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 \( d = \sum_{i=0}^{n} a_i \cdot 2^i \), 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 \( P_k = \lfloor \frac{d}{B^k} \rfloor \), where if \( a \) is real, \( \lfloor a \rfloor \) is the greatest integer not exceeding \( a \). Then \( P_k \equiv \lfloor \frac{a_k}{B^k} \rfloor \) \( \pmod{B} \), \((k = 0, 1, ..., n)\).

Proof: \( d = \sum_{i=1}^{n-k} i k \cdot a_i \cdot B^i \cdot a_k + \sum_{i=1}^{n-k} B^i \). Put \( f_k = \sum_{i=1}^{k} a_i \cdot B^i \). Since \( m = ax \cdot j = B - I \), then

\[ 0 \leq f_k < (B - I) \cdot i = 1, B^i = 1. \]

Putting \( S_k = \sum_{i=1}^{n-k} a_i \cdot B^i \), 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, \( P_k \equiv a_k \pmod{B} \).

Definition 1.1: The decimal integer \( d \) is said to contain \( 2^k \) in its binary number representation if and only if \( a_k = l \)

\((k = 0, 1, ..., n)\) in \( d = \sum_{i=0}^{n} a_i \cdot 2^i \).

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,

\[ \lfloor \frac{94}{4} \rfloor = \lfloor \frac{23}{2} \rfloor = 23, \text{ odd.} \]

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

Cn | A; A, C, n INTEGERS

A certain class of problems have the a priori condition that only those

[102]
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: \[ d = \sum_{i=0}^{m} a_i B^i, \]
where \( B \) is some integer greater than
I, each \( a_i \), \( (i = 0, 1, ..., m) \) 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
\[ d = \sum_{i=0}^{m} a_i B^i. \]
If, and only if,
(i) there exists an \( r \), such that
\[ \theta \leq r < C^a \]
and \( d^* \equiv r \text{ (mod } C^a) \);
and (ii) there exists an \( r \), such that
\[ \theta \leq r < C^a \]
and \( \overline{d} \equiv r \text{ (mod } C^a) \), implies either
(iii) \( r_1 + r_2 = 0 \) or \( r_1 + r_2 = C^a \),
then \( C^a | d \).

Proof:
(1) \( d^* = I\theta + r_n \), where \( 0 \leq r_n < C^a \)
and \( I_\theta \) is some integer,
(2) \( \overline{d} = I_\theta C^a + r_\theta \), where \( 0 \leq r_\theta < C^a \)
and \( I_\theta \) is some integer.

But,
(3) \[ d = d^* + \overline{d} = (I_\theta + I_\theta) C^a + \]
\[ (r_1 + r_2). \]

The “if” case is valid since, by hypo-
thesis, either \( (r_1 + r_2) = 0 \) but in
either case \( C^a | d \).

To show the “only if” case assume the hypothesis and the negative of the conclusion and arrive at the following con-
tradiction:

By hypothesis, there exists an integer
(4) \( d = I_\theta, C^a. \)

Therefore, from (3) and (4) \( C^a | (r_1 + r_2) \). But from (1) and (2), \( \theta \leq (r_1 + r_2) < 2C^a \), that is, \( \theta \leq (r_1 + r_2) < 2 \).

The negative of the conclusion asserts
\[ \frac{r_1 + r_2}{C^a} + \theta = 0 \text{ and } \frac{r_1 + r_2}{\overline{d}} + \overline{d} = 1. \]
we arrive at the assertion that \( C^a \nmid (r_1 + r_2) \).

Corollary 2.1: If \( C^a | \overline{d} \) and \( C^a | d^* \), then
\( C^a | \overline{d}. \)

Proof: \( r_1 = r_\theta = 0 \) and apply theorem 2.1.

Corollary 2.2: If
(i) \( C^a | B \) or \( C^a | a_i, \ (i = n, n + 1, \)
and
(ii) \( C^a | d^* \), then \( C^a | \overline{d}. \)

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

Example 2.1:

Does \( 2^a | 3 1 4 1 5 9 2 6 5 3 6 \) ?
Yes! Since \( 8 \text{ } 5 \text{ } 3 \text{ } 6 \).

Does \( 2^a | 2 7 1 8 2 8 1 8 2 8 5 \) ?
No! Since \( 1 6 \text{ } 4 \text{ } 8 \text{ } 2 8 5 \).

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


Manuscript received September 19, 1959.