DIVISIBILITÉ	Série	Dr. Amine Touati

Autour des nombres entiers

1. ■ La conjecture suivante est-elle exacte : tout nombre entier naturel peut s'écrire sous forme de la différence de deux carrés.

2. ■ À quelle condition un entier naturel peut-il s'écrire comme somme de plusieurs entiers consécutifs ?

Diviseurs-Multiples

3. ■ Trouver un multiple de 7 qui ne s'écrit qu'avec des 9.

4. ■ Démontrer que quels que soient les entiers naturels a et b, le nombre $(a+b)^7 - a^7 - b^7$ est un multiple de 7. Étudier une généralisation de ce résultat.

5. ■ Démontrer que tous les termes de la suite définie pour n 0 par

$u_n = n(n+1)(2n+1)(3n^2+3n-1)$

sont des multiples de 30.

6. ■ a et b sont deux entiers naturels. Démontrer que $ab(a^2 - b^2)$ est un multiple de 3.

7. ■ Démontrer que si le nombre entier naturel n n'est pas un multiple de 3, alors $n^2 - 1$ est un multiple de 3.

Quand l'algèbre vole au secours de l'arithmétique

8. ■ 1) Vérifier que $2^{4n+2} + 1 = (2^{2n+1} - 2^{n+1} + 1)(2^{2n+1} + 2^{n+1} + 1)$, où n désigne un entier naturel.
2) En déduire trois diviseurs de $2^{58} + 1$.

9. ■ a désigne un réel quelconque
Montrer que :
$a^8 - a^6 + a^4 - a^2 + 1 = (a^4 + 5a^3 + 7a^2 + 5a + 1)^2 - 10a(a^3 + 2a^2 + 2a + 1)^2$
En déduire que :
$a^{10} + 1 = (a^2 + 1)\left((a^4 + 5a^3 + 7a^2 + 5a + 1)^2 - 10a(a^3 + 2a^2 + 2a + 1)^2\right)$
2) En déduire une factorisation de $10^{30} + 1$ comportant 3 facteurs.

Conditions pour qu'un entier b divise un entier a

10. ■ Comment choisir l'entier relatif n pour que $n + 7$ divise $3n + 27$?

11. ■ Soit n un entier naturel.
Montrer que : $n^3 - n = (n + 2)(n^2 - 2n + 3) - 6$
En déduire les valeurs de n pour lesquelles $\frac{n^3 - n}{n + 2}$ est un entier.

12. ■ Trouver tous les entiers positifs n tels que $\frac{n^3 + 5}{n^2 + 7}$ soit un entier.

13. ■ Déterminer tous les entiers relatifs n tels que $p = n^2 - 3n + 6$ soit un multiple de 5. On pourra à cet effet calculer la différence $p - (n - 9)^2$.

14. ■ Pour vérifier qu'un nombre est divisible par 7, on peut appliquer la méthode suivante :
on prend tous les chiffres sauf le dernier ;
on soustrait 2 fois le dernier ;
on vérifie si le résultat est divisible par 7.
Appliquer cette méthode aux nombre 364, 123769.
Expliquer pourquoi ce critère fonctionne.

Les nombres entiers de la forme $2^n - 1$.

15. ■ 1) Soit n un entier naturel non nul et d un diviseur positif de n.
Montrer que pour tout a 1, $a^n - 1$ est divisible par $a^d - 1$.
En déduire des diviseurs des entiers suivants :
$2^{18} - 1$;
$2^{54} - 1$;
$2^{254} - 1$.
Est-il possible d'obtenir par cette méthode des diviseurs de $2^{11} - 1$? Ce nombre admet-il pour autant des diviseurs ?
2) En déduire que $2^{1998} - 1$ est divisible par 3, 7, 9 et 511.

Équations diophantiennes

16. ■ Une équation diophantienne est une équation que l'on cherche à résoudre en nombres entiers (Diophante fut un mathématicien grec qui a vécu entre le II^{e} et le V^{e} siècle de notre ère). Trouver si possible *des* solutions aux équations diophantiennes suivantes :

$a^2 + b^2 = c^2$
$a^3 + b^3 = c^3$
$a^3 + b^3 = c^3 + 1$
$a^3 + b^3 + c^3 = d^3$

(Indication : il existe une solution constituée d'entiers consécutifs)

5) $a^3 + b^4 = d^5$ *(Indication : $2^3 + 2^3 = 2^4$...)*

17. ■ Trouver tous les entiers naturels dont le produit dépasse la somme de 129.

18. ■ Une puissance de 2 augmentée d'une unité peut-elle être un cube ?

19. ■ Déterminer les solutions a b dans ^{2} de $\frac{a+b}{a^2+b^2} = \frac{6}{37}$.

Division euclidienne

20. ■ Sachant qu'il existe un entier q tel que $100^{100} = 13q + 35$, écrire la division euclidienne de 100^{100} par 13.

21. ■ Soit n un entier supérieur ou égal à 1. Déterminer le quotient et le reste de la division euclidienne :

1) de $n^2 + n + 1$ par $n + 1$;
2) de $n^2 + n + 1$ par $n + 2$;
3) de $2^n - 1$ par 2^{n-1}.

22. ■ x est un entier relatif.

1) a) Montrer que le reste de la division euclidienne de x^2 par 8 est 0, 1 ou 4.

b) Que dire de ces restes si $x = 2k + 1$ où k est un entier relatif ?

2) a) Résoudre l'équation $x^2 = 8y + 1$ d'inconnue (x, y) dans $\times$.

b) Montrer que la parabole $(\mathcal{P})$ d'équation $y = \frac{x^2 - 1}{8}$ passe par une infinité de points à coordonnées entières.

23. ■ 1) Déterminer le reste de la division euclidienne de 2^{6n} par 9 pour tout entier naturel n, puis le reste de 2^{18} par 19.

2) En déduire que $2^{2^{6n+2}} + 3$ est divisible par 19 pour tout entier naturel n.

24. ■ n étant un entier naturel, on pose $A_n = n^2 - n + 1$.

Montrer que les nombres A_n et A_{n+7} ont le même reste dans la division euclidienne par 7.

Étudier les restes successifs des divisions euclidiennes par 7 des nombres A_n.

En déduire les entiers naturels n tels que A_n soit divisible par 7.

Donner le reste de la division euclidienne par 7 de $2008^2 - 2008 + 1$ puis de

$23456789^2 - 23456789 + 1$.

DIVISIBILITÉ Corrigé Dr. Amine Touati

Autour des nombres entiers

25. ■ On peut d'abord tenter d'examiner ce qui se passe en examinant la répartition des premiers carrés :

0 1 4 9 16 25 36 49 64 81

+1 +3 +5 +7 +9 +11 +13 +15 +17

On constate que la différence entre deux carrés consécutifs donne un nombre impair. Ceci se généralise sans peine : si on considère le nombre impair $2k + 1$, il est clairement égal à la différence de deux carrés $(k + 1)^2 - k^2$.

Reste donc le problème des entiers naturels pairs.

Il se règle facilement pour les multiples de 4. En effet, on peut observer que :

$4 = 2^2 - 0^2$;

$8 = 3^2 - 1^2$;

$12 = 4^2 - 2^2$

etc.

et plus généralement, pour k 1 :

$(k + 1)^2 - (k - 1)^2 = k^2 + 2k + 1 - (k^2 - 2k + 1) = 4k$.

Par suite, n'importe quel nombre de la forme $4k$, avec k 1, peut s'écrire comme différence de deux carrés.

Quid des entiers congrus à 2 modulo 4, comme 2, 6, 10, 14, etc. À première vue, il semble impossible de les écrire comme différence de deux carrés.

Examinons de plus près une égalité du type

$a^2 - b^2 = 4k + 2$ soit

$(a - b)(a + b) = 2(2k + 1)$

avec a, b et k entier naturels, $a > b$.

Tout est basé sur l'argument suivant : $a - b$ et $a + b$ ont toujours la même parité, tous les deux pairs ou tous les deux impairs (vérification immédiate).

L'égalité est impossible puisque l'autre membre représente un nombre qui est le produit de 2 par un nombre impair, autrement dit le produit de deux nombres de parités différentes (si $a - b$ et $a + b$ sont tous les deux pairs, après simplification par 2, on arrive à un nombre impair égal à un nombre pair ; si $a - b$ et $a + b$ sont tous les deux impairs, leur produit est impair et ne peut pas être égal à un nombre pair).

Bilan : les nombres qui peuvent s'écrire sous la forme de deux carrés sont tous les entiers, exceptés ceux qui sont congrus à 2 modulo 4.

26. ■ Là encore des essais s'imposent. La question est volontairement ouverte. Après quelques calculs rapides, on constate que ni 2 ni 4 ni 8 ne peuvent se mettre sous la forme d'une somme d'entiers consécutifs. En revanche

$1 = 0 + 1$; $3 = 1 + 2$; $5 = 2 + 3$; $6 = 1 + 2 + 3$; $7 = 3 + 4$; $9 = 4 + 5 = 2 + 3 + 4$

La tentation est grande de conjecturer que n peut s'écrire comme somme d'entiers consécutifs si et seulement si n n'est pas égal à une puissance de 2 (hormis le cas $2^0 = 1$).

Examinons d'abord ce que sont les sommes d'entiers consécutifs :

$$\sum_{i=0}^{q} p + i = p + (p+1) + \ldots + (p+q) = \frac{(q+1)(2p+q)}{2}$$ (…suite arithmétique...)

Or, $q + 1$ et $2p + q$ sont de parités différentes (regarder ce qui se passe lorsque q est pair, puis lorsque q est impair).

Il y a donc nécessairement un facteur impair dans la décomposition de la somme, ce qui justifie que la somme ne pourra jamais être égale à une puissance de 2.

Réciproquement, si n est un entier qui n'est pas une puissance de 2, il possède au moins un facteur impair $b > 1$. On peut donc l'écrire sous la forme $n = a \times b$, où a est un entier éventuellement égal à 1.

Il reste à trouver p et q tels que $\frac{(q + 1)(2p + q)}{2} = a \times b$ soit encore $(q + 1)(2p + q) = 2ab$.

Par identification, on peut trouver *a priori* deux solutions au moins :

$$\begin{cases} q + 1 = 2a \\ 2p + q = b \end{cases} \text{ ou } \begin{cases} q + 1 = b \\ 2p + q = 2a \end{cases}$$

soit :

$$\begin{cases} q = 2a - 1 \\ p = \dfrac{b - 2a + 1}{2} \end{cases} \text{ ou } \begin{cases} q = b - 1 \\ p = \dfrac{2a - b + 1}{2} \end{cases}$$

Remarquons que b étant impair, $b - 2a + 1 = b - (2a - 1)$ est pair, ainsi d'ailleurs que le nombre $2a - b + 1 = 2a - (b - 1)$: la division par 2 donne bien un nombre entier… En changeant la valeur de b, lorsque c'est possible, on peut trouver d'autres solutions…

Ainsi, pour $n = 244 = 4 \times 61$, avec donc $a = 4$ et $b = 61$, on sera amené par exemple à résoudre le système :

$$\begin{cases} q + 1 = 8 \\ 2p + q = 61 \end{cases} \text{ soit } \begin{cases} p = 27 \\ q = 7 \end{cases}.$$

Ce qui donne $27 + 28 + \ldots + 34 = 244$… comme le confirme la calculatrice :

Diviseurs-Multiples

27. ■ Plusieurs approches sont possibles. Utilisons les plus simples pour ce chapitre.

- Commençons par une méthode constructive : la multiplication à trous que l'on complète en commençant par les chiffres des unités et en n'oubliant pas les retenues…

	?	?	?	?	?	
×						7
…	9	9	9	9	9	

Par exemple, le premier chiffre à droite est forcément un 7, car $7 \times 7 = 49$; donc on pose 9 et on retient 4.

Pour le chiffre qui vient après, c'est forcément un 5 car $7 \times 5 = 35$, plus 4 de retenue donne 39 ; on pose 9 et l'on retient 3. Etc. On s'arrête quand il n'y a plus de retenue et qu'on peut écrire la multiplication complète. Ce qui arrive assez rapidement…

1	4	2	8	5	7	
×						7
…	9	9	9	9	9	

De façon analogue, on peut poser la division de 9999... par 7 (en adjoignant un 9 de plus dans l'écriture à chaque étape) et on s'arrête au premier reste nul.

9	9	9	9	…	7

On obtient finalement $999\,999 = 7 \times 142\,857$.

- Enfin une autre méthode, liée au développement décimal périodique de $\frac{1}{7}$, peut être signalée : la plus joli sans doute, la plus rapide aussi…

On sait que $\frac{1}{7} = 0{,}142857\,142857...$

Par suite, $\frac{10^6}{7} = 142857{,}142857... = 142857 + \frac{1}{7}$, si bien que $\frac{999999}{7} = 142857$.

Par suite, on en tire $7 \times 142857 = 999999$.

Remarquons aussi que 111111 est un multiple de 7, qui ne s'écrit qu'avec des 1.

28. ■ Il suffit d'écrire :

$$\begin{aligned} (a+b)^7 - a^7 - b^7 &= \binom{7}{1}a^6b + \binom{7}{2}a^5b^2 + \binom{7}{3}a^4b^3 + \binom{7}{4}a^3b^4 + \binom{7}{5}a^2b^5 + \binom{7}{6}ab^6 \\ &= 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 \\ &= 7\left(a^6b + 3a^5b^2 + 5a^4b^3 + 5a^3b^4 + 3a^2b^5 + ab^6\right) \end{aligned}$$

On a bien un multiple de 7 car les coefficients $\binom{7}{k}$ qui interviennent sont des multiples de 7 … et que le deuxième facteur de cette égalité est un nombre entier…

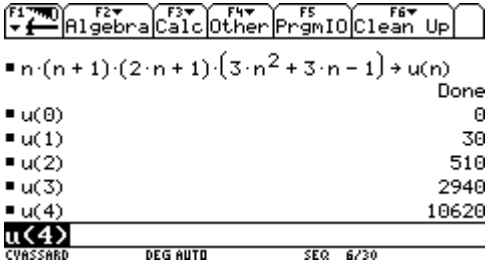
Pour généraliser, on peut montrer que si p est un nombre premier, alors pour tout entier k tel que $0 < k < n$, $\binom{p}{k}$ est un multiple de p.

En effet, on a : $\binom{p}{k} = \dfrac{p!}{k!(p-k)!} = \dfrac{p(p-1)(p-2)\ldots(p-k+1)}{k(k-1)\ldots 2\times 1}$.

Si p est premier, on sait que chacun des nombre k, $k-1$, ..., 2, 1 est premier avec p : il en est de même de $k!$.
Comme par ailleurs $k!$ divise $p(p-1)\ldots(p-k+1)$, c'est donc que $k!$ divise $(p-1)\ldots(p-k+1)$: on en déduit donc que $\binom{p}{k}$ est un multiple de p.

Par suite, le résultat proposé est aussi vrai si p est un nombre premier.

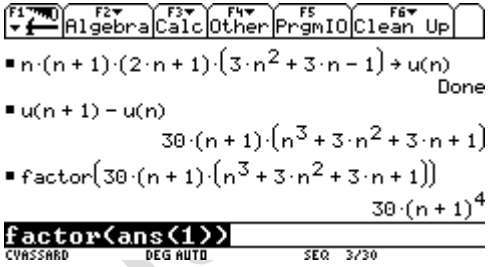
29. ■ On peut commencer par calculer les premiers termes, à l'aide d'une Voyage 200 :



Remarquons que

$$\begin{aligned} u_{n+1}-u_n &= (n+1)(n+2)\left(2(n+1)+1\right)\left(3(n+1)^2+3(n+1)-1\right)-n(n+1)(2n+1)\left(3n^2+3n-1\right)\\ &= (n+1)\left((n+2)(2n+3)\left(3n^2+9n+5\right)-n(2n+1)\left(3n^2+3n-1\right)\right)\\ &= (n+1)\left(6n^4+39n^3+91n^2+89n+30-6n^4-9n^3-n^2+n\right)\\ &= (n+1)\left(30n^3+90n^2+90n+30\right)\\ &= 30(n+1)\left(n^3+3n^2+3n+1\right) = 30(n+1)^4 \end{aligned}$$

La calculatrice peut d'ailleurs effectuer ce calcul pénible.



Il est immédiat que $u_{n+1}-u_n$ est un multiple de 30, quel que soit l'entier naturel n.
Par suite $u_n = (u_n-u_{n-1})+(u_{n-1}-u_{n-2})+\ldots+(u_2-u_1)+(u_1-u_0)+u_0$ est un multiple de 30 comme somme de multiples de 30.

30. ■ Si a ou b sont des multiples de 3, c'est immédiat.
Sinon ils peuvent s'écrire sous la forme

$$a = 3k+\varepsilon_1,\ b = 3k+\varepsilon_2$$

avec $\varepsilon_1 = \pm 1$ et $\varepsilon_2 = \pm 1$.
Alors :

$$\begin{aligned} a^2-b^2 &= \left(3k_1+\varepsilon_1\right)^2-\left(3k_2+\varepsilon_2\right)^2 = 9k_1{}^2-9k_2{}^2+6\varepsilon_1k_1-6\varepsilon_2k_2+\varepsilon_1{}^2-\varepsilon_2{}^2\\ &= 9k_1{}^2-9k_2{}^2+6\varepsilon_1k_1-6\varepsilon_2k_2 \end{aligned}$$

car $\varepsilon_1{}^2 = \varepsilon_2{}^2 = 1$.
Ce dernier nombre est clairement un multiple de 3, ce qu'il fallait prouver.

31. ■ Un entier naturel n qui n'est pas multiple de 3 s'écrit sous la forme $n = 3k \pm 1$.
Par conséquent $n^2-1 = (3k\pm 1)^2-1 = 9k^2\pm 6k+1-1 = 9k^2\pm 6k = 3\left(3k^2\pm 2k\right)$.
Comme $3k^2\pm 2k$ est un entier naturel, on a bien prouvé que n^2-1 est un multiple de 3. Remarquons qu'il ne l'est pas lorsque $n = 3k$.
Alors $n^2-1 = 9k^2-1 = (9k^2-3)+2 = 3(3k^2-1)+2$ a pour reste 2 dans la division par 3.

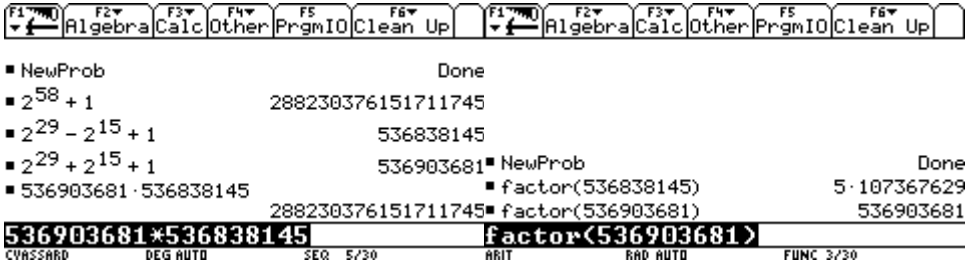
Quand l'algèbre vole au secours de l'arithmétique
32. ■ 1) Il suffit d'écrire...

$$\left(2^{2n+1}-2^{n+1}+1\right)\left(2^{2n+1}+2^{n+1}+1\right)=\left(2^{2n+1}+1\right)^2-\left(2^{n+1}\right)^2$$
$$=2^{4n+2}+2\times 2^{2n+1}+1-2^{2n+2}=2^{4n+2}+1$$

2) Ceci permet de factoriser les nombres de la forme $2^p - 1$ quand p est de la forme $4n + 2$... comme le montre l'exemple suivant :

$$2^{58}+1=2^{4\times 14+2}+1=\left(2^{2\times 14+1}-2^{14+1}+1\right)\left(2^{2\times 14+1}+2^{14+1}+1\right)$$
$$=\left(2^{29}-2^{15}+1\right)\left(2^{29}+2^{15}+1\right)$$

La factorisation obtenue est confirmée par la calculatrice, alors qu'elle aurait été obtenue très difficilement avec factor :



C'est un nombre de 18 chiffres que la calculatrice parvient à factoriser avec sa fonction factor, mais assez péniblement. La factorisation algébrique déjà obtenue facilite grandement les choses : chacun des deux nombres intermédiaires obtenus se factorise presque instanément.

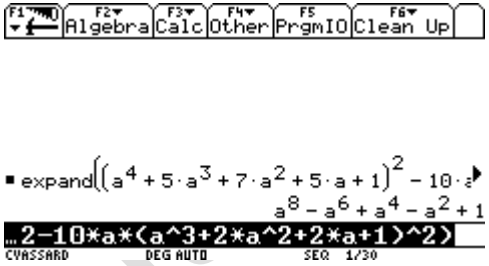
Remarquons que, sans le calculer, on peut remarquer que $2^{29} - 2^{15} + 1$ est divisible par 5. En effet, on sait que $2^4 \equiv 1 \pmod 5$, donc $2^{29} \equiv 2^{28} \times 2 \equiv 2 \pmod 5$.

Enfin, $2^{15} \equiv 2^{12} \times 2^3 \equiv 3 \pmod 5$.

Si bien que $2^{29} - 2^{15} + 1 \equiv 2 - 3 + 1 \equiv 0 \pmod 5$.

Une factorisation complète de $2^{106} + 1$ peut être tentée par ce procédé.

33. ■ 1) C'est l'objet d'un calcul algébrique classique, un peu pénible, que la calculatrice gère parfaitement...



Par ailleurs, on sait que

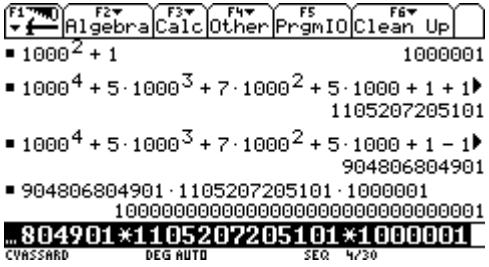
$$a^8-a^6+a^4-a^2+1=1+\left(-a^2\right)+\left(-a^2\right)^2+\left(-a^2\right)^3+\left(-a^2\right)^4$$
$$=\frac{1-\left(-a^2\right)^5}{1-\left(-a^2\right)}=\frac{1+a^{10}}{1+a^2}$$

D'où le résultat : $a^{10} + 1 = (a^2 + 1)\left((a^4 + 5a^3 + 7a^2 + 5a + 1)^2 - 10a(a^3 + 2a^2 + 2a + 1)^2\right)$

2) C'est un résultat qui permet des factorisations, comme celle de $10^{30} + 1$...

$$10^{30}+1=\left(1000\right)^{10}+1$$
$$=\left(1000^2+1\right)\left(\left(1000^4+5\times 1000^3+7\times 1000^2+5\times 1000+1\right)^2-10000\left(1000^3+2\times 1000^2+2\times 1000+1\right)^2\right)$$

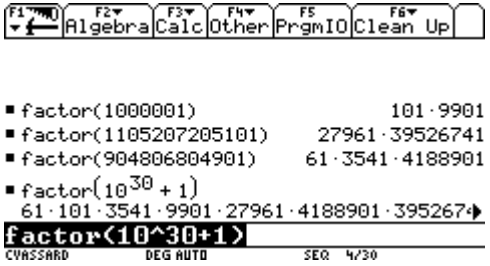
Comme 10000 est le carré de 100, on peut factoriser la deuxième parenthèse. Pour gagner du temps, il vaut mieux faire les calculs avec la voyage 200.



On obtient donc la décomposition :

$$10^{30} + 1 = 1000001 \times 1105207205101 \times 904806804901$$

On peut alors, grâce à la fonction factor de la calculatrice la décomposition complète en facteurs premiers, en décomposant chacun des petits facteurs obtenus :



La décomposation directe de $10^{30} + 1$ demande près d'une minute de travail à la voyage 200.

Conditions pour qu'un entier b divise un entier a

34. ■ On peut écrire, par exemple par division euclidienne :

$$\frac{3n+27}{n+7} = 3 + \frac{6}{n+7}$$

Dire que $\frac{3n+27}{n+7}$ est un entier équivaut à dire que $\frac{6}{n+7}$ en est un, autrement dit que $n + 7$ divise 6.

Les diviseurs de 6 sont 1 et –1, 2 et –2, 3 et –3, 6 et –6.

Ce qui donne pour n les valeurs :

$n + 7 = 1$, soit $n = -6$;
$n + 7 = -1$, soit $n = -8$;
$n + 7 = 2$, soit $n = -5$;
$n + 7 = -2$, soit $n = -9$;
$n + 7 = 3$, soit $n = -4$;
$n + 7 = -3$, soit $n = -10$;
$n + 7 = 6$, soit $n = -1$;
$n + 7 = -6$, soit $n = -13$.

35. ■ Il est immédiat de vérifier que, pour tout entier n, $n^3 - n = (n + 2)(n^2 - 2n + 3) - 6$.

Par suite $\frac{n^3-n}{n+2} = n^2 - 2n + 3 - \frac{6}{n+2}$ (on aurait pu aussi obtenir ce résultat en effectuant la division euclidienne de $n^3 - n$ par $n + 2$).

Il est clair que $n^2 - 2n + 3$ est un entier lorsque n en est un.

Par suite, $\frac{n^3-n}{n+2}$ est un entier si et seulement si $n + 2$ divise 6.

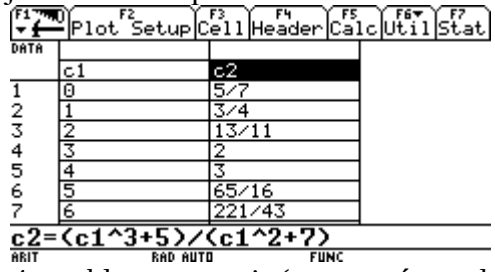
Les diviseurs de 6 sont 1 et –1, 2 et –2, 3 et –3, 6 et –6.

Ce qui donne pour n les valeurs :

$n + 2 = 1$, soit $n = -1$;
$n + 2 = -1$, soit $n = -3$;
$n + 2 = 2$, soit $n = 0$;
$n + 2 = -2$, soit $n = -4$;
$n + 2 = 3$, soit $n = 1$;
$n + 2 = -3$, soit $n = -5$;
$n + 2 = 6$, soit $n = 4$;
$n + 2 = -6$, soit $n = -8$.

Et ce sont les seules valeurs.

36. ■ On peut conjecturer une réponse à l'aide de la calculatrice…



Seuls $p = 3$ ou $p = 4$ semblent convenir (on a testé tous les entiers de 0 à 30).

Transformons l'écriture par division euclidienne :

$$\frac{n^3+5}{n^2+7} = \frac{n\left(n^2+7\right)-7n+5}{n^2+7} = n - \frac{7n-5}{n^2+7}$$

Procédons à l'analyse du problème.

Soit n tel que $\frac{n^3+5}{n^2+7}$ soit un entier. Alors $p = n - \frac{n^3+5}{n^2+7} = \frac{7n-5}{n^2+7}$ en est aussi un.

Manifestement n ne peut pas être égal à 0 (–5/7 n'étant pas un entier) ; par conséquent, n est au moins égal à 1, et p est un entier positif.

Plus précisément, p vérifie la relation :

$p = \dfrac{7n-5}{n^2+7}$ soit $pn^2 - 7n + 7p + 5 = 0 \ldots$

Une équation du second degré se cache derrière cette égalité… sauf si $p = 0$ qui conduirait à $n = 5/7$… qui est impossible !

p est donc un entier strictement positif.

n est donc effectivement solution de l'équation $pX^2 - 7X + 7p + 5 = 0$. Le discriminant de cette équation vaut :

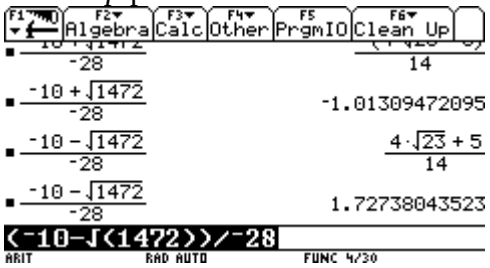
$$\Delta = 49 - 4p(7p+5) = -28p^2 - 20p + 49.$$

L'équation ayant au moins une solution, n, ce discriminant est positif ou nul…

Ce discriminant est lui-même un trinôme du second degré en p, dont le discriminant réduit vaut :

$$100 - (-28) \times 49 = 1472 > 0$$

… par suite, le trinôme en p possède deux racines :



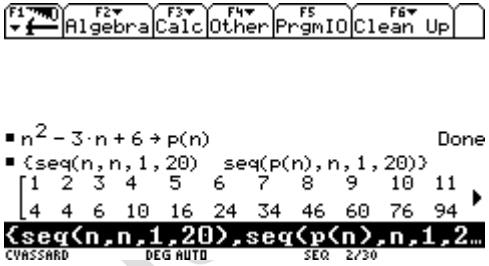
Puisque $\Delta = -28p^2 - 20p + 49 > 0$, p est donc situé entre les racines. La seule valeur entière possible est : $p = 1$ (0 a déjà été exclu).

Finalement n est solution de l'équation $X^2 - 7X + 12 = 0$, dont les solutions sont 3 et 4…

Réciproquement, ces valeurs conduisent bien à ce que $\dfrac{n^3+5}{n^2+7}$ soit un entier.

On l'a d'ailleurs déjà vérifié à la calculatrice.

37. ■ Une recherche à la calculatrice permet d'anticiper la réponse :



Calculons la différence $p - (n-9)^2$:

$$p - (n-9)^2 = n^2 - 3n + 6 - n^2 + 18n - 81 = 15n - 75 = 5(3n - 15)$$

Ce dernier résultat est un multiple de 5. Donc dire que p est un multiple de 5 équivaut donc à dire que $(n-9)^2$ l'est aussi.

Ceci a lieu si et seulement si $n - 9$ est un multiple de 5 (en effet, si 5 divise $(n-9)^2$, le facteur premier 5 intervient dans la décomposition de $(n-9)^2$, donc dans celle de $n - 9$; la réciproque est immédiate).

Autrement dit, il existe un entier k tel que $n - 9 = 5k$ soit $n = 5k + 9 = 5K + 4$: n est donc congru à 4 modulo 5.

Réciproquement si $n = 5K + 4$, alors $(n-9)^2 = 5K - 5$ est clairement un multiple de 5.

38. ■ Les critères de divisibilité peuvent être vus comme la mise en oeuvre simple d'algorithmes. En fait deux algorithmes sont en confrontation : celui de la division et le critère de divisibilité proprement dit (avec 7, la division est à peine plus longue, ce qui fait que le critère de divisibilité est peu employé).

Appliquons le critère proposé. On applique de proche en proche le procédé jusqu'à reconnaître un multiple de 7, ou non :

pour 364, $36 - 2 \times 4 = 28$ qui est un multiple de 7 ;

pour 123769, $12376 - 2 \times 9 = 12358$; $1235 - 2 \times 8 = 1219$; $121 - 2 \times 9 = 103$; $10 - 2 \times 3 = 4$ qui n'est pas un multiple de 7.

L'explication peut être donnée sur un exemple, le premier 364.

Dire que 364 est divisible par 7 équivaut à dire que le sont chacun des nombres suivants :

$36 \times 10 + 4$

$36 \times 10 + 4 - 21 \times 4$

$36 \times 10 - 4 \times 20$

$(36 - 2 \times 4) \times 10$

$36 - 2 \times 4$ aussi.

Soit A un entier naturel, se décomposant en base 10 sous la forme $\overline{a_n a_{n-1} \ldots a_1 a_0}$. Montrons plus généralement que : 7 divise n si et seulement si 7 divise $\overline{a_n a_{n-1} \ldots a_1} - 2 \times a_0$.

Supposons d'abord que 7 divise $\overline{a_n a_{n-1} \ldots a_1 a_0}$; comme par ailleurs 7 divise 21, on peut affirmer que :

$$7 \text{ divise } \overline{a_n a_{n-1} \ldots a_1 a_0} - 21a_0 = \overline{a_n a_{n-1} \ldots a_1} \times 10 + a_0 - 21a_0$$
$$= \overline{a_n a_{n-1} \ldots a_1} \times 10 - 20a_0 = 10\left(\overline{a_n a_{n-1} \ldots a_1} - 2a_0\right)$$

Comme 7 est premier et que 7 ne divise pas 10, d'après le théorème de Gauss, on en déduit que 7 divise $\overline{a_n a_{n-1} \ldots a_1} - 2 \times a_0$.

Réciproquement, si 7 divise $\overline{a_n a_{n-1} \ldots a_1} - 2 \times a_0$, il divise aussi $10\left(\overline{a_n a_{n-1} \ldots a_1} - 2a_0\right)$ qui est égal à $\overline{a_n a_{n-1} \ldots a_1} \times 10 - 20a_0$ et donc aussi $\overline{a_n a_{n-1} \ldots a_1} \times 10 - 20a_0 + 21a_0 = \overline{a_n a_{n-1} \ldots a_1 a_0}$.

Les nombres entiers de la forme $2^n - 1$

De nombreux résultats d'algèbre, en particulier ceux liés aux polynômes, trouvent naturellement une application en arithmétique. On retrouve en particulier les identités remarquables suivantes (x et y sont des entiers relatifs et n un entier naturel) :

$x^2 - y^2 = (x - y)(x + y)$

$x^3 - y^3 = (x - y)(x^2 + xy + y^2)$

$x^4 - y^4 = (x - y)(x^3 + x^2y + xy^2 + y^3)$

Plus généralement,

$$\boldsymbol{x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots xy^{n-2} + y^{n-1})}$$

ce que l'on vérifie immédiatement en développant le membre de droite.

En supposant maintenant n impair, on peut donc écrire, en remplaçant y par $-y$:

$$x^n - (-y)^n = x^n + y^n = (x - (-y))(x^{n-1} + x^{n-2}(-y) + x^{n-3}(-y)^2 + \ldots + x(-y)^{n-2} + (-y)^{n-1})$$

On obtient ainsi une autre identité remarquable très utile en arithmétique :

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \ldots - xy^{n-2} + y^{n-1})$$

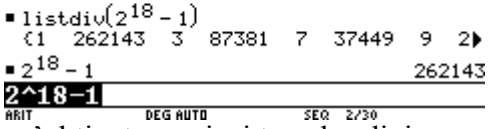
39. ■ Comme d est un diviseur positif de n, on peut écrire $n = dk$, avec k entier naturel.

$$a^n - 1 = \left(a^d\right)^k - 1^k$$

dont on sait, en utilisant la première des identités remarquables rappelées plus haut, qu'il est divisible par $a^d - 1$.

Ceci permet d'obtenir des diviseurs de $2^{18} - 1$:

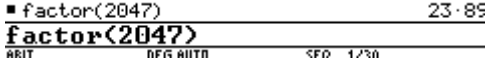
$2^{18} - 1 : 2^9 + 1 = 513$; $2^6 + 1 = 65$; $2^3 + 1 = 9$; $2^2 + 1 = 5$; $2^1 + 1 = 3$.



Remarquons qu'on n'obtient pas ainsi tous les diviseurs... Par exemple 87381 est passé entre les mailles…

Même raisonnement pour les deux autres nombres.

On n'obtient pas de diviseurs propres de $2^{11} - 1$ par cette méthode car 11 est premier. Pourtant ce nombre admet des diviseurs, comme le montre l'écran suivant :



2) Les premiers diviseurs de 1998 sont : 2, 3, 6, 9, 18 etc.

Par conséquant, $2^{1998} - 1$ est divisible par :

$2^2 - 1 = 3$

$2^3 - 1 = 7$

$2^6 - 1 = 63$

$2^9 - 1 = 511$

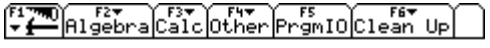
Pourquoi est-il divisible par 9, comme le demande l'énoncé ? Le nombre est en fait divisible par $2^{18} - 1 = 262143$… qui lui-même est un multiple de 9.

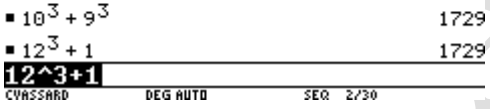
Équations diophantiennes

40. ■ $a^2 + b^2 = c^2$: Un triplet d'entiers solution de cette équation est appelé *triplet pythagoricien*. Le plus célèbre est sans doute (3,4,5).

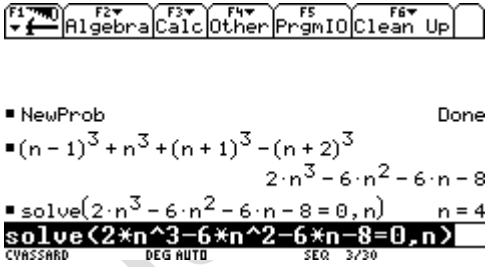
$a^3 + b^3 = c^3$: un des cas particuliers du célèbre théorème de Fermat.
Autour de 1637, Fermat a écrit dans la marge de son livre des *Arithmétiques* de Diophante :
« D'autre part, un cube n'est jamais la somme de deux cubes, une puissance quatrième n'est jamais la somme de deux puissances quatrièmes, et plus généralement, aucune puissance supérieure à 2 n'est la somme de deux puissances analogues. J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir. »
Malheureusement, personne n'a retrouvé la *merveilleuse démonstration* de Fermat, probablement fausse d'ailleurs… De nombreux mathématiciens, et non des moindres, se sont attelés à la tâche mais le grand théorème de Fermat, dans toute sa généralité, s'est obstiné à demeurer inaccessible. Il a fallu attendre plus de 350 ans pour qu'Andrew Wiles, en 1993 (mais il y a avait un « trou » dans sa démonstration), puis en 1994 (sans « trou » cette fois), propose à la communauté mathématique une démonstration de cette conjecture.

$a^3 + b^3 = c^3 + 1$:





$a^3 + b^3 + c^3 = d^3$
Cherchons avec la calculatrice une solution constituée d'entiers consécutifs.



On a donc $3^3 + 4^3 + 5^3 = 6^3$.

5) $a^3 + b^4 = d^5$
On sait que $2^{24} + 2^{24} = 2^{25}$ soit $\left(2^8\right)^3 + \left(2^6\right)^4 = \left(2^5\right)^5$. Une solution est 256, 64, 32.

41. ■ Si on appelle x et y les entiers cherchés, l'équation à résoudre est :
$$xy - (x + y) = 129.$$
Pour résoudre cette équation, on se ramène à une recherche de diviseurs en factorisant.
Il suffit de remarquer que $(x-1)(y-1) = xy - x - y + 1$.
L'équation équivaut donc à :
$$(x-1)(y-1) = 130.$$
Tout revient à chercher $x - 1$ et $y - 1$ parmi les diviseurs de 130, qui sont :
$$\{1,2,5,10,13,26,65,130\}$$
Les solutions, pour celles qui sont toutes les deux positives, sont :
$x - 1 = 1$ et $y - 1 = 130$ soit $x = 2$ et $y = 131$
$x - 1 = 2$ et $y - 1 = 65$ soit $x = 3$ et $y = 66$
$x - 1 = 5$ et $y - 1 = 26$ soit $x = 6$ et $y = 27$
$x - 1 = 10$ et $y - 1 = 13$ soit $x = 11$ et $y = 14$
$x - 1 = 13$ et $y - 1 = 10$ soit $x = 14$ et $y = 11$
… mais on constate ici que l'on retrouve les mêmes valeurs que plus haut, en échangeant x et y.
Réciproquement ces solutions conviennent toutes.

42. ■ Il s'agit de résoudre en entiers naturels l'équation $2^n + 1 = m^3$.
Supposons qu'il existe une solution (n,m) à cette équation. Il est alors clair que m^3 est impair, donc m l'est aussi.

On a donc :

$2^n = m^3 - 1$

$2^n = (m-1)(m^2 + m + 1)$

Il existe donc des entiers naturels s et t, inférieurs ou égaux à n, tels que :

$$\begin{cases} m-1 = 2^s \\ m^2+m+1 = 2^t \end{cases}$$

Remarquons qu'on ne peut pas avoir $s = 0$ (m vaudrait 2 d'après la première équation… mais la seconde ne serait pas vérifiée…), ni $t = 0$ (m vaudrait 0 ou –1 d'après la seconde équation… impossible d'après la première…)

Par conséquent, $(m-1)^2 = m^2 - 2m + 1 = 2^{2s}$.

On en déduit que :

$$(m^2+m+1) - (m^2-2m+1) = 2^t - 2^{2s}$$

$$3m = 2^t - 2^{2s}$$

Le second membre est bien un nombre pair car t et s sont non nuls.
Or, comme m est impair, $3m$ l'est aussi ; il ne peut pas être égal à un nombre pair. L'équation proposée n'a donc pas de solutions.

43. ■ Soit (a,b) un couple solution. Posons $S = a + b$ et $P = a \times b$.
On a alors :

$$\frac{S}{S^2-2P} = \frac{6}{37} \text{ soit } 37S = 6(S^2-2P) \text{ soit } 12P = S(6S-37).$$

En conséquence, 12 divise $S(6S – 37)$.
Remarquons que ni 2 ni 3 ne peuvent diviser $6S – 37$ (sinon ils diviseraient 37).
En d'autres termes, $6S – 37$ ne possède ni le 2 ni le 3 dans sa décomposition en facteurs premiers.
Comme $S(6S – 37)$ est un multiple de 12, c'est nécessairement S est un multiple de 12.
Il existe donc un entier relatif k tel que $S = 12k$.
On en déduit :

$$P = k(72k-37)$$

a et b sont donc solutions de l'équation du second degré :

$$X^2 - 12kX + 72k^2 - 37k = 0.$$

Le discriminant réduit de cette équation est :

$$\delta = 36k^2 - (72k^2 - 37k) = 37k - 36k^2.$$

Comme l'équation admet par hypothèse des solutions, c'est que ce discriminant est > 0.
Donc k est situé entre les racines, qui sont 0 et 37/36 : les deux seules valeurs possibles de k sont donc 0 ou 1.
$k = 0$ conduit à $S = 0$, ce qui est impossible car alors 6/37 serait nul !
$k = 1$ donne $\delta = 1$, donc les solutions de l'équation sont $a = 7$ et $b = 5$ (on rappelle que $a \quad b$)

Réciproquement, on peut vérifier que $\frac{7+5}{7^2+5^2} = \frac{6}{37}$.

Division euclidienne

44. ■ Il est clair que $100^{100} = 13q + 2 \times 13 + 9$ soit $100^{100} = 13(q + 2) + 9$.
Comme $0 \leqslant 9 < 13$, cette dernière écriture est bien celle de la division euclidienne.
Ce résultat peut se retrouver avec la calculatrice et mod… Mieux encore, avec ses neurones, en remarquant que 13 est un nombre premier, donc le petit théorème de Fermat permet de prouver que :

$$100^{12} \equiv 1 \pmod{13} \text{ donc } (100^{12})^9 = 100^{96} \equiv 1 \pmod{13}.$$

Par conséquent,

$$100^{100} = 100^{96} \times 100^4 \equiv 100^4 \pmod{13}.$$

D'autre part, $100 \equiv –4$ donc $100^2 \equiv 16 \equiv 3$ et $100^4 \equiv 9$ (mod 13).
On retrouve le fait que $100^{100} = 13q + 9$.

45. ■ 1) Il est clair que $n^2 + n + 1 = n(n+1) + 1$. On a bien $0 \leqslant 1 < n + 1$ car n est un entier non nul. Le quotient est donc n et le reste 1.
2) On peut écrire $n^2 + n + 1 = (n-1)(n+2) + 3$ (c'est ce que suggère la division euclidienne de $n^2 + n + 1$ par $n + 2$).
On a donc envie d'écrire que le reste dans la division de $n^2 + n + 1$ par $n + 2$ est 3… c'est bien le cas si $3 < n + 2$ c'est-à-dire si $n > 1$. le quotient est alors $n – 1$.

Si $n = 1$, il s'agit d'effectuer la division euclidienne de 3 par 3 : le quotient est 1 et le reste 0.
3) On a $2^n - 1 = 2 \times 2^{n-1} - 1 = 2^{n-1} + 2^{n-1} - 1$. Le quotient est 1, le reste de $2^n - 1$ et on a bien 0 ℂ $2^{n-1} - 1 < 2^{n-1}$ pour n entier naturel 1.

46. ■ 1) x peut donc s'écrire $8k$, $8k \pm 1$, $8k \pm 2$, $8k \pm 3$, $8k + 4$, avec k entier relatif quelconque.
Dans le premier cas, $x^2 = 64k$ et le reste dans la division euclidienne de x^2 par 8 est 0.
Dans le deuxième cas, on a $x^2 = 64k^2 \pm 16k + 1$ et il est clair que le reste dans la division euclidienne de x^2 par 8 est alors 1.
Dans le troisième cas, on a $x^2 = 64k^2 \pm 48k + 9 = 64k^2 \pm 48k + 8 + 1$ et le reste est alors 1. Dans le dernier cas, on a $x^2 = 64k^2 \pm 64k + 16$ et le reste est 0.
b) Dans ce cas, cela correspond à $x = 8k \pm 1$ ou $x = 8k \pm 3$, et on constate que le reste vaut toujours 1.
Autrement dit un nombre impair est toujours congru à 1 modulo 8, et si un nombre a son carré congru à 1 modulo 8 il est nécessairement impair.
2) a) Soit (x, y) un couple d'entiers solution de cette équation. Alors, $x^2 \equiv 1$ (mod 8)… ce qui prouve que x est nécessairement un nombre impair.
Posons donc $x = 2k + 1$. En remplaçant dans l'équation, il vient :

$$(2k+1)^2 = 8y + 1 \text{ soit } 4k^2 + 4k + 1 = 8y + 1 \text{ d'où } 4k(k+1) = 8y.$$

On en déduit que $y = \dfrac{k(k+1)}{2}$ (le produit de deux entiers consécutifs est toujours pair, donc y est bien un entier).

On a donc $(x,y) = \left(2k+1, \dfrac{k(k+1)}{2}\right)$.

Réciproquement, on peut montrer que ces solutions conviennent effectivement.
b) Une solution de l'équation précédente est donc un point à coordonnées entières de la parabole $(\mathcal{P})$ d'équation $y = \dfrac{x^2 - 1}{8}$. Il y a donc autant de solutions que de valeurs de k soit une infinité. Exemples de points : $A(1,0)$, $B(3,1)$, etc.

47. ■ 1) Une étude à la calculatrice laisse penser que 2^{6n} est congru à 1 modulo 9. C'est immédiat car $2^{6n} - 1 = (2^6)^n - 1$ est divisible par $2^6 - 1 = 64 - 1 = 63$. C'est donc en particulier un multiple de 9.
$2^4 = 16 \equiv -3$ (mod 19), donc $2^8 \equiv 9$ (mod 19) et $2^{16} \equiv 81 \equiv 5$ (mod 19).
De proche en proche, $2^{17} \equiv 10$ (mod 19) et 2^18 ≡ 20 ≡ 1 (mod 19).
Ce qu'on aurait pu directement écrire d'après le petit théorème de Fermat puisque 19 est un nombre premier…
2) On sait qu'il existe un entier relatif k tel que $2^{6n} = 9k + 1$. Donc :

$$2^{6n+2} = 2^{6n} \times 2^2 = 4(9k+1) = 36k + 4.$$

Par conséquent :

$$2^{2^{6n+2}} = 2^{36k+4} = \left(2^{18}\right)^{2k} \times 2^4 \equiv 2^4 \equiv -3 \pmod{19}$$

ce qui prouve bien que $2^{2^{6n+2}} + 3$ est un multiple de 19 pour tout entier naturel n.

48. ■ Montre que $A_{n+7} - A_n$ est un multiple de 7… il suffit de l'écrire :

$$A_{n+7} - A_n = (n+7)^2 - (n+7) + 1 - n^2 + n - 1 = n^2 + 14n + 49 - n - 7 + 1 - n^2 + n - 1$$
$$= 14n + 42$$

pour constater que c'est bien un multiple de 7. De proche en proche on peut démontrer que pour tout entier relatif k :

$$A_n, A_{n+7}, A_{n+2\times7}, \ldots, A_{n+k\times7}$$

ont même reste dans la division par 7.
Il suffit de regarder ce qui se passe pour les entiers de 0 à 6 :

$A_0 = 0^2 - 0 + 1 = 1$ a pour reste 1 dans la division par 7 et les A_{7k} aussi ;
$A_1 = 1^2 - 1 + 1 = 1$ a aussi pour reste 1 dans la division par 7 et les A_{7k+1} aussi ;
$A_2 = 2^2 - 2 + 1 = 3$ a pour reste 3 dans la division par 7 et les A_{7k+2} aussi ;
$A_3 = 3^2 - 3 + 1 = 7$ a pour reste 0 dans la division par 7 et les A_{7k+3} aussi ;
$A_4 = 4^2 - 4 + 1 = 6$ a pour reste 6 dans la division par 7 et les A_{7k+4} aussi ;

$A_5 = 5^2 - 5 + 1 = 21$ a pour reste 0 dans la division par 7 et les A_{7k+5} aussi ;

$A_6 = 6^2 - 6 + 1 = 31$ a pour reste 3 dans la division par 7 et les A_{7k+6} aussi.

Les A_n qui sont divisibles par 7 sont de la forme A_{7k+3} et A_{7k+5}.

2008 est de la forme $7k + 6$, donc le reste demandé est 3…

123456789 est de la forme $7k + 1$ donc le reste demandé est 1.