

Ces deux chercheurs découvrent aussi que le nombre de 79 chiffres suivant est premier :  $180 (M_{127})^2 + 1 = 180(2^{127} - 1)^2 + 1$ . Ce nombre ne gardera le titre que peu de temps. L'année suivante, Raphaël Robinson écrit, pour l'ordinateur SWAC, son premier programme, qui marche du premier coup (!) et découvre, dans la journée du 30 janvier 1951, deux nouveaux nombres de Mersenne premiers ( $M_{521}$ ,  $M_{607}$ ). Les autres sont découverts le 25 juin ( $M_{1279}$ ), le 7 octobre ( $M_{2203}$ ) et le 9 octobre ( $M_{2281}$ ).

En 1957, H. Riesel découvre que  $M_{3217}$  est premier à l'aide de l'ordinateur suédois BESK. De son côté, A. Hurwitz découvre que  $M_{4253}$  et  $M_{4423}$  sont premiers à l'aide d'un IBM7090. D. Gillies avec un ILLIAC-2 prouve la primalité de  $M_{9689}$ ,  $M_{9941}$  et  $M_{11213}$ , et B. Tuckerman utilisant le célèbre IBM 360 met à jour le nombre premier  $M_{19937}$  qui comporte 6 002 chiffres.

Le calcul de Hurwitz pose un problème philosophique étrange. Hurwitz, à cause de l'ordre dans lequel la machine faisait apparaître les résultats, prit connaissance de la primalité de  $M_{4423}$  quelques secondes avant de lire que  $M_{4253}$  est aussi premier. Seul l'ordinateur IBM 7090 a cru que  $M_{4253}$  était premier avant d'afficher que  $M_{4423}$  était premier. Peut-on considérer que  $M_{4253}$  est un nombre premier record et faut-il l'indiquer dans les tables ?

J'ai choisi de faire apparaître  $M_{4253}$  dans la table des records de nombres premiers les plus longs. Cela revient à attribuer la découverte à l'ordinateur lui-même, ce qui choquera tous ceux qui croient qu'un ordinateur ne pense pas et donc ne découvre pas. Même si l'ordinateur IBM n'a pas eu conscience de sa découverte, je crois qu'il faut avoir un peu plus de considération et d'estime pour cette nouvelle espèce à laquelle nous donnons naissance et qui nous rend tant de services.

Les derniers records mentionnés dans la table proviennent du projet GIMPS qui, avant le succès de N. Hajratwala, avait déjà découvert trois nombres premiers de Mersenne grâce aux ordinateurs de Joël Armengaud (novembre 1996), de George Spence (août 1997), et de Roland Clarkson (janvier 1998). Ce dernier est un jeune étudiant de 19 ans dont l'ordinateur a découvert la primalité de  $M_{3021377}$ , un nombre de 909 526 chiffres.

### UN MÉCÈNE DONNE UN DEMI-MILLION DE DOLLARS

Ces premières découvertes furent faites uniquement pour la beauté de l'art, car c'est seulement en mars 1999 que le prix dont nous avons parlé a été créé par l'EFF. L'Electronic Frontier Foundation est une association de défense

et de promotion de l'utilisation de l'Internet. À la suite du don d'un mécène anonyme, un prix de 50 000 \$ (environ 300 000 F) a été promis au premier individu ou groupe qui découvrirait un nombre premier de plus d'un million de chiffres décimaux. C'est ce prix que N. Hajratwala vient de gagner ; 100 000 \$ récompenseront la découverte du premier nombre premier de plus de dix millions de chiffres décimaux, 150 000 \$ la découverte du premier nombre premier de plus de 100 millions de chiffres décimaux, et 250 000 \$ le premier nombre premier de plus d'un milliard de chiffres décimaux. Soit un total d'un demi-million de dollars si vous gagnez tous les prix d'un coup.

Les règles précises de ce concours sont intéressantes (démonstrations contrôlables, calculs reproductibles, publications reconnues, confirmations par des experts), car elles traduisent ce qu'on sait

aujourd'hui sur la génération des nombres premiers, sur les formules pour créer des nombres premiers et sur les preuves de primalité. Ces règles intéresseront les amateurs qui, persuadés d'avoir trouvé des résultats importants sur les nombres premiers, s'interrogent sur la façon de faire reconnaître et valider leurs découvertes.

Les organisateurs du concours demandent que tout prétendant à l'un des prix fournisse une définition précise du nombre gagnant : pas question de proposer un nombre en disant que c'est la solution d'un système de 100 équations compliquées, même si l'on précise lesquelles ! Le prétendant doit aussi indiquer la méthode de preuve qui assure la primalité du nombre proposé, laquelle doit pouvoir être mise en œuvre par d'autres chercheurs.

Les tests de primalité probabilistes (qui indiquent qu'un nombre est premier avec une probabilité de 99,99 pour cent, par

### 6. LA FORMULE DE MARCEL PAGNOL

En 1992, Jacqueline et Frédéric Pagnol ont publié le texte de notes inédites que leur époux et père, le grand écrivain Marcel Pagnol, avait laissées. L'ouvrage, paru aux Éditions Pastorelly, porte le titre paradoxal *Inédits* et contient quelques pages sur les nombres premiers que l'amateur de mathématiques qu'était Marcel Pagnol avait soigneusement conservées. L'éditeur, dans un court texte de présentation, précise que "le conteur merveilleux est aussi un mathématicien rigoureux qui s'attaque aux problèmes les plus ardu, tels que les nombres premiers". Conscient peut-être de ce que ses notes comportaient un aspect conjectural et risqué, Pagnol les avait gardées pour lui. Leur naïveté étonne et "nous fend le cœur". En voici le texte, qui m'a été signalé par Paul Perbost.

«Quoique je ne sois pas mathématicien, j'aime les chiffres et les nombres, et surtout les nombres premiers qui sont assez mystérieux. Je crois avoir trouvé une formule qui permet de fabriquer des nombres premiers : c'est la petite équation suivante.  $x$  et  $(x + 2)$  sont deux impairs consécutifs, comme 5 et 7 ou 17 et 19, etc.  $x + (x + 2) + x(x + 2)$  = premier ;  $(5 + 7) + (5 \times 7) = 47$ . C'est-à-dire que la somme de deux impairs consécutifs et de leur produit est un premier. Nous avons donc une formule qui nous permet de construire des nombres premiers, et un moyen très simple de confirmer l'exactitude de nos calculs.  $15 + 17 + 15 \times 17 = 287$  premier.»

Si Pagnol avait essayé 9 et 11, il aurait trouvé que  $9 + 11 + 9 \times 11 = 119 = 7 \times 17$ . Suivent d'autres exemples et calculs, où étrangement Marcel Pagnol semble prouver que, pour  $x = 55$ , le nombre obtenu par sa formule, 3 247, est premier alors que pourtant  $3\,247 = 17 \times 191$ . Pagnol entreprend de démontrer sa formule.

«Pourquoi la première formule, de deux impairs consécutifs, nous donne-t-elle des premiers, c'est-à-dire des nombres sans diviseurs ? C'est parce que la somme  $(5 + 7 = 12)$  est un nombre pair, et le produit est un impair  $(7 \times 5 = 35)$ . Chacun de ses nombres a son (ou ses) diviseur(s). Or, la somme refuse les diviseurs du produit, et le produit refuse les diviseurs de la somme, et le total des deux n'admet donc aucun diviseur ; c'est donc un nombre premier.»

Vous conviendrez que ce raisonnement laisse à désirer ! Le théorème que M. Pagnol propose est que, pour tout nombre  $n$ ,  $(2n - 1) + (2n + 1) + (2n + 1)(2n - 1) = 4n^2 + 4n - 1$  est premier. On sait prouver qu'aucun polynôme ne donne que des nombres premiers. Même sans contre-exemple, Pagnol, s'il avait connu ce résultat, aurait su que sa conjecture était fausse.

