CONGRUENCES

Problème, 240 minutes

Au programme ici :

– le théorème chinois qui, lorsqu'un nombre m se décompose en $m_1 \times m_2$, fait le lien entre les congruences modulo m et celles modulo m_1 et m_2 ; il est mentionné pour la première fois par Sun Zi au III$^{\text{ième}}$ siècle ;

– l'algorithme d'Euclide étendu, démontré partiellement par Bachet en 1624 avant d'être généralisé par Bézout au XVIII$^{\text{ième}}$ siècle,

– l'indicatrice d'Euler, qu'il a introduit et dont il a étudié les propriétés dès 1750.

Le formalisme des congruences a quant à lui été introduit par Gauss au tout début du XIX$^{\text{ième}}$ siècle.

Partie I — Généralités sur les congruences

Dans tout le sujet, les lettres m, m_1, m_2, etc., représentent des nombres strictement positifs et plus précisément (hormis dans cette partie) des *entiers* strictement positifs. On rappelle que deux nombres a et b sont *congrus* modulo m lorsque $b-a$ est un multiple entier de m (ce qui veut dire : il existe $k \in \mathbf{Z}$ tel que $b-a = k \times m$). On écrit alors $a \equiv b\ [m]$. Par exemple

$$\frac{19\pi}{3} \equiv \frac{\pi}{3}\ [2\pi] \qquad \text{et} \qquad 42 \equiv -9\ [17].$$

On notera $\mathrm{mod}(a, m)$ l'unique nombre dans l'intervalle $[0\,;\,m[$ qui est congru à a modulo m. En Python (et dans de nombreux langages de programmation) cela s'écrit a `%` m.

QUESTION 1.1 — *Que vaut* $\mathrm{mod}(15, 2)$ *?*

QUESTION 1.2 — *Justifier les deux congruences données en exemples ci-dessus.*

Lorsqu'on a affirmé « $\mathrm{mod}(a, m)$ est l'unique nombre dans l'intervalle $[0, ; m[$ congru à a modulo m », on sous-entend deux choses : premièrement qu'un tel nombre existe, et deuxièmement qu'il est effectivement unique. L'objet des deux prochaines questions est de justifier ces deux points.

QUESTION 1.3 — *On commence par le deuxième point : l'unicité. Supposons qu'il existe deux nombres* b_1 *et* b_2 *dans* $[0\,;\,m[$ *qui sont congrus à* a *modulo* m*. Justifier que* $|b_2 - b_1| < m$*, et en déduire que* $b_1 = b_2$*.*

QUESTION 1.4 — *Pour prouver le premier point (l'existence) on considère les nombres* $a - 0m$*,* $a - 1m$*,* $a - 2m$*,* $a - 3m$*, etc.. Que dire de la suite qu'ils forment ? Justifier que parmi eux, il y a un nombre strictement plus petit que* m*. Appelons-le* b'*. Démontrer que parmi les nombres* $b' + 0m$*,* $b' + 1m$*,* $b' + 2m$*, etc. il y a un nombre dans l'intervalle* $[0\,;\,m[$ *qui est congru à* a*.*

Désormais, et jusqu'à la fin du sujet, tous les nombres considérés (a, b, m, m_1, m_2, etc.) sont des *entiers*.

QUESTION 1.5 — *Justifier que* $\mathrm{mod}(a, m)$ *est alors lui aussi un nombre entier. Comment peut-on dans ce contexte préciser la phrase «* $\mathrm{mod}(a, m)$ *est dans l'intervalle* $[0\,;\,m[$ *» ?*

QUESTION 1.6 — *Comment interpréter* $\mathrm{mod}(a, m)$ *avec la division euclidienne ? On justifiera la réponse.*

Partie II — Inversibles modulo m

On rappelle l'un des énoncés du théorème de Bézout : si x et y sont deux entiers relatifs et si d est leur PGCD, alors il existe deux nombres $u, v \in \mathbf{Z}$ tels que $xu + yv = d$. L'algorithme d'Euclide « étendu » calcule ces nombres u et v ; le voici : il renvoie aussi le PGCD de x et y (c'est la valeur finale de la variable r dans le programme).

```
def Bézout(x, y) :
    r = abs(x) ; r_ = abs(y)
    u = 1 ; u_ = 0
    v = 0 ; v_ = 1
    while r_ > 0 :
        q = r // r_
        (r, r_) = (r_, r - q * r_)
        (u, u_) = (u_, u - q * u_)
        (v, v_) = (v_, v - q * v_)
    if x < 0 :
        u = -u
    if y < 0 :
        v = -v
    return (r, u, v)
```

QUESTION 2.1 — *À l'aide d'un contre-exemple, montrer que la réciproque « s'il existe deux nombres $u, v \in \mathbf{Z}$ tels que $xu + yv = d$, alors le* PGCD *de x et y est égal à d » est fausse. On prendra $d = 2$.*

QUESTION 2.2 — *Justifier que s'il existe $u, v \in \mathbf{Z}$ tels que $xu + yv = d$, alors le* PGCD *de x et y est un diviseur de d. En déduire que la réciproque du théorème de Bézout est vraie lorsque $d = 1$.*

Soit m un entier strictement positif. On dit qu'un nombre x est *inversible* modulo m lorsqu'il existe $u \in \mathbf{Z}$ tel que $x \times u \equiv 1\ [m]$. Ce nombre u est appelé un *inverse* de x.

QUESTION 2.3 — *Démontrer que 4 est inversible modulo 9.*

QUESTION 2.4 — *Démontrer que si* $\text{PGCD}(x, m) = 1$, *alors x est inversible modulo m.*

Le programme ci-dessous permet de calculer l'inverse de x (lorsqu'il est inversible, évidemment).

```
def Inverse(x, m) :
    (r, u, v) = Bézout(x, m)
    if r != 1 :
        raise Exception("Le nombre n'est pas inversible.")
    return u
```

QUESTION 2.5 — *Résoudre l'équation* $19x \equiv 3\ [208]$.

QUESTION 2.6 — *Démontrer la réciproque de la question* **2.4** *: si x est inversible modulo m, alors* $\text{PGCD}(x, m) = 1$.

Partie III — Le théorème chinois

Soit m un entier strictement positif. On définit l'ensemble

$$\frac{\mathbf{Z}}{m\mathbf{Z}} = \{0\,;\,1\,;\,2\,;\,\ldots\,;\,m-1\}\,,$$

qu'on notera parfois avec la barre de fraction oblique : $\mathbf{Z}/m\mathbf{Z}$. Le cardinal de cet ensemble est évidemment m. Soient m_1 et m_2 deux entiers strictement positifs dont le PGCD est égal à 1. On définit deux fonctions

$$f : \frac{\mathbf{Z}}{m_1m_2\mathbf{Z}} \longrightarrow \frac{\mathbf{Z}}{m_1\mathbf{Z}} \times \frac{\mathbf{Z}}{m_2\mathbf{Z}} \qquad \text{et} \qquad g : \frac{\mathbf{Z}}{m_1\mathbf{Z}} \times \frac{\mathbf{Z}}{m_2\mathbf{Z}} \longrightarrow \frac{\mathbf{Z}}{m_1m_2\mathbf{Z}}$$

de la manière suivante :

$$f(x) = (\mathrm{mod}(x, m_1)\,;\, \mathrm{mod}(x, m_2))$$

et

$$g(a, b) = \mathrm{mod}(bm_1u + am_2v, m_1m_2),$$

avec u et v les coefficients de Bézout de m_1 et m_2 (c'est-à-dire $m_1u + m_2v = 1$).

QUESTION 3.1 — *On prend $m_1 = 3$ et $m_2 = 8$. Calculer $f(10)$, puis $g(1, 2)$.*

QUESTION 3.2 — *D'une manière générale, démontrer que si $f(x) = (a, b)$ alors $g(a, b) = x$, et réciproquement si $g(a, b) = x$, alors $f(x) = (a, b)$. C'est le* théorème chinois.

Le théorème chinois permet de résoudre les systèmes de congruences. En voici un exemple :

$$\begin{cases} x & \equiv & 8 & [15] \\ x & \equiv & 6 & [28]. \end{cases}$$

QUESTION 3.3 — *Calculer (à la main) le* PGCD *de $m_1 = 15$ et $m_2 = 28$ et les coefficients de Bézout associés.*

QUESTION 3.4 — *Soit $x \in \mathbf{Z}/(15 \times 28)\mathbf{Z}$ une solution du système. Que vaut $f(x)$?*

QUESTION 3.5 — *En déduire la valeur de x. On expliquera la démarche.*

Partie IV — L'indicatrice d'Euler

Dans la deuxième partie on a démontré que les inversibles modulo m sont exactement les nombres x pour lesquels $\mathrm{PGCD}(x, m) = 1$. On note

$$\left(\frac{\mathbf{Z}}{m\mathbf{Z}}\right)^{\times} = \left\{ x \in \frac{\mathbf{Z}}{m\mathbf{Z}} \;\middle|\; x \text{ est inversible modulo } m \right\}$$

et on appelle $\varphi(m)$ son cardinal. La fonction φ s'appelle l'*indicatrice d'Euler*.

QUESTION 4.1 — *Expliciter l'ensemble $(\mathbf{Z}/8\mathbf{Z})^{\times}$ et en déduire la valeur de $\varphi(8)$.*

QUESTION 4.2 — *Soit p un nombre premier et soit $r \in \mathbf{N} - \{0\}$. Justifier que $\mathrm{PGCD}(x, p^r) = 1$ si et seulement si x n'est pas divisible par p, et en déduire que $\varphi(p^r) = p^r - p^{r-1}$.*

QUESTION 4.3 — *On reprend les fonctions f et g de la partie précédente, pour deux nombres m_1 et m_2 tels que $m = m_1 \times m_2$ et $\mathrm{PGCD}(m_1, m_2) = 1$. Soit $x \in \mathbf{Z}/m\mathbf{Z}$ et soit $(a, b) = f(x)$. Démontrer que $x \in (\mathbf{Z}/m\mathbf{Z})^{\times}$ si et seulement si $a \in (\mathbf{Z}/m_1\mathbf{Z})^{\times}$ et $b \in (\mathbf{Z}/m_2\mathbf{Z})^{\times}$.*

QUESTION 4.4 — *En déduire que lorsque $\mathrm{PGCD}(m_1, m_2)$, on a $\varphi(m_1 \times m_2) = \varphi(m_1) \times \varphi(m_2)$.*

QUESTION 4.5 — *Calculer $\varphi(120)$.*

FIN