$\left(3+\sqrt{5}\right)^n$

Le *Google Code Jam* est un concours de programmation organisé par Google. Les candidats doivent résoudre, en temps limité, quelques problèmes spécialement concoctés pour cette occasion, à l'aide du langage, voire des langages de programmation de leur choix. Les sélections se font en plusieurs tours, du *Qualification Round* (en 2013 : 25 heures pour 4 exercices, 21 273 candidats, 17 054 qualifiés) aux *World Finals* (en 2013 : 4 heures pour 5 exercices, 24 candidats, et... un seul gagnant, le Biélorusse Ivan Metelsky).

En 2008, un des exercices du Tour 1 reposait sur de jolies mathématiques.

Exercice. Étant donné n, calculer les trois derniers chiffres avant la virgule de $(3+\sqrt{5})^n$.

On va expliquer ici comment résoudre cet exercice avec une utilisation en fait assez minimale de l'ordinateur, en découvrant au passage une jolie propriété de ce nombre $3+\sqrt{5}$.

I. $(3+\sqrt{5})^n$ est presque entier

Posons $\rho = 3+\sqrt{5}$. Commençons par calculer (par exemple à l'aide du site WolframAlpha) les premières valeurs de ρ^n.

$\rho^0 \approx$	1,000	$\rho^8 \approx$	564 991,884
$\rho^1 \approx$	5,236	$\rho^9 \approx$	2 958 335,911
$\rho^2 \approx$	27,416	$\rho^{10} \approx$	15 490 047,932
$\rho^3 \approx$	143,554	$\rho^{11} \approx$	81 106 943,948
$\rho^4 \approx$	751,659	$\rho^{12} \approx$	424 681 471,960
$\rho^5 \approx$	3 935,740	$\rho^{13} \approx$	2 223 661 055,970
$\rho^6 \approx$	20 607,801	$\rho^{14} \approx$	11 643 240 447,977
$\rho^7 \approx$	107 903,848	$\rho^{15} \approx$	60 964 798 463,982

On observe que ρ^n semble se rapprocher d'un entier au fur et à mesure que n tend vers l'infini. C'est effectivement le cas, et comprendre la raison de ce phénomène nous permettra de calculer efficacement les trois derniers chiffres de la partie entière $\lfloor \rho^n \rfloor$.

Reprenons le calcul de ρ^n, cette fois-ci en valeur exacte.

$\rho^0 =$	1	$\rho^5 =$	$1\,968 + 880\sqrt{5}$
$\rho^1 =$	$3 + \sqrt{5}$	$\rho^6 =$	$10\,304 + 4\,608\sqrt{5}$
$\rho^2 =$	$14 + 6\sqrt{5}$	$\rho^7 =$	$53\,952 + 24\,128\sqrt{5}$
$\rho^3 =$	$72 + 32\sqrt{5}$	$\rho^8 =$	$282\,496 + 126\,336\sqrt{5}$
$\rho^4 =$	$376 + 168\sqrt{5}$	$\rho^9 =$	$1\,479\,168 + 661\,504\sqrt{5}$

On observe que les ρ^n appartiennent tous à l'ensemble $\mathrm{A} = \left\{x+y\sqrt{5} \,\middle|\, x,y \in \mathbb{Z}\right\}$. Cela n'est pas très surprenant : à cause de la formule

$$\left(a+b\sqrt{5}\right)\cdot\left(\alpha+\beta\sqrt{5}\right) = \left(a\alpha+5b\beta\right)+\left(a\beta+\alpha b\right)\sqrt{5},$$

cet ensemble est stable par multiplication [1] : puisqu'il contient ρ, il doit contenir toutes ses puissances.

On sait bien que la manipulation de quantités comme $a+b\sqrt{5}$ fait souvent appel à *la quantité conjuguée* $a-b\sqrt{5}$. En termes plus précis, on a une opération $\varphi : \mathrm{A} \to \mathrm{A}$ définie par $\varphi\left(a+b\sqrt{5}\right) = a-b\sqrt{5}$.

1. Comme vous l'avez sûrement remarqué, cet ensemble A est même un sous-anneau de $\mathbb{R}$: l'appartenance de 0 et 1 à A et la stabilité par addition sont encore plus faciles à établir que la stabilité par multiplication.

Il est important de remarquer que cette opération est bien définie. Cela vient du fait qu'un élément de A ne peut s'écrire sous la forme $x+y\sqrt{5}$ que d'une seule façon : si l'on a des entiers x, y, ξ, η tels que $x+y\sqrt{5}=\xi+\eta\sqrt{5}$, on peut déduire $(x-\xi)=(\eta-y)\sqrt{5}$ et l'irrationalité de $\sqrt{5}$ entraîne que $x-\xi=\eta-y=0$. L'écriture de départ est donc unique, ce qui entraîne que la « conjugaison » φ est bien définie.

La propriété capitale de cette opération est que si a et b appartiennent à A, on a $\varphi(ab)=\varphi(a)\cdot\varphi(b)$, ce que l'on vérifie [2] par un simple calcul. Enfin, par sa définition même, on voit qu'un élément $a\in$A est un entier si et seulement s'il vérifie $\varphi(a)=a$. En particulier, les élements de la forme $a+\varphi(a)$ sont toujours des entiers !

Toutes ces remarques algébriques illustrent maintenant le fait que ρ^n est « presque entier » : d'après ce qui précède, le nombre réel

$$\mathrm{R}_n=\rho^n+\varphi\left(\rho^n\right)=\rho^n+\varphi(\rho)^n=\left(3+\sqrt{5}\right)^n+\left(3-\sqrt{5}\right)^n$$

est bel et bien un entier.

Or, $3-\sqrt{5}\approx 0,76$ est un nombre compris (strictement) entre 0 et 1 : ses puissances tendent donc vers 0. On a donc

$$\mathrm{R}_n-\rho^n=\left(3-\sqrt{5}\right)^n\to 0,$$

ce qui explique bien le phénomène observé dès les premiers calculs [3].

Comme $0<\mathrm{R}_n-\rho^n<1$ pour tout $n>1$, on a $\mathrm{R}_n-1<\rho^n<\mathrm{R}_n$ et déterminer les derniers chiffres avant la virgule de ρ^n revient donc à déterminer les derniers chiffres de l'entier R_n-1.

$$\forall n\geqslant 0,\lfloor\rho^n\rfloor=\mathrm{R}_n-1.$$

II. Suites linéaires récurrentes du deuxième ordre

Pour terminer le calcul, nous avons besoin d'un aparté : il nous faut nous souvenir d'un domaine où l'on rencontre aisément des expressions du type

$$\mathrm{R}_n=\left(3+\sqrt{5}\right)^n+\left(3-\sqrt{5}\right)^n,$$

celui des *suites récurrentes linéaires du deuxième ordre.*

Une suite récurrente linéaire du deuxième ordre est une suite réelle (par exemple) (L_n) vérifiant une relation du type

$$\forall n\geqslant 0,\mathrm{L}_{n+2}=a\mathrm{L}_{n+1}+b\mathrm{L}_n,$$

où a et b sont deux nombres réels fixés. La plus célèbre de ces suites est sans doute la suite de Fibonacci définie par la relation de récurrence

$$\forall n\geqslant 0,\mathrm{F}_{n+2}=\mathrm{F}_{n+1}+\mathrm{F}_n$$

et par les premiers termes $\mathrm{F}_1=\mathrm{F}_2=1$.

2. Encore une fois, on montre sans difficulté que φ est en fait un morphisme d'anneaux bijectif.

3. On peut énoncer ce résultat de manière un peu différente : *la suite* $(\rho^n \bmod 1)_{n\in\mathbb{N}}$ *tend vers* 0. Ce résultat s'applique en fait à une classe infinie de nombres algébriques, les *nombres de Pisot,* dont $3+\sqrt{5}$ fait partie.

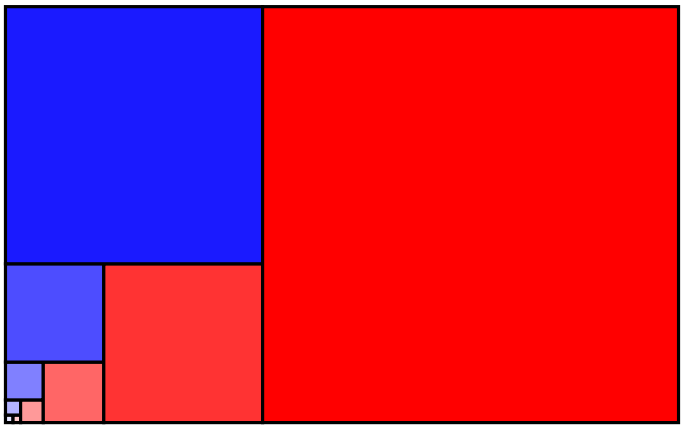

FIGURE 1 – Les carrés de côté $F_0, F_1, \ldots, F_n$ s'emboîtent pour former un rectangle de taille $F_n \times F_{n+1}$

Cette suite

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \ldots,$$

est sans doute l'une des rares suites à avoir (un peu) pénétré la culture populaire.

Comme on l'apprend lors des premières années de l'université, l'obtention d'une formule pour une suite récurrente (L_n) de ce type dépend des racines du polynôme de second degré

$$P(X) = X^2 - aX - b.$$

Le cas qui nous intéresse ici est celui où le polynôme P a deux racines réelles distinctes [4] r et $s \in \mathbb{R}$, c'est-à-dire celui où $\Delta(P) = a^2 + 4b > 0$. Dans ce cas, la suite L_n est de la forme

$$L_n = \lambda r^n + \mu s^n,$$

où λ et μ sont deux nombres réelles.

Par exemple, le polynôme $X^2 - X - 1$ a deux racines réelles :

$$\varphi = \frac{1+\sqrt{5}}{2} \qquad \text{et} \qquad \psi = \frac{1-\sqrt{5}}{2},$$

donc la suite de Fibonacci est du type $F_n = \lambda\varphi^n + \mu\psi^n$. Les deux premiers termes $F_1 = F_2 = 1$ permettent de déterminer les coefficients. On obtient ainsi la célèbre *formule de Binet*

$$F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

Ici, nous allons plutôt faire marcher la machine à l'envers : supposons que l'on tombe par hasard sur l'expression

$$L_n = \varphi^n + \psi^n.$$

Pour des raisons similaires à celles que l'on a explicitées dans la section précédente, L_n est un nombre entier pour tout n. Mais en fait, on peut ici en dire plus : d'après ce qui précède, L_n est l'unique suite vérifiant la relation de récurrence de Fibonacci

$$\forall n \geqslant 0, L_{n+2} = L_{n+1} + L_n$$

4. Si P a une racine double r, la solution générale est du type $L_n = (\lambda n + \mu) \cdot r^n$. Si P a deux racines complexes conjuguées $re^{\pm i\theta}$, la solution générale est du type $L_n = (\lambda\cos(n\theta) + \mu\sin(n\theta)) \cdot r^n$. Dans tous les cas, la connaissance de deux termes de la suite (L_n) permet de déterminer les coefficients λ et μ.

et telle que $L_0 = 2$ et $L_1 = \varphi + \psi = 1$. Cette cousine de la suite de Fibonacci porte en fait déjà un nom : c'est la *suite de Lucas*.

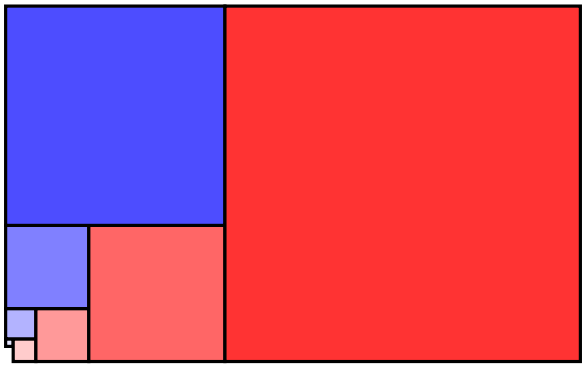

FIGURE 2 – Les « carrés de Lucas » s'emboîtent aussi (mais le début est moins joli) !

III. Calcul des derniers chiffres de R_n

Revenons à notre entier $R_n = \left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$. Comme pour la suite de Lucas, on peut faire un peu de *reverse engineering* pour trouver une relation de récurrence : les réels $3 \pm \sqrt{5}$ sont les racines (réelles et distinctes) du polynôme du second degré

$$P(X) = X^2 - 6X + 4.$$

Ainsi, la suite (R_n) vérifie la relation de récurrence

$$\forall n \geqslant 0, R_{n+2} = 6R_{n+1} - 4R_n.$$

Cette relation de récurrence est en fait la clef qui va nous permettre de calculer les derniers chiffres de R_n en faisant très peu de calculs, grâce à deux simplifications successives.

Première simplification : calculer par récurrence le nombre entier $R_n = 6R_{n-1} - 4R_{n-2}$ requiert un calcul de plus en plus long (la formule $R_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n$ elle-même montre que R_n croît exponentiellement). Cependant, seuls les trois derniers chiffres de R_n nous intéressent ! Or, pour calculer les trois derniers chiffres de $R_n = 6R_{n-1} - 4R_{n-2}$, il suffit de connaître les trois derniers chiffres de R_{n-1} et R_{n-2}...

Autrement dit, il s'agit de calculer les trois derniers chiffres de R_n, c'est-à-dire le résidu de R_n modulo 1 000. Or, pour toute paire (x, y) d'entiers, le résidu modulo 1 000 de $6x - 4y$ est

$$6\overline{x} - 4\overline{y} \in \mathbb{Z}/1\,000\mathbb{Z},$$

où $\overline{x}$ et $\overline{y}$ sont les résidus de x et y modulo 1 000 [5].

Ainsi, la suite $(\overline{R}_n) = (R_n \bmod 1\,000)$ des résidus modulo 1 000 est simplement la suite d'éléments de $\mathbb{Z}/1\,000\mathbb{Z}$ définie par la même relation de récurrence

$$\forall n \geqslant 0, \overline{R}_{n+2} = 6\overline{R}_{n+1} - 4\overline{R}_n$$

et par les premiers termes $\overline{R}_0 = R_0 \bmod 1\,000 = \overline{2}$ et $\overline{R}_1 = \overline{6}$.

5. Encore une fois, on peut dire cet argument de manière plus savante : la surjection canonique $\mathbb{Z} \to \mathbb{Z}/1\,000\mathbb{Z}$ est un morphisme d'anneaux.

$$\begin{array}{l|l}
\overline{\mathrm{R}}_0 = \overline{2} & \overline{\mathrm{R}}_8 = \overline{992} \\
\overline{\mathrm{R}}_1 = \overline{6} & \overline{\mathrm{R}}_9 = \overline{336} \\
\overline{\mathrm{R}}_2 = \overline{28} & \overline{\mathrm{R}}_{10} = \overline{48} \\
\overline{\mathrm{R}}_3 = \overline{144} & \overline{\mathrm{R}}_{11} = \overline{944} \\
\overline{\mathrm{R}}_4 = \overline{752} & \overline{\mathrm{R}}_{12} = \overline{472} \\
\overline{\mathrm{R}}_5 = \overline{936} & \overline{\mathrm{R}}_{13} = \overline{56} \\
\overline{\mathrm{R}}_6 = \overline{608} & \overline{\mathrm{R}}_{14} = \overline{448} \\
\overline{\mathrm{R}}_7 = \overline{904} & \overline{\mathrm{R}}_{15} = \overline{464}
\end{array}$$

Seconde simplification : La réduction à $\mathbb{Z}/1\,000\mathbb{Z}$ nous a permis de faire moins de calcul, mais elle a un autre avantage, plus conceptuel. La suite $(\overline{\mathrm{R}}_n)$ ne peut maintenant plus prendre que mille valeurs. Comme il y a une infinité de nombres entiers, cela implique que la suite (R_n) sera contrainte à se répéter au moins une fois [6] : il existe deux entiers m_0 et $m_1 = m_0 + \mathrm{T} > m$ tels que $\overline{\mathrm{R}}_{m_0+\mathrm{T}} = \overline{\mathrm{R}}_{m_0}$.

Encore mieux, les couples $(\overline{\mathrm{R}}_n, \overline{\mathrm{R}}_{n+1})$ de termes successifs ne peuvent prendre qu'un million de valeurs. Pour la même raison, on pourra trouver deux nombres n_0 et $n_1 = n_0 + \mathrm{T} > n_0$ tels que

$$(\overline{\mathrm{R}}_{n_0+\mathrm{T}}, \overline{\mathrm{R}}_{n_0+\mathrm{T}+1}) = (\overline{\mathrm{R}}_{n_0}, \overline{\mathrm{R}}_{n_0+1}).$$

Mais, à cause de la relation de récurrence, cette coïncidence a une conséquence drastique : si $\overline{\mathrm{R}}_{n_0+\mathrm{T}} = \overline{\mathrm{R}}_{n_0}$ et $\overline{\mathrm{R}}_{n_0+\mathrm{T}+1} = \overline{\mathrm{R}}_{n_0+1}$, la relation de récurrence entraîne que $\overline{\mathrm{R}}_{n_0+\mathrm{T}+2} = \overline{\mathrm{R}}_{n_0+2}$. Une nouvelle application de la relation de récurrence entraînera que $\overline{\mathrm{R}}_{n_0+\mathrm{T}+3} = \overline{\mathrm{R}}_{n_0+3}$, et ainsi de suite : la suite $(\overline{\mathrm{R}}_n)$ ne pourra désormais plus éviter de prendre les mêmes valeurs encore et encore : on aura

$$\forall n \geqslant n_0, \overline{\mathrm{R}}_n = \overline{\mathrm{R}}_{n+\mathrm{T}} = \overline{\mathrm{R}}_{n+2\mathrm{T}} = \cdots$$

Une fois que l'on aura déterminé n_0 et T, on pourra donc calculer presque instantanément $\overline{\mathrm{R}}_n$ pour des valeurs arbitrairement grandes de n, pourvu que l'on soit capable de calculer la division euclidienne de n par T.

En fait, on vérifie simplement (c'est le seul endroit où l'ordinateur se révèle en fait nécessaire) que $n_0 = 3$ et $\mathrm{T} = 100$ conviennent : à partir de $n = 3$, la suite se répète avec une période égale à 100.

	0	1	2	3	4	5	6	7	8	9
	2	6	28	**144**	**752**	936	608	904	992	336
1_	48	944	472	56	448	464	992	96	608	264
2_	152	856	528	744	352	136	408	904	792	136
3_	648	344	472	456	848	264	192	96	808	464
4_	552	456	528	344	952	336	208	904	592	936
5_	248	744	472	856	248	64	392	96	8	664
6_	952	56	528	944	552	536	8	904	392	736
7_	848	144	472	256	648	864	592	96	208	864
8_	352	656	528	544	152	736	808	904	192	536
9_	448	544	472	656	48	664	792	96	408	64
10_	752	256	528	**144**	**752**	936	608	904	992	⋯

Une fois ces quelques valeurs calculées, on peut donc calculer instantanément $\overline{\mathrm{R}}_n$ pour de très grandes valeurs de n : Par exemple, $\overline{\mathrm{R}}_{10^{10^{10}}+42} = \overline{\mathrm{R}}_{42} = \overline{528}$, résultat évidemment inaccessible par le calcul direct...

Puisque $\lfloor \rho^n \rfloor = \mathrm{R}_n - 1$, on est donc capable de déterminer les trois derniers chiffres avant la virgule de toutes les puissances de $(3+\sqrt{5})^n$. Pour reprendre l'exemple $\overline{\mathrm{R}}_{10^{10^{10}}+42} = \overline{528}$, on a

$$\left(3+\sqrt{5}\right)^{10^{10^{10}}+42} = \ldots\mathbf{527},\ldots$$

6. Alors que la suite initiale (R_n), elle, ne prend jamais deux fois la même valeur.