AN ALGORITHM FOR FINDING THE GREATEST COMMON DIVISOR

V. C. HARRIS
San Diego State College, San Diego, California

Our problem is to find the greatest common divisor (m,n) of two positive integers m and n. If $m = 2^aM$ and $n = 2^bN$ where M and N are odd and a and b are nonnegative integers, then $(m,n) = (2^a, 2^b)(M,N)$. Since $(2^a, 2^b)$ is obtained by inspection, we are mainly concerned with finding (M,N). Alternatively, we assume m and n are odd.

Suppose m and n odd with $n < m$. Then

$$m = q_1n + R_1, \qquad 0 \le R_1 < n \ , \tag{1}$$

and

$$m = (q_1 + 1)n + (R_1 - n), \quad 0 \le R_1 < n, \ -n \le R_1 - n < 0 \ . \tag{2}$$

Select (1) or (2) according as R_1 or $R_1 - n$ is even (since n is odd, one of R_1 and $R_1 - n$ is even, the other odd) and call the remainder s_1 so that $s_1 = 2^cr_1$ where r_1 is odd and c is positive. Then $(m,n) = (n, r_1)$ and the next division is with n and r_1. At each step, the even remainder is chosen, and the even part divided out, before the next division is performed. The last nonzero remainder is (m,n).

As an example, we find $(28567, 3829)$. The divisions are

$$\begin{aligned} 28567 &= 7 \cdot 3829 + 4 \cdot 441 \\ 3829 &= 9 \cdot 441 - 4 \cdot 35 \\ 441 &= 11 \cdot 35 + 8 \cdot 7 \\ 35 &= 5 \cdot 7 \end{aligned}$$

Hence $(28567, 3829) = 7$. Four divisions are required. One notes that Euclid's method requires 6 divisions and the least absolute value algorithm requires 5 divisions in finding this g. c. d.

We have the theorem:

If $\eta(a,b)$ is the number of divisions required to find (a,b) by the given algorithm, then the pair (a,b) with the smallest sum such that $\eta(a,b) = k$ is the pair $(2^{k+1} - 3,\ 2^k - 1)$ whose sum is $3 \cdot 2^k - 4$.

Working backward, we see that the divisions involving the smallest dividend and divisor at each step for various values of η are:

η	Divisions			
1	$1 = 1 \cdot 1$			
2	$5 = 1 \cdot 3 + 2 \cdot 1$	$3 = 3 \cdot 1$		
3	$13 = 1 \cdot 7 + 2 \cdot 3$	$7 = 3 \cdot 3 - 2 \cdot 1$	$3 = 3 \cdot 1$	
4	$29 = 1 \cdot 15 + 2 \cdot 7$	$15 = 3 \cdot 7 - 2 \cdot 3$	$7 = 3 \cdot 3 - 2 \cdot 1$	$3 = 3 \cdot 1$
5	$61 = 1 \cdot 31 + 2 \cdot 15$	$31 = 3 \cdot 15 - 2 \cdot 7$	$\cdots$	
$\cdots$		$\cdots$		
n	$2^{n+1} - 3 = 1 \cdot (2^n - 1) + 2 \cdot (2^{n-1} - 1), \quad n \geq 1$			

As a consequence, if $a < 2^k - 1$, then $\eta(a,b) < k$. The results are tabulated:

No. of digits in a	1	2	3	4	5	6	7	8	9	10
$\eta(a,b) <$	4	7	10	14	17	20	24	27	30	34

It may be remarked that primes 3, or 5, and so on, may be removed from m and n, so that all factors of 3, 5 and so on, may be dropped from the subsequent divisors. Of course, for other than small primes, this would not reduce the work involved. Also, if base 2 is used, dropping factors of 2 from the divisors is trivial.