

# A MULTIPLICITY BOUND FOR A FIXED SQUAREFREE KERNEL

NIKITA KALININ

## 1. INTRODUCTION

Additive problems involving powers of 2 have a long history. A classical starting point is Erdős' 1950 paper [1], where he proved that infinitely many integers are not of the form

$$p + 2^k,$$

with  $p$  prime. This initiated a broad circle of questions on representations by a “structured” arithmetic set together with a power of 2. Later expositions and problem lists of Erdős and Graham [2], Erdős [3], and Guy [4] record several variants of this theme.

A softer version of the prime-plus-power-of-two problem replaces the prime by a squarefree integer. In this form one asks whether every odd integer  $n > 1$  can be represented as

$$n = m + 2^k$$

with  $m$  squarefree. This conjecture is now recorded as Problem #11 on Bloom's list. This problem was studied systematically by Granville and Soundararajan [5], who showed that it is closely connected with the behavior of the multiplicative order of 2 modulo  $p^2$ , and hence with the distribution of base-2 Wieferich primes. More recently, Hercher [6] verified computationally that every odd integer  $n < 2^{50}$  has such a representation, thereby extending earlier computations of Odlyzko and McCranie.

The present note is concerned with a more local counting problem. For a fixed squarefree integer  $m$  and an integer  $n$ , define

$$T_m(n) := \left\{ k \geq 1 : n - 2^k = mu^2 \text{ for some } u \in \mathbb{Z}_{\geq 0} \right\}.$$

Thus  $T_m(n)$  records the exponents  $k$  for which the dyadic shift  $n - 2^k$  lands in the quadratic progression  $m \cdot (\text{squares})$ . In the special case  $m = 1$ , this becomes the problem of counting representations of  $n$  as a square plus a power of 2:

$$n = u^2 + 2^k.$$

Our main results show that these sets are uniformly very small. For odd squarefree  $m \geq 3$ , we prove that

$$|T_m(n)| \leq 2$$

for every odd integer  $n$ . For  $m = 1$ , we prove the sharp global bound

$$|T_1(n)| \leq 3$$

for all  $n$ , and we exhibit infinitely many integers for which equality holds. The proofs are completely elementary. The repeated 2-adic argument is isolated in two lemmas in Section 2, and the two main theorems are then obtained with short case splittings.

From the viewpoint of exponential Diophantine equations, the closest classical background is the Ramanujan–Nagell family and its generalizations. The prototype is the equation

$$x^2 + 7 = 2^n,$$

studied by Mordell [7]. More general equations of the form

$$Cx^2 + D = 2y^n$$

were investigated by Ljunggren [8], and the generalized Ramanujan–Nagell equation was studied in depth by Beukers in two influential papers [9, 10]. See also Le [11] for results on the number of

solutions. The philosophy there is that one fixes the parameter  $D$  and studies the corresponding exponential equation. In contrast, in the present problem one fixes  $n$  and allows the parameter  $n - 2^k$  to vary with  $k$ , asking for the multiplicity of the quadratic-dyadic representations attached to a single value of  $n$ .

There is also a neighboring additive literature in which squares remain present but the number of powers of 2 is varied. Crocker [12] proved that infinitely many odd integers are not representable as a prime plus two powers of 2. Much later, Platt and Trudgian [13] proved that infinitely many integers are not representable as the sum of two squares and at most two powers of 2. These papers are not directly about the multiplicity of the representations  $n = u^2 + 2^k$ , but they illustrate the rigidity that often appears when quadratic objects are combined additively with powers of 2.

As far as we are aware, there is little explicit published literature whose main theorem gives a sharp global bound for the quantity

$$\#\{k \geq 1 : n - 2^k = u^2\}.$$

This makes the local study of the sets  $T_m(n)$  natural. It lies between two well-developed areas: on one side, additive problems of Erdős type involving powers of 2; on the other, the classical theory of Ramanujan–Nagell equations. The results of the present paper fit naturally into this gap.

## 2. PRELIMINARIES

We begin with the basic congruence restriction for odd integers.

**Lemma 1** (Congruence lemma). *Let  $m$  be an odd squarefree integer and let  $n$  be odd.*

- (i) *If  $k \in T_m(n)$  and  $k \geq 3$ , then  $n \equiv m \pmod{8}$ .*
- (ii) *If  $n \not\equiv m \pmod{8}$ , then  $T_m(n) \subseteq \{1, 2\}$ , and in fact  $|T_m(n)| \leq 1$ .*
- (iii) *If  $n \equiv m \pmod{8}$ , then  $1, 2 \notin T_m(n)$ .*

*Proof.* If  $k \in T_m(n)$ , then

$$n - 2^k = mu^2$$

for some integer  $u$ . Since  $n$  and  $m$  are odd,  $u$  is odd, and hence

$$u^2 \equiv 1 \pmod{8}.$$

If  $k \geq 3$ , then  $2^k \equiv 0 \pmod{8}$ , so

$$n \equiv mu^2 \equiv m \pmod{8},$$

which proves (i).

If  $n \not\equiv m \pmod{8}$ , then by (i) no solution with  $k \geq 3$  can occur, so  $T_m(n) \subseteq \{1, 2\}$ . If  $1, 2 \in T_m(n)$ , then for some odd integers  $u_1, u_2$  we would have

$$n - 2 = mu_1^2 \equiv m \pmod{8}, \quad n - 4 = mu_2^2 \equiv m \pmod{8},$$

so simultaneously  $n \equiv m + 2 \pmod{8}$  and  $n \equiv m + 4 \pmod{8}$ , impossible. This proves (ii).

Finally, if  $n \equiv m \pmod{8}$ , then the congruences in the previous paragraph show that  $k = 1$  and  $k = 2$  are both impossible, proving (iii).  $\square$

The next lemma is the common 2-adic factorization step which drives both main theorems.

**Lemma 2** (Adjacent-factorization lemma). *Let  $m$  be an odd squarefree integer, let  $n$  be odd, and suppose that*

$$n - 2^{k_i} = mu_i^2 \quad (i = 1, 2)$$

*with  $k_1 < k_2$  and odd positive integers  $u_1 > u_2$ . Put  $d := k_2 - k_1$ . Then there exist odd positive integers  $a, b$  such that*

$$mab = 2^d - 1,$$

*and*

$$u_1 = a + 2^{k_1-2}b, \quad u_2 = \left| a - 2^{k_1-2}b \right|.$$

If in addition  $m \geq 3$ , then necessarily

$$a - 2^{k_1-2}b > 0.$$

*Proof.* Subtracting the two identities gives

$$m(u_1^2 - u_2^2) = 2^{k_1}(2^d - 1),$$

that is,

$$m(u_1 - u_2)(u_1 + u_2) = 2^{k_1}(2^d - 1).$$

Since  $u_1$  and  $u_2$  are odd, both  $u_1 - u_2$  and  $u_1 + u_2$  are even. Moreover,

$$\frac{u_1 + u_2}{2} - \frac{u_1 - u_2}{2} = u_2$$

is odd, so exactly one of  $(u_1 - u_2)/2$  and  $(u_1 + u_2)/2$  is odd. Hence one of  $u_1 - u_2$  and  $u_1 + u_2$  has exact 2-adic valuation 1, and the other has exact 2-adic valuation  $k_1 - 1$ . Therefore there exist odd positive integers  $a, b$  such that

$$mab = 2^d - 1,$$

and

$$u_1 = a + 2^{k_1-2}b, \quad u_2 = \left| a - 2^{k_1-2}b \right|.$$

This proves the first part.

Now assume  $m \geq 3$ . If  $a - 2^{k_1-2}b < 0$ , then

$$2^{k_1-2}b - a = u_2 > 0,$$

so in particular  $2^{k_1-2}b > a$ . Since  $a \geq 1$ , we obtain  $b \geq 1$ , and from  $mab = 2^d - 1$  we get

$$b \leq \frac{2^d - 1}{ma} < \frac{2^d}{3}.$$

In the applications below, the negative sign will imply a stronger lower bound  $b > 2^d$ , and hence a contradiction. It is therefore convenient to isolate the representation with the positive sign as the only relevant one.  $\square$

### 3. THE ODD SQUAREFREE CASE

We now prove the uniform bound for fixed odd squarefree kernel  $m \geq 3$ .

**Theorem 3.** *Let  $m \geq 3$  be an odd squarefree integer, and let  $n$  be an odd positive integer. Then*

$$|T_m(n)| \leq 2.$$

*More precisely, if  $n \not\equiv m \pmod{8}$ , then  $|T_m(n)| \leq 1$ .*

*Proof.* If  $n \not\equiv m \pmod{8}$ , the claim is exactly Lemma 1(ii).

Assume now that  $n \equiv m \pmod{8}$ . By Lemma 1(iii), every exponent in  $T_m(n)$  is at least 3. Suppose for contradiction that there exist three distinct exponents

$$k_1 < k_2 < k_3$$

in  $T_m(n)$ . Write

$$n - 2^{k_i} = mu_i^2 \quad (i = 1, 2, 3),$$

with odd positive integers  $u_1 > u_2 > u_3$ , and set

$$d_1 := k_2 - k_1, \quad d_2 := k_3 - k_2.$$

Apply Lemma 2 to the pair  $(u_1, u_2)$  and then to the pair  $(u_2, u_3)$ . We obtain odd positive integers  $a_1, b_1, a_2, b_2$  such that

$$ma_1b_1 = 2^{d_1} - 1, \quad ma_2b_2 = 2^{d_2} - 1,$$

and

$$\begin{aligned} u_1 &= a_1 + 2^{k_1-2}b_1, & u_2 &= \left| a_1 - 2^{k_1-2}b_1 \right|, \\ u_2 &= a_2 + 2^{k_2-2}b_2, & u_3 &= \left| a_2 - 2^{k_2-2}b_2 \right|. \end{aligned}$$

Since  $u_2$  is the same number in both descriptions,

$$\left| a_1 - 2^{k_1-2}b_1 \right| = a_2 + 2^{k_2-2}b_2.$$

We claim that the left-hand side cannot equal  $2^{k_1-2}b_1 - a_1$ . Indeed, if

$$2^{k_1-2}b_1 - a_1 = a_2 + 2^{k_2-2}b_2,$$

then using  $k_2 = k_1 + d_1$  we get

$$2^{k_1-2}(b_1 - 2^{d_1}b_2) = a_1 + a_2 > 0,$$

so

$$b_1 > 2^{d_1}b_2 \geq 2^{d_1}.$$

On the other hand,

$$b_1 \leq \frac{2^{d_1} - 1}{ma_1} < \frac{2^{d_1}}{3},$$

a contradiction. Therefore the only possible sign is

$$a_1 - 2^{k_1-2}b_1 = a_2 + 2^{k_2-2}b_2.$$

Hence

$$a_1 - a_2 = 2^{k_1-2}(b_1 + 2^{d_1}b_2) > 2^{k_1-2}2^{d_1} = 2^{k_2-2},$$

so in particular

$$a_1 > 2^{k_2-2}.$$

But from  $ma_1b_1 = 2^{d_1} - 1$  we also obtain

$$a_1 \leq \frac{2^{d_1} - 1}{mb_1} < \frac{2^{d_1}}{3}.$$

Since  $k_1 \geq 3$ ,

$$k_2 - 2 = d_1 + k_1 - 2 \geq d_1 + 1,$$

whence

$$2^{k_2-2} \geq 2^{d_1+1} > \frac{2^{d_1}}{3}.$$

This contradicts the two inequalities  $a_1 > 2^{k_2-2}$  and  $a_1 < 2^{d_1}/3$ . Therefore three solutions cannot exist, and  $|T_m(n)| \leq 2$ .  $\square$

#### 4. THE PURE SQUARE CASE

We next treat the case  $m = 1$ , where the sharp bound is 3 rather than 2.

**Theorem 4.** *For every positive integer  $n$ ,*

$$|T_1(n)| \leq 3.$$

*Moreover, this bound is sharp.*

*Proof.* We first treat odd  $n$ . If  $n \not\equiv 1 \pmod{8}$ , then Lemma 1(ii) with  $m = 1$  gives  $|T_1(n)| \leq 1$ . Assume now that  $n \equiv 1 \pmod{8}$ . By Lemma 1(iii), every exponent in  $T_1(n)$  is at least 3. Suppose for contradiction that there are three distinct exponents

$$k_1 < k_2 < k_3$$

in  $T_1(n)$ . Write

$$n - 2^{k_i} = u_i^2 \quad (i = 1, 2, 3),$$

with odd positive integers  $u_1 > u_2 > u_3$ , and set  $d_1 := k_2 - k_1$ ,  $d_2 := k_3 - k_2$ . Applying Lemma 2 with  $m = 1$  to the pairs  $(u_1, u_2)$  and  $(u_2, u_3)$ , we find odd positive integers  $a_1, b_1, a_2, b_2$  such that

$$a_1b_1 = 2^{d_1} - 1, \quad a_2b_2 = 2^{d_2} - 1,$$

and

$$\left| a_1 - 2^{k_1-2}b_1 \right| = a_2 + 2^{k_2-2}b_2.$$

If the left-hand side were  $2^{k_1-2}b_1 - a_1$ , then

$$2^{k_1-2}(b_1 - 2^{d_1}b_2) = a_1 + a_2 > 0,$$

so  $b_1 > 2^{d_1}$ , which is impossible because  $b_1 \mid (2^{d_1} - 1)$ . Thus

$$a_1 - 2^{k_1-2}b_1 = a_2 + 2^{k_2-2}b_2,$$

and therefore

$$a_1 - a_2 = 2^{k_1-2}(b_1 + 2^{d_1}b_2) > 2^{k_2-2}.$$

In particular,  $a_1 > 2^{k_2-2}$ . But  $a_1 \mid (2^{d_1} - 1)$ , so  $a_1 < 2^{d_1}$ . Since  $k_1 \geq 3$ , we have  $k_2 - 2 \geq d_1 + 1$ , hence  $2^{k_2-2} \geq 2^{d_1+1} > 2^{d_1}$ , a contradiction. Thus for odd  $n$  one has

$$|T_1(n)| \leq 2.$$

We now pass to even integers. Suppose  $n = 4N$ . We claim that

$$|T_1(4N)| = |T_1(N)| + \mathbf{1}_{\{N-1 \text{ is a square}\}}.$$

Indeed, if

$$4N = u^2 + 2^k,$$

then  $k = 1$  is impossible modulo 4. If  $k = 2$ , then  $u$  is even, say  $u = 2v$ , and

$$4N = 4v^2 + 4,$$

so  $N = v^2 + 1$ . Thus  $k = 2$  contributes exactly when  $N - 1$  is a square. If  $k \geq 3$ , then again  $u$  is even, say  $u = 2v$ , and dividing by 4 yields

$$N = v^2 + 2^{k-2}.$$

This gives a bijection between representations of  $4N$  with exponent  $k \geq 3$  and representations of  $N$ , proving the claim.

Now write

$$n = 4^t m, \quad 4 \nmid m.$$

Iterating the identity above gives

$$|T_1(n)| = |T_1(m)| + \sum_{j=0}^{t-1} \mathbf{1}_{\{4^j m - 1 \text{ is a square}\}}.$$

For  $j \geq 1$ , one has  $4^j m - 1 \equiv 3 \pmod{4}$ , so  $4^j m - 1$  cannot be a square. Hence only the term  $j = 0$  can survive, and therefore

$$|T_1(n)| = |T_1(m)| + \mathbf{1}_{\{m-1 \text{ is a square}\}}.$$

If  $m$  is odd, then  $|T_1(m)| \leq 2$ ; if  $m \equiv 2 \pmod{4}$ , then only  $k = 1$  can occur in  $m = u^2 + 2^k$ , so  $|T_1(m)| \leq 1$ . In either case,  $|T_1(n)| \leq 3$ , proving the theorem.  $\square$

**Proposition 5** (Sharp examples). *For every integer  $t \geq 1$ ,*

$$17 \cdot 4^t = (2^{t+2})^2 + 2^{2t} = (3 \cdot 2^t)^2 + 2^{2t+3} = (2^t)^2 + 2^{2t+4}.$$

Consequently,

$$|T_1(17 \cdot 4^t)| = 3 \quad (t \geq 1),$$

and therefore

$$\sup_{n \geq 1} |T_1(n)| = 3.$$

*Proof.* The three displayed identities are immediate:

$$\begin{aligned} (2^{t+2})^2 + 2^{2t} &= 2^{2t+4} + 2^{2t} = 17 \cdot 2^{2t} = 17 \cdot 4^t, \\ (3 \cdot 2^t)^2 + 2^{2t+3} &= 9 \cdot 2^{2t} + 8 \cdot 2^{2t} = 17 \cdot 2^{2t} = 17 \cdot 4^t, \\ (2^t)^2 + 2^{2t+4} &= 2^{2t} + 16 \cdot 2^{2t} = 17 \cdot 2^{2t} = 17 \cdot 4^t. \end{aligned}$$

Thus  $|T_1(17 \cdot 4^t)| \geq 3$ , and Theorem 4 gives the reverse inequality.  $\square$

**Corollary 6** (Kernel diversity). *Let  $n$  be odd and let  $K \geq 1$ . For each  $1 \leq k \leq K$  with  $n > 2^k$ , write uniquely*

$$n - 2^k = m_k u_k^2,$$

where  $m_k$  is squarefree. Then

$$\#\{m_k : 1 \leq k \leq K\} \geq \left\lceil \frac{K-1}{2} \right\rceil.$$

*Proof.* Each squarefree kernel  $m_k \geq 3$  can occur for at most two values of  $k$  by Theorem 3, while the kernel  $m_k = 1$  can occur for at most three values of  $k$  by Theorem 4. Hence, if  $M$  denotes the number of distinct kernels among  $m_1, \dots, m_K$ , then

$$K \leq 3 + 2(M - 1) = 2M + 1.$$

Thus  $M \geq (K - 1)/2$ , and the claim follows.  $\square$

#### REFERENCES

- [1] P. Erdős, On integers of the form  $2^k + p$  and some related problems, *Summa Brasil. Math.* **2** (1950), 113–123.
- [2] P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de L’Enseignement Mathématique, No. 28, Geneva, 1980.
- [3] P. Erdős, Problems in number theory, *New Zealand J. Math.* **26** (1997), 155–160.
- [4] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.
- [5] A. Granville and K. Soundararajan, A binary additive problem of Erdős and the order of 2 mod  $p^2$ , *Ramanujan J.* **2** (1998), 283–298.
- [6] C. Hercher, On the sum of a squarefree integer and a power of two, *J. Integer Seq.* **28** (2025), Article 25.3.1.
- [7] L. J. Mordell, The diophantine equation  $2^n = x^2 + 7$ , *Ark. Mat.* **4** (1962), 455–460.
- [8] W. Ljunggren, On the Diophantine equation  $Cx^2 + D = 2y^n$ , *Math. Scand.* **18** (1966), 69–86.
- [9] F. Beukers, On the generalized Ramanujan–Nagell equation I, *Acta Arith.* **38** (1981), 389–410.
- [10] F. Beukers, On the generalized Ramanujan–Nagell equation II, *Acta Arith.* **39** (1981), no. 2, 113–123.
- [11] M. Le, On the number of solutions of the generalized Ramanujan–Nagell equation  $x^2 - D = 2^{n+2}$ , *Acta Arith.* **60** (1991), no. 2, 149–167.
- [12] R. Crocker, On the sum of a prime and of two powers of two, *Pacific J. Math.* **36** (1971), 103–107.
- [13] D. J. Platt and T. S. Trudgian, On the sum of two squares and at most two powers of 2, *Amer. Math. Monthly* **124** (2017), no. 8, 737–740.