# THE NUMBER OF REPRESENTATIONS OF $n$ OF THE FORM $n = x^2 - 2^y$, $x > 0$, $y \ge 0$

RICHARD J. MATHAR

Abstract. We count solutions to the Ramanujan-Nagell equation $2^y + n = x^2$ for fixed positive $n$.

The computational strategy is to count the solutions separately for even and odd exponents $y$, and to handle the odd case with modular residues for most cases of $n$.

## 1. Scope

We consider the number of ways to represent $n > 0$ as

$$n = x^2 - 2^y, \tag{1}$$

for pairs of the non-negative unknowns $x$ and $y$. Equivalently we count the $y$ such that

$$n + 2^y = x^2 \tag{2}$$

are perfect squares.

**Remark 1.** *For $n = 0$ the number of solutions is infinite because each even value of $y$ creates one solution.*

The $n$ for which the count is nonzero end up in [8, A051204].

**Remark 2.** *Negative $n$ for which solutions exists are listed in* [8, A051213] [4, 2].

The solutions are counted separately for even $y$ and odd $y$ and added up. The total count is at most 4 [6].

## 2. Even Exponents $y$

Counting the squares $x^2$ of the format (2) considering only even $y$ is basically a matter of considering the values $y = 0, 2, 4, \ldots$ in turn and checking explicitly each $y^2 + n$ against being a square. An upper limit to the $y$ is determined as follows:

- The $y$-values in the range $2^y < n$ are all checked individually.
- For larger $y$ the values of $2^y + n$ on the left hand side of (2) are represented in binary by some most significant bit contributed by $2^y$ and—after a train of zero bits depending of how much larger $2^y$ is than $n$—the trailing bits of $n$. A lower exact bound of the $x$ on the right hand side is $x = 2^{y/2}$, contributing to the count if $n$ were zero. So the next higher candidate on the right hand side is $(x+1)^2 = (2^{y/2}+1)^2 = 2^y + 2^{1+y/2} + 1$. If this value is larger than the left hand side $2^y + n$, there are no further solutions because

*Date*: October 19, 2014.
*Key words and phrases.* Ramanujan-Nagell, Exponential Diophantine.

$n$ is so small that it falls into the gap between consecutive squares. In summary, the search range for this branch of the algorithm can be reduced to $2^{1+y/2}+1 \le n$.

The sequence of the number of representations of $n \ge 1$ with even $y$ (i.e., the number of representations $n = x^2 - 4^y$) is 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 2, 0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1,. . . .

The smallest $n$ which has $r$ representations of the form $n = x^2 - 4^y$ is the greedy inverse of this sequence, which is $n = 1$ for $r = 0$, $n = 3$ for $r = 1$, $n = 33$ for $r = 2$, $n = 105$ for $r = 3$ and $n = 1680$ for $r = 4$. There are no $n$ for $r \ge 5$ [6].

## 3. Odd Exponents $y$

The count of solutions to (2) with odd $y$ is split into cases (i) for $n$ being multiples of 4, (ii) $n$ represented by at least one modulus $m$ such that an upper limit of $y$ is found by considering the equation modulo $m$, and (iii) other (discriminants) $n$ that apparently do not fall into these categories.

### 3.1. $n$ which are multiples of 4.

If $4 \mid n$ in (2) for odd $y = 2y_o + 1$, the left hand side is even, so the right hand side and $x = 2x_e$ must also be even. Then considering the equation modulo 4, the case $y_o = 0$ cannot yield a solution, and one may divide each term of the equation by 4. This reduces recursively the number of solutions to the number of solutions for $n/4$.

### 3.2. $n$ with associated moduli.

The sequences $2^y + n = 2^{2y_e+1} + n$ ($y_e = 0, 1, 2, \ldots$) and $x^2$ ($x = 0, 1, 2, \ldots$) on both sides of (2) have generating functions which are rational functions and therefore have Pisano periods if read reduced some modulus $m$ [7, 10, 11].

**Remark 3.** *For the sequence $x^2$ [8, A000290] the length of the Pisano periods is tabulated in [8, A186646] as a function of $m$. For polynomial sequences like $x^2$, the period length is obviously limited to $m$ and always a divisor of $m$. Discarding duplicates in the period, the number of squares modulo $m$ is also finite [8, A000224].*

**Remark 4.** *If 2 and $m$ are coprime, the length of the Pisano period of $2^y$ is the multiplicative order of $2 \pmod m$ [8, A002326].*

The sequences $2^y + n \pmod m$ generally start with a transient list of moduli at small $y$ before entering the period.

**Example 1.** *The sequence $2^y \pmod{68}$ reads 1, 2, 4, 8, 16, 32, 64, 60, 52, 36, 4, 8, 16, 32, 64, 60, 52, . . . for $y \ge 0$ with a transient part containing 1 and 2 and a periodic part containing 4, 8, 16, 32, 64, 60, 52, 36.*

The computational strategy is to find a modulus $m$ given $n$ such that the two periods of $2^{2y_e+1} + n \pmod m$ and of $x^2 \pmod m$ have no common element. If such a modulus $m$ is found, the length of the transient part of the $2^y + n$ residua defines the maximum exponent $y$ that needs to be searched, because for all larger $y$ the moduli of both sides of (2) are distinct.

**Remark 5.** *There is no transient part in the residua of the polynomials like $x^2$.*

Cases of a search for $m$ for some small $n$ are illustrated in Table 1. Only successful $m$ are listed, as indicated by distinct sets of moduli in the penultimate and ultimate column in the table. Cases where $n$ is a multiple of 4 are left out because the reduction of Section 3.1 makes them uninteresting.

**Remark 6.** *Chosing $m = 3$ works if $3 \mid n$ because $2^y \pmod 3 = 1, 2, \ldots$ $(y \ge 0)$ and because $x^2 \pmod 3 = 0, 1, 1, \ldots$, $(x \ge 0)$ both periodically repeated. Since we are considering only odd $y$, the set of residua contains $\{2\}$ for $2^y$ and $\{0, 1\}$ for $x^2$, and these do not intersect.*

The cases of odd $n$ which are not in the table are apparently not accessible by the method of residue and are discussed in Section 3.3.

Note that a shortcut exists for $n$ which are two times an odd number, $n = 2n_o$. Then $2^y + n = 2^{2y_o+1} + 2n_o = x^2$ requires $x$ to be even, $x = 2x_e$, so $2^{2y_o+1} + 2n_o = 4x_e^2$ and $2^{2y_o} + n_o = 2x_e^2$. Since the right hand side is even, the left hand side is even which requires $2^{2y_o}$ to be odd and $y_o = 0$ or no solution at all. This is decided by direct inspection. (See [8, A056220] for the $n_o$ that do have a solution.)

3.3. **Other $n$.** For $n = 1, 17, 41, 49, 73, 89, \ldots$ no such modulus $m$ has been found that separates the residue sets of $2^y + n$ and $x^2$. These $n$ are discussed individually [9]:

- For $n = 1$ only the solution with $y = x = 3$ exists [1].
- For $n = 17$ the maximum number of 4 solutions [5, 9] is known, represented by $(x, y) = (5, 3), (7, 5), (9, 6)$ and $(23, 9)$. (One of these is created by an even $y$ and already counted in Section 2.)
- For $n = 41$ we have $(x, y) = (7, 3)$ or $(13, 7)$. Because 41 is in [8, A031396], the associated equation $u^2 - 41v^2 = -1$ has solutions (explicit $u = 32$ in [8, A249021]). and according to Le's second theorem [5] there are no more than 2 solutions.
- For $n = 49$ we have $(x, y) = (9, 5)$. This is the only solution. [Proof: Solving $2^y + 49 = x^2$ for $y \ge 1$ needs odd $x$ by considering the parity of both sides. So this is $2^y = (x + 7)(x - 7)$ where $x \pm 7$ are both even. Furthermore comparison of the prime factorization of both sides enforces that $x \pm 7$ are powers of 2, say $x - 7 = 2^\alpha$, $x + 7 = 2^{\alpha+\delta}$. Subtraction of both equations gives $14 = 2^\alpha(2^\delta - 1) = 2 \cdot 7$. Necessarily $\alpha = 1$, $\beta = 3$ and finally $x = 9$. See [3].]
- For $n = 73$ we have $(x, y) = (9, 3)$. This is the only solution [9]
- For $n = 89$ we have $(x, y) = (11, 5)$ or $(91, 13)$. Again 89 is in [8, A031396] and these are all solutions according to Le's second theorem [5].
- For $n = 97$ we have $(x, y) = (15, 7)$ as the only solution [9].
- For $n = 113$ we have $(x, y) = (11, 3)$ or $(25, 9)$. Again 113 is in [8, A031396] and these are all solutions according to Le's second theorem [5].
- For $n = 161$ the maximum number of 4 solutions [5] is known, represented by $(x, y) = (13, 3), (15, 6), (17, 7)$ and $(47, 11)$. (One of these is created by an even $y$ and already counted in Section 2.)
- For $n = 833$ the maximum number of 4 solutions [5] is known, represented by $(x, y) = (29, 3), (31, 7), (33, 8)$ and $(95, 13)$. (One of these is created by an even $y$ and already counted in Section 2.)

TABLE 1. Examples of the dividing property of moduli $m$ for small $n$, odd $y$. The double column entitled $2^y+n$ shows the transient values of $2^y+n \pmod m$ and the values of $2^y+n \pmod m$ in the period. The column entitled $x^2$ shows the period of $x^2 \pmod m$ (of length $m$, not necessarily reduced to the smallest subperiod).

| $n$ | $m$ | $\pi(2^y+n)$ | | $\pi(x^2)$ |
|---|---|---|---|---|
| 2 | 4 | 0 | 2 | 0 1 0 1 |
| 3 | 3 | | 2 | 0 1 1 |
| 5 | 5 | | 2 3 | 0 1 4 4 1 |
| 6 | 3 | | 2 | 0 1 1 |
| 7 | 4 | 1 | 3 | 0 1 0 1 |
| 9 | 3 | | 2 | 0 1 1 |
| 10 | 4 | 0 | 2 | 0 1 0 1 |
| 11 | 4 | 1 | 3 | 0 1 0 1 |
| 13 | 8 | 7 | 5 | 0 1 4 1 0 1 4 1 |
| 14 | 4 | 0 | 2 | 0 1 0 1 |
| 15 | 3 | | 2 | 0 1 1 |
| 18 | 3 | | 2 | 0 1 1 |
| 19 | 4 | 1 | 3 | 0 1 0 1 |
| 21 | 3 | | 2 | 0 1 1 |
| 22 | 4 | 0 | 2 | 0 1 0 1 |
| 23 | 4 | 1 | 3 | 0 1 0 1 |
| 25 | 5 | | 2 3 | 0 1 4 4 1 |
| 26 | 4 | 0 | 2 | 0 1 0 1 |
| 27 | 3 | | 2 | 0 1 1 |
| 29 | 8 | 7 | 5 | 0 1 4 1 0 1 4 1 |
| 30 | 3 | | 2 | 0 1 1 |
| 31 | 4 | 1 | 3 | 0 1 0 1 |
| 33 | 3 | | 2 | 0 1 1 |
| 34 | 4 | 0 | 2 | 0 1 0 1 |
| 35 | 4 | 1 | 3 | 0 1 0 1 |
| 37 | 8 | 7 | 5 | 0 1 4 1 0 1 4 1 |
| 38 | 4 | 0 | 2 | 0 1 0 1 |
| 39 | 3 | | 2 | 0 1 1 |
| 42 | 3 | | 2 | 0 1 1 |
| 43 | 4 | 1 | 3 | 0 1 0 1 |
| 45 | 3 | | 2 | 0 1 1 |
| 46 | 4 | 0 | 2 | 0 1 0 1 |
| 47 | 4 | 1 | 3 | 0 1 0 1 |
| 50 | 4 | 0 | 2 | 0 1 0 1 |
| 51 | 3 | | 2 | 0 1 1 |
| 53 | 8 | 7 | 5 | 0 1 4 1 0 1 4 1 |
| 54 | 3 | | 2 | 0 1 1 |
| 55 | 4 | 1 | 3 | 0 1 0 1 |
| 57 | 3 | | 2 | 0 1 1 |
| 58 | 4 | 0 | 2 | 0 1 0 1 |
| 59 | 4 | 1 | 3 | 0 1 0 1 |
| 61 | 8 | 7 | 5 | 0 1 4 1 0 1 4 1 |
| 62 | 4 | 0 | 2 | 0 1 0 1 |
| 63 | 3 | | 2 | 0 1 1 |
| 65 | 5 | | 2 3 | 0 1 4 4 1 |
| 66 | 3 | | 2 | 0 1 1 |
| 67 | 4 | 1 | 3 | 0 1 0 1 |
| 69 | 3 | | 2 | 0 1 1 |

## References


1. K. Chao, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$*, Sci. Sinica (Notes) **14** (1964), 457–460.
2. J. H. E. Cohn, *The diophantine equation $x^2+c = y^n$*, Acta Arithm. **65** (1993), no. 4, 367–381. MR 1259344
3. ———, *The diophantine equation $x^2 + 2^k = y^n$, ii*, Int. J. Math. Math. Sci. **22** (1999), no. 3, 459–462.
4. Hemar Godinho, Diego Marques, and Alain Togbé, *On the diophantine equation $x^2 = 2^\alpha 5^\beta 17^\gamma = y^n$*, Commun. Math. **20** (2012), no. 2, 81–88. MR 3032806
5. Maohua Le, *On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - d = 2^{n+2}$*, Acta Arithm. **60** (1991), no. 2, 149–167. MR 1139052
6. ———, *A note on the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - d = k^n$*, Acta Arithm. **78** (1996), no. 1, 11–18. MR 1424998
7. D. W. Robinson, *A note on linear reccurent sequences modulo $m$*, Am. Math. Monthly **73** (1966), no. 6, 619–621. MR 0201376
8. Neil J. A. Sloane, *The On-Line Encyclopedia Of Integer Sequences*, Notices Am. Math. Soc. **50** (2003), no. 8, 912–915, http://oeis.org/. MR 1992789 (2004f:11151)
9. Nicholas Tzanakis, *On the diophantine equation $y^2 - d = 2^k$*, J. Number Theory **17** (1983), no. 2, 144–164.
10. Morgan Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Am. Math. Soc. **33** (1931), no. 1, 153–165. MR 1501582
11. ———, *The arithmetical theory of linear recurring series*, Trans. Am. Math. Soc. **35** (1933), no. 3, 600–628. MR 1501705


*URL*: `http://www.mpia.de/~mathar`

Max-Planck Institute of Astronomy, Königstuhl 17, 69117 Heidelberg, Germany