Un exercice d'arithmétique

1 Introduction

L'exercice ci-dessous, que nous désignerons sous le nom d'exercice de Julie [1], a pour objectif de montrer l'existence d'un entier x tel que x^3, dans son écriture en base 10, se termine par 2009. Il s'agit ici de préciser les ressorts de cet exercice et ses généralisations éventuelles.

Une première remarque c'est qu'il s'agit d'un exercice sur les congruences. En effet, il s'agit de trouver x vérifiant $x^3 \equiv 2009 \pmod{10000}$. Une deuxième remarque c'est que, s'il y a un nombre x solution, tous les nombres y congrus à x modulo 10000 sont aussi solutions (car $x \equiv y \pmod{10000}$ implique $x^3 \equiv y^3 \pmod{10000}$). En particulier, en remplaçant x par ses quatre derniers chiffres, on voit qu'il y a une solution comprise entre 1 et 10000.

On se propose de montrer le théorème général suivant :

1.1 Théorème. *Soient a et p des entiers positifs premiers avec 10. Il existe un entier x tel que $x^p \equiv a \pmod{10000}$.*

Pour changer de l'exemple de Julie, on montrera, par exemple, qu'il existe un entier x tel que l'écriture en base 10 de x^{153} se termine par 1729.

2 Preuve du théorème

2.1 Le principe

On va chercher x sous la forme a^u avec u entier. Pour cela on montrera qu'il existe un entier r tel que $a^r \equiv 1 \pmod{10000}$, puis, si r est premier avec p, on utilisera une égalité de Bézout $pu + rv = 1$ et l'on écrira (à peu de choses près) $a = a^{pu+rv} = (a^u)^p \times (a^r)^v \equiv (a^u)^p$.

2.2 Les puissances cinq-centièmes

Dans l'exercice de Julie, on montrait, entre autres, une congruence du genre $2009^{250} \equiv 1 \pmod{625}$. Ce type de congruences est très général. Précisément :

1. Car il a été proposé par Julie Anfray pour une épreuve sur dossier.

2.1 Lemme. *Soit a premier avec 10. On a $a^{500} \equiv 1 \pmod{10000}$.*

Démonstration. Comme on a $10000 = 2^4 \times 5^4 = 16 \times 625$, avec 16 et 625 premiers entre eux, il suffit de montrer que a^{500} est congru à 1 modulo 16 et modulo 625. En effet, si p et q divisent n (ici $n = a^{500} - 1$) et sont premiers entre eux, le produit pq divise n, cela vient de la formule $ppcm(p, q) \times pgcd(p, q) = pq$.

Modulo 16 c'est facile car a est congru à ± 1 ou ± 3 ou ± 5 ou ± 7. S'il est congru à ± 1 ou ± 7 son carré est congru à 1, s'il est congru à ± 3 ou ± 5, son carré est congru à $9 \equiv -7$ et sa puissance quatrième est congrue à 1. Comme 500 est multiple de 4 on a le résultat.

Pour 625 c'est un peu plus compliqué. On note d'abord, par examen des cas [2], qu'on a $a^4 \equiv 1 \pmod{5}$. On a donc $a^4 = 1 + 5k$. On calcule alors $a^{500} = (a^4)^{125}$ par la formule du binôme. On a :

$$a^{500} = (1+5k)^{125} = 1+125\times 5k+\binom{125}{2}5^2k^2+\binom{125}{3}5^3k^3+\binom{125}{4}5^4k^4+\cdots$$

On vérifie que les coefficients binômiaux d'ordre 2 et 3 sont multiples de 125 et on note que tous les termes à partir de 4 contiennent au moins $5^4 = 625$ en facteur. Tous les termes sauf le premier sont donc multiples de 625, de sorte que a^{500} est bien congru à 1 modulo 625.

2.2 *Remarque.* Avec 1729 comme avec 2009, il suffit d'élever à la puissance 250 pour obtenir 1 mais cela ne marche pas toujours. Par exemple avec 1731 il faut vraiment utiliser 500.

2.3 Une application de Bézout

2.3 Lemme. *Soit p un entier positif premier à 10 (donc à 500). Il existe des entiers positifs u, v tels que $pu = 1 + 500v$.*

Démonstration. En vertu de Bézout, il existe $u_0, v_0 \in \mathbf{Z}$ vérifiant $pu_0 + 500v_0 = 1$. Si on pose $u = u_0 + 500k$ et $v' = v_0 - pk$, on a aussi $pu + 500v' = 1$. Pour k assez grand, u est positif et v' négatif et on a le résultat en posant $v = -v'$.

2.4 Conclusion

On applique d'abord le lemme 2.3. On a $up = 1+500v$, donc $a^{up} = a\times a^{500v}$ ou encore $(a^u)^p = a \times (a^{500})^v$. Modulo 10000, on a $a^{500} \equiv 1$ en vertu de 2.1, donc, si on pose $x = a^u$, on a bien $x^p \equiv a$.

2. Ou par le petit théorème de Fermat si l'on est savant et un peu pédant.

3 Calcul pratique

3.1 Bézout

Pour trouver un entier x qui vérifie $x^{153} \equiv 1729 \pmod{10000}$, on cherche d'abord des entiers u, v positifs tels que $153u = 1 + 500v$. L'algorithme d'Euclide, tel qu'il apparaît dans le papier *Un programme pour Bézout* (voir sur ma page web) donne $-183 \times 153 + 56 \times 500 = 1$. On cherche des solutions de la forme $(-183+500k)\times 153+(56-183k)\times 500 = 1$ avec $u = 500k-183 > 0$ et $v' = -v = 56-183k < 0$. La solution avec $k = 1$ donne $u = 317$ et $v = 97$. Le nombre $x = 1729^{317}$ se termine donc par 1729.

3.2 Puissances

Pour avoir un entier y compris entre 0 et 10000 tel que y^3 se termine par $a = 1729$, il suffit de trouver y avec $x \equiv y \pmod{10000}$, ou encore de trouver les quatre derniers chiffres de $x = 1729^{317}$.

On peut faire ce calcul avec la calculatrice [3] (sans programmer). Attention, on ne peut tout de même pas calculer directement 1729^{317} (la calculatrice répond ∞). Il faut donc faire quelques étapes. Voici une solution. On calcule 1729^{10} et on ne garde que les 4 derniers chiffres : 3201. On a donc $1729^{100} \equiv 3201^{10}$ que l'on calcule, et on garde les derniers chiffres : 2001. On calcule ensuite $2001^3 \equiv 6001$. On a donc $1729^{300} \equiv 6001$. Par ailleurs on a $1729^{17} \equiv 5009$, d'où $1729^{317} \equiv 6001 \times 5009 \equiv 9009$. Le nombre cherché est donc 9009. On vérifie [4] qu'on a :

$$9009^{153} = 11628342 \cdots 24151729.$$

On peut aussi écrire un programme ou une fonction pour faire automatiquement ce calcul de puissance. En voici deux, le premier est plus simple [5], mais le second bien plus rapide (une seconde au lieu de six pour le calcul ci-dessus). Chacun de ces programmes calcule la puissance r-ième de a modulo p. Le premier consiste à multiplier a^k par a et à réduire modulo p à chaque pas :

```
power(a,r,p)
Func
Local k,z
1 → z
```

3. Voire à la main !
4. Bien que ce nombre ait 605 chiffres, la calculatrice le donne !
5. Et facile à retrouver.

```
For k,1,r
mod(a*z,p) → z
EndFor
Return z
EndFunc
```

Le second programme utilise les puissances de 2 pour grimper plus vite :

```
powerv(a,r,p)
Func
Local z
1 → z
While r > 0
If entPrec(r/2)= r/2 Then
r/2 → r
mod(a^2,p) → a
Else
(r-1)/2 → r
mod(z*a,p) → z
mod(a^2,p) → a
EndIf
EndWhile
Return z
EndFunc
```

4 Généralisation

Le nombre 10000 peut être remplacé par un n entier positif quelconque, mais il faut faire un peu attention aux hypothèses sur a et p. Rappelons quelques résultats que l'on peut trouver (par exemple) dans [DP].

On considère l'anneau quotient $\mathbf{Z}/n\mathbf{Z}$. Si n n'est pas premier, cet anneau n'est pas un corps, mais il a cependant des éléments inversibles pour la loi $\times$. L'ensemble de ces éléments est noté $(\mathbf{Z}/n\mathbf{Z})^*$ et c'est un groupe multiplicatif. Une conséquence facile du théorème de Bézout [6] permet d'affirmer qu'un nombre $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$ est inversible si et seulement si x est premier avec n. Cela permet de déterminer le cardinal de $(\mathbf{Z}/n\mathbf{Z})^*$, qui est donc le nombre d'entiers compris entre 1 et n et premiers avec n. On le note $\varphi(n)$ et on appelle fonction indicatrice d'Euler la fonction φ. On montre que si n est

6. Car $ux + vn = 1$ se lit $ux \equiv 1$ dans le quotient.

décomposé en produit de facteurs premiers : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ on a :

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1).$$

Le théorème de Lagrange (dans un groupe, l'ordre d'un élément divise le cardinal du groupe) montre alors qu'on a, pour tout a premier avec n, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

4.1 *Remarque.* Dans le cas $n = 10000 = 2^4 \times 5^4$, on a $\varphi(n) = 8 \times 500 = 4000$. On a donc $a^{4000} \equiv 1$. Comme on l'a vu en 2.1, on peut montrer mieux : $a^{500} \equiv 1$.

Le problème de Julie admet alors la généralisation suivante :

4.2 Théorème. *Soit n un entier > 0, a un entier premier avec n et p un entier premier avec $\varphi(n)$. Il existe un entier x tel que $x^p \equiv a \pmod{n}$.*

Démonstration. Une adaptation facile de 2.3 montre qu'il existe des entiers u, v positifs vérifiant : $up = 1 + v\varphi(n)$. On élève alors le nombre a à la puissance up et on a $a^{up} = a \times a^{\varphi(n)v}$ et on en déduit $(a^u)^p \equiv a \pmod{n}$.

4.3 *Remarque.* Comme on l'a remarqué plus haut, il existe un x vérifiant $x^p \equiv a \pmod{n}$ et compris entre 1 et n. Un tel x est d'ailleurs unique. En effet, si on a $x^p \equiv y^p \pmod{n}$, on a $(x^{-1}y)^p \equiv 1 \pmod{n}$. Mais, comme le groupe $(\mathbf{Z}/n\mathbf{Z})^*$ est de cardinal $\varphi(n)$ premier à p, cela implique $x^{-1}y \equiv 1 \pmod{n}$ (toujours le théorème de Lagrange), donc $x \equiv y \pmod{n}$ et comme tous deux sont entre 1 et n cela impose $x = y$.

5 Référence

[DP] PERRIN Daniel, *Cours d'algèbre*, Ellipses, 1996.