COLLOQUIUM MATHEMATICUM

VOL. 112 2008 NO. 2

ON THE SUM OF TWO SQUARES AND TWO POWERS OF k

BY

ROGER CLEMENT CROCKER (London)

This article is dedicated to the memory of my father, Lester G. Crocker, a very distinguished scholar of the Enlightenment

Abstract. It can be shown that the positive integers representable as the sum of two squares and one power of k (k any fixed integer ≥ 2) have positive density, from which it follows that those integers representable as the sum of two squares and (at most) two powers of k also have positive density. The purpose of this paper is to show that there is an infinity of positive integers *not* representable as the sum of two squares and two (or fewer) powers of k, k again any fixed integer ≥ 2.

It should first be noted that the sum of one square and any fixed maximum number of powers of k is clearly insufficient to represent all sufficiently large positive integers, while the sum of three squares and a maximum of two (and hence a larger fixed number of) powers of k being sufficient to represent all sufficiently large (and in fact all) positive integers is easily dealt with (given the three-square theorem), while the same result involving (in place of three) four (and hence any fixed maximum number greater than four) squares is immediately dealt with (given the four square theorem; then of course no powers of k are needed)—hence the sum of *two* squares (and a fixed maximum number of powers of k) being involved in this paper. The present problem is suggested by the even better known one of representing, as the sum of a prime and a fixed maximum number of powers of two or powers of (fixed) $k \geq 2$, positive integers (odd or even as the case may be); here, the sum of two squares replaces the prime summand (and the problem now concerns the representation of positive integers, both even and odd, as parity considerations no longer effectively discriminate against either class). This replacement of a prime summand by the sum of two squares is not uncommon—e.g. the sum of a prime and two squares by the four-square problem (though the historical order is reversed), or the sum of a prime and a kth power (such as a square or a cube) by the sum of two squares and a kth power (though k must be odd in this two-square case to represent "almost

2000 *Mathematics Subject Classification*: Primary 11P32; Secondary 11A41.

Key words and phrases: additive number theory, two squares, two powers of k.

all" or all positive integers), or for that matter the sum of two primes (the yet unsolved Goldbach problem of even numbers) by the sum of a prime and two squares (for both odd and even numbers). And of course primes, powers of k, and kth powers are among the most important and "natural" of summands in additive problems ([1]) (with $k = 2$—giving squares or powers of 2—being especially fundamental and interesting among values of k) and it is important to investigate the various possible additive problems formed by possible combinations of these summands. Here, the maximum number of powers of k is limited to two as (will be seen) this presents enough difficulty for large classes of k; dealing with more than two powers of k (for such classes) would be hopeless; meanwhile, one can deal with *all* $k \geq 2$ if this maximum is held to two.

The main purpose of this paper, as already indicated, is to show the following proposition.

For each fixed $k \geq 2$, there is an infinity of positive integers not representable as the sum of two squares and (at most) two powers of k.

NOTATION. All quantities involved are integers and usually positive integers. The p_i are positive primes. The symbol $\|$ is used in the standard way, namely, $r^\alpha \| s \to r^\alpha \mid s$ but $r^{\alpha+1} \nmid s$. The classical phrase "2 belongs to $m \pmod p$" will be used in preference to its equivalent "$\operatorname{ord}_p 2 = m$".

The most difficult case of $k = 2$ will be dealt with first.

THEOREM 1. *There is an infinity of distinct positive* (*even*) *integers not representable as* $M^2 + N^2 + 2^a + 2^b$ *nor as* $M^2 + N^2 + 2^a$ (*nor as* $M^2 + N^2$), $a, b \geq 0$ ([2]).

The following two lemmas are to be used in the proof of Theorem 1.

LEMMA 1. *Given any positive integer* t *such that* $t \equiv 0 \pmod{36}$ *and* t *is not representable as* $M^2 + N^2 + 2^a + 2^b$ *nor as* $M^2 + N^2 + 2^a$ *nor as* $M^2 + N^2$, $a, b \geq 0$. *Then for every integral* $\alpha \geq 0$, $2^\alpha t$ *is not so representable.*

Proof. By the hypothesis of the lemma, $2^\alpha t$ for $\alpha = 0$ is not representable as above. Now assume $2^\alpha t$ is not representable as above for (i.e. the lemma

([1]) There are other summands of importance, of course, with which the reader no doubt will be familiar.

([2]) I usually take the (personal) viewpoint that for the purposes of additive theorems involving k^a (and k^b—both for fixed k), it suffices to deal with $a \geq 1$ (and $b \geq 1$) since *arithmetically* speaking $k \nmid k^0$ and hence (*arithmetically* speaking) k^0 should not really be regarded as a power of k in this context. However, for Theorem 1, it is easily seen that $a = 0$ and $b = 0$ must be included since otherwise Lemma 1 will be undermined. And in this paper, $a = 0$ and $b = 0$ might as well be included, where possible, for the other results as well since this inclusion (which is usually possible) is also usually provable and most often in an utterly trivial way.

is true for) an arbitrary but fixed $\alpha \geq 0$. Consider $2^{\alpha+1}t$. If $2^{\alpha+1}t = M^2 + N^2 + 2^a + 2^b$ with both $a, b > 0$, then $M^2 + N^2$ is even so that with $2 = 1^2 + 1^2$, $M^2 + N^2 = 2(M_1^2 + N_1^2)$ for some (integral) M_1, N_1, from which $2^{\alpha+1}t = 2(M_1^2 + N_1^2) + 2^a + 2^b$ so that $2^\alpha t = M_1^2 + N_1^2 + 2^{a-1} + 2^{b-1}$ with $a - 1, b - 1 \geq 0$, a contradiction with the above assumption for $2^\alpha t$. Thus (given that assumption) $2^{\alpha+1}t \neq M^2 + N^2 + 2^a + 2^b$, $a, b > 0$. Without loss of generality, take $a \leq b$. Now suppose $2^{\alpha+1}t = M^2 + N^2 + 2^a + 2^b$ with $a = 0$, $b \geq 0$; then if $b = 0$, remembering that $t \equiv 0 \pmod 4$ so that $2^{\alpha+1}t \equiv 0 \pmod 8$, then $M^2 + N^2 \equiv 6 \pmod 8$, an impossibility; (next) if $b \geq 2$, $M^2 + N^2 \equiv 3 \pmod 4$, again an impossibility; (finally) if $b = 1$, remembering that $t \equiv 0 \pmod 9$ so that $2^{\alpha+1}t \equiv 0 \pmod 9$, then $M^2 + N^2 \equiv 6 \pmod 9$ from which $3 \parallel M^2 + N^2$, again an impossibility. Thus $2^{\alpha+1}t \neq M^2 + N^2 + 2^a + 2^b$ for $a = 0$, $b \geq 0$, and hence, from above, for $a \geq 0$, $b \geq 0$. Furthermore $2^{\alpha+1}t \neq M^2 + N^2 + 2^a$ if $a > 0$, since from what has just been shown, it follows that $2^{\alpha+1}t \neq M^2 + N^2 + 2^{a-1} + 2^{a-1}$, $a - 1 \geq 0$. And also $2^{\alpha+1}t \neq M^2 + N^2 + 2^a$, $a = 0$, since $M^2 + N^2 \not\equiv 7 \pmod 8$. Thus $2^{\alpha+1}t \neq M^2 + N^2 + 2^a$, $a \geq 0$. Lastly $2^{\alpha+1}t \neq M^2 + N^2$ since otherwise $1^2 + 1^2 = 2 \mid M^2 + N^2$ and so one would have $2^\alpha t = M_1^2 + N_1^2$ for some integral M_1, N_1, which contradicts the above initial assumption for $2^\alpha t$. Hence (given that assumption) $2^{\alpha+1}t$ is not representable in any of the above ways. Thus the truth of the lemma for an arbitrary $\alpha \geq 0$ implies the truth of the lemma for $\alpha + 1$. And (as already stated) by the hypothesis of the lemma, the lemma is true for $\alpha = 0$. By induction on α the lemma follows. ∎

The following rather routine lemma will be useful later in the paper in avoiding some lengthy numerical calculations. It will be presented here, however, so as not to interfere with the continuity of the argument later on.

LEMMA 2. *Suppose* $2^D + 8 \equiv 2^E + 2 \pmod p$ *for some non-negative* $D, E < m$, *where* 2 *belongs to* $m \pmod p$ *but* $2^m \not\equiv 1 \pmod{p^2}$, p *an odd prime. Then, for* $0 \leq k, k' \leq p - 1$, *one can find a value of* k, *say* K, *and a value of* k', *say* K', *such that* $2^{D+Km} + 8 \equiv 2^{E+K'm} + 2 \pmod{p^2}$ *with* $(p-1)/2 \leq K$, $K' \leq p - 1$, *so that* $m(p-1)/2 \leq D + Km$, $E + K'm < mp$.

Proof. For the value of D and the value of E concerned, given that $2^D + 8 \equiv 2^E + 2 \pmod p$, one can write $2^D + 8 \equiv 2^E + 2 \equiv R \pmod p$ for some *fixed* R. And since $2^{D+km} \equiv 2^D \pmod p$ and $2^{E+k'm} \equiv 2^E \pmod p$, for any $0 \leq k, k' \leq p - 1$, $2^{D+km} + 8 \equiv 2^{E+k'm} + 2 \equiv R \pmod p$. Then it follows that for each k $(0 \leq k \leq p - 1)$, $2^{D+km} + 8 \equiv R + np \pmod{p^2}$ with some n such that $0 \leq n \leq p - 1$—and it is easily shown from this that as k assumes each integer consecutively from 0 to $p - 1$ (that is, once and only once), n assumes each integer (in some order) from 0 to $p - 1$ once and only once. For if one could find two different non-negative values of k, say k_1, k_2

with (without loss of generality) $k_1 < k_2 \leq p-1$, giving the same value for n, then one would have $2^{D+k_1 m}+8 \equiv 2^{D+k_2 m}+8 \pmod{p^2}$, in which case [with $(2,p)=1$] $2^{(k_2-k_1)m} \equiv 1 \pmod{p^2}$ with $k_2-k_1 < p$, which is impossible since 2 belongs to $mp \pmod{p^2}$ [the last being a well-known and easily proved consequence of 2 belonging to $m \pmod{p}$ while $2^m \not\equiv 1 \pmod{p^2}$]. And if one could find two different non-negative values of n, say $n_1 < n_2 \leq p-1$, given by the same value of k, then $2^{D+km}+8 \equiv R+n_1 p \equiv R+n_2 p$, in which case $n_1 \equiv n_2 \pmod{p}$, contradicting non-negative $n_1 < n_2 \leq p-1$. The above result thus proved can also be stated as there being a one-to-one correspondence between the values of k, $0 \leq k \leq p-1$, and those of n, $0 \leq n \leq p-1$ [in $2^{D+km}+8 \equiv R+np \pmod{p^2}$]. And starting with k', n' and $2^{E+k'm}+2$, in place of k, n and $2^{D+km}+8$ respectively, the same result can be proved in the same way for the values of k', $0 \leq k' \leq p-1$, and those of n', $0 \leq n' \leq p-1$ [in $2^{E+k'm}+2 \equiv R+n'p \pmod{p^2}$ with (from above) the same value of R]. Now take the $(p+1)/2$ consecutive values of k' running from $(p-1)/2$ to $p-1$; from the one-to-one correspondence between k' and n', it follows that to these values of k' will correspond exactly $(p+1)/2$ distinct values of n'. Assign these same $(p+1)/2$ values of n' to n; from the above one-to-one correspondence between k and n, to these $(p+1)/2$ distinct values of n, there must correspond $(p+1)/2$ distinct values of $k \leq p-1$, at least one of which is $\geq (p-1)/2$ on account of there being at most $(p-1)/2$ [$< (p+1)/2$] non-negative values $< (p-1)/2$ that k can possibly assume. Any such $k \geq (p-1)/2$ may be chosen; call it K. Take the value of n corresponding to K; call it N. Since $n = N$ is one of the same $(p+1)/2$ values of n' assigned above to n (i.e. the values of n' corresponding to the consecutive values of k' running from $(p-1)/2$ to $p-1$), $n' = N$ also corresponds to a value of $k' \geq (p-1)/2$; call it K'. Thus for K, K', which correspond to $n = n' = N$, one has $2^{D+Km}+8 \equiv R+Np \equiv 2^{E+K'm}+2 \pmod{p^2}$ with $K, K' \geq (p-1)/2$—and as all values of k, k' are $\leq p-1$, it follows (since K, K' each assumes a value of k, k' respectively) that $K, K' \leq p-1$. Thus, with $K, K' \geq (p-1)/2$, both $D+Km, E+K'm \geq m(p-1)/2$; since $D, E < m$ and $K, K' \leq p-1$, one also has both $D+Km, E+K'm < m+(p-1)m = mp$. The lemma follows. ∎

Proof of Theorem 1. It follows from Lemma 1 that *if* a positive integer $t = t_1$ can be found simultaneously satisfying $t \equiv 28 \pmod{32}$—in which case $t \equiv 0 \pmod{4}$—and $t \equiv 0 \pmod{3^2}$ and such that $t = t_1$ itself is not representable as in the hypothesis of lemma 1, *then* there is an infinity of distinct positive (even) integers not so representable—which conditionally proves Theorem 1. To prove the existence of such a number t_1, again consider $t - 2^a - 2^b$ where, for the moment, without loss of generality, take $a \leq b$. If $a \neq 1$ or 3, then unless $a = 0$, $b = 0$ or 1, or unless $a = 2$, $b = 2$, 3 or 4, one

has—remembering $t \equiv 28 \pmod{32}$—$t - 2^a - 2^b = 2^s(4z+3)$ [$s = 0$, 2, or 3] so that $t - 2^a - 2^b \neq M^2 + N^2$. One need then only consider (the *principal* cases) $a = 1$ or 3 [each with a large number of b, namely those b such that $t - 2^a - 2^b \geq 0$ for $t = t_1$; as will be seen later in the proof, $t = t_1 < 2^{1417}$ so that it suffices to consider $b \leq 1416$], and also (the *special* cases) $a = 0$, $b = 0$ or 1, and also $a = 2$, $b = 2$, 3 or 4. Furthermore, if $a \neq 1$ or 3, then $t - 2^a = 2^s(4z+3)$ [$s = 0$, 2 or 3] so that $t - 2^a \neq M^2 + N^2$; if $a = 1$ or 3, these cases coincide with those for $t - 2^a - 2^b$ with $a, b = 0$ or $a, b = 2$ (already included in the *special* cases above) so that $t - 2^a$ (≥ 0) is dealt with (i.e. $\neq M^2 + N^2$) if $t - 2^a - 2^b$ (≥ 0) is dealt with. And $t = 4(4z+3) \neq M^2 + N^2$. Returning then to $t - 2^a - 2^b$, to complete the proof that $t = t_1$ is not representable as in the hypothesis of lemma 1, it suffices to settle the above *principal* and *special* cases set out for $t - 2^a - 2^b$, noting however that two of these *special* cases, those of $a = 0$, $b = 1$ and $a = 2$, $b = 3$, are equivalent to $a = 1$, $b = 0$ and $a = 3$, $b = 2$ respectively and hence are included in the *principal* cases $a = 1$ or 3 if henceforth one allows $a > b$ as well as $a \leq b$, which will in fact be allowed. (That leaves three of the above *special* cases above to be dealt with later—$a, b = 0$, $a, b = 2$ and $a = 2$, $b = 4$.)

To settle these *principal* and *special* cases, first it is desirable to set out system (1) and then system S, which will occupy a number of pages.

Now consider the following system (1) of congruences $x_i \equiv a_i \pmod{m_i}$ [with $0 \leq a_i < m_i$], $1 \leq i \leq 139$: for $i = 1, 2, 3$, every non-negative *even* integer ≤ 1416 satisfies at least one of the corresponding congruences; the same again is true for the congruences corresponding to $4 \leq i \leq 12$; for $13 \leq i \leq 74$, every positive *odd* integer ≤ 1416 satisfies at least one of the corresponding congruences, while the same again is true for the congruences corresponding to $75 \leq i \leq 139$. All these assertions are verifiable numerically in the most straightforward manner ([3]) and should be remembered throughout the proof. *System* (1) is as follows:

For $i = 1, 2, 3$: 0 (mod 2), 0 (mod 3), 0 (mod 42).

For $4 \leq i \leq 12$: 0 (mod 2), 0 (mod 10), 4 (mod 18), 3 (mod 5), 7 (mod 15), 16 (mod 30), 19 (mod 45), 34 (mod 45), 160 (mod 495).

For $13 \leq i \leq 40$: 0 (mod 3), 9 (mod 10), 17 (mod 18), 8 (mod 11), 1 (mod 5), 9 (mod 14), 0 (mod 23), 5 (mod 58), 29 (mod 66), 33 (mod 35), 19 (mod 39), 15 (mod 82), 13 (mod 51), 49 (mod 106), 1 (mod 7), 75 (mod 130), 43 (mod 138), 25 (mod 162), 5 (mod 83), 7 (mod 178), 50 (mod 99), 145 (mod 210), 21 (mod 37), 185 (mod 226), 27 (mod 50), 49 (mod 94), 73 (mod 102), 20 (mod 155).

([3]) The numerical calculations used for verification are omitted here because they are completely straightforward and routine but would be so lengthy and tedious as to spoil the continuity of the argument and its presentation. (They were all carried out by pen and paper with occasional use of a pocket calculator.) There are one or two other similar situations in the course of the paper, in which a pocket calculator was sometimes used.

For $41 \leq i \leq 74$: 1 (mod 13), 1 (mod 19), 1 (mod 22), 15 (mod 26), 1 (mod 29), 1 (mod 34), 1 (mod 41), 1 (mod 43), 43 (mod 51), 1 (mod 54), 21 (mod 73), 54 (mod 79), 81 (mod 91), 64 (mod 113), 104 (mod 153), 27 (mod 166), 47 (mod 198), 47 (mod 214), 203 (mod 230), 53 (mod 231), 227 (mod 239), 209 (mod 246), 231 (mod 266), 257 (mod 270), 1 (mod 411), 387 (mod 466), 385 (mod 522), 0 (mod 105), 357 (mod 378), 147 (mod 546), 189 (mod 378), 9 (mod 55), 89 (mod 114), 1 (mod 155).

For $75 \leq i \leq 105$: 5 (mod 11), 3 (mod 5), 1 (mod 14), 12 (mod 23), 39 (mod 58), 21 (mod 66), 19 (mod 35), 32 (mod 39), 65 (mod 82), 24 (mod 51), 15 (mod 106), 3 (mod 7), 119 (mod 130), 83 (mod 138), 7 (mod 15), 137 (mod 162), 73 (mod 83), 87 (mod 178), 77 (mod 95), 68 (mod 99),5 (mod 210), 9 (mod 37), 203 (mod 226), 0 (mod 119), 1 (mod 50), 60 (mod 131), 92 (mod 135), 1 (mod 94), 57 (mod 102), 19 (mod 45), 34 (mod 45).

For $106 \leq i \leq 139$: 3 (mod 13), 5 (mod 17), 3 (mod 19), 3 (mod 22), 1 (mod 26), 3 (mod 29), 3 (mod 34), 5 (mod 38), 3 (mod 41), 3 (mod 43), 11 (mod 50), 8 (mod 51), 3 (mod 54), 65 (mod 70), 5 (mod 78), 15 (mod 110), 78 (mod 121), 159 (mod 166), 146 (mod 175), 72 (mod 179), 73 (mod 183), 85 (mod 191), 68 (mod 251), 173 (mod 303), 145 (mod 323), 257 (mod 346), 235 (mod 350), 12 (mod 359), 3 (mod 411), 149 (mod 418), 12 (mod 419), 389 (mod 442), 375 (mod 490), 3 (mod 155).

Now for each m_i ($1 \leq i \leq 139$), there is a corresponding $p_i \equiv 3 \pmod 4$ such that 2 belongs to $m_i \pmod{p_i}$ but such that $2^{m_i} \not\equiv 1 \pmod{p_i^2}$; this is verifiable numerically (see factor tables [1], [11] where the factorisations demonstrate this); the p_i will in fact be set out below. From the above system (1), construct the following *simultaneous* congruence system:

- First, for $i = 1, 2, 3$ and for $13 \leq i \leq 40$, take the congruences
  $t \equiv 8 + 2^{a_i + k_i m_i} \pmod{p_i^2}$, the k_i to be set out below;
- then, for $41 \leq i \leq 74$, take (the congruences)
  $t \equiv 8 + 2^{a_i} \pmod{p_i}$;
- then, for $4 \leq i \leq 12$ and for $75 \leq i \leq 105$, take
  $t \equiv 2 + 2^{a_i + k_i m_i} \pmod{p_i^2}$, the k_i to be set out below;
- finally, for $106 \leq i \leq 139$, take
  $t \equiv 2 + 2^{a_i} \pmod{p_i}$.

To this simultaneous system constructed from system (1) will now be attached the following three *additional* simultaneous congruences [not obtained from system (1)] with $p_i \equiv 3 \pmod 4$ for $i = 140, 141$ set out below, as well as the p_i for $i = 142$:

- for $i = 140$, take
  $t \equiv p_i + 8 \pmod{p_i^2}$;
- for $i = 141$, take
  $t \equiv p_i + 20 \pmod{p_i^2}$;
- last (for $i = 142$)—and crucially—take
  $t \equiv 28 \pmod{p_i^5}$.

Taking these (142) congruences to be satisfied *simultaneously* (by t), call the resulting simultaneous congruence *system* S. [In each of the above systems, (1) and S, the congruences for $i = 1, 2, 3$, and $13 \le i \le 74$, relate to the *principal* case $a = 3$ (above) while those for $4 \le i \le 12$, $75 \le i \le 139$, relate to the *principal* case $a = 1$ (above).]

The p_i, $1 \le i \le 142$, will now be given.

- First, $p_1 = 3$, $p_2 = 7$, $p_3 = 5419$;
- then, for $4 \le i \le 12$, $p_i = 3, 11, 19, 31, 151, 331, 631, 23311, 991$ respectively;
- then, for $13 \le i \le 40$, p_i takes on (the p_i increasing with i) the consecutive primes $\equiv 3 \pmod 4$, beginning with $p_i = 7$ (for $i = 13$) and ending with 311 (for $i = 40$), with the exception of 151, 191, 239, 263, 271 [most of these p_i are $2m_i + 1$ if m_i is odd or ($p_i =$) $m_i + 1$ if m_i is even, the only exceptions being (those p_i for) $i = 17, 18, 27, 35, 37, 38, 39$];
- then, for $41 \le i \le 74$ (the m_i increasing with i, for $41 \le i \le 67$), $p_i = 2^{13} - 1$, $2^{19} - 1$, 683, 2731, 1103, 43691, 13367, 431, 11119, 87211, 439, 2687, 911, 3391, 919, 499, 5347, 643, 691, 463, 479, 739, 4523, 811, 823, 467, 523, 29191, 379, 547, 119827, 3191, 571, 11471 respectively;
- then, for $75 \le i \le 105$: first, for $75 \le i \le 103$, p_i takes on (the p_i increasing with i) the consecutive primes $\equiv 3 \pmod 4$, beginning with ($p_i =$) 23 (for $i = 75$) and ending with 307 (for $i = 103$), while for $i = 104$, 105, $p_i = 631$, 23311 respectively [most of these p_i are equal to p_i for smaller i (with equal values of m_i of course); all such duplications in value will be made explicit below];
- then, for $106 \le i \le 139$ (with the m_i for $106 \le i \le 138$ increasing with i) $p_i = 2^{13} - 1$, $2^{17} - 1$, $2^{19} - 1$, 683, 2731, 1103, 43691, 174763, 13367, 431, 4051, 2143, 87211, 86171, 22366891, 2971, 727, 1163, 39551, 359, 367, 383, 503, 607, 647, 347, 1051, 719, 823, 419, 839, 443, 491, 11471 respectively; indeed, for $i = 106$, $108 \le i \le 112$, $i = 114$, 115, 118, 134, 139, the p_i duplicate those (already listed) for $41 \le i \le 48$, $i = 50$, 65, 74 in the same order;
- finally, for $i = 140$, 141, and 142, $p_i = 487$, 563, and 2 respectively.

Throughout the rest of the proof of Theorem 1, for each i, p_i will have the value given above. The k_i in system S can be set out as follows ($k_i < p_i$ for every i for which k_i is introduced):

- for $i = 1, 2, 3$, $k_i = 0$;
- for $4 \le i \le 12$, $k_i = 2$, 5, 14, 0, 150, 330, 630, 23310, 990 respectively;
- for $13 \le i \le 19$, $k_i = 0$, 0, 4, 14, 0, 7, 16 respectively;
- for $i = 22$, 27, 40, $k_i = 25$, 79, 310 respectively;
- for $75 \le i \le 78$, $k_i = 6$, 0, 28, 24 respectively;

- for $i = 81, 86, 89, 93, 98, 100, 101, 104, 105$, $k_i = 1, 115, 150, 190, 238, 262, 270, 630, 23310$ respectively;
- finally, (denoting $i = i_1$ or i_2 by $i = [i_1, i_2]$), for $i = [20, 79], [21, 80], [23, 82], [24, 83], [25, 84], [26, 85], [28, 87], [29, 88], [30, 90], [31, 91], [32, 92], [33, 94], [34, 95], [35, 96], [36, 97], [37, 99], [38, 102], [39, 103]$, in each *bracketed* pair of i, the existence of an appropriate k_i for each member of the pair will be shown.

The setting out of system S now being sufficiently complete, it must now be shown that S has at least one positive integral solution that cannot be represented as $M^2+N^2+2^a+2^b$ or as $M^2+N^2+2^a$, $a, b \geq 0$, or as M^2+N^2 (i.e. as set out in Theorem 1). First, it must be shown that S has positive integral solutions. To do this, it will first be shown that (those congruences with) equal moduli have equal residues [equal residues (in connection with equal moduli) will be used in this proof to mean residues in the same residue class (for the equal moduli)]. To demonstrate this crucial property, one need look at the various cases (in S) in turn. First, examine the equal moduli in the congruences (mod p_i^2) in S. To begin with, for each of the *bracketed* pairs of i listed above (*the* p_i *and thus the moduli* p_i^2 *being equal for both members* i *of a pair*) it is verifiable numerically in a straightforward manner that the conditions in the hypothesis of Lemma 2 are satisfied [with $p = p_i$ for both i, $D = a_i$ for the smaller i, $E = a_i$ for the larger i, and $m = m_i$ for both i, remembering from above that 2 belongs to m_i (mod p_i) for both i with their equal p_i (so that the m_i are of course equal); however, the a_i are not equal for both i in a bracketed pair; all a_i, m_i, p_i are given numerically above] for the m_i, p_i and the (two distinct) a_i corresponding to the members of the pair. Let $k = k_i$ for the smaller i of the pair, $k' = k_i$ for the larger i, with $0 \leq k, k' \leq p-1$. Then it follows from (the conclusion of) Lemma 2 that for each bracketed pair of i, values for the (two) k_i can be found (and then chosen), corresponding to K and K' respectively in Lemma 2, in order that the residues [in the congruences (for t in S) corresponding to the members i of the pair], namely $8 + 2^{a_i+k_i m_i}$ for the first k_i and smaller i, $2 + 2^{a_i+k_i m_i}$ for the second k_i and larger i, can be made congruent (mod p_i^2) [i.e. equal in the above sense] for the equal moduli p_i^2 for both i of the pair. Proceeding to the other (unbracketed) equal moduli p_i^2: for $i = 1, 4$, one has $p_1 = p_4 = 3$, $k_1 = 0$, $k_4 = 2$, $m_1 = m_4 = 2$, $a_1 = a_4 = 0$, all as given above, and indeed one has as a result that $t \equiv 8 + 2^{a_1+k_1 m_1} \equiv 2 + 2^{a_4+k_4 m_4} \equiv 0 \pmod{3^2}$ [and $t \equiv 0 \pmod 9$ also is necessary for the application of Lemma 1]. Similarly (with all those p_i, m_i, a_i, k_i given above and using the corresponding congruences, also given above, for t in system S) for $i = 2, 13$ ($p_i = 7$); $i = 5, 14$ ($p_i = 11$); $i = 6, 15$ ($p_i = 19$); $i = 7, 17, 76$ ($p_i = 31$); $i = 8, 89$ ($p_i = 151$); $i = 10, 104$ ($p_i = 631$); $i = 11, 105$ ($p_i = 23311$); $i = 16, 75$ ($p_i = 23$);

$i = 18, 77$ ($p_i = 43$); $i = 19, 78$ ($p_i = 47$); $i = 22, 81$ ($p_i = 71$); $i = 27, 86$ ($p_i = 127$); in each case, straightforward numerical calculation gives the desired result (for the equality of the residues of the equal moduli p_i^2). Next, one must examine the equal moduli in the congruences (mod p_i) in S. As has already been pointed out above when listing the p_i in S, for $i = 106$, $108 \leq i \leq 112$, $i = 114, 115, 118, 134, 139$, the p_i duplicate those for $41 \leq i \leq 48$, $i = 50, 65, 74$ and in the same order; the p_i are given above in the paragraph dealing with p_i for $41 \leq i \leq 74$. Again, in each case (for each pair of i with [moduli] p_i of equal value) using the relevant a_i, m_i, p_i in the corresponding congruences (all given above), a straightforward numerical calculation shows that the residues are equal for equal moduli p_i. Hence all equal moduli in S have equal residues (the *only* congruence not having modulus p_i or p_i^2 has the modulus p_i^5 with $p_i = 2$, corresponding to $i = 142$; this modulus is distinct). The above crucial property has thus been established. Next, observe that in S, p_i of equal value occur to the same power (whether it be 1 or 2) as moduli in the congruences containing them and in S then give equal moduli that in turn give [from the above established crucial property—while remembering, of course, that the coefficients of t in the congruences in S are all equal (to 1)] equivalent congruences. That is, in S, p_i of equal value give equivalent congruences.

Now, starting with the congruence in system S for $i = 1$, one can select this congruence and then select each congruence in S for each successive i for which and only for which p_i is *not* equal to the p_i for *all preceding* (smaller) i in S. In this way, one obtains a reduced simultaneous congruence system, call it S′. The moduli and their congruences in S′ are those in S for the following i: $i = 1, 2, 3, 5 \leq i \leq 12, 16 \leq i \leq 74$ except for $i = 17$; $i = 93, 98, 100, 101, 107, 113, 116, 117, 119 \leq i \leq 138$ except for $i = 134$; $i = 140, 141, 142$. Since each p_i so eliminated from S (to obtain S′) is equal to a p_i (for a smaller i of course) allowed in S′, it follows from above that each congruence eliminated from S (to obtain S′) is equivalent to a congruence allowed in S′; it then follows that S and S′ are either both solvable or not solvable, and if solvable have the same solutions (i.e. they are equivalent systems). And since by the elimination process all p_i in S′ are distinct, it follows [since all moduli are distinct primes raised to powers (1, 2, or 5)] that all moduli in S′ are distinct *and relatively prime*. Thus by the Chinese Remainder Theorem, S′ *and hence* S (which has identical solutions) have solutions which can be written as $t = H + wP$, for all integral w, where P is the product of *all* the moduli in S′ and one may consider $0 < H < P$, H itself (fixed and) a solution of S′ and S (from S′, $H \neq 0$). Now by straightforward calculation $P < 10^{374} < 10^{426} < 2^{1417}$; letting v be the largest integer for which $vP < 2^{1417}$, then $v \geq 10^{52}$. Hence there are at least ($v \geq$) 10^{52} (distinct) positive (integral) solutions of (S′ and hence) S which

are $< 2^{1417}$; $t = H + wP$ for all integral w such that $0 \leq w \leq v - 1$ are certainly such solutions. (See the *principal* cases above for the relevance of 2^{1417}.)

It will next be shown (in fact this will be the concern of virtually the rest of the proof of Theorem 1) that at least one of these solutions t of S cannot be represented as in Theorem 1 ([4]). (In what follows, t will be considered positive though this may be mentioned occasionally as a reminder. And obviously negative integers cannot be so represented.) Most of the remainder of the proof concerns the *principal* cases for $a = 1$, 3; these will be settled first. First, (in S) for (each) $i = 1, 2, 3$ and $13 \leq i \leq 40$, [corresponding to the principal case $a = 3$] one has $t - 8 \equiv 2^{a_i + k_i m_i} \pmod{p_i^2}$, from which $t - 8 \equiv 2^{a_i + k_i m_i} \pmod{p_i}$. Since, with 2 belonging to $m_i \pmod{p_i}$, $2^{m_i} \equiv 1 \pmod{p_i}$ and hence $2^{m_i |L|} \equiv 1 \pmod{p_i}$, it immediately follows from congruence multiplication (for $L \geq 0$) and from congruence division (for $L < 0$, see footnote 5, second, third and especially the following sentence in parenthesis) that $t - 8 \equiv 2^{a_i + k_i m_i + L m_i} \pmod{p_i}$ for any integer L (whether ≥ 0 or < 0) for which $a_i + k_i m_i + L m_i \geq 0$. But since $p_i \parallel 2^{m_i} - 1$ (for each i in S) it follows from a well-known result (see footnote 14 from the third sentence onward) that $2^{m_i |L|} \not\equiv 1 \pmod{p_i^2}$ if and only if $p_i \nmid L$. From this latter result, together with $t - 8 \equiv 2^{a_i + k_i m_i} \pmod{p_i^2}$, it follows that if and only if $p_i \nmid L$, $t - 8 \not\equiv 2^{a_i + k_i m_i + L m_i} \pmod{p_i^2}$ [for any L (≥ 0 or < 0) such that $a_i + k_i m_i + L m_i \geq 0$] ([5]); then, if and only if $p_i \nmid L$,

([4]) Part of the proof of Theorem 1, particularly, much of the current part dealing with the principal cases has its origins in the method used in [4], [5], [9], [10] (the method of showing that there is an infinity of positive integers not representable as $p + 2^a$, p prime), the core of which is reproduced in footnote 8; indeed, compare the part of the sixth sentence (of the paragraph of the main text in which this footnote occurs) involving congruence multiplication to arrive at $t - 8 \equiv 2^{a_i + k m_i + L m_i} \pmod{p_i}$ for $L \geq 0$, and especially footnote 8, to the references just given (though there is no $k_i m_i$ term in these references, since this term has not been introduced in them but only added in the present paper; footnote 8 is thus really a more precise reproduction of the core of the method in these references, though with $t - 8$ and then with $t - 2$ in place of t). However, very considerable modification and extension, as well as additional results and arguments not part of that method, are needed and have been made throughout the present proof.

([5]) If $p_i \mid L$ and $L \geq 0$, then multiplying the congruence $t - 8 \equiv 2^{a_i + k_i m_i} \pmod{p_i^2}$ by $1 \equiv 2^{m_i L} \pmod{p_i^2}$ gives $t - 8 \equiv 2^{a_i + k_i m_i + L m_i} \pmod{p_i^2}$ [here $a_i + k_i m_i + L m_i \geq 0$]. The well-known rule for dividing congruences will now be stated for expediency—if $x \equiv y \pmod{m}$ and $e \equiv f \pmod{m}$ where $e \mid x$ and $f \mid y$, with $(e, m) = 1$ or equivalently $(f, m) = 1$, then it follows $x/e \equiv y/f \pmod{m}$. First ($p_i \mid L$ still) let $L < 0$, in which case let $x = t - 8$, $y = 2^{a_i + k_i m_i}$, $e = 1$, $f = 2^{m_i |L|}$, and $m = p_i^2$; $(e, m) = 1$; then one has $t - 8 \equiv 2^{a_i + k_i m_i + L m_i} \pmod{p_i^2}$ for $a_i + k_i m_i + L m_i \geq 0$. [The division rule with the same x, y, e, f but with $m = p_i$ has been used above; if $m = p_i$ rather than p_i^2, it does not matter if $p_i \mid L$ or not.] Next, consider the cases where $p_i \nmid L$. First take $L > 0$ (since $p_i \nmid L$, $L \neq 0$); then letting $x = t - 8$, $y = 2^{a_i + k_i m_i + L m_i}$ (with $a_i + k_i m_i + L m_i > 0$), $e = t - 8$, and $f = 2^{a_i + k_i m_i}$, $m = p_i^2$, with obviously $(f, m) = 1$ [since for $i \neq 142$, $(2, m) = 1$],

$p_i \,\|\, t-8-2^{a_i+k_im_i+Lm_i}$, for (each) $i = 1, 2, 3$ and $13 \le i \le 40$ (and for any L such that $a_i + k_im_i + Lm_i \ge 0$); this holds for every t satisfying S. Hence [having $p_i \equiv 3 \pmod 4$], for every t satisfying S, $t-8-2^b \ne M^2+N^2$ *if* for some i (among those i just above) $b = a_i + k_im_i + Lm_i$ [$\equiv a_i \pmod{m_i}$] and $p_i \nmid L$, or equivalently *if* for some i (among those i just above) b satisfies $x_i \equiv a_i \pmod{m_i}$ in system (1) and yet for that i, $b \not\equiv a_i + k_im_i \pmod{m_ip_i}$. By exactly the same reasoning (including footnote 5 which applies exactly the same way when replacing $t-8$ by $t-2$ throughout), for each i among those $4 \le i \le 12$ and $75 \le i \le 105$ [corresponding to the principal case $a = 1$], it follows that for every t satisfying S, one has $p_i \,\|\, t-2-2^{a_i+k_im_i+Lm_i}$ (for any L such that $a_i+k_im_i+Lm_i \ge 0$) if and only if $p_i \nmid L$. Hence [having $p_i \equiv 3 \pmod 4$] it follows, for every t satisfying S, that $t-2-2^b \ne M^2+N^2$ *if* for some i (among those i just above) $b = a_i+k_im_i+Lm_i$ [$\equiv a_i \pmod{m_i}$] and $p_i \nmid L$, or equivalently *if* for some i (among those i just above) b satisfies $x_i \equiv a_i \pmod{m_i}$ in the system (1) and yet for that i, $b \not\equiv a_i + k_im_i \pmod{m_ip_i}$ ([6]).

it would follow using the division rule that $1 \equiv 2^{m_i|L|} \pmod{p_i^2}$, a contradiction when $p_i \nmid L$. Hence, given $e \equiv f \pmod m$, if $L > 0$, then $x \not\equiv y \pmod m$ for the latest x, y, e, f, and m ($= p_i^2$). Next take $L < 0$; again let $x = e = t-8$, but now let $y = 2^{a_i+k_im_i}$, and $f = 2^{a_i+k_im_i+Lm_i}$ (i.e. reversing the previous choices of y and f) with $a_i+k_im_i+Lm_i \ge 0$, and let $m = p_i^2$ again, with obviously $(f, m) = 1$. Again, using the division rule it would follow that $1 \equiv 2^{m_i|L|} \pmod{p_i^2}$, a contradiction when $p_i \nmid L$. Hence, given now that $x \equiv y \pmod m$, if $L \le 0$, then $e \not\equiv f \pmod m$ for the latest x, y, e, f, m ($= p_i^2$). I have chosen to present the details of this argument in a footnote rather than in the main text to, hopefully, help the flow of the main text.

([6]) Each pair of equal moduli (whether p_i or p_i^2) in S which simultaneously deals with two (usually distinct) residue classes of b, i.e. for $0 \le b \le 1416$, *and* where one of these residue classes is for $8+2^b+M^2+N^2$ and the other is for $2+2^b+M^2+N^2$, genuinely does double duty—for while each such pair indeed deals simultaneously with two residue classes of b, one for each principal case, both its members are used in equivalent congruences in S and hence *only one* member of each pair need be used in (only one congruence in) S′. The trick of course is to ensure that such equal moduli do indeed have equal residues; for those pairs of equal moduli p_i^2, the introduction of the k_i is usually necessary for this purpose. Meanwhile, this use of equal moduli—allowing such double duty—is necessary to keep the product of the moduli in S′ (and the *distinct* moduli in S) $< 2^{1417}$. Otherwise, without the use of such equal moduli in S (in which case S′ would be synonymous with S and would not even have to be introduced) many more distinct moduli (and some of these far larger than most of those actually used here) would be needed (with the accompanying increase in the number of congruences) and the product of the distinct moduli would then greatly exceed 2^{1417} (even if squares of p_i were avoided, which in any case would cause other considerable problems) in which case the proof would probably be impossible as the existence of a solution $< 2^{1417}$ of S′ or S would be extremely unlikely and certainly unprovable. And any corresponding increase of 2^{1417} (to match this product of the distinct moduli) would merely necessitate still considerably more (and many of them even larger) distinct moduli, thus probably not retrieving the situation. Finally, the advantage of using p_i^2 for many moduli in S (as opposed to p_i) is to ensure (for as many values of b as possible)

Next, for $i = 1, 2, 3$ and $13 \leq i \leq 40$ [in system (1)], one must further examine those $b \equiv a_i + k_i m_i \pmod{m_i p_i}$ [in which case $b \equiv a_i \pmod{m_i}$], $0 \leq b \leq 1416$—since (from above) for each such b, $p_i^2 \mid t - 8 - 2^b$ for the relevant i. It will be shown for each such b that *either* (and preferably) there is, another, different value of i [among those i just above] for which $b \equiv a_i \pmod{m_i}$ *but* for which $b \not\equiv a_i + k_i m_i \pmod{m_i p_i}$ [in which case, from the reasoning above, one has, for every t satisfying S, ($p_i \parallel t - 8 - 2^b$ for this i and so) $t \neq M^2 + N^2 + 8 + 2^b$ for the b in question; i.e. this b will have been dealt with for the principal case $a = 3$]—*or* if no such additional i exists, that $b \equiv a_i \pmod{m_i}$ for some i in system (1) such that $41 \leq i \leq 74$ (such b will also be dealt with below). And similarly, for $4 \leq i \leq 12$ and $75 \leq i \leq 105$, one must further examine those $b \equiv a_i + k_i m_i \pmod{m_i p_i}$, $0 \leq b \leq 1416$; again, for each such b, it will be shown that *either* (and preferably) there is, another, different value of i [among those $4 \leq i \leq 12$ and $75 \leq i \leq 105$] for which $b \equiv a_i \pmod{m_i}$ *but* for which $b \not\equiv a_i + k_i m_i \pmod{m_i p_i}$ [in which case from the reasoning above, one has, for every t satisfying S, $t \neq M^2 + N^2 + 2 + 2^b$ for the b in question; i.e. this b will have been dealt with for the principal case $a = 1$]—*or* if no such additional i exists, that $b \equiv a_i \pmod{m_i}$ for some i in system (1) such that $106 \leq i \leq 139$ (such b also to be dealt with below). Those b, or any subset thereof, which must be further examined as set out in this paragraph, will be referred to as *unresolved* (values of) $b \leq 1416$. And such unresolved b—i.e. initially those non-negative $b \equiv a_i + k_i m_i \pmod{m_i p_i}$ and ≤ 1416—for numerically specified values of i will be referred to as *unresolved* $b \leq 1416$ for those values of i ([7]). (When $b \leq 1416$ is omitted with unresolved b, it is understood.) As will become apparent, the unresolved $b \leq 1416$ will steadily "thin out" as an increasing number of them are satisfactorily dealt with or resolved for the purpose of proving the theorem. [There remain values of b—in connection with $t - 8 - 2^b$—which satisfy system (1) for *only* i such that $41 \leq i \leq 74$ (leading *only* to congruences in S not involving p_i^2), and also values of b—in connection with $t - 2 - 2^b$—which satisfy system (1) for *only* i such that $106 \leq i \leq 139$ (leading *only* to congruences in S not involving p_i^2); these values of b will also be dealt with later in the proof.]

Now to deal with the unresolved values of b, starting with the *even* ones for the principal case $a = 3$.

---

that for each b, $p_i \parallel t - 8 - 2^b$ (for some i) and $p_i \parallel t - 2 - 2^b$ (for some i), while enabling the identification of those b (as few as possible) for which both these "$\parallel$" relationships (or at least one of them) must yet be shown (for at least one value of $t < 2^{1417}$). And the values of the k_i needed to ensure that the members of a pair of equal moduli have equal residues (mod p_i^2) are easily seen to be connected.

([7]) It should be mentioned that judicious choices of k_i often help to reduce the number of unresolved integers. This will become apparent as the proof proceeds.

First, looking at $i = 1$, with $x_1 \equiv 0 \pmod 2$ in system (1) satisfied by *all* non-negative even integers, the *only* even values of b (≤ 1416) that are unresolved are [those unresolved for $i = 1$, i.e.] $b \equiv 0 \pmod 6$ [from $b \equiv a_1 + k_1 m_1 \pmod{m_1 p_1}$ with $a_1 = 0$, $m_1 = 2$, $k_1 = 0$, $p_1 = 3$; by part of the same argument, $p_1 \parallel t - 8 - 2^b$ for $b \equiv 0 \pmod 2$ but $\not\equiv 0 \pmod 6$]. And these values of b [$\equiv 0 \pmod 6$] are just those even values satisfying [$x_i \equiv a_i \pmod{m_i}$ for $i = 2$, i.e. satisfying] $x_2 \equiv 0 \pmod 3$; then the only even values of $b \leq 1416$ that are now unresolved are [those unresolved for $i = 2$, i.e.] $b \equiv 0 \pmod{21}$ [from $b = a_2 + k_2 m_2 \pmod{m_2 p_2}$ with $a_2 = 0$, $m_2 = 3$, $k_2 = 0$, $p_2 = 7$; by part of the same argument, $p_2 \parallel t - 8 - 2^b$ for $b \equiv 0 \pmod 6$ but $\not\equiv 0 \pmod{21}$]. And those values of b [$\equiv 0 \pmod{21}$] that are even [$\equiv 0 \pmod{42}$] are just those values of b satisfying $x_3 \equiv 0 \pmod{42}$; then the only even values of $b \leq 1416$ that are now unresolved are [those unresolved for $i = 3$, i.e.] $b \equiv 0 \pmod{227598}$ [from $b \equiv a_3 + k_3 m_3 \pmod{m_3 p_3}$ with $a_3 = 0$, $m_3 = 42$, $k_3 = 0$, $p_3 = 5419$; $p_3 \parallel t - 8 - 2^b$ for $b \equiv 0 \pmod{42}$ but $\not\equiv 0 \pmod{227598}$]. The only such non-negative $b \leq 1416$ is $b = 0$, in which case $t - 8 - 2^b \equiv 3 \pmod 4 \neq M^2 + N^2$. Hence, for any non-negative *even* $b \leq 1416$, $t - 8 - 2^b \neq M^2 + N^2$—for every t satisfying S. Next to deal with the unresolved *even* values of b for the principal case $a = 1$. First, looking at $i = 4$, with $x_4 \equiv 0 \pmod 2$ in system (1) satisfied by *all* non-negative even integers, the *only* even values of b (≤ 1416) that are unresolved are [those unresolved for $i = 4$, i.e.] $b \equiv 4 \pmod 6$ [from $b \equiv a_4 + k_4 m_4 \pmod{m_4 p_4}$ with $a_4 = 0$, $m_4 = 2$, $k_4 = 2$, $p_4 = 3$; $p_4 \parallel t - 2 - 2^b$ for $b \equiv 0 \pmod 2$ but $\not\equiv 4 \pmod 6$]. Now for each of the following values of i, the only unresolved even values of b (≤ 1416) are the following (determined as above using the appropriate a_i, k_i, m_i, p_i): $b \equiv 50 \pmod{110}$, $b \equiv 256 \pmod{342}$, $b \equiv 3 \pmod{155}$, for $i = 5, 6, 7$ respectively [for $i = 8, 9, 10, 11, 12$, still using $b \equiv a_i + k_i m_i \pmod{m_i p_i}$ of course, it is easily seen numerically that for each i, there are no non-negative even $b \leq 1416$ that are unresolved]. Since each value of $b \equiv 4 \pmod 6$—from above, those $b \equiv 4 \pmod 6$ being the *only* unresolved even values of b—satisfies $x_i \equiv a_i \pmod{m_i}$ in system (1) for at least one i such that $5 \leq i \leq 11$ [seen by writing each $a_i \pmod{m_i}$, $5 \leq i \leq 11$, in terms of residue classes (mod 90) and comparing with the residue classes (mod 90) corresponding to $b \equiv 4 \pmod 6$] and since there are no unresolved even values of $b \leq 1416$ for $8 \leq i \leq 11$, the only even values of b now unresolved are those even values of b unresolved for $i = 5, 6, 7$. [It is clear from the whole argument so far that as regards all other non-negative even $b \leq 1416$, for each such b, $p_i \parallel t - 2 - 2^b$ for some i, $4 \leq i \leq 11$.] But from above, these remaining unresolved even values of b must *also* satisfy $b \equiv 4 \pmod 6$; hence the only values of b then actually remaining unresolved for $i = 5$ are those $b \equiv 50 \pmod{110}$ which simultaneously satisfy $b \equiv 4 \pmod 6$, and thus only those $b \equiv 160 \pmod{330}$, while the only even values

of b actually remaining unresolved for $i = 7$ are those $b \equiv 3 \pmod{155}$ which simultaneously satisfy $b \equiv 4 \pmod 6$, and thus only those $b \equiv 778 \pmod{930}$. [Those $b \equiv 256 \pmod{342}$ for $i = 6$ are also unresolved, a matter which will be dealt with below; already those $b \equiv 4 \pmod 6$ and so are not "thinned" by the latter congruence.] The non-negative even values of $b \leq 1416$ actually remaining unresolved for $i = 5, 7$ are then precisely the following: (for $i = 5$) $b = 160$, 490, 820, 1150, and (for $i = 7$) $b = 778$. However, $b = 490$, 778 satisfy $x_6 \equiv 4 \pmod{18}$, but those $b \not\equiv 256 \pmod{342}$ so that $p_6 = 19 \parallel t - 2 - 2^b$ for those b. And $b = 160$, 1150 satisfy $x_{12} \equiv 160 \pmod{495}$, but as already asserted, those $b \not\equiv a_i + k_i m_i \pmod{m_i p_i}$ for $i = 12$, so that $p_{12} = 991 \parallel t - 2 - 2^b$ for those b. And $b = 820$ satisfies $x_i \equiv a_i \pmod{m_i}$ for $i = 91$, so that (from Lemma 2 applied to the bracketed pair $[31, 91]$, which as shown below implies that there are no unresolved values of $b \leq 1416$ of either parity for $i = 91$) $p_{91} = 167 \parallel t - 2 - 2^b$ for $b = 820$. Thus, the only even values of $b \leq 1416$ now unresolved are those even values of b (≤ 1416) unresolved for $i = 6$, i.e. (from above) those $b \equiv 256 \pmod{342}$. Now the only values of $b \equiv 4 \pmod 6$ satisfying $x_6 \equiv 4 \pmod{18}$, namely those $b \equiv 4 \pmod{18}$, but which do not satisfy $x_i \equiv a_i \pmod{m_i}$ for $i = 5$, $7 \leq i \leq 11$, are those $b \equiv 4 \pmod{90}$ [which is seen when writing each $a_i \pmod{m_i}$, $5 \leq i \leq 11$, in terms of residue classes (mod 90) as above]. Since the smallest non-negative integer satisfying simultaneously $b \equiv 4 \pmod{90}$ and $b \equiv 256 \pmod{342}$ is $b = 1624$, there is no unresolved $b \leq 1416$ for $i = 6$ that has not already been resolved through consideration of $i = 5$, $7 \leq i \leq 11$. Hence there are no unresolved (non-negative) even values of $b \leq 1416$ remaining. [Indeed, it is clear from the argument given so far that for each non-negative even $b \leq 1416$, $p_i \parallel t - 2 - 2^b$ for some i with $4 \leq i \leq 12$ or $i = 91$, where $p_i \equiv 3 \pmod 4$.] Hence for any non-negative even $b \leq 1416$, $t - 2 - 2^b \neq M^2 + N^2$—for every t satisfying S.

Thus for the principal cases $a = 1, 3$, all non-negative *even* $b \leq 1416$ have been dealt with—for every t satisfying S—though only for (positive) $t < 2^{1417}$ will this be of value in proving Theorem 1. Next, consider the bracketed pairs of i listed above; these have already been discussed during the earlier use of Lemma 2 in connection with equal residues for equal moduli in S. Indeed, one has (from Lemma 2, using the same substitutions as earlier in its hypothesis and conclusion) that in each bracketed pair of i, both k_i (for the two values of i in the pair) may be chosen together so that [not only are (as above) the appropriate residues (mod p_i^2) equal but also] $(p_i - 1)m_i/2 \leq a_i + k_i m_i < m_i p_i$ for both i in the pair. And checking the m_i and p_i for each pair (of i)—for both i, the m_i are equal and the p_i are equal—it follows (numerically) that $(p_i - 1)m_i/2 > 1416$ for both i in each pair, so that $a_i + k_i m_i > 1416$ for both i of each pair; also since from above $a_i + k_i m_i < m_i p_i$ for both i of each pair, it follows that $a_i + k_i m_i - L m_i p_i < 0$

for $L \geq 1$. Hence in each pair, for both i and the corresponding values of $b \equiv a_i \pmod{m_i}$, there is no non-negative $b \leq 1416$ such that $b \equiv a_i + k_i m_i \pmod{m_i p_i}$. Thus for every i in the (seventeen) bracketed pairs, there are no (non-negative) unresolved $b \leq 1416$—from which of course, it follows (for $b \leq 1416$) that in each pair, for the smaller i, $p_i \parallel t - 8 - 2^b$, $b \equiv a_i \pmod{m_i}$, while for the larger i, $p_i \parallel t - 2 - 2^b$, $b \equiv a_i \pmod{m_i}$, $p_i \equiv 3 \pmod 4$. [And while indeed, this conclusion for the bracketed pairs applies to those b of either parity, the only even b for which it is needed is $b = 820$ (see above in connection with the even values of b) satisfying the congruence for $i = 91$ in system (1), thus needing (this conclusion for) the bracketed pair $[31, 91]$. Otherwise this conclusion for the bracketed pairs will be needed only for odd b.]

Now to deal with all positive *odd* $b \leq 1416$ and hence ≤ 1415 for each of the two principal cases. [It should be remembered that every positive odd integer ≤ 1415 satisfies at least one of the congruences in (1) corresponding to $13 \leq i \leq 74$ (for the principal case $a = 3$); the same is true for the congruences corresponding to $75 \leq i \leq 139$ (for the principal case $a = 1$).] First, looking at each i such that $13 \leq i \leq 40$ (i.e. relating to $t - 8 - 2^b$, for the principal case $a = 3$) the only non-negative *odd* values of $b \leq 1416$ that are unresolved are those $b \leq 1415$ and satisfying at least one of the congruences $b \equiv 0 \pmod{21}$ [$\equiv 21 \pmod{42}$], $b \equiv 9 \pmod{110}$, $b \equiv 89 \pmod{342}$, $b \equiv 162 \pmod{253}$, $b \equiv 1 \pmod{155}$, $b \equiv 107 \pmod{602}$, $b \equiv 368 \pmod{1081}$, $b \equiv 908 \pmod{2485}$, $b \equiv 554 \pmod{889}$, $b \equiv 48070 \pmod{48205}$, for $i = 13$, 14, 15, 16, 17, 18, 19, 22, 27, 40 respectively [as before, of course, these are easily verified from the values of a_i, k_i, m_i, p_i inserted into $b \equiv a_i + k_i m_i \pmod{m_i p_i}$; it is easily seen that there actually are no unresolved odd $b \leq 1415$ for $i = 19$, 22, 27, 40. The values of i with $13 \leq i \leq 40$ other than the ten values just listed have been dealt with already in the bracketed pairs; there are, as just shown using Lemma 2, no unresolved odd values of $b \leq 1415$ for these i]. The unresolved odd values of $b \leq 1415$ then are (for $i = 13$) $b = 21$, 231, 441, 651, 861, 1071, 1281, 189, 399, 609, 819, 1029, 1239, 63, 483, 525, 1365, 777, 987 [with the remaining (fifteen) odd values of $b \equiv 0 \pmod{21}$ and ≤ 1415 to be listed and dealt with later]; (for $i = 14$) $b = 9$, 119, 229, 339, 449, 559, 669, 779, 889, 999, 1109, 1219, 1329; (for $i = 15$) $b = 89$, 431, 773, 1115; (for $i = 16$) $b = 415$, 921; (for $i = 17$) $b = 1$, 311, 621, 931, 1241; (for $i = 18$) $b = 107$, 709, 1311. However, $b = 9$, 339, 669, 999, 1329, 921, 621, 1311 satisfy [$x_i \equiv a_i \pmod{m_i}$ for $i = 13$, i.e.] ($b =$) $x_{13} \equiv 0 \pmod 3$ but for these b, $b \not\equiv 0 \pmod{21}$ so that (for these b) $p_{13} = 7 \parallel t - 8 - 2^b$. And $b = 89$, 709, 189, 399, 609, 819, 1029, 1239 satisfy $x_{14} \equiv 9 \pmod{10}$ but $\not\equiv 9 \pmod{110}$ so that $p_{14} = 11 \parallel t - 8 - 2^b$ for these b. And $b = 107$ satisfies $x_{15} \equiv 17 \pmod{18}$ but $\not\equiv 89 \pmod{342}$ so that $p_{15} = 19 \parallel t - 8 - 2^b$ for this b. And $b = 63$, 525, 987 satisfy $x_{16} \equiv 8 \pmod{11}$ but $\not\equiv 162 \pmod{253}$ so that

$p_{16} = 23 \,\|\, t - 8 - 2^b$ for these b. And $b = 431$, 21, 231, 441, 651, 861, 1071, 1281 satisfy $x_{17} \equiv 1 \pmod 5$ but $\not\equiv 1 \pmod{155}$ so that $p_{17} = 31 \,\|\, t - 8 - 2^b$ for these b. And $b = 779$, 1115, 415, 1241 satisfy $x_{18} \equiv 9 \pmod{14}$ but $\not\equiv 107 \pmod{602}$ so that $p_{18} = 43 \,\|\, t - 8 - 2^b$ for these b. And $b = 483$ satisfies $x_{19} \equiv 0 \pmod{23}$ but $\not\equiv 368 \pmod{1081}$ so that $p_{19} = 47 \,\|\, t - 8 - 2^b$ for this b. And $b = 931$ satisfies $x_{25} \equiv 13 \pmod{51}$ so that (from the above conclusion for the bracketed pairs applied to $[25, 84]$) $p_{25} = 103 \,\|\, t - 8 - 2^b$ for $b = 931$. And $b = 1109$ satisfies $x_{26} \equiv 49 \pmod{106}$ so that (remembering the bracketed pair $[26, 85]$) $p_{26} = 107 \,\|\, t - 8 - 2^b$ for $b = 1109$. And $b = 449$, 1219, 1 satisfy $x_{27} \equiv 1 \pmod 7$ but $\not\equiv 554 \pmod{889}$ so that $p_{27} = 127 \,\|\, t - 8 - 2^b$ for these b. And $b = 777$ satisfies $x_{37} \equiv 27 \pmod{50}$ so that (remembering the bracketed pair $[37, 99]$) $p_{37} = 251 \,\|\, t - 8 - 2^b$ for $b = 777$. And $b = 1365$ satisfies $x_{38} \equiv 49 \pmod{94}$ so that (remembering the bracketed pair $[38, 102]$) $p_{38} = 283 \,\|\, t - 8 - 2^b$ for $b = 1365$. And $b = 889$ satisfies $x_{39} \equiv 73 \pmod{102}$ so that (remembering the bracketed pair $[39, 103]$) $p_{39} = 307 \,\|\, t - 8 - 2^b$ for $b = 889$. Next, $b = 119$, 229, 559 satisfy $x_{72} \equiv 9 \pmod{55}$ so that from the argument ([8]) in footnote 8 applied to the corresponding congruence in S, $p_{72} = 3191 \,|\, t - 8 - 2^b$ for these b. Also, $b = 773$ satisfies $x_{73} \equiv 89 \pmod{114}$, so that one has similarly from the corresponding congruence in S, $p_{73} = 571 \,|\, t - 8 - 2^b$ for this b. And also, $b = 311$ satisfies $x_{74} \equiv 1 \pmod{155}$, so that from the corresponding congruence in S, $p_{74} = 11471 \,|\, t - 8 - 2^b$ for this b. The remaining fifteen odd values referred to above of $b \equiv 0 \pmod{21}$ and ≤ 1415 will now be dealt with. First, $b = 105$, 1197 satisfy $x_{41} \equiv 1 \pmod{13}$ so that (from the argument in footnote 8 applied to the corresponding congruence in S) $p_{41} = 2^{13} - 1 \,|\, t - 8 - 2^b$ for these b. Next, $b = 1407$ satisfies $x_{42} \equiv 1 \pmod{19}$ so that $p_{42} = 2^{19} - 1 \,|\, t - 8 - 2^b$ for this b. Next, $b = 903$ satisfies $x_{43} \equiv 1 \pmod{22}$ so that $p_{43} = 683 \,|\, t - 8 - 2^b$ for this b. Next, $b = 273$ satisfies $x_{46} \equiv 1 \pmod{34}$ so that $p_{46} = 43691 \,|\, t - 8 - 2^b$ for this b. Next, $b = 315$, 735, 945, 1155 satisfy $x_{68} \equiv 0 \pmod{105}$ so that $p_{68} = 29191 \,|\, t - 8 - 2^b$ for these b. Next $b = 357$, 1113 satisfy $x_{69} \equiv 357 \pmod{378}$ so that $p_{69} = 379 \,|\, t - 8 - 2^b$ for these b. Next, $b = 147$, 693 satisfy $x_{70} \equiv 147 \pmod{546}$ so that $p_{70} = 547 \,|\, t - 8 - 2^b$ for these b. Finally, $b = 567$, 1323 satisfy $x_{71} \equiv 189 \pmod{378}$ so that $p_{71} = 119827 \,|\, t - 8 - 2^b$ for these b.

([8]) For any i such that $41 \leq i \leq 74$, from system S above, $t - 8 \equiv 2^{a_i} \pmod{p_i}$. Since [with 2 belonging to $m_i \pmod{p_i}$] $2^{m_i} \equiv 1 \pmod{p_i}$, it follows that $2^{Lm_i} \equiv 1 \pmod{p_i}$ for $L \geq 0$. Thus by congruence multiplication one has, for every t satisfying S, $t - 8 \equiv 2^{a_i + Lm_i} \pmod{p_i}$ [$a_i < m_i < p_i$, $L \geq 0$]. Hence, if $b = a_i + Lm_i$ [i.e. b satisfies $x_i \equiv a_i \pmod{m_i}$ in system (1)] for some i, $41 \leq i \leq 74$, then, for every t satisfying S, $p_i \,|\, t - 8 - 2^b$ (for that i). Similarly, it can been shown that if b satisfies $x_i \equiv a_i \pmod{m_i}$ in system (1) for some i, $106 \leq i \leq 139$, then, for every t satisfying S, $p_i \,|\, t - 2 - 2^b$ for that i. [It is clear that 2 belonging to $m_i \pmod{p_i}$ is a sufficient but not a necessary condition in this argument. All that is actually needed is that $2^{m_i} \equiv 1 \pmod{p_i}$.] Again, I have chosen to present this argument in a footnote, so as to help the flow of the main text.

Thus, to sum up, for every t satisfying S, it has been shown that for each odd $b \leq 1415$ which satisfies $x_i \equiv a_i \pmod{m_i}$ for some i with $13 \leq i \leq 40$, $p_i \,\|\, t-8-2^b$ for that i (in S), $p_i \equiv 3 \pmod 4$—with the following exceptions: $b = 119,\ 229,\ 559$ [(satisfying $x_i \equiv a_i \pmod{m_i}$) for $i = 72$], $b = 773$ [for $i = 73$], $b = 311$ [for $i = 74$], $b = 105,\ 1197,\ 903,\ 1407,\ 273,\ 315,\ 735,\ 945,\ 1155,\ 147,\ 693,\ 567,\ 1323,\ 357,\ 1113$ [each (of these last fifteen values) satisfying system (1) for at least one of $i = 41,\ 42,\ 43,\ 46,\ 68,\ 69,\ 70,\ 71$ as set out above] making a total of twenty distinct exceptions, each of which is still an unresolved b (corresponding to $t - 8 - 2^b$)—and for each of which [from (the argument in) footnote 8 (applied to the appropriate congruence in S)] for every t satisfying S, $p_i \,|\, t - 8 - 2^b$ for some i in S, $41 \leq i \leq 74$, where for each of these twenty values of b, i is as just set out.

Next, looking at each i such that $75 \leq i \leq 105$ (i.e. relating to $t-2-2^b$, for the principal case $a = 1$), the only non-negative *odd* values of $b \leq 1416$ that are unresolved are those $b \leq 1415$ and satisfying at least one of the congruences $b \equiv 71 \pmod{253}$, $b \equiv 3 \pmod{155}$, $b \equiv 393 \pmod{602}$ for $i = 75,\ 76,\ 77$ respectively [using $b \equiv a_i + k_i m_i \pmod{m_i p_i}$ for each i of course, these congruences are easily verified numerically, while using $b \equiv a_i + k_i m_i \pmod{m_i p_i}$ for $i = 78,\ 81,\ 86,\ 89,\ 93,\ 98,\ 100,\ 101,\ 104,\ 105$, it is easily verified numerically from these ten congruences that there are actually no unresolved non-negative odd $b \leq 1415$ for these ten values of i; the other values of i with $75 \leq i \leq 105$ have already been dealt with in the bracketed pairs—there are, as already shown, no unresolved odd values of $b \leq 1415$ for these bracketed i.] The unresolved odd values of $b \leq 1415$, then, are (for $i = 75$) $b = 71,\ 577,\ 1083$; (for $i = 76$) $b = 3,\ 313,\ 623,\ 933,\ 1243$; (for $i = 77$) $b = 393,\ 995$. However, $b = 71$ satisfies $x_{77} \equiv 1 \pmod{14}$ but $b \not\equiv 393 \pmod{602}$ so that $p_{77} = 43 \,\|\, t-2-2^b$ for this b. And $b = 577,\ 3$ satisfy $x_{86} \equiv 3 \pmod 7$ but $b \not\equiv a_i + k_i m_i \pmod{m_i p_i}$ for $i = 86$, i.e. $b \not\equiv 808 \pmod{889}$, so that $p_{86} = 127 \,\|\, t-2-2^b$ for these b. And $b = 1083,\ 393$ satisfy $x_{76} \equiv 3 \pmod 5$ but $b \not\equiv 3 \pmod{155}$ so that $p_{76} = 31 \,\|\, t - 2 - 2^b$ for these b. And $b = 313,\ 995$ satisfy $x_{75} \equiv 5 \pmod{11}$ but $b \not\equiv 71 \pmod{253}$ so that $p_{75} = 23 \,\|\, t-2-2^b$ for these b. And $b = 623$ satisfies $x_{90} \equiv 137 \pmod{162}$ (so that, from the above conclusion for the bracketed pairs applied to $[30, 90]$) $p_{90} = 163 \,\|\, t - 2 - 2^b$ for this b. Finally, $b = 933,\ 1243$ satisfy (for $i = 139$) $x_i \equiv 3 \pmod{155}$ so that (from the argument in footnote 8 applied to the corresponding congruence in S) $p_{139} = 11471 \,|\, t - 2 - 2^b$ for these b.

Thus, to sum up, for every t satisfying S, it has been shown that for each odd $b \leq 1415$ which satisfies $x_i \equiv a_i \pmod{m_i}$ for some i with $75 \leq i \leq 105$, $p_i \,\|\, t-2-2^b$ for that i (in S), $p_i \equiv 3 \pmod 4$, with the following exceptions: $b = 933,\ 1243$ [satisfying system (1) for $i = 139$] making a total of two distinct exceptions, each of which is still an unresolved b (corresponding to $t-2-2^b$) and for each of which—from (the argument in) footnote 8 (applied

to the corresponding congruence in S)—for every t satisfying S, $p_i \mid t-2-2^b$ for $i = 139$ in S.

There are also exactly seventy *odd* values of $b \leq 1415$ (in connection with $t-8-2^b$, the principal case $a = 3$), each of which satisfies $x_i \equiv a_i \pmod{m_i}$ *only* for (at least) one i with $41 \leq i \leq 74$ (thus, among the congruences in S concerning $a = 3$, leading *only* to (at least) one congruence whose modulus is p_i and *not* p_i^2)—these b may be determined by straightforward use of $x_i \equiv a_i \pmod{m_i}$, $13 \leq i \leq 40$ to verify their existence and number (i.e. finding all odd $b \leq 1415$ satisfying at least one of these congruences and then those that do not satisfy any of them) ([9]). And these seventy odd values of b will *also* be referred to as unresolved (corresponding to $t-8-2^b$)—since they have not yet been satisfactorily dealt with for the purpose of proving this theorem. However, for each of these (seventy) values of b as well, again from footnote 8 it follows that for every t satisfying S, $p_i \mid t-8-2^b$ for some i, $41 \leq i \leq 74$ in S, [$p_i \equiv 3 \pmod 4$], where $b \equiv a_i \pmod{m_i}$ for that i. Together with the twenty unresolved values of b (corresponding to $t-8-2^b$) already given in the first summing up—and to which footnote 8 also applies—there are as yet a total of ninety unresolved b corresponding to $t-8-2^b$. And there are also exactly 160 *odd* values of $b \leq 1415$ (in connection with $t-2-2^b$, the principal case $a = 1$), each of which satisfies $x_i \equiv a_i \pmod{m_i}$ *only* for (at least) one i such that $106 \leq i \leq 139$ (thus, among the congruences in S concerning $a = 1$, leading *only* to (at least) one congruence whose modulus is p_i and *not* p_i^2)—these b may be determined by straightforward use of the $x_i \equiv a_i \pmod{m_i}$, $75 \leq i \leq 105$, to verify their existence and number (see footnote 9 which would apply here as well, with the corresponding changes in the values of i). These 160 odd values of b will *also* be referred to as unresolved (corresponding to $t-2-2^b$)—again, since they have not yet been satisfactorily dealt with for the purpose of proving this theorem. However, for each of these (160) values of b as well, [again from footnote 8] for any t satisfying S, $p_i \mid t-2-2^b$ for some i such that $106 \leq i \leq 139$ in S, [$p_i \equiv 3 \pmod 4$], where $b \equiv a_i \pmod{m_i}$ for that i. Together with the two unresolved values of b (for $t-2-2^b$) already given in the second summing up—and to which footnote 8 also applies—there are

([9]) This numerical work can be done in conjunction with the verification (referred to) in footnote 3—since one is identifying the odd integers taken on by system (1) for each $13 \leq i \leq 74$, which itself is part of the lengthy verification referred to in footnote 3. (One might also cross-check the odd integers already found as above to satisfy system (1) *only* for (at least) one i with $41 \leq i \leq 74$ against those satisfying system (1) for at least one i, $13 \leq i \leq 40$—the two mutually exclusive sets together should take on all positive odd integers ≤ 1416). The whole process, including the verification referred to in footnote 3, involves a lengthy list of consecutive positive odd numbers—even without the cross-checking.

as yet 162 unresolved values of b corresponding to $t-2-2^b$. And while some of the unresolved b for $t-8-2^b$ are also unresolved b for $t-2-2^b$, in the present situation, each of these values of b must be counted twice (as will become apparent from the rest of the argument below; see footnote 13 especially). Hence, altogether there are as yet $(90+162=)$ 252 unresolved values of b.

Now take $t=H+wP$, H and P already defined in setting out what are the demonstrated solutions (to S′ and hence) to S. And from above, for $t<2^{1417}$, w can be taken consecutively from 0 through all integers to $v-1$ with fixed $v\geq 10^{52}$; however, it suffices here to take $0\leq w\leq 345$, giving $t=H+wP$ $(<2^{1417})$ for consecutive integers $0\leq w\leq 345$; it is these (346) values of t, (positive) solutions $<2^{1417}$ to S, which will now be of greatest significance. First, to deal with the (90) remaining unresolved values of b corresponding to $t-8-2^b$. Given any (remaining unresolved value of) b corresponding to $t-8-2^b$, it follows from above that for the given b, $p_i \mid H+wP-8-2^b$ for some i, $41\leq i\leq 74$, and for all w, where (with p_i being one of the above ([10]) assigned in S to $41\leq i\leq 74$) $p_i\geq 379>346$. Then, *if* for the given b, $p_i^2 \mid H+wP-8-2^b$ for some w such that $0\leq w\leq 345$, say w_0, *then* since (again remembering that p_i is one of the above assigned to $41\leq i\leq 74$) $p_i \parallel P$, $p_i^2 \mid H+wP-8-2^b$ for the given b *only if* $w\equiv w_0 \pmod{p_i}$ and, since $p_i>346$ (while $0\leq w_0\leq 345$), *only if* $w=w_0$ [since for any other $w\equiv w_0 \pmod{p_i}$ one has either $w\geq w_0+p_i>w_0+346>345$, or $w\leq w_0-p_i<w_0-346<0$]. Hence, for the given b, $p_i \parallel H+wP-8-2^b$ for all $0\leq w\leq 345$ except for w_0; in other words, for the given b there is (at most ([11])) one value of w—among the (346) values $0\leq w\leq 345$—for which it is possible that $H+wP-8-2^b=M^2+N^2$. Since this argument indeed applies to *any* given (remaining unresolved value of) b corresponding to $t-8-2^b$, there are (at most) 90 values of w, $0\leq w\leq 345$, for which it is possible that $H+wP-8-2^b=M^2+N^2$—with the (90) remaining unresolved values of b and hence (since for all other non-negative values of $b\leq 1416$, it has been shown above that $H+wP-8-2^b\neq M^2+N^2$ for any w and a

([10]) If a given b satisfies $x_i\equiv a_i \pmod{m_i}$, $41\leq i\leq 74$, for more than one i, then there will be more than one p_i (among the above assigned p_i) for which $p_i \mid H+wP-8-2^b$ and which may thus be used for that value of b. The argument here needs (any) one such p_i to be used; for example, the p_i used may be the (one) p_i assigned above to the smallest i $(41\leq i\leq 74)$ for which (that value of) $b\equiv a_i \pmod{m_i}$, the other p_i then becoming unnecessary to use and can be ignored here for that value of b—as the argument in the text will make clear. This comment, with $106\leq i\leq 139$ in place of $41\leq i\leq 74$, will also apply to (the same argument for) any given (remaining unresolved value of) b corresponding to $t-2-2^b$.

([11]) Since $p_i\geq 379>346$, it obviously may be that there is no value of w, $0\leq w\leq 345$, for which this is possible for the given b; in fact, the larger the p_i (for the given b) actually is, the greater the likelihood of there being no such w, $0\leq w\leq 345$.

fortiori for $0 \le w \le 345$) with b such that $0 \le b \le 1416$. Then, by the same argument applied to the 162 remaining unresolved values of b corresponding to $t - 2 - 2^b$ (with $106 \le i \le 139$ in place of $41 \le i \le 74$ and 347 in place of 379 [but both > 346]), there are (at most ([12])) 162 values of w, $0 \le w \le 345$, for which it is possible that $H + wP - 2 - 2^b = M^2 + N^2$—with the (162) remaining unresolved values of b and hence (since for all other non-negative values of $b \le 1416$, it has been shown that $H + wP - 2 - 2^b \ne M^2 + N^2$ for any w and *a fortiori* for $0 \le w \le 345$) with b such that $0 \le b \le 1416$. Thus, there are (at least) $346 - (90 + 162) = 94$ (distinct) values ([13]) of w, $0 \le w \le 345$, for each of which *both* $H + wP - 8 - 2^b \ne M^2 + N^2$ *and* $H + wP - 2 - 2^b \ne M^2 + N^2$—with b such that $0 \le b \le 1416$. The above *principal* cases of $a = 1, 3$ can thus be finally settled—remembering that for each of these [(at least) 94 distinct] positive values of w, $t = H + wP < 2^{1417}$; any of these values of t can then be taken to settle the *principal* cases.

There are still three *special* cases to be dealt with (referred to at the beginning of this proof; as has been pointed out there as well, the other [two] special cases—$a = 0$, $b = 1$ and $a = 2$, $b = 3$—are covered by the principal cases). From $i = 140$ (with the corresponding congruence) in S, $p_i = 487 \,\|\, t - 2^3$, $487 \equiv 3 \pmod 4$, so that $t \ne M^2 + N^2 + 2^3$ and thus $t \ne M^2 + N^2 + 2^2 + 2^2$ for any t (and *a fortiori* any $t < 2^{1417}$). From $i = 141$ in S, $p_i = 563 \,\|\, t - 20$, $563 \equiv 3 \pmod 4$, so that $t \ne M^2 + N^2 + 20$ and thus $t \ne M^2 + N^2 + 2^2 + 2^4$ for any t. Finally, from $i = 2$ in S, $t \equiv 9 \pmod{49}$ so that $t - 2 \equiv 7 \pmod{7^2}$, and since $7 \,\|\, t - 2$, $t \ne M^2 + N^2 + 2$ from which $t \ne M^2 + N^2 + 2^0 + 2^0$ for any t. Thus the three special cases are disposed of for any t—most significantly for any of the [(at least) 94] positive values of t above settling the *principal* cases. Then (see the beginning of this proof) each of these values of t is not representable as in the hypothesis of Lemma 1.

Given any of these values of t, say t_1; then applying Lemma 1 to $t = t_1$ [also noting of course, from $i = 1, 4$ in S, $(t_1 =)\ t \equiv 0 \pmod 9$, and from $i = 142$ in S, $(t_1 =)\ t \equiv 0 \pmod 4$], the proof is complete and Theorem 1 follows. ∎

COMMENT. It should be noted that there seems to be no way of using fewer than two principal cases in the proof of Theorem 1. If one tries, for example, to use 30 (mod 32), then there are still two unavoidable principal

([12]) The previous footnote applies here as well (with 347 in place of 379) for any given (unresolved value of) b.

([13]) If a value of b is an unresolved value for both $t - 8 - 2^b$ and $t - 2 - 2^b$, then one—and a different—value of w_0 may be involved in each case—thus the possibility of having to eliminate (i.e. subtract from 346) two values of w altogether for that b. Thus any such b, as pointed out above, has to be and has been counted twice (in calculating the total number [252] of unresolved values) to give an upper bound to the number of values of w to be subtracted from 346.

cases corresponding to $a = 0$ and $a = 2$. Failure to address $a = 0$ would undermine the use of Lemma 1 (as mentioned in footnote 1). Use of e.g. 24 (mod 32) would require three principal cases, while use of e.g. 0 (mod 32) or 16 (mod 32) would no longer limit the number of principal cases at all. Nor would changing the modulus 32 help. As for non-representability (as in Theorem 1) of *odd* integers (see later in the paper) it is possible to use only one principal case—but then there seems to be no equivalent to or suitable modification of Lemma 1, so that only a finite number of non-representable (odd) integers can be proved (as far as I can see, by present methods anyway).

THEOREM 2. *For any fixed positive* $k \equiv 2 \pmod 8$ *and* $k \geq 10$, *there is an infinity of positive* (*even*) *integers not representable as* $M^2+N^2+k^a+k^b$ *or as* $M^2+N^2+k^a$ (*or as* M^2+N^2), $a, b \geq 0$.

Proof. Let $k_1 = k + 1 \equiv 3 \pmod 4$. It will now be shown that $k_1^3 2^n$ cannot be represented as above (for the k in question) for n sufficiently large (≥ 8). Let $K = k_1^3 2^n - k^a - k^b \geq 0$ (since if $K < 0$, certainly $K \neq M^2 + N^2$); then $a, b < \log_k(k_1^3 2^n) = 3 \log_k k_1 + n \log_k 2$, and for $k \geq 10$, $n \geq 8$, one has $3 \log_k k_1 + n \log_k 2 \leq 3 \log_{10} 11 + n \log_{10} 2 < n - 2$, so that $a, b < n - 2$, from which $a, b \leq n - 3$. Without loss of generality, take $a \geq b$. Now $K = 2^b(k_1^3 2^{n-b} - 2^{a-b} q^a - q^b)$ with $k = 2q$, $q \equiv 1 \pmod 4$ [so that $q^a \equiv q^b \equiv 1 \pmod 4$]. First, if $a = b$, it follows, remembering that $n - b \geq 3$, that $K = 2^{b+1} I$ with $I = k_1^3 2^{n-b-1} - q^b \equiv 3 \pmod 4$, so that $K \neq M^2 + N^2$. Next, let $a \geq b + 2$; one has $n - b > a - b \geq 2$, in which case $K = 2^b J$ with $J \equiv 3 \pmod 4$, so that again $K \neq M^2 + N^2$. Finally, if $a = b + 1$, from above one has $K = k_1^3 2^n - k^b(k + 1)$ and since $k_1 \parallel k + 1$ while $(k_1, k) = 1$, it follows that $k_1 \parallel K$ so that again $K \neq M^2 + N^2$. Thus $K \neq M^2 + N^2$ with $a \geq b$ (and thus $K \neq M^2 + N^2$). Now let $K = k_1^3 2^n - k^a \geq 0$; one has $a \leq \log_k(k_1^3 2^n)$ and then, arguing as above, one again has that for $k \geq 10$ and $n \geq 8$, $a < n - 2$. Now $K = 2^a(k_1^3 2^{n-a} - q^a)$ with $n - a > 2$ and $k = 2q$, $q \equiv 1 \pmod 4$. Then $K = 2^a H$ with $H \equiv 3 \pmod 4$ so that $K \neq M^2 + N^2$. And finally, with $k_1 \equiv 3 \pmod 4$, $k_1^3 2^n$ itself $\neq M^2 + N^2$. ∎

Now, for the purpose of proving Theorem 3, the following lemma is needed.

LEMMA 3. *Take any fixed positive* $k \equiv 5 \pmod 8$. *Then for each successive* $n \geq 1$, *there exists a* (*prime*) $p_n \mid k^{\prod_{i=1}^{n-1} p_i} + 1$ *with* $\prod_{i=1}^{n-1} p_i$ *taken as* 1 *if* $n = 1$, *where* $p_n \equiv 3 \pmod 4$ *and* $p_n \neq p_i$, $i < n$.

Proof. $k + 1 \equiv 6 \pmod 8$ so that there is indeed a $p_1 \mid k + 1$ with $p_1 \equiv 3 \pmod 4$; $p_1 \neq p_i$, $i < 1$ since p_i for $i < 1$ does not exist here. The lemma is thus proven for $n = 1$. Now assume the lemma holds for each m such that $1 \leq m \leq n$, $n \geq 1$, n arbitrary but fixed. Let $D = k^{\prod_{i=1}^{n} p_i} + 1 / k^{\prod_{i=1}^{n-1} p_i} + 1$,

$n \geq 1$. Let $E = D/p_n$. D is immediately seen to be (positive) integral. Now since $p_n^{\alpha_n} \parallel k^{\prod_{i=1}^{n-1} p_i} + 1$ where (from the above assumption of the lemma for n) $\alpha_n \geq 1$, then $p_n^{\alpha_n+1} \parallel k^{\prod_{i=1}^{n} p_i} + 1$ ([14]). Hence $p_n \parallel D$ (so that E is positive integral) and one thus has $p_n \nmid E$. And when $n \geq 2$, from the above assumption of the lemma for each m, $1 \leq m \leq n$, one has for each m with $1 \leq m \leq n-1$, $p_m \mid k^{\prod_{i=1}^{m-1} p_i} + 1 \mid k^{\prod_{i=1}^{n-1} p_i} + 1$, so that $p_m^{\alpha_m} \parallel k^{\prod_{i=1}^{n-1} p_i} + 1$ ($\alpha_m \geq 1$); then remembering (from the above assumption of the lemma for n) that $p_m \neq p_n$, it follows (from the first result in footnote 14) that (for each m with $1 \leq m \leq n-1$) $p_m^{\alpha_m} \parallel k^{\prod_{i=1}^{n} p_i} + 1$. Hence, for each m with $1 \leq m \leq n-1$, $p_m \nmid D$ and thus $p_m \nmid E$ for $n \geq 2$; the same also can be considered to hold (in a vacuous sense) for $n = 1$, the p_m for $m \leq n-1$ ($= 0$) being non-existent. Since $D \equiv 1 \pmod 4$ [because its numerator and denominator are each $\equiv 6 \pmod 8$] and since (from the above assumption of the lemma for n) $p_n \equiv 3 \pmod 4$, one has $E \equiv 3 \pmod 4$ [*so that* $E > 1$]. And having shown that $p_m \nmid E$ for each m with $1 \leq m \leq n$, it follows that there exists a $p_{n+1} \mid E$ (> 1) such that $p_{n+1} \neq p_m$, $1 \leq m \leq n$ *and* such that $p_{n+1} \equiv 3 \pmod 4$; also (since $p_{n+1} \mid E$) one has $p_{n+1} \mid k^{\prod_{i=1}^{n} p_i} + 1$. The lemma thus holds for $n+1$ (and the induction is complete). ∎

Comment. This routine lemma could very easily be deduced from the well-known result usually attributed to Bang, *except* for the necessity of $p_n \equiv 3 \pmod 4$. Some of the steps in the proof of the lemma could in fact be used and may have been used to prove a special case of Bang's result. However, even if that is so, using his result would not significantly simplify an already straightforward proof (which the present way is also more self-contained). Because of the requirement $p_n \equiv 3 \pmod 4$, some of the steps that could be or may have been used in proving Bang's result would have to be used again here explicitly anyway (and with a few added as well) to ensure $p_n \equiv 3 \pmod 4$.

Theorem 3. *For each fixed* (*positive*) $k \equiv 5 \pmod 8$, *there is an infinity of positive even integers neither representable as* $M^2 + N^2 + k^a + k^b$ *nor as* $M^2 + N^2 + k^a$ (*nor as* $M^2 + N^2$), $a, b \geq 0$.

([14]) Use is made in this proof of a well-known (and easily proved) result—that (for p any odd prime) if $p^\alpha \parallel k^f + 1$, $\alpha \geq 1$, and if $d = ef$ with $p^\beta \parallel e$, $\beta \geq 0$ and $2 \nmid e$, then $p^{\alpha+\beta} \parallel k^d + 1$. For the two applications in the (proof of the) present lemma, $\beta = 1$ and $\beta = 0$. This result is closely related to the following well-known and easily proved result—if $p^\alpha \parallel k^f - 1$, $\alpha \geq 1$, and if $d = ef$ with $p^\beta \parallel e$, $\beta \geq 0$, then $p^{\alpha+\beta} \parallel k^d - 1$. It is indeed possible to use the latter result in Theorem 1. However, one of the consequences of this result—namely that if $p \parallel 2^f - 1$, then $p \parallel 2^{ef} - 1$ if $p \nmid e$, while $p^2 \mid 2^{ef} - 1$ if $p \mid e$—is even more easily proved on its own and is all that is actually needed in Theorem 1—and also easily leads to the well-known result [that 2 belongs to $mp \pmod{p^2}$ if 2 belongs to $m \pmod p$ and if $p \parallel 2^m - 1$] used in Lemma 2.

Proof. Let $t \equiv 0 \pmod 8$ [which will apply to all t throughout the proof]. For any such t, $t - k^a \equiv 3 \pmod 4$ [$\neq M^2 + N^2$] for $a \geq 0$. And for any such t and for $a, b \geq 0$ with a, b having the same parity, $t - k^a - k^b \equiv 6 \pmod 8 \neq M^2 + N^2$. Now let a, b (≥ 0) be of opposite parity, taking (without loss of generality) $a > b$, so that $a - b$ is (positive and) *odd* (and will be so throughout the rest of the proof). From Lemma 3, for each successive $n \geq 1$, there exists a $p_n \equiv 3 \pmod 4$ such that

$$p_n \mid k^{\prod_{i=1}^{n-1} p_i} + 1 \quad \text{where } p_n \neq p_i,\ i < n \tag{1}$$

and where if $n = 1$, $\prod_{i=1}^{n-1} p_i$ is then to be taken as 1 as in Lemma 3. Now *first* [in (1)] assume (the first of *two* alternatives) that for each successive $n \geq 1$, $p_n^2 \nmid k^{\prod_{i=1}^{n-1} p_i} + 1$, so that here, for each successive $n \geq 1$,

$$p_n \parallel k^{\prod_{i=1}^{n-1} p_i} + 1. \tag{2}$$

Then take $t = 24 \prod_{i=1}^{n} p_i^2$, $n \geq 2$. Also assume, for the moment, that such $t < k^{\prod_{i=1}^{n} p_i}$. For any $n \geq 2$, consider $t - k^a - k^b = t - k^b(k^{a-b} + 1) \geq 0$; then $a, b < \prod_{i=1}^{n} p_i$ and so $a - b < \prod_{i=1}^{n} p_i$. Then for each $a - b < \prod_{i=1}^{n} p_i$, there is some r, $1 \leq r \leq n$, such that $p_r \nmid a - b$ in which case, for the *smallest* such r—from (1) with that r in place of n (but still allowing $r = n$ when applicable) and from the fact that $\prod_{i=1}^{r-1} p_i \mid a - b$ (the quotient being *odd*, including when $r = 1$ in which case $\prod_{i=1}^{r-1} p_i$ is of course [as above, for $n = 1$] taken as 1)—one has $p_r \mid k^{a-b} + 1$; while for that (same smallest) r—from (2) with r in place of n (but still allowing $r = n$ when applicable) and from $p_r \nmid a - b$ while $\prod_{i=1}^{r-1} p_i \mid a - b$ and from (the first result referred to in) footnote 14, with $p = p_r$, $\alpha = 1$, $f = \prod_{i=1}^{r-1} p_i$, $d = a - b$, and $\beta = 0$ [since if $\beta \neq 0$, $p_r \mid e \mid a - b$]—one has $p_r \parallel k^{a-b} + 1$. Then with $(p_r, k) = 1$, one has $p_r \parallel k^a + k^b$ so that, with $p_r^2 \mid t$ above, $p_r \parallel t - k^a - k^b$ and thus $t - k^a - k^b \neq M^2 + N^2$ for a, b (of opposite parity and hence from above for a, b) ≥ 0. Now it remains to prove the above assumption that $t < k^{\prod_{i=1}^{n} p_i}$ for $n \geq 2$. If $k \geq 5$ and $Q \geq 4$, then $24Q^2 < 5^Q \leq k^Q$ (as is easily proved by induction on Q); letting $Q = \prod_{i=1}^{n} p_i$, one then has $t < k^{\prod_{i=1}^{n} p_i}$ for $n \geq 2$, since $k \geq 5$ and $Q = \prod_{i=1}^{n} p_i \geq 3(7) > 4$ for $n \geq 2$ ([15]).

([15]) One may in fact, for each successive $n \geq 2$, take the simultaneous system

$$t \equiv 0 \left(\bmod 8 \prod_{i=1}^{n} p_i^2\right), \quad t \equiv 27 \pmod{81}, \quad t < k^{\prod_{i=1}^{n} p_i}.$$

It can then be shown in the same way that for each n, the set of solutions to the system satisfying Theorem 3 [still, of course, under the assumption that $p_n \parallel k^{\prod_{i=1}^{n-1} p_i} + 1$ for each successive $n \geq 1$]; as n increases, the number of integers in each corresponding set (of solutions to the above system for n) increases with enormous rapidity though the "density" of the set decreases, since the modulus involved increases with n (so that the integers satisfying Theorem 3 still do not have "positive density"). There can be some

Next assume [in (1)] the other alternative—that there exists some $g \geq 1$ such that $p_n \parallel k^{\prod_{i=1}^{n-1} p_i} + 1$ for each successive positive $n < g$, but for $n = g$,

$$p_g^2 \mid k^{\prod_{i=1}^{g-1} p_i} + 1, \tag{3}$$

where if $g = 1$, $\prod_{i=1}^{g-1} p_i$ is taken to be 1.

Then take the simultaneous congruence system (call it S)

$$t \equiv 0 \left(\mathrm{mod}\ 8 \prod_{i=1}^{g-1} p_i^2\right), \qquad t \equiv p_g \ (\mathrm{mod}\ p_g^2)$$

From the Chinese Remainder Theorem, there is an infinity (in fact an A.P.) of positive integers t satisfying S. Then for each (odd) $a-b$, *either* $p_r \nmid a-b$ for some r, $1 \leq r \leq g$, and the smallest such $r < g$, in which case, for that (smallest) r, $p_r \parallel t-k^a-k^b$ by the relevant part of the same argument as used for the first alternative in (1); *or* $p_r \nmid a-b$ for some $r \leq g$ and the smallest such $r = g$, in which case from (3), $p_g^2 \mid k^{\prod_{i=1}^{g-1} p_i} + 1 | k^{a-b} + 1 | k^a + k^b$ so that, with $p_g \parallel t$ in S above, one has $p_g \parallel t - k^a - k^b$; *or* finally $\prod_{i=1}^{g} p_i \mid a-b$, in which case [remembering (3) and the first result referred to in footnote 14] one now has $p_g^3 \mid k^{\prod_{i=1}^{g} p_i} + 1 \mid k^{a-b} + 1 \mid k^a + k^b$ so that, with $p_g \parallel t$ in S, it again follows that $p_g \parallel t - k^a - k^b$. Thus $t - k^a - k^b \neq M^2 + N^2$ for (a, b of opposite parity and hence for) $a, b \geq 0$. Finally, if $t = 24 \prod_{i=1}^{n} p_i^2$, $n \geq 2$ [corresponding to (2), the first alternative in (1)], either $3 \parallel t$ or $3^3 \parallel t$ so that $t \neq M^2 + N^2$; while if t satisfies system S [corresponding to (3), the other alternative in (1)], $p_g \parallel t$, so that again $t \neq M^2 + N^2$.

Thus corresponding to either alternative in (1), the theorem follows. ∎

It remains to consider the other values of k (> 1) not already dealt with in the previous theorems. One can show that for each of these values of k, there is an infinity (and even a positive density of integers) not representable ([16]) as $M^2+N^2+k^a+k^b$ or as $M^2+N^2+k^a$ or as M^2+N^2. And since M^2+N^2 may be odd or even with virtually equal frequency, the question of parity, i.e. representing just odd integers or representing just even integers has only very secondary importance. Still, in this section, some distinction will be made, even for values of k in earlier theorems. And, as already said, the existence of "positive density" will be investigated for all values of k not

"overlap" between sets for successive n, though this is easily dealt with. I have an aesthetic preference in the present proof to use just $t = 24 \prod_{i=1}^{n} p_i^2$ as above and thus relegating the system in this footnote to passing mention and not actually using it in the proof of Theorem 3. But I do feel a mention is called for.

([16]) For brevity, the relevant integers will be said to be not representable "as above" (for $a, b \geq 0$ or for $a, b \geq 1$ as the case may be). When the integers not so representable are expressed explicitly in terms of k, these integers are of course understood not to be so representable for that k (as in the case of Theorems 2 and 3).

covered by the previous theorems; furthermore, it will be brought up for some of the values of k in earlier theorems. The proofs are, for most part, just indicated.

- If $k \equiv 0$ or $4 \pmod 8$, take $t \equiv 3 \pmod 4$. From the relevant residues—those of t, k^a, $k^b \pmod 4$—it follows that each such t cannot be represented as above (for $a, b \geq 1$). Also, if $k \equiv 0 \pmod 8$, from the relevant residues $(\mathrm{mod}\, 8)$, it follows that all $t \equiv 6 \pmod 8$ cannot be represented as above $(a, b \geq 1)$.
- If $k \equiv 1 \pmod 8$, take $t \equiv 24 \pmod{72}$ [which $\equiv 0 \pmod 8$ of course]. From the relevant residues (mod 8) and from $3 \parallel t$, it follows that every such t cannot be represented as above $(a, b \geq 0)$.
- If $k \equiv 3$, 6 or $7 \pmod 8$, take $t \equiv 2k + k^3 \pmod{k^4}$. Then $k \parallel t - k^a - k^b$ if $a, b \geq 1$, unless $a = b = 1$, in which case $k^3 \parallel t - k^a - k^b$. Also $k \parallel t - k^a$ if $a \geq 1$. And $k \parallel t$. [Note that if $k \equiv 6 \pmod 8$, then $k = 2(4L + 3)$.] Thus, all such t cannot be represented as above $(a, b \geq 1)$ for the k in question. Consider further $k \equiv 6 \pmod 8$; then $t \equiv 2k + k^3 \pmod{k^4}$ implies $t \equiv 0 \pmod 4$. Take (without loss of generality) $a \geq b$; then if $a \geq 2$, $b = 0$, one has $t - k^a - k^b \equiv 3 \pmod 4$ while if $a = 0$, $t - k^a \equiv 3 \pmod 4$. Thus if $k \equiv 6 \pmod 8$, t cannot be represented as above if $a, b \geq 0$ unless $a = 0$ or 1, $b = 0$. It is then easily shown that if $k \equiv 6 \pmod 8$, "almost all" $t \equiv 2k + k^3 \pmod{k^4}$ cannot be represented as above if $a, b \geq 0$. (Here and in what follows, it would be straightforward to replace each "almost all" in the constructed A.P. by *all* the integers in an A.P. with a larger common difference [or modulus, in congruence terms]).

Collecting all results arrived at so far, it is thus the case that for each $k \geq 2$, there is an infinity of positive integers not representable as above [for $a, b \geq 0$ unless $k \equiv 3 \pmod 4$, in which case for $a, b \geq 1$]—the primary goal of this paper—[and a "positive density" of such non-representable integers for $k = 0$, 1, 3, 4, 6 or $7 \pmod 8$].

Now consider $k \equiv 0$ or $4 \pmod 8$ [$k \equiv 0 \pmod 4$], in which case $k \equiv 4I \pmod{64}$, I assuming every non-negative integer ≤ 15. Then using residues (mod 64), it can be shown straightforwardly that if $k \equiv M \pmod{64}$, then "almost all" $t \equiv M' \pmod{64}$ cannot be represented as above $(a, b \geq 0)$ if for $M = 0$, 4, 12, 16, 32, 36 or 48, $M' = 60$; if for $M = 8$, $M' = 56$; if for $M = 20$, 28 or 52, $M' = 12$; if for $M = 24$ or 56, $M' = 48$; if for $M = 40$, $M' = 24$; if for $M = 44$, $M' = 28$; if for $M = 60$, $M' = 44$—[the "almost all" comes from one or more of the cases (depending on M) $a = b = 0$, $a = b = 1$, $a = 2, b = 1$ (equivalent to $a = 1$, $b = 2$)]. These results ([17]), together with

([17]) To be sure, for $k \equiv 0 \pmod 8$, the even integers $t \equiv 6 \pmod 8$ cannot be represented as above $(a, b \geq 1)$, as already pointed out. However, for the even integers t

some previous ones in this paper, show that for each $k \geq 2$, there is an infinity of *even* integers not representable as above for either $a, b \geq 0$ if $k \not\equiv 3 \pmod 4$, or if $k \equiv 3 \pmod 4$, for $a, b \geq 1$ [and for $k = 0$, 1, 3, 4, 6 or 7 (mod 8) a "positive density" of *even* integers not representable as above—and more will be said later about the "positive density" of *even* integers not representable as above for some special cases of $k \equiv 2$ or 5 (mod 8)]. And for each $k \equiv 0$, 3, 4 or 7 (mod 8), it has been shown that there is an infinity (and also a "positive density") of *odd* integers not representable as above ($a, b \geq 1$). And for each $k \equiv 6 \pmod 8$, taking $t \equiv 2k + k^3 \pmod{k^4/16}$ and simultaneously $t \equiv 7 \pmod 8$, it can be shown straightforwardly that "almost all" such (odd) t cannot be represented as above for $a, b \geq 0$ [in a manner similar to that for $k \equiv 6 \pmod 8$ above—remembering that $k^4/16 = (k/2)^4$ where $k/2 \equiv 3 \pmod 4$, and that $k/2 \parallel t - k^a - k^b$ for $a, b \geq 1$, unless $a = b = 1$ in which case $(k/2)^3 \parallel t - k^a - k^b$, and also remembering that $k/2 \parallel t - k^a$, $a \geq 1$, and that $k/2 \parallel t$. Also using residues (mod 8), one can deal with a or $b = 0$]; thus there is an infinity (and also a "positive density") of *odd* integers not representable as above ($a, b \geq 0$). And if $k \equiv 1 \pmod 8$ and also $\equiv 1 \pmod{16}$, then using the relevant residues (mod 16), it can be shown very straightforwardly that "almost all" $t \equiv 13 \pmod{16}$ cannot be represented as above ($a, b \geq 0$), i.e. there is also an infinity (and "positive density") of *odd* integers not representable as above [for $k \equiv 1 \pmod{16}$].

Next, consider those $k \equiv 1 \pmod 8$ and also $\equiv 9 \pmod{16}$. While there is a large subset of such k for each of which it is possible to show an infinity of *odd* integers not representable as above (though some of these k are more easily dealt with than others—see "more accessible" values of k, below), there still remains an infinity of $k \equiv 9 \pmod{16}$ for each of which it is not possible at present to show an infinity of odd numbers not representable as above.

Next, consider $k \equiv 2$ or 5 (mod 8). Apart from "more accessible" values of k (to be elucidated below) for which it is straightforward to show an infinity of positive *odd* integers not representable as above—while it still seems most likely that for each ("less accessible" and hence each) value of $k \equiv 2$ or 5 (mod 8) there is an infinity of odd integers not representable as above (indeed there are some suggestive heuristic arguments), actual proofs again seem out of reach at present for at least most "less accessible" k.

However, as regards the especially interesting case of $k = 2$, the following might be worth noting. It is indeed possible to generate lengthy finite sequences of positive *odd* integers not representable as above ($a, b \geq 0$). If

just shown not to be representable as above for $k \equiv 0 \pmod 8$, $a, b \geq 1$ may be replaced by $a, b \geq 0$, not a significant extension, but one that might just as well be made since $k \equiv 4 \pmod 8$ can be handled along with $k \equiv 0 \pmod 8$ and cannot be handled—as regards *even* integers not representable as above—in a simpler way.

one considers the (positive) integers $t \equiv 15 \pmod{16}$, the only way (apart from a small number of exceptional values of a and b easily dealt with) that t might be represented as $M^2 + N^2 + 2^a + 2^b$ (taking $a \leq b$ without loss of generality) is if $a = 1$ [whereas for $t \equiv 28 \pmod{32}$ in Theorem 1 above, one has to deal with both $a = 1$ and $a = 3$ simultaneously—the so-called *principal cases* (see above)]. Thus, generating finite blocks of integers for which $t \equiv 15 \pmod{16}$ is not representable as above is far easier than for $t \equiv 28 \pmod{32}$ [which has been done in Theorem 1 above]. However, in dealing with odd integers, there is probably no equivalent to Lemma 1 above, and without that, generating an infinity of odd integers not representable as above seems completely out of reach at present.

Among "more accessible" values of $k \equiv 2$ or $5 \pmod 8$ and $k \equiv 9 \pmod{16}$—as far as an infinity of *odd* integers not representable as above—are those k for which there is a prime $P \equiv 3 \pmod 4$ such that $P \mid k$, and also those k (whether or not there is such a prime $P \mid k$) for which there is a prime $P \equiv 3 \pmod 4$ such that $P^2 \mid k - 1$; while for $k \equiv 9 \pmod{16}$, those values of k for which there is a prime $P \equiv 3 \pmod 4$ such that $P^2 \mid k + 1$ are *also* "more accessible" (so that for $k \equiv 9 \pmod{16}$, those k for which there is a prime $P \equiv 3 \pmod 4$ such that $P^2 \mid k^2 - 1$ are among those "more accessible"). And for all these "more accessible" values of k, it is straightforward enough to show that there is not only an infinity but also a "positive density" of odd integers not representable as above.

It might be added that while it has already been shown that for each $k \equiv 2 \pmod 8$ there is an infinity of *even* integers not representable as above, in fact for each of the same "more accessible" values (already given in the previous paragraph) of $k \equiv 2 \pmod 8$ pertaining to non-representable *odd* integers, it can also be shown that the *even* integers not representable as above have "positive density". And for $k \equiv 5 \pmod 8$, while for every such k it has been shown that there is an infinity of *even* integers not representable as above, the "more accessible" values of k—as far as non-representable even integers are concerned—are those for which there is a prime $P \equiv 3 \pmod 4$ such that $P \mid k$ and also those k for which there is a prime $P \equiv 3 \pmod 4$ such that $P^2 \mid k^2 - 1$; for each of these "more accessible" values of k, the even integers not representable as above can in fact be shown—and in a straightforward enough manner—to have "positive density". And for each of those k to which (3) for some $g \geq 1$ applies in the latter part of the proof of Theorem 3, it is shown (in that proof) that the even integers not representable as above have "positive density" [though those k to which (3) for $g = 1$ applies are already handled by the "more accessible" values of k just given for $k \equiv 5 \pmod 8$].

Positive integers not representable as the sum of two squares and (at most) one power of k will now be further discussed.

The results above for the non-representability of positive integers show, of course, *a fortiori* that—first, for each $k \geq 2$, there is an infinity (and for some of these k, a "positive density") of positive integers not representable as $M^2 + N^2 + k^a$ or as $M^2 + N^2$; second, for each $k \geq 2$, there is an infinity (and for some of these k a "positive density") of positive *even* integers not so representable; third, that for each $k \equiv 0$, 3, 4, 6 or 7 (mod 8) and for each $k \equiv 1$ (mod 16), there is an infinity (and also a "positive density") of positive *odd* integers not so representable. Furthermore, that for each $k \equiv 1$ (mod 8) [which of course includes $k \equiv 1$ (mod 16) just above] there is an infinity (and also a "positive density") of positive odd integers not so representable follows by letting $b = 0$ in the first [$t \equiv 24$ (mod 72)] of the above results for $k \equiv 1$ (mod 8). Finally, that for each $k \equiv 2$ or 5 (mod 8) there is an infinity (and for some of these k, a "positive density") of positive odd integers not so representable follows by letting $b = 0$ in Theorems 1, 2 and 3 respectively. Thus for each $k \geq 2$, one has an infinity (and for some of these k, a "positive density") of positive odd integers not representable as $M^2 + N^2 + k^a$ or as $M^2 + N^2$.

However, in light of considerations of independence of proof and, in some cases, simplicity of proof, or the existence of a "positive density", or even the existence of a greater "positive density" than would be obtainable from above, or (least significantly) allowing for all $k \geq 2$ the inclusion of $a = 0$, the following will be listed and can be proved straightforwardly along lines used above (concerning non-representability as the sum of two squares and two [or fewer] powers of k) for $k \equiv 0$, 1, 3, 4, 6 or 7 (mod 8) or for "more accessible" $k \equiv 2$ or 5 (mod 8).

For each $k \geq 2$, there are the following infinite classes, or class, of integers t not representable as $M^2 + N^2 + k^a$, $a \geq 0$, or as $M^2 + N^2$.

- If $k \equiv 0$, 2, 4 or 6 (mod 8), i.e. if k is even, "almost all" integers $t \equiv 6$ (mod 8); if $k \equiv 2$ or 6 (mod 8), "almost all" integers $t \equiv 3$ (mod 4), while if $k \equiv 0$ or 4 (mod 8), all $t \equiv 7$ (mod 8).
- If $k \equiv 1$ (mod 8), all $t \equiv 24$ (mod 72) and all $t \equiv 23$ (mod 24).
- If $k \equiv 3$ or 7 (mod 8), "almost all" $t \equiv 2k + 2k^2$ (mod $8k^2$) [t then being even] and "almost all" $t \equiv 2k + k^2$ (mod $8k^2$) [t then being odd].
- If $k \equiv 5$ (mod 8), all $t \equiv 24$ (mod 72).

All these classes of t have "positive density" of course.

- Finally, if $k \equiv 5$ (mod 8), the infinity of odd positive integers $t - k^b$ for any *fixed* b (such that $t - k^b > 0$; included are each of the infinite classes $t - 1$, $t - k$) where the odd integers t satisfy Theorem 3 above. While for the "more accessible" (as defined earlier) $k \equiv 5$ (mod 8) and for those $k \equiv 5$ (mod 8) to which (3) for $g > 1$ applies in the latter part of the proof of Theorem 3 [those $k \equiv 5$ (mod 8) to which (3)

for $g = 1$ applies are already dealt with by those "more accessible" values of k] the non-representable odd t can be shown to have "positive density", there is an infinity of $k \equiv 5 \pmod 8$ [e.g. 5, 13, 29, 61] for which "positive density" of non-representable odd integers is an open question. Indeed, it is only for the non-representability of *odd* integers for each k from this infinite subset of $k \equiv 5 \pmod 8$ that there are any values of k for which the existence of "positive density" of t is unknown and indeed suspect.

Briefest note on other additive problems. It might be worth noting that there is an infinity of positive integers not representable as the sum of two squares and two fourth powers, namely, those integers $23(16^a)$, for all $a \geq 0$. Furthermore, these integers are not representable as the sum of a square and six fourth powers.

The proofs parallel and are almost identical to the well-known proof that the integers $79 \cdot 16^a$, $a \geq 0$, are not the sum of fifteen fourth powers and hence they need not be written out here.

It may be worthwhile to distinguish additive problems (those involving representations of all integers, or predesignated subsets of them, by sums) by the number of different *types* of summands involved in the problem in question. First, there are those problems involving just one kind of summand—where the summands are all primes or all squares or all cubes etc. Among these problems are the Goldbach problems involving only prime summands, the Waring problem (including the case of squares of course), and the Waring–Goldbach problem. Then there are those problems involving two types of summand—such as the "almost" Goldbach problem, or (those integers representable by) the sum of a prime and a kth power ($k \geq 2$), or the sum of two squares and a kth power, or the sum of a prime and two squares, or the sum of a prime and two powers of k ($k \geq 2$), or the problems dealt with in the present paper. Obviously there are problems involving three or more types of summand such as (those integers representable as) the sum of a prime, a square and a cube or the sum of a prime, a square, and a biquadrate ([18]). It seems clear that the problems involving just one kind of summand are generally regarded to be of the greatest interest, while those involving just two kinds come next, and those involving three kinds next etc. [The only exception might be the problem of representing integers $z_1^2 + z_2^3 + \cdots + z_{k-1}^k$, $k \geq 4$, where the summands have an obvious relation to each other through the powers $2, 3, \ldots, k$ being consecutive.]

Postscript. As pointed out at the beginning of this article, the main problem treated here is suggested by that of representing (positive) integers

([18]) In the context of this classification two summands are considered different types, even if one is a proper subset of the other, such as squares and biquadrates.

(odd or even as the case may be) as the sum of a prime and a fixed maximum number of powers of (fixed) $k \geq 2$, the replacement of a prime summand by the sum of two squares being not uncommon. In particular, Theorem 1 of the present paper corresponds to an analogous result concerning odd integers not representable as the sum of a prime and two (or fewer) powers of 2; the latter result has been arrived at in a paper of mine on which I would like to close by making a few comments.

1. It has been shown in [3] that there is an infinity of distinct positive odd integers not representable as $p + 2^a + 2^b$ (nor as $p + 2^a$). I would like to refute the claim made by P. X. Gallagher at the end of his paper [6] that according to De Polignac [7], Euler had shown this result concerning $p + 2^a + 2^b$ by using a different method—indeed, Gallagher's claim in [6] is totally inaccurate. I have read De Polignac's article [7]—he makes no mention of Euler ever having solved, or even having considered, this problem. In fact, neither Euler, to the best of my knowledge, nor De Polignac ever refers in any way to the problem of the representation of positive odd numbers as $p + 2^a + 2^b$. Furthermore, De Polignac does *not* even credit Euler with having solved—and neither Euler nor De Polignac ever did solve—the much less difficult (though still non-trivial) problem of proving that there is an infinity of positive odd numbers not representable as $p + 2^a$ (a result first proved in [4] and then by a different method in [2]). All that Euler managed to do, according to De Polignac, was to find *just one number* (959) not representable as $p + 2^a$, thus in effect (to De Polignac's obvious chagrin!) disproving De Polignac's conjecture that *every* odd number ≥ 3 is representable as $p + 2^a$.

2. [3] gives a link between the size of the factors of infinitely many Fermat numbers and the number—call it $N(x)$—of positive odd integers $\leq x$ representable as $p + 2^a + 2^b$. If one can establish, for all sufficiently large x (or even for every x in a set consisting of an infinity, no matter how "thin", of the integers $2^{2^n} - 1$) a sufficiently strong—stronger than at present but possibly attainable—lower bound for $N(x)$, then lower bounds for the smallest factors of infinitely many Fermat numbers can be arrived at—through [3]—which are far better than any known at present.

3. In light of the well-known history of results showing the unreliability of numerical evidence suggesting the contrary to these results, it might be interesting to search for the smallest (non-trivial) positive odd integer not representable as the sum of a prime and (at most) two powers of 2. Regardless of the numerical choices that can be made in [3], the positive odd integers not so representable which are generated by the method of [3] are in fact enormous; if there are smaller ones, trial and error (using a fast computer) would probably be the way to carry out the suggested search. Perhaps such a number (or if it cannot be found, a lower bound for it)

would be large enough to again emphasize how unreliable and misleading numerical evidence can be (or in the present instance could have been) concerning number-theoretic results (after all, if positive integers up to e.g. 10^{15} are representable as the sum of a prime and [at most] two powers of 2, one could certainly be misled into suspecting the contrary to what has in fact been proven in [3]).

4. I used the nomenclature "overlapping" congruence system where terms like "superabundant" (congruence system) or "covering" system are frequently used. I did so because of the way the term in Hungarian in [5] was originally translated for me by a professional translator. Personally, I prefer the term "all-inclusive" although I have never seen this term actually used for such systems. For the purpose of showing that there is an infinity of (positive) odd integers not representable as $p + 2^a$, the one such "overlapping" (or "all-inclusive") congruence system used for this purpose in [9] and [10] is 0 (mod 2), 0 (mod 3), 1 (mod 4), 3 (mod 8), 7 (mod 12), 23 (mod 24) [this system is based on the one in [4] with the same moduli]; it has as few congruences as any system used for the above problem for $p + 2^a$ can have.

5. In the numerical "overlapping" system (1) on page 106 of [3], I noticed long ago that the congruence 37 (mod 120) is redundant in that the previous congruences [in system (1)] 13 (mod 48) and 37 (mod 48) absorb it completely. Thus either the modulus 120 can be omitted completely *or* one can replace the final congruence [in system (1)] 229 (mod 360) by 229 (mod 120) or equivalently 109 (mod 120); in either case the number of congruences in (1) can be reduced by one. I have also found a third possibility—replacing 37 (mod 120) by 73 (mod 120) at the same time replacing 229 (mod 360) by—and strengthening it to—49 (mod 180) while keeping the other two congruences (mod 180) already in (1); the two congruences (mod 144) can then be eliminated, reducing the number of congruences in (1) by two. The modulus 180 can be used three times since there are three distinct primes p_i such that 2 belongs to 180 (mod p_i). Of course in a system of twenty-eight congruences, a reduction to twenty-seven or twenty-six is really insignificant and in constructing (1) originally, I made no attempt to find the very shortest such system. Indeed, in contrast to many "overlapping" congruence systems, the number of congruences in (1) must be comparatively large due to the condition that $(2^{2^n} - 1, p_i) = 1$ (see page 105 of [3]), a condition originally (to the best of my knowledge) introduced—in connection with "overlapping" congruence systems—in [3]. This condition prevents certain small moduli (most significantly 2, 4, 8) being used in (1), thus considerably increasing the number of (moduli and) congruences needed there.

6. When at the very beginning of [3] I point out that it has been shown by different methods that there is an infinity of positive odd integers not

representable as $p+2^a$, there are, to the best of my knowledge, just two such genuinely different methods, the first in [5] and the second in [2]. The first of these methods is also found in [4] (which actually was written earlier), quoted more often than [5], presumably because it is in English rather than Hungarian; however it does have a lacuna (filled in in [5]) and is also presented in a very condensed form—hence my preference for [5] over [4]. And, as should be completely obvious in the course of reading [3], it is this method in [5] slightly modified as in [9] that I have discussed on page 103 and at the very top of page 104 in [3]—with due acknowledgement there of [5] and [9], [9] being referred to as [4] in [3]—and to which I have referred when saying "the method used in [4]..." (on page 103 of [3]) and "the method of [4]" (on page 104 of [3]—see second footnote there). I should point out here that [9] has been more recently reproduced in [10].

7. For the reason expressed in footnote 2 in the present paper, Theorem I in [3] deals with positive odd integers not representable as $p+2^a+2^b$ (even if 1 is counted as a prime), $a, b > 0$. Just for absolute completeness I shall mention the following. These same integers constructed to prove Theorem I in [3] are also not representable as $p+2^a$, $a > 0$ [of course non-representability as $p+2^a+2^b$, $a, b \geq 1$, implies non-representability as $p+2^a$, $a \geq 2$, but the latter result in slightly stronger form (non-representability as $p+2^a$, $a \geq 1$) is actually used in [3]—as I explicitly made clear there, giving appropriate references—as one of the significant ingredients of the proof of Theorem I]. It follows that Theorem I holds with a or b also allowed to be 0. Indeed, the case of $a = b = 0$ is immediately seen to be equivalent to non-representability as $p + 2^a$, $a = 1$ (as suggested by footnote 4 of [3]), while $a > 0$, $b = 0$ can be trivially shown to demand representability as $p + 2^a$, $p = 3$, $a \geq 1$ (contradicting the above)—so that the integers constructed to prove Theorem I in [3] are not representable as $p + 2^a + 2^b$, $a, b \geq 0$. And being odd and > 3, they are also not representable as $p + 2^a$, $a = 0$. Also they are composite, this fact being made obvious in the course of the proof of Theorem I (of [3]) itself (however, since being a prime does not in itself represent a sum, I did not feel the need to explicitly state their compositeness). Thus the integers generated to prove Theorem I of [3] cannot be represented as $p+2^a+2^b$, nor as $p+2^a$ (nor as p), $a, b \geq 0$. Hence, no matter what the reader's viewpoint regarding footnote 2 in the present paper or anything else in that direction, every possibility is dealt with.

8. In the second line of footnote 1 on page 104 of [3], page reference [4, p. 413] should read [4, p. 414].

9. The article [2] occurs (as noted in the reference) on pages 316, 344. The continuation of page 316 on page 344 is just that; it is *not* an *erratum* or postscript. Since I was not sent a proof to read before publication, I did not

know in advance that the editors were planning to do this rather unusual page separation and hence could not object. Finally, there is a reference at the beginning of [2] to "existing proofs of this theorem"; both proofs (referred to as [4] and [5] in the present article) use the same method—see comment 6 above.

REFERENCES

[1] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman and S. S. Wagstaff, *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, 2nd ed., Contemp. Math. 22, Amer. Math. Soc., 1988.

[2] R. Crocker, *A theorem concerning prime numbers*, Math. Mag. 34 (1960/61), 316 and 344; MR 25#2994.

[3] —, *On the sum of a prime and of two powers of two*, Pacific J. Math. 36 (1971), 103–107; MR 43#3200.

[4] P. Erdős, *On integers of the form $2^r + p$ and some related problems*, Summa Brasil. Math. 2 (1947–51), 113–123; MR 13,437.

[5] —, *On a problem concerning congruence systems*, Mat. Lapok 3 (1952), 122–128 (in Hungarian); MR 17,14.

[6] P. X. Gallagher, *Primes and powers of 2*, Invent. Math. 29 (1975), 125–142.

[7] A. de Polignac, *Recherches nouvelles sur les nombres premiers*, C. R. Acad. Sci. Paris 29 (1849), 397–401, 738–739.

[8] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.

[9] W. Sierpiński, *Elementary Theory of Numbers*, PWN, Warszawa, 1964.

[10] —, *Elementary Theory of Numbers*, 2nd ed., edited by A. Schinzel, PWN, Warszawa, 1988.

[11] S. S. Wagstaff, *Divisors of Mersenne numbers*, Math. Comp. 40 (1983), 385–397.

6 Carlton Mansions
14 Holland Park Gardens
London W14 8DW, UK

Received 23 October 2006 (4807)