Liaison Lycée-Enseignement supérieur
Compléments de cours sous forme de problèmes
IREM 2015/2016

Damien Achard, Aubry Colombet

Baptiste Cordeil, Jean-Étienne Rombaldi

10 juin 2016

Table des matières

1

Rapport d'activités

1.1 Présentation

L'objectif principal de ce travail est de montrer aux élèves qui se destinent à des études scientifiques dans le supérieur les exigences mathématiques que l'on attendra d'eux l'année qui suit leur bac.

Nous présentons deux problèmes qui utilisent des notions à la marge du programme de terminale scientifique. L'un tournant autour du théorème de Fermat et des nombres de Carmichaël, l'autre autour du théorème de Rolle et quelques applications.

Nous avons voulu insister sur l'idée légitime qu'en mathématiques on travaille à partir d'axiomes, définitions et théorèmes, le tout avec le maximum de rigueur. Ces exigences de précision et de rigueur sont parfois difficiles à respecter au vu des notions qui apparaissent dans les programmes actuels : par exemple, il est intéressant de démontrer le résultat essentiel en analyse réelle qui lie les variations d'une fonction dérivable au signe de sa dérivée.

Ce groupe de travail a été créé sur proposition de Christine Kazantsev qui nous a demandé de solliciter davantage les élèves de terminale scientifique en leur présentant des exercices plus exigeants que ceux du baccalauréat.

1.2 Dichotomie et théorème de Rolle

Nous sommes partis du constat que dans plusieurs démonstrations du programme de terminale scientifique, nous utilisons le fait qu'une fonction de dérivée nulle sur un intervalle est une fonction constante. Ce résultat semble très naturel car sa réciproque est évidente et les élèves n'ont pas conscience de la difficulté que revêt une telle démonstration. L'objectif de ce problème est donc de compléter les connaissances de terminale pour pallier en particulier ce manque.

Pour ce problème, nous utilisons l'axiome sur les suites croissantes majorées pour démontrer le théorème des valeurs intermédiaires admis en terminale scientifique. Puis, nous démontrons le théorème de Rolle duquel découle le théorème des accroissements finis. Nous pouvons alors démontrer en toute rigueur le théorème qui relie les variations d'une fonction dérivable au signe de sa dérivée.

Ce problème a été traité en classe, guidé par le professeur, en quatre séances d'une heure.

Lors de la première séance, nous avons démontré le théorème des valeurs intermédiaires. Lorsque nous demandons aux élèves de citer le théorème, ils énoncent tous une version ayant comme hypothèse la stricte monotonie de la fonction pour aboutir à l'existence et l'unicité d'une solution de l'équation $f(x) = 0$.

Aucun élève n'a retenu la version standard sans hypothèse de monotonie. Ceci est dû au fait que nous utilisons peu cette version dans les exercices abordés en terminale scientifique. Ce problème est l'occasion de clarifier ce point. Dans la question 2-a), les élèves pensent à la démonstration par récurrence mais ils ont du mal à la rédiger. Cependant 4 élèves proposent une rédaction correcte. Dans la question 2-b), certains élèves reconnaissent une suite géométrique de raison $\frac{1}{2}$ et concluent. Dans la question 2-c), certains élèves répondent facilement. Après explications par le professeur, tous reconnaissent un raisonnement classique utilisé régulièrement en terminale scientifique. La question 2-d) est expliquée rapidement par le professeur car le temps de la séance est écoulé.

Lors de la deuxième séance, le théorème de Rolle est abordé jusqu'à la question 2-c). Dans la question 1-a), plusieurs élèves ne se contentent pas d'une courbe avec un seul changement de variation et envisagent des courbes plus élaborées (comme par exemple des courbes de fonctions périodiques). Une bonne partie des élèves, construisent correctement α_1 et β_1. Aucun élève n'envisage qu'une fonction ne soit pas dérivable en certains

points de l'intervalle. Dans la question 1-b), une discussion s'installe entre les élèves et le professeur. Les élèves proposent leurs conjectures :

- la longueur des intervalles tend vers 0
- les suites (α_n) et (β_n) tendent vers la même limite
- on s'approche d'un extremum local
- on s'approche d'un point où la dérivée est nulle

Ainsi, les élèves parviennent à pressentir le théorème de Rolle. Dans la question 2-a), les élèves pensent à utiliser le théorème des valeurs intermédiaires mais se confrontent à plusieurs problèmes. Certains cherchent le sens de variation de la fonction alors qu'il n'est pas utile ici. Peu comprennent l'hypothèse à vérifier pour appliquer ce théorème : $g(a)g(\frac{a+b}{2}) \leq 0$. Enfin, certains élèves parviennent à la solution sans aide. La question 2-c) difficile est admise car la séance se termine.

Au début de la troisième séance, le professeur explique oralement la question 2-c), étant donnée sa difficulté.

Pour l'itération du procédé, le professeur demande aux élèves : « comment feriez-vous ? », réponse : « c'est le même principe» et « on ferait une récurrence», ce qui suffit.

La question 4. est correctement faite par un élève assez rapidement.

Pour la question 5. il y a quelques erreurs intéressantes, par exemple « $\ell - \alpha_n \neq 0$ existe car une limite n'est jamais atteinte ». Aucun élève ne sait résoudre sans aide. En précisant que la question 2-c) est importante, un élève comprend immédiatement que l'intervalle ouvert de la question 2-c) entraîne la stricte monotonie des suites. C'est l'occasion pour le professeur de montrer que pour une suite convergente strictement monotone la limite n'est jamais atteinte.

Pour 5-b), trois élèves pensent au taux de variations.

La conclusion en 5-c) n'est pas évidente pour les élèves, il faut leur donner l'indication sur l'importance du signe des $u_n v_n$.

Pour la quatrième et dernière séance on s'est intéressé à l'application du théorème de Rolle au théorème des accroissements finis et à son utilité pour l'étude des variations des fonctions dérivables.

Avec l'aide du professeur, cette séance s'est déroulée de façon efficace, faisant abstraction de quelques maladresses.

Le fait que les quatre séances étaient clairsemées a été une difficulté (il faut se remémorer le problème).

1.3 Sur le théorème de Fermat

La première question présente une démonstration élémentaire du théorème de Fermat en exploitant tout simplement le fait que, pour tout entier relatif a, le groupe cyclique $\frac{\mathbb{Z}}{p\mathbb{Z}}$ est engendré par $\overline{a}$ si, et seulement si, a est premier avec p.

Dans ce cas, on a :

$$\frac{\mathbb{Z}}{p\mathbb{Z}} = \{\overline{r_0}, \overline{r_1}, \cdots, \overline{r_{p-1}}\}$$

où, pour k compris entre 0 et $p-1$, r_k est le reste dans la division euclidienne de ka par p, ce qui permet de vérifier que $(p-1)!a^{p-1} \equiv r_1 r_2 \cdots r_{p-1} \pmod{p}$, puis que $a^{p-1} \equiv 1 \ (p)$.

Avec les questions 3. et 4. on explique comment construire des exercices qui consistent à trouver le reste dans la division euclidienne par un nombre premier p d'un entier de la forme a^b. Utilisant le théorème de Fermat, c'est un jeu d'enfant.

Avec les questions 4. et 5. on s'intéresse à un test de non primalité et un test de primalité.

Pour des élèves motivés, on pourrait introduire la fonction indicatrice d'Euler φ et sur la base du théorème qui suit construire un problème (toujours avec les restrictions des programmes actuels). Ce théorème donne plusieurs caractérisations des nombres premiers.

Théorème 1.1 *Pour tout entier $n \geq 2$, les assertions suivantes sont équivalentes :*

1. *n est premier ;*
2. *pour tout entier naturel non nul α, on a $\varphi(n^\alpha) = (n-1)\, n^{\alpha-1}$, ;*
3. *$\varphi(n) = n-1$;*
4. *n est premier avec tout entier compris entre 1 et $n-1$;*
5. *$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un corps ;*
6. *$\frac{\mathbb{Z}}{n\mathbb{Z}}$ est intègre ;*

7. $(n-1)! \equiv -1 \pmod{n}$ *(théorème de Wilson)* ;
8. $(n-2)! \equiv 1 \pmod{n}$;
9. *pour tout* k *compris entre* 1 *et* n, *on a* $(n-k)!\,(k-1)! \equiv (-1)^k \pmod{n}$;
10. $n = 2$ *ou* n *est impair et* $\left(\left(\frac{n-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{n+1}{2}} \pmod{n}$;
11. *pour tout entier* k *compris entre* 1 *et* $n-1$, *on a* $\binom{n}{k} \equiv 0 \pmod{n}$;
12. *pour tout entier* k *compris entre* 1 *et* $n-1$, *on a* $\binom{n}{k} \equiv 0 \pmod{n}$ *et* $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$;
13. *il existe un entier relatif* a *premier avec* n *tel que* $(X+\overline{a})^n = X^n + \overline{a}$ *dans* $\mathbb{Z}_n[X]$.

On s'intéresse ensuite à une « réciproque » du théorème de Fermat.
Cette « réciproque » est fausse comme le montre l'exemple suivant.

La décomposition en facteurs premiers de $n = 561$ est $n = 3 \cdot 11 \cdot 17 = \prod_{k=1}^{3} p_k$.

Dire que l'entier a est premier avec 561 équivaut à dire qu'il est premier avec chaque p_k et le théorème de Fermat nous dit que $a^{p_k-1} \equiv 1 \pmod{p_k}$ et en remarquant que 560 est divisible par chaque $p_k - 1$ ($560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$), on en déduit que $a^{560} \equiv 1 \pmod{p_k}$ pour $k = 1, 2, 3$.

L'entier $a^{560} - 1$ est donc multiple de chaque p_k et en conséquence de leur ppcm qui vaut $\prod_{k=1}^{3} p_k = n$, soit $a^{560} \equiv 1 \pmod{561}$.
En conclusion $n = 561$ est tel que $a^{n-1} \equiv 1 \pmod{n}$ pour tout a premier avec n et n'est pas premier.
Cela nous conduit à la définition des nombres de Carmichaël.
On propose de montrer une partie du théorème suivant.

Théorème 1.2 (Korselt) *Soit* $n \geq 3$ *un entier. Les assertions suivantes sont équivalentes :*

1. *il existe un entier* $r \geq 3$ *et des nombres premiers* $3 \leq p_1 < \cdots < p_r$ *tels que* $n = \prod_{j=1}^{r} p_j$ *et, pour tout indice* j *compris entre* 1 *et* r, $p_j - 1$ *divise* $n-1$;
2. n *est non premier et :*
$$\forall x \in \frac{\mathbb{Z}}{n\mathbb{Z}},\ x^n = x$$
3. n *est un nombre de Carmichaël.*

Nous faisons remarquer aux élèves que c'est en 1994 qu'il a été montré qu'il existe une infinité de nombres de Carmichaël (Alford, Granville et Pomerance).
L'expérimentation avec quelques élèves a été intéressante. Ce problème a été donné en devoir libre aux élèves de spécialité mathématique. Peu d'élèves l'ont rendu. Ce problème étant difficile, il eut été plus efficace de le traiter en classe avec le professeur comme guide. Mais c'est faute de temps et de moyens (accompagnement personnalisé, etc...) que cela n'a pas été fait.
Les élèves ayant rendu une copie ont traité une bonne partie du problème et le résultat est relativement satisfaisant malgré quelques erreurs.
De manière générale, les problèmes d'arithmétique sont déstabilisants pour les élèves du fait que les raisonnements effectués ne sont pas habituels pour eux. De plus, nous sommes limités aux élèves de spécialité et la notion de nombre premier est plutôt abordée en fin d'année.

1.4 Conclusions

Comme l'année précédente, cette expérience a semblé enrichissante pour les élèves motivés. Ils ont pu se confronter à de réelles difficultés mais cela ne les a pas découragés. De notre point de vue, il est clair que ce type d'expérience est à généraliser.
On peut signaler que la R. M. S. (Revue de la filière Mathématique : www.rms-math.com) publie des articles et notes de cours portant sur des questions liées à l'enseignement secondaire avec la rubrique « Du côté des élèves de terminale scientifique ». Il serait bon d'inciter les élèves motivés à consulter cette revue (disponible dans quelques Lycées).
Par exemple, dans le numéro 3 d'avril 2016, on peut trouver l'énoncé suivant.
Questions proposées aux élèves de terminale scientifique.

1. Soit $n \in \mathbb{N}^*$. On dit que n est un nombre parfait si la somme de ses diviseurs positifs est $2n$.
   Déterminer l'ensemble des nombres parfaits n tels que $n-1$ et $n+1$ sont tous deux premiers.
2. Soient x, y deux nombres réels distincts strictement positifs.
   Démontrer l'inégalité :
   $$\sqrt{x^2+y^2} + \sqrt{xy} > \frac{x+y}{2} + \frac{x-y}{\ln(x) - \ln(y)}$$
3. Soient (Γ) un cercle de l'espace et $ABCD$ un quadrilatère convexe inscrit dans (Γ). Soit S un point de l'axe de (Γ) (c'est-à-dire de la perpendiculaire au plan de (Γ) passant par son centre). Pour $M \in \{A, B, C, D\}$, on note N et P les sommets de $ABCD$ voisins de M et on appelle angle dièdre d'arête (SM) l'angle dièdre des plans (SMN) et (SMP).
   Démontrer que la somme des angles dièdres d'arêtes (SA) et (SC) est égale à la somme des angles dièdres d'arêtes (SB) et (SD).
4. Soit $(X_n)_{n\in\mathbb{N}^*}$ une suite de variables aléatoires continues de même loi, mutuellement indépendantes. On définit la variable aléatoire Y en fonction de cette suite de la façon suivante :
   S'il existe $n \in \mathbb{N}^*$ tel que $X_1 \leq \cdots \leq X_n$ et $X_{n+1} < X_n$, l'entier n est unique et Y prend la valeur $n+1$.
   Dans le cas contraire, Y prend la valeur $+\infty$.
   Déterminer la loi de Y puis calculer son espérance.

Problème : l'inégalité de Fisher

$\cdots$ (voir le numéro correspondant de la R. M. S.).

2

Annexes

2.1 Problème 1 : Dichotomie et théorème de Rolle

– I – Le théorème des valeurs intermédiaires

1. Énoncer le théorème des valeurs intermédiaires.
2. *On propose une démonstration du théorème des valeurs intermédiaires.*
   Soient $a < b$ deux réels et $f : [a, b] \to \mathbb{R}$ une fonction continue telle $f(a) < 0 < f(b)$.
   On construit, par récurrence, les suites réelles $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ de la manière suivante :
   $a_0 = a$, $b_0 = b$;
   pour tout $n \geq 0$:
   $$\begin{cases} \text{si } f\left(\dfrac{a_n + b_n}{2}\right) > 0, \text{ alors } a_{n+1} = a_n \text{ et } b_{n+1} = \dfrac{a_n + b_n}{2} \\ \text{sinon } a_{n+1} = \dfrac{a_n + b_n}{2} \text{ et } b_{n+1} = b_n \end{cases}$$
   (a) Montrer que, pour tout entier $n \geq 0$, on a :
   $$a \leq a_n \leq a_{n+1} \leq b_{n+1} \leq b_n \leq b$$
   (b) Montrer que la suite $(b_n - a_n)_{n\in\mathbb{N}}$ converge vers 0.
   (c) Montrer que les suites $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$, convergent vers une même limite $\ell \in [a, b]$.
   (d) Montrer que $f(\ell) = 0$.

– II – Le théorème de Rolle

Soient $a < b$ deux réels et $f : [a, b] \to \mathbb{R}$ une fonction continue telle $f(a) = f(b)$.

1. *Pour cette question, un logiciel de géométrie dynamique peut être utile.*
   (a) En dessinant la courbe représentative d'une telle fonction f, placer approximativement sur l'axe des abscisses deux réels $\alpha_1 < \beta_1$ dans $]a, b[$ tels que :
   $$\begin{cases} \beta_1 - \alpha_1 \leq \dfrac{b-a}{2} \\ f(\alpha_1) = f(\beta_1) \end{cases} \tag{2.1}$$
   (b) En itérant ce procédé, que peut-on conjecturer ?
2. *L'objectif de cette question est de prouver l'existence d'un couple de réels (α_1, β_1) vérifiant (2.1) avec la condition $a < \alpha_1 < \beta_1 < b$.*
   (a) En désignant par g la fonction définie par :
   $$\forall x \in \left[a, \frac{a+b}{2}\right],\ g(x) = f\left(x + \frac{b-a}{2}\right) - f(x)$$
   montrer qu'il existe un réel $\alpha \in \left[a, \dfrac{a+b}{2}\right]$ tel que $g(\alpha) = 0$.

(b) Montrer qu'il existe un réel $\beta \in \left[\dfrac{a+b}{2}, b\right]$ tel que $\beta - \alpha = \dfrac{b-a}{2}$ et $f(\beta) = f(\alpha)$.

(c) Déduire de ce qui précède l'existence de deux réels $\alpha_1 < \beta_1$ dans $]a,b[$ tels que :

$$\begin{cases} \beta_1 - \alpha_1 \leq \dfrac{b-a}{2} \\ f(\alpha_1) = f(\beta_1) \end{cases}$$

Il est conseillé de faire des dessins.

3. *Itération du procédé.*
Justifier l'existence de deux suites réelles $(\alpha_n)_{n\in\mathbb{N}}$ et $(\beta_n)_{n\in\mathbb{N}}$ telles que :

$$\begin{cases} \alpha_0 = a,\ \beta_0 = b \\ \forall n \in \mathbb{N}^*, \begin{cases} [\alpha_n, \beta_n] \subset]\alpha_{n-1}, \beta_{n-1}[\\ \beta_n - \alpha_n \leq \dfrac{\beta_{n-1} - \alpha_{n-1}}{2} \\ f(\alpha_n) = f(\beta_n) \end{cases} \end{cases}$$

4. *Convergence du procédé.*
Montrer que les suites $(\alpha_n)_{n\in\mathbb{N}}$ et $(\beta_n)_{n\in\mathbb{N}}$ convergent vers une même limite $\ell \in]a,b[$.

5. On suppose pour cette question que la fonction f est dérivable sur l'intervalle $]a,b[$.
On définit les suites $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ par :

$$\forall n \in \mathbb{N}^*, \begin{cases} u_n = \dfrac{f(\ell) - f(\alpha_n)}{\ell - \alpha_n} \\ v_n = \dfrac{f(\beta_n) - f(\ell)}{\beta_n - \ell} \end{cases}$$

(a) Justifier l'existence de $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$.

(b) Montrer que :

$$\lim_{n\to+\infty} u_n = \lim_{n\to+\infty} v_n = f'(\ell)$$

(c) Montrer que $f'(\ell) = 0$.
En définitive, nous avons montré le :
Théorème (Rolle) : Si f est une fonction à valeurs réelles définie sur un segment $[a,b]$ non réduit à un point, continue sur cet intervalle et dérivable sur l'intervalle ouvert $]a,b[$ avec $f(a) = f(b)$, il existe alors un réel $\ell \in]a,b[$ tel que $f'(\ell) = 0$.

– III – Applications

Soient $a < b$ deux réels et f une fonction numérique continue sur $[a,b]$ et dérivable sur $]a,b[$.

1.

(a) Déterminer l'expression réduite de la fonction affine h qui coïncide avec f en a et b.

(b) En appliquant le théorème de Rolle à une fonction judicieusement choisie, montrer qu'il existe un réel $c \in]a,b[$ telle que :

$$f(b) - f(a) = (b-a) f'(c)$$

Ce résultat est le *théorème des accroissements finis*.

2. Montrer (enfin) les théorèmes admis en classe de première :

(a) La fonction f est croissante sur $[a,b]$ si, et seulement si, sa dérivée f' est positive sur $]a,b[$.

(b) La fonction f est constante sur $[a,b]$ si, et seulement si, sa dérivée f' est nulle sur $]a,b[$.

(c) Si f' est strictement positive sur $]a,b[$, la fonction f est alors strictement croissante sur $[a,b]$.

(d) Qu'en est-il de la réciproque du résultat précédent ?

2.2 Problème 2 : Sur le théorème de Fermat

Pour tout entier naturel n, la factorielle de n est l'entier $n!$ défini par $0! = 1$ et pour $n > 1$, $n! = n \cdot (n-1) \cdot \cdots \cdot 1$.
Soient n un entier naturel et a, b deux entiers relatifs.
On dit que a est congru à b modulo n si, et seulement si, n divise $b - a$, ce qui se note :

$$a \equiv b \ (n)$$

On rappelle le théorème de division euclidienne.
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si les seuls diviseurs positifs de p sont 1 et p.

On rappelle le théorème de Gauss : soient a, b, c des entiers relatifs non nuls, si a divise bc et a est premier avec b alors a divise c.

On rappelle le lemme d'Euclide : soient p un nombre premier et r un entier naturel supérieur ou égal à 2, si p divise le produit $n_1 n_2 \cdots n_r$ de r entiers naturels non nuls, alors p divise l'un des n_k.

1. **Une démonstration du théorème de Fermat.**
   Soit $p \geq 2$ un nombre premier.

   (a) Soit a un entier relatif premier avec p.
   Pour tout entier k compris entre 1 et $p-1$, on note r_k le reste dans la division euclidienne de ka par p.
   Montrer que les r_k sont deux à deux distincts et compris entre 1 et $p-1$.

   (b) En utilisant les notations de la question précédente, montrer que pour tout entier relatif a premier avec p, on a :
   $$(p-1)!\ a^{p-1} \equiv r_1 r_2 \cdots r_{p-1} \ (p)$$

   (c) En déduire que, pour tout entier relatif a premier avec p, on a :
   $$a^{p-1} \equiv 1 \ (p)$$
   (théorème de Fermat).

2. Soit n un nombre premier. Montrer que les assertions suivantes sont équivalentes :
   (i) pour tout entier relatif a premier avec n, on a : $a^{n-1} \equiv 1 \ (n)$
   (ii) pour tout entier relatif a, on a : $a^n \equiv a \ (n)$

3. (a) Calculer le reste dans la division euclidienne de 3045^{2018} par 13.
   (b) Calculer le reste dans la division euclidienne de 3044^{2018} par 13.

4. De manière plus générale, comment simplifier le calcul du reste dans la division euclidienne par un nombre premier p d'un entier de la forme a^b, où a, b sont des entiers naturels plus grands que p ?

5. **Un test de non primalité.**
   Comment utiliser le théorème de Fermat comme test de non primalité d'un entier $n \geq 3$?

6. Soit $n \geq 2$ un entier tel que $a^{n-1} \equiv 1 \ (n)$ pour tout entier a compris entre 2 et $n-1$.
   En utilisant le théorème de Bézout, montrer que n est premier.

   Définition : On appelle nombre de Carmichaël tout entier $n \geq 3$ non premier tel que pour tout entier relatif a premier avec n, on a $a^{n-1} \equiv 1 \ (n)$ (propriété de Fermat).

7. Montrer qu'un nombre de Carmichaël est impair.

8. 561 **est un nombre de Carmichaël.**

   (a) Donner la décomposition en facteurs premiers de l'entier $n = 561$ (sans utiliser de calculatrice, bien sûr).

(b) Vérifier que 560 est divisible par 2, par 10 et par 16.

Soit $a \in \mathbb{Z}$ premier avec 561.

(c) Montrer que a est premier avec chaque entier $p_1 = 3$, $p_2 = 11$ et $p_3 = 17$.

(d) Montrer que, pour $k = 1, 2, 3$, p_k divise $a^{p_k - 1} - 1$.

(e) Montrer que, pour $k = 1, 2, 3$, p_k divise $a^{560} - 1$.

(f) En déduire que 561 divise $a^{560} - 1$ et conclure.

9. Soit $n \geq 3$ un entier pour lequel il existe un entier $r \geq 2$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n - 1$.

   (a) Dans cette question nous allons démontrer que nécessairement $r \geq 3$.
   On suppose que $r = 2$, c'est-à-dire que $n = p_1 p_2$ avec $p_1 < p_2$ premiers tels que $p_1 - 1$ et $p_2 - 1$ divisent $n - 1$.
   En effectuant la division euclidienne de $n - 1$ par $p_2 - 1$ de deux manières différentes, montrer que l'on aboutit à une contradiction et conclure.

   (b) Montrer que n un nombre de Carmichaël.

   (c) Vérifier que 1105 et 41041 sont des nombres de Carmichaël.

10. Soit $a \in \mathbb{N}^*$ tel que les entiers $p_1 = 6a + 1$, $p_2 = 12a + 1$ et $p_3 = 18a + 1$ soient premiers.
Montrer que $n = p_1 p_2 p_3 = p_1 (2p_1 - 1) (3p_1 - 2)$ est un nombre de Carmichaël.
Donner des exemples.
On peut montrer le résultat suivant, ce qui est plus difficile.

Théorème 2.1 (Korselt) *Soit $n \geq 3$ un entier. Les propriétés suivantes sont équivalentes :*

1. *il existe un entier $r \geq 3$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n - 1$;*
2. *n est non premier et :*
$$\forall a \in \mathbb{Z},\ a^n \equiv a\ (n)$$
3. *n est un nombre de Carmichaël.*