PACIFIC JOURNAL OF MATHEMATICS
Vol. 36, No. 1, 1971

ON THE SUM OF A PRIME AND OF TWO POWERS OF TWO

ROGER CROCKER

It has been shown 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 which had been made in the nineteenth century. The question then arises as to whether or not all sufficiently large positive odd integers can be represented as the sum of a prime and of *two* positive powers of 2; that is, as $p + 2^a + 2^b$, where a, $b > 0$ and p is prime. (The corresponding question has been discussed for bases other than 2 but is really quite trivial.) Theorem I gives a negative answer to this question.

THEOREM I. **There is an infinity of distinct, positive odd integers not representable as the sum of a prime and of two positive powers of 2.**

NOTATION. Throughout this paper, each p_i represents an odd prime. All quantities are integers and usually positive integers. As usual, "prime" is understood to mean "positive prime".

The method used in [1] gives Lemma I and Lemma II, below. The method used in [4] a slight modification of [3] is then combined with Lemma II to show that there is an infinity of positive odd integers not the sum of a prime and a positive power of 2 nor the sum of a prime and of two *distinct* positive powers of 2. Theorem I follows immediately.

First, to reproduce the counterexample in [4, p. 413] slightly generalized here, consider an "overlapping" congruence system (1) (i.e., given any positive integer, it will satisfy at least one of the equations of the system; such a system occurs below)

$$x_i \equiv a_i \pmod{m_i}\,, \quad 1 \leqq i \leqq h\,. \tag{1}$$

Suppose that from this system, one can construct the following simultaneous congruence system

$$t \equiv \begin{cases} 2^{a_i} \pmod{p_i},\ 1 \leqq i \leqq h, \quad \text{where } 2^{m_i} \equiv 1 \pmod{p_i}; \\ c \pmod{p_{h+1}}, \text{ where } p_{h+1} = 2^p - 1,\ p \text{ a prime, and} \\ \quad c \not\equiv p_i + 2^d \pmod{p_{h+1}} \text{ for } 0 \leqq d \leqq p-1,\ 1 \leqq i \leqq h; \\ 1 \pmod 2 \end{cases} \tag{2}$$

with all moduli p_i, $1 \leqq i \leqq h+1$, distinct. (The m_i need not be

distinct and p may be any prime, so long as all p_i are distinct.) As shown by the method used in [4, p. 413], none of these odd integers is the sum of a prime and a power of 2, so that the counterexample is valid. Finally, in reference to the supposition just above, for the actual numerical choice of (1) one must show the existence of *distinct* p_i and of c satisfying the above conditions; this will be done later for the choice of (1) made in this paper.

Now one arrives at

LEMMA I.[1] *For every* $n \geqq 3$, $2^{2^n}-1$ *cannot be expressed as the sum of a prime and of two distinct positive powers of* 2.

Proof. Taking $a > b$ (which results in no loss of generality), consider $2^{2^n} - 1 - 2^a - 2^b = 2^{2^n} - 1 - 2^b\,(2^{a-b} + 1)$ where $a,\ b < 2^n$. Since $a - b < 2^n$, it follows that for each $a - b$,

$2^{2^r} + 1 \mid 2^{2^n} - 1 - 2^b(2^{a-b} + 1)$ for some $r < n$ (r being the largest power of 2 contained in $a - b$). But since $2^{2^n} - 1 - 2^{2^{n-1}} - 2^{2^{n-2}} = 2^{2^{n-2}} - 1 > 2^{2^{n-1}} + 1$ for $n \geqq 3$, it follows that $2^{2^n} - 1 - 2^a - 2^b > 2^{2^r} + 1$. The lemma follows.

The result in Lemma I may be generalized very considerably to give

LEMMA II.[2] *For* $n \geqq 3$ *and* $w \equiv 1 \pmod{16}$, *consider* $w \prod_{i=0}^{n-1} B_i \leqq 2^{2^n} - 1$, *where* $B_i \mid 2^{2^i} + 1$ *and* $B_i > 1$ (*though not necessarily prime or* $< 2^{2^i} + 1$). *Then* $w \prod_{i=0}^{n-1} B_i$ ($\leqq 2^{2^n} - 1$) *cannot be expressed as the sum of a prime and of two positive distinct powers of* 2.

Proof. If $n = 3$, 4 or 5, Lemma I is immediately applicable. Suppose $n \geqq 6$. Consider

$$w \prod_{i=0}^{n-1} B_i - 2^a - 2^b = w \prod_{i=0}^{n-1} B_i - 2^b\,(2^{a-b} + 1) > 0$$

[1] This Lemma was communicated to me by A. Schinzel after he had read [**1**], and also appears in [**4**, p. 413] where some acknowledgment is made of [**1**]. I arrived at Lemma I independently, however but did not publish it, since by itself it is quite incomplete. It might be added that, contrary to the impression given in [**4** p. 414], Lemma I is a trivial generalization of [**1**] using exactly the same method; this can easily be seen by comparing the proof in [**1**] with the above proof of Lemma I.

[2] 16 is far from the only possible modulus for w; any power of two > 16 would be suitable. For example, 64 could be used; $w \equiv 1 \pmod{64}$, $w \equiv 3 \pmod{64}$, or many other residue classes (mod 64) could then be chosen, with only obvious and trivial changes in the subsequent proofs. If $w \equiv 3 \pmod{64}$ is chosen, the integers satisfying Theorem I $\equiv 1 \pmod 4$. Incidentally, it occurred to me at first that it might be possible to "combine" Lemma I with the method in [**3**]. I then realized that some generalization of Lemma I would be necessary. My search led to Lemma II, which I then was able to "combine" with the method of [**4**]).

where (without loss of generality) $a > b$; then $a,\ b < 2^n$ and so $a - b < 2^n$. Now for each $a - b$, $B_r \mid w \prod_{i=0}^{n-1} B_i - 2^b(2^{a-b} + 1)$ for some $r < n$, remembering that $B_r \mid 2^{2^r} + 1 \mid 2^{a-b} + 1$ for some $r < n$.

Now suppose $w \prod_{i=0}^{n-1} B_i - 2^a - 2^b = B_r$; then $w \prod_{i=0}^{n-1} B_i = 2^a + 2^b + B_r$. Now $\prod_{i=0}^{n-1} B_i = \prod_{i=0}^{4} B_i \prod_{i=5}^{n-1} B_i \equiv -1 \pmod{16}$ (remembering that $B_i \equiv 1 \pmod{2^{i+1}}$ or for $i \geqq 5$, $B_i \equiv 1 \pmod{16}$). Since $w \equiv 1 \pmod{16}$, it follows that $w \prod_{i=0}^{n-1} B_i \equiv -1 \pmod{16}$. Now with $r < n$, one has $w \prod_{i=0}^{n-1} B_i > B_0 B_1 B_r = 15 B_r$ so that $w \prod_{i=0}^{n-1} B_i - B_r > 14 B_r \geqq 42$ (since $B_r \geqq 3$); thus $2^a + 2^b \geqq 42$ and since $a > b$, one must have $a > 3$. Therefore $2^a \equiv 0 \pmod{16}$. But since $b \geqq 1$, $r \geqq 0$, one has 2^b congruent (mod 16) to 0, 2, 4 or 8 and B_r congruent (mod 16) to 1, 3 or 5. Hence $2^a + 2^b + B_r \not\equiv -1 \pmod{16}$; therefore $w \prod_{i=0}^{n-1} B_i \neq 2^a + 2^b + B_r$. Thus $w \prod_{i=0}^{n-1} B_i - 2^a - 2^b \neq B_r$. The lemma follows.

Proof of Theorem I. Take $2^{2^n} - 1/G_k$ for some chosen fixed k, where $n > k$, $G_k \mid 2^{2^k} + 1$ ($k = 10$ will actually be chosen later), and $1 < G_k < 2^{2^k} + 1$. Now assume that one can choose an overlapping congruence system [(1), above] such that in the corresponding simultaneous congruence system [(2), above] one can have

$$(p_i,\ 2^{2^n} - 1) = 1 \text{ for any } p_i \text{ and } n$$

and also

$$16 \prod_{i=1}^{k+1} p_i < G_k, \text{ say } \left(16 \prod_{i=1}^{k+1} p_i\right) v < G_k < (v+1) \left(16 \prod_{i=1}^{k+1} p_i\right)$$

for some *fixed* $v \geqq 1$.

Consider the system (2) having these properties, together with the *additional* simultaneous [3] conditions (3)

$$(3) \qquad \begin{aligned} t &\equiv 0 \left(\mathrm{mod}\ \frac{2^{2^n}-1}{G_k}\right) \\ t &\equiv -1 \pmod{16} \\ t &\leqq 2^{2^n} - 1\ ; \end{aligned}$$

choose any $n (> k)$. Call this enlarged simultaneous system S_n.

Now by the Chinese Remainder Theorem, S_n is satisfied by any integer t (and only those integers) such that

$$t \equiv q_n \left(\mathrm{mod}\ 16 \frac{2^{2^n}-1}{G_k} \prod_{i=1}^{k+1} p_i\right), \qquad t \leqq 2^{2^n} - 1$$

where one may consider that $0 < q_n < 16 (2^{2^n} - 1/G_k) \prod_{i=1}^{k+1} p_i$ and q_n, itself satisfying S_n, is obviously fixed for the chosen n (but from (3)

[3] The condition $t \equiv -1 \pmod{16}$ absorbs, of course, that in (2), $t \equiv 1 \pmod{2}$.

depends on the choice of n; $q_n \neq 0$). Clearly, there are $v\,(\geqq 1)$ or $v+1$ positive integers satisfying this congruence and $\leqq 2^{2^n}-1$, that is, satisfying the conditions in S_n. Now from (3), each of these (v or $v+1$) integers satisfying the conditions in S_n satisfies Lemma 2. For let B_i in Lemma 2 be $2^{2^i}+1$ here except when $i=k$, in which case let $B_k = 2^{2^k}+1/G_k$ (the B_i satisfy the conditions required of them in the hypothesis of Lemma 2). Then $\prod_{i=0}^{n-1} B_i = 2^{2^n}-1/G_k$, so that from the first two conditions in (3), one has $t = w\prod_{i=0}^{n-1} B_i \equiv -1 \pmod{16}$, where since $\prod_{i=0}^{n-1} B_i \equiv -1 \pmod{16}$, one has $w \equiv 1 \pmod{16}$. From the remaining condition in (3), $t \leqq 2^{2^n}-1$ so that $t = w\prod_{i=0}^{n-1} B_i \leqq 2^{2^n}-1$. Hence positive integers satisfying the conditions in S_n satisfy the hypothesis of Lemma 2. Thus each of these (v or $v+1$) positive integers is not the sum of a prime and of two distinct positive powers of 2. However each of these integers satisfies the system (2) and therefore is not the sum of a prime and a power of 2 (and[4] thus of a prime and of two identical powers of 2). Hence each of these integers satisfies (the desired property in) Theorem I. Now for $n+1\,(>k+1)$, each of the (v or $v+1$) positive integers satisfying (S_{n+1} and hence) Theorem I is divisible by $2^{2^n}+1$ (using $n+1$ in place of n in (3)) and hence $\geqq 2^{2^n}+1$; for n, each of the integers $< 2^{2^n}+1$. Thus the integers, satisfying Theorem I, which one obtains for integer n are less than those obtained for the successive integer $n+1$. Since *any* $n\,(>k)$ may be chosen, Theorem I follows.

Finally, choose $k=10$, $G_k = 2^{2^{10}}+1/2^{12}\cdot 11131+1$, and (1) to be

0(mod 3) 0(mod 5) 1(mod 9) 1(mod 10) 8(mod 12) 8(mod 15) 4(mod 18) 7(mod 20) 5(mod 24) 29(mod 30) 2(mod 36) 14(mod 36) 17(mod 40) 34(mod 45) 43(mod 45) 13(mod 48) 37(mod 48) 16(mod 60) 19(mod 60) 26(mod 72) 62(mod 72) 52(mod 90) 37(mod 120) 49(mod 144) 121(mod 144) 103(mod 180) 106(mod 180) 229(mod 360).

(1) can be shown to be an overlapping congruence system by a very straightforward (though lengthy) numerical[5] method – namely by writing all these congruences (mod 720), 720 being the L. C. M. of the m_i's chosen here, and then checking that one obtains a complete residue system mod 720. (For each congruence (mod m_i) one obtains, of course, $720/m_i$ congruences (mod 720) which take the form a_i+fm_i (mod 720), $0 \leqq f < 720/m_i$).

Taking $p_{h+1} = 2^{13}-1$ (for an appropriate c), it will now be shown

[4] Actually, not being the sum of a prime and a positive power of 2 implies not being the sum of a prime and of two identical positive powers of 2 but is really slightly stronger (since 2 itself is a power of 2 but not the sum of two identical positive powers of 2).

[5] Actually there is a relatively short way of showing this result related to a short cut I used originally to construct this system. However I hope to make this a topic of another paper.

that one can in fact construct a system (2) such that the conditions stated above for the p_i in system (2) are satisfied. For it is well known that for any positive integer $e \neq 6$, there is at least one prime, say p', such that 2 belongs to $e \pmod{p'}$. Hence for each distinct[6] m_i in the numerical choice for (1), there exists a p_i such that 2 belongs to $m_i \pmod{p_i}$; (this can also be shown numerically); these p_i are of course distinct. For each nondistinct m_i occurring in the above numerical choice for (1), the existence of a *distinct* p_i such that 2 belongs to $m_i \pmod{p_i}$ has in fact been shown for general purposes numerically [2]. Now since $m_i = 2^{g_i}k'$ where k' is odd and > 1 in the numerical choice for (1), $m_i \nmid 2^n$ (since $k' \nmid 2^n$). But 2 belongs to $m_i \pmod{p_i}$; hence $2^{2^n} \not\equiv 1 \pmod{p_i}$ for otherwise m_i would divide 2^n. Thus $(p_i, 2^{2^n}-1) = 1$. Also $13 \nmid 2^n$; since 2 belongs to $13 \pmod{p_{h+1}}$, $2^{2^n} \not\equiv 1 \pmod{p_{h+1}}$. Thus $(p_{h+1} = 2^{13}-1, 2^{2^n}-1) = 1$. Also $13 \nmid m_i$ *here*; again $(p_{h+1}, p_i) = 1$ or $p_{h+1} \neq p_i$, $1 \leqq i \leqq h$. Finally by simple numerical calculation and estimation,

$$16 \prod_{i=1}^{h+1} p_i < 2^{434} < 2^{998} < G_k;$$

v thus exists and in fact is seen to be very large here. It remains to show the existence of c satisfying the required condition in system (2). There are $2^{13}-1$ possible distinct residues of $2^{13}-1 (= p_{h+1})$; there are also 13 distinct residues of $2^d \pmod{2^{13}-1}$ and at most 28 $(=h)$ distinct residues $(\text{mod } 2^{13}-1)$ of the p_i's (not counting p_{h+1} here), and thus there are at most 13 (28) distinct residues of $p_i + 2^d \pmod{2^{13}-1}$. Since $13\ (28) < 2^{13}-1$, the existence of c follows. (There are, in fact, at least $2^{13} - 1 - 13\ (28) = 7827$ possible distinct choices for c).

REFERENCES

1. R. Crocker, *A theorem concerning prime numbers*, Math. Magazine **34** (1960/61), 316 and 344.
2. L. E. Dickson, *History of the Theory of Numbers*, New York, 1952.
3. P. Erdös, *On a problem concerning congruence systems*, Mat. Lapok **3** (1952), 122-128.
4. W. Sierpinski, *Elementary Theory of Numbers*, Warszawa, 1964.

Received September 3, 1969.

JOHN CARROLL UNIVERSITY

[6] By a distinct m_i in the system is meant an $m_i \neq m_j$, if $i \neq j$.