ON THE NUMBER OF DIVISIONS NEEDED IN FINDING THE GREATEST COMMON DIVISOR

DALE D. SHEA
Student, San Diego State College, San Diego, California

Let $n(a,b)$ and $N(a,b)$ be the number of divisions needed in finding the greatest common divisor of positive integers a, b using the Euclidean algorithm and the least absolute value algorithm, respectively. In addition to showing some properties of periodicity of $n(a,b)$ and $N(a,b)$, the paper gives a proof of the following theorems:

Theorem 1. If $n(a,b) = k > 1$, then $a + b \geq f_{k+3}$ and the pair (a,b) with the smallest sum such that $n(a,b) = k$ is the pair (f_{k+1}, f_{k+2}), where

$$f_1 = 1, \quad f_2 = 1 \quad \text{and} \quad f_{n+2} = f_{n+1} + f_n, \quad n = 1, 2, 3, \cdots .$$

Theorem 2. If $N(a,b) = k > 1$, then $a + b \geq x_{k+1}$ and the pair (a,b) with smallest sum such that $N(a,b) = k$ is the pair $(x_k, x_k + x_{k-1})$, where $x_1 = 1$, $x_2 = 2$, and $x_k = 2x_{k-1} + x_{k-2}$, $k = 3, 4, \cdots$. These results may be compared with other results found in [1], [2].

Since $n(a,b) = n(b,a)$ we can assume $a \leq b$. To prove the first theorem, let $n(a,b) = k$ and assume the k steps in finding (a,b) are

$$\begin{aligned} b &= q_1 a + r_1 \\ a &= q_2 r_1 + r_2 \\ &\cdots \\ r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1} \\ r_{k-2} &= q_k r_{k-1} \quad . \end{aligned}$$

If $k = 1$, then $r_1 = 0$ so $b = q_1 a$ and the smallest pair (a,b) is $(1,1)$ so

$$a = f_1, \qquad b = f_2, \qquad a + b = f_3 = 2.$$

Note this case is not included in the theorem. In case $k > 1$ it is evident the smallest values of a, b will be obtained for $r_{k-1} = 1$ and all the q's $= 1$ except q_k, which cannot be 1 but is 2. Thus the pairs $(r_{k-1}, r_{k-2}), \cdots, (a,b)$ are $(1,2), \cdots, (f_{k+1}, f_{k+2})$. Since $a + b = f_{k+1} + f_{k+2} = f_{k+3}$, the theorem is proved.

We have

Corollary 1. If $a + b < f_{k+3}$, then $n(a,b) < k$ for $k > 1$.

For $b = a + i$, i a fixed positive integer so that $b < 2a$, the quantities satisfy

(1) $$n(a + mi,\ a + [m + 1]i) = n(a,\ a + i), \qquad m = 0, 1, 2, \cdots .$$

This follows from the remark that if $n(a,b) = k$, then $n(a + b,\ 2a + b) = k + 1$, $k = 1, 2, 3, \cdots$. This is evident since the first division would be $(2a + b) = 1(a + b) + a$ and

$$n(a,\ a + b) = n(a,\ b) = k\ .$$

Equation (1) is a consequence since each n is one more than $n(i,\ a + mi) = n(i, a)$. The periodicity is evident in the table of values of $n(a,b)$ for $a \le b < 2a$. (See Fig. 1.)

a =	
1	1
2	1 2
3	1 2 3
4	1 2 2 3
5	1 2 3 4 3
6	1 2 2 2 3 3
7	1 2 3 3 4 4 3
8	1 2 2 4 2 5 3 3
9	1 2 3 2 3 4 3 4 3
10	1 2 2 3 3 2 4 4 3 3
11	1 2 3 4 4 3 4 5 5 4 3
12	1 2 2 2 2 4 2 5 3 3 3 3
13	1 2 3 3 3 5 3 4 6 4 4 4 3
14	1 2 2 4 3 4 3 2 4 5 4 5 3 3
15	1 2 3 2 4 2 3 3 4 4 3 5 3 4 3

Figure 1

$n(a,b)$ for $b = a,\ a + 1, \cdots, 2a - 1$.

To prove Theorem 2, assume the steps in finding (a,b) with $N(a,b) = k$ are

$$b = q_1 a \pm r_1$$

$$a = q_2 r_1 \pm r_2$$

$$\cdots$$

$$r_{k-3} = q_{k-1} r_{k-2} \pm r_{k-1}$$

$$r_{k-2} = q_k r_{k-1} \qquad ,$$

where

$$0 < r_1 \le \frac{1}{2}a, \quad 0 < r_2 \le \frac{1}{2}r_1, \cdots, \quad 0 < r_{k-1} \le \frac{1}{2}r_{k-2}\ .$$

Because of the restriction on the remainders, we must have $q_2, q_3, \cdots, q_k$ equal to or greater than 2. But since $2r_i + r_{i+1} \le 3r_i - r_{i+1}$, $i = 1, \cdots, k - 1$, in each case we obtain the smallest sum $a + b$ with $q_2 = \cdots = q_k = 2$ and with $q_1 = 1$. For $k = 1$, we have $1 = 1 \cdot 1$ so $a = b = 1$. Set $x_i = r_{k-i}$. For $k > 1$, $a = x_k = 2x_{k-1} + x_{k-2}$ and $b = x_{k+1} = x_k + x_{k-1}$. Then $a + b = 2x_k + x_{k-1} = x_{k+1}$. This completes the proof of the theorem.

Corollary 2. If $a + b < x_{k+1}$, then $N(a,b) < k$ for $k > 1$.

Figure 2 exhibits the periodicity for i fixed):

(2) $$N(a,\ a+i) = N(a+mi,\ a+[m+1]i), \qquad 1 \le i \le a/2$$

and the symmetry:

(3) $$N(a,\ a+i) = N(a,\ 2a-i), \qquad 1 \le i \le a-1\ .$$

a	
a = 1	1
2	2
3	2 2
4	2 2 2
5	2 3 3 2
6	2 2 2 2 2
7	2 3 3 3 3 2
8	2 2 3 2 3 2 2
9	2 3 2 3 3 2 3 2
10	2 2 3 3 2 3 3 2 2
11	2 3 3 3 3 3 3 3 3 2
12	2 2 2 2 4 2 4 2 2 2 2
13	2 3 3 3 4 3 3 4 3 3 3 2
14	2 2 3 3 3 3 2 3 3 3 3 2 2
15	2 3 2 3 2 3 3 3 3 2 3 2 3 2
16	2 2 3 2 3 2 4 2 4 2 3 2 3 2 2
17	2 3 3 3 4 3 4 3 3 4 3 4 3 3 2 2
18	2 2 2 3 4 2 4 2 2 2 4 2 4 3 2 2 2
19	2 3 3 3 3 3 4 4 3 3 4 4 3 3 3 3 3 2
20	2 2 3 2 2 3 3 3 4 2 4 3 3 3 2 2 3 2 2
21	2 3 2 3 3 3 2 4 3 3 3 3 4 2 3 3 3 2 3 2
22	2 2 3 3 4 2 3 3 4 3 2 3 4 3 3 2 4 3 3 2 2
23	2 3 3 3 4 3 4 3 4 4 3 3 4 4 3 4 3 4 3 3 3 2

Figure 2

$N(a,b)$ for $b = a+1, \cdots, 2a-1$

I wish to acknowledge the assistance of Professor V. C. Harris in shortening the proofs.

REFERENCES

1. R. L. Duncan, "Note on the Euclidean Algorithm," The Fibonacci Quarterly, 4 (1966), pp. 367-368.
2. A. W. Goodman and W. M. Zaring, "Euclid's Algorithm and the Least Remainder Algorithm," The Amer. Math. Monthly, 59 (1952), pp. 156-159.