DIOPHANTINE EQUATIONS COMING FROM BINOMIAL NEAR-COLLISIONS

Nikos Katsipis[1]
Department of Mathematics and Applied Mathematics, University of Crete, Greece
katsipis@gmail.com

Received: 1/31/19, Accepted: 1/27/20, Published: 2/14/20

Abstract

In this paper we solve the diophantine equation $\binom{m}{l} - \binom{n}{k} = d$ (where m, n are positive integer unknowns) when $(k, l) = (6, 3), (3, 6)$ for various values of d and when $(k, l) = (8, 2)$ and $d = 1$. As a byproduct of our results we will obtain that $(k, l)-$near collisions with difference 1 do not exist if $(k, l) = (3, 6), (8, 2)$, thus establishing a conjecture stated in the article published in 2017 by Blokhuis, Brouwer and de Weger.

1. Introduction

The quadraple (n, k, l, m) is said to be a *(binomial) near collision with difference* d if there exists a pair (m, n) of integers with $2 \leq k \leq n/2$, $2 \leq l \leq m/2$, such that $\binom{m}{l} - \binom{n}{k} = d$ and $\binom{m}{l} \geq d^3$. Note that the above restrictions on k, l are very natural in view of the symmetries $\binom{m}{l} = \binom{m}{m-l}$ and $\binom{n}{k} = \binom{n}{n-k}$.

If we consider $k, l \geq 2$ and $d \neq 0$ (not-necessarily positive) as given fixed integers with $k \neq l$, we obtain the Diophantine equation

$$\binom{m}{l} - \binom{n}{k} = d, \tag{1}$$

in the positive integer unknowns m, n, without any restriction on the size of $\binom{m}{l}$ compared to d. In Section 2 we will solve (1) when $(k, l) = (3, 6)$ and $d = \pm 1$, and in Section 3 we will solve (1) with $(k, l) = (8, 2)$ and $d = 1$. Our main results, Theorems 2.2, 2.4, 3.1 respectively imply Corollaries 2.3, 2.5, 3.2. As a consequence we have that (k, l)*-near collisions with difference 1 do not exist if* $(k, l) \in \{(6, 3), (3, 6), (8, 2)\}$, thus establishing certain cases of Conjecture 2 in [1].

[1]This work is part of the author's Doctoral Thesis at the Department of Mathematics and Applied Mathematics, University of Crete.

We now sketch the method for solving the equations mentioned above, which we apply in Sections 2 and 3 . For each equation we work as follows. We reduce its resolution to the problem of finding the points (u, v) with integral coordinates on a certain elliptic curve C whose equation is not in Weierstrass form. We find a Weierstrass model E and an explicit birational transformation

$$C \ni (u,v) \longrightarrow (x,y) = (\mathcal{X}(u,v), \mathcal{Y}(u,v)) \in E$$
$$C \ni (\mathcal{U}(x,y), \mathcal{V}(x,y)) = (u,v) \longleftarrow (x,y) \in E$$

between C and E. This is accomplished by the MAPLE implementation of van Hoeij's algorithm [6]. The typical point on C is denoted by P^C and the corresponding point on E via the above birational transformation by P^E. We will also use the notation $(u(P), v(P))$ for the coordinates of the point P viewed as a point on C, hence $(u(P), v(P)) = P^C$, and $(x(P), y(P))$ for the coordinates of the point P viewed as a point on E, hence $(x(P), y(P)) = P^E$. Thus, if $P^C = (u, v) = (u(P), v(P))$ and $P^E = (x, y) = (x(P), y(P))$, then $x = \mathcal{X}(u, v)$, $y = \mathcal{Y}(u, v)$ and $u = \mathcal{U}(x, y)$, $v = \mathcal{V}(x, y)$.

Our problem is reduced to the following:

To compute explicitly all points $P^E \in E(\mathbb{Q})$ such that $P^C \in C(\mathbb{Z})$.

We deal with this problem as follows. Using the routine `MordellWeilBasis` of MAGMA[2] based on the work of many contributors, like J. Cremona, S. Donelly, T. Fisher, M. Stoll, to mention a few of them, we compute a Mordell-Weil basis for $E(\mathbb{Q})$ and let $P_1^E, \ldots, P_r^E$ be generators of the free part of $E(\mathbb{Q})$. In certain cases, especially when the rank of the elliptic curve is ≥ 5, it is necessary to improve the Mordell-Weil basis computed by MAGMA, in the sense of the Remark at the end of Section 2; see also the "Important computational issue" of [7]; we will need to do this in both Sections 2 and 3. Let $P^C = (u, v)$ denote the typical unknown point with integral coordinates. Its transformed point P^E via the previously mentioned birational transformation is a point with rational coordinates, therefore $P^E = m_1P_1^E + \cdots + m_rP_r^E + T^E$, where $m_1, \ldots, m_r$ are unknown integers and T^E denotes the typical torsion point (only finitely many and, actually, very few options for T^E exist). To this we associate the linear form

$$L(P) = (m_0 + \frac{s}{t})\,\omega_1 + m_1\mathfrak{l}(P_1) + \cdots + m_r\mathfrak{l}(P_r)\ \{\pm\mathfrak{l}(P_0)\}. \qquad (2)$$

Some explanations are in place here. Firstly, $\mathfrak{l}$ denotes the map $\mathfrak{l} : E(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}\omega_1$, closely related to the elliptic-logarithm function, which is defined and discussed in detail in Chapter 3 of [14], especially, Theorem 3.5.2. Next, ω_1 is the minimal positive real period of E, m_0 is an extra integer whose size depends explicitly on $M := \max_{1\leq i\leq r}|m_i|$, and s, t are relatively prime integers as follows: $t \geq 1$ divides the lcm of the orders of the non-zero torsion points of E and s is such that

$-1/2 < s/t \leq 1/2$. [2] Last, the indication $\{\}$ in the summand $\pm\mathfrak{l}(P_0)$ means that this is present only in Section 2, where P_0 is a certain explicitly known point. The *Elliptic Logarithm Method* exploits the fact that u, v are integers in order to find an upper bound for $|L(P)|$ in terms of M (see (17)) and, on the other hand, applies a deep result of S. David [3] in order to obtain a lower bound for $|L(P)|$ in terms of M. Comparing the two bounds of $|L(P)|$ we obtain the relation

$$\rho M^2 \leq \frac{c_{11}c_{13}}{2\theta}(\log(\alpha M+\beta)+c_{14})(\log\log(\alpha M+\beta)+c_{15})^{r+3}+\gamma+\frac{c_{11}}{2\theta}\log\frac{c_9}{1+\theta}+\tfrac{1}{2}c_{10}, \tag{3}$$

where all constants involved in it are explicit; see relation (9.8), Theorem 9.1.3 of [14]. It is clear that, if M is larger than an explicit bound B, then the left-hand side is *larger* than the right-hand side and this contradiction certainly implies that $M \leq B$. Since B is explicit, this allows us to compute all integer points $P^C = (u, v)$ as follows: for each $(m_1, \ldots, m_r)$ in the range $|m_i| \leq M$ $(i = 1, \ldots, r)$ we compute each point $P^E = m_1P_1^E + \cdots + m_rP_r^E + T^E$ with T^E a torsion point and then we compute its transformed point P^C via the previously mentioned birational transformation; if P^C has integer coordinates, then we have gotten an integer point $P^C = (u, v)$.

In principle, this procedure allows to pick-up all integer points (u, v) and, indeed, this is so if the bound B is small, say around 30. But the bound obtained from (3) is huge and we must reduce it to a manageable size. This is accomplished with de Weger's [15] technique, the basic tool of which is the *LLL-algorithn* of Lenstra-Lenstra-Lovász [5]. The *reduction process* appropriate for our purpose is described in Chapter 10 of [14].

2. Equation (1) with $(k, l) = (3, 6)$ and $d = \pm 1$

Replacing in (1) d by $-d$, we obtain the equation

$$\binom{n}{3} = \binom{m}{6} + d\,, \tag{4}$$

which we study in this section. Putting $u := n - 1$ and $v := (m-2)(m-3)/2$, we have

$$\binom{n}{3} = \frac{1}{6}((u+1)u(u-1))\,, \quad \binom{m}{6} = \frac{(v-3)(v-1)v}{6\cdot 5\cdot 3}\,,$$

so that equation (4) implies

$$15(u^3 - u - 6d) = v^3 - 4v^2 + 3v. \tag{5}$$

[2] Note that, by a famous theorem of B. Mazur, $11 \neq t \leq 12$; see [8], [9], or Theorem 7.5 of [11].

We rewrite equation (5) as $g(u,v)=0$, where

$$g(u,v)=15u^3-v^3+4v^2-90d-15u-3v. \tag{6}$$

In case that $d=(N^3-N)/6$, where N is an explicitly known non-zero integer, it is shown in [7] how the method of Chapter 8 of [14] can be applied in order to compute –at least in principle– all integer solutions of (6). A rough description of the above mentioned method is as follows: The curve $C: g(u,v)=0$, being a non-singular cubic, has genus one. Moreover, $(u,v)=(n,1)$ is a rational point of C, so that C is a model of an elliptic curve over $\mathbb{Q}$. The MAPLE implementation of van Hoeij's algorithm [6] gives the birational transformation between C and the Weierstrass model

$$E: y^2=x^3-1575x+A(N) \tag{7}$$

$$A(N):=33750N^3-33750N-\frac{1366875}{4}N^6+\frac{1366875}{2}N^4-\frac{1366875}{4}N^2+52650.$$

The birational transformation between C to E mentioned in page 2, as well as all other "technical" information is exposed in detail in [7]. As a result, the following theorem is the specialization of (3) in our present situation.

Theorem 2.1. *If $|u(P)|\geq 3|N|$, then either $M\leq c_{12}$ or*

$$\rho M^2\leq c_{13}(\log(\alpha M+\beta)+c_{14})(\log\log(\alpha M+\beta)+c_{15})^{r+3}+\gamma+\log 0.085+\tfrac{1}{2}\log(200|N|^3),$$

where r is the rank of the elliptic curve (7), ρ (>0) is the least eigenvalue of the (positive-definite) height-pairing matrix of the Mordell-Weil basis which we have computed for that elliptic curve, and all other constants involved in the above relation depend on N, are positive and can be explicitly calculated.

Remark. According to the end of Section 1, Theorem 2.1 implies an explicit bound of M. Moreover, it is not difficult to see that the resulting upper bound is a *decreasing function* of ρ. In Section 2 and more importantly in Section 3, the value of ρ plays a crucial role when we apply the reduction process described in Chapter 10 of [14]. More specifically, the reduced upper bound given by the relation (10.5) in that reference, heavily depends on a parameter κ_4 which is a positive multiple of ρ: the larger ρ (hence also κ_4) is, the smaller is the reduced upper bound. Therefore, if the value of ρ resulting from a certain Mordell-Weil basis $\mathcal{B}_2$ is larger than the value of ρ resulting from another basis $\mathcal{B}_1$, we consider $\mathcal{B}_2$ as a *better basis* than $\mathcal{B}_1$ for the application of the Elliptic Logarithm Method. The method which we apply in this paper in order to obtain a better Mordell-Weil basis starting from a given one, is exposed in [12]; see also [4] for another interesting approach to computing better (in the above sense) Mordell-Weil bases.

Of special interest are the cases $N=\mp 2$ for which $d=(N^3-N)/6=\mp 1$, so that equation (4) becomes, respectively, a $(3,6)$ and $(6,3)$ near-collision with difference

1; these are two of the three unsolved collision problems in [1] which we manage to solve here; see Corollaries 2.3 and 2.5.

The case $d = -1$ is the most difficult one, and therefore we discuss it in some detail. Now our elliptic curve C becomes (cf. (6))

$$C : g(u, v) = 0, \quad \text{where} \quad g(u, v) = 15u^3 - v^3 + 4v^2 - 15u - 3v + 90 \tag{8}$$

and its birationally equivalent Weierstrass model (7) is

$$E : y^2 = x^3 - 1575x - 12451725 =: f(x). \tag{9}$$

The Mordell-Weil group $E(\mathbb{Q})$ of rational points of the elliptic curve curve E has rank 5 (in the notation of Theorem 2.1, $r = 5$) and trivial torsion subgroup (in subsequent notation $r_0 = 1$). The free part of $E(\mathbb{Q})$ is generated by the points

$$P_1^E = (235, 395)\,,\ P_2^E = (615, 14805)\,,\ P_3^E = (3055, 168805)\,,$$

$$P_4^E = (1350, 49455)\,,\ P_5^E = \left(\frac{1185}{4}, -\frac{28935}{8}\right).$$

Actually, the Mordell-Weil basis formed by the above five points is an improvement of the Mordell-Weil basis furnished by MAGMA, in the sense of the above Remark; see also the Remark immediately after Corollary 2.3.
The birational transformation between the models C and E is:

$$\mathcal{X}(u, v) = \frac{3(40u^2 + 55uv + v^2 - 60u + 106v - 277)}{(u + 2)^2}$$

$$\mathcal{Y}(u, v) = \frac{3(2505u^3 + 90u^2v + 220uv^2 + 5595u^2 - 685uv + 437v^2 - 6360u - 1718v - 15069)}{(u + 2)^3},$$

and

$$\begin{aligned} \mathcal{U}(x, y) &= \frac{2x^3 - 60x^2 + 3xy - 49455x + 26865y + 68298525}{-x^3 + 360x^2 - 20925x + 66442950} \\ \mathcal{V}(x, y) &= \frac{15(18x^2 + 11xy + 80325x - 1311y + 8004285)}{-x^3 + 360x^2 - 20925x + 66442950} \end{aligned} \tag{10}$$

The linear form (2) is now

$$L(P) = \left(m_0 + \frac{s}{t}\right)\omega_1 + m_1\mathfrak{l}(P_1) + m_2\mathfrak{l}(P_2) + m_3\mathfrak{l}(P_3) + m_4\mathfrak{l}(P_4) + m_5\mathfrak{l}(P_5) \pm \mathfrak{l}(P_0),$$

where

$$P_0^E = (3\zeta^2 + 165\zeta + 120,\ 660\zeta^2 + 270\zeta + 7515),$$

and ζ is the cubic root of 15.

Since $f(X)$ has only one real root, namely $e_1 \approx 234.0452973361$, we have $E(\mathbb{R}) = E_0(\mathbb{R})$ (= the unbounded component of $E/\mathbb{R}$) and therefore $\mathfrak{l}(P_i)$ coincides with the elliptic logarithm of P_i^E for $i = 1, \ldots, 5$ (see Chapter 3 of [14], especially Theorem 3.5.2). On the other hand, P_0^E has irrational coordinates. As MAGMA does not possess a routine for calculating elliptic logarithms of non-rational points, we wrote our own routine in MAPLE for computing $\mathfrak{l}$-values of points with algebraic coordinates. The six points P_i^E, $i = 0, 1, \ldots, 5$, are $\mathbb{Z}$-linearly independent because their regulator is non-zero (see Theorem 8.1 in [10]). Therefore our linear form $L(P)$ falls under the scope of the second "bullet" on page 99 of [14] and we have $r_0 = 1$, $s/t = s_0/t_0 = 0/1 = 0$, $d = 1$, $r = 5$, $n_i = m_i$ for $i = 1, \ldots, 4$, $n_5 = \pm 1$, $n_0 = m_0$, $k = r + 1 = 6$, $\eta = 1$ and $N = \max_{0 \le i \le 5} |n_i| \le r_0 \max\{M, \frac{1}{2}rM + 1\} + \frac{1}{2}\eta r_0 = \frac{5}{2}M + \frac{3}{2}$, so that, in the relation (9.6) of [14] we can take

$$\alpha = 5/2, \ \beta = 3/2. \tag{11}$$

We compute the canonical heights of $P_1^E, P_2^E, P_3^E, P_4^E, P_5^E$ using MAGMA.[3] The corresponding height-pairing matrix $\mathcal{H}$ has minimum eigenvalue

$$\rho \approx 0.7722274789. \tag{12}$$

Next we apply Proposition 2.6.3 of [14] in order to compute a positive constant γ with the property that $\hat{h}(P^E) - \frac{1}{2}h(x(P)) \le \gamma$ for every point $P^E = (x(P), y(P)) \in E(\mathbb{Q})$, where h denotes Weil height; [4] it turns out that

$$\gamma \approx 4.6451703657. \tag{13}$$

Note that the constants in (11), (12) and (13) appear in the inequality of Theorem 2.1. Further, we have to specify the constants $c_{12}, c_{13}, c_{14}, c_{15}$ defined in Theorem 9.1.2 of [14]. This is a rather straightforward task if one follows the detailed instructions of "Preparatory to Theorem 9.1.2" [14], which can be carried out even with a pocket calculator, except for the computation of various canonical heights. At this point we need to compute also the canonical height of the point P_0^E. Since this point has irrational coordinates we confine ourselves to the upper bound $\hat{h}(P_0^E) \le 7.300572483$ proved in [7]. Carrying out all these computations is quite a boring job; fortunately, it can be performed almost automatically with a MAPLE program. In this way we compute

$$c_{12} \approx 1.210103 \cdot 10^{27}, \quad c_{13} \approx 1.342820 \cdot 10^{281}, \quad c_{14} \approx 2.09861, \quad c_{15} \approx 25.03975. \tag{14}$$

[3]For the definition of the canonical height we follow J.H. Silverman; as a consequence the values displayed here for the canonical heights are the halves of those computed by MAGMA and the least eigenvalue ρ of the height-pairing matrix $\mathcal{H}$ below, is half of that computed by MAGMA; cf. "Warning" at bottom of p. 106 in [14].

[4]In the notation of that Proposition, as a curve D we take the minimal model of E, which is E itself.

Now, in view of Theorem 2.1 and (11), (12), (13), (14), we conclude that, if $|u(P)| \geq 6$, then either $M \leq c_{12}$ or

$$0.77222 \cdot M^2 \leq 1.34 \cdot 10^{281} \times (\log(2.5M + 1.5) + 2.0986) \\ \times(\log(0.4342 \log(2.5M + 1.5)) + 25.0397)^5 + 5.4159.$$

But for all $M \geq 6.86 \cdot 10^{147}$, we check that the left-hand side is strictly larger than the right-hand side, which implies that $M < 6.86 \cdot 10^{147}$. Therefore,

$$|u(P)| \geq 6 \;\text{ implies }\; M \leq \max\{c_{12},\ 6.86 \cdot 10^{147}\} = 6.86 \cdot 10^{147}. \tag{15}$$

An easy straightforward computation shows that all integer points P^C with $|u(P)| \leq 5$ (equivalently, all integer solutions (u, v) of (8) with $|u| \leq 5$) are the following:

$$P^C = (-2, 0),\ (-2, 1),\ (-2, 3),\ (-1, 6),\ (0, 6),\ (1, 6). \tag{16}$$

In order to find explicitly all points P^C with $|u(P)| \geq 6$ it is necessary to reduce the huge upper bound (15) to an upper bound of manageable size. This is accomplished in [7] using standard LLL-reduction; as a result it is shown that $M \leq 27$. Therefore, we have to check which points

$$P^E = m_1P_1^E + m_2P_2^E + m_3P_3^E + m_4P_4^E + m_5P_5^E, \quad \text{with } \max_{1\leq i\leq 5} |m_i| \leq 27,$$

have the property that $P^E = (x, y)$ maps via the transformation (10) to a point $P^C = (u, v) \in C$ with integer coordinates. We remark here that every point P^C with $u(P)$ integer and $|u(P)| \geq 6$ is obtained in this way, but the converse is not necessarily true, i.e. if $\max_{1\leq i\leq 5} |m_i| \leq 27$ and the above P^E maps to P^C with integer coordinates, it is not necessarily true that $|u(P)| \geq 6$.

If we were going to check all 5-tuples $(m_1, m_2, m_3, m_4, m_5)$ in the range $-27 \leq m_i \leq 27$ by "brute force" this would take more than 15 days of computation. Therefore, we apply a simple but very effective trick to speed up this final search. This trick, called in [12] *inequality trick*, is based on the observation that, for every 5-tuple $(m_1, m_2, m_3, m_4, m_5)$ corresponding to a point $P^E = m_1P_1^E + m_2P_2^E + m_3P_3^E + m_4P_4^E + m_5P_5^E$, the upper bound of $|L(P)|$ mentioned just above (3), more specifically,

$$|L(P)| \leq k_1 \exp(k_2 - k_4M^2) \tag{17}$$

must be satisfied for the six-tuple $(m_0, m_1, \ldots, m_5)$, where m_0 is the extra parameter appearing in (2) with $|m_0| \leq 27$. The heuristic observation is that the above inequality is very unlikely to be satisfied by points P^E with at least one large coefficient m_i. The reason is that the elliptic logarithms $\mathfrak{l}(P_i)$ are more or less randomly distributed (at least there is no reason to assume otherwise) so that the linear $L(P)$ is rarely very small. Checking whether the $L(P)$, coming from a certain 6-tuple $(m_0, m_1, m_2.m_3, m_4, m_5)$ in the range $-27 \leq m_i \leq 27$, satisfies the above displayed inequality requires real number computations which are considerably faster than those required for computing symbolically $P^E = m_1P_1^E + m_2P_2^E + m_3P_3^E + m_4P_4^E + m_5P_5^E$ and then checking whether the corresponding point P^C is integral. Actually, this reduces the computation to a few hours and furnishes us with the points figuring in Table 1.

m_1	m_2	m_3	m_4	m_5	$P^E=(x,y)$	$P^C=(u,v)$
-1	0	0	-1	1	$(27075,-4455045)$	$(-2,1)$
-1	0	0	0	0	$(235,-395)$	$(1,6)$
0	0	-1	-1	0	$(495,-10395)$	$(-1,6)$
0	0	-1	0	-1	$(555,12555)$	$(-138,-339)$
0	0	-1	0	0	$(3055,-168805)$	$(-2,3)$
0	0	0	0	1	$(1185/4,-28935/8)$	$(0,6)$

Table 1: All points $P^E=\Sigma_i m_i P_i^E$ with $P^C=(u,v)\in\mathbb{Z}\times\mathbb{Z}$.

Only the point P^C which corresponds to $(m_1,m_2,m_3,m_4,m_5)=(0,0,-1,0,-1)$ has $|u(P)|\geq 6$. The remaining five points $P^C=(u,v)$ satisfy $|u|<6$ and therefore they are contained in the already found list of points (16). This list contains one more point, namely $(u,v)=(-2,0)$, which is not among the points of the above table, because it does not correspond to a point P^E via the (affine) birational transformation of page 5. We have thus proved the following.

Theorem 2.2. *The integer solutions of the equation* (8) *are*

$$(u,v)=(-138,-339),\ (-2,0),\ (-2,1),\ (-2,3),\ (-1,6),\ (0,6),\ (1,6).$$

Corollary 2.3. *No* $(3,6)$ *near-collision with difference* 1 *exists.*

Proof. Assume that $(n,3,m,6)$ is a near collision with difference 1. Then $\binom{m}{6}-\binom{n}{3}=1$, which is equation (4) with $d=-1$. At the beginning of Section 2 we saw that, if we put $u=n-1$ and $v=(m-2)(m-3)/2$, then (u,v) is an integer solution of the equation (5) with $d=-1$, i.e. (u,v) is an integral point on the curve (8). By the restrictions on the definition of collision, $n\geq 6$, so $u\geq 7$ and by Theorem 2.2, no solution (u,v) to (8) exists with $u\geq 7$. □

Remark. As mentioned below (9), the online MAGMA calculator (`V2.24-3`) returns a different Mordell-Weil basis for the elliptic curve (9). The value of ρ corresponding to that basis is $\rho\approx 0.410937$. As a consequence, the initial upper bound for M (cf. (15)) is $M<6.86\cdot 10^{147}$ and after four reduction steps, the final reduced upper bound is 34. Therefore the final check for all 6-tuples $(m_0,m_1,\ldots,m_5)$ in the range $-34\leq m_i\leq 34$ needs at least four times $(4\approx(34/27)^6)$ more computation time; actually, according to our experiments, it needs much more.

The case $d=1$ is treated in a way completely analogous to that of case $d=-1$. [5] Now our curve is $C\,:\,15u^3-v^3+4v^2-15u-3v-90=0$ and the birationally equivalent Weierstrass model E is, by (7), $E\,:\,y^2=x^3-1575x-12046725$. All computations are *much simpler* because E has rank $r=2$, and $P_1=(26745/4,-4373685/8), P_2=(2995,163855)$ is a Mordell-Weil basis. As a result we have the following.

[5] More details in [7].

Theorem 2.4. *The only integer solution of the equation* $15u^3 - v^3 + 4v^2 - 15u - 3v - 90 = 0$ *is* $(u, v) = (2, 3)$.

Corollary 2.5. *No* $(6, 3)$ *near-collision with difference* 1 *exists.*

Proof. Assume that $(n, 6, m, 3)$ is a near collision with difference 1. Then $\binom{m}{3} - \binom{n}{6} = 1$ and, on interchanging m, n, we are led to equation (4) with $d = 1$. According to Section 2, if in (4) we put $u = n - 1$ and $v = (m-2)(m-3)/2$, then (u, v) is an integer solution of the equation (5) with $d = 1$. Moreover, by the restrictions on the definition of collision, $n \geq 6$, so $u \geq 7$. According to Theorem 2.4, the only solution is $(u, v) = (2, 3)$, and this concludes the proof. □

3. Equation (1) with $(k, l) = (8, 2)$ and $d = 1$

We write our equation as follows:

$$\frac{\left(n^2 - 7n\right)\left(n^2 - 7n + 6\right)\left(n^2 - 7n + 10\right)\left(n^2 - 7n + 12\right)}{3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8} + 2 = (m^2 - m).$$

Putting

$$u = \frac{1}{2}n^2 - \frac{7}{2}n + 6, \quad v = 210m - 105, \tag{18}$$

we are led to

$$v^2 = 35u^4 - 350u^3 + 945u^2 - 630u + 315^2, \tag{19}$$

hence, it suffices to explicitly solve equation (19). The most straightforward thing for doing this, would be to turn to MAGMA's routine `IntegralQuarticPoints`, which is based on [13] and was firstly developed in 1999 by Emmanuel Herrmann and further improved in the years 2006-2013 by Stephen Donnelly and other people of MAGMA group. Indeed, we ran the above routine for (19) on a computer Intel i5-7200U @ 2.50GHz, but after five days, MAGMA gave up without results, with the message "Killed". Consequently we had to solve (19) "non-automatically", following the method of [13], as exposed in Chapter 6 of [14]. For the successful accomplishment of this, crucial role play:

1. Our Mordell-Weil basis, which is an improvement of the one computed by MAGMA, as explained in the Remark at the end of this section.
2. The application of an *inequality trick* completely analogous to that which we start discussing a few lines above (17).

We will deal with the elliptic curve

$$C : v^2 = Q(u) := 35u^4 - 350u^3 + 945u^2 - 630u + 315^2.$$

We use the notation, results etc of Chapter 6 of [14]; thus we have $a = 35$, $b = -350$, $c = 945$, $d = -630$, $e = 315$. By relation (6.3) in [14] the Weierstrass model which is birationally equivalent to the curve C is

$$E : y^2 = f(x) := x^3 + Ax + B, \tag{20}$$

where $A=-13968675$ and $B=3410363250$, and the birational functions

$$C \ni (u,v) \mapsto (\mathcal{X}(u,v)\,,\mathcal{Y}(u,v)) = (x,y) \in E$$
$$E \ni (x,y) \mapsto (\mathcal{U}(x,y)\,,\mathcal{V}(x,y)) = (u,v) \in C$$

are

$$\begin{aligned} \mathcal{X}(u,v) &= \frac{315(u^2-2u-2v+630)}{u^2} \\ \mathcal{Y}(u,v) &= -\frac{630(175u^3-945u^2-uv+945u+630v-198450)}{u^3} \end{aligned} \tag{21}$$

(relation (6.4) in [14]) and

$$\begin{aligned} \mathcal{U}(x,y) &= -\frac{630(x+y+109935)}{x^2-630x-13792275} \\ \mathcal{V}(x,y) &= -315(x^4+630x^3+2x^2y-529200x^2+439740xy+22441718250x \\ &\quad -110933550y-196956864680625) : (x^2-630x-13792275)^2 \end{aligned} \tag{22}$$

(relations (6.5) and (6.6) in [14]).

We have to calculate the three real roots $e_1 > e_2 > e_3$ of $f(x)$ and a fundamental pair of periods $\omega_1 \in \mathbb{R}$, $\omega_2 \in i\mathbb{R}$ for the Weierstrass $\wp$ function which parametrizes E. Now we refer to Section 1, the notations of which we adopt here. The rank of E is 5 and the torsion subgroup $E_{tors}(\mathbb{Q})$ is trivial. The following points form a Mordell-Weil basis for $E(\mathbb{Q})$:[6]

$$P_1^E = (-1799, 150724),\ P_2^E = (105, -44100),\ P_3^E = (-315, -88200),$$
$$P_4^E = (8985, 776700),\ P_5^E = (3885, 88200).$$

We note that, for $i=1,2,3$, the points P_i^E belong to $E_1(\mathbb{R})$, the bounded component ("egg") of $E(\mathbb{R})$ and therefore by "Conclusions and remarks" (1) in page 51 of [14], $\mathfrak{l}(P_i)$ is the elliptic logarithm of the point $P_i^E + Q_2^E$, where $Q_2^E = (e_2, 0)$. Now $P_i^E + Q_2^E$ belongs to the unbounded component $E_0(\mathbb{R})$ of $E(\mathbb{R})$, but its coordinates are non-rational, belonging to the cubic extension of $\mathbb{Q}(e_2)/\mathbb{Q}$. Therefore, for $i = 1,2,3$, $\mathfrak{l}(P_i)$ is equal to the elliptic logarithm of $P_i^E + Q_2^E$, which we compute using our MAPLE routine, mentioned a few lines above (11). The points P_4^E and P_5^E belong to $E_0(\mathbb{R})$ and therefore, for $i = 3,4$, $\mathfrak{l}(P_i)$ is equal to the elliptic logarithm of P_i^E. Next we need to calculate approximate values of the canonical heights (cf. footnote 3), the height-pairing matrix $\mathcal{H}$ and its minimum eigenvalue (cf. footnote 6)

$$\rho \approx 0.5764009469.$$

We compute a positive number γ such that $\hat{h}(P^E) - \frac{1}{2}h(x(P)) \leq \gamma$, where h denotes Weil height, by applying Proposition 2.6.3 of [14]. In the notation of that

[6] See the Remark at the end of this section.

proposition, as a curve D we take the minimal model of E, which is E itself, and following the simple instructions therein, we compute $\gamma = 6.4974558131$. Finally, in order to compute the constants involved in Theorem 9.1.2 of [14] that are necessary for the application of Theorem 9.1.3 of [14], we replace the pair of fundamental periods ω_1, ω_2, for which $\tau := \omega_1/\omega_2$ does not belong to the fundamental region of the complex upper half-plane, by the pair $(\varpi_1, \varpi_2) = (\omega_2, -\omega_1)$; for this pair, $\tilde{\tau} := \varpi_1/\varpi_2$ satisfies $|\tilde{\tau}| \geq 1$, $\Im\tilde{\tau} > 0$ and $|\Re\tilde{\tau}| < 1/2$, hence it belongs to the fundamental region.

In order to obtain a relation of the form (3), we will apply Theorem 9.1.3 of [14]. That theorem applies to points $P^C = (u(P), v(P))$ with $|u(P)|$ sufficiently large. Table 6.1 in Chapter 6 of [14] indicates a procedure for computing how large $|u(P)|$ should be; actually, we must have $|u(P)| \geq \max\{u^{**}, \overline{u}^{**}\}$ and $u^{**}, \overline{u}^{**}$ are calculated as explained in that table. The existence of two columns in Table 6.1 of Chapter 6 of [14] and in its specialization to our case, which is Table 2 below, is explained as follows: At this stage it is convenient, instead of searching for solutions of $Q(u) = v^2$ with $v \geq 0$ and u of whatever sign, to look for solutions of both equations $Q(u) = v^2$ and $\overline{Q}(u) := Q(-u) = v^2$ with $u, v \geq 0$. Thus, a "bar" over a constant refers to the second equation. The constant $\max\{c_7, \overline{c}_7\}(= 13$ in our case) is used in the application of Theorem 9.1.3 of [14].

$Q(u) =$ $35u^4 - 350u^3 + 945u^2 - 630u + 99225$	$\overline{Q}(u) =$ $35u^4 + 350u^3 + 945u^2 + 630u + 99225$
$\sigma = 1$	$\overline{\sigma} = -1$
$\mathrm{x}(u) = 315\dfrac{u^2 - 2u + 630 + 2(Q(u))^{1/2}}{u^2}$	$\bar{\mathrm{x}}(u) = 315\dfrac{u^2 + 2u + 630 + 2(\overline{Q}(u))^{1/2}}{u^2}$
$u^{**} = 3$ and $c_7 = 13$	$\overline{u}^{**} = 80$ and $\overline{c}_7 = 13$
$P_0^E =$ $(630\sqrt{35} + 315, 110250 + 630\sqrt{35})$	$\overline{P}_0^E =$ $(630\sqrt{35} + 315, -110250 - 630\sqrt{35})$
$\mathfrak{l}(P_0)$	$\mathfrak{l}(\overline{P}_0) = -\mathfrak{l}(P_0)$
$L(P) = \mathfrak{l}(P) - \mathfrak{l}(P_0)$	$\overline{L}(P) = \mathfrak{l}(P) + \mathfrak{l}(P_0)$

Table 2: Parameters and auxiliary functions for the solution of the quartic elliptic equation according to the Table 6.1 in [14]

From Table 2 it follows that the conditions of Theorem 6.8 in [14], which are also necessary for the application of Theorem 9.1.3 in [14], are fulfilled for all points $P^C \in C(\mathbb{Z})$ with $v(P) > 0$ and $|u(P)| \geq 80$. A quick computer search shows that the only points in $P^C(\mathbb{Z})$ with $|u(P)| < 80$ are those points (u, v) listed in Table 3 with $|u| < 80$. From Table 2 it follows also that, on applying Theorem 9.1.3 of [14], we must take $c_7 = 13$ and $L(P) = \mathfrak{l}(P) \pm \mathfrak{l}(P_0)$. We have already computed approximations of the coefficients ω_1 and ℓ_i $(i = 1, \ldots, 5)$ of the linear form $\mathfrak{l}(P)$, and using our aforementioned MAPLE routine we also compute $\ell_0 :=$

$\mathfrak{l}(P_0) \approx -0.179410143$.

Using the routine `IsLinearlyIndependent` of MAGMA, we see that the points P_i^E $(i = 0, \dots, 5)$ are $\mathbb{Z}$-linearly independent, so that we are in the situation described in the second "bullet", page 99 in [14]. Therefore, the parameters in the linear form (9.2) of [14] are

$$k = r + 1 = 6,\ d = 1,\ r_0 = 1,\ (n_1, n_2, n_3, n_4, n_5) = (m_1, m_2, m_3, m_4, m_5),$$
$$n_6 = \pm 1,\ \ell_6 = \ell_0.$$

In the notation of relation (9.3) in [14] we have $N_0 = \frac{5}{2}M + \frac{3}{2}$, hence $(\alpha, \beta) = (5/2, 3/2)$.

In order to compute various constants involved in the upper bound for M furnished by Theorem 9.1.3 of [14], we also need to compute $\hat{h}(P_0^E)$. Since P_0 is not a rational point we confine ourselves to the reasonably good upper bound of its canonical height obtained from Proposition 2.6.4 of [14]. In the notation of that proposition we take as curve D our curve E and obtain the bound $\hat{h}(P_0^E) \leq 14.72$.

We see that the degree of the number field generated by the coordinates of all points P_i $(i = 0, \dots, 5)$ is 6, hence, in the notation of "Preparatory to Theorem 9.1.2" of [14], $D = 6$. Following the instructions therein and Theorem 9.1.2 we compute

$$c_{12} = 6.76211752 \cdot 10^{30},\ c_{13} = 3.6856633 \cdot 10^{286},\ c_{14} = 2.79176,\ c_{15} = 28.91$$

and, in the notation of Theorem 9.1.3 in [14], $c_{16} = 0.68,\ c_{17} = 1.832,\ c_{18} = 1$. By that theorem, which in our case is Theorem 2.1, either $M \leq c_{12}$, or $\mathcal{B}(M) > 0$, where $\mathcal{B}(M) = c_{18}c_{13}(\log(\alpha M+\beta)+c_{14})(\log\log(\alpha M+\beta)+c_{15})^{k+2}+\gamma+c_{18}\log c_{16}+c_{17} - \rho \cdot M^2$. Note that all parameters in $\mathcal{B}(M)$ have already been computed and are displayed in this and the previous pages. Now it is straightforward to check that, for $M \geq 6.28 \cdot 10^{150}$, we have $\mathcal{B}(M) < 0$, hence

$$M \leq \max\{c_{12}, 6.28 \cdot 10^{150}\} = 6.28 \cdot 10^{150}.$$

We are now in a situation completely similar to that after relation (16). This time the process for the reduction of the above upper bound of M is repeated three times, giving successively the upper bounds 170, 30 and 28; the last upper bound cannot be further reduced. Next, we check which points $P^E = m_1P_1^E + \cdots + m_5P_5^E$ in the range $\max_{1\leq i\leq m} |m_i| \leq 28$ correspond to a point P^C with integral coordinates, using the *inequality trick*, as explained in the last paragraph above Table 1. The computation on a computer Intel i5-7200U @ 2.50GHz took a little more than 70 hours of computation and the results are comprised in Table 3. In particular, we have the following.

Theorem 3.1. *All integer solutions of the equation* (19) *are those listed in the seventh column of* Table 3.

Remark. The online MAGMA calculator (`V2.24-3`) returns the following Mordell-Weil basis for the elliptic curve (20): $(19705/81, 3758300/729), (14665/4, -307475/8)$,

$(8985, -776700), (693805, -577896200), (28035, -4652550)$. Using this basis and the method of [12], we obtained the considerably better basis (in the sense of the "Remark" immediately after Theorem 2.1) displayed a few lines below (22). Indeed, as we have already seen, the value of ρ for the improved basis is ≈ 0.5764, while the approximate value of ρ for the above displayed basis is 0.1284705. As a consequence, the initial upper bound for M is $M < 1.34 \cdot 10^{151}$. This is not essentially worse than the upper bound for M displayed a few lines above Theorem 3.1. *However*, after four reduction steps – and here ρ plays its important role – the reduced upper bound is 62 and cannot be further reduced (remember that the final reduced bound with the better basis is 28). Therefore, had we used the above Mordell-Weil basis, the final check for all 6-tuples $(m_0, m_1, \ldots, m_5)$ in the range $-62 \le m_i \le 62$ would require at least $(62/28)^6$ times more computation time, which amounts to *at least one year of computation time!*

m_1	m_2	m_3	m_4	m_5	$P^E = (x, y)$	$P^C = (u, v)$
0	0	0	0	1	$(3885, 88200)$	$(111, -69615)$
1	1	1	1	-1	$(-4427535/1369, 6153669900/50653)$	$(111, 69615)$
0	0	0	1	-1	$(5355, 286650)$	$(-22, -3535)$
1	1	1	0	1	$(-465570/121, 18522000/1331)$	$(-22, 3535)$
0	0	1	0	-1	$(-3570, 88200)$	$(-102, 64575)$
1	1	0	1	1	$(1228395/289, 709061850/4913)$	$(-102, -64575)$
0	0	1	0	0	$(-315, -88200)$	$(1, 315)$
1	1	0	1	0	$(396585, -249738300)$	$(1, -315)$
0	1	-1	1	-1	$(4110, 124200)$	$(-294, -520065)$
1	0	2	0	1	$(-170085/49, 34428150/343)$	$(-294, 520065)$
0	1	0	0	0	$(105, -44100)$	$(3, 315)$
1	0	1	1	0	$(44205, -9261000)$	$(3, -315)$
0	1	0	0	1	$(-2765, 144550)$	$(36, 6615)$
1	0	1	1	-1	$(14665/4, 307475/8)$	$(36, -6615)$
0	1	0	1	-1	$(-1491, 144648)$	$(15, 945)$
1	0	1	0	1	$(3801, -72324)$	$(15, -945)$
0	1	0	1	0	$(-9135/4, -1223775/8)$	$(-4, 385)$
1	0	1	0	0	$(28035, 4652550)$	$(-4, -385)$
0	1	1	0	-1	$(4761, 211716)$	$(-35, -8295)$
1	0	0	1	1	$(-3771, 49608)$	$(-35, 8295)$
0	1	1	0	0	$(11235, -1124550)$	$(6, -315)$
1	0	0	1	0	$(210, 22050)$	$(6, 315)$
0	0	1	0	1	$(12105, 1268100)$	$(-7, -595)$
1	0	0	1	-1	$(-3195, -124200)$	$(-7, 595)$
1	1	1	1	0	$(-629, -109306)$	$(0, 315)$
0	0	0	0	0	$\mathcal{O}$	$(0, -315)$

Table 3: All points $P^E = \Sigma_i m_i P_i^E$ with $P^C = (u, v) \in \mathbb{Z} \times \mathbb{Z}$.

We must also check the points $(x, y) \in E(\mathbb{Q})$ that are zeros of the polynomial $q(x) = x^2 - 630x - 13792275$ that appears in the denominator of $\mathcal{U}(x, y)$ and $\mathcal{V}(x, y)$. But the zeros of $q(x)$ are irrational, so we do not have any new solutions.

Finally, we come back to the collision equation $\binom{m}{2} = \binom{n}{8} + 1$ from which we started. We have $m = (v + 105)/210$, hence $105|v$, and $2u = n^2 - 7n + 12$. The only solutions (u, v) with v divisible by 105 are those listed in Table 4, where also the corresponding values of $(m, n) \in \mathbb{N}^2$ are listed.

(u, v)	$(m, n) \in \mathbb{N}^2$
$(1, 315)$	$(2, 5)$, $(2, 2)$
$(3, 315)$	$(2, 6)$, $(2, 1)$
$(36, 6615)$	$(32, 12)$
$(15, 945)$	$(5, 9)$
$(6, 315)$	$(2, 0)$, $(2, 7)$
$(0, 315)$	$(2, 4)$, $(2, 3)$

Table 4: Positive integer solutions of the collision equation $\binom{m}{2} = \binom{n}{8} + 1$

Note that no pair (m, n) in the above table satisfies the condition $m \geq 4$ and $n \geq 16$, therefore we have proved the following.

Corollary 3.2. *There is no* $(8, 2)$ *near-collision with difference* 1.

Acknowledgment. The author thanks the anonymous referee for his/her careful reading and the well-aimed comments, which greatly helped him to clarify the meaning of “good” Mordell-Weil basis in the context of this paper.

References

[1] A. Blokhuis, A. Brouwer, B. de Weger, Binomial collisions and near collisions, *Integers* **17** (2017), A64.

[2] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235-265.

[3] S. David, Minorations de formes linéaires de logarithmes elliptiques, *Mém. Soc. Math. Fr. (N.S.)* No 62, **123** (1995), fasc. 3, 143 pp.

[4] L. Hajdu, T. Kovács, Parallel LLL-reduction for bounding the integral solutions of elliptic Diophantine equations, *Math. Comp.* **78** No 266 (2009), 1201-1210.

[5] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515-534.

[6] M. van Hoeij, An algorithm for computing the Weierstrass normal form, *ISSAC' 95 Proceedings* (1995), 90-95.

[7] N. Katsipis, Diophantine equations coming from binomial near-collisions, *arXiv:1901.03841*.

[8] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. Inst. Hautes Études Sci.* **47** (1977), 33-186.

[9] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), *Invent. Math.* **44** (1978), 129-162.

[10] S. Schmitt, H. Zimmer, *Elliptic Curves: A Computational Approach*, Studies in Mathematics 31, De Gruyter, Berlin/New York 2003.

[11] J.H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Graduate Texts in Mathematics 106 - Springer, Dordrecht-Heidelberg-London-New York, 2009.

[12] R. J. Stroeker, N. Tzanakis, On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an Improvement, *Exp. Math.* **8** No. 2 (1999), 135-149.

[13] N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, The quartic case, *Acta Arith.* **75** (1996), 165-190.

[14] N. Tzanakis, *Elliptic Diophantine Equations: A concrete approach via the elliptic logarithm*, Series in Discrete Mathematics and Applications 2, De Gruyter, Berlin/Boston 2013.

[15] B.M.M. de Weger, *Algorithms for Diophantine equations*, CWI Tract 65, Amsterdam 1989.