ON THE LEAST ABSOLUTE REMAINDER EUCLIDEAN ALGORITHM

Thomas E. Moore
Bridgewater State College, Bridgewater, MA 02325
(Submitted July 1990)

To the memory of my friend and mentor Fr. Thomas E. Lockary, C.S.C.

1. Introduction

The usual operation of the Euclidean algorithm uses the least positive remainder at each step of division. However, the Euclidean algorithm can be modified to allow positive or negative remainders provided the absolute value of the remainder is less than the divisor in each step of division.

For example, in computing the greatest common divisor of 3 and 5, there are three Euclidean algorithms in this extended sense:

5 = 3(2) - 1	5 = 3(1) + 2	5 = 3(1) + 2
3 = 1(3) + 0	3 = 2(1) + 1	3 = 2(2) - 1
	2 = 1(2) + 0	2 = 1(2) + 0

the first of which uses the least absolute remainder at each step and which is shorter than the others.

A theorem of Kronecker, see Uspensky & Heaslet [3], says that no Euclidean algorithm is shorter than the one obtained by taking the least absolute remainder at each step of division.

Goodman & Zaring [1] have shown that the number of steps of division in the least positive remainder Euclidean algorithm exceeds the number of steps in the least absolute remainder Euclidean algorithm by just the number of negative remainders occurring in the least absolute remainder variant.

We became interested in exactly which pairs M and N of positive integers have their greatest common divisor, denoted $\gcd(M, N)$, computed in strictly fewer steps by the least absolute remainder (LAR) Euclidean algorithm than by the least positive remainder (LPR) Euclidean algorithm.

Accordingly, a computer program to graphically display such pairs was written in Applesoft BASIC (see Figure 1) and can be modified easily for other BASICs. The program uses counters DC and ADC to count the number of steps of division needed by the LPR and LAR Euclidean algorithms, respectively, in computing $\gcd(M, N)$ with $M \geq N$. The program lights a pixel on the monitor at screen location (M, N) provided ADC < DC in this computation.

When performing the LAR Euclidean algorithm, the program (lines 320-390) chooses between the quotient Q with least positive remainder R and the quotient $Q + 1$ with the alternative negative remainder AR and, if $R = ABS(AR)$, then it breaks the tie by selecting Q and R in agreement with [1].

The resulting image (see Figure 2) reveals some interesting features of the distribution of the lit (black) points (M, N) in the range $1 \leq M \leq 191$, $1 \leq N \leq 191$, with $M \geq N$. Some of these are described in Section 2.

2. Analysis

Definition: If $M \geq N$ is a pair of positive integers for which the LAR Euclidean algorithm is shorter than the LPR Euclidean algorithm, then we will say that M *is a Kronecker number for* N and also that (M, N) is an (ordered) *Kronecker pair*.

```
90 REM STUDY OF LAR VERSUS LPR ALGORITHMS
110 REM DC COUNTS STEPS OF LPR ALGORITHM
120 REM ADC COUNTS STEPS OF LAR ALGORITHM
125 HGR2:REM HI-RES GRAPHICS PAGE IN MEMORY
128 HCOLOR=3:HPLOT 0,0 TO 0, 191 TO 191,191
130 FOR N=1 TO 191
140 FOR M=N TO 191
150 DC=0:ADC=0
170 GOSUB 240
180 GOSUB 310
190 IF ADC>=DC THEN 220
200 REM PLOT ONLY KRONECKER PAIRS
210 HPLOT M, 192-N
220 NEXT M
230 NEXT N
235 GOTO 999
240 REM ROUTINE FOR USUAL LPR ALGORITHM
250 M1=M:N1=N
255 Q=INT(M1/N1)
260 R=M1-N1*Q
270 DC=DC+1
280 M1=N1
290 N1=R
300 IF R>0 THEN 255
305 RETURN
310 REM ROUTINE FOR LAR ALGORITHM
320 M1=M:N1=N
325 Q=INT(M1/N1)
330 R=M1-N1*Q
340 AR=M1-N1*(Q+1)
345 ADC=ADC+1
350 IF R<=ABS(AR) THEN 380
360 M1=N1
370 N1=ABS(AR):GOTO 400
380 M1=N1
390 N1=R
400 IF N1>0 THEN 325
410 RETURN
999 END
```

Figure 1

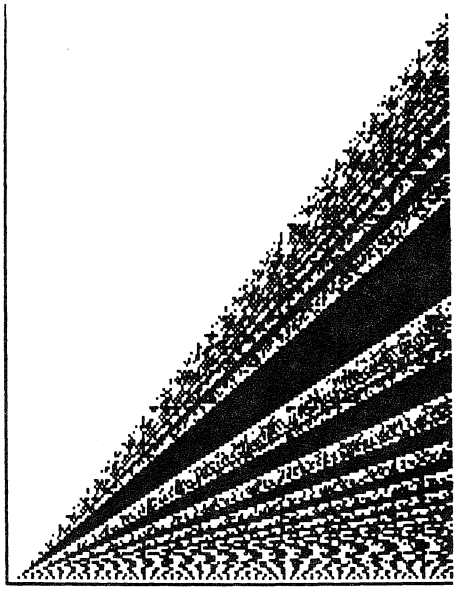

Figure 2

Looking again at Figure 2, we observe the densest region of contiguous Kronecker pairs that is bounded by the lines $N = (2/3)M$ and $N = (1/2)M$.

Considering the coordinates of lit points in this region, we construct a table (see Table 1) of Kronecker numbers M for each N, along with the lengths of the blocks of these consecutive M.

Table 1

N	Consecutive Kronecker Numbers $M > N$	Block Length
3	5	1
4	7	1
5	8, 9	2
6	10, 11	2
7	11, 12, 13	3
8	13, 14, 15	3
9	14, 15, 16, 17	4
10	16, 17, 18, 19	4
11	17, 18, 19, 20, 21	5
12	19, 20, 21, 22, 23	5
13	20, 21, 22, 23, 24, 25	6
14	22, 23, 24, 25, 26, 27	6

Table 1 suggests the next result.

Theorem 1: (i) For $N = 2t + 1$, $t \geq 1$, the t consecutive integers

$$(3N + 1)/2,\ (3N + 3)/2,\ \ldots,\ 2N - 1$$

are all Kronecker numbers for N.

(ii) For $N = 2t$, $t \geq 2$, the $t - 1$ consecutive integers

$$(3N + 2)/2,\ (3N + 4)/2,\ \ldots,\ 2N - 1$$

are all Kronecker numbers for N.

Proof: We prove part (i).

For a fixed integer $t \geq 1$ and any one of the integers $(3N+1)/2$, $(3N+3)/2$, $\ldots$, $2N+1$, say $(3N + k)/2$, where $1 \leq k \leq N - 2$ and k is odd, the LAR Euclidean algorithm must decide, in the first step of division, between the two choices

$$(3N + k)/2 = N(1) + (N + k)/2,$$

in which $(N + k)/2 < N$ because $k \leq N - 2$, or

$$(3N + k)/2 = N(2) + (k - N)/2,$$

in which $\mathrm{ABS}((k - N)/2) < N$ because $N > -k$.

The decision is made for the latter choice according to the comparison

$$\mathrm{ABS}((k - N)/2) < (N + k)/2,$$

which is true since $N - k < N + k$.

The result now follows from the Goodman & Zaring result.

Part (ii) of the theorem is proved similarly.

Corollary 1: For each $t \geq 2$, we may specify a positive integer N and t consecutive integers that are all Kronecker numbers for N.

Proof: Immediate.

Lemma 1: If M is a Kronecker number for N, then $M + Nk$ is also a Kronecker number for N, for all integers $k \geq 1$.

Proof: Suppose the LAR Euclidean algorithm for $\gcd(M, N)$ is

$$\begin{aligned} M &= Nq_1 + e_1r_1,\ r_1 < N, \\ N &= r_1q_2 + e_2r_2,\ r_2 < r_1, \\ r_1 &= r_2q_3 + e_3r_3,\ r_3 < r_2, \\ &\vdots \\ r_s &= r_{s+1}q_{s+2} \end{aligned}$$

so that $\gcd(M, N) = r_{s+1}$ and each $e_i = \pm 1$.

Since M is a Kronecker number for N, at least one $e_i = -1$, by the Goodman & Zaring result.

The LAR Euclidean algorithm for $M + Nk$ and N is then

$$\begin{aligned} M + Nk &= N(q_1 + k) + e_1r_1, \\ N &= r_1q_2 + e_2r_2, \\ &\vdots \\ r_s &= r_{s+1}q_{s+2} \end{aligned}$$

with the same set of values r_i and e_i. Hence, at least one negative e_i occurs and, again by the result of Goodman & Zaring, $M + Nk$ is a Kronecker number for N.

Once more observing the patterns in the lit points in Figure 2 we see that, for each second coordinate N, the values of first coordinates fall into certain progressions.

Theorem 2: For each integer $N \geq 3$ there are arithmetic progressions of integers $M > N$ that are all Kronecker numbers for N. More precisely,

(i) if $N = 2t + 1$, $t \geq 1$, then the arithmetic progressions

$$\{Nk + t + 1\}, \{Nk + t + 2\}, \ldots, \{Nk + t + (N - 1)/2\}, k \geq 1,$$

consist of integers each of which is a Kronecker number for N, and

(ii) if $N = 2t$, $t \geq 2$, then the arithmetic progressions

$$\{Nk + t + 1\}, \{Nk + t + 2\}, \ldots, \{Nk + t + (N - 2)/2\}, k \geq 1,$$

consist of integers each of which is a Kronecker number for N.

Proof: We prove part (i).

By Lemma 1, since the common difference in each progression is N, it is enough to show that the first term in each progression is a Kronecker number for N.

When $k = 1$ the first terms are, respectively,

$$N + t + 1, N + t + 2, \ldots, N + t + (N - 1)/2.$$

Since $t = (N - 1)/2$, these terms are, respectively,

$$(3N + 1)/2, (3N + 3)/2, \ldots, 2N - 1,$$

which are Kronecker numbers for N by Theorem 1.

In the above theorems we have begun with the smaller value N of a Kronecker pair and then constructed the companion number M. In the reverse direction, we offer the next result.

Theorem 3: (i) If M is odd, $M \geq 7$, then M is a Kronecker number for both $(M \pm 1)/2$.

(ii) If M is even, $M \geq 8$, then M is a Kronecker number for both $(M \pm 2)/2$.

Proof: (i) We prove the case $(M + 1)/2$. The LPR Euclidean algorithm here is

$$\begin{aligned} M &= (1)((M + 1)/2) + (M - 1)/2, \\ (M + 1)/2 &= (1)((M - 1)/2) + 1, \\ (M - 1)/2 &= ((M - 1)/2)(1) + 0, \end{aligned}$$

done in three steps, while the LAR Euclidean algorithm begins

$$M = (2)((M + 1)/2) + -1,$$

because ABS(-1) < $(M - 1)/2$, since $M > 3$, and continues

$$(M + 1)/2 = ((M + 1)/2)(1) + 0,$$

done in two steps.

Similarly, we can show that M is also a Kronecker number for $(M - 1)/2$.

(ii) We prove the case $(M + 2)/2$. The LPR Euclidean algorithm here begins

$$\begin{aligned} M &= (1)((M + 2)/2) + (M - 2)/2, \\ (M + 2)/2 &= (1)((M - 2)/2) + 2, \end{aligned}$$

and the next division [by 2 into $(M - 2)/2$] is the last step, or next to last, according as $(M - 2)/2$ is even or odd. So this routine takes three or four steps, accordingly.

The LAR Euclidean algorithm begins

$$M = (2)((M + 2)/2) + -2,$$

because ABS(-2) < $(M - 2)/2$, since $M > 6$, and there are either one or two steps more according to the parity of $(M + 2)/2$. Since $(M + 2)/2$ and $(M - 2)/2$ have the same parity, this means that the LAR variant is accomplished in one step less than the LPR Euclidean algorithm.

Similarly, we can show that M is a Kronecker number for $(M - 2)/2$.

3. The Fibonacci Numbers

The Fibonacci numbers, which are defined by the relations $F_1 = F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$, play an extremal role in questions relating to the number of steps in the LPR Euclidean algorithm. For example, in [2] Shea shows that the pair of integers with the smallest sum whose gcd takes exactly k steps using the LPR Euclidean algorithm is F_{k+1}, F_{k+2}. Not surprisingly, the Fibonacci numbers enter our investigation in a similar way.

Theorem 4: Any positive integer n may be specified as the difference in the number of steps of division performed in computing gcd(M, N) by the LPR and LAR Euclidean algorithms. In fact, this difference n is attained in the computation of both gcd(F_{2n+2}, F_{2n+3}) and gcd(F_{2n+3}, F_{2n+4}).

Proof: It is well known that the LPR Euclidean algorithm applied to consecutive Fibonacci numbers F_k and F_{k+1} takes $k - 1$ steps of division, each with quotient 1 and hence with sequence of remainders F_{k-1}, F_{k-2}, F_{k-3}, ..., F_2, and 0.

The first quotient in the LAR Euclidean algorithm applied to F_k and F_{k+1} is 2 with remainder $-F_{k-2}$. If k is an even integer, then each subsequent division uses a quotient of 3, because of the inequality

$$2F_{2t} < F_{2t+2} < 3F_{2t} \text{ for all } t \geq 2,$$

which may be proved by induction on t. Thus, the sequence of remainders is $-F_{k-2}$, $-F_{k-4}$, $-F_{k-6}$, ..., $-F_2$, and 0. So there are $k/2$ steps of division.

Hence, the difference in the number of steps of the two methods is

$$(k - 1) - k/2 = (k - 2)/2.$$

As k varies over the even integers, $k \geq 4$, this difference $(k - 2)/2$ varies over all the positive integers. For $k = 2n + 2$ in particular, gcd(F_{2n+2}, F_{2n+3}) shows a difference of exactly n steps of division.

The rest of the theorem is proved similarly.

As noted by an anonymous referee, it seems interesting to point out that, whereas the usual Euclidean algorithm leads to the familiar continued fraction

$$F_{2k+3}/F_{2k+2} = (1; 1, 1, \ldots, 1), \ 2k + 1 \text{ ones},$$

the least absolute remainder Euclidean algorithm leads to

$$F_{2k+3}/F_{2k+2} = (2; -3, -3, \ldots, -3), \ k \text{ threes}.$$

References

1. A. W. Goodman & W. M. Zaring. "Euclid's Algorithm and the Least-Remainder Algorithm." *Amer. Math. Monthly* 59 (1952):156-59.
2. D. D. Shea. "On the Number of Divisions Needed in Finding the Greatest Common Divisor." *Fibonacci Quarterly* 7.4 (1969):337-40.
3. J. V. Uspensky & M. A. Heaslet. *Elementary Number Theory*. New York and London: McGraw-Hill, 1939.

*****