Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2025, Volume 31, Number 3, 460–470
DOI: 10.7546/nntdm.2025.31.3.460-470

Solution of an odds inversion problem

Robert K. Moniot

Department of Computer and Information Science, Fordham University
113 W. 60th St, New York, NY 10023, USA
e-mail: moniot@fordham.edu

Received: 26 November 2024 **Revised:** 1 August 2025
Accepted: 2 August 2025 **Online First:** 4 August 2025

Abstract: Consider the problem of determining the possible numbers of balls of two different colors in an urn such that if two are drawn out at random, the odds that they are different colors are a given value. We present a general solution of this problem for all odds from nil to certainty. The solution methods use relatively simple concepts from number theory such as modular inverses and the Pell equation. We find upper bounds on the number of solutions and the magnitude of solutions for those cases that have at most a finite number of solutions. We also define solution classes for cases that have an infinite number of solutions, and identify cases having a determinate number of solution classes.

Keywords: Pell equation, Modular inverses, Combinatorial probability, Quadratic Diophantine equations, Linear congruences, Odds inversion.
2020 Mathematics Subject Classification: 11A07, 11D09, 11D45, 60C05.

1 Introduction

Suppose an urn contains red and blue balls, and we would like to find the numbers of balls of each color such that if two balls are drawn out, the probability that they are different colors is any chosen value between 0 and 1. This problem, which is a generalization of a *Varsity Math* problem from the U.S. National Museum of Mathematics [6], was treated in some detail in [4]. It has a number of interesting features. For instance, if the probability is $\frac{1}{2}$, the solutions are pairs of successive triangular numbers. If the probability is less than $\frac{1}{2}$, then in most cases there is an infinite number of solutions, and solutions for a given probability (though not necessarily all solutions) can be found using the Pell equation. For a probability greater than $\frac{1}{2}$, the number of solutions is finite and may be zero. That case was studied by [1], who found conditions for the existence of solutions in some cases and characterized several families of solutions.

The seemingly closely related problem where the first ball is replaced before drawing the second was solved in [2]. Perhaps surprisingly, probabilities greater than $\frac{1}{2}$ cannot be achieved in that case.

In this paper we solve the problem for all rational probabilities from 0 to 1 and find upper bounds on the number and magnitude of possible solutions for those cases that have at most a finite number of solutions. Some of this material was treated in [4] and [1], but neither of those articles presented complete solutions except for some special cases.

2 Preliminaries

If we denote by x and y the numbers of red and blue balls, respectively, in an urn, then if we draw out two balls, the probability that they are different colors is

$$P(x,y)=\frac{2xy}{(x+y)(x+y-1)}. \tag{1}$$

If we require $P(x,y)$ to equal some desired value $\frac{p}{q}$ where p,q are relatively prime natural numbers, then the odds-inversion problem is to find all values of (x,y) that yield that value.

Provided there are at least 2 balls in the urn, setting $P(x,y)=\frac{p}{q}$ we can rearrange (1) as the Diophantine equation

$$px^2-2(q-p)xy+py^2-px-py=0. \tag{2}$$

Since (2) is symmetrical in x and y, we adopt the convention $x\le y$ to have distinct solutions. In order for the solution to represent at least 2 balls in the urn, we require $x\ge 0$, $y\ge 0$, and $x+y\ge 2$ for a solution to be admissible. Note that there are always 3 solutions of (2) that do not correspond to at least 2 balls in the urn, but that will play a role in solving the equation. They are $(x,y)\in\{(0,0),(0,1),(1,0)\}$. We will call these the *trivial solutions.*

The equation simplifies if we make the following change of variables:

$$t=x+y,\quad v=y-x. \tag{3}$$

Since we keep $x\le y$, we require $v\ge 0$ for distinct solutions, and $t>1$ for admissible solutions. Note that x and y are integer if and only if t and v are integer and of the same parity.

In terms of (t,v), (2) becomes

$$(q-2p)t^2+2pt-qv^2=0. \tag{4}$$

If $\frac{p}{q}=\frac{1}{2}$, the coefficient of t^2 vanishes. That case will be solved separately. Otherwise, $q-2p\neq 0$, and we can remove the linear term by completing the square. Let

$$u=(q-2p)t+p. \tag{5}$$

Then in terms of (u,v), (4) becomes

$$u^2 - Dv^2 = p^2 \tag{6}$$

where

$$D = q(q-2p). \tag{7}$$

If $D > 0$, which occurs for $\frac{p}{q} < \frac{1}{2}$, (6) describes a hyperbola; if $D < 0$, $\frac{p}{q} > \frac{1}{2}$ and it describes an ellipse. Since the changes of variables are linear, the shapes of (2) and (4) are the same class of conic section as (6). If $D = 0$, then $\frac{p}{q} = \frac{1}{2}$, which invalidates (6). In this case, (2) or (4) is a parabola.

We will deal with each of these three categories of solutions in turn.

3 Parabolic case

This case is the original *Varsity Math* problem, which can be solved using only simple algebra. The solution is given in [4], but we repeat it here since the proof is brief.

Theorem 3.1. *If* $P(x,y) = \frac{1}{2}$*, then the number of solutions is infinite, and all of the admissible solutions of* (2) *are pairs of successive triangular numbers.*

Proof. If $\frac{p}{q} = \frac{1}{2}$, then (4) becomes

$$t = v^2. \tag{8}$$

Solving back for x and y, for any integer value of v we find

$$x = \frac{t-v}{2} = \frac{v(v-1)}{2}, \quad y = \frac{t+v}{2} = \frac{v(v+1)}{2}.$$

If $v > 1$, these are pairs of successive triangular numbers. There is an infinite number of solutions. □

4 Elliptical case

This case was solved in [1] for the special class of probabilities of the form $\frac{m}{2m-1}$. Here we solve it for all probabilities in the elliptical regime.

We can write probabilities greater than $\frac{1}{2}$ in the form $P(x,y) = \frac{m}{2m-n}$, where $m, n \in \mathbb{Z}^+$. To have this in lowest terms, we require $\gcd(m,n) = 1$. We exclude the probability $P(x,y) = 1$ because it is an exception to some general statements we will be making. It has the single admissible solution $(x,y) = (1,1)$. Therefore, we require $m > 1$ and $1 \leq n < m$ so that $\frac{1}{2} < P(x,y) < 1$.

Setting $p = m$ and $q = 2m - n$ in (4) and solving for v^2,

$$v^2 = \frac{t(2m-nt)}{2m-n}. \tag{9}$$

Now, $v^2 \geq 0$ requires $t \leq \frac{2m}{n}$. Equality only occurs when $n = 1$, for which the solutions $(x,y) = (m,m)$ and $(m-1,m)$ always exist [1]. Following [1], we call these *balanced solutions.*

(The other possibility, namely $t = m$ when $n = 2$, is excluded, since in that case m must be odd, while $v = 0$ is even, giving fractional x, y.) Also, $x + y \geq 2$ implies $t > 1$. For imbalanced solutions, therefore, $1 < t < \frac{2m}{n}$, and in case $n = 1$, we have the stricter inequality $1 < t < 2m - 1$.

4.1 Solution

Since the two balanced solutions exist if and only if $n = 1$ and they are known, we now seek only imbalanced solutions.

Theorem 4.1. *If there are imbalanced solutions (t, v) giving $P(t, v) = \frac{m}{2m-n}$, where $m > 1$, $1 \leq n < m$, and $\gcd(m, n) = 1$, they are of the form*

$$t = aa', \quad v = \sqrt{a'(b'n \bmod a)}, \tag{10}$$

where a is a member of a pair of integers (a, b) such that $ab = 2m - n$ with $a > 1$, $b > 1$, and $\gcd(a, b) = 1$, and a' and b' are the least positive modular inverses of $a \pmod b$ and $b \pmod a$, respectively.

Proof. Let $w = v^2$. If (t, v) is a solution of (9), w is integer. Rewrite (9) as

$$(2m - n)w = t(2m - nt). \tag{11}$$

The right-hand side is a factorization of the left-hand side. Therefore, there must exist positive integers a, b, w_1, and w_2 such that $t = aw_1$ and $2m - nt = bw_2$, with $ab = 2m - n$ and $w_1w_2 = w$. Since $aw_1 = t \leq \frac{2m}{n} - 1 = \frac{2m-n}{n} = \frac{ab}{n}$, we have $w_1 \leq b/n$. We can turn this into a strict inequality, since for $n = 1$, we have $t < 2m - 1 = ab$ so $w_1 < b$, while for $n > 1$, $w_1 \leq \frac{b}{n} < b$. So we can write $0 < w_1 < b$. Similarly, since $t > 1$, $bw_2 = 2m - nt < 2m - n = ab$, so we have $0 < w_2 < a$.

By construction, $t \equiv 0 \pmod a$ and $2m - nt \equiv 0 \pmod b$. Now, $2m - n = ab \implies 2m - n \equiv 0 \pmod{ab} \implies 2m \equiv n \pmod{ab}$. This implies both $2m \equiv n \pmod a$ and $2m \equiv n \pmod b$. Then since $2m - nt \equiv 0 \pmod b \implies 2m \equiv nt \pmod b$, we have

$$2m \equiv n \pmod b \implies nt \equiv n \pmod b. \tag{12}$$

If $\gcd(n, b) = 1$, then a modular inverse of $n \pmod b$ exists, and the congruence (12) reduces to $t \equiv 1 \pmod b$. Since $t = aw_1$, w_1 must be a modular inverse of $a \pmod b$. In order for this modular inverse to exist, it is necessary that $a > 1$, $b > 1$, and $\gcd(a, b) = 1$. Since $0 < w_1 < b$, we denote this by $w_1 = a'$, the least positive modular inverse of $a \pmod b$.

If $n > 1$, it is possible to have $d = \gcd(n, b) > 1$. Since $2m - n = ab$, d must divide $2m$. It cannot divide m since $\gcd(m, n) = 1$, so $d = 2$. Thus in this case $nt \equiv n \pmod b$ has 2 solutions. If $t = aw_1$ is the solution satisfying $t \equiv 1 \pmod b$, then the second solution is $t \equiv (aw_1 + \frac{b}{2}) \pmod b$. But this solution cannot satisfy $t \equiv 0 \pmod a$. Therefore the only solution is $t = aa'$.

Now, from $2m \equiv n \pmod a$, we have $2m - nt \equiv n - nt \pmod a$. Then

$$t \equiv 0 \pmod a \implies bw_2 = 2m - nt \equiv n \pmod a. \tag{13}$$

Now, since we showed that $a > 1$, $b > 1$, and $\gcd(a, b) = 1$, a modular inverse of $b \pmod{a}$, which we denote by b', exists. Then the congruence (13) can be solved, giving $w_2 \equiv b'n \pmod{a}$. Above we showed $0 < w_2 < a$. Therefore we can set $w_2 = b'n \bmod a$ where b' is the least positive modular inverse of $b \pmod{a}$. Thus $v^2 = w = w_1 w_2 = a'(b'n \bmod a)$. In taking the square root, we use only the positive branch since $v \geq 0$ as noted above. Thus t, v are of the form (10). □

This theorem provides a method of solving (1), by testing all factorizations $ab = 2m - n$ satisfying the conditions of the theorem, rejecting any that do not yield $t = aa' < \frac{2m}{n}$ and $v^2 = a'(b'n \bmod a)$ a perfect square.

Corollary 4.1. *For the probability $P(x, y) = \dfrac{m}{2m - n}$, if $2m - n$ is a prime power, then there are no imbalanced solutions. If $n > 1$, then there are no solutions.*

Proof. If $2m - n$ is a prime power, it is not possible to find a factorization $ab = 2m - n$ with $a > 1$ and $b > 1$ and $\gcd(a, b) = 1$ to give a solution in the form (10). It is necessary for the prime factors of a and b to be in disjoint nonempty subsets of those of $2m - n$, which is not possible for a set of size 1. By Theorem 4.1, there can be no other imbalanced solutions. Therefore, there are no imbalanced solutions. Balanced solutions occur only for $n = 1$, so for $n > 1$ there are no solutions. □

4.2 Upper bound on number of solutions

Theorem 4.2. *The upper bound on the number of distinct admissible solutions (x, y) giving probability $P(x, y) = \frac{m}{2m-n}$ with $m > 1$, $1 \leq n < m$, and $\gcd(m, n) = 1$ is 2^k if $n = 1$ and $2^k - 2$ if $n > 1$, where $k = \omega(2m - n)$, the number of distinct prime factors of $2m - n$.*

Proof. If $2m-n$ is a prime power, for which $k = 1$, then by Corollary 4.1 there are no imbalanced solutions. If $n = 1$, there are always the two balanced solutions, so the number of solutions is 2, and the bound holds and is always met for this case. If $n > 1$, there are no solutions, so the bound of 0 holds as well.

Otherwise, $k > 1$. There are $2^k - 2$ distinct ways to partition the k prime power factors of $2m - 1$ into two products a and b satisfying the conditions $a > 1, b > 1$, and $\gcd(a, b) = 1$. (The number of subsets of k distinct primes is 2^k, but the two subsets giving either $a = 1$ or $b = 1$ are excluded.)

For each such pair (a, b), there is a solution (t, v) if and only if $t = aa' < \frac{2m}{n}$ and $v^2 = a'(b'n \bmod a)$ is a perfect square. (Note that the alternative solution in which a and b are swapped will appear in one of the other partitions of the set of k prime power factors.) We require $v \geq 0$, and $t = aa'$ is unique for a given (a, b), and so each pair (a, b) yields at most one solution (t, v), which yields at most one solution (x, y).

Therefore each of the $2^k - 2$ choices of (a, b) yields at most one imbalanced solution (x, y). Theorem 4.1 excludes any other imbalanced solutions than those of this form. If $n = 1$, there are also 2 balanced solutions. Including these gives the upper bound of 2^k for all solutions. If $n > 1$, there can be only the $2^k - 2$ imbalanced solutions. □

Note: With $n = 1$, this paper proves Conjectures 1 and 2 of [1]. It also generalizes them to include $n > 1$, i.e., to all probabilities greater than $\frac{1}{2}$. (Their Conjecture 2 needs to be slightly modified, as it includes the balanced solutions and allows $a = 1$ or $b = 1$. The balanced solutions do not result from any choices of (a, b) where $ab = 2m - 1$, and the factorizations with $a = 1$ or $b = 1$ do not yield admissible solutions. Theorem 4.1 is a corrected statement of Conjecture 2.)

4.2.1 Examples

When $n = 1$, the bound for $k > 1$ is achieved in some cases. Here are two examples:

- $P = \frac{8}{15}$, $k = 2$: 4 solutions $\{(2, 4), (4, 6), (7, 8), (8, 8)\}$.
- $P = \frac{1008}{2015}$, $k = 3$: 8 solutions $\{(72, 84), (315, 336), (392, 414), (594, 616), (672, 693), (924, 936), (1007, 1008), (1008, 1008)\}$.

For $n > 1$, a search determined that the bound for $k > 1$ is not achieved for any probabilities for which there is at least one solution having both x and y less than 1000. The search found 5 cases with 3 solutions (all having $k \geq 4$, so the bound is 14 or more), and none with more. This is not surprising considering that the maximum acceptable values of a' and b' are much smaller than those allowed when $n = 1$. The case with the smallest m is:

- $P = \frac{715}{1428}$ $(n = 2)$, $k = 4$: 3 solutions $\{(55, 65), (130, 143), (275, 286)\}$.

4.3 Upper bound on magnitude of solutions

Theorem 4.3. *If* $\frac{p}{q} > \frac{1}{2}$, *any admissible solutions of* (2) *obey*

$$t = x + y \leq \frac{2p}{2p - q}. \tag{14}$$

Proof. This follows immediately by requiring $v^2 \geq 0$ and $t > 0$ in (4). □

5 Hyperbolic case

For this case, where $\frac{p}{q} < \frac{1}{2}$ and $D > 0$, it is most convenient to work with (6). If $u < 0$, it yields negative x, y, so we seek only solutions where $u > 0$. We also require $v \geq 0$ to have $x \geq y$.

5.1 Case of D square

If D is square, then (6) factors:

$$(u - \sqrt{D}v)(u + \sqrt{D}v) = p^2. \tag{15}$$

This case was solved in [4]. The method of solution is to factor p^2 into a product of two of its divisors, say $d_1 d_2 = p^2$, equate $u - \sqrt{D}v = d_1$ and $u + \sqrt{D}v = d_2$, and solve these two linear equations for u and v. Solutions that do not yield integer x, y are rejected. It is clear that this method yields all solutions that exist.

5.1.1 Upper bound on number of solutions for D square

When D is square, the number of solutions is finite, since the number of ways to factor p^2 is finite.

Theorem 5.1. *The number of distinct admissible solutions of* (2) *when* $\frac{p}{q} < \frac{1}{2}$ *and* D *is square is less than or equal to* $\frac{k-3}{2}$ *where* k *is the number of divisors of* p^2.

Proof. According to (15), any solution of (6) must correspond to a factorization $d_1 d_2 = p^2$. Interchanging the factors d_1 and d_2 yields the same solution except changing the sign of v, so for distinct solutions one can require $d_1 \leq d_2$ which implies $d_1 \leq p$. Each of these solutions (u, v) yields at most one solution (x, y). Thus the number of distinct solutions of (2) is less than or equal to the number of divisors of p^2 that are less than or equal to p. Since p itself is always a divisor, and the other divisors occur in pairs d_1 and $\frac{p^2}{d_1}$, the number of divisors giving distinct solutions is $\frac{k+1}{2}$ where k is the number of divisors of p^2. This number includes the two trivial solutions having $v \geq 0$. Removing them gives the bound $\frac{k-3}{2}$. □

Note that this bound is 0 if p is prime.

5.1.2 Examples

A search of probability ratios $\frac{p}{q}$ with $q < 10^6$ having square D and a nonzero bound on the number of solutions found only 4 cases achieving the bound, which is 3 for all of those cases. The instance with the smallest p is:

- $P = \frac{323}{648}$, $\frac{k-3}{2} = 3$: 3 solutions $\{(570, 646), (646, 731), (12\,236, 13\,685)\}$.

5.1.3 Upper bound on magnitude of solutions for D square

Theorem 5.2. *If* $\frac{p}{q} < \frac{1}{2}$ *with* D *square, all positive solutions of* (2) *obey the bound*

$$t = x + y \leq \frac{(p-1)^2}{2(q-2p)}. \tag{16}$$

Proof. Setting $p^2 = d_1 d_2$ with $d_1 = d$ and $d_2 = \frac{p^2}{d}$ in (15) for some divisor d of p^2 and solving for u yields

$$u = \frac{p^2 + d^2}{2d} = \frac{1}{2}\left(\frac{p^2}{d} + d\right).$$

The extrema occur when $d = 1$ or $d = p^2$, giving the bound

$$u \leq \frac{1}{2}\left(p^2 + 1\right).$$

This gives

$$t = \frac{u - p}{q - 2p} \leq \frac{(p-1)^2}{2(q-2p)}.$$ □

5.2 Case of D nonsquare

We first show that an infinite number of admissible solutions of (2) can be found by solving the Pell equation. Next we examine the classes to which solutions can belong, and then proceed to a method for finding all solutions.

5.2.1 Infinite number of solutions

Theorem 5.3. *The Diophantine equation* (2) *has an infinite number of admissible solutions for any values of* p *and* q *such that* $D > 0$ *is nonsquare.*

Proof. Divide both sides of (6) by p^2. Then setting $r = \frac{u}{p}$ and $s = \frac{v}{p}$, we have

$$r^2 - Ds^2 = 1. \tag{17}$$

This is the well-known Pell equation, and for $D > 0$ nonsquare, it always has an infinite number of integer solutions.

Now, suppose (r, s) is the fundamental solution of (17), defined as the solution for which r and s are positive and minimal. It can be found, for instance, by the method of continued fractions. All positive solutions of (17) are then given by [3, §10.9]:

$$(r_n + s_n\sqrt{D}) = (r + s\sqrt{D})^n, \quad n \in \mathbb{N}. \tag{18}$$

From (18) and $(u, v) = (pr, ps)$, we have that if (u, v) is a solution of (6), and (r, s) is a solution of (17), then (u', v') satisfying

$$u' + v'\sqrt{D} = (u + v\sqrt{D})(r + s\sqrt{D}) \tag{19}$$

is also a solution. This leads to the recurrence

$$u_{n+1} = ru_n + Dsv_n, \quad v_{n+1} = su_n + rv_n. \tag{20}$$

Clearly, this generates positive solutions (u_n, v_n), which give positive values (x_n, y_n). But because the mapping from (u, v) to (x, y) involves division by $2(q - 2p)$, integer solutions (u, v) are not guaranteed to yield integer (x, y). However, in [4] it is shown that this recurrence yields integer (x, y) on at least every other iteration. Therefore the number of solutions to the odds inversion problem is infinite for all probabilities in the hyperbolic regime, except those for which D is square. □

5.2.2 Solution classes

Other solutions may exist that are not generated by applying the recurrence (20) to (pr, ps). Solutions can be grouped into classes based on whether they are related by (19) for some values of r, s that are a solution of (17). Solving (19) for r and s gives

$$r = \frac{uu' - Dvv'}{p^2}, \quad s = \frac{vu' - uv'}{p^2}. \tag{21}$$

Two solutions (u, v) and (u', v') are members of the same class if and only if these expressions for r and s are integer [5, §58].

Theorem 5.4. *When* $p = 1$*, with* $D > 0$ *non-square, all solutions of* (6) *belong to a single class. When* $p > 1$*, there are always at least three classes, namely those to which the trivial solutions belong.*

Proof. When $p = 1$ the expressions in (21) are always integer, so there is only one class, to which all solutions belong.

Now consider $p > 1$. The trivial solution $(x, y) = (0, 0)$ corresponds to $(u, v) = (p, 0)$. The other two trivial solutions $(x, y) = (0, 1)$ and $(1, 0)$ correspond to $(u, v) = (q - p, 1)$ and $(q-p, -1)$, respectively. Setting $(u, v) = (p, 0)$ and $(u', v') = (q-p, \pm 1)$ in (21) gives $s = \mp \frac{q-p}{p^2}$, which is fractional if $p > 1$ since p and q are relatively prime. Setting $(u, v) = (q - p, 1)$ and $(u', v') = (q - p, -1)$ gives $s = \frac{2(q-p)}{p^2}$, which is also fractional if $p > 1$. Thus no two of the trivial solutions are in the same class if $p > 1$. Since the trivial solutions always exist, these three classes of solutions always exist. □

If (u, v) is a solution of (6), then $(u, -v)$ is also a solution. We call the classes to which these two solutions belong *conjugate classes*. In most cases these classes are distinct, but in some cases (in particular, for our problem, when $v = 0$ or $p = 1$), they may be the same. We call those classes *ambiguous classes* [5, §58]. The fundamental solution of a class can be defined as the member of the class for which $v \geq 0$ is the least. If the class is not ambiguous, then u is also uniquely determined. If the class is ambiguous, then we remove the ambiguity by requiring $u > 0$. If K is a solution class, we will denote its conjugate class by $\overline{K}$.

In what follows, we will denote the solution class of the trivial solution $(u, v) = (p, 0)$ by K_0, the class of $(q - p, 1)$ by K_1, and that of $(q - p, -1)$ by $K_{-1} = \overline{K}_1$.

Let $a = q - p$. Require $a > p$ to have $D > 0$, and $\gcd(a, p) = 1$. Then $D = q(q - 2p) = (a + p)(a - p) = a^2 - p^2$ and (6) can be rewritten $u^2 - a^2v^2 = (1 - v^2)p^2$. Since all non-trivial solutions have $v^2 > 1$, we reverse the terms so both sides are positive, and write it in factored form:

$$(av - u)(av + u) = (v^2 - 1)p^2. \tag{22}$$

Observe that changing the sign of u or v yields the same equation. Changing one changes the solution to the conjugate class, while changing both keeps the solution in the same class.

Lemma 5.1. *If $av \pm u$ in* (22) *is divisible by p^2, then the solution (u, v) belongs to K_1 or K_{-1}.*

Proof. Suppose $av - u = np^2$, where n is an integer. Inserting that solution $(u, v) = (av - np^2, v)$ and the trivial solution $(u', v') = (a, 1)$ into (21) and simplifying gives $r = v - an$ and $s = n$. These are integer, showing that this solution is in class K_1. Changing the sign of u so that $av + u = np^2$ yields a solution in the conjugate class K_{-1}. □

Theorem 5.5. *If p is prime, then* (6) *has exactly 3 solution classes, namely K_0, K_1, and K_{-1}.*

Proof. First, consider solutions for which $\gcd(u, v) = 1$. Clearly, since $\gcd(a, p) = 1$, $av - u$ and $av + u$ cannot both be divisible by p. Therefore, if p is prime, the only possible partitioning of the left-hand side of (22) is for one of these terms to be a multiple of p^2 and the other not divisible by p. Hence by Lemma 5.1 the solution is a member of either K_1 or K_{-1}.

Now, if $\gcd(u, v) > 1$, for prime p the only possibility is $\gcd(u, v) = p$, which reduces (6) to the Pell equation. The fundamental solution gives $(u, v) = (pr, ps)$. This solution results from applying the recurrence (20) to $(p, 0)$, which belongs to K_0. □

5.2.3 Solution methods

The special cases $p = 1$ and $p = 2$ were treated in [4]. The smallest solutions of (2) are $(x, y) = (1, 2q - 1)$ and $(1, q - 1)$, respectively. All larger solutions can be found via the recurrence

$$x_{n+1} = y_n, \quad y_{n+1} = \frac{y_n(y_n - 1)}{x_n}, \quad n = 1, 2, \ldots \tag{23}$$

This allows one to avoid solving the Pell equation for these cases. For $p > 2$, we proceed by solving (6) and sifting for solutions that yield admissible (x, y).

If (u, v) is a fundamental solution of a class, then all solutions of the class are given by (19) as r and s run over all solutions of (17), including $(r, s) = (\pm 1, 0)$ [5, §58]. Equivalently, one can use the recurrence (20) with (r, s) the fundamental solution of (17).

If p is prime, according to Theorem 5.5 all solutions belong to one of the trivial-class solutions. They can be generated by applying the recurrence (20) to the trivial solutions.

The number of solution classes of (6) is finite; a bound on the maximum magnitude of v for the fundamental solution of any class is

$$|v| \leq \frac{ps}{\sqrt{2(r + 1)}}, \tag{24}$$

where (r, s) is the fundamental solution of (17) [5, §58]. In principle, this bound allows one to find the fundamental solutions of all classes by a search on v in a finite number of steps, from which all solutions can be obtained via the recurrence (20). This method is quite efficient if the bound on v is small. However, for some cases, even some with modest values of p and q, the bound may be very large, rendering such a search impractical. The method of continued fractions can be adapted to find the solutions more efficiently, as follows.

Hua [3, §11.5] provides a recursive method for finding all solutions of (6) for $D > 0$ nonsquare, which we state concisely here. If $p^2 < \sqrt{D}$, then any solutions of (6) are found among the convergents of $\sqrt{D}$. Due to periodicity this involves only a finite number of steps. If $p^2 > \sqrt{D}$, initiate the recursion by setting $\delta = 1$ and $f = p^2$. In later stages of the recursion, $\delta = \pm 1$ will carry the sign while we keep $f > 0$. The equation to be solved is $u^2 - Dv^2 = \delta f$. Now reduce the right-hand side to be smaller in magnitude than $\sqrt{D}$ as follows. Seek integers l, h satisfying

$$\eta h = \frac{l^2 - D}{\delta f}, \quad h > 0, \; \eta = \pm 1. \tag{25}$$

This requires that $l^2 - D \equiv 0 \pmod{f}$, with $0 \leq l \leq \frac{h}{2}$. The congruence (25) is equivalent to $l^2 = D + fh$. It is sufficient to search for perfect squares using the range $-h_{\max} \leq h \leq h_{\max}$ where

$$h_{\max} = \max\left(\frac{f}{4}, \frac{D}{f}\right).$$

Since $f > \sqrt{D}$, it is guaranteed that $h < f$. There can be multiple solutions (l, h). For each one, solve $\xi^2 - D\nu^2 = \eta h$. If $h < \sqrt{D}$, solve directly by searching the convergents of $\sqrt{D}$; otherwise set $\delta f = \eta h$ and repeat recursively. Since f is reduced on each step, the recursion is guaranteed to terminate. Once one has a solution to $\xi^2 - D\nu^2 = \eta h$, solutions to $u^2 - Dv^2 = \delta f$ are given by

$$u = \frac{D\nu \pm l\xi}{h}, \quad v = \frac{\xi \pm l\nu}{h}, \tag{26}$$

using the same sign for each.

The solutions given by convergents are always coprime, while solutions of (6) may have common divisors, which must also divide p^2. To find these solutions, one can solve (6) divided by the square of each divisor of p, using the method in the previous paragraph.

6 Conclusion

We have presented feasible solution methods for each of the regimes of this problem: elliptical (probability $> \frac{1}{2}$), parabolic (probability $= \frac{1}{2}$), and hyperbolic (probability $< \frac{1}{2}$). Upper bounds on the number of solutions, and on the magnitude of solutions, for the elliptical case and for those hyperbolic cases having D a perfect square were obtained. It was shown that for hyperbolic cases with D nonsquare, there are always solutions, and cases were identified for which there are just 1 or 3 solution classes. An open question is whether upper bounds on the number of solution classes that are tighter than the bounds implied by (24) can be found in general.

Acknowledgements

Thanks to Dick Hess of the National Museum of Mathematics for creating the *Varsity Math* problem that was the starting point for this work. I would also like to acknowledge the late Bill Hildebrand, my friend who started me on this problem.

References

[1] Hilmer, K., Jin, A., Lycan, R., & Ponomarenko, V. (2023). The elliptical case of an odds inversion problem. *Involve*, 16(3), 431–452.

[2] Hilmer, K., Lycan, R., & Ponomarenko, V. (2022). Odds inversion problem with replacement. *The American Mathematical Monthly*, 129(9), 885.

[3] Hua, L. (1982). *Introduction to Number Theory* (translated from the Chinese by Peter Shiu). Springer-Verlag Berlin Heidelberg.

[4] Moniot, R. K. (2021). Solution of an odds inversion problem. *The American Mathematical Monthly*, 128(2), 140–149.

[5] Nagell, T. (1964). *Introduction to Number Theory* (2nd ed.). Chelsea Publishing Co., New York.

[6] National Museum of Mathematics, New York City (2017). Fifty-Fifty. *Varsity Math*, Week 117. Available online at: `https://momath.org/all-events/ongoing-programs/varsity-math/varsity-math-week-117/`