談　話　室

双児素数について*

奥川俊二**

本誌 Vol. 3 No. 3 および No. 5 に和田英一氏と石橋善弘氏が，e の計算について書いておられ，面白く読ませていただきました．当時1,000桁の計算時間の記録は9秒でしたが，その後次々と高速計算機が発表され，e の計算時間も随分短縮されました．たとえば，昨年秋京大工学部で完成しました小形研究用高速計算機 KT-P で，和田氏の方法でやりましたのが，e 1,000 桁が 1.62 秒，5,000 桁が 37.2 秒でした．

KT-P は 1024 語のコアメモリ（約10 μs）のほかに，128 語の薄膜メモリ（約1 μs）を持っていますが e の計算では，どうしてもコアの方も使用せざるを得ず，また1語 20 ビットですので，その高速性を十分発揮することができません．それに現在ではさらに 1,000 桁 0.41 秒という日本記録（この会誌がでる頃には，さらに速い記録がでているかもしれません）も生まれているそうですから，いまさら大きな顔もできません．そこで機械の長時間連続運転の際の安定性の試験をかねて，何か思白い，べら棒に時間のかかる計算はないものか，というので始めましたのが，ここに紹介させていただく双児素数さがしです．

整数論における素数は，古くより数学者の興味をよんだものですが，その概念は小学生にも十分理解できるほど至極簡単なものであるのに，証明は非常に難解なものが多く，何世紀にもわたって，最高の数学者によって解決への努力が続けられてきたにもかかわらず，意外に多くの，未解決の問題が残されています．たとえば双児素数（相隣る二つの奇数がともに素数であるもの），Mersenne の素数（素数 p について $M_p=2^p-1$ が素数であるもの），および Fermat の素数（自然数 m について $F_m=2^{2^m}+1$ が素数であるもの）が無限に存在するかどうかは，未解決です（周知のように素数が無限に存在することは2,000年以上前に，ユークリッドによって証明されています）．

Lehmer の素数表は 10^7 余りまでありますが，その終りの方に，(10001441, 10001443) なる双児素数がみられます（現在では 10^8 ぐらいまでの素数表ができているそうです）．Mersenne および Fermat の素数については，特にアメリカで最近高速計算機を使って，盛んに追求されているらしく，最近の Mathematics of Computation 誌に，その結果が次々と発表されています．

Mersenne の素数については従来知られていた 20 個のほかに，最近イリノイ大学の新しい計算機 Illiac II により，M_{9689}, M_{9941}, M_{11213} の3個が発見され（これは本誌 Vol. 4 No. 5 のニュース欄にも紹介されています），演算時間はそれぞれ，83分，90分，135分であったそうです．判定法は Lucas-Lehmer Test によりますが，これは「$S_{n+1}=S_n^2-2$ ($S_1=4$) によって順次 S を計算して，$S_{p-1}\equiv 0$ (Mod. M_p) ならば，その時に限り $M_p=2^p-1$ は素数である」というもので，$S_1=10$ でもよいそうです．

Fermat の素数についても，特別の判定法があり，従来知られていた F_0, F_1, F_2, F_3, F_4 のほかに最近計算機によって，F_{10}, F_{16} の2個が発見されているそうですが，F_{17} が素数かどうかを完全に test するには，IBM 7090 でぶっ続けで計算して 128 週間かかるだろうということです（Mathematics of Computation Vol. 18 No. 85）．双子素数についての試みはまだあまり耳にしませんので，その分布，素数に対する割合などを，KT-P の2語長で扱える 10^{12} 余りまでについて調べてみよう，と思いたちました．なんだ 10^{12} ぐらいと思われる方もあるかもしれません．たしかに，Illiac II の発見した M_{11213} は 10^{3000} 以上ですから，それと比較すれば全く微々たるものです．

しかし双児素数については，何らの法則もわかっていないようですから，特別の判定法もなく，したがって結局素数表作りとほとんど同じ時間がかかることになります．普通 N が素数であることを test するには，$\sqrt{N}$ を越えないすべての素数で割る必要があります（何かもっと早い判定法を御存知の方がありましたら，

* On Twin Prime Numbers, by Syunji Okugawa (Faculty of Engineering, Kyoto University)
** 京都大学工学部数理工学教室

教えて下さい). 10^{12} 辺りまでですと，10^6 までの素数は 78,498 個ありますから，80 K ぐらいの容量の高速メモリを持つ計算機が必要です．現実は残念ながらほど遠いものですから，苦しいやりくりをしてプログラムで細工しても，かえって遅くなるので馬鹿正直に全奇数で割っていき，商≦除数となるまで続けることにしました．

プログラムは簡単そのものですから，十分薄膜メモリにおさまります．素数表を store できる場合に比して，約6倍の時間がかかりますが，ない袖はふれませんから仕方がありません．このようにして 10^{12} 近辺の素数の場合には約 50 万回ループをまわりますから，判定に約70秒を要します．

10^6 までの全分布を求めるのは至極容易です(プリント時間も含めて1.3時間) が，10^6 以上はもちろんごく一部分しか調べていません．といいますのは，10^{12} 余りまでの全区間の分布を調べるとすると，80 K の容量の高速メモリを持っていても，実に1万年以上かかることになり (10^{12}～$10^{12}+10^4$ の区間だけで，8時間2分を要しました)，クロック 1,000 Mc，メモリサイクル数十ns の超高速計算機でも，100年ぐらいかかることになるでしょうから，分布の様子を 10^3 ごとの区間について示したのが，**第1表**です．たとえば，

第 1 表

	1	1000	2000	3000	4000	5000	6000	7000	8000	9000
1	168 35	135 26	127 20.5	120 21.5	119 23	114 17	117 19	107 13	110 14.5	112 15.5
10^3	81 6	93 9.5	87 12.5	80 10	91 11	82 5	92 14	76 5	91 12	88 11
10^4	75 11	77 6	81 9	72 9	63 4	73 9	82 11	76 7	79 10	75 8
10^7	61 4	60 7	66 8	60 3	58 7	71 7	59 3	60 8	54 2	65 6
10^8	54 5	56 4	57 6	55 3	57 7	61 8	57 7	56 6	47 2	51 2
10^9	49 3	50 4	35 2	58 4	50 5	52 2	44 4	50 2	46 2	53 3
10^{10}	44 2	42 0	40 0	40 4	38 0	32 3	45 1	40 1	35 1	50 2
10^{11}	47 1	41 3	39 4	38 3	35 1	47 3	36 3	34 2	40 2	36 1
10^{12}	37 4	33 2	33 0	35 2	40 2	32 3	37 2	28 2	33 1	27 2

10^{12}～$10^{12}+10^3$ の区間には，素数 37 個のうち4組の双児素数があります．表中，双児素数の組数が9.5のようになっているのは，(101999, 102001) のように区間にまたがったものを示しています．

第2表に 10^{11}～$10^{11}+10^4$，および 10^{12}～$10^{12}+10^4$ の区間の双児素数を示します．なおこの区間を探すのにそれぞれ，3時間25分，8時間2分を要しました．表中，線で囲んだところは，2組の双児素数が続いているもので，10の区間にこれ以上素数が密集することは絶対にないわけであり，非常に珍しいものです．以上の結果からは，10^{12} あたりまでにはまだまだ相当な割

第 2 表

10^{11}～$10^{11}+10^4$		10^{12}～$10^{12}+10^4$	
100000000817	100000000819	1000000000061	1000000000063
100000001237	100000001239	1000000000331	1000000000333
100000001837	100000001839	1000000000787	1000000000789
100000001921	100000001923	1000000000931	1000000000933
100000002059	100000002061	1000000001261	1000000001263
100000002497	100000002499	1000000001771	1000000001773
100000002911	100000002913	1000000003799	1000000003801
100000002941	100000002943	1000000003841	1000000003843
100000003067	100000003069	1000000004681	1000000004683
100000003379	100000003381	1000000004891	1000000004893
100000003757	100000003759	1000000005077	1000000005079
100000004987	100000004989	1000000005647	1000000005649
100000005431	100000005433	1000000005707	1000000005709
100000005671	100000005673	1000000006457	1000000006459
100000005881	100000005883	1000000006769	1000000006771
100000006037	100000006039	1000000007507	1000000007509
100000006277	100000006279	1000000007519	1000000007521
100000006409	100000006411	1000000008101	1000000008103
100000007531	100000007533	1000000009499	1000000009501
100000007537	100000007539	1000000009649	1000000009651
100000008209	100000008211		
100000008737	100000008739		
100000009397	100000009399		

合で，双児素数が存在することだけはわかりました．もちろんこれだけでは，その分布の法則などをみつけるなどということは不可能です．

なお補足ですが，整数論ではこのほかに未解決の問題として，Goldbach および Euler の予想として有名な「4以上のすべての偶数は二つの素数の和で表わせる．したがってまた，5以上の奇数はすべて三つの素数の和として表わせる」というのがあり，これは 9×10^5 まで成立することは実証されているそうですが，Vinogradov によって「ある大きな数 C より大きいすべての奇数は，三つの素数の和で表わせる．C は十分に大きな数である」ということは証明されていますが，まだ完全にこの予想は証明されていないそうです．今回みつかった一番大きな双児素数の近辺での，素因数分解および素数和分解（仮りにこう名づけます）の結果を**第3表**に示します．もちろん素数和分解は素因数分解のように一意性は持っていません．

たとえば偶数の場合，2組の双児素数を $(2n-1,$

第 3 表

1000000009640	$2^3 \cdot 5 \cdot 2243 \cdot 11145787$	13+1000000009627
1000000009641	$3 \cdot 61 \cdot 157 \cdot 1153 \cdot 30187$	3+11+1000000009627
1000000009642	$2 \cdot 571 \cdot 875656751$	3+1000000009639
1000000009643	$17 \cdot 647 \cdot 90917357$	3+13+1000000009627
1000000009644	$2^2 \cdot 3 \cdot 80221 \cdot 1038797$	5+1000000009639
1000000009645	$5 \cdot 7 \cdot 13 \cdot 19 \cdot 5273 \cdot 21937$	5+13+1000000009627
1000000009646	$2 \cdot 11 \cdot 45454545893$	7+1000000009639
1000000009647	$3^2 \cdot 23 \cdot 4830917921$	3+51000000009639
1000000009648	$2^4 \cdot 127 \cdot 223 \cdot 2206843$	149+1000000009499
1000000009649	1000000009649	3+7+1000000009639
1000000009650	$2 \cdot 3 \cdot 5^2 \cdot 47 \cdot 97 \cdot 439 \cdot 3331$	11+1000000009639
1000000009651	1000000009651	3+149+1000000009499
1000000009652	$2^2 \cdot 7 \cdot 3514286059$	3+1000000009649
1000000009653	$3 \cdot 333333336551$	3+11+1000000009639
1000000009654	$2 \cdot 43 \cdot 59 \cdot 739 \cdot 266689$	3+1000000009651
1000000009655	$5 \cdot 233 \cdot 858369107$	3+13+1000000009639
1000000009656	$2^3 \cdot 3^2 \cdot 37 \cdot 271 \cdot 1385149$	5+1000000009651
1000000009657	$11 \cdot 197 \cdot 461467471$	3+5+1000000009649
1000000009658	$2 \cdot 13 \cdot 41 \cdot 938086313$	7+1000000009651
1000000009659	$3 \cdot 7 \cdot 47619048079$	3+5+1000000009651

$2n+1)$, $(2m-1, 2m+1)$ としますと，$2(m+n)$ は $(2n-1)+(2m+1)$ とも $(2n+1)+(2m-1)$ とも表わせるからです（ここにも双児素数が関係します）．偶数の素数和分解は，やはり順次素数を引いてみて，残りが素数になるかどうかを調べるという，至極幼稚な方法しか仕方がないようです．第3表に示した例は幸いすぐ見つかったからよかったですが，もし 5×10^{11} 近辺の二つの素数の和としてしか表わせない数だと，一体どのくらいの計算時間が必要か，ちょっと見当もつかないくらいです．

以上馬鹿げた計算の一例をお話ししました．素数計算は，その実用的意味は一応論外として，最も時間のかかる計算の一つであり，高速計算機によって，可能となったものです．なお，以上の計算はすべて，同じ計算を二回行ない，その結果の一致を確認しました．そもそもこの馬鹿げた計算は，最初にふれましたように，機械の長時間連続運転の際の安定度の試験という，錦の御旗の下に行なったものであり，その目的は十分に果たすことができたようです．

（昭和39年4月13日受付）