Zimmermann の GMP-ECMによる 円分数の素因子分解の報告

宮 本 泉
山梨大学 工学部
izumi@esi.yamanashi.ac.jp

群計算を中心とする代数的数式処理ソフトウェアパッケージ GAP[5] のシェアパッケージ ParGAP (Parallel GAP/MPI)[3] を使用した並列/分散計算実験により、楕円曲線法による整数の素因数分解で新記録の結果が得られました。実験環境は、筆者の所属するコンピュータ・メディア工学科の教育用パソコン 75 台です。授業・演習で学生が使用するのが用途ですから、重たいプロセスが長時間走っていることは稀で、プロセスの優先度を十分下げても並列計算実験をすることは可能ですが、もちろん本来の使用目的の妨げにならないように注意して使用する必要があります。また、その様な環境ですから、普通の 100BaseLAN の通信網である上に、学生の使用状況によってネットワークが不安定な状態になることも考えられます。実際、本実験では、小さい場合の問題を使った試行実験では計算が完了しても、本来の目的のための実験では、原因を特定できないまま、途中でプロセスが死んでしまった場合が多々ありました。さらに、セキュリティを考慮すると、ネットワークによる接続には障壁を高くしておかなければなりません。しかし、これはネットワークを利用した並列計算には困難をもたらします。コンピュータシステムを設計した業者が設定して、学科のシステム管理者も認識していない障壁も中にはあったようです。

並列計算の場合は、通常、通信が安定していて切れないことが前提条件となりますが、本環境ではそれは保証されません。しかし、多くのコンピュータ設備は、上に述べたような状況になっていると思います。したがって、本実験の目的は、このような一般的な状況で行う並列/分散計算の経過の報告とそのような状況に対処する工夫の紹介、適した並列アルゴリズムの研究にあります。実験にあたっては、計算機システムの目的を考えて、システム管理者に本実験のために便宜を図ることは依頼しないようにしました。

使用しているパソコンは Pentium III, 800MHz, Memory 256MB, OS は Linux です。プロセスの実行には、計算時間の限度が CPU time で 60 分、使用可能メモリ 100MB の制約がありましたが、これはユーザーで変更可能でしたので、計算時間の限度は適宜延長しました。メモリに関しては、X Window System 関係で半分近

くが常時使用されていますので、増やすことは実際的に無理なばかりかでなく、むしろ、自粛して使用する必要があると思われます。

1　楕円曲線法による素因数分解

楕円曲線 $y^2 = x^3 + ax + b$ を利用した整数の素因数分解法で、曲線の係数を変えて何回も素因数分解を試みる方法です。使用した Zimmermann の GMP-ECM[7] では、計算の効率化のため楕円曲線は、$by^2 = x^3 + ax^2 + x$ を使用しています。まだわからない素因数を法として考えた曲線上の点の成す群の位数が適当に bound1 として定めた数以下の素数および素数ベキの積であることを期待します。この bound1 を大きくとれば分解の成功する確率は高くなりますが、計算時間およびメモリー使用量も増えます。アルゴリズムはもう少し工夫されていて、通常 bound1 の 100 倍程度の大きさの bound2 を設定して、上の素数および素数ベキの積に bound1 から bound2 までの間の一つの素数をかけた数までの位数で計算します。この bound2 は、特に設定しなくても、楕円曲線法の分解プログラムが bound1 から適当に定めてくれます。bound1 は上のことを考慮して適当に定めれば、毎回変える必要はありません。曲線の係数はプログラムが乱数で定めますので、毎回同じ入力で計算をすることになります。

したがって、並列/分散計算をするまでもなく、それぞれのマシンで繰返し計算するシェルプログラムをバックグラウンドで動かしておけば良いのですが、(75 台のマシンでこの様に実行することが現実的かどうかは別として) 一般的計算機システムにおける並列計算の実験用問題として、各マシンに計算実行の指令を出す、各マシンから計算結果を受取る、素因数分解が成功していれば計算は終了、失敗の場合は再度、計算実行の指令を出す、という方法で行いました。具体的には、ParGAP[3] をインタフェースとして使用し、各マシンで GMP-ECM[7] を起動させるという方法で行ないました。また、このとき、出力も簡単な計算データのメッセージに、成功したときには因数が追加されるだけですので、通信への負荷は非常に軽くなっています。

メモリを自粛して使用する必要があることから、計算実験の終りの方では GMP-ECM のプログラムでメモリの使用が大きくなる一ヶ所を繰返し計算するように書換えて使用しました。

2　計算実験

素因数分解した整数に関するデータは、下にまとめた通りです。楕円曲線法では、分解の困難さは素因数の大きさによります。楕円曲線法による素因数分解記録では、ここで得られた 10 進 55 桁の素因数は、約 2 年ぶりに前の記録を越える新記録になりました (cf. [1])。

素因数分解した整数 (112 桁)

```
(629^59 - 1)/(628 * 365377296628421249503829 71
                                    * 13274814114538692574828847)
```

素因数 (55 桁)

```
72308801275268216939250595089720829527021330045523462 81
```

商 (57 桁)

```
599055788512257114593036852972837566170071937294830361923
```

実験時間

```
trial * time : 約 28000 曲線 * 55 CPU-min = 1000 CPU-days
                                        (1000/75 = 約 2 週間)(合計)
```

```
Bound1=45,000,000
sigma=267937500 (係数のための乱数の値)
```

注: 素因数分解した整数は三島さんのホームページ [6] の cyclotomic number からです。what's new / history / errata (August 19, 2001)
(59 629 (13274814114538692574828847)(C 138))By Masaki Ukai(August03,2001)

以下のデータは、P. Zimmermann に計算していただきました。

```
Group order = 2^10*3*13*103*151*1123*12619*15649*26249*404197
              *4742809*25268183*41286269351
        = 72308801275268216939250595125167554207112832071145584 64
Distance = 3544672468009150202562212183
P-1 =2^3*3*5*7^2*11*59*12451*54469849267*382541885447633
                                        *73034782187622411 79
P+1 =2*123661*5865679*4984368234991696091660199134866334322464839
```

なを、この方面の記録としては、一番強力と考えられている Special Number Field Sieve 法を使った Cabal グループによる 233 桁の分解 [2] で、2000 年 11 月に、総計約 2 万 CPU-time の計算で得られた結果があります。楕円曲線法による伊豆さんの結果もあります (cf.[1])。

毎回の計算の概要は下のようになりましたが、まとめると、計算時間や使用メモリーに制限のあることを知らずに bound の設定を大きくしすぎた失敗計算約 40,000 回の後に、約 28,000 回の計算で素因数分解に成功しました。この計算回数は並列計算で行った楕円曲線法素因数分解の計算回数の合計であって、下に報告するように、並列計算は何回も途中で止まってしまい、正常に終了することは稀でした。なを、bound1 が 45,000,000 のときは、約 75,000 曲線の計算で確率 50%で素因数分解されることを、R. Brent に教えていただきました。彼のホームページ [1] に、これに関する記述があります。

開始時間	終了時間	
Thu Aug 23 14:19:54 JST 2001	Thu Aug 23 16:44:08 JST	(約 1 時間 20 分)

Limit1(=Bound1):=100,000,000; Curves:=150(計算する曲線数); (正常終了)
Curve no. 34 failed UNIX_time : 3601 (秒　実時間)
Curve no. 5 failed UNIX_time : 3602
Curve no. 11 failed UNIX_time : 3601
....
Curve no. 149 failed UNIX_time : 3713
Curve no. 150 failed UNIX_time : 3624 (最後の曲線)
Curve no. 146 failed UNIX_time : 4903

Thu Aug 23 20:01:23 JST 2001 Aug 25 00:19 (約 24 時間)
Limit1:=100,000,000; Curves:=15,000;
....
Curve no. 2071 failed UNIX_time : 3602
Curve no. 2072 failed UNIX_time : 3602 (約 2000 曲線の計算で途中終了)

以下、同様に、Limit1:=100,000,000; Curves:=15,000; の入力に途中終了。
Sat Aug 25 10:35:18 JST 2001 Aug 27 12:53 (約 50 時間 20 分)
Tue Aug 28 10:46:50 JST 2001 Sep 3 16:04 (約 6 日 5 時間 20 分)
Mon Sep 3 19:32:56 JST 2001 Sep 4 05:46 (約 9 時間)
(出力テスト)Tue Sep 4 18:56:21 JST 2001
                                    Tue Sep 4 19:56:24 JST 2001
  その後の実験も、Limit1:=120,000,000 など大きすぎて失敗計算
Tue Sep 4 20:27:27 JST 2001 Wed Sep 12 15:57:35 JST 2001
....   (計算トラブル?、正常終了) (約 7 日 19 時間 30 分)
Thu Sep 13 10:24:35 JST 2001 Sep 17 21:56 (約 4 日 11 時間 20 分)
Tue Sep 18 19:31:39 JST 2001   Sep 18 19:55 ?? (約 25 分)
Tue Sep 18 20:09:38 JST 2001 Thu Sep 20 16:06:03 JST 2001
....   (約 1 日 20 時間) (計算トラブル、正常終了)
Curve no. 24000 failed by 57 crux10 UNIX_time : 0 14:38:25
Thu Sep 20 20:07:50 JST 2001   Sep 21 11:13 (約 15 時間)

以上の約 40,000 curves では、時間超過で毎回の楕円曲線法の計算が途中 1 時間で打ち切りになっていた。Limit1(=B1) が大き過ぎた。 その他の障害もあり、計算が完了できたのは、下の約 28,000 curves。

Fri Sep 21 11:27:22 JST 2001 Sep 25 18:04 (約 4 日 6 時間 30 分)
Limit1:=40,000,000;
Tue Sep 25 18:14:43 JST 2001 Oct 6 05:22 (約 10 日 11 時間)
Limit1:=45,000,000;
Sat Oct 6 11:54:11 JST 2001 Sat Oct 6 16:52:25 JST 2001 (約 5 時間)

..... (正常終了)

```
[ 278 (Curve no.),
"GMP-ECM 4c-m0, by P. Zimmermann (Inria), 16 Dec 1999, with contri\
butions from T. Granlund, P. Leyland, C. Curry, A. Stuebinger, G. \
Woltman, JC. Meyrignac, A. Yamasaki, and the invaluable help from \
P.L. Montgomery. Input number is 433170059643319045108479137066914\
324703799675942540484239636962663651858901540191436138776045066795\
7626053058363 (112 digits) Using B1=45000000, B2=43295692440, poly\
nomial x^1, sigma=267937500 Step 1 took 2603480ms for 589347784 mu\
ls, 3 gcdexts Step 2 took 973400ms for 269164894 muls, 186285 gcde\
xts ********** Factor found in step 2: 72308801275268216939250595089720829527021330045523462 81Found probable prime factor of 55 digi\
ts: 7230880127526821693925059508972082952702133004552346281 Report\
 your potential champion to Richard Brent <rpb@comlab.ox.ac.uk> (s\
ee ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richardo.Bre\
nt/champs.txt) Probable prime cofactor 599055788512257114593036852\
9728375661700719372948303619 23 has 57 digits " ]
```

楕円曲線法の困難さは得られる素因数の大きさに依存し、Sieve法の困難さは分解する整数の大きさに依存します。今回、分解した整数は112桁ですからSieve法でする方が簡単と思われます。終りに、楕円曲線法の方が楽な例の並列計算結果を報告します。Bound1 = 45,000,000で行いました。

例 ：193桁の数の素因数分解 (Cunningham tables[4] Page 87 より)

```
4666  2,2358M c231 29853437573848018732367754264926734261. c193
 by Zimmermann ECMNET

c193
459570757140559336797736836413018674283232477227786312350853020494\
374889951517849663270624940783204709660545530008698993668624410557\
683958006907593169850423558081694711739629444547591759724777 3
```

得られた素因数

p1=1126022037855281940233176930855453903879451041 (46桁, 193桁から)

p2=5140853648305217410902915102611320468253284273 (46桁, 148桁から)

p3=247834521954635532745500626340983855795239624057
(48桁, 102桁から)

商

p4=32033799618725220247140159842929725981579807510003507 73 (55桁)

計算時間

```
p1  :   372 curves * 7500 CPU-sec =   32 days   sigma=1168827276
p2  :   2200 curves * 4900 CPU-sec = 125 days   sigma=1886020754
p3  :   3000 curves * 2900 CPU-sec = 100 days   sigma=2087103149

32 + 125 + 100 = 257 days ( / 75 = 3.5 days)
```

実際は、Oct 20 11:43 から Oct 27 16:52 までの間のうちの 4日間

参考文献

[1] R. Brent, http://www.comlab.ox.ac.uk/oucl/work/richard.brent/factors.html, ftp://ftp.comlab.ox.ac.uk/pub/Documents/techpapers/Richard.Brent/champs.txt

[2] "The Cabal", ftp://ftp.cwi.nl/pub/herman/SNFSrecords/SNFS-233

[3] G. Cooperman, http://www.ccs.neu.edu/home/gene/pargap.html

[4] "Cunningham tables" http://www.cerias.purdue.edu/homes/ssw/cun/ index.html

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version4*, Lehrstuhl D f Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany and School of Mathematical and Computational Sciences, Univ. St. Andrews, Scotland, 1997.

[6] H. Mishima, http://www.asahi-net.or.jp/ KC2H-MSM/cn/index.htm

[7] P. Zimmermann, http://www.loria.fr/ zimmerma/records/ecmnet.html