ON ADDITION CHAINS

ALFRED BRAUER

We consider a set $a_0=1<a_1<a_2<\cdots<a_r=n$ of integers such that every element a_ρ can be written as sum $a_\sigma+a_\tau$ of preceding elements of the set. Such sets of integers have been called "addition chains (Additionsketten) for n" by A. Scholz.† For example, for $n=666$,

$$1, 2, 4, 8, 16, 24, 40, 80, 160, 320, 640, 664, 666$$

forms an addition chain with $r=12$; the same holds for

$$1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 324, 648, 666.$$

In any case, we must have $a_1=2$ and $a_2=3$ or 4.

By the length $l=l(n)$ of n, Scholz understands the smallest l for which there exists an addition chain $a_0, a_1, \cdots, a_l=n$.

The following question leads to addition chains: The least positive residue of $c^n \pmod m$ (c, m, n given integers) is to be formed using the smallest possible number of multiplications. Then $l(n)$ multiplications will always suffice.

A. Scholz published the following inequalities for $l(n)$ in the form of problems:

$$m+1 \leqq l(n) \leqq 2m \quad \text{for} \quad 2^m+1 \leqq n \leqq 2^{m+1}, \qquad m \geqq 1, \tag{1}$$

$$l(ab) \leqq l(a)+l(b). \tag{2}$$

In (1), we have $l(n)<2m$ whenever $m>2$; moreover,

$$l(2^{m+1}-1) \leqq m+l(m+1). \tag{3}$$

In connection with (3), Scholz surmises that (1) can be improved generally. He further raises the question of whether or not the inequality

$$1 \leqq \limsup_{n\to\infty} \frac{\log 2}{\log n} l(n) \leqq 2, \tag{4}$$

which easily follows from (1), can be improved.

It is easy to prove the formulas (1) and (2). I cannot decide whether (3) is always true. In the following, I will show that

$$l(2^{m+1}-1) \leqq m+l^*(m+1),$$

† Jahresbericht der deutschen Mathematiker-Vereinigung, class II, vol. 47 (1937), p. 41.