Les terminaisons des carrés parfaits

Michel Lafond(*)

I) Le problème.

Tout le monde sait bien qu'en base 10, un carré parfait ne peut se terminer que par 0, 1, 4, 5, 6 ou 9.
Il y a 6 terminaisons possibles sur 10.
Pour n ≥ 2 entier, il est naturel de s'intéresser aux terminaisons à n chiffres des carrés parfaits et de se demander combien il y en a en fonction de n.

L'objet de cet article est de répondre à cette question.
On n'utilise que des résultats simples sur les congruences.

Dans la foulée, nous démontrerons ce curieux résultat :

En base 10, une longue séquence de chiffres aléatoire a environ 7 chances sur 100 d'être la terminaison d'un carré parfait.

Notons $T_1 = \{0, 1, 4, 5, 6, 9\}$ l'ensemble des terminaisons à un chiffre des carrés.
Les nombres précédents sont ce qu'on appelle les résidus quadratiques (ou carrés) modulo 10.

II) Les terminaisons à deux chiffres et à trois chiffres.

On tolérera une terminaison commençant par un ou plusieurs 0 comme 04 dans $52^2 = 2704$.
Les terminaisons à deux chiffres cherchées sont les carrés modulo 100.
Pour les déterminer, il suffit de calculer les carrés de 0^2 à 25^2 puisque :

$(50 + x)^2 = 2500 + 100x + x^2 = x^2 + 100n$ est congru à x^2 modulo 100 ;
$(50 - x)^2 = 2500 - 100x + x^2 = x^2 + 100m$ est congru à x^2 modulo 100.

On trouve :

n	n^2 mod 100	n	n^2 mod 100	n	n^2 mod 100
0	**00**				
1	**01**	11	**21**	21	**41**
2	**04**	12	**44**	22	**84**
3	**09**	13	**69**	23	**29**
4	**16**	14	**96**	24	**76**
5	**25**	15	**25**	25	**25**
6	**36**	16	**56**		
7	**49**	17	**89**		
8	**64**	18	**24**		
9	**81**	19	**61**		
10	**00**	20	**00**		

(*) mlafond001@yahoo.fr

Il y a exactement 22 terminaisons à deux chiffres, celles de l'ensemble :
$T_2 = \{00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96\}$.

Continuons. Les ordinateurs nous donnent rapidement les terminaisons possibles à trois chiffres des carrés :
$T_3 = \{000, 001, 004, 009, 016, 024, 025, 036, 041, 044, 049, 056, 064, 076, 081, 084, 089, 096, 100, 104, 116, 121, 124, 129, 136, 144, 156, 161, 164, 169, 176, 184, 196, 201, 204, 209, 216, 224, 225, 236, 241, 244, 249, 256, 264, 276, 281, 284, 289, 296, 304, 316, 321, 324, 329, 336, 344, 356, 361, 364, 369, 376, 384, 396, 400, 401, 404, 409, 416, 424, 436, 441, 444, 449, 456, 464, 476, 481, 484, 489, 496, 500, 504, 516, 521, 524, 529, 536, 544, 556, 561, 564, 569, 576, 584, 596, 600, 601, 604, 609, 616, 624, 625, 636, 641, 644, 649, 656, 664, 676, 681, 684, 689, 696, 704, 716, 721, 724, 729, 736, 744, 756, 761, 764, 769, 776, 784, 796, 801, 804, 809, 816, 824, 836, 841, 844, 849, 856, 864, 876, 881, 884, 889, 896, 900, 904, 916, 921, 924, 929, 936, 944, 956, 961, 964, 969, 976, 984, 996\}$
Il y en a exactement 159.

III) Notations.

Si on note C(n) le nombre de carrés modulo n, alors C(10^n) est le nombre de terminaisons possibles à n chiffres des carrés parfaits en base 10.

C(10) = 6, C(10^2) = 22, C(10^3) = 159, C(10^4) = 1 044, C(10^5) = 9 121, C(10^6) = 78 132, C(10^7) = 748 719, C(10^8) = 7 161 484, C(10^9) = 70 800 861, etc.

Cette suite est répertoriée dans l'encyclopédie des suites sous la référence A 000993 (voir sitographie).

Il faudra patienter un peu (paragraphe VII et sitographie) pour avoir « la formule générale » donnant C(10^n).

On remarque tout de suite que, par rapport aux 10^n terminaisons possibles des nombres entiers à n chiffres, la proportion des terminaisons des seuls carrés parfaits à savoir $\mathrm{pr}_n = \dfrac{\mathrm{C}(10^n)}{10^n}$ diminue assez vite :

n	proportion pr_n
1	0,600
2	0,220
3	0,159
4	0,104
5	0,091
6	0,078

La question qui brûle les lèvres est : la limite de pr_n, si elle existe, est-elle égale à 0 ? Eh bien non ! Et, ce qui est plus surprenant, est que cette limite est le rationnel

$$\mathrm{L} = \frac{5}{72} \approx 0{,}069\,444\ldots$$

D'où le résultat affirmé dans le paragraphe I).

La démonstration est assez longue, mais pas trop difficile si on sait manipuler un peu les congruences.

IV) Un théorème clé.

Dans la suite, on supposera que les carrés modulo m sont dans l'ensemble $\{0, 1, 2, \dots, m-1\}$.
Il y aura donc constamment des abus de langage confondant les entiers modulo m avec leurs représentants dans $\{0, 1, 2, \dots, m-1\}$.

Puisqu'on veut seulement compter les carrés modulo 10^n (et non les calculer), il s'agit d'un problème de pur dénombrement, et un théorème va simplifier le travail :

Théorème : **Si p et q sont deux entiers naturels premiers entre eux, $C(pq) = C(p)\,C(q)$.**

Démonstration :

Notons $A = \{a_1 ; a_2 ; \dots ; a_\alpha\} \subset \{0, 1, \dots, p-1\}$ les carrés modulo p ;
$B = \{b_1 ; b_2 ; \dots ; b_\beta\} \subset \{0, 1, \dots, q-1\}$ les carrés modulo q et
$M = \{c_1 ; c_2 ; \dots ; c_\gamma\} \subset \{0, 1, \dots, pq-1\}$ les carrés modulo pq.

Si $c \in M$ est un carré modulo pq il existe un entier x tel que $x^2 \equiv c \bmod pq$.
On en déduit immédiatement $x^2 \equiv c \bmod p$ et $x^2 \equiv c \bmod q$.
Donc il existe a_i unique dans A et b_j unique dans B tels $c \equiv a_i \bmod p$ que et $c \equiv b_j \bmod q$.
Notons φ l'application de M dans $A \times B$ qui, à tout carré c modulo pq de M associe le couple $\varphi(c) = (a_i ; b_j)$ de $A \times B$ défini ci-dessus.

<u>φ est bijective</u> :
En effet, cherchons à résoudre dans M l'équation d'inconnue c :

$$\varphi(c) = (a_i ; b_j)$$

pour $(a_i ; b_j)$ donné dans $A \times B$.
Cette équation équivaut à

$$c \equiv a_i \bmod p \text{ et } c \equiv b_j \bmod q \qquad (1)$$

Posons $c = a_i + \lambda p$. (1) est équivalente au système d'inconnues c, λ :

$$c = a_i + \lambda p \text{ et } \lambda p \equiv b_j - a_i \bmod q \qquad (2)$$

Dans l'anneau des entiers modulo q, p est inversible puisque p et q sont premiers entre eux.
Si p' est l'inverse (unique) de p mod q, (2) équivaut à

$$c = a_i + \lambda p \text{ et } \lambda \equiv p'(b_j - a_i) \bmod q \qquad (3)$$

λ est unique mod q et par conséquent, $c = a_i + \lambda p$ est unique modulo pq.

L'équation $\varphi(c) = (a_i ; b_j)$ a pour tout $(a_i ; b_j)$ dans $A \times B$ une solution unique c dans M.

φ est bijective, donc le cardinal de M est égal au cardinal de A × B c'est à dire

$$C(pq) = C(p)\ C(q).$$

Le corollaire qui nous intéresse est :

$$\mathbf{C(10^n) = C(2^n)\ C(5^n).}$$

On se ramène donc au calcul du nombre de carrés modulo 2^n et au calcul du nombre de carrés modulo 5^n.

Malheureusement la structure des résidus modulo p^n où p est premier n'est pas la même pour $p = 2$ et pour p impair. Il va falloir deux études.

V) Calcul de $C(2^n)$, nombre de carrés modulo 2^n.

Examinons ce qui se passe pour n de 1 à 7 dans le tableau ci-dessous, où on a séparé les carrés pairs et les carrés impairs [Dans {0, 1, 2, … , $m - 1$} on peut parler de parité] :

n	Résidus quadratiques (carrés) modulo 2^n	
	Carrés pairs	Carrés impairs
1	0	1
2	0	1
3	0 4	1
4	0 4	1 9
5	0 4 16	1 9 17 25
6	0 4 16 36	1 9 17 25 33 41 49 57
7	0 4 16 36 64 68 100	1 9 17 25 33 41 49 57 65 73 81 89 97 105 113 121

Exemple : $n = 5$.

Pour obtenir tous les carrés modulo 32, il suffit d'en examiner le quart. En effet :

Si on sépare les entiers modulo 32 [pris par commodité de – 8 à 23] en deux moitiés [de – 8 à 7 et de 8 à 23] puis la première moitié en deux quarts [de – 8 à – 1 et de 0 à 7], on passe des carrés de la première moitié aux carrés de la seconde moitié en effectuant $x^2 \to (x + 16)^2 \equiv x^2 + 32\,x + 256 \equiv x^2 \bmod 32$ et on passe des carrés du premier quart aux carrés du second quart en effectuant $x^2 \to (-x)^2 \equiv x^2 \bmod 32$.

On obtient ainsi $0^2 \equiv 0$; $1^2 \equiv 1$; $2^2 \equiv 4$; $3^2 \equiv 9$; $4^2 \equiv 16$; $5^2 \equiv 25$; $6^2 \equiv 36 \equiv 4$; $7^2 \equiv 17$, soient sept carrés modulo 32 : {0, 1, 4, 9, 16, 17, 25} dont trois pairs et quatre impairs.

Avec un peu d'attention on remarque qu'à partir de $n = 3$:

– les carrés pairs modulo 2^n sont égaux aux carrés (pairs et impairs) modulo 2^{n-2} que multiplie 4,

– les carrés impairs modulo 2^n sont composés des carrés impairs modulo 2^{n-1} et de ces mêmes carrés auxquels on a ajouté 2^{n-1}.
La démonstration figure en annexe 1 sur le site de l'APMEP avec l'article complet.

Connaissant leur structure, on peut passer au dénombrement des carrés modulo 2^n.
Leur nombre $C(2^n)$ est la somme du nombre P_n des carrés pairs, et du nombre I_n des carrés impairs [on est toujours dans $\{0, 1, \dots, 2n-1\}$].

Pour les carrés impairs (voir le tableau précédent) : $I_1 = 1$; $I_2 = 1$; $I_3 = 1$; et si $n \geq 4$, les carrés impairs modulo 2^n sont composés des carrés impairs modulo 2^{n-1} et des carrés impairs modulo 2^{n-1} auxquels on a ajouté 2^{n-1}.
Si $n \geq 4$, on a donc $I_n = 2\,I_{n-1}$ d'où immédiatement : $I_1 = 1$; $I_2 = 1$ et si $n \geq 3$ $I_n = 2^{n-3}$.

Pour les carrés pairs : $P_1 = 1$; $P_2 = 1$; $P_3 = 2$; et si $n \geq 4$ les carrés pairs modulo 2^n sont égaux aux carrés (pairs et impairs) modulo 2^{n-2} que multiplie 4, c'est-à-dire : $P_n = P_{n-2} + I_{n-2}$.

D'après ce qu'on vient de voir, si $n \geq 5$,

$$P_n = P_{n-2} + I_{n-2} = P_{n-2} + 2^{n-5} \qquad (4)$$

La suite (P_n) vérifie une relation linéaire d'ordre 2.

On a d'après (4) :
– Pour les indices pairs, $P_4 = 2$; $P_6 = P_4 + 2^1$; $P_8 = P_4 + 2^1 + 2^3$; $P_{10} = P_8 + 2^5 = P_4 + 2^1 + 2^3 + 2^5$, etc. Donc :

$$P_{2k} = P_4 + 2^1 + 2^3 + \dots + 2^{2k-5} = 2 + 2\,\frac{4^{k-2} - 1}{3} = \frac{4 + 2^{2k-3}}{3} \quad (k \geq 2).$$

- Pour les indices impairs, $P_3 = 2$; $P_5 = P_3 + 2^0$; $P_7 = P_5 + 2^2 = P_3 + 2^0 + 2^2$, etc. Donc :

$$P_{2k+1} = P_3 + 2^0 + 2^2 + \dots + 2^{2k-4} = 2 + \frac{4^{k-1} - 1}{3} = \frac{5 + 2^{2k-2}}{3} \quad (k \geq 2).$$

En résumé : $P_n = \dfrac{4 + 2^{n-3}}{3}$ si n pair ≥ 4 et $P_n = \dfrac{5 + 2^{n-3}}{3}$ si n impair ≥ 5

D'où :

$$C\left(2^n\right) = P_n + I_n = \frac{4 + 2^{n-3}}{3} + 2^{n-3} = \frac{4 + 2^{n-1}}{3} \text{ si } n \text{ est pair quelconque}^{(1)}.$$

$$C\left(2^n\right) = P_n + I_n = \frac{5 + 2^{n-3}}{3} + 2^{n-3} = \frac{5 + 2^{n-1}}{3} \text{ si } n \text{ est impair quelconque}^{(2)}.$$

(1) $C(2) = 2$ donc l'expression donnée pour n pair ≥ 4 fonctionne aussi pour $n = 2$.
(2) $C(1) = 2$, $C(2) = 3$ donc l'expression donnée pour n impair ≥ 5 fonctionne aussi pour $n = 1$ ou 3.

VI) Calcul de C(5^n), nombre de carrés modulo 5^n.

La situation est un peu différente de la précédente :
Examinons ce qui se passe pour n de 1 à 3 dans le tableau ci-dessous, où on a séparé les résidus multiples de 5 et les autres :

n	Résidus quadratiques (carrés) modulo 5^n	
	Carrés multiples de 5	Carrés non multiples de 5
1	0	1 4
2	0	1 4 6 9 11 14 16 19 21 24
3	0 25 100	1 4 6 9 11 14 16 19 21 24 26 29 31 34 36 39 41 44 46 49 51 54 56 59 61 64 66 69 71 74 76 79 81 84 86 89 91 94 96 99 101 104 106 109 111 114 116 119 121 124

On démontre dans l'annexe 2 (sur le site de l'APMEP avec l'article complet) qu'à partir de $n = 2$:
– Si n est pair, les carrés modulo 5^n sont composés de 0 et des carrés non nuls modulo 5^{n-1} auxquels on a ajouté $k \cdot 5^{n-1}$ avec $k \in \{0, 1, 2, 3, 4\}$.
– Si n est impair, les carrés modulo 5^n sont composés des carrés non nuls modulo 5^{n-1} auxquels on a ajouté $k \cdot 5^{n-1}$ avec $k \in \{0, 1, 2, 3, 4\}$, et de 5^{n-1} que multiplie 0, 1 ou 4 (les carrés modulo 4).

On peut passer au <u>dénombrement des carrés modulo 5^n</u>.

Leur nombre C(5^n) vérifie : C(5) = 3 ; C(5^2) = 11 ; C(5^3) = 5^3 et pour $n \geq 4$:

si n pair :

$$C(5^n) = 1 + 5\,[C(5^{n-1}) - 1]$$

[1 pour $c = 0$ et 5 [C(5^{n-1}) − 1] pour $c = 5^{n-1}\,k + d$ avec $k \in \{0, 1, 2, 3, 4\}$ et d carré non nul modulo 5^{n-1}] ;

si n impair :

$$C(5^n) = 3 + 5\,[C(5^{n-1}) - 1]$$

[3 pour $c = 5^{n-1}\,k$ avec $k \in \{0, 1, 4\}$ et 5 [C(5^{n-1}) − 1] pour $c = 5^{n-1}\,k + d$ avec $k \in \{0, 1, 2, 3, 4\}$ et d carré non nul modulo 5^{n-1}].

Or la suite U définie par $U_1 = 3$, $U_2 = 11$, $U_3 = 53$ et pour $n \geq 4$:

$$U_n = \frac{5^{n+1} + 7}{12} \text{ si } n \text{ pair et } U_n = \frac{5^{n+1} + 11}{12} \text{ si } n \text{ impair,}$$

vérifie elle aussi la récurrence :

si n pair : $U_n = 1 + 5\,[U_{n-1} - 1]$ et si n impair : $U_n = 3 + 5\,[U_{n-1} - 1]$.

En effet :

si n est impair, $3+5\left[U_{n-1}-1\right]=3+5\left[\dfrac{5^n+7}{12}-1\right]=\dfrac{5^{n+1}+11}{12}=U_n$ et

si n est pair, $1+5\left[U_{n-1}-1\right]=1+5\left[\dfrac{5^n+11}{12}-1\right]=\dfrac{5^{n+1}+7}{12}=U_n$.

Donc les suites C et U sont identiques et :

$$C\left(5^n\right)=\frac{7+5^{n+1}}{12} \text{ si } n \text{ pair quelconque,}$$

$$C\left(5^n\right)=\frac{11+5^{n+1}}{12} \text{ si } n \text{ impair quelconque.}$$

VII) Calcul de C(10^n) et passage à la limite.

Avec C(pq) = C(p) C(q) et les résultats de V) et de VI), on est enfin en mesure de calculer C(10^n) :
Si n pair :

$$C\left(10^n\right)=C\left(2^n\right)C\left(5^n\right)=\frac{4+2^{n-1}}{3}\frac{7+5^{n+1}}{12}=\frac{5\times10^n+40\times5^n+7\times2^n+56}{72} \quad (5)$$

Si n impair :

$$C\left(10^n\right)=C\left(2^n\right)C\left(5^n\right)=\frac{5+2^{n-1}}{3}\frac{11+5^{n+1}}{12}=\frac{5\times10^n+50\times5^n+11\times2^n+110}{72} \quad (6)$$

Lorsque n tend vers l'infini, la limite de $\dfrac{C(10^n)}{10^n}$ est bien égale à

$$L=\frac{5}{72}\approx0{,}069\,444\ldots.$$

Autrement dit : En base 10, une longue séquence aléatoire de n chiffres, a environ 5 chances sur 72 d'être une terminaison de carré parfait.

Bibliographie : Un article de « The American Mathematical Monthly » de décembre 1960 « On the final digits of squares. » de W. Penney, p. 1000-1002.

Sitographie : Le site http://oeis.org/
[OEIS est le sigle de On-line Encyclopedia of Integer Sequences].

La suite a_n = C(10^n) a la référence A000993.

En tapant les cinq premiers termes dans la case réservée à cet effet, le site donne :

«Number of distinct quadratic residues mod 10^n = number of distinct n-digit endings of base 10 squares.»

1, 6, 22, 159, 1044, 9121, 78132, 748719, 7161484, 70800861, 699869892, 6978353179, 69580078524, 695292156201, 6947835288052, 69465637212039, 694529215501164, 6944974263529141, 69446563720728612, 694457689921141299, 6944497426351013404

ce qui montre que la suite est connue de la base de données.

Il est frappant de constater que le résultat essentiel qui a nécessité plusieurs pages de démonstration, à savoir : limite de $\frac{C(10^n)}{10^n} \approx 0{,}0694444\ldots$ peut presque être conjecturé par le simple examen des vingt premiers termes.

Dans les commentaires sur la suite $a_n = C(10^n)$, est mentionnée la récurrence :

$$a_{n+8} = 130\, a_{n+6} - 3\,129\, a_{n+4} + 13\,000\, a_{n+2} - 10\,000\, a_n \qquad (7)$$

qui n'a rien d'étonnant car en reprenant les expressions des formules (5) et (6) du paragraphe VII, à savoir : si n est pair $C(10^n) = u_n$ et si n est impair $C(10^n) = v_n$ on aboutit à :

$$C\left(10^n\right) = \frac{1+(-1)^n}{2} u_n + \frac{1-(-1)^n}{2} v_n,$$

c'est-à-dire à la formule unique :

$$a_n = \frac{1}{72}\left[5\times 10^n + \left(45 - 5(-1)^n\right)\times 5^n + \left(9 - 2(-1)^n\right)\times 2^n - 27(-1)^n + 83\right].$$

C'est une combinaison linéaire de termes géométriques a^n où les bases a sont ± 1, ± 2, ± 5, ± 10,

Le polynôme caractéristique est :

$(x^2 - 1)(x^2 - 4)(x^2 - 25)(x^2 - 100) = x^8 - 130\, x^6 + 3\,129\, x^4 - 13\,000\, x^2 + 10\,000$,

ce qui explique les mystérieux coefficients de (7).

On peut aussi vérifier directement (7) à partir de (5) et (6) du paragraphe VII.