nombre, es-tu premier ?

une calculatrice programmable et un peu d'arithmétique donnent la réponse un jour de pluie

J'ai profité d'un jour de pluie pour montrer à papa, ingénieur retraité, passionné de jeux en général, mathématicien en particulier, ce qu'on peut faire avec une calculatrice (TI-59). En une vingtaine de minutes, il a compris les principes d'utilisation. En quelques heures, il a pu rédiger de petits programmes. Soudain, il s'est exclamé, en regardant, les yeux mi-clos, la fumée de sa cigarette :

« Mais alors, on peut déterminer rapidement si un nombre est premier ou non !

— Euh ! oui, pourquoi pas ?

— Allez, vas-y, fiston.

— Dans le fond, ce n'est pas difficile, il suffit de diviser ce nombre par la suite des entiers naturels à partir de 2 jusqu'à la racine carrée de ce nombre lui-même. »

Ainsi est né ce petit programme qui permet de déterminer si un nombre est premier ou de donner sa décomposition en une suite de facteurs.

Lorsqu'on considère un nombre entier (les mathématiciens disent un *entier naturel*), on peut dresser la liste de ses *diviseurs*. Par exemple, 6 a pour diviseurs les quatre nombres 1, 2, 3 et 6.

Un nombre qui n'admet pas d'autres diviseurs que lui-même et 1 est appelé un *nombre premier*. Ainsi, les nombres premiers sont 1, 2, 3, 5, 7, 11... Rechercher les diviseurs d'un nombre n, c'est trouver tous les nombres a tels que n/a soit un nombre entier.

Pour trouver si un nombre n est premier, il suffit donc de le diviser successivement par tous les nombres 2, 3, 4... n-1 et de voir si le quotient est, ou non, un nombre entier. Si aucune des divisions ne donne un quotient entier, c'est que le nombre est premier !

En fait, on démontre qu'il n'est pas besoin d'essayer chacune des n-2 valeurs 2, 3, ... n-1, et qu'il suffit d'essayer les nombres 2, 3, ... x où x est le plus petit entier tel que $x^2 > n$. Ainsi, pour 29, au lieu d'essayer 2, 3, 4... 28 (soit 27 divisions), il suffit d'essayer 2, 3, 4, 5 et 6 puisque $5^2 = 25 < 29$ et $6^2 = 36 > 29$. On ne fait donc que 5 divisions. (Approximativement, on fait $\sqrt{n}$ divisions au lieu de n).

Un raffinement supplémentaire consiste, après avoir vérifié en divisant par 2 que le nombre n'est pas pair, à ne diviser que par les nombres impairs compris entre 3 et x. Soit, pour 29 : 3 et 5. Ceci permet encore de diminuer de moitié le nombre de divisions.

Un dernier raffinement, enfin, consiste à diviser non pas par 2 puis

Séquences d'instructions

000	76	LBL	015	56	56	030	57	57	047	13	C	064	58	58	081	32	X:T
001	11	A	016	02	2	031	59	INT	048	43	RCL	065	43	RCL	082	43	RCL
002	99	PRT	017	42	STO	032	75	-	049	58	58	066	58	58	083	59	59
003	98	ADV	018	58	58	033	43	RCL	050	99	PRT	067	77	GE	084	67	EQ
004	98	ADV	019	61	GTO	034	57	57	051	43	RCL	068	17	B'	085	18	C'
005	98	ADV	020	16	A'	035	95	=	052	57	57	069	61	GTO	086	43	RCL
006	98	ADV	021	76	LBL	036	42	STO	053	42	STO	070	16	A'	087	59	59
007	98	ADV	022	16	A'	037	55	55	054	59	59	071	76	LBL	088	99	PRT
008	42	STO	023	43	RCL	038	25	CLR	055	61	GTO	072	18	C'	089	98	ADV
009	59	59	024	59	59	039	32	X:T	056	16	A'	073	98	ADV	090	98	ADV
010	34	FX	025	55	÷	040	43	RCL	057	76	LBL	074	98	ADV	091	98	ADV
011	85	+	026	43	RCL	041	55	55	058	12	B	075	98	ADV	092	91	R/S
012	01	1	027	58	58	042	67	EQ	059	43	RCL	076	98	ADV			
013	95	=	028	95	=	043	13	C	060	56	56	077	91	R/S			
014	42	STO	029	42	STO	044	61	GTO	061	32	X:T	078	76	LBL			
						045	12	B	062	01	1	079	17	B'			
						046	76	LBL	063	44	SUM	080	01	1			

les nombres impairs (soit les nombres 2, 3, 5, 7, 11, 13, 15, 17), mais par les nombres premiers successifs (soit 2, 3, 5, 7, 11, 13, 17...). Cette dernière méthode suppose, hélas, que l'on ait en mémoire le début de la liste des nombres premiers, jusqu'à la valeur x telle que $x^2 > n$.

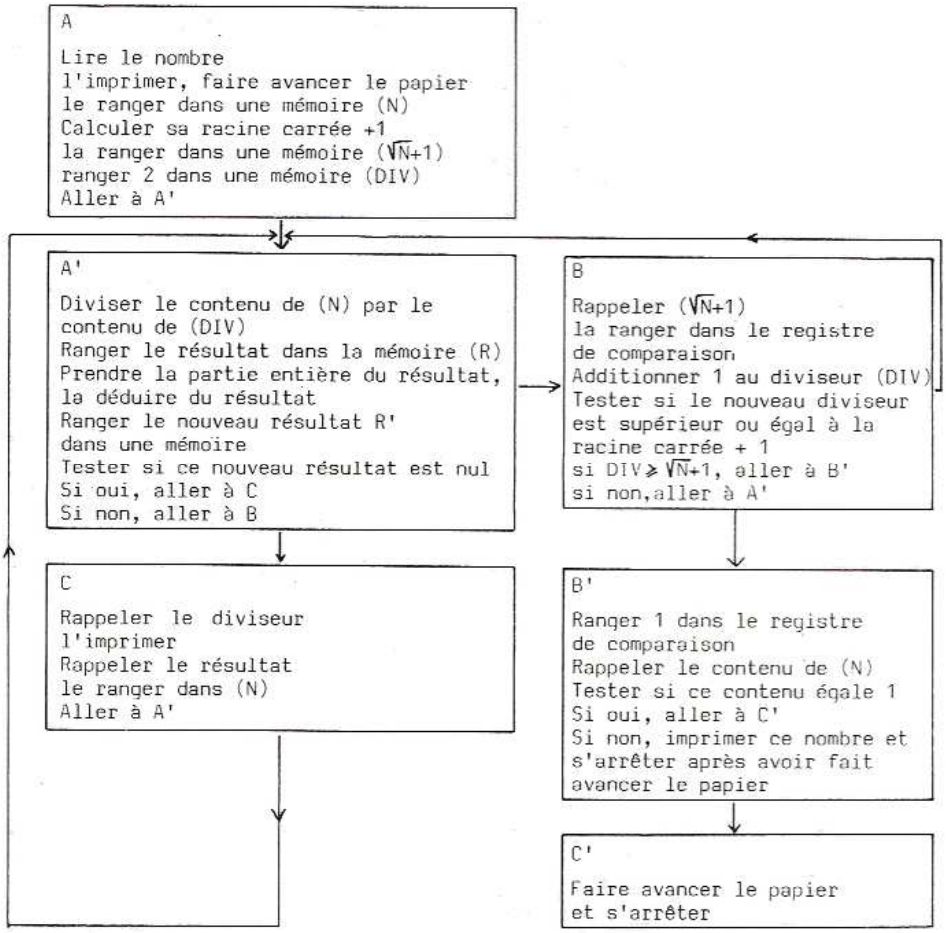
Le programme est assez simple

En établissant ce programme, nous n'avons pas cherché de finesse mathématique ; il existe probablement des approches, notamment probabilistes, plus élégantes ou plus rapides ; ceci étant dit, voyons quèl est l'organigramme et quelles sont les séquences de programmation.

Ce programme est un peu « brut de fonderie » ; nul doute qu'il soit susceptible d'amélioration ; notamment, on doit pouvoir gagner quelques instructions dans la séquence A' (instructions 36 à 41).

— Les *labels* utilisés sont : A, A', C, B, C' et B'.

— Les *mémoires* utilisées sont :
. mémoire n° 59 : N nombre introduit au départ, puis états successifs de ce nombre après ses divisions par des facteurs ;
. mémoire n° 58 : DIV diviseur : 2 au départ puis 3, 4, 5 etc. jusqu'à $\sqrt{n} = 1$;
. mémoire n° 57 : résultats successifs de la division de N par le diviseur ;
. mémoire n° 56 : n = 1 : cette expression ne change pas ;
. mémoire n° 55 : R' résultat de R moins la partie entière de R ; lorsque ce résultat est nul, ce que l'on teste, R est un nombre entier et DIV un facteur de division.



Marc Chernet