ma
the
ma
tisch

cen
trum

MC

AFDELING NUMERIEKE WISKUNDE NW 153/83 MEI
(DEPARTMENT OF NUMERICAL MATHEMATICS)

H.J.J. TE RIELE

NEW VERY LARGE AMICABLE PAIRS

Preprint

amsterdam 1983

stichting
mathematisch
centrum

MC

AFDELING NUMERIEKE WISKUNDE NW 153/83 MEI
(DEPARTMENT OF NUMERICAL MATHEMATICS)

H.J.J. TE RIELE

NEW VERY LARGE AMICABLE PAIRS

Preprint

kruislaan 413 1098 SJ amsterdam

Printed at the Mathematical Centre, Kruislaan 413, Amsterdam, The Netherlands.

The Mathematical Centre, founded 11 February 1946, is a non-profit institution for the promotion of pure and applied mathematics and computer science. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

1980 Mathematics subject classification: Primary 10A40; Secondary 10A25, 10-04

New very large amicable pairs*)

by

Herman J.J. te Riele

ABSTRACT

Computations are described which led to the discovery of many very large amicable pairs, which are much larger than the largest amicable pair thus far known.

KEY WORDS & PHRASES: *amicable pair; Thabit-rule; primality test*

*) This report will be submitted for publication elsewhere.

1. INTRODUCTION

200 years ago, to be more precise: on September 18, 1783, Leonhard Euler died. He left 59 new amicable pairs (APs) as a result of an extensive, systematic study ([7]). (A pair of positive integers (m_1,m_2) is called amicable, if $m_1 \neq m_2$ and if each number is the sum of the proper divisors of the other, i.e., $\sigma(m_1) - m_1 = m_2$ and $\sigma(m_2) - m_2 = m_1$, where $\sigma(\cdot)$ denotes the sum of *all* the divisors - function.) The following AP of Euler's will play a crucial rôle in this paper:

$$(1) \qquad \begin{cases} 11498355 \\ 12024045 \end{cases} = 3^4 5 \cdot 11 \cdot \begin{cases} 29 \cdot 89 \\ 2699 \end{cases}.$$

Prior to Euler, only three APs were known, namely,

$(220, 284) = (2^2 5\cdot 11, 2^2 71)$ (known to the Pythagoreans [9, p. 97]),
$(17296, 18416) = (2^4 23\cdot 47, 2^4 1151)$ (Ibn Al-Bannā' [4]) and
$(9363584, 9437056) = (2^7 191\cdot 383, 2^7 73727)$ (Descartes [9, p. 99]).

After Euler, many more APs have been found (cf. [8] and [11]), most of them with the help of Euler's methods and with methods recently found by the present author ([11]). A small minority of the known APs were found by systematic computer searches (i.e., by testing for *all* m in a given interval, whether $s(s(m)) = m$ (where $s(m) = \sigma(m) - m$)). It is generally believed, although unproved, that there are infinitely many APs.*) The largest AP thus far known consists of two 152-digit numbers ([10]).

In this short paper we describe computations by which we have found many very large APs, the largest pair consisting of two 282-digit numbers, and we indicate the rôle played by Euler's pair (1) in this work.

2. A METHOD FOR FINDING AMICABLE PAIRS

Very recently, we have discovered methods for constructing APs from *given* APs, which turned out to be very "prolific": from a "mother" list of 1592 known APs, 2325 *new* APs were constructed ([11]). About half the number of these new pairs were found by using the following lemma (which is a

*) The author maintains a file of about 4000 APs. Anyone who is really interested may send a request for a print-out, or a copy on tape.

special case of Method 2 given in [11]; the proof of this lemma is left to the reader).

LEMMA 1. *Let (au,ap) be a given amicable pair with $\gcd(a,u) = \gcd(a,p) = 1$, where p is a prime. If a pair of prime numbers (r,s) with $r < s$ and $\gcd(a,rs) = 1$ exists, satisfying the bilinear Diophantine equation*

$$(2) \qquad (r-p)(s-p) = \frac{\sigma(a)}{a}\left(\sigma(u)\right)^2 =: R,$$

and if a third prime q exists, with $\gcd(au,q) = 1$ and

$$(3) \qquad q = r + s + u,$$

then (auq,ars) is also an amicable pair.

If the factorization of R into primes is known, equation (2) can easily be solved by writing R in all possible ways as the product $R = A\cdot B$, with $2 \le A < B$, so that $r = p + A$ and $s = p + B$. For nearly all known APs of the form (au,ap), u is the product of 2, 3, 4 or 5 distinct prime numbers (compare the examples given in the introduction). As a consequence, R usually has *many* divisors, and this explains, at least heuristically, the large number of new APs found with Lemma 1.

EXAMPLE. For Borho's AP ([2]) mentioned in the "Note added in proof" in [11] we have $a = 2\cdot 5^3 19\cdot 67$, $u = 15959\cdot 5346599$ and $p = 85331735999$, so that $R = 2^{17}3^6 5^4 7^4 13\cdot 17\cdot 19^3 67$, a number with 44800 even divisors less than its square root and with even co-divisor. By testing all these cases, we found 145 new APs with Lemma 1. $\square$

The program used in [11] could not handle cases with $R > 10^{25}$, so that we could not yet apply Lemma 1 to the largest known APs of the form (au,ap). (also the 152-digit AP mentioned above is of this form).

Fortunately, my colleague D.T. Winter has recently developed a very fast package for multi-precision integer arithmetic. This package was used by A.K. Lenstra in his implementation of a primality proving program on a CDC Cyber 750 computer (the algorithm used in this program was based on ideas of Adleman, Pomerance and Rumeley ([1]) and of Cohen and H.W. Lenstra, Jr. ([5])). With this program it is possible now to prove primality of numbers of up to 200 decimal digits in a reasonable amount of computer time.

Winter's package and A.K. Lenstra's program enabled us to apply Lemma 1 to the largest known APs of the form (au,ap). In this way we found 3 new APs (with 123-, 127- and 141-digit members) from the 81-digit AP given in [10] and 11 new APs (with 231-, 232-, 233-, 235-, 239-, 246-, 248-, 249-, 250-, 263- and 282-digit members) from the 152-digit AP given in [10].

Some details of our computations which led to the 282-digit AP are given in the next section.

3. THE 282-DIGIT NEW AMICABLE PAIR

In 1972, Borho ([3]) presented his so-called Thabit-rules, which are generalizations of the following formula, due to the Arabian mathematician Thabit ibn Kurrah ([6]): *If* $p = 3\cdot 2^{n-1} - 1$, $q = 3\cdot 2^{n} - 1$ *and* $r = 9\cdot 2^{2n-1} - 1$ *are primes and* $n \geq 2$, *then* $2^{n}pq$ *and* $2^{n}r$ *form an amicable pair* (examples are the three pre-Euler APs mentioned in the Introduction). Many of Borho's Thabit-rules are *constructed* from given APs. In particular, Borho constructed the following Thabit-rule from Euler's AP (1): *If the two numbers* $q_1 = 5281^{n}2582 - 1$ *and* $q_2 = 5281^{n}2582\cdot 2700 - 1$ *are primes and* $n \geq 1$, *then* $3^4 5\cdot 11\cdot 29\cdot 89\cdot 5281^{n}q_1$ *and* $3^4 5\cdot 11\cdot 5281^{n}q_2$ *form an amicable pair*. Lee ([3]) found that indeed q_1 and q_2 are both primes for $n = 1$, and te Riele ([10]) showed that $n = 19$ is the next value of n for which this rule is successful. Borho ([2]) found that these are the *only* successful cases for $n \leq 267$.

Application of Lemma 1 to the "$n = 19$" - AP gave

$$R = 2^{11}3^4 5^4 11\cdot 19\cdot 41\cdot 139\cdot 311\cdot 1291^2 5281^{19} 6661\cdot 33331\cdot 13944481\cdot 75019421\cdot$$
$$\cdot 24027536081\cdot 92192755565941\cdot 155588291031361,$$

which is a 156-digit number with 30720000 even divisors less than its square root and with even co-divisor. Estimates of the running time of our program revealed that testing *all* these divisors (as in Lemma 1) would consume too much computer time. Therefore, we made a selection of about 700000 divisors A of R for which $A \equiv R/A \equiv 0 \pmod{30}$. This enlarged the chance of finding primes r and s, since for these A and $B(=R/A)$ none of the primes 2, 3 and 5 divides r and s.

The divisor

$$A = 2\cdot 3\cdot 5\cdot 139\cdot 1291^2 5281^2 6661\cdot 33331$$

yielded the 282-digit amicable pair, the numerical details of which read as follows (a "\" -symbol means: continuation of the number on the next line):

$$\begin{cases} m_1 = 3^4 5\cdot 11\cdot 5281^{19} 29\cdot 89\cdot \mathrm{P}\cdot \mathrm{Q} \\ m_2 = 3^4 5\cdot 11\cdot 5281^{19} \mathrm{R}\cdot \mathrm{S} \end{cases} \quad \text{where}$$

```
P= (  75 DIGITS )
139175701888775976308855532899186267927088632551744230583288018723382689621
Q= ( 130 DIGITS )
6417976467106377983899074271257515017287808217523810874305651125787167909571 2\
2879980472794001735522210540613508382850696964000 9869
R= (  78 DIGITS )
375774395099695136033909938827802923403139307889709465608574062970334684854 66\
9
S= ( 130 DIGITS )
641797646710637798389907427125751501728780821752381013931876945116123702250 51\
5955920204701706228671634408139104338921158423324 3399

DECIMAL REPRESENTATION  ( BOTH MEMBERS HAVE 282 DIGITS ) :
553610649407886992367379908722703828635124338440205855045898068631854856561 31\
816319616559073822997568562257512746133163331906296693672462340051660630522 41\
199078258371384155343551406293972127278208968662449298159499260040720297491 49\
92170100222242668348702205839132213604876472648 1795
579135510810265354278157982778496837394357114989754284627634554554826854988 87\
837085265040796911245187828896835018627257768194979469061679075155803598195 67\
168202271836497015019139851462990225721043204383481074191897849571778232198 86\
153751513747229819951505729702954824327231219438205
```

4. HISTORICAL COMMENTS

To the best of our knowledge, Lemma 1 has never been explicitly stated in the literature. Euler already gave two APs: $(2^4 23\cdot 47\cdot 9767,\ 2^4 1583\cdot 7103)$ and $(3^2 7\cdot 13\cdot 5\cdot 17\cdot 1187,\ 3^2 7\cdot 13\cdot 131\cdot 971)$ which could have been found with Lemma 1 from the pairs (also known to Euler) $(2^4 23\cdot 47,\ 2^4 1151)$ and $(3^2 7\cdot 13\cdot 5\cdot 17,\ 3^2 7\cdot 13\cdot 107)$, respectively. Unfortunately, Euler did not explain how he found these two APs. Escott ([6]) gave at least 36 APs which could have been found with Lemma 1, so it is not unreasonable to assume that he was aware of it.

ACKNOWLEDGEMENT

I wish to thank A.K. Lenstra for his help in proving all the pseudoprimes which I gave to him, to be prime.

REFERENCES

[1] ADLEMAN, L.M., C. POMERANCE & R.S. RUMELY, *On distinguishing prime numbers from composite numbers*, Ann. Math. 117 (1983), 173-206.

[2] BORHO, W., *Grosse Primzahlen und befreundete Zahlen: über den Lucas-Test und Thabit-Regeln*, to appear in Mitt. Math. Gesells. Hamburg.

[3] BORHO, W., *On Thabit ibn Kurrah's formula for amicable numbers*, Math. Comp. 26 (1972), 571-578.

[4] BORHO, W., *Some large primes and amicable numbers*, Math. Comp. 36 (1981), 303-304.

[5] COHEN, H. & H.W. LENSTRA, Jr., *Primality testing and Jacobi sums*, Report 82-18, Dept. of Mathematics, University of Amsterdam, October 1982.

[6] ESCOTT, E.B., *Amicable numbers*, Scripta Math. 12 (1946), 61-72.

[7] EULER, L., *De numeris amicabilibus*, *Leonhardi Euleri Opera Omnia*, Teubner, Leipzig and Berlin, Ser. I, vol. 2, 1915, 63-162.

[8] LEE, E.J. & J.S. MADACHY, *The history and discovery of amicable numbers*, J. Recr. Math. 5 (1972), Part I: 77-93, Part II: 153-173, Part III: 231-249.

[9] ORE, O., *Number theory and its history*, McGraw-Hill Book Company, New York etc. 1948.

[10] RIELE, H.J.J. TE, *Four large amicable pairs*, Math. Comp. 28 (1974), 309-312.

[11] RIELE, H.J.J. TE, *On generating new amicable pairs from given amicable pairs*, to appear in Math. Comp. .