SOME COUNTER-EXAMPLES IN THE ADDITIVE THEORY OF NUMBERS

A THESIS

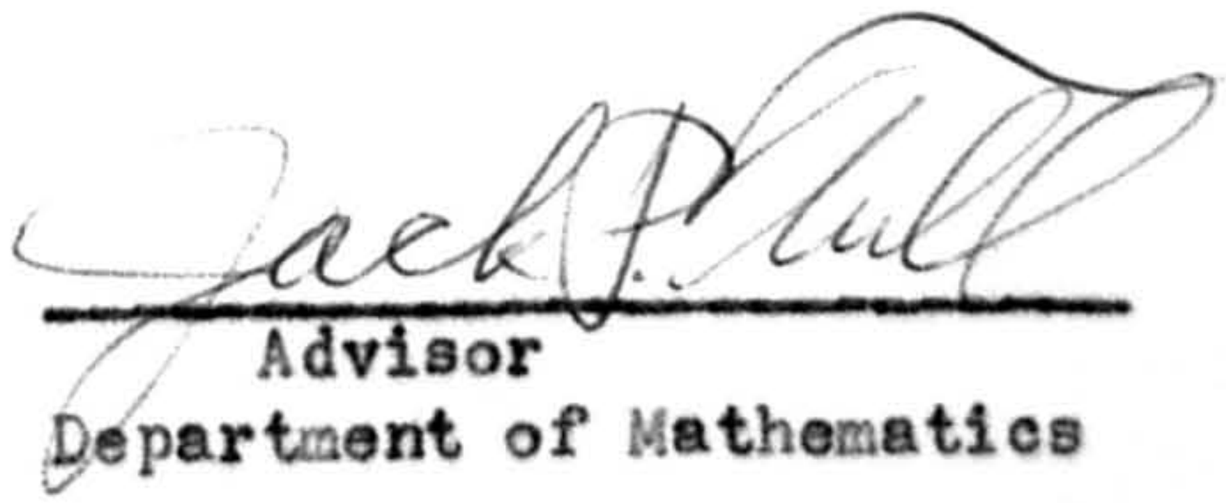
Presented in Partial Fulfillment of the Requirements
for the Degree Master of Arts

by

Roger Clement Crocker, B.A.

The Ohio State University
1962

Approved by



Advisor
Department of Mathematics

ACKNOWLEDGMENT

It is a pleasure to acknowledge my gratitude to Professor J. P. Tull for his advice and guidance in the writing of this thesis.

An important problem in the additive theory of numbers is concerned with the positive odd integers which are representable as the sum of an odd prime and a power of 2 (with positive exponent). (It is understood that primes are positive.) Romanoff, in 1934, showed that these integers have positive asymptotic density [1]. He then conjectured that every positive odd integer from some point onward is representable in this manner. It is now known that, on the contrary, there is an infinity of odd positive integers not having this property [2, 3]; in fact, there is an arithmetic progression of positive odd integers not having this property, so that the positive integers not the sum of a prime and a power of 2 also have positive density [2]. (We shall give this result in greater generality as lemma 1.)

It is then interesting to inquire further as to whether there is an infinity of pairs of consecutive odd numbers not having this property. Theorem 1 shows the answer to this question to be in the affirmative.

It is also interesting to consider whether every odd number from some point onward is a sum

$$p + 2^c + 2^{2^s}$$

with p a prime and c and s positive integers. Theorem 2 shows the answer to this question to be in the negative.

Theorem 3 produces a class of odd numbers not the sum of a prime and a power of 2. These numbers have been investigated in other well-known ways, particularly where the exponent is prime.

These first three theorems use techniques and reach results which are extensions of those of [3].

The last two theorems are deductions from lemma 1, the result obtained in [2]. The first of these shows that there exists an arithmetic progression of positive integers not representable as the difference of a prime and a power of 2.

A well-known problem is the investigation of positive integers which are the sum of a prime and a k^{th} power for a given $k \geq 2$. It has been shown in this regard that for each $k \geq 2$, almost all positive integers are representable as the sum of a prime and a k^{th} power [4]. The last theorem shows the existence, for a certain k, of an infinity of positive integers not the sum of a prime and a non-negative k^{th} power, nor the sum of a prime and a power of 2, thus combining two well-known problems.

Lemma 1. There exists an arithmetic progression of odd integers, $ax + b$ (where x takes all integer values and $(a,b) = 1$) which are not representable as $2^c \pm p$ with p a prime.

Proof: Consider a residue system $g_i \pmod{n_i}$, $1 \leqslant i \leqslant w$, with $g_i \geqslant 0$, $0 < n_1 < n_2 < \ldots < n_w$, $n_i \neq 6$, such that for every x there is an i with $x \equiv g_i \pmod{n_i}$. Now for each i, there exists a prime p_i such that $2^{n_i} \equiv 1 \pmod{p_i}$, and such that $2^{n_j} \not\equiv 1 \pmod{p_i}$ for $n_j < n_i$. This is true by a theorem stating that for each $n \neq 6$, there exists a prime p such that $p \mid 2^n - 1$ but $p \nmid 2^m - 1$, for $m < n$ [5]. By the Chinese remainder theorem there is an integer t such that $t \equiv 2^{g_i} \pmod{p_i}$, for all i, $1 \leqslant i \leqslant w$, and $t \equiv 2^{n_w + 2} + 2^{n_w + 1} + 1 \pmod{2^{n_w + 3}}$, since no two p_i's are identical and no $p_i = 2$. Since the solution of this simultaneous system is unique modulo the product of the moduli, if b is one solution then, $t = 2^{n_w + 3} \left(\prod_{i=1}^{w} p_i\right) x + b = ax + b$ gives all solutions as x varies over the integers. Since for each i, $(2^{g_i}, p_i) = 1$, and since $(2^{n_w+2} + 2^{n_w+1} + 1, 2^{n_w + 3}) = 1$, then $(a,b) = 1$.

Now $2^{g_i} \equiv t \pmod{p_i}$ and since $2^{n_i} \equiv 1 \pmod{p_i}$, $2^{kn_i} \equiv 1 \pmod{p_i}$, for every k positive or 0. Hence, for each i, $2^{g_i + kn_i} \equiv t \pmod{p_i}$. Now by our choice of the g_i and n_i, for each positive integer c there exist i and k such that $c \approx g_i + kn_i$. Thus for each c there exists i such that $t \equiv 2^c \pmod{p_i}$ for all $t \equiv b \pmod{a}$. Since $p_i < 2^{n_w}$, it only remains to show

$| t - 2^c > 2^{n_w}$.

Now $t - 2^c \equiv 2^{n_w+2} + 2^{n_w+1} - 2^c + 1 \pmod{2^{n_w+3}}$.

If $c \geq n_w + 3$, then $2^c \equiv 0 \pmod{2^{n_w+3}}$. Therefore

$|t - 2^c|\ 2^{n_w+1} - 1 > 2^{n_w}$, for $c \geq n_w + 3$. Now for

$0 < c \leq n_w + 2$, if t is positive, $t \geq 2^{n_w+2} + 2^{n_w+1} + 1$

and so $t - 2^c \geq 2^{n_w+1} + 1 > 2^{n_w}$. If t is negative,

$t \leq - 2^{n_w+1} + 1$ and so $t - 2^c < - 2^{n_w+1} + 1$ and

$| t - 2^c| > 2^{n_w+1} - 1 > 2^{n_w}$. Thus $|t - 2^c|$ is composite for all $t \equiv b \pmod{a}$ and all $c > 0$.

Q. E. D.

Throughout the following, p denotes an arbitrary odd prime, and $ax + b$ an arithmetic progression with $(a,b) = 1$ which, for each integer x, is not representable as $2^c \pm p$, with $c > 0$.

Lemma 2. For each integer $n \geq 3$, $2^{2^n} - 1$ is not representable as $p + 2^c + 2^d$, $c \neq d$.

Proof: Suppose that $c > d > 0$, $N = 2^{2^n} - 1 - 2^c - 2^d > 0$, and let 2^r be the largest power of 2 dividing $c - d$ $(r < n)$. Then $2^{2^r} + 1 \mid 2^{c-d} + 1 \mid 2^c + 2^d$ and since $r < n$, $2^{2^r} + 1 \mid 2^{2^n} - 1$. Hence $2^{2^r} + 1 \mid N$. On the other hand, for $n \geq 3$, $N \geq 2^{2^n-2} - 1 > 2^{2^{n-1}} + 1 \geq 2^{2^r} + 1$; i.e., $N > 2^{2^r} + 1$. Therefore N is composite and the lemma follows.

Q. E. D.

Theorem 1. There is an infinity of pairs of consecutive odd numbers not representable as $p + 2^c$.

Proof: Consider for $n \geq 3$, $2^{2^n} - 5$ and $2^{2^n} - 3$. If $2^{2^n} - 5 = 2^c + p$, then $c < 2^n$ and $2^{2^n} - 1 = 2^2 + 2^c + p$; hence by lemma 2, $c = 2$ and so $p = 2^{2^n} - 9 = (2^{2^{n-1}} + 3)(2^{2^{n-1}} - 3)$, which is impossible. If $2^{2^n} - 3 = 2^c + p$, then $2^{2^n} - 1 = 2 + 2^c + p$; hence by lemma 2, $c = 1$ and $p = 2^{2^n} - 5$. However, if $n \equiv 2 \pmod 4$ and $n > 2$, since 2 is a primitive root mod 11, and $2^{4k+2} \equiv 4 \pmod{10}$, then $2^{2^n} \equiv 2^4 \equiv 5 \pmod{11}$. Thus for $n \equiv 2 \pmod 4$, $(n \geq 3)$, $2^{2^n} - 5$ is composite. Therefore none of the numbers $2^{2^{4x+2}} - 5$ and $2^{2^{4x+2}} - 3$, is a sum of a prime and a power of 2.

Q. E. D.

Theorem 2. There is an infinity of odd numbers not expressible as $p + 2^c + 2^{2^s}$, with c and s positive integers.

Proof: Take $2^{2^{2n}} - 1$, n an integer ≥ 2. Suppose that $N = 2^{2^{2n}} - 1 - 2^c - 2^{2^s} > 0$. By the lemma 2, N is composite if $c \neq 2^s$. If $c = 2^s$, $N = 2(2^{2^{2n-1}} - 1) - (2^{2^{s+1}} - 1)$. Now $2^{2^r} + 1 \mid 2^s + 1$, where 2^r is the largest power of 2 dividing s ($r < n$ since $s < 2^n$).

Hence $2^{2^{2r}} + 1 - 1 \mid 2^{2^s} + 1 - 1$.

Now $2^{2^r} + 1 \mid 2^{2^n} - 1$, hence $2^{2^{2^r}} + 1 - 1 \mid 2^{2^{2^n}} - 1 - 1$ $(r < n)$. Therefore $2^{2^{2^r}} + 1 - 1 \mid N$ $(r < n)$; also if $c = 2^s$, $N \geq 2^{2^{2^n}} - 1 - 1 - 2^{2^{2^n} - 1} > 2^{2^{2^n} - 2} - 1 >$ $2^{2^{2^n} - 1} + 1 - 1 \geq 2^{2^{2^r}} + 1 - 1$, i.e., $N > 2^{2^{2^r}} + 1 - 1$.

Thus the number N is also composite for $c = 2^s$.

Q. E. D.

Theorem 3. If $n \geq 3$, then $2^{2^{2^n} - 1} - 1$ is not representable as $p + 2^c$.

Proof: Consider $N = 2^{2^{2^n} - 1} - 1 - 2^c = (2^{2^{2^n} - 1} - 1) - 2^c$.

If $N > 0$, $c < 2^{2^n} - 1$, and hence by lemma 2, N is composite.

Q. E. D.

From lemma 1, it follows

Theorem 4. There is an arithmetic progression of positive odd integers not representable as $p - 2^c$.

Proof: Choose x_0 such that $ax_0 + b < 0$. Then for all $x \leq x_0$, since by lemma 1, $ax + b$ is not of the form $2^c - p$, $|ax + b| = -ax - b$ is not of the form $p - 2^c$.

Q. E. D.

Theorem 5. There exists $k \geq 2$ such that an infinity of positive odd integers is not representable as $p + y^k$ (y positive or 0), nor as $p + 2^c$.

Proof: Consider $(ax + b)^{\phi(a) + 1}$, x positive.

Now $b^{\phi(a)} \equiv 1 \pmod{a}$ as a and b are coprime;

thus $b^{\phi(a) + 1} \equiv b \pmod{a}$.

But $(ax + b)^{\phi(a) + 1} \equiv b^{\phi(a) + 1} \pmod{a}$.

Hence $(ax + b)^{\phi(a) + 1} \equiv b \pmod{a}$; thus $(ax + b)^{\phi(a) + 1} = ax' + b$. Therefore $(ax + b)^{\phi(a)+1}$ is not representable as $p + 2^c$. (Actually it is not representable as $2^c - p$, as well).

Now if $2 \leq q \leq ax + b$ or if $q = 0$, then $(ax + b)^{\phi(a) + 1} - (ax + b - q)^{\phi(a) + 1}$ is composite.

For $q = 1$, one has a polynomial of degree $\phi(a)$ which is composite for an infinity of x by a well-known theorem. Therefore for an infinity of x, $(ax + b)^{\phi(a) + 1}$ is not representable as $p + y^k$, $k = \phi(a) + 1$.

Q. E. D.

Note: $(ax + b)^{\phi(a) + 1} - (ax + b - q)^{\phi(a) + 1}$ is composite for $q > ax + b$; hence, as $\phi(a) + 1$ is odd, $(ax + b)^{\phi(a) + 1}$ is not representable as $p - y^k$, with y positive or 0, $k = \phi(a) + 1$.

References

[1]. N.P. Romanoff, "Über einige Sätze der Additiven Zahlentheorie," Math. Ann., 109, 1934, pp. 668-678.

[2]. P. Erdös, "On a Problem Concerning Congruence Systems," Mat. Lapok, 3, 1952, pp. 122-128.

[3]. R. Crocker, "A Theorem Concerning Prime Numbers," Math. Magazine, 1961, pp. 316, 344.

[4]. H. Davenport and H. Heilbronn, "Note on a Result in the Additive Theory of Numbers," Proc. London Math. Soc., (2) 43, 1937, pp. 142-151.

[5]. L.E. Dickson, "On the Cyclotomic Function," Amer. Math. Monthly, 12, 1905, pp. 86-89.