Extraction mentale de racines n-ièmes.

Michel Lafond(*)

Un spectacle que les médias aiment bien est la présentation d'un calculateur prodige capable d'exécuter des prouesses mathématiques à la rapidité de l'éclair. Nous ne parlerons ici que de l'extraction mentale de racines n-ièmes.
Le but de cet article est d'une part de montrer que les problèmes les plus difficiles ne sont pas toujours ceux qu'on croit (c'est ce qu'on appelle le paradoxe de la fausse difficulté) et d'autre part d'exposer quelques-uns des algorithmes utilisés pour extraire mentalement des racines n-ièmes.
Les mathématiques utilisées ici sont de niveau Terminale S en spécialité.

I. Le paradoxe de la fausse difficulté.

Un article de Jean Paul Delahaye

(https://interstices.info/jcms/c_33536/un-calcul-revolutionnaire)

explique que : extraire mentalement
– la racine carrée d'un nombre de 80 chiffres est **très difficile** (jamais encore réalisé).
– la racine 13-ème d'un nombre de 100 chiffres est **difficile** mais pas extraordinaire (souvent réalisé).
– la racine 1789-ème d'un nombre de 7000 chiffres est **enfantin** (tout le monde peut le faire en deux secondes, même sans savoir ce qu'est une racine !).

1. Le protocole de l'expérience.

Avant toute chose il faut préciser les conditions dans lesquelles se déroule ce genre d'expérience.
Le calculateur et les témoins savent que le calculateur aura à extraire la racine ω-ème d'un entier N qui est la puissance ω-ème exacte d'un entier n inconnu (mais non multiple de 10) choisi au dernier moment, disons au hasard par ordinateur.
De plus le nombre de chiffres de $N = n^{\omega}$ est fixé au préalable (disons k) et par conséquent le calculateur a pu préparer des algorithmes spécifiques aux valeurs ω et k des paramètres et s'entraîner suffisamment.
Le calculateur doit effectuer le calcul mentalement sans aide humaine ou matérielle.
Au début de l'expérience, les expérimentateurs écrivent (en général sur un tableau bien visible du public) la puissance $N = n^{\omega}$, enclenchent les chronomètres, etc.

Un tel protocole rigoureux est nécessaire pour pouvoir comparer les records successifs, homologuer éventuellement les records et éviter les tricheries. Le fait de fixer au préalable ω et k permet aux différents compétiteurs de se mesurer sur des problèmes de difficultés comparables.

Nous noterons dans la suite :

(*) mlafond001@yahoo.fr

$\mathbf{E}_{\omega}$ l'expérience consistant à extraire la racine ω-ème d'un entier donné ; $\mathbf{E}_{\omega}(k)$ l'expérience consistant à extraire la racine ω-ème d'un entier donné de k chiffres, k fixé.

2. Une mesure de la difficulté.

Un moyen simple de mesurer la difficulté de l'expérience $E_{\omega}(k)$ est de compter le nombre de réponses *a priori* possibles à la question posée.
Ainsi, dans l'expérience $E_{13}(100)$, il y a environ 8 000 000 réponses possibles.
Il est logique de mesurer la ***difficulté*** par le ***logarithme décimal du nombre de réponses*** *a priori* possibles. Ainsi, la difficulté (apparente) de $E_{13}(100)$ est $\log 8\,000\,000 \approx 7$.
C'est un bon exercice en spécialité de Terminale S de démontrer que la difficulté de $E_{1789}(7000)$ mentionnée au début est à peine égale à 1.
La difficulté de $E_2(80)$ consistant à trouver la racine carrée d'un nombre de 80 chiffres est d'environ $\log\left(10^{40}-10^{39}\right)\approx 40$ puisqu'on attend un nombre de 40 chiffres. C'est énorme.
Bien entendu, si on vous demande la racine carrée n du carré parfait à 80 chiffres
N = 13838994610814461742892747457162664969216818541973244800831847988807810541895936,
vous devinerez que n se termine par 4 ou 6 (mais lequel des deux ?).
Si vous calculez bien, ou si, comme tous les calculateurs prodiges, vous connaissez par cœur $37^2 = 1369$ et $38^2 = 1444$, vous verrez même instantanément que n commence par 37 puisque

$$37^2\times 10^{76} < \mathrm{N} < 38^2\times 10^{76} \Rightarrow 37\times 10^{38} < n < 38\times 10^{38}$$

Mais pour le reste ?

3. On peut surestimer la difficulté du problème.

Étudions plus en détail l'expérience $E_{13}(100)$: « ***extraire la racine 13-ème d'un nombre de 100 chiffres*** ».
$N = n^{13}$ est écrit sur un tableau, les chronomètres sont enclenchés et l'expérience commence.
Le passage mental de N à n semble infaisable en quelques minutes, MAIS il n'y a que 8 chiffres à trouver puisqu'on peut démontrer que n appartient à [41246264, 49238826].
Ensuite, les deux paramètres : exposant 13, et nombre de chiffres 100 ont été astucieusement choisis pour que le résultat commence toujours par le même chiffre (ici 4) et pour que le chiffre des unités de n soit le même que celui de N.
En effet nous verrons dans le paragraphe II que pour tout entier $n, \mathrm{N} = n^{13} \equiv n \pmod{10}$
Il n'y a donc que 8 – 2 = 6 chiffres à trouver. La difficulté passe subitement à $\log\left(10^6\right) = 6$.
De manière générale, l'obtention des chiffres à trouver (4 pour $E_{13}(50)$, 8 pour $E_{13}(100)$) se fait par l'usage de plusieurs techniques mathématiques, congruences

avec le théorème chinois, tables diverses ou formules mémorisées, la pratique de nombreux trucs classiques de calcul mental et l'utilisation de plusieurs astuces de calcul numérique mises en œuvre spécialement pour ce problème, avec l'aide de l'informatique.
Nous verrons quelques-unes de ces techniques dans les paragraphes II et III.

II. Quelques résultats utiles pour la suite.

Nous nous intéressons uniquement à l'expérience E_{13} « ***extraire la racine 13-ème d'un nombre donné*** **N**, dont on sait que N est un entier de la forme $N = n^{13}$ ne se terminant pas par 0 pour des raisons évidentes.

1. Le petit théorème de Fermat : la congruence modulo 2730.

Pour tout entier n

$$N = n^{13} \equiv n \pmod{10}. \qquad (1)$$

En effet selon *le petit théorème de Fermat qui stipule que, si p est premier, pour tout entier n on a* : $n^p \equiv n \pmod{p}$; on en déduit aussitôt par récurrence que pour tout entier naturel k : $n^{k(p-1)+1} \equiv n \pmod{p}$.

On a donc que $n^{13} \equiv n \pmod{p}$, pour tout nombre premier p tel que $p - 1$ divise 12.
Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. Les nombres premiers solutions sont donc 2, 3, 5, 7, 13.
Puisque 5, 6, 7, 13 sont premiers entre eux deux à deux, et $5 \times 6 \times 7 \times 13 = 2730$, n^{13} est congru à n modulo le produit de ces nombres, c'est-à-dire 2730.
Nous noterons dans toute la suite :

$$R_k = N \pmod{k},\ r_k = n \pmod{k},$$

D'après (1), pour tout diviseur d de 2730,

$$r_d \equiv R_d \pmod{d} \qquad (2)$$

2. Le théorème des restes chinois (TRC) ; calcul de r_{30} ; R_{30} et r_{2730} ; R_{2730}

Soient p et q ***deux entiers premiers entre eux.***

Si $\begin{cases} x \equiv a \pmod{p} \\ x \equiv b \pmod{q} \end{cases}$ et si on a l'égalité de Bézout-Bachet : $pu - qv = 1$, alors :

$$x \equiv p(b-a)u + a \pmod{pq} \qquad \text{(TRC)}$$

En effet, on a

$$x \equiv p(b-a)u + a \equiv a \pmod{p}$$

et puisque

$$pu = 1 + qv \equiv 1 \pmod{q}$$

$$x \equiv p(b-a)u + a \equiv pu(b-a) + a \equiv (b-a) + a \equiv b \pmod{q}$$

Application 1. En partant de la décomposition 2730 = 91 × 30, on prend $p = 91$, $q = 30$. L'égalité de Bézout-Bachet s'écrit ici 91 − 3 × 30 = 1, donc $u = 1$, $v = 3$. Si on appelle r, a, b les restes de N par 2730, 91 et 30 respectivement, la formule TRC ci-dessus donne : $r \equiv 91(b-a) + a \pmod{2730}$, formule qui permet de calculer le reste de N par 2730 quand on a les restes par 91 et 30.
Avec les notations du 1

$$r_{2730} \equiv \mathrm{R}_{2730} \equiv \mathrm{R}_{91} + 91(\mathrm{R}_{30} - \mathrm{R}_{91}) \pmod{2730} \qquad (3)$$

Application 2. Avec 3 × 10 = 30, prenons $p = 10$ et $q = 3$, $u = 1$, $v = 3$, on obtient, comme 30 divise 2730, d'après (2) et TRC.

$$r_{30} \equiv \mathrm{R}_{30} \equiv \mathrm{R}_{10} + 10(\mathrm{R}_3 - \mathrm{R}_{10}) \pmod{30} \qquad (4)$$

R_{10} = N (mod 10) est le dernier chiffre de N.
R_3 = N (mod 3) est particulièrement simple à obtenir mentalement, puisqu'il est égal à la somme des chiffres de N, calculée modulo 3, donc en « oubliant » les chiffres 0, 3, 6, 9 ainsi que les divers « paquets » tels 75, 42, etc.

3. Deux astuces finales ; calcul de r_{91} et R_{91} ; r_{11} et R_{11}

Soit N = *abcd … uvw xyz* l'écriture décimale de N, décomposée en *tranches de 3 chiffres à partir de la droite*. Si T_i est la *i*-ème tranche, on a

$$\mathrm{N} = \ldots + \mathrm{T}_3 10^9 + \mathrm{T}_2 10^6 + \mathrm{T}_1 10^3 + \mathrm{T}_0.$$

Mais 1001 = 7 × 11 × 13 = 11 × 91 donc $1000 \equiv -1 \pmod{11}$ et $1000 \equiv -1 \pmod{91}$

Donc $\mathrm{N} \equiv \ldots - \mathrm{T}_3 + \mathrm{T}_2 - \mathrm{T}_1 + \mathrm{T}_0 \pmod{91}$ et $\pmod{11}$.

D'après (2), comme 91 divise 2730, $n \equiv \mathrm{N} \pmod{91}$. Donc $r_{91} \equiv \mathrm{R}_{91} \pmod{91}$ et :

Si N = … $\mathrm{T}_2\mathrm{T}_1\mathrm{T}_0$ est l'écriture décimale d'un entier N, décomposée en tranche de 3 chiffres à partir de la droite (la première tranche pouvant n'avoir qu'un ou deux chiffres), alors

$$r_{91} \equiv \mathrm{R}_{91} \equiv \ldots - \mathrm{T}_3 + \mathrm{T}_2 - \mathrm{T}_1 + \mathrm{T}_0 \pmod{91} \qquad (5)$$

$$\mathrm{R}_{11} \equiv \ldots - \mathrm{T}_3 + \mathrm{T}_2 - \mathrm{T}_1 + \mathrm{T}_0 \pmod{11} \qquad (5')$$

Calcul de r_{11}
Il n'y a pas r_{11} dans la formule (5′) parce que 11 ne divise pas 2730. Procédons autrement.
D'après le petit théorème de Fermat, pour tout entier n,

$$n^{10} \equiv 1 \pmod{11} \Rightarrow n^{90} \equiv 1 \pmod{11}$$

D'où $\mathrm{R}_{11}^7 \equiv \mathrm{N}^7 \equiv \left(n^{13}\right)^7 \equiv n^{91} \equiv n^{90} \times n \equiv n \equiv r_{11} \pmod{11}$

Donc R_{11} est donné par (5′) et

$$r_{11} \equiv R_{11}^7 \pmod{11} \qquad (5')$$

R_{11}^7 se calcule facilement avec $x^7 = \left(x^2 \cdot x\right)^2 \cdot x$ (les multiplications étant faites modulo 11).

III L'expérience E_{13} (50)

Nous allons, à propos de cette expérience, exploiter la propriété (1) :

$$n^{13} \equiv n \pmod{2730}.$$

Il faut trouver la racine treizième d'un nombre N de 50 chiffres dont on sait (sauf le calculateur prodige !) que c'est la puissance 13 d'un entier donné n.

On a alors $49 \leq \log(N) < 50$, donc $\frac{49}{13} \leq \log(n) < \frac{50}{13}$.

Par conséquent $3{,}76 \leq \log(n) < 3{,}85$ et ainsi $0{,}76 \leq \log\left(\frac{n}{1000}\right) < 0{,}85$.

Mais tout calculateur prodige connaît les logarithmes décimaux des premiers entiers : $\log(5) \approx 0{,}699$, $\log(6) \approx 0{,}778$, $\log(7) \approx 0{,}845$, $\log(8) \approx 0{,}903$.

Une interpolation « à vue de nez » donne $5{,}7 < \frac{n}{1000} < 7{,}2$ soit $5700 < n < 7200$; ainsi on sait déjà que n appartient à un intervalle de largeur 1500. Cela donne une difficulté de $\log(1500) \approx 3{,}2$. C'est peu.

Ainsi, si on se donne un nombre N de 50 chiffres, dont on sait qu'il est la puissance 13-ème d'un entier n, on a sur ce dernier deux informations : $\begin{cases} 5700 < n < 7200 \\ n \equiv N \pmod{2730} \end{cases}$,

qui le déterminent totalement.

Nous n'avons donc plus qu'à trouver la valeur de N modulo 2730.

(En pratique le calculateur sait qu'il doit trouver un entier n compris entre 5879 et 7017 puisque 587913 et 701713 sont les deux puissances 13-èmes minimale et maximale à 50 chiffres. Il n'a donc pas besoin des interpolations ci-dessus.)

Voyons sur un exemple : ***Trouver la racine treizième de***

N = 63848873722100055045214564683172021583939466824939.

On sait que n est congru à $r_{2730} \equiv N \pmod{2730}$ et que n est compris entre 5700 et 7200.

Modulo 91 : (Propriété 5)

63 − 848 + 873 − 722 + 100 − 55 + 45 − 214 + 564 − 683 + 172 − 21 + 583 − 939 + 466 − 824 + 939 = − 501

Donc $R_{91} \equiv -501 \equiv -501 + 6 \times 91 = 45 \pmod{91}$.

La transformation « $-501 + 6 \times 91$ » a seulement pour but de diminuer la grandeur du nombre manipulé.

Modulo 30 : (Propriété 4) $R_{30} \equiv R_{10} + 10\left(R_3 - R_{10}\right) \left(\text{mod } 30\right)$.

$R_3 = 2$ (Somme des chiffres modulo 3 de N) et $R_{10} = 9$ (dernier chiffre de N)

Donc $R_{30} \equiv 9 + 10 \times \left(2 - 9\right) \equiv -61 \equiv -1 \left(\text{mod } 30\right)$.

Modulo 2730 : (Propriété 3) $r_{2730} = R_{2730} \equiv R_{91}\left(R_{30} - R_{91}\right) \left(\text{mod } 2730\right)$.

$r_{2730} \equiv 45 + 91\left(-1 - 45\right) \equiv -4141 \equiv -4141 + 2 \times 2730 \equiv 1319 \left(\text{mod } 2730\right)$.

Comme on veut un résultat entre 5700 et 7200, on prendra

$$n = 1319 + 2 \times 2730 = 6779.$$

Tous les calculs nécessaires figurent ci-dessus : ce n'est quand même pas la mer à boire ! Évidemment, ce sera plus délicat avec l'expérience $E_{13}(100)$ qui est proposée sur le site.

Infographie.

• Pour l'historique concernant les records de l'expérience $E_{13}(100)$ voir :
Wikipédia : *Racine treizième d'un nombre de 100 chiffres*

• Le site de Gérard Vuillemin donne de nombreuses informations sur les expériences d'extraction mentale de racines 13-èmes :
villemin.gerard.free.fr/Wwwgvmm/Analyse/Racine13.htm

• Pour le théorème chinois, l'origine de l'appellation et les extensions (non nécessaires ici) :
Wikipédia : *Théorème des restes chinois*