8. Intermède: le problème facile de Waring

$$g(3) \leqslant 11 ,$$

à montrer que tous les entiers inférieurs à cette limite sont également C_{11}. La vérification numérique se fait par une méthode de descente très simple, en ôtant de chaque entier le plus grand cube inférieur ou égal (avec une légère modification pour les deux dernières étapes): il suffit que tout entier inférieur à $2{,}5355.10^9$ soit C_{10}, que tout entier inférieur à $5{,}578.10^6$ soit C_9, que tout entier compris entre 240 et 94 758 soit C_8, et enfin que tout entier compris entre 455 et 6 665 soit C_7. Cette dernière condition résulte des tables connues (jusqu'à 40 000, 239 est le plus grand nombre qui nécessite 9 cubes, 454 le plus grand qui en nécessite 8, tous ceux au-delà étant C_7).

8. Intermède: le problème facile de Waring

Alias « the easier problem of Waring ».

Ce problème nous sera utile non pas pour son énoncé et ses résultats mais pour les identités qui interviennent dans sa résolution. Il s'agit d'écrire tout entier sous la forme $N = \pm y_1{}^k \pm y_2{}^k \pm \ldots \pm y_s{}^k$ (les y_j étant des entiers positifs, mais cela n'a guère d'importance) et d'établir l'existence d'une constante $v(k)$ telle que l'on puisse toujours prendre $s \leqslant v(k)$.

On utilise des identités valables pour les entiers dans certaines progressions arithmétiques. Ainsi pour les cubes:

$$6n = (n+1)^3 + (n-1)^3 - 2n^3$$

$$6n + 3 = (2n-5)^3 + n^3 - (2n-4)^3 - (n-4)^3$$

et pour les bicarrés:

$$4\,080n = (2n-1)^4 + (n+8)^4 - (2n+1)^4 - (n-8)^4$$

L'existence de $v(k)$ dans le cas général résulte de l'identité

$$n^k - C_{k-1}^1 (n-1)^k + C_{k-1}^2 (n-2)^k - \ldots + (-1)^{k-1} (n-k+1)^k = k\,!\,n + \beta$$

(β entier indépendant de n)

(la démonstration est immédiate: calcul de la $(k-1)$-ième différence finie du polynôme x^k).

Nous retiendrons cette identité sous la forme suivante:

LEMME. *Pour tout entier positif k il existe des entiers positifs $R = R(k)$, $S = S(k)$, α, $a_1, \ldots, a_R$, $c_1, \ldots, c_S$, et des entiers quelconques β, $b_1, \ldots, b_R$, $d_1, \ldots, d_S$, tels que l'on ait l'identité*

$$\sum_{i=1}^{R} (a_i n + b_i)^{2k} = \sum_{j=1}^{S} (c_j n + d_j)^{2k} - (\alpha n + \beta).$$

9. Théorème de Hilbert. L'identité fondamentale

La méthode de Hilbert pour démontrer l'existence de $g(n)$ est fondée sur la donnée, pour tout k, d'une identité de même forme que celle que nous avons vue pour les sommes de bicarrés:

$$M(x_1^2 + x_2^2 + \ldots + x_5^2)^2 = \sum_{i=1}^{N} m_i (a_{i1} x_1 + a_{i2} x_2 + \ldots + a_{i5} x_5)^{2k}.$$

Mais cette identité permet uniquement de démontrer l'existence de $g(2k)$ en supposant établie celle de $g(k)$. Hilbert a donc dû, pour montrer l'existence de $g(n)$ pour les valeurs impaires de n, imaginer un raisonnement par récurrence que nous trouvons personnellement assez compliqué. Après Hilbert, de nombreux mathématiciens se sont efforcés de simplifier sa démonstration mais les améliorations ont pratiquement toutes porté sur l'établissement de l'identité fondamentale.

Nous nous proposons ici de supprimer la seconde partie de la démonstration de Hilbert et de prouver, sans aucune récurrence, que $g(n)$ existe pour tout n pair (d'où il s'ensuit trivialement que $g(n)$ existe aussi pour tout n impair). Outre l'utilisation déjà annoncée des identités du problème facile de Waring, nous aurons besoin au préalable de préciser quelque peu l'identité fondamentale de Hilbert.

LEMME. *Pour tout entier positif k il existe des entiers positifs M, $N = (2k+1) \ldots (2k+5)/24$, $m_1, \ldots, m_{N-1}$, m_N, avec M et m_N strictement positifs, et des entiers $a_{11}, \ldots, a_{15}$, $a_{21}, \ldots, a_{N5}$, tels que l'on ait l'identité*

$$M(x_1^2 + \ldots + x_5^2)^k = \sum_{i=1}^{N-1} m_i (a_{i1} x_1 + \ldots + a_{i5} x_5)^{2k} + m_N x_5^{2k}.$$

(L'innovation par rapport à l'identité de Hilbert est: m_N est strictement positif).