TWO APPLICATIONS OF ELEMENTARY NUMBER THEORY

A. A. MULLIN
University of Illinois, Urbana

INTRODUCTION

This note is concerned with two applications of elementary number theory to numerical quantification theory. The first application deals with a numerical aspect of symbolic logic and the second application is directed toward determining a "shortcut" procedure for indicating when a certain class of integers divides another class of integers. The results are given in terms of some general theorems and some specific examples.

SYMBOLIC LOGIC

For compactness of notation, frequently one represents a sequence of binary digits as a decimal integer with fewer digits (Caldwell, 1958, and Mullin, 1958). However, such a procedure is accompanied by the apparent difficulty of quickly regenerating from the decimal integer either some or all of the binary digits. Hence one is motivated to consider operations involving only the decimal integers to retrieve some or all of the binary digits (Mullin, 1958, and Abrahams, 1955). A method to effect this wish is given in the corollary of the following:

Theorem 1.1: Put $d = \sum_{i=0}^{n} a_i B^i$, where B is some integer greater than 1, each a_i $(i=0,1,...,n)$ is an integer satisfying the condition $0 \leq a_i < B$ and n is a non-negative integer. Put $P_k = [\frac{d}{B^k}]$, where if a is real, $[a]$ is the greatest integer not exceeding a. Then $P_k \equiv a_k$ $(mod\ B)$, $(k= 0, 1, ..., n)$.

Proof: $\frac{d}{B^k} = \sum_{i=1}^{n-k} a_{i+k} B^i + a_k + \sum_{i=1}^{k} a_{k-i} B^{-i}$.

Put $f_k = \sum_{i=1}^{k} a_{k-i} B^{-i}$. Since $\max_j a_j = B-1$, then

$0 \leq f_k < (B-1) \cdot \sum_{i=1}^{\infty} B^{-i} = 1$.

Putting $S_k = \sum_{i=1}^{n-k} a_{i+k} B^i$, notice that there exists an integer I_k such that $S_k = B \cdot I_k$.

Hence $P_k = S_k + a_k = B \cdot I_k + a_k$.

Therefore, $P_k \equiv a_k$ $(mod\ B)$.

Definition 1.1: The decimal integer d is said to contain 2^k in its binary number representation if and only if $a_k = 1$ $(k = 0, 1, ..., n)$ in $d = \sum_{i=0}^{n} a_i 2^i$.

Corollary 1.1: The decimal integer d contains 2^k in its binary number representation if and only if $[d \cdot 2^{-k}]$ is odd.
Proof: Put $B = 2$ in Theorem 1.1.
Example 1.1: Does 94 contain 2^2 in its binary number representation?
Consider,

$$[\frac{94}{4}] = [23\ 1/2] = 23, \text{ odd.}$$

Therefore, 94 does contain 2^2 in its binary number representation. In fact 94 is a brief representation for *1 0 1 1 1 1 0*, where the *1* in the third position from the right indicates the presence of $1 \cdot 2^2$.

$C^n \mid A$; A, C, n INTEGERS

A certain class of problems have the *a priori* condition that only those integers which satisfy any other conditions of the problem are to be called solutions. This is the case with Diophantine analysis (Landau, 1958). The following results are useful, in some instances, for the purpose of giving a quick check to determine whether the *a priori* necessary condition is satisfied.

Theorem 2.1: Put $d = \sum_{i=0}^{m} a_i B^i$, where B is some integer greater than 1, each a_i $(i = 0, 1, \ldots, m)$ is an integer satisfying the condition $0 \leq a_i < B$ and m is a non-negative integer. Put $d^* = \sum_{i=0}^{n-1} a_i B^i$, where n is an integer satisfying the condition, $0 \leq n \leq m$. Put $\overline{d} = \sum_{i=n}^{m} a_i B^i$. If, and only if,

(i) there exists an r_1 such that $0 \leq r_1 < C^n$ and $d^* \equiv r_1 \pmod{C^n}$

and (ii) there exists an r_2 such that $0 \leq r_2 < C^n$ and $\overline{d} \equiv r_2 \pmod{C^n}$, implies either

(iii) $r_1 + r_2 = 0$ or $r_1 + r_2 = C^n$

then $C^n | d$.

Proof:

(1) $d^* = I_1 C^n + r_1$, where $0 \leq r_1 < C^n$ and I_1 is some integer,

(2) $\overline{d} = I_2 C^n + r_2$, where $0 \leq r_2 < C^n$ and I_2 is some integer.

But,

(3) $d = d^* + \overline{d} = (I_1 + I_2) C^n + (r_1 + r_2)$.

The "if" case is valid since, by hypothesis, either $(r_1 + r_2) = \begin{cases} 0 \\ C^n, \end{cases}$ but in either case $C^n | d$.

To show the "only if" case assume the hypothesis and the negative of the conclusion and arrive at the following contradiction:

By hypothesis, there exists an integer I_3 such that

(4) $d = I_3 C^n$.

Therefore, from (3) and (4) $C^n | (r_1 + r_2)$. But from (1) and (2), $0 \leq (r_1 + r_2) < 2C^n$, that is, $0 \leq \frac{(r_1 + r_2)}{C^n} < 2$.

The negative of the conclusion asserts that $\frac{r_1 + r_2}{C^n} \neq 0$ and $\frac{r_1 + r_2}{C^n} \neq 1$. Thus we arrive at the assertion that $C^n \nmid (r_1 + r_2)$.

Corollary 2.1: If $C^n | \overline{d}$ and $C^n | d^*$, then $C^n | d$.

Proof: $r_1 = r_2 = 0$ and apply theorem 2.1.

Corollary 2.2: If

(i) $C | B$ or $C | a_i$, $(i = n, n + 1, \ldots, m)$ and

(ii) $C^n | d^*$, then $C^n | d$.

Proof: If $C | B$ or $C | a_i$, $(i = n, n + 1, \ldots, m)$ then $C^n | \overline{d}$. Now apply corollary 2.1.

Example 2.1:

Does $2^3 | 3\,1\,4\,1\,5\,9\,2\,6\,5\,3\,6$?
Yes! Since $8 | 5\,3\,6$.

Does $2^4 | 2\,7\,1\,8\,2\,8\,1\,8\,2\,8\,5$?
No! Since $1\,6 \nmid 8\,2\,8\,5$.

Summary

Five general propositions dealing with the application of elementary number theory to numerical aspects of symbolic logic and Diophantine analysis are proved. For concreteness, some specific examples are given to demonstrate the use of the propositions.

Literature Cited

Abrahams, P. W. 1955. The Modified Quine-McCluskey reduction procedure. Elec. Eng. Dept. Memo., Mass. Inst. Tech., 4 pp.

Caldwell, S. H. 1958. Switching circuit and logical design. New York, John Wiley and Sons, 686 pp.

Landau, E. 1958. Elementary number theory. New York, Chelsea Publ. Co., 256 pp.

Mullin, A. A. 1958. A residue test for boolean functions. Trans. Ill. St. Acad. Sci., 51 (3 and 4): 14-19.

Manuscript received September 19, 1959.