MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 79–81

Not Every Number is the Sum or Difference of Two Prime Powers

By Fred Cohen and J. L. Selfridge

Abstract. Every odd number less than 262144 is the sum or difference of a power of two and a prime. An interesting example is $113921 = p - 2^{141}$. Using covering congruences, we exhibit a 26-digit odd number which is neither the sum nor difference of a power of two and a prime. The method is then modified to exhibit an arithmetic progression of numbers which are not the sum or difference of two prime powers.

In 1950, P. Erdös [1] used covering congruences to exhibit numbers not of the form $2^n + p$. Using similar methods, we study the sequences $2^n + M$ and $\pm(2^n - M)$ for a fixed integer M. In particular, we prove

THEOREM 1. *There exists an arithmetic progression of odd numbers which are neither the sum nor difference of a power of two and a prime.*

Via the proof of Theorem 1 and primality testing programs of M. Wunderlich, we show

COROLLARY. 47867742232066880047611079 *is prime and neither the sum nor difference of a power of two and a prime.*

A modification of the proof of Theorem 1 yields

THEOREM 2. *There exist odd numbers which are neither the sum nor difference of a power of two and a prime power.*

Curiously, numbers satisfying Theorem 1 appear relatively difficult to find. We have calculated (on an IBM 360) that if $M < 2^{18}$ and M is odd, then M is the sum or difference of a power of two and a prime. The M for which it is most difficult to verify this fact is 113921. Here $113921 + 2^{141}$ is prime (proved using Lucas sequences) and 141 is the smallest n such that $|113921 \pm 2^n|$ is prime.

Proof of Theorem 1 *and its Corollary.* Recall that a collection of congruences $n \equiv b_i(h_i)$ is called a covering if each integer satisfies at least one of the congruences. We exhibit two coverings of the integers. For each congruence in either cover, we require M to satisfy a related congruence. Any M which satisfies these related congruences enjoys the following property: There is a list of 18 primes such that for any nonnegative integer n, $M + 2^n \equiv 0(p_i)$ and $M - 2^n \equiv 0(p_j)$ for some p_i and some p_j in our list. Theorem 1 follows directly; the number in the corollary satisfies the requisite congruences on M.

Received May 23, 1974.
AMS (MOS) subject classifications (1970). Primary 10J15; Secondary 10–04.

Congruences on M		Covering Congruences
$M + 2^n \equiv 0(p_i)$	iff	$n \equiv b_i(h_i)$
$M + 2^1 \equiv 0(3)$		$n \equiv 1(2)$
$M + 2^0 \equiv 0(5)$		$n \equiv 0(4)$
$M + 2^6 \equiv 0(17)$		$n \equiv 6(8)$
$M + 2^{10} \equiv 0(13)$		$n \equiv 10(12)$
$M + 2^2 \equiv 0(97)$		$n \equiv 2(48)$
$M + 2^{10} \equiv 0(257)$		$n \equiv 10(16)$
$M + 2^{18} \equiv 0(241)$		$n \equiv 18(24)$
$M \equiv 2^n(p_i)$	iff	$n \equiv b_i(h_i)$
$M \equiv 2^0(3)$		$n \equiv 0(2)$
$M \equiv 2^0(7)$		$n \equiv 0(3)$
$M \equiv 2^{17}(109)$		$n \equiv 17(36)$
$M \equiv 2^{35}(37)$		$n \equiv 35(36)$
$M \equiv 2^{11}(19)$		$n \equiv 11(18)$
$M \equiv 2^5(73)$		$n \equiv 5(9)$
$M \equiv 2^{25}(331)$		$n \equiv 25(30)$
$M \equiv 2^1(41)$		$n \equiv 1(20)$
$M \equiv 2^{31}(61)$		$n \equiv 31(60)$
$M \equiv 2^2(31)$		$n \equiv 2(5)$
$M \equiv 2^3(11)$		$n \equiv 3(10)$
$M \equiv 2^4(151)$		$n \equiv 4(15)$.

End Theorem 1 proof.

We remark that it is impossible to cover both $M + 2^n$ and $M - 2^n$ with primes less than 331. More precisely, for any M there is an n such that either $M + 2^n$ or $M - 2^n$ has all its prime factors greater than 330. On the other hand, by using more primes we can dispense with 3; that is, we can find an M and a set of 42 primes so that $3M + 2^n$ and $3M - 2^n$ are simultaneously covered.

Proof of Theorem 2. We find additional conditions on M and additional primes (16 in all).

First we will insure that all terms, $M + 2^n$, divisible by 3^3 are divisible by 37 or 109. Put $M + 2^{17} \equiv 0(3^3)$ and thus 3^3 divides $M + 2^n$ when $n \equiv 17(18)$. To cover $n \equiv 17(36)$ we put $M + 2^{17} \equiv 0(37)$ and to cover $n \equiv 35(36)$ we put $M + 2^{35} \equiv 0(109)$.

Next we add conditions on the remaining primes covering $M + 2^n$.

$$M + 2^8 \equiv 0(5^2 \cdot 11) \qquad M + 2^{34} \equiv 0(97^2 \cdot 389)$$
$$M + 2^6 \equiv 0(17^2 \cdot 137) \qquad M + 2^{18} \equiv 0(241^2 \cdot 1447)$$
$$M + 2^2 \equiv 0(13^2 \cdot 53) \qquad M + 2^{10} \equiv 0(257 \cdot 673)$$

Note that we have used our cover from Theorem 1 with the positions of 13 and 97 interchanged.

Now notice that $M + 2^n$ can never be a prime power.

Consider $|M - 2^n|$. First we have $M \equiv 2^8(3^2)$ from above, and each term with $n \equiv 8(6)$ is either $n \equiv 8(12)$ or $n \equiv 2(4)$. But since $M \equiv 2^8(13)$ and $M \equiv 2^2(5)$ from above, we have a second prime factor whenever 3^2 divides $|M - 2^n|$. Finally, we add conditions for the remaining primes covering $|M - 2^n|$, noticing that the conditions for 11, 37, and 109 are consistent with those already described.

$$M \equiv 2^3(7^2 \cdot 43) \quad (\text{note } M \equiv 2^0(3 \cdot 7))$$
$$M \equiv 2^{17}(109^2 \cdot 2617)$$
$$M \equiv 2^{35}(37^2 \cdot 149)$$
$$M \equiv 2^{11}(19^2 \cdot 571)$$
$$M \equiv 2^5(73^2 \cdot 439)$$
$$M \equiv 2^{25}(331^2 \cdot 1987)$$
$$M \equiv 2^1(41^2 \cdot 83)$$
$$M \equiv 2^{31}(61 \cdot 1321)$$
$$M \equiv 2^2(31^2 \cdot 311)$$
$$M \equiv 2^3(11^2 \cdot 23)$$
$$M \equiv 2^{19}(151^2 \cdot 907) \quad (\text{note } M \equiv 2^4(3 \cdot 151))$$

Hence $|M - 2^n|$ has at least two distinct prime factors provided that it is greater than 331. End Theorem 2 proof.

A routine use of Lehmer's linear equation solver shows that 6120 6699060672 7677809211 5601756625 4819576161 6319229817 3436854933 4512406741 7420946855 8999326569 satisfies these congruences.

Finally, we wish to thank M. Wunderlich for his primality testing program and D. H. Lehmer for his multiple-precision package.

Mathematics Department
Northern Illinois University
DeKalb, Illinois 60115

1. P. ERDÖS, "On integers of the form $2^k + p$ and some related problems," *Summa Brasil. Math.*, v. 2, 1950, pp. 113–123. MR 13, 437.