Aliquot Sequence 3630 Ends After Reaching 100 Digits

Manuel Benito, Wolfgang Creyaufmüller, Juan L. Varona, and Paul Zimmermann

CONTENTS

2000 AMS Subject Classification: Primary 11Y55; Secondary 11A25

Keywords: Aliquot sequences, sum of divisors, perfect number, amicable pair, sociable numbers, aliquot cycles

In this paper we present a new computational record: the aliquot sequence starting at 3630 converges to 1 after reaching a hundred decimal digits. Also, we show the current status of all the aliquot sequences starting with a number smaller than 10,000; we have reached at leat 95 digits for all of them. In particular, we have reached at least 112 digits for the so-called "Lehmer five sequences," and 101 digits for the "Godwin twelve sequences." Finally, we give a summary showing the number of aliquot sequences of unknown end starting with a number less than or equal 10^6.

1. INTRODUCTION

For a positive integer n, let $\sigma(n)$ denote the sum of its divisors (including 1 and n), and $s(n) = \sigma(n) - n$ the sum of its proper divisors (without n). A perfect number is a number n such that $s(n) = n$, and an amicable pair of numbers (n, m) satisfies $s(n) = m$, $s(m) = n$. In a similar way, tuples of numbers $(a_1, a_2, \dots, a_l)$ such that $s(a_i) = a_{i+1}$ for $1 \le i \le l-1$ and $s(a_l) = a_1$, are known as aliquot cycles or sociable numbers.

Given n, the way to compute $\sigma(n)$ (and then, $s(n)$) is as follows: We find the prime decomposition of $n = p_1^{a_1} \cdots p_d^{a_d}$. Then

$$\sigma(p_1^{a_1} \cdots p_d^{a_d}) = (1 + p_1 + \cdots + p_1^{a_1}) \cdots (1 + p_d + \cdots + p_d^{a_d}) \tag{1–1}$$

$$= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_d^{a_d+1} - 1}{p_d - 1}. \tag{1–2}$$

Indeed, if we expand the expression on the right in Equation (1–1), all the divisors of $p_1^{a_1} \cdots p_d^{a_d}$ appear as summands.

By iterating the function s, i.e., taking $s^0(n) = n$ and $s^{k+1}(n) = s(s^k(n))$, we get the so-called aliquot sequence $\{s^k(n)\}_{k=0}^{\infty}$. For each one of these sequences, there are four possibilities:

© A K Peters, Ltd.
1058-6458/2001 $0.50 per page

(i) it terminates at 1 (the previous term being a prime number);

(ii) it reaches a perfect number;

(iii) it reaches an amicable pair or a cycle;

(iv) it is unbounded.

The Catalan-Dickson conjecture says that *(iv)* does not actually happen. But other researchers disagree with this conjecture and think that there are unbounded sequences; in fact, the alternative conjecture from Guy-Selfridge [Guy and Selfridge 75] (see also [Erdős 76]) states that there are many sequences that go to infinity, perhaps almost all those that start at an even number (i.e., the proportion of even integers n such that $\{s^k(n)\}_{k=0}^{\infty}$ is bounded tends to zero).

This new conjecture is based upon the existence of several multiplicative patterns $2^a p_1 \cdots p_m$ that, when appearing in the factor decomposition of n, show up again, with a high order of probability, in the factor decomposition of $s(n)$. Following [Guy and Selfridge 75], these patterns are called *drivers* or *guides*.

By definition, a guide is of the form 2^a, together with a subset of prime factors of $\sigma(2^a)$ $(= 2^{a+1} - 1)$; a driver is of the form $2^a v$ with $a > 0$, $v \mid \sigma(2^a)$ and $2^{a-1} \mid \sigma(v)$. This last condition ensures that the power of the prime 2 tends to persist, at least, as much as if the driver is 2, for which the condition is trivial. Actually, drivers are much more stable than guides. As stated in [Guy and Selfridge 75], the only drivers are 2, $2^3 \cdot 3$, $2^3 \cdot 3 \cdot 5$, $2^5 \cdot 3 \cdot 7$, $2^9 \cdot 3 \cdot 11 \cdot 31$, and the even perfect numbers. Examples of guides that are not drivers are 2^a $(a > 1)$, $2^3 \cdot 5$, $2^5 \cdot 3$, $2^5 \cdot 3^2$, $2^5 \cdot 3^2 \cdot 7$, $2^7 \cdot 3 \cdot 5, \ldots$.

Using (1–1), it is easy to observe the behavior of drivers (and guides). For instance, let us take $n = 2^3 \cdot 3 \cdot 5pq$, with p and q prime numbers, $p \neq q$, $p, q > 5$. We get the same result if we have more than two prime factors greater than 5 but, for simplicity, we use this example. We can check that $s(n) = (1+2+4+8) \cdot 4 \cdot 6(p+1)(q+1) - 2^3 \cdot 3 \cdot 5pq = 15 \cdot 2^2 \cdot 2 \cdot 3(p+1)(q+1) - 2^3 \cdot 3 \cdot 5pq = 2^3 \cdot 3 \cdot 5 \cdot [3(p+1)(q+1) - pq] = 2^3 \cdot 3 \cdot 5m$, with m an odd number that is not divisible by 3. Then, we again get $2^3 \cdot 3 \cdot 5$ with 2 and 3 raised to the same power as before (however, it is possible that the power of 5 changes; this may cause the loss of the driver at a later point). The behavior is similar if the prime factors greater than 5 are raised to an odd power, because $1 + p + \cdots + p^a$ is even when a is odd. However, a factor p^a with a an even number does not contribute with a factor 2 in the first summand of m.

It is easy to prove that, if m is a perfect number, or $s(m) > m$, and we have m a proper divisor of n, then $s(n) > n$ (of course, we are not considering the trivial case $n =$ perfect number). Thus, we have $\sigma(m) \geq 2m$ and $n = lm$ with $l > 1$. To prove the claim, we must check $\sigma(lm) > 2lm$. Let $\{1, d_1, d_2, \ldots, d_r\}$ be the divisors of m. Then, $1, l, ld_1, ld_2, \ldots, ld_r$ are divisors of lm. Therefore, $\sigma(lm) \geq 1 + l + ld_1 + ld_2 + \cdots + ld_r > l(1 + d_1 + d_2 + \cdots + d_r) = l\sigma(m) \geq 2lm$.

As a consequence, all the drivers, with the exception of 2 (the "downdriver," as we show below), make $s(n) > n$. And, as the structure is preserved, it seems that we can get an always increasing sequence. But a driver can, eventually, disappear. Let us consider some examples, this time, with the driver $2^3 \cdot 3$. Here, and in what follows, we will use p, q to denote distinct prime numbers, $p, q > 3$.

When we have a number of the form $n = 2^3 \cdot 3p$, it follows $s(n) = (1 + 2 + 4 + 8) \cdot 4(p + 1) - 2^3 \cdot 3p = 2^2 \cdot 3 \cdot [5(p + 1) - 2p]$. Now, if p has the form $p = 4r + 1$, then $s(n) = 2^3 \cdot 3 \cdot [5(2r + 1) - p]$, and the expression between square brackets is even, so the power of 2 in $s(n)$ is at least 4. However, if $p = 4r + 3$, we get $s(n) = 2^3 \cdot 3 \cdot [5(2r+2) - p]$ and, this time, the expression between square brackets is odd, so the power of 2 remains.

The driver $2^3 \cdot 3$ can also disappear with numbers of the form $n = 2^3 \cdot 3^2 pq$. Here, $s(n) = 15 \cdot 13(p+1)(q+1) - 8 \cdot 9pq$. If $p, q \equiv 1 \bmod 4$, then the 2^3 disappears and, in its place, 2^2 arises. If $p, q \equiv 3 \bmod 4$, the 2^3 persists. If $p \equiv 1$ and $q \equiv 3 \bmod 4$, then, at least, we have a factor 2^3; but the power of 2 goes up if 8 is not a divisor of $q + 1$, i.e., if $q \equiv 3 \bmod 8$.

When the driver of the sequence is 2, the sequence usually decreases. For instance, if $n = 2pq$, then $s(n) = 3(p + 1)(q + 1) - 2pq = pq + 3(p + q + 1)$. When p and q are big enough, $3(p + q + 1)$ is tiny compared with pq, and so $s(n) < n$.

As for the other drivers, the driver 2 can disappear. For instance, let $n = 2p$, with $s(n) = 3(p+1) - 2p = p+3$. If $p = 4r + 3$, then $s(n) = 2(2r + 3)$. But, if $p = 4r + 1$, then $s(n) = 2^2(r+1)$ and so we have, at least, a factor 2^2. The behavior is similar if $n = 2p^2q$, or if n has more prime factors raised to even powers.

Guides in the form 2^a for $a > 1$ make the sequence oscillate; we have $s(n) < n$ or $s(n) > n$ according to the other factors. And these guides change very easily.

And, what occurs when n is odd? If $n = p$ prime, $s(n) = 1$ and the sequence finishes. Now, let us assume $n = pq$. Then, $s(n) = (p + 1)(q + 1) - pq = p + q + 1$ is also odd (usually, $s(n) < n$). The same occurs, for instance, with $n = p^2q$. But it is also possible that n is odd but $s(n)$ is even. This is what happens when $n = p^2$; indeed, in this case, $s(n) = (p^2 + p + 1) - p^2$, which is even.

It is possible (but not very common) that an aliquot sequence reaches a perfect number, an amicable pair or a cycle; this is the end of the aliquot sequence. Otherwise, to get a terminating sequence, it must reach an odd prime number. Usually, most terms of a sequence are even. Let us see the way in which an even term n changes to an odd term $s(n)$. This occurs when $n = 2^ap^2$, with $a > 0$ (or similar cases with p^{2b} or more primes up to even powers). Indeed, $s(n) = (2^{a+1} - 1)(1 + p + p^2) - 2^ap^2$, an odd number, which may or may not be prime. The sequence either reachs an even term (case previously considered) or it continues with odd tems until a prime term appears, where it stops.

Finally, let us also note that, although it seems unlikely that an always increasing aliquot sequence exists (of course, this would refute Catalan-Dickson conjecture), H. W. Lenstra proved that it is possible to construct arbitrarily long monotonic increasing aliquot sequences (that is, for any k, we can found m such that $s^0(m) < s^1(m) < \cdots < s^k(m)$); the proof can be found in [Erdős 76].

2. BACKGROUND

Many other people have been working with aliquot sequences, including P. Poulet, D. H. Lehmer, P. Erdős, J. Godwin, H. Cohen, R. K. Guy, M. Dickerman, H. J. J. te Riele, ... An extensive bibliography on this subject can be found in [Guy 94, B6].

The first sequence whose end was in doubt started with 138; Lehmer found its end $s^{177}(138) = 1$. For numbers $n < 1000$, Lehmer could not find the end of the sequences starting from 276, 552, 564, 660, 840 and 966. Except for 840, which finished with $s^{747}(840) = 1$ (found by A. Guy and R. K. Guy), the end for the others is still unknown; they are the "Lehmer five." In a similar way, the doubtful sequences starting between 1000 and 2000 are known as Godwin sequences; now, "Godwin twelve."

Regarding classifications of unknown sequences, we note the following: Suppose that, for two different numbers n_1 and n_2 (say, $n_1 < n_2$), there exist k_1 and k_2 such that $s^{k_1}(n_1) = s^{k_2}(n_2)$. Then, both sequences are the same from that point on. In this case, we say that n_1 is the *main* sequence and n_2 is a *side* sequence. Only the main sequences are studied.

According to (1–1) or (1–2), to compute an aliquot sequence, we have to decompose m into factors to calculate $s(m)$; and this must be done for many ms. This is difficult when the number m is large. The discovery of better factoring methods and the increase in the speed of computers lead to progress in the experimental knowledge of the behavior of aliquot sequences.

Recently, different people have extended the range of aliquot sequences that have been studied; W. Bosma, J. Gerved, S. Wagstaff, P.-L. Montgomery, H. J. J. te Riele, W. Lioen, A. Lenstra, and the authors have made contributions. Here are some recent advances.

In [Benito and Varona 99], two of the authors, following previous work of A. Guy and R. K. Guy, present a table with the status of doubtful main aliquot sequences starting at $n < 10000$. In this paper, we give an update: see Table 1.

In the table, we include the number of decimal digits of the last term $s^k(n)$ known for each sequence and the guide in that stage. Actually, all the sequences have a driver in the current stage (a driver is more stable than a guide), except the ones marked with $^{(*)}$.

In [Benito and Varona 99], all the sequences in the table had been pursued up to, at least, 75 decimal digits. Now, we have reached more than 95 digits for all of them; and 100 digits for many of them. We have reached at least 112 digits for the Lehmer sequences and 101 digits for the Godwin sequences.

It is curious to note that the driver $2^9 \cdot 3 \cdot 11 \cdot 31$ has appeared in no place in any of the sequences given in Table 1.

W. Creyaufmüller is leading a project to study all the aliquot sequences starting at every $n \leq 10^6$; of course, there are many of them, so they are being studied up to fewer digits than in this paper. For a compilation of his work, see [Creyaufmüller 00]. Here, we summarize the present state of such aliquot sequences with unknown status in Table 2.

We have not found new experimental evidence in favour of the Guy-Selfridge conjecture, because drivers and guides disappear from time to time. For instance, when we increase the size of the last term reached for the sequences starting at every $n \leq 10^6$, the percentage of unknown sequences decreases in a significative way.

It seems feasible that Catalan's conjecture is true. But the question is, "How big are intermediate numbers that we need to factor to reach the end of the sequence?" As we see below, for $n = 840$, we had to go up to 49 digit numbers; for $n = 1248$, up to 58 digit numbers; for $n = 3630$, up to 100 digit numbers. Perhaps we must

n	276	552	564	660	966	1074	1134	1464	1476
k	1284	818	3048	468	526	1585	2249	1897	1055
digits	117	118	115	112	114	105	127	101	106
guide	$2\cdot3$	$2^5\cdot3\cdot7$	$2^2\cdot7$	$2^{2(\bullet)}$	$2\cdot3$	$2^2\cdot7$	$2^5\cdot3\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$
n	1488	1512	1560	1578	1632	1734	1920	1992	2232
k	824	1632	1336	1109	713	1404	1992	985	390
digits	103	101	101	104	102	103	108	102	102
guide	$2^2\cdot7$	$2^2\cdot7$	$2^5\cdot3\cdot7$	$2^{2(\bullet)}$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^{6(\bullet)}$
n	2340	2360	2484	2514	2664	2712	2982	3270	3366
k	471	974	796	2866	761	1347	826	417	1062
digits	99	95	97	105	100	95	97	98	100
guide	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^3\cdot3$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^4\cdot31$	$2^5\cdot3\cdot7$	$2^{3(\bullet)}$
n	3408	3432	3564	3678	3774	3876	3906	4116	4224
k	840	933	779	1201	1193	830	704	1192	519
digits	95	103	100	98	98	96	100	105	98
guide	$2^3\cdot3\cdot5$	$2^3\cdot3\cdot5$	$2^3\cdot3$	$2^2\cdot7$	$2^7\cdot3^{(\bullet)}$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3$	$2^3\cdot3\cdot5$
n	4290	4350	4380	4788	4800	4842	5148	5208	5250
k	953	1165	965	2152	1135	473	1545	1710	1567
digits	106	97	100	105	101	98	95	96	100
guide	$2^2\cdot7$	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^4\cdot31$	$2^2\cdot7$	$2\cdot3$	$2^3\cdot3\cdot5$	$2^{4(\bullet)}$
n	5352	5400	5448	5736	5748	5778	6160	6396	6552
k	746	2776	1185	1093	1091	742	1630	1272	932
digits	106	102	96	100	108	95	96	105	102
guide	$2^2\cdot7$	$2^2\cdot7$	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^4\cdot31$	$2^{2(\bullet)}$	$2^3\cdot3\cdot5$	$2^3\cdot3$
n	6680	6822	6832	6984	7044	7392	7560	7890	7920
k	1880	1177	885	1764	1113	498	846	891	1014
digits	106	97	104	96	102	96	97	99	109
guide	$2^4\cdot31$	$2^4\cdot31$	$2^3\cdot3$	$2^4\cdot31$	$2^4\cdot31$	$2^3\cdot3\cdot5$	$2^3\cdot5^{(\bullet)}$	$2^2\cdot7$	$2^6\cdot127$
n	8040	8154	8184	8288	8352	8760	8844	8904	9120
k	2240	647	1241	849	1291	2157	1184	963	580
digits	106	96	102	103	96	97	101	95	103
guide	$2^3\cdot3\cdot5$	$2^2\cdot7$	$2^2\cdot7$	$2^{8(\bullet)}$	$2^2\cdot7$	$2^{4(\bullet)}$	$2^4\cdot31$	$2^2\cdot7$	$2^3\cdot3$
n	9282	9336	9378	9436	9462	9480	9588	9684	9708
k	556	608	2198	638	447	1028	1848	643	710
digits	106	97	101	102	97	98	103	101	106
guide	$2^3\cdot3$	$2^6\cdot127$	$2^2\cdot7$	$2\cdot3$	$2^3\cdot3\cdot5$	$2\cdot3$	$2^5\cdot3\cdot7$	$2^5\cdot3\cdot7$	$2^2\cdot7$
n	9852								
k	669								
digits	105								
guide	$2^2\cdot7$								

TABLE 1. Aliquot sequences whose end is in doubt.

go up to 200 or 1000 digit numbers for $n = 276$, which would make this sequence out of reach. (Perhaps only 130 digits, which would make this sequence computable with today's computers and algorithms.)

Interval	Number of sequences	Limits of computation
$[1, 100000]$	925	$> 10^{80}$
$(100000, 200000]$	975	$> 10^{80}$
$(200000, 300000]$	963	$> 10^{60}$
$(300000, 400000]$	903	$> 10^{60}$
$(400000, 500000]$	940	$> 10^{60}$
$(500000, 600000]$	990	$> 10^{60}$
$(600000, 700000]$	987	$> 10^{60}$
$(700000, 800000]$	990	$> 10^{60}$
$(800000, 900000]$	982	$> 10^{80}$
$(900000, 10^6]$	987	$> 10^{80}$

TABLE 2. Number of aliquot sequences of unknown status starting with a number $\leq 10^6$.

3. MAXIMUM OF A TERMINATING SEQUENCE

There has been considerable progress with respect to the length of aliquot sequences that are known to terminate. When D. H. Lehmer found the end of the aliquot sequence starting at 138, he found a maximum $s^{117}(138)$ of 12 decimal digits. Later, A. Guy and R. K. Guy found the end for 840 after finding a maximum $s^{287}(840)$ of 49 digits; and M. Dickerman did the same for 1248, with a maximum $s^{583}(1248)$ of 58 digits. (Of course, if p is a prime number, $s(p) = 1$ so the sequence starting in p finishes trivially. These trivial results are not considered in records.)

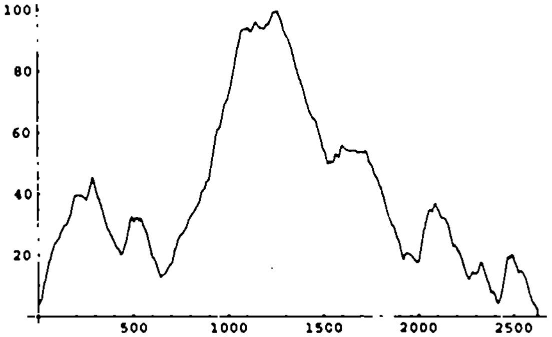

FIGURE 1. The aliquot sequence starting at 3630.

In [Benito and Varona 99], we show that the sequence starting at 4170 converges to 1 after 869 iterations, reaching a maximum of 84 decimal digits at iteration 289; this was a new record for the highest terminating aliquot sequence (found in December 22, 1996).

Later, in October 1999, W. Bosma broke this record: he found that the aliquot sequence starting with 44922 terminates after 1689 iterations (at 1), after reaching a maximum of 85 digits at step 1167. On December 3, 1999, he again broke the record, finding that the sequence starting at 43230 finished: it terminates (at 1) after 4357 iterations, after reaching a maximum of 91 digits at step 967.

As of June 10, 2001, M. Benito and J. L Varona have found the end of the aliquot sequence starting at 3630. It finishes at $s^{2624}(3630) = 1$ after reaching a maximum $s^{1263}(3630)$ with a hundred digits, and is the present record for the highest known terminating aliquot sequence. In Figure 1, we show the shape of the sequence: the horizontal axis is the index k, and the vertical axis is $\log_{10}(s^k(3630))$.

Moreover, $3630 < 10000$ so Table 1 has one fewer entry than the table that appears in [Benito and Varona 99] (the aforementioned sequences found by W. Bosma start at a number > 10000). There are 82 main aliquot sequences (starting at a number < 10000) whose end is still unknown.

For sequences of unknown status, the sequence 1134 has been extended by P. Zimmermann up to 127 digits; this is the largest term of an aliquot sequence computed so far.

We maintain the following web pages related to aliquot sequences:
http://home.t-online.de/home/Wolfgang.Creyaufmueller/aliquote.htm
http://www.unirioja.es/dptos/dmc/jvarona/aliquot.html
http://www.loria.fr/~zimmerma/records/aliquot.html

On these pages, one can find links to the aliquot web pages of other authors (in particular, those of W. Bosma and J. Howell). The sequences of Table 1 can also be found at the ftp server ftp://mat.unirioja.es/pub/aliquot/00xxxx.

4. THE METHOD

To compute an aliquot sequence, we have to decompose m into factors to calculate $s(m)$, and iterate this procedure numerous times. This is difficult when the number m is large. Since we are dealing with numbers of up to more than a hundred digits, powerful algorithms are necessary. In particular, we have used the elliptic curve method (ECM) and the multiple polynomial quadratic sieve (MPQS); see a recent report (with many references) about the use of MPQS in [Boender and te Riele 96]. We have checked the primality of the factors with the Adleman-Pomerance-Rumely (APR) primality test.

All our work has been done using packages available on the internet. The authors began to investigate the behavior of aliquot sequences around 1985. They have used many different kinds of computers, mainly PCs, but also Unix workstations and Macintosh computers. In total, approximately 200 years of CPU time has been used.

The following packages are available at their corresponding web pages (or anonymous ftp sites):

- UBASIC, ftp://rkmath.rikkyo.ac.jp/pub/ubibm/
- PARI-GP, http://www.parigp-home.de/
- KANT-KASH (see [Daberkow et al. 97]), http://www.math.tu-berlin.de/algebra/
- MIRACL, http://indigo.ie/~mscott/
- GMP, http://www.swox.com/gmp/

UBASIC programs to get aliquot sequences can also be downloaded from Creyaufmüller's web page. PARI-GP and KANT-KASH programs can be downloaded from Varona's web page. An implementation of ECM for GMP can be downloaded from Zimmermann's web page.

One of the most titanic efforts undertaken has been to factorize the 109-digit cofactor in $s^{1267}(276)$. The computation time is the equivalent of about 220 days of CPU time on an 800 Mhz Pentium III computer (actually, the sieving was carried out on a cluster of PCs). This kind of number is the reasonable limit for the MPQS method. For larger numbers, it will be better to use a new method of factorization: the number fields sieve (NFS); see, for instance [Cavallar et al. 99].

ACKNOWLEDGEMENTS

The authors thank all those who helped factorizing numbers from the Lehmer and several Godwin (1074 and 1134) sequences: Conrad Curry, Jim Howell, Arjen Lenstra, Paul Leyland, Sam Wagstaff. We also thank Wieb Bosma for his calculations on aliquot sequences starting with a number between 10000 and 50000.

Also, thanks to Peter Montgomery for making his program `ecmfft` available, Herman te Riele and Walter Lioen for their MPQS program, Sam Wagstaff for having done some aliquot factorizations on his MasPar, and Arjen Lenstra for his enormous help with the `ppmpqs` program. And to Yuji Kida for his programs (ECM and PPMPQS implementations) written in UBASIC.

Finally, thanks to Laureano Lambán, Eloy Mata, David Ortigosa and Julio Rubio for allowing us to use their personal computers to do some of the computations that appear in this paper.

The first author was on a study leave supported by Consejería de Educación, Cultura, Juventud y Deportes of Gobierno de La Rioja. Research of the third author was supported by Grant BFM2000-0206-C04-03 of the DGI and API-01/B38 of the UR.

REFERENCES

[Boender and te Riele 96] H. Boender and H.J.J. te Riele. "Factoring integers with large-prime variations of the quadratic sieve." *Experimental Mathematics* **5** (1996), 257–273.

[Benito and Varona 99] M. Benito and J.L. Varona, "Advances in aliquot sequences." *Math. Comp.* **68** (1999), 389–393.

[Cavallar et al. 99] S. Cavallar, B. Dodson, A.K. Lenstra, P.C. Leyland, W.M. Lioen, P.L. Montgomery, B.A. Murphy, H.J.J. te Riele, and P. Zimmermann. "Factorization of RSA-140 using the Number Field Sieve," in *Advances in Cryptology, Asiacrypt'99* (Berlin, 1999), *Lecture Notes in Computer Science* **1716**, pp. 195–207, Springer-Verlag, Berlin-Heidelberg, 1999.

[Creyaufmüller 00] W. Creyaufmüller. *Primzahlfamilien*, 3rd ed., Verlagsbuchhandlung Creyaufmüller, Stuttgart, 2000.

[Daberkow et al. 97] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. "KANT V4." *J. Symbolic Comput.* **24** (1997), 267–283.

[Erdős 76] P. Erdős, "On asymptotic properties of aliquot sequences." *Math. Comp.* **30** (1976), 641–645.

[Guy 94] R.K. Guy, *Unsolved Problems in Number Theory*, 2nd ed., Springer-Verlag, Berlin-Heidelberg, 1994.

[Guy and Selfridge 75] R.K. Guy and J.L. Selfridge, "What drives an aliquot sequence?" *Math. Comp.* **29** (1975), 101–107. "Corrigendum." *ibid.* **34** (1980), 319–321.

Manuel Benito, Instituto Sagasta, Glorieta del Doctor Zubía s/n, 26003 Logroño, Spain (mbenit8@palmera.pntic.mec.es)

Wolfgang Creyaufmüller, Freie Waldorfschule Aachen, Anton-Kurze-Allee 10, D-52074 Aachen, Germany (Wolfgang.Creyaufmueller@t-online.de)

Juan L. Varona, Departamento de Matemáticas y Computación, Universidad de La Rioja, Edificio J. L. Vives, Calle Luis de Ulloa s/n, 26004 Logroño, Spain (jvarona@dmc.unirioja.es)

Paul Zimmermann, INRIA Lorraine, Technopôle de Nancy-Brabois, 615 rue du Jardin Botanique, BP 101, F-54600 Villers-lès-Nancy, France (Paul.Zimmermann@inria.fr)

Received July, 10, 2001; accepted in revised form December 3, 2001.