Equal binomial coefficients: some elementary considerations

Benjamin M.M. de Weger

Econometric Institute, Erasmus University Rotterdam,

P.O. Box 1738, 3000 DR Rotterdam, The Netherlands.

(e-mail: dweger@wis.few.eur.nl)

August 1995

1 Introduction

In the Pascal Triangle, consisting of the binomial coefficients $\binom{n}{k}$ for $n = 0, 1, 2, \ldots$ and $0 \le k \le n$, one encounters each natural number (with the exception of 2) at least twice, and many numbers more than twice. There are three well known relations that account for this, namely

$$\binom{n}{k} = \binom{n}{n-k}, \quad \binom{n}{0} = 1, \quad \binom{n}{1} = n$$

for $n = 0, 1, 2, \ldots$, $0 \le k \le n$. Notice that the third relation above implies $\binom{\binom{n}{k}}{1} = \binom{n}{k}$, so that there are infinitely many numbers occurring at least 4 times in the Pascal Triangle.

Stripped of these trivialities, the more interesting problem becomes to determine the natural numbers that occur at least twice as binomial coefficients of the shape $\binom{n}{k}$ with $2 \le k \le \frac{1}{2}n$, and this is yet unsolved in its full generality. The only nontrivial solutions known at this time are the following (see the Figure on the next page):

$$\binom{16}{2} = \binom{10}{3} = 120, \quad \binom{21}{2} = \binom{10}{4} = 210, \quad \binom{56}{2} = \binom{22}{3} = 1540,$$
$$\binom{120}{2} = \binom{36}{3} = 7140, \quad \binom{153}{2} = \binom{19}{5} = 11628, \quad \binom{221}{2} = \binom{17}{8} = 24310,$$
$$\binom{78}{2} = \binom{15}{5} = \binom{14}{6} = 3003,$$

and an infinite family:

$$\binom{F_{2i+2}F_{2i+3}}{F_{2i}F_{2i+3}} = \binom{F_{2i+2}F_{2i+3} - 1}{F_{2i}F_{2i+3} + 1} \quad \text{for} \quad i = 1, 2, \ldots,$$

$\binom{n}{k}$	$k=2$	3	4	5	6	7	8	9	10	$\cdots$
$n=4$	6									
5	10									
6	15	20								
7	21	35								
8	28	56	70							
9	36	84	126							
10	45	$\boxed{120}$	$\boxed{210}$	252						
11	55	165	330	462						
12	66	220	495	792	924					
13	78	286	715	1287	1716					
14	91	364	1001	2002	$\boxed{3003}$	3432				
15	105	455	1365	$\boxed{3003}$	5005	6435				
16	$\boxed{120}$	560	1820	4368	8008	11440	12870			
17	136	680	2380	6188	12376	19448	$\boxed{24310}$			
18	153	816	3060	8568	18564	31824	43758	48620		
19	171	969	3876	$\boxed{11628}$	27132	50388	75582	92378		
20	190	1140	4845	15504	38760	77520	125970	167960	184756	
21	$\boxed{210}$	1330	5985	20349	54264	116280	203490	293930	352716	
22	231	$\boxed{1540}$	7315	26334	74613	170544	319770	497420	646646	
23	253	1771	8855	33649	100947	245157	490314	817190	1144066	
24	276	2024	10626	42504	134596	346104	735471	1307504	1961256	
$\vdots$										
36	630	$\boxed{7140}$	58905							
$\vdots$										
56	$\boxed{1540}$	27720								
$\vdots$										
78	$\boxed{3003}$	76076								
$\vdots$						$\boxed{\binom{103}{40}}$				
$\vdots$					$\boxed{\binom{104}{39}}$					
120	$\boxed{7140}$	280840								
$\vdots$										
153	$\boxed{11628}$	585276								
$\vdots$										
221	$\boxed{24310}$	1774630								
$\vdots$								$\boxed{\binom{713}{273}}$		
							$\boxed{\binom{714}{272}}$			
										$\boxed{\binom{4894}{1870}}$
									$\boxed{\binom{4895}{1869}}$	
										$\ddots$

where F_n is the nth Fibonacci number (defined by $F_0 = 0, F_1 = 1$, and $F_{n+1} = F_n + F_{n-1}$ for $n = 1, 2, \ldots$). This infinite family is due to D.A. Lind [L] and D. Singmaster [Sin2]. Its first few members (not counting the trivial $\binom{2}{0} = \binom{1}{1}$) are

$$\binom{15}{5} = \binom{14}{6} = 3003, \quad \binom{104}{39} = \binom{103}{40} = 61218182743304701891431482520,$$

$$\begin{aligned}\binom{714}{272} = \binom{713}{273} = \; & 3537835171522765057006983148520718494957187357011427136\backslash \\ & 6913752273880826066845830326660883349620614619010 9\backslash \\ & 0477513197821330000906170565587040820236444389470 7\backslash \\ & 0157551509232541760603309541615191409027157780780 0\,, \quad \ldots\end{aligned}$$

and the existence of this family implies the existence of infinitely many numbers occurring at least 6 times in the Pascal Triangle. It's an amusing exercise to start from the equation $\binom{n}{k} = \binom{n-1}{k+1}$, and to arrive at this infinite family of solutions.

There are no other nontrivial solutions of $\binom{n}{k} = \binom{m}{\ell}$ with $\binom{n}{k} \leq 10^{30}$ or $\max\{n, m\} \leq 1000$, as we could show without difficulties in a few hours on a personal computer. Notice that D. Singmaster [Sin2] searched up to $2^{48} \approx 2.8 \times 10^{14}$.

We did this computer search as follows. To start with, all solutions to $\binom{n}{k} = \binom{m}{\ell}$ with $\max\{k, \ell\} \leq 4$, are known, see below. Next, we made a list of all $\binom{n}{k} \leq 10^{30}$ with $5 \leq k \leq \frac{1}{2}n$, and sorted this list. Thus numbers occurring twice in the list are easily found. Next, for each member of the list we checked whether they were of the form $\binom{m}{\ell}$ for $\ell = 2, 3, 4$ (which was the most time-consuming step). All these computations were done in exact (i.e. 30 digit) arithmetic. Finally, we made a list of all $\binom{n}{k} > 10^{30}$ with $\max\{n, m\} \leq 1000$ in 8 digit precision only, sorted this list, and checked for pairs being close enough.

Let $N(a)$ be the number of occurrences of a as a binomial coefficient. Then $N(1) = \infty$, $N(2) = 1$, and clearly $2 \leq N(a) < \infty$ for all $a \geq 3$. D. Singmaster [Sin1] proved that $N(a) = \mathrm{O}(\log a)$, and conjectured that $N(a) = \mathrm{O}(1)$. Later [Sin2] he even conjectured that $N(a) \leq 10$ for all $a \geq 2$. H.L. Abbott, P. Erdös and D. Hanson [AEH] showed that the average and normal order of $N(a)$ is 2, and that $N(a) = \mathrm{O}(\frac{\log a}{\log\log a})$. Maybe even the following is (too good to be) true.

Conjecture A *The equation* $\binom{n}{k} = \binom{m}{\ell}$ *has no nontrivial solutions but those given above.*

This conjecture would imply $N(a) \leq 8$ for all $a \geq 2$, and $N(a) \leq 6$ for all $a \geq 2$ with the exception of $a = 3003$, where the upper bound $N(a) = 6$ is attained infinitely often.

In this note we will contribute a little bit to the knowledge on this conjecture, and show that the special case $\binom{n}{3} = \binom{m}{4}$ has essentially been settled over 30 years ago by L.J. Mordell, without anybody having realized this (so it seems). The special cases $\binom{n}{2} = \binom{m}{3}$ and $\binom{n}{2} = \binom{m}{4}$ have been settled before, but by much more complicated methods than we (and Mordell) need. Further, we will also prove a partial result on *rational* solutions of $\binom{n}{3} = \binom{m}{4}$. We restrict ourselves entirely to elementary methods, i.e. the deepest mathematics we require are only the first essentials of algebraic number theory.

2 Integral solutions

In the context of diophantine equations, it's a bit more natural to study the equation $\binom{n}{k} = \binom{m}{\ell}$ for the extended definition of $\binom{n}{k}$ to all $n, k \in \mathbb{Z}$ with $k \geq 0$, as follows:

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!}.$$

In this more general sense (and, by the way, also in the restricted sense), for fixed k, ℓ (with $k < \ell$) the equation $\binom{n}{k} = \binom{m}{\ell}$ has been completely solved in two cases only, namely the case $(k, \ell) = (2, 3)$ by È.T. Avanesov [Av] using Skolem's method, and the case $(k, \ell) = (2, 4)$, after Richard K. Guy had drawn attention to the problem in Section D3 of [G], by the present author [dW] and independently by Ákos Pintér [Pi], both using the Gelfond-Baker method.

It is the first purpose of this note to show that the case $(k, \ell) = (3, 4)$ is comparatively easy, as it is an almost trivial consequence of the result of L.J. Mordell [M1], which itself has a more or less elementary proof. In this paper, Mordell determines the products of 2 consecutive integers that are equal to products of 3 consecutive integers. It is quite remarkable that this connection between Mordell's well known result and our binomial diophantine equation seems to have been unnoticed for over 30 years.

So here's our first main theorem, which might come as a disappointment to the reader expecting nontrivialities.

Theorem 1 *The only solutions $n, m \in \mathbb{Z}$ to $\binom{n}{3} = \binom{m}{4}$ are the following trivial ones:*

$$(n, m) \in \{0, 1, 2\} \times \{0, 1, 2, 3\}, \quad (n, m) = (3, 4), (3, -1), (7, 7), (7, -4).$$

Proof Write out the equation $\binom{n}{3} = \binom{m}{4}$ as

$$\frac{1}{6}n(n-1)(n-2) = \frac{1}{24}m(m-1)(m-2)(m-3).$$

Suggested by symmetry we put

$$X = n - 1, \quad Y = \frac{1}{2}m(m-3),$$

and then we obtain the equation

$$Y^2 + Y = X^3 - X.$$

In other words, we are looking for products $Y(Y+1)$ of two consecutive integers being equal to products $(X-1)X(X+1)$ of three consecutive integers. Mordell's Theorem 2 below gives us all the solutions for (X, Y), which are easily traced back to the trivial solutions for (n, m) given above. This completes the proof. □

Theorem 2 (Mordell, 1963) *The only solutions in $X, Y \in \mathbb{Z}$ to the equation*

$$Y^2 + Y = X^3 - X$$

are the following 10*:*

$$(X, Y) \in \{-1, 0, 1\} \times \{-1, 0\}, \quad (X, Y) = (2, 2), (2, -3), (6, 14), (6, -15).$$

Theorem 2 was proved in an elementary way by L.J. Mordell [M1] in 1963 (see also Theorem 2 in Chapter 27 of his book [M2]). By 'elementary' we mean that the deepest results that are used are the explicit knowledge of a class group and generators of a unit group in a certain cubic number field. For a different approach, that seems to be more complicated, see Exercise 9.13 of J.H. Silverman's book [Sil]. We mention that a third line of proof (using much more machinery, both theoretical and computational) is made possible by the recent method of elliptic logarithms, developed independently by R.J. Stroeker and N. Tzanakis [ST], by J. Gebel, A. Pethö and H.G. Zimmer [GPZ] (see also the software package Simath [Simath]), and by N.P. Smart [Sm]. Below we will return to Mordell's proof.

3 Rational solutions

Note that we can even extend the definition of $\binom{n}{k}$ further, to $n \in \mathbb{Q}$ (of course we can just as well take $n \in \mathbb{R}$, or even $n \in \mathbb{C}$, but we do not want to leave the area of number theory). When we want to study the equation $\binom{n}{k} = \binom{m}{\ell}$ for fixed k, ℓ in this context, we enter the domain of arithmetic algebraic geometry.

In the case $(k, \ell) = (2, 3)$ the equation $\binom{n}{2} = \binom{m}{3}$ is a Weierstraß equation of an elliptic curve. This curve has trivial torsion, and rank 2, and the group of rational points is generated by $(n, m) = (1, 0)$ and $(n, m) = (1, 1)$. Now, using the addition law on the elliptic curve, one can start producing the infinitely many rational solutions. In other words, the set of solutions $n, m \in \mathbb{Q}$ of $\binom{n}{2} = \binom{m}{3}$ is infinite, but well understood. For practical computations with such elliptic curves it is useful to have available computer software such as Pari [Pari] and Apecs [Apecs] (see also [Sil]).

In the case $(k,\ell)=(2,4)$ the equation $\binom{n}{2}=\binom{m}{4}$ also is an equation of an elliptic curve. This curve has a torsion group of order 2, generated by $(n,m)=(0,1)$, and the free part of the group of rational points is of rank 2, and is generated by $(n,m)=(0,0)$ and $(n,m)=(1,1)$. Thus again the set of solutions $n,m\in\mathbb{Q}$ of $\binom{n}{2}=\binom{m}{4}$ is infinite, but well understood.

In the case $(k,\ell)=(3,4)$ things are different, because the algebraic curve defined by the equation $\binom{n}{3}=\binom{m}{4}$ has genus 2, and thus, by Faltings' work [F], has only finitely many rational points. It is notoriously difficult to solve such problems of explicit determination of rational or integral points on curves of genus >1. That we succeeded above in proving our Theorem 1 on the integral points on our curve $\binom{n}{3}=\binom{m}{4}$, is due to the remarkable fact that this curve is (in geometric language) a double cover of an elliptic curve, namely the one given by Mordell's equation $Y^2+Y=X^3-X$ (this is just a reformulation of our proof of Theorem 1 above). The rational points on this elliptic curve are again not too difficult to describe, in fact, that's what Silverman uses in his Exercise 9.13 referred to above. The curve has trivial torsion, rank 1, and the group of rational points is generated by $(X,Y)=(0,0)$.

It is an interesting challenge to find out, e.g. on the basis of the facts mentioned above, what can be said about the set of rational points on the curve $\binom{n}{3}=\binom{m}{4}$. With Apecs we searched for solutions coming from the rational points $N\cdot(0,0)$ on the elliptic curve $Y^2+Y=X^3-X$, for $|N|\le 50$ only (but note that the numerator and denominator of the second coordinate of $50\cdot(0,0)$ are already numbers of about 85 digits). So we feel safe to formulate the following guess.

Conjecture B *The only solutions $n,m\in\mathbb{Q}$ to $\binom{n}{3}=\binom{m}{4}$, besides the integral ones given in Theorem 1 above, are*

$$(n,m)=\left(\frac{5}{4},\frac{1}{2}\right),\left(\frac{5}{4},\frac{5}{2}\right).$$

It is the second theme of this note to extend Mordell's elementary proof of Theorem 2 [M1] to make a first step towards the solution of this problem. Our extension concerns so-called S-integral solutions, i.e. rational solutions of which the denominators have prime divisors from a fixed finite set of primes only. We now restrict ourselves to the set consisting of the prime 2. Thus we have the following result.

Theorem 3 *The only solutions $n,m\in\mathbb{Q}$ of which the denominators are powers of 2 to the equation $\binom{n}{3}=\binom{m}{4}$, are the ones given in Conjecture B above.*

Note that this result extends Theorem 1. Following the above proof of Theorem 1, it is clear that Theorem 3 is a consequence of the following result, which is an analogous extension to the S-integral case of Mordell's Theorem 2.

Theorem 4 *The only solutions $X, Y \in \mathbb{Q}$ of which the denominators are powers of 2 to the equation $Y^2 + Y = X^3 - X$, besides the integral ones given in Theorem 2 above, are*

$$(X,Y) = \left(\frac{1}{4}, \frac{-5}{8}\right), \left(\frac{1}{4}, \frac{-3}{8}\right), \left(\frac{161}{16}, \frac{-2065}{64}\right), \left(\frac{161}{16}, \frac{2001}{64}\right).$$

4 Proof of Theorem 4

We will now prove Theorem 4, partly following, and partly extending the line of argument in Mordell's original proof of Theorem 2 [M1]. Note that our proof is completely elementary.

Proof of Theorem 4 We see at once that there is an integer $k \geq 0$, and integers X_1, Y_1, such that

$$X = \frac{X_1}{2^{2k}}, \quad Y = \frac{Y_1}{2^{3k}}.$$

Then the equation $Y^2 + Y = X^3 - X$ leads to

$$Y_1^2 + 2^{3k} Y_1 = X_1^3 - 2^{4k} X_1.$$

The idea is to complete the square in the left hand side of the equation, and then factor both sides in the ring of integers of an appropriate number field. For convenience we put

$$U = 2X_1, \quad V = 2Y_1 + 2^{3k},$$

and so obtain the equation

$$2V^2 = U^3 - 2^{4k+2} U + 2^{6k+1}, \tag{1}$$

in which the left hand side has the obvious factorization $2 \times V \times V$ over $\mathbb{Z}$.

Let θ be any root of the polynomial $u^3 - 4u + 2$. Then the right hand side of equation (1) factors over the ring of integers $\mathcal{O}_{\mathbb{K}}$ of the cubic number field $\mathbb{K} = \mathbb{Q}(\theta)$ as

$$U^3 - 2^{4k+2} U + 2^{6k+1} = \left(U - \theta 2^{2k}\right)\left(U^2 + \theta 2^{2k} U + (-4 + \theta^2) 2^{4k}\right).$$

The following facts of the field $\mathbb{K}$ are well known (or can be computed easily, e.g. using packages such as Pari [Pari] or KANT [KANT], see also Cohen's book [C]): the field discriminant is $148 = 2^2\,37$, a $\mathbb{Z}$-basis for the ring of integers $\mathcal{O}_{\mathbb{K}}$ is $\{1, \theta, \theta^2\}$, the class group is trivial, and the free part of the unit group of $\mathcal{O}_{\mathbb{K}}$ is generated by

$$\epsilon_1 = -1 + \theta, \quad \epsilon_2 = 1 - 2\theta - \theta^2.$$

Further we have the following factorizations into prime ideals:

$$(2) = (\theta)^3, \quad (-4 + 3\theta^2) = (\theta)^2 (1 + \theta + \theta^2),$$

and we have

$$N\epsilon_1 = N\epsilon_2 = 1, \quad N\theta = -2, \quad N(1 + \theta + \theta^2) = 37.$$

Note that Mordell [M1] uses $-\epsilon_1^2 \epsilon_2 = 2\theta - 1$ instead of ϵ_2 as second fundamental unit, and $4\theta - 3 = \epsilon_1 (1 + \theta + \theta^2)$ instead of $1 + \theta + \theta^2$.

Let δ be the squarefree part of $U-\theta 2^{2k}$. If a prime element $\pi \in \mathcal{O}_{\mathbb{K}}$ divides δ, it divides 2 or V^2. In the latter case even π^2 divides $2V^2$, and because δ is squarefree, π must divide the other factor of the right hand side of (1), $U^2+\theta 2^{2k}U+(-4+\theta^2)2^{4k}$, too. But then π will divide any linear combination of $U-\theta 2^{2k}$ and $U^2+\theta 2^{2k}U+(-4+\theta^2)2^{4k}$, in particular it will divide

$$\left(U^2+\theta 2^{2k}U+(-4+\theta^2)2^{4k}\right)-\left(U+\theta 2^{2k+1}\right)\left(U-\theta 2^{2k}\right)=(-4+3\theta^2)2^{4k}.$$

In view of the above prime factorizations this leaves for π only the possibilities θ and $1+\theta+\theta^2$, up to units.

Hence we can write

$$U-\theta 2^{2k}=\delta \times \text{ a square}, \tag{2}$$

where

$$\delta=(-1)^a\epsilon_1^b\epsilon_2^c\theta^d(1+\theta+\theta^2)^e$$

for some $a,b,c,d,e \in \{0,1\}$, and the square is an algebraic integer, i.e. an element of $\mathcal{O}_{\mathbb{K}}$. For the norm of δ we have on the one hand

$$N\delta=(-1)^{a+d}2^d 37^e,$$

and on the other hand, by (1), it differs by a rational integral square factor from

$$N\left(U-\theta 2^{2k}\right)=U^3-2^{4k+2}U+2^{6k+1}=2V^2.$$

It follows that $a=d=1$ and $e=0$. This leaves us four possibilities for δ, namely

$$\delta \in \{-\epsilon_1\theta, -\epsilon_1\epsilon_2\theta, -\theta, -\epsilon_2\theta\}.$$

At this point, to show that two of these four cases do not admit solutions, we use an argument that we find somewhat more elegant and more general than Mordell's arguments (on p. 1351 of [M1]). We study the three embeddings $\sigma_1, \sigma_2, \sigma_3$ of $\mathbb{K}$ into $\mathbb{R}$. They send θ to $\sigma_1(\theta)=-2.21\ldots$, $\sigma_2(\theta)=0.53\ldots$, and $\sigma_3(\theta)=1.67\ldots$. Because

$$U^3-2^{4k+2}U+2^{6k+1}=\left(U-2^{2k}\sigma_1(\theta)\right)\left(U-2^{2k}\sigma_2(\theta)\right)\left(U-2^{2k}\sigma_3(\theta)\right)=2V^2$$

has to be positive, we have two possibilities: either $U>2^{2k}\sigma_3(\theta)$, or $2^{2k}\sigma_1(\theta)<U<2^{2k}\sigma_2(\theta)$. Because by (2) for each $i \in \{1,2,3\}$ the sign of $U-2^{2k}\sigma_i(\theta)$ has to be equal to the sign of $\sigma_i(\delta)$, we study the signs of these explicitly known numbers:

	θ	ϵ_1	ϵ_2	$-\epsilon_1\theta$	$-\epsilon_1\epsilon_2\theta$	$-\theta$	$-\epsilon_2\theta$
σ_1	$-$	$-$	$+$	$-$	$-$	$+$	$+$
σ_2	$+$	$-$	$-$	$+$	$-$	$-$	$+$
σ_3	$+$	$+$	$-$	$-$	$+$	$-$	$+$

This shows that in the case $U>2^{2k}\sigma_3(\theta)$ it must be true that $\delta=-\epsilon_2\theta$ (we call this *the first case*), and in the case $2^{2k}\sigma_1(\theta)<U<2^{2k}\sigma_2(\theta)$ we must have $\delta=-\theta$ (we call this *the second case*).

The first case.

Let us first treat the case $U > 2^{2k}\sigma_3(\theta)$, thus $\delta = -\epsilon_2\theta = -2+3\theta+2\theta^2$. Making explicit the square in (2), for some $A, B, C \in \mathbb{Z}$ we have

$$U - \theta 2^{2k} = (-2+3\theta+2\theta^2)(A+B\theta+C\theta^2)^2.$$

Working out the brackets and comparing coefficients, we find the following system of three quadratic equations:

$$\begin{aligned} A^2+3B^2+9C^2+3AB+6AC+8BC &= 0, && (3)\\ 3A^2+8B^2+20C^2+12AB+16AC+36BC &= -2^{2k}, && (4)\\ -2A^2-6B^2-16C^2-8AB-12AC-24BC &= U. \end{aligned}$$

We may assume without loss of generality that A, B, C are coprime, and that $B \geq 0$.

From now on our proof diverges from Mordell's proof. We feel that for the situation we're in, with k not necessarily zero, our line of argument works prettier, but this is to some extent a matter of taste.

We view equation (3) as a quadratic equation in the variable A. Its discriminant should be a square, if rational solutions are to exist. Hence for a $D \in \mathbb{Z}$ we have

$$D^2 = (3B+6C)^2 - 4(3B^2+8BC+9C^2) = B(4C-3B).$$

Here we are lucky, because the quadratic form in B, C in the right hand side factors over $\mathbb{Z}$. We let β be a prime divisor of the squarefree part of B. Then β divides also the squarefree part of $4C-3B$, and since β divides both B and $4C-3B$, we find that β divides $4C$. If β divides both B and C then (3) implies that β also divides A, and this contradicts (4). Hence $\beta = 2$, and by $B \geq 0$ our conclusion is that B is a square or twice a square.

In the case $B = E^2$ for an $E \in \mathbb{Z}$, also $4C-3B$ is a square, say F^2, and we have $D = \pm EF$. We now solve (3) for A:

$$A = -\frac{3}{2}B - 3C \pm \frac{1}{2}D,$$

and express everything in E, F. In this way we find

$$A = \frac{1}{4}(-15E^2 \pm 2EF - 3F^2), \quad B = E^2, \quad C = \frac{1}{4}(3E^2+F^2).$$

Because of symmetry ($F \leftrightarrow -F$) we may take the $\pm$-sign to be a $+$-sign. We insert the above expressions for A, B, C into equation (4), and obtain

$$\frac{1}{16}(-25E^4+12E^3F+18E^2F^2-4EF^3-F^4) = -2^{2k}.$$

We are lucky again, since the binary form in the left hand side of this equation factors over $\mathbb{Z}$, and we thus find

$$(E-F)(25E^3+13E^2F-5EF^2-F^3) = 2^m, \tag{5}$$

where $m = 2k+4$. Had we not been this lucky, we would have arrived at a so-called Thue-Mahler equation. Procedures for solving such equations are known (see [TW2]), but are far from elementary.

Before studying this equation, we first mention that the second case, when $B = 2E^2$, leads to the same expressions for A, B, C in terms of E, F as above, multiplied by a factor 2. Hence we find the same quartic equation (5), but this time with $m = 2k + 2$.

Returning to equation (5), let us write $(E, F) = (-1)^g 2^h (P, Q)$ for some nonnegative integers g, h, such that P, Q are coprime, and $P > Q$. Now we proceed to solve

$$(P - Q)(25P^3 + 13P^2Q - 5PQ^2 - Q^3) = 2^n,$$

with $n = m - 4h$. Because $P - Q$ divides 2^n, there is an integer $\ell \geq 0$ such that $P - Q = 2^\ell$. Substituting $P = Q + 2^\ell$ into the above equation we find

$$32Q^3 + 2^{\ell+5}3Q^2 + 2^{2\ell+3}11Q + 2^{3\ell}25 = 2^{n-\ell}. \tag{6}$$

If $\ell = 0$ then (6) immediately yields that $n = 0$. So we have to solve

$$4Q^3 + 12Q^2 + 11Q + 3 = 0,$$

which is easily seen to have only $Q = -1$ as integral solution. It leads to $P = 0$, and, using the fact that A, B, C are coprime, further to $(E, F) = (0, -2)$ with $m = 4$, and to $(A, B, C) = (-3, 0, 1)$ with $k = 0$. Finally, this gives $(U, V) = (2, \pm 1)$, and $(X, Y) = (1, 0), (1, -1)$.

If $\ell = 1$ then (6) becomes

$$32Q^3 + 192Q^2 + 352Q + 200 = 2^{n-1}.$$

The first terms $32Q^3$, $192Q^2$ and $352Q$ are all divisible by 32, whereas the last term 200 is only divisible by 8, and not anymore by 16. Hence the entire left hand side is divisible by 8 but not by 16, so $n - 1 = 3$, and we find the equation

$$Q^3 + 6Q^2 + 11Q + 6 = 0.$$

It has the solutions $Q = -3, -2, -1$, leading to $P = -1, 0, 1$. The case $(P, Q) = (-1, -3)$ leads to $(E, F) = (-1, -3)$ with $m = 4$, and to $(A, B, C) = (-9, 1, 3)$ with $k = 0$. Finally, this gives $(U, V) = (12, \pm 29)$, and $(X, Y) = (6, 14), (6, -15)$. The case $(P, Q) = (0, -2)$ does not satisfy the requirements of P, Q being coprime (and is seen to lead to the solutions found above at $\ell = 0$). The case $(P, Q) = (1, -1)$ leads to $(E, F) = (1, -1)$ with $m = 4$, and to $(A, B, C) = (-5, 1, 1)$ with $k = 0$. Finally, this gives $(U, V) = (4, \pm 5)$, and $(X, Y) = (2, 2), (2, -3)$.

It remains to treat the case $\ell \geq 2$. This time in (6) the last three terms $2^{\ell+5}3Q^2$, $2^{2\ell+3}11Q$ and $2^{3\ell}25$ are divisible by 64, whereas the first term $32Q^3$ is only divisible by 32, but not by 64. It follows that $n - \ell = 5$. Note that in Mordell's original work only $k = 0$ is treated, in which case $n \leq 4$, so that then the case $\ell \geq 2$ is trivial.

Putting, for convenience,

$$Z = Q + 2^\ell, \quad W = 2^{\ell-2},$$

we find the equation

$$Z^3 - 4ZW^2 + 2W^3 = 1. \tag{7}$$

Equation (7) is a so-called Thue equation, that we conjecture to have only the following solutions:

$$(Z, W) = (1, 2), (1, 0), (-1, -1), (-5, -3), (-31, 14).$$

This can probably be proved by the deep methods of the Gelfond-Baker method, cf. [TW1]. But for us it would be like firing a cannon to kill a mosquito, because all we need is those solutions of (7) for which W is a power of 2. This can be done in an elementary way as follows.

First we show that if $|W| \geq 2$ then $\left|\frac{Z}{W}\right| < 2.61$. Namely, let $\theta_1, \theta_2, \theta_3$ be the three roots of $t^3 - 4t + 2 = 0$ (thus the θ_i are the $\sigma_j(\theta)$ defined above, but not necessarily in the same order). The equation (7) now factors as

$$(Z - \theta_1 W)(Z - \theta_2 W)(Z - \theta_3 W) = 1,$$

and for a given solution Z, W we take indices such that

$$|Z - \theta_1 W| < |Z - \theta_2 W| < |Z - \theta_3 W|.$$

Either $|Z - \theta_1 W| \geq \frac{1}{2}|W| \min |\theta_i - \theta_j| > 0.567|W|$, and then

$$1 = \prod_{i=1}^{3} |Z - \theta_i W| > |Z - \theta_1 W|^3 \geq (0.567|W|)^3,$$

and then it follows that $|W| \leq 1$, or $|Z - \theta_1 W| < \frac{1}{2}|W| \min |\theta_i - \theta_j|$, and then for $k = 2, 3$ we find

$$|Z - \theta_k W| \geq |W||\theta_1 - \theta_k| - |Z - \theta_1 W| > \frac{1}{2}|W| \min |\theta_i - \theta_j| > 0.567|W|,$$

and thus by $|W| \geq 2$

$$\left|\frac{Z}{W}\right| \leq |\theta_1| + \left|\frac{Z}{W} - \theta_1\right| = |\theta_1| + \frac{1}{|Z - W\theta_2||Z - W\theta_3||W|} < 2.22 + \frac{1}{0.567^2|W|^3} < 2.61.$$

Next we show that when $Z \neq 1$ and ℓ is large, then so is $\left|\frac{Z}{W}\right|$. Namely, we look at (7) $\pmod{2^{2\ell-2}}$:

$$Z^3 = 4ZW^2 - 2W^3 + 1 = Z2^{2\ell-2} - 2^{3\ell-5} + 1 \equiv 1 \pmod{2^{2\ell-2}},$$

provided that $\ell \geq 3$, and it follows that

$$2^{2\ell-2} \bigm| (Z^3 - 1) = (Z - 1)(Z^2 + Z + 1).$$

Since $Z^2 + Z + 1$ is always odd, we have $Z \equiv 1 \pmod{2^{2\ell-2}}$, hence $Z = 1$ or $|Z| \geq 2^{2\ell-2} - 1$. In the latter case we must have

$$\left|\frac{Z}{W}\right| \geq \frac{2^{2\ell-2} - 1}{2^{\ell-2}} = 2^\ell - \frac{1}{2^{\ell-2}}.$$

Putting things together, on noting that $2^\ell - \frac{1}{2^{\ell-2}} < 2.61$ implies $\ell = 1$, we find for the case $\ell \geq 2$ only the possibilities $|W| \leq 1$ or $Z = 1$ (note that $\ell = 2$ implies $W = 1$). The solutions of (7) satisfying these conditions are easy to determine: the only one is $(Z, W) = (1, 2)$, with $\ell = 3$. It leads to $(P, Q) = (1, -7)$, and to $(E, F) = (1, -7)$ with $m = 8$, further to $(A, B, C) = (-44, 1, 13)$ with $k = 2$, to $(U, V) = (322, \pm 4066)$, and finally to $(X, Y) = \left(\frac{161}{16}, \frac{-2065}{64}\right), \left(\frac{161}{16}, \frac{2001}{64}\right)$.

The second case.

Now we treat the case $2^{2k}\sigma_1(\theta) < U < 2^{2k}\sigma_2(\theta)$ where $\delta = -\theta$. Note that in Mordell's original work only $k = 0$ is treated, in which case we have at once $-2 \leq U \leq 1$, which is trivial.

We proceed as in the first case above. So for some $A, B, C \in \mathbb{Z}$ we have

$$U - \theta 2^{2k} = -\theta(A + B\theta + C\theta^2)^2.$$

Working out the brackets and comparing coefficients, we find the following system of three quadratic equations:

$$\begin{aligned} -C^2 + AB + 4BC &= 0, & (8)\\ -A^2 - 4B^2 - 16C^2 - 8AC + 4BC &= -2^{2k}, & (9)\\ 2B^2 + 8C^2 + 4AC &= U. \end{aligned}$$

We may assume without loss of generality that A, B, C are coprime, and that $B \geq 0$.

We are lucky once more, in that equation (8) now gives at once

$$(C - 2B)^2 = B(A + 4B),$$

so that again B is a square or twice a square.

In the case $B = E^2$ we have $A + 4B = F^2$, and we may take $C = 2E^2 + EF$. We substitute this into (9), and thus obtain

$$12E^4 + 28E^3F + 24E^2F^2 + 8EF^3 + F^4 = 2^m \tag{10}$$

with $m = 2k$. And again, in the case $B = 2E^2$ we find the same equation (10), but with $m = 2k - 2$.

This time the binary form in the left hand side of (10) does not factor over $\mathbb{Z}$, so now we seem to have run out of luck, and have to turn to non-elementary methods such as [TW2]. But fortunately this is not so. To start with, if $m \geq 1$ then F is even, say $F = 2F_1$. Hence

$$2^{m-2} = 3E^4 + 14E^3F_1 + 24E^2F_1^2 + 16EF_1^3 + 4F_1^4,$$

and we see that if $m \geq 3$ then also E is even. This means that by dividing out common divisors of E, F all solutions can be traced back to solutions with $m \leq 2$.

Further, our luck is that (10) does not have any linear factors over $\mathbb{R}$. Using this, we observe that $x^4 + 8x^3 + 24x^2 + 28x + 12$ has as minimal value 1 (at $x = -1$), and then by (10) we get

$$2^m = E^4\left(\left(\frac{F}{E}\right)^4 + 8\left(\frac{F}{E}\right)^3 + 24\left(\frac{F}{E}\right)^2 + 28\frac{F}{E} + 12\right) \geq E^4.$$

But then we see $E^4 \leq 2^m \leq 4$, hence $|E| \leq 1$. Now it is easily seen that in fact there are only three solutions: $(E, F) = (0, 1), (1, -1), (1, -2)$. The case $(E, F) = (0, 1)$ with $m = 0$ leads to $(A, B, C) = (1, 0, 0)$ with $k = 0$, further to $(U, V) = (0, \pm 1)$, and finally to $(X, Y) = (0, 0), (0, -1)$. The case $(E, F) = (1, -1)$ with $m = 0$ leads to $(A, B, C) = (-3, 1, 1)$ with $k = 0$, further to $(U, V) = (-2, \pm 1)$, and finally to $(X, Y) = (-1, 0), (-1, -1)$. The case $(E, F) = (1, -2)$ with $m = 2$ leads to $(A, B, C) = (0, 1, 0)$ with $k = 1$, further to $(U, V) = (2, \pm 2)$, and finally to $(X, Y) = \left(\frac{1}{4}, \frac{-5}{8}\right), \left(\frac{1}{4}, \frac{-3}{8}\right)$.

This completes the proof. $\square$

References

[AEH] H.L. Abbott, P. Erdös and D. Hanson, "On the number of times an integer occurs as a binomial coefficient", *American Mathematical Monthly* **81** [1974], 256–261.

[Av] È.T. Avanesov, "Solution of a problem on figurative numbers" (Russian), *Acta Arithmetica* **12** [1966/67], 409–420.

[C] Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[F] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Inventiones Mathematicae* **73** [1983], 349–366.

[G] Richard K. Guy, *Unsolved Problems in Number Theory*, Second Edition, Springer-Verlag, New York, 1994.

[GPZ] J. Gebel, A. Pethö and H.G. Zimmer, "Computing integral points on elliptic curves", *Acta Arithmetica* **68** [1994], 171–192.

[L] D.A. Lind, "The quadratic field $\mathbb{Q}(\sqrt{5})$ and a certain diophantine equation", *Fibonacci Quarterly* **6** [1968], 86–93.

[M1] L.J. Mordell, "On the integer solutions of $y(y+1) = x(x+1)(x+2)$", *Pacific Journal of Mathematics* **13** [1963], 1347–1351.

[M2] L.J. Mordell, *Diophantine equations*, Academic Press, New York, 1969.

[Pi] Ákos Pintér, "A note on the diophantine equation $\binom{x}{4} = \binom{y}{2}$", *Publ. Math. Debrecen* [1995], to appear.

[Sil] J.H. Silverman *The arithmetic of elliptic curves*, Springer-Verlag, Berlin, 1986.

[Sin1] D. Singmaster, "How often does an integer occur as a binomial coefficient?", *American Mathematical Monthly* **78** [1971], 385–386.

[Sin2] D. Singmaster, "Repeated binomial coefficients and Fibonacci numbers", *Fibonacci Quarterly* **13** [1975], 295–298.

[Sm] N.P. Smart, "S-integral points on elliptic curves", *Mathematical Proceedings of the Cambridge Philosophical Society* **116** [1994], 391–399.

[ST] R.J. Stroeker and N. Tzanakis, "Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arithmetica* **67** [1994], 177–196.

[TW1] N. Tzanakis and B.M.M. de Weger, "On the practical solution of the Thue equation", *Journal of Number Theory* **31** [1989], 99–132.

[TW2] N. Tzanakis and B.M.M. de Weger, "How to explicitly solve a Thue-Mahler equation", *Compositio Mathematica* **84** [1992], 223–288.

[dW] B.M.M. de Weger, "A binomial diophantine equation", *Quarterly Journal of Mathematics* [1995], to appear.

Software packages

[Apecs] APECS, software for elliptic curve computations, written by I. Connell in Maple, available by anonymous ftp from `math.mcgill.ca`.

[KANT] KANT V2, software for algebraic number theory computations, written by M. Pohst et al. in C on the Magma platform, available by anonymous ftp from `ftp.math.tu-berlin.de`.

[Pari] PARI, software for algebraic number theory computations, written by H. Cohen et al. in C and assembler languages, available by anonymous ftp from `megrez.math.u-bordeaux.fr`.

[Simath] SIMATH, software for number theory computations, written by H.G. Zimmer et al., available by anonymous ftp from `ftp.math.uni-sb.de`.