Quadrature

Magazine de mathématiques pures et appliquées

"La mathématique ouvre plus d'une fenêtre sur plus d'un monde"

Oct 1993
70 F Belgique 650 FB.

Des Jeunes sur la Planète Maths

Congrès Mathématique Junior, Cité des Sciences et de l'Industrie, 6, 7, 8 Juillet 1992.

Quadrature

est édité par les

ÉDITIONS DU CHOIX
SARL au capital de 50 000 F
Boite Postale 129
95103 Argenteuil Cedex

tél. (1) 39 98 06 82
Fax : (1) 39 82 92 57

ISSN n° 1142-2785

Directeur de la Publication
Jean-Pierre Boudine

Rédacteur en Chef
Pierre Audin

Rédacteurs en Chef Adjoints
Robert Férréol et René Veillet

Comité de Rédaction
Pierre Audin, Gil Pagès
Jean-Pierre Boudine,
Francis Casiro, Joseph Césaro
Robert Férréol, René Veillet.

Maquette-PAO
Yamina Dumoutier

Gestion-abonnements
Malika Hameurlain

Promotion et Publicité
Houria Boukouiren

Quadrature est imprimé chez
BERGER-LEVRAULT
Route de Villay Saint-Etienne
ZI Croix de Metz 54200 TOUL

Adresse (courrier, abonnement) :
« Quadrature »
Éditions du Choix
B.P. 129
Argenteuil Cedex 95103

Bimestriel N° 16 Sept.-Oct. 1993
France : 40 Frs. Belgique : 290 FB.
Suisse : 12 F

ÉDITO

par Jean-Pierre Boudine

Le Congrès Mathématique Junior fut un moment exceptionnel de la vie mathématique, s'il faut englober sous ce terme également un aspect populaire des mathématiques. Quadrature, partenaire du CMJ et du "Kangourou", lui-même intégré au CMJ, publie une première partie des documents, un second numéro consacré au CMJ paraîtra au printemps 94.

Nous espérons que nos lecteurs, et les enseignants des lycées et des collèges auxquels ce numéro est adressé, apprécieront tant les contributions des mathématiciens que celles des jeunes. **Nous avons voulu que ce numéro puisse être un OUTIL pour la classe, donne un ensemble de PISTES, de suggestions, d'IDEES à creuser. A vous de nous dire si ce pari est gagné.**

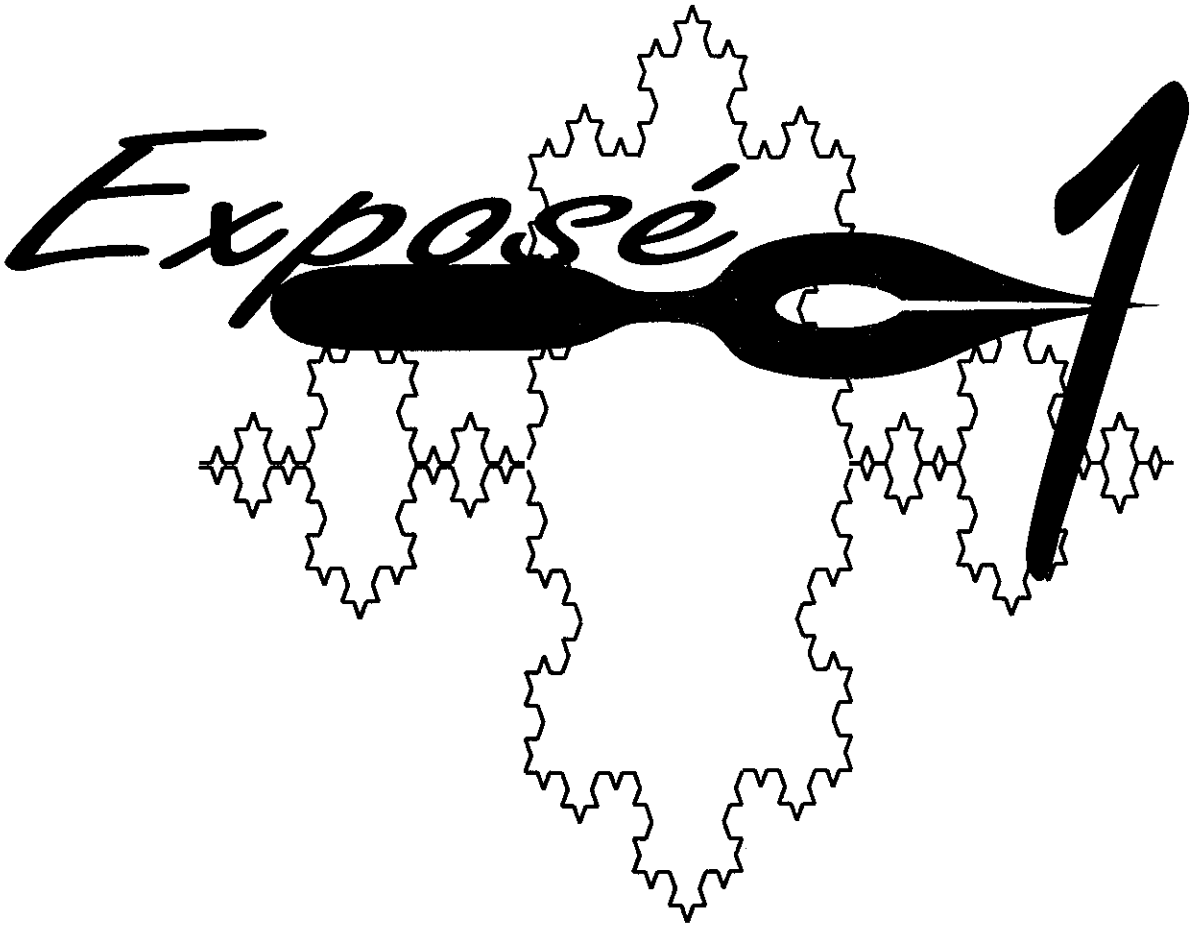
L'évènement CMJ a fait découvrir à des jeunes que les chercheurs en mathématiques existent, vivent, cherchent, sèchent et parfois trouvent ... des choses qui les passionnent. Il a également fait progresser au sein de la communauté mathématique l'idée que les lycéens, même ceux qui n'intégreront jamais Normale Sup, existent mathématiquement parlant, et qu'un effort de la part des professionnels pour propager la mathématique comme dimension culturelle, un tel effort a un sens. Cette seconde prise de conscience n'est plus aisée, ni moins importante que la première. Que cette mathématique "culturelle et populaire" soit dans l'air du temps est confirmé par deux bonnes nouvelles.

La constitution cet été de l'association **"Math pour Tous"**, qui réunit déjà Christian Mauduit et Pierre Duchet, chercheurs ; Jean Pierre Boudine et Maurice Glaymann, enseignants et éditeurs ; Pierre Audin, du département de mathématiques du Palais de la Découverte ; Michèle Chouchan, productrice d'émissions à France Culture. Cette association réunit du même coup des animateurs de "Maths en Jeans" et du "Kangourou des Lycées".

Seconde nouvelle : la mise en chantier d'un numéro commun "Quadrature"-"Gazette des Mathématiciens" sur la saga séculaire du théorème de Fermat-Willes. Ce numéro paraitra vers Février, le temps que les spécialistes du monde entier aient levé les derniers doutes*.

Le numéro 17 de "Quadrature" paraîtra quinze jours après celui-ci, c'est à dire dans les premiers jours de novembre, avec les rubriques habituelles et les énoncés du Championnat de France des Jeux Mathématiques et Logiques.

* Didier Nordon nous communique à l'instant une nouvelle qui va faire du bruit. Un mathématicien bordelais aurait démontré ***la réciproque du théorème de Fermat !***



NOMBRES PREMIERS ET CODES SECRETS

par **Jean-Louis NICOLAS**

(Université Claude Bernard, Lyon 1)

NOTES PRISES PENDANT L'EXPOSÉ
DE JEAN-LOUIS NICOLAS
CONGRES MATHÉMATIQUES JUNIOR 7-9 JUILLET 1993

(Les encadrés reprennent les transparents qui étaient projetés, le texte résume le commentaire oral.)

I

$2^{756839} - 1$

est un nombre premier

(Slowinski, mars 1992)

En mars 1992, il a été annoncé à la radio un record : le plus grand nombre premier connu à ce jour est $2^{756839} - 1$ (Slowinski).

Comment faire la "carte d'identité" de ce nombre, qui est beaucoup trop grand pour pouvoir être affiché sur un écran de calculatrice ?

a) On peut se demander tout d'abord combien il a de chiffres.
Il suffit pour le savoir d'avoir à sa disposition une calculette. L'utilisation des logarithmes décimaux permet alors de montrer qu'il a 227 832 chiffres. Il faut tout un cahier pour l'écrire !!

b) L'utilisation de la fonction 10^x sur la calculette montre alors que **ce nombre commence par 1741...**

c) En base 2, il s'écrit :

$$\underbrace{111\ldots111}_{\text{756 839 fois}}$$

Sur la calculette, on fait :

	2
$\log_{10}$	0,3010299957
x	756839
=	227831,240888
−	227831
=	0,240888
10^x	1,741

On en déduit :

Si	$10^n \leq x < 10^{n+1}$
alors x a $(n+1)$ chiffres et	$n \leq \log_{10} x < n+1$
Notre nombre a	227 832 chiffres
Il commence par	1741 ....
En base 2 :	$2^3 = 1000$
	$2^3 - 1 = 111$

$2^{756839} - 1 = \underbrace{111\ldots.111}_{\text{756 839 fois}}$

d) Comment se termine ce nombre ?

Examinons les puissances de 2 successives. Leur chiffre terminal est 2, puis 4, 8, 6, 2, 4, 8, 6 etc…

Il dépend du reste de la division de l'exposant considéré par 4.

Le reste de la division par 4 de 756839 est 3 : on en déduit que 2^{756839} se termine par 8, donc notre nombre par 7.

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 32$
$2^6 = 64$
$2^7 = 128$
$2^8 = 256$
$2^9 = 512$
$2^{10} = 1\,024$

Si le reste de la division de a par 4 vaut :

	Alors, 2^a se termine par :	
0		**6**
1		**2**
2		**4**
3		**8**

$756\,839 = 4 \times 189\,209 + 3$

2^{756839} **se termine par 8**

$2^{756839} - 1$ se termine par 7

En examinant de même **les deux derniers chiffres** des puissances successives de 2, on peut vérifier qu'ils forment une suite périodique de période 20, et le nombre considéré finit par 87.

Nous avons utilisé ici la notion de "congruence modulo 4" et de "congruence modulo 20", pour calculer ce nombre premier "modulo 10", puis "modulo 100".

$756\,839 = 20 \times 37\,841 + 10$

2756839 se termine par **88**

2756839 – 1 se termine par **87**.

a ≡ b *mod* c
signifie que
a – b* est un multiple de *c

Congruence :

a ≡ 3 *mod* 4 $\Rightarrow$

$2^a \equiv 8 \; mod \; 10$

a ≡ 19 *mod* 20 $\Rightarrow$

$2^a \equiv 88 \; mod \; 100$

Exercice :

Quel est le dernier chiffre de 4444^{4444} ?

e) Malheureusement, si on veut en savoir plus long, la méthode que nous avons utilisée ici est de plus en plus pénible à mettre en œuvre. Il nous faudrait un gros ordinateur ou … quelques astuces.

Si nous calculons 2^8 par la méthode la plus simple :

$2^8 = 2 \times 2 \times \ldots \times 2$

nous effectuons 7 multiplications.

Mais si nous remarquons que

$2^8 = ((2^2)^2)^2$,

3 multiplications suffisent.

De même 2^{1024} peut se calculer en 10 élévations au carré, au lieu de 1024 multiplications !

Calculer 2^8

1) $2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

7 multiplications

$((2^2)^2)^2$

2) $2^2 = 4$

$4^2 = 16$

$16^2 = 256$

3 multiplications

2^{1024} peut se calculer en 10 multiplications (car $1024 = 2^{10}$).

Nous donnons une recette pour le cas général, appliquée ici à 2^{13}

2^{13} ?

Recette :

1. Ecrire 13 en base 2

   1101

2. Supprimer le "1" à gauche

   101

3. Remplacer
   1 par CM
   0 par C

   CMCCM

4. On part de 2, on effectue les opérations à partir de la gauche

   C: élévation au carré

   M: multiplication par 2.

2 C 4 M 8 C 64 C 4096 M 8192 = 2^{13}

Coût : 5 multiplications.

En appliquant cette recette à notre nombre, en ne conservant jamais dans les calculs que les 5 derniers chiffres, on trouve qu'il finit par 77887.

1. Ecrire 756 839 en base 2 :

1011 1000 1100 0110 0111

2. Supprimer 1 à gauche et remplacer 1 par CM, 0 par C

CCMCMCMCCCCMCMCCCCMCMCCCMCMCM

On peut calculer 2^{756839} avec 29 multiplications :

19 élévations au carré

10 multiplications par 2.

On peut effectuer ces 29 opérations en ne gardant que les 5 derniers chiffres. On trouve que

2^{756839} se termine par 77888

Plus généralement, considérons les nombres premiers, c'est-à-dire les nombres qui ne peuvent pas s'écrire comme un produit de deux nombres distincts de 1.

Quelques mois auparavant, le plus grand nombre premier **connu** était $2^{216091} - 1$. Il a seulement 65 000 et quelques chiffres !! Et juste avant, c'était encore un "nombre de Mersenne", cad un nombre premier qui s'écrit comme une puissance de 2 moins 1.

Nombres premiers

$15 = 3 \times 5$

$18 = 2 \times 9 = 3 \times 6$

13 = premier

$1189 = 29 \times 41$

Un nombre premier ne peut pas s'écrire comme produit de deux nombres distincts de 1

La suite des nombres premiers est :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,...

$N = 2^{216091} - 1$ est premier

$216091 \times log_{10} 2 = 65049.8728$

N a donc 65 050 chiffres en base 10 et commence par : 746...

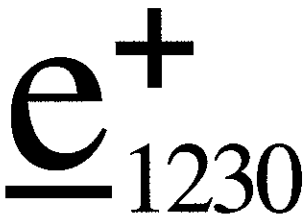
391 581 × 2216193 – 1 **était** le plus grand nombre premier connu **avant mars 1992** C'est un nombre de 65 087 chiffres.

On connaît aussi de grands nombres premiers qui ne sont pas de cette forme : François Morain, par exemple, en a mis en évidence qui utilisent les décimales de *e*.

Pour cela, il a utilisé un "test de primalité", dont la mise en œuvre a nécessité des mois de travail et un très gros équipement (voir page suivante, document).

RECORDS DU MONDE DE PRIMALITÉ

FRANÇOIS MORAIN



Le plus grand facteur de $\underline{e}_{1230} = [10^{1230} e]$ (e la base des logarithmes népériens) est le nombre

754303029791338134517381433347021810294210698365557503390117831041450906111370978319888497523424931994191079149763592952192861114029759295418690316968836371156903274031673971408062222127467101937180956121162746047313082134792001244323198169870261305902895579589998449330893899448466050875233161748222535644687914811516311397891889100659026507911395956027725171548499794413365082289655270132699533851789226855461196855636557918836543660622256307948413233838957174561685729796444985199569587648771904646229658834669901200886629913929291983063740965744342464647347590138494859167785575750488734063410308883597332419905663540800779180305887903445481152574071158220232256277043463711094634995478808204095684487654162158069528509268788906048613001598063736693634317287421423141473474775486262573562262257360145412593302079584277914615594000339520614089459420770710476225494454048512727255215020420365374941543314492830718226116589867672200993659582755237953096753452615328986524876252775401800620391126769767833278292292208593061856453246049344706635769479840604209693659848427368912608164303280787110155886911794976571752000574860728692251069376868083488226018552935140764198810330147899544759266784038897649411908770991935237731

C'est un nombre **premier** de 1226 chiffres. Il n'a aucune propriété arithmétyique connue (ce n'est pas un nombre de Mersenne de la forme $2^p - 1$). Il a fallu 668 jours de temps équivalent SUN 3/60 pour en apporter la preuve, au moyen d'un programme écrit en Le_Lisp distribué entre une dizaine de stations de travail.

NOUVEAU RECORD EN DATE DU 19 AVRIL 1992.

245030218166453241586653241796461975384627230976746458684591248743748581384002301352181805277576961291235683111871571660417804143817845721047276545995712704881096332032903878047988248512844759208219761951024171234890906403927596839807482870832385624893921029384020470516298025875562603401744997585575471842397648827730460896016800508609297909174830858718206013209730869624891139286445460936107665107298438697537471810966883507437388091781208582616088902793837373102135204614627267568562301640307032815666910895676449803788141358349255178436607536596797766157896130448972895400822750929734427548519945650982513712846849548361473714710810013241119841398754433583917904242256809956926221147092967093505158336515344702825237094130396201592407154762214097234736192190122974875445475142203956163281874971191803546832518726750524794962016741636277189648947252893920539079755976572034031744030876393778831042834902107420321651585457788763222561540274512040504905499022719037059978986501498612953829870818210683461366143578033780941241395196861157894489262348905813071530675853344888595111712454112635599660152621595475260097423037575032985303439306439049484140343303578814558723684565658676891157152450834587281950736408650565624029896764690961808039138414799325188733456170104505682313894519405341289565583843877366332638100795674477194623397417424644012653711368557474907104845961637261891518490549214463705229622317803178231882996339425839348460674803561849737412599491776046036173899258112891555242329659043 73

Cet entier se note $p_{1840926}$. Il représente le nombre de façons d'écrire 1840926 comme somme d'entiers positifs. A titre d'exemple, $p_5 = 7$ car 5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1.
C'est un nombre **premier** de 1505 chiffres. Il a fallu 4 ans de temps équivalent SUN 3/60 pour en apporter la preuve, au moyen de programmes écris en Le_Lisp et Verb+C+, distribués entre une vingtaine de stations de travail. *Le record date du 19 avril 1992.*

A quoi servent donc ces grands nombres premiers ?

Il y a quelques années seulement, les scientifiques se sont aperçu que ces nombres ne sont pas seulement un amusement pour matheux, en commençant à les utiliser pour des problèmes de cryptographie : il s'agit d'envoyer des messages codés, d'utiliser une carte bancaire sans risque etc...

Pour coder avec facilité un message, on peut par exemple effectuer une permutation circulaire des lettres de l'alphabet. On peut alors, pour faciliter le décodage, calculer le nombre d'apparitions de chaque lettre (e est la lettre la plus fréquente en français) : cette méthode n'est pas du tout sûre.

A L L E Z A L A V I L L E T T E
1 2 3
S I V O U S P A S S E Z P A R L A
4
C A S E D E P A R T R E C E V E Z
5 6 7 8 9
V I N G T M I L L E F R A N C S
10

E	= 10	A	=	L	=	S	=
Z	=	V	=	I	=	T	=
P	=	R	=	C	=	N	=
O	=	U	=	D	=	G	=
M	=	F	=				

CNNGB C NC
XKNNGVVG UK XQWU
RCUUGB RCT NC
ECUG FGRCTV
TGEGXGB XKPIV
OKNNG HTCPEU

Nombres d'occurences :

G : 10	C : 9	N : 8	U : 6
B : 4	X : 4	K : 4	V : 4
R : 3	T : 3	E : 3	P : 2
Q : 1	W : 1	F : 1	I : 1
O : 1	H : 1		**Total 66**

Il existe une méthode bien plus sophistiquée, qui utilise la propriété suivante : si un nombre n est égal au produit de nombres premiers p et q "grands", il est difficile de retrouver p et q à partir de n : dès que n a une centaine de chiffres, il faut plusieurs années sur ordinateur.

Choisissez deux nombres premiers $\boldsymbol{p}$ et $\boldsymbol{q}$.

Multipliez l'un par l'autre :

$$n = pq$$

Il est difficile, si $\boldsymbol{p}$ et $\boldsymbol{q}$ sont grands de retrouver $\boldsymbol{p}$ et $\boldsymbol{q}$ à partir de n.

Exemples : $n = 2759$

$n = 1\,657\,913$

Si n a plus de 150 chiffres, il est actuellement impossible de retrouver $\boldsymbol{p}$ et $\boldsymbol{q}$.

Cette idée est utilisée dans le système de cryptographie à clé publique "RSA".

Le système de cryptographie à clé publique R.S.A.

1. Choisir deux nombres premiers p et q de 100 chiffres environ
2. Calculer $n = pq$
3. Calculer $\varphi = (p-1)(q-1)$
4. Choisir d premier avec φ
5. Calculer e tel que $ed \equiv 1 \ mod \ \varphi$

n et e sont publics
p, q, φ, d sont secrets

Pour envoyer un message numérique M, on calcule

$$C \equiv M^e \ mod \ n$$

On envoie C qui est le message codé.
L'auteur du code calcule

$$M \equiv C^d \ mod \ n$$

Connaissant e,
calculer d est équivalent à factoriser n.

Com A.C.M. Février 1978