Entiers et Congruences

Pour travailler dans $\mathbb{Z}/N\mathbb{Z}$, on utilise `(...)` `mod` N qui veut dire "évaluer `(...)` dans $\mathbb{Z}/N\mathbb{Z}$". Une *forme neutre* (ou *inerte*) dans les `(...)` retarde l'évaluation jusqu'à ce que le domaine ($\mathbb{Z}/N\mathbb{Z}$) soit connu [*ne pas confondre avec* `('...')` `mod` N *qui empècherait complètement l'évaluation*]. Par exemple, pour l'exponentiation, utiliser la forme neutre x `&^` i `mod` N au lieu de x`^`i `mod` N. Le résultat est réduit modulo N après chaque multiplication et non pas tout a la fin du calcul : les entiers traités restent donc petits tout au long de l'algorithme au lieu d'exploser en route.

Une forme neutre s'obtient en précédant un opérateur du signe & comme ci-dessus, ou en remplaçant la première lettre d'une fonction par une majuscule (si les auteurs de MAPLE l'ont prévu [`?mod` *recense les possibilités*]). Exemples : `Gcd`, `Factor`, `Nullspace` (par contre `Kernel` n'existe pas), etc. Attention, ce n'est pas seulement une question d'efficacité : MAPLE travaille implicitement dans le domaine le plus "simple" qui contient les données (en général $\mathbb{Z}$), et bien des résultats dépendent du domaine sous-jacent [*comparer* `factor` *et* `Factor` *sur des exemples, par exemple* x^2+1 *modulo* 5 *; trouver des exemples pour d'autres fonctions*]

L'opérateur `mod` n'affecte que l'évaluation, pas le résultat : on obtient un représentant canonique dans une classe de congruence, mais toute trace de son caractère modulaire a disparu. Le résultat de `2 mod 4` n'est pas une "classe modulo 4", mais l'entier 2. On peut utiliser les représentants habituels dans $[0,N[$ (`modp`, comportement par défaut) ou symétriques $]-N/2,N/2]$ (`mods`).

Problème I (Autour de Bezout)

On rappelle que deux entiers a et b sont premiers entre eux (n'ont aucun diviseurs premiers communs) si et seulement s'il existe u et v entiers relatifs tels que $au+bv=1$. Plus généralement, on appelle pgcd de $(a_1,\dots,a_n)$ un générateur de l'idéal (principal) $a_1\mathbb{Z}+\cdots+a_n\mathbb{Z}$ [*on prend en général le générateur positif*]. En particulier, si δ est un pgcd de (a,b), il existe u et v comme ci-dessus tels que $au+bv=\delta$ [*montrer qu'alors* $\operatorname{pgcd}(u,v)=1$].

1) [*Euclide*] L'algorithme suivant retourne-t'il le pgcd de a et b ? Si non, le corriger.

`Effectuer` r `:=` a `mod` b `;` a `:=` b `;` b `:=` r `; tant que` r `est non nul.`
`Renvoyer` a.

2) [*Euclide étendu*] Montrer que l'algorithme suivant [`igcdex` *sous* MAPLE] calcule des entiers u, v et δ comme ci-dessus

`Si` $a=0$, `renvoyer` $\delta=b$, $u=0$, $v=1$.
`On pose` $x=a$, $y=b$, $v_x=0$, $v_y=1$.
`Tant que` $y\neq 0$ [*on pourra vérifier qu'ici* $v_x b\equiv x \pmod a$ *et* $v_y b\equiv y \pmod a$]
  `trouver` q, r `réalisant la division euclidienne` $x=qy+r$.
  `remplacer` (v_x,v_y) `par` (v_y,v_x-qv_y).
  `remplacer` (x,y) `par` $(y,x-qy)$ [*c'est-à-dire* (y,r)]
`Renvoyer` $\delta=x$, $u=(x-bv_x)/a$, `et` $v=v_x$.

Remarquer que q et r sont calculés simultanément [*par exemple* `q := iquo(x,y,'r')`. *Ecrire la variante utilisant* `irem`]. Comparer avec la méthode naïve ("Euclide et on remonte").

3) En déduire un algorithme permettant, étant donnés une famille d'entiers $(a_1,\dots,a_n)$, le calcul d'entiers $(u_1,\dots,u_n)$ tels que

$$\sum_{i=1}^{n} a_i u_i = \operatorname{pgcd}(a_1,\dots,a_n).$$

4) Interpréter l'algorithme d'Euclide étendu comme une suite de modification du système linéaire d'inconnues (a,b)

$$\begin{pmatrix} u_x & v_x \\ u_y & v_y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}$$

Trouver une matrice U de déterminant ± 1 telle que $(a,b)U = (\mathrm{pgcd}(a,b), 0)$.

★★ **5)** En s'inspirant de la question précédente, montrer qu'il existe une matrice U dans $\mathrm{GL}(n,\mathbb{Z})$ (entière, de déterminant ± 1) telle que

$$(a_1,\dots,a_n)U = (\mathrm{pgcd}(a_1,\dots,a_n), 0, \dots, 0)$$

[*ne traiter que 2 coordonnées à la fois*]

Note : cette question est une version "concrète" (d'un cas particulier) du théorème des diviseurs élémentaires pour les modules de type fini sur les anneaux principaux [*appliqué au dual* $(\mathbb{Z}^n)^*$ *et au sous* $\mathbb{Z}$*-module engendré par la forme linéaire* $(a_1,\dots,a_n)$]. Les diviseurs élémentaires sont donnés par le membre de droite.

Expliquer comment calculer U [*se rappeler l'astuce de la matrice identité auxiliaire dans l'algorithme du pivot de Gauss*]. Que dire de sa première colonne ? Si b et $(a_1,\dots,a_n)$ sont des entiers fixés, expliquer comment résoudre l'équation $\sum a_i x_i = b$ en nombre entiers (x_i) [*intercaler* $UU^{-1} = \mathrm{Id}$]. Résoudre les équations $1009x+345y+56z = 1$ et $143x+195y+165z = 3$.

★ **6)** Comment résoudre un système de plusieurs équations sur $\mathbb{Z}^n$? [*la question précédente permet de se ramener à un système triangulaire*]

Problème II (Restes Chinois)

1) Déduire du problème précédent un algorithme permettant de décider si un entier x est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$, et le cas échéant de déterminer son inverse.

2) Soient a et b deux entiers > 0. On considère le système d'inconnue N

$$\begin{cases} N & \equiv & \alpha \pmod a \\ N & \equiv & \beta \pmod b \end{cases}$$

et on pose $\delta = \mathrm{pgcd}(a,b)$, puis u et v deux entiers tels que $au + bv = \delta$.

a) Montrer que le système n'a pas de solution si $\alpha \not\equiv \beta \pmod \delta$.

b) Sinon, montrer que

$$N := \alpha + u\frac{a}{\delta}(\beta - \alpha) = \beta + v\frac{b}{\delta}(\alpha - \beta) = u\frac{a}{\delta}\beta + v\frac{b}{\delta}\alpha$$

convient. Montrer que cette solution est unique modulo ab/δ.

Note : c'est une généralisation du "théorème chinois" au cas ou les modules ne sont pas nécessairement premiers entre eux. Si $\delta = \mathrm{pgcd}(a,b) = 1$, on trouve bien un isomorphisme (explicite) entre $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$ (qui à (α,β) associe N).

3) En déduire un algorithme pour résoudre un nombre quelconque de congruences simultanées.

4) Après une série de rapines, une troupe de 14 pirates partage (équitablement) le butin et laisse le reliquat, 3 écus, au cuisinier chinois, le $15^{\text{ème}}$ homme d'équipage. Le lendemain, un flibustier tombe à la mer et n'est pas repéché à temps ; après avoir envisagé le versement de sa part à des œuvres, les pirates refont le partage en incluant sa part ; le cuistot reçoit 2 écus. La semaine se passe sans encombres, mais trois pirates ivres se disputent sur leurs parts respectives et deux d'entre eux sont tués. Notre cuisinier récupère 5 écus. La fin du mois est mauvaise et 3 pirates périssent dans une embuscade ; mais le cuistot est content : il garde ses 5 écus.

Quel magot peut-il espérer empocher quand il décide d'empoisonner le reste de la bande ?

Problème III (Exponentiation)

1) Etant donné $n \geqslant 0$, écrire une procédure renvoyant la liste des bits de n, c'est-à dire, la suite $(\varepsilon_k, \ldots, \varepsilon_0) \in \{0,1\}^{k+1}$ telle que $n = \sum \varepsilon_i 2^i$ et $\varepsilon_k \neq 0$ [*remarquer que la division euclidienne de* $(\varepsilon_k, \ldots, \varepsilon_0)_2$ *par 2 est particulièrement simple ; on peut aussi utiliser* `convert(`n`, base, 2)`]. Que vaut k en fonction de n ?

2) [*droite à gauche*] Soit $x \in E$, un ensemble muni d'une multiplication. Montrer que l'algorithme suivant calcule x^n :

```
Poser y = 1, z = x
Pour i = 0,...,k
  si ε_i ≠ 0 on remplace y par yz
  on remplace z par z^2
Renvoyer y.
```

Modifier ce programme pour qu'il effectue simultanément l'écriture binaire et le calcul. Quel est le nombre de multiplications nécessaires ? Ce nombre reflète-t-il le temps d'exécution du programme ? [*discuter suivant E*]

★ **3)** [*gauche à droite*] Modifier l'algorithme ci-dessus pour qu'il lise les bits de n de gauche à droite, et n'effectue que des multiplications par x et des élévations au carré. Intérêt ?

Problème IV (Racines primitives)

On rappelle que le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est de cardinal[1]

$$\varphi(n) = n \sum_{d|n} \mu(d)/d = n \prod_{p|n} (1 - 1/p).$$

Il est cyclique ssi $n = 4$ ou est de la forme p^k ou $2p^k$, avec p premier impair et $k \geqslant 0$.

La bibliothèque `numtheory` [*chargée par* `with(numtheory)`] contient les commandes `order`, `primroot` et `mlog` pour respectivement calculer l'ordre de $b \in (\mathbb{Z}/n\mathbb{Z})^*$, un générateur g [*racine primitive, ou* primitive root *en anglais*] de $(\mathbb{Z}/n\mathbb{Z})^*$ à condition qu'il soit cyclique, et résoudre l'équation $g^x \equiv b \pmod{n}$.

1) Si G est un groupe dans lequel $x^n = 1$, montrer que x est d'ordre n ssi $x^{n/p} \neq 1$, pour tout diviseur premier p de n. En supposant connue la factorisation de $p-1$, comment calculer l'ordre d'un $b \in (\mathbb{Z}/p\mathbb{Z})$. Comparer avec la méthode naïve.

2) Combien y a-t-il de racines primitives dans $(\mathbb{Z}/p\mathbb{Z})^*$? En supposant qu'on en connaît une, comment les obtenir toutes ?

★ **3)** Calculer un ordre moyen pour $\varphi(n)/n$ [*utiliser la somme sur* $d|n$ *et inverser les sommations*]

Note : On montre que

$$\varphi(n)/n \geqslant (e^{-\gamma} + \varepsilon)/\log\log(n)$$

pour tout $\varepsilon > 0$ fixé pourvu que n soit assez grand. C'est (assez) facile de le déduire des estimations de Tchebychev et de la *formule de Mertens*

$$\prod_{p \leqslant x} (1 - 1/p) \sim e^{-\gamma} \frac{1}{\log(x)}$$

4) Pour déterminer une racine primitive modulo p, on essaie successivement 2, 3, etc. Décrire les détails de la méthode et évaluer ses chances de succès. Quid en pratique ?

Note : on note $g(p)$ la plus petite racine primitive modulo p. Un résultat célèbre de Burgess (1968) montre que $g(p) \ll p^{1/4+\varepsilon}$ pour tout $\varepsilon > 0$. Dans l'autre direction, Turán (1950) a montré que $g(p) > c \log p$ pour un $c > 0$ et une infinité de premiers p.

En moyenne, on sait montrer (Burgess et Eliott, 1968) que

$$\frac{1}{\pi(x)} \sum_{p \leqslant x} g(p) \ll (\log x)^2 (\log\log x)^4$$

[1] La fonction μ peut se définir par l'équation $\zeta(s) \sum \mu(n) n^{-s} = 1$ i.e. μ est multiplicative avec $\mu(p) = -1$, $\mu(p^e) = 0$ si $e > 1$. Ou encore $\mu(1) = 1$, $\mu(p_1 \ldots p_k) = (-1)^k$ si les p_i sont distincts et 0 sinon.

ce qui montre que $g(p)$ est souvent plus petite que $(\log p)^{2+\varepsilon}$. *En admettant GRH*[2], Murata (1997) arrive même à

$$\frac{1}{\pi(x)}\sum_{p\leqslant x} g(p) \ll \log x(\log\log x)^7$$

qui prouverait que le résultat de Turán est essentiellement optimal et qu'on peut s'attendre à trouver une racine primitive dans $[1,\ldots,\log p]$.

★ **5)** Soit g une racine primitive modulo p premier. Montrer que g ou $g+p$ est une racine primitive modulo p^k pour tout $k \geqslant 1$ ($k \leqslant 2$ si $p=2$). Expliquer comment choisir entre les deux possibilités. Montrer que si g est une racine primitive modulo p^k ($p>2$), g ou $g+p^k$ est une racine primitive modulo $2p^k$. Expliquer comment choisir.

Remarque : cette question prouve (algorithmiquement, c'est-à-dire en fournissant explicitement une racine) que $(\mathbb{Z}/n\mathbb{Z})^*$ est bien cyclique dans les cas prévus par l'énoncé. Il est facile de voir que ce sont les seuls possible à l'aide du lemme des restes chinois :

$$(\mathbb{Z}/mn\mathbb{Z})^* \simeq (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

si $(m,n)=1$, et du fait qu'un groupe cyclique d'ordre N contient exactement un sous-groupe d'ordre d pour chaque diviseur d de N. Il faut encore travailler un peu pour éliminer $\mathbb{Z}/2^k\mathbb{Z}$, $k>2$ (on montre que 5 n'est pas un carré, mais est d'ordre 2^{k-2}).

★★ **6)** Ecrire une fonction `RacinePrimitive(`n`)` qui calcule une racine primitive modulo n si elle existe et renvoie une erreur sinon. Comparer avec celle de MAPLE .

Problème V (Conjecture d'Artin)

On s'intéresse au problème dual : étant donné $g \in \mathbb{Z}$, existe-t-il une infinité de premiers p tels que g soit une racine primitive modulo p ?

1) Montrer que si $g=-1$ ou un carré parfait, la réponse est non. La *Conjecture d'Artin* (formulée en 1927) prédit que pour tout autre g, la réponse est oui.

2) Trouver la liste des premiers < 5000 tels que 2 soit racine primitive modulo p. Même question avec 3 et 5.

Note : En supposant GRH, Hooley (1967) montre que

$$\#\{p, g \text{ racine primitive mod } p\} \sim C(g)\pi(x)$$

pour une constante $C(g)>0$ explicite (et compliquée). En particulier, sous ces hypothèses, la conjecture d'Artin est vraie.

Inconditionnellement, Heath-Brown (1986) a montré que si q,r,s sont trois entiers multiplicativement indépendants tels que l'ensemble $\{q,r,s,-3qr,-3qs,-3rs,qrs\}$ ne contienne pas de carré parfait, alors l'un des trois est racine primitive modulo une infinité de p. En particulier, il existe au plus 2 premiers p tels que la conjecture d'Artin soit fausse pour $g=p$ (sans conjecture, on n'en connaît encore aucun tel qu'elle soit vraie, ni tel qu'elle soit fausse d'ailleurs).

[2] L'hypothèse de Riemann (RH) prédit que tous les 0 non réels de la fonction $\zeta(s)=\sum n^{-s}$ de Riemann sont sur la droite $\Re(s)=1/2$. On sait qu'ils sont tous dans la bande $0<\Re(s)<1$, que RH est vraie pour une proportion positive d'entre eux, et pour les premiers 10^9 zéros (en les classant par partie imaginaire croissante). GRH (pour Generalized Riemann Hypothesis) est une généralisation pour des fonctions ζ plus compliquées, liées à des corps de nombres et non plus à $\mathbb{Q}$, et tordues par des caractères. RH et GRH sont des conjectures standards, sans espoir de démonstration pour l'instant.