2003 - 16 \times 123) = 2 \times 123 + 112 \times 123 - 7 \times 2003 = 114 \times 123 - 7 \times 2003$$

$u = 114$ et $v = -7$ conviennent.

(b) En déduire un entier relatif k_0 tel que $123k_0 \equiv 1[2003]$.
D'apèrs la question précédente on a :

$$114 \times 123 - 7 \times 2003 = 1 \Longleftrightarrow 114 \times 123 - 1 = 7 \times 2003$$

Par conséquent 2003 divise $114 \times 123 - 1$ donc :

$$114 \times 123 - 1 \equiv 0[2003] \Longleftrightarrow 114 \times 123 \equiv 1[2003]$$

$k_0 = 114$.

(c) Montrer que, pour tout entier relatif x on a $123x \equiv 456[2003]$ si et seulement si $x = 456k_0[2003]$.

$\Longrightarrow$) Si $123x \equiv 456[2003]$ alors $123xk_0 \equiv 456k_0[2003]$.
Or, $123k_0 \equiv 1[2003]$ donc $123xk_0 \equiv x[2003]$, par conséquent :

$$x \equiv 456k_0[2003]$$

$\Longleftarrow$) Si $x \equiv 456k_0[2003]$. Puisque $123k_0 \equiv 1[2003]$ il suit que $123xk_0 \equiv x[2003]$ par conséquent :

$$123k_0x \equiv 456k_0[2003]$$

Donc 2003 divise $123k_0x - 456k_0 = k_0(123x - 456)$. Or, 2003 est premier avec k_0 (2003 étant un nombre premier) il divise d'après le théorème de Gauss $123x - 456$ par conséquent :

$$123x - 456 \equiv 0[2003] \Longleftrightarrow 123x \equiv 456[2003]$$

(d) Déterminer l'ensemble des entiers relatifs x tels que : $123x \equiv 456[2003]$.
On vient de démontrer que $123x \equiv 456[2003] \Longleftrightarrow x \equiv 456k_0[2003]$ ce qui équivaut à $2003|x - 456k_0$. Par conséquent on a $2003k = x - 456k_0$ où k est un entier relatif quelconque i.e. :

$$x = 2003k + 456k_0 = 2003k + 51984 \qquad k \in \mathbb{Z}$$

(e) Montrer qu'il existe un unique entier n tel que : $1 \leq n \leq 2002$ et $123n \equiv 456[2003]$.
n est de la forme $2003k + 51984 \qquad k \in \mathbb{Z}$ d'après la question précédente. Si $k > 0$ $n > 2002$. Il faut donc

choisir $k<0$. Pour $k=-25$ on trouve $n=2003\times(-25)+51984=1909$. Il existe donc bien un entier n tel que $1\leq n\leq 2002$ et $123n\equiv 456[2003]$.
Celui-ci est unique puisque tous les entiers naturels n vérifiant $123n\equiv 456[2003]$ s'exprime sous la forme $2003k+51984 \qquad k\in\mathbb{Z}$ la fonction $k\longmapsto 2003k+51984$ est strictement croissante sur $\mathbb{R}$, or pour $k=-24$, il se trouve que $2003k+51984>2002$ et pour $k=-26$ il se trouve que $2003k+51984<0$.

2. Soit a un entier tel que $1\leq a\leq 2002$.

   (a) Déterminer PGCD$(a;2003)$.
   2003 étant premier et $a<2003$ on a PGCD$(a;2003)=1$

   (b) En déduire qu'il existe un entier m tel que $am\equiv 1[2003]$.
   D'après le théorème de Bezout il existe deux entiers relatifs m et n tels que :

$$am+2003n=1\Longleftrightarrow am-1=2003\times(-n)\Longleftrightarrow am-1\equiv 0[2003]\Longleftrightarrow am\equiv 1[2003]$$

   (c) Montrer que, pour tout entier b, il existe un unique entier x tel que $0\leq x\leq 2002$ et $ax\equiv b[2003]$.
   D'après la question précédente il existe un entier m tel que $am\equiv 1[2003]$ par conséquent $amb\equiv b[2003]$. Il existe donc bien un entier $x=mb$ tel que $ax\equiv b[2003]$. Or puisque $am\equiv 1[2003]$ il vient que $x\equiv mb[2003]$ donc x est de la forme $2003k+mb$ avec $k\in\mathbb{Z}$. La fonction $k\longmapsto 2003k+mb$ est strictement croissante sur $\mathbb{R}$. On sait qu'il existe une valeur de k telle que $axequivb[2003]$ et $0\leq x\leq 2002$, pour $k'>k$ on a $2003k'+mb>2003k+mb+2003>2002$, de même pour $k'<k$ on a $2003k'+mb<2003+mb-2003<0$ d'où l'unicité.