NOTE ON THE NUMBER OF DIVISIONS REQUIRED IN FINDING THE GREATEST COMMON DIVISOR

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

Lamé [1] has shown that in applying Euclid's algorithm to two positive integers a and b, the number of divisions required is not greater than five times the number of digits in the smaller of a and b. (Only base ten is considered in this note.) In the proof given by Uspensky and Heaslet [2] an upper limit for the number $n \leq 1$ of divisions required is shown to be $p/\log_{10}\xi + 1$ where p is the number of digits in the smaller of a and b and

$$\xi = (1 + \sqrt{5})/2 \ .$$

We have $\xi = 1.61803^{+}$ so that $\log_{10}\xi > 0.208978$ and $1/\log_{10}\xi < 4.7852$. Hence the number N of divisions required is

$$N = n + 1 < p(4.7852) + 1 \ .$$

Hence

$$N < 5p - 0.2148p + 1$$

and so

$$N \leq 5p + 1 + [-0.2148p] \ .$$

One could use the simpler but less accurate $N \leq 5p - [p/5]$. Using this, the improvement over Lame's statement would be 1 for $5 \leq p \leq 9$, 2 for $10 \leq p \leq 14$, etc.

REFERENCES

1. G. Lamé, "Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers," C. R. Acad. Sci., Paris, 19, 1844, pp. 867-870.
2. Uspensky and Heaslet, Elementary Number Theory, McGraw-Hill, New York, 1939, Ch. III.