COLLOQUIUM MATHEMATICUM

VOL. XX 1969 FASC. 1

A THEOREM IN ADDITIVE NUMBER THEORY

BY

ROGER CROCKER (LONDON)

It has been shown [1], [2], by different methods that there is an infinity of positive odd integers not representable as the sum of a prime and a (positive) power of 2, thus disproving a conjecture to the contrary that had been made last century. It is easily shown [4] that for each fixed (integral) $k \geqslant 2$, there is an infinity of positive integers not representable as the sum of a prime and the k^{th} power of a positive integer. The purpose of this paper is to present

THEOREM I. *For each fixed (integral) $k \geqslant 2$, there is an infinity of positive odd integers neither representable as the sum of a prime and a positive power of 2, nor representable as the sum of a prime and the k^{th} power of a positive integer.*

Notation. Throughout this paper, each p_i represents an odd prime. All quantities are integers and usually positive integers.

First, to reproduce the counterexample in [2] — slightly modified as in [3], consider an "overlapping" congruence system (1) (i.e., given any positive integer, it will satisfy — at least — one of equations of the system; several such systems occur below):

$$x_i \equiv a_i (\operatorname{mod} n_i), \quad 1 \leqslant i \leqslant h. \tag{1}$$

From this system, one constructs the following simultaneous congruence system

$$\tau \equiv \begin{cases} 2^{a_i} (\operatorname{mod} p_i), \ 1 \leqslant i \leqslant h, & \text{where } 2^{n_i} \equiv 1 (\operatorname{mod} p_i); \\ c (\operatorname{mod} p_{h+1}), & \text{where } p_{h+1} = 2^p - 1, p \text{ a prime } (^1), \text{ and} \\ \qquad c \not\equiv p_i + 2^d (\operatorname{mod} p_{h+1}) & \text{for } 0 \leqslant d \leqslant p-1, \ 1 \leqslant i \leqslant h; \\ 1 (\operatorname{mod} 2) \end{cases} \tag{2}$$

with all moduli p_i, $1 \leqslant i \leqslant h+1$, distinct. As shown in [2] and [3], none of these odd integers is the sum of a prime and a power of 2, so that the counterexample is complete.

(1) Any prime may be chosen for p so long as p_{h+1} is distinct from the other p_i's.

Now choose a fixed $k \geqslant 2$. Taking (2), suppose 2 to be a k^{th} power residue of each p_i, $1 \leqslant i \leqslant h$. This is a sufficient (though not a necessary) condition that 2^{a_i} be a k^{th} power residue of the corresponding p_i. Thus, for each i, there exists an s_i such that $s_i^k \equiv 2^{a_i} (\operatorname{mod} p_i)$; s_i may then be replaced by any integer $r_i \equiv s_i (\operatorname{mod} p_i)$. Also, suppose c to be a k^{th} power residue of p_{h+1} so that there exists an s_{h+1} such that $s_{h+1}^k \equiv c (\operatorname{mod} p_{h+1})$; then s_{h+1} may be replaced by $r_{h+1} \equiv s_{h+1} (\operatorname{mod} p_{h+1})$. Hence, every solution of the simultaneous congruence system $w \equiv s_i (\operatorname{mod} p_i)$, $1 \leqslant i \leqslant h+1$, $w \equiv 1 (\operatorname{mod} 2)$, will have the property that $w^k \equiv 2^{a_i} (\operatorname{mod} p_i)$ for all $1 \leqslant i \leqslant h$ and that $w^k \equiv c (\operatorname{mod} p_{h+1})$; also that $w^k \equiv 1 (\operatorname{mod} 2)$. The solutions to this system form an arithmetic progression; if w' is one solution, the others may be written as

$$w = w' + j \prod_{i=1}^{h+1} p_i,$$

j any positive integer. Now consider w^k; none of these (odd) integers is the sum of a prime and a power of 2 (since they all satisfy (2)). It is trivially shown (almost exactly as in [4]) that for an infinity of j, w^k is not the sum of a prime and a k^{th} power, for the chosen k.

Thus, to establish the validity of Theorem I for any particular k, an "overlapping" congruence system (1) must be found such that 2 is a k^{th}-power residue of p_i, $1 \leqslant i \leqslant h$; also c must be a k^{th}-power residue of p_{h+1} (as well as satisfying the condition imposed upon it in (2)).

It is immediately seen that if Theorem I is valid for all prime values of k, it is valid for all k; hence in the following, k may be considered prime (inclusive of 2).

First consider any particular (prime) $k \geqslant 5$. Take $0 (\operatorname{mod} 2)$, $0 (\operatorname{mod} 3)$, $1 (\operatorname{mod} 4)$, $3 (\operatorname{mod} 8)$, $7 (\operatorname{mod} 12)$, $23 (\operatorname{mod} 24)$ for the choice of (1). Then one constructs for (the simultaneous congruence system) (2)

$$t \equiv 1 (\operatorname{mod} 3),\ t \equiv 1 (\operatorname{mod} 7),\ t \equiv 2 (\operatorname{mod} 5),\ t \equiv 2^3 (\operatorname{mod} 17),$$

$$t \equiv 2^7 (\operatorname{mod} 13),\ t \equiv 2^{23} (\operatorname{mod} 241),\ t \equiv 16 (\operatorname{mod} 31),\ t \equiv 1 (\operatorname{mod} 2).$$

Now for $p_i = 3, 5, 7, 13, 17$ and $k \geqslant 5$, one has $(k, p_i - 1) = 1$ so that 2 is a k^{th}-power residue of these p_i's (by the well-known generalization of Euler's criterion). For $p_i = 241$ or 31 and $k > 5$, one again has $(k, p_i - 1) = 1$ so that 2 is a k^{th}-power residue of 241 and 16 is a k^{th}-power residue of 31. For $k = 5$, since $241 \mid 2^{48} - 1$, 2 is a k^{th}-power residue of 241. Similarly, for $k = 5$, 16 is a k^{th}-power residue of 31 (it also satisfies the condition for c in (2)).

Now consider $k = 3$. Take $0 (\operatorname{mod} 2)$, $1 (\operatorname{mod} 4)$, $3 (\operatorname{mod} 8)$, $0 (\operatorname{mod} 5)$, $3 (\operatorname{mod} 10)$, $7 (\operatorname{mod} 20)$, $37 (\operatorname{mod} 40)$ for the choice of (1). Then one constructs for (2)

$$t \equiv 1 (\mathrm{mod}\ 3),\ t \equiv 2 (\mathrm{mod}\ 5),\ t \equiv 2^3 (\mathrm{mod}\ 17),\ t \equiv 1 (\mathrm{mod}\ 31),$$
$$t \equiv 2^3 (\mathrm{mod}\ 11),$$
$$t \equiv 2^7 (\mathrm{mod}\ 41),\ t \equiv 2^{37} (\mathrm{mod}\ 61681),\ t \equiv 64 (\mathrm{mod}\ 127),\ t \equiv 1 (\mathrm{mod}\ 2).$$

Now for $p_i = 3, 5, 11, 17, 41$, it is true that $(3, p_i - 1) = 1$ so that 2 is a cubic residue of p_i (²).

For $p_i = 31$ or 61681, $2^{(p_i-1)/3} \equiv 1 (\mathrm{mod}\ p_i)$ so that 2 is a cubic residue of these p_i. Finally, it is immediate that 64 is a cubic residue of 127 (it also satisfies the condition for c).

Finally, consider $k = 2$, certainly the most interesting and also the hardest special case. Take

$$0 (\mathrm{mod}\ 2),\ 0 (\mathrm{mod}\ 3),\ 0 (\mathrm{mod}\ 5),\ 3 (\mathrm{mod}\ 8),\ 1 (\mathrm{mod}\ 15),\ 7 (\mathrm{mod}\ 16),$$
$$13 (\mathrm{mod}\ 20),\ 17 (\mathrm{mod}\ 24),\ 25 (\mathrm{mod}\ 32),\ 37 (\mathrm{mod}\ 40),\ 47 (\mathrm{mod}\ 48),$$
$$31 (\mathrm{mod}\ 48),\ 49 (\mathrm{mod}\ 60),\ 17 (\mathrm{mod}\ 80),\ 29 (\mathrm{mod}\ 96),\ 29 (\mathrm{mod}\ 120),$$
$$137 (\mathrm{mod}\ 160),\ 101 (\mathrm{mod}\ 240),\ 461 (\mathrm{mod}\ 480)$$

for the choice of (1). Then one considers (2) found from (1), with $p_{h+1} = 2^{13} - 1$ so that $t \equiv c (\mathrm{mod}\ 2^{13} - 1)$. Now it can easily be verified numerically that 2 is a quadratic residue of (distinct) (³) p_i's corresponding to those $n_i \leqslant 60$. Corresponding to those $n_i > 60$, it is also easily shown that there is a (different) p_i in each case having 2 as a quadratic residue. For consider $2^{g \cdot 2^m} - 1$, g any odd positive integer and $m \geqslant 3$. Now there exists a prime, say p_m, such that 2 belongs to $g \cdot 2^m \,\mathrm{mod}\, p_m$ (from a well-known theorem). Hence $p_m \equiv 1 (\mathrm{mod}\ g \cdot 2^m)$ so that $p_m \equiv 1 (\mathrm{mod}\ 8)$. Thus, 2 is a quadratic residue of p_m. Since the above $n_i > 60$ are of the form $g \cdot 2^m$ where $m \geqslant 3$, one obtains the desired result. Finally, there exists a positive integer c which is a quadratic residue of $2^{13} - 1$ and which also satisfies the condition for c in (2), where $p = 13$. For there are $2^{12} - 1$ distinct quadratic residues of $2^{13} - 1$. There are 13 distinct residues of $2^d (\mathrm{mod}\ 2^{13} - 1)$; there are also at most h distinct residues of $p_i (\mathrm{mod}\ 2^{13} - 1)$, $h = 19$. Hence there are at most 13 (19)

(²) Here in particular, when $p_i = 3$, 17, or 31, for 2^{α_i} to be a cubic residue of the corresponding p_i, it is sufficient but not necessary that 2 be a cubic residue of p_i. However, for the uniformity of argument, this fact is not used.

(³) In principle at least; because of the large p_i's occurring, the arguments below are mainly those of proving existence. However, for $n_i < 60$, $p_i = 3, 7, 31, 17, 151, 257, 41, 241, 65537, 61681, 97, 673, 1321$.

distinct residues of p_i+2^d (mod $2^{13}-1$) from which, since 13 (19) $< 2^{12}-1$, the desired result (the existence of c) follows (in fact, there are at least $2^{12}-1-13$ (19) or 3848 possibly distinct choices for c), q.e.d.

Obviously, Theorem I holds for "the k^{th} power of a *negative* integer" as well, since [4] does.

REFERENCES

[1] R. Crocker, *A theorem concerning prime numbers*, Mathematical Magazine 34, No 6 (1960/61), p. 316 and 344.

[2] P. Erdős, *On a problem concerning congruence systems*, Mat. Lapok 3 (1952), p. 122-128.

[3] W. Sierpiński, *Elementary theory of numbers*, Warszawa 1964, Chap. XII.

[4] *Representation of integers in the form: a k-th power plus a prime*, in Advanced problems and solutions, American Mathematical Monthly 56 (1949), p. 561.

QUEEN ELIZABETH COLLEGE
UNIVERSITY OF LONDON

Reçu par la Rédaction le 23. 1. 1968