ON THE SOLUTION TO A GENERALIZED FERMAT EQUATION: ARITHMETIC AND COMBINATORICS

AMIR BARGHI AND JOHN CULLINAN

Abstract. The equation $(x \mid k)_n + (y \mid k)_n = (z \mid k)_n$ is a degree-n, falling-factorial version of the Fermat equation, where $(x \mid k)_n = x(x-k)(x-2k)\cdots(x-(n-1)k)$. We give an interpretation of the integral and rational solutions to this problem in terms of a probabilistic game and then use the theory of elliptic curves over function fields to generate all such solutions when $n = 3$. We conclude with some observations on the combinatorial properties of solutions for $n \geqslant 4$. This generalizes the recent work of Green [G].

1.. Introduction

It is now nearly 20 years since perhaps the most famous Diophantine problem was solved: there are no non-trivial integer solutions to the Fermat equation $x^n + y^n = z^n$ once $n > 2$. Variants on this problem abound and we take as our motivation a recent one which appeared in [G]; to describe it we recall the standard notation for the falling Pochammer symbol. Let K be a field of characteristic 0 and n a positive integer. Then for $x \in K$ we define

$$x^{\underline{n}} \stackrel{\text{def}}{=} x(x-1)\cdots(x-n+1).$$

In [G] Green posed the Diophantine problem of determining the integral solutions to $x^{\underline{n}} + y^{\underline{n}} = z^{\underline{n}}$. Such an equation defines an algebraic curve and the number of its rational points is related to its genus: if the genus is greater than 1, then there are only finitely many rational points and if the genus is 0, then if there is one rational point, there are infinitely many. The interesting case is that of genus 1, where the algebraic curve (an elliptic curve) may have a finite number of rational points or an infinite number.

In this paper we consider a generalization of Green's Diophantine equation and offer an interesting combinatorial interpretation of the solution. We begin by introducing the notation

$$(x \mid k)_n \stackrel{\text{def}}{=} x(x-k)(x-2k)\cdots(x-(n-1)k),$$

so that $x^{\underline{n}} = (x \mid 1)_n$. The aim of this paper is to interpret the solutions to

$$(x \mid k)_n + (y \mid k)_n = (z \mid k)_n \tag{1.1}$$

in the context of a probabilistic combinatorial variant on "roulette". We will describe the game in detail in the next section, but give a brief introduction here.

Let x be a positive integer and consider a circle ("wheel") divided into x arcs ("slots") of equal size, labeled clockwise with the integers $1, \ldots, x$. Fix a positive integer n and choose an $(n-1)$-tuple of nonnegative integers $(k_1, \ldots, k_{n-1})$ with the condition that $x \geqslant k_1 + \cdots + k_{n-1}$. In round 0 a player spins the wheel. Whatever slot the ball lands on, that slot along with the following $k_1 - 1$ slots (in clockwise order) will be considered "toxic." In each subsequent round (say the ith) if the ball lands in a toxic slot, the game is over. If not, that slot along with the following $k_i - 1$ non-toxic slots will henceforth be considered toxic (previously-declared toxic slots will be skipped over at this stage). The player wins if she survives n rounds, including the 0th. Assuming the ball is equally likely

to land on all slots, what is the probability of her winning? If X is the Bernoulli random variable for her success, it is easy to see that

$$\mathbb{P}(X = 1) = \frac{\prod_{i=0}^{n-1} (x - s_i)}{x^n}$$

where $s_i = \sum_{j=1}^{i} k_j$ with the assumption that $s_0 = 0$. In the special case $k_i = k$ for all $1 \leqslant i \leqslant n-1$, which is what we focus on for this paper, we have

$$\mathbb{P}(X = 1) = \frac{(x \mid k)_n}{x^n},$$

and the total number of cases where she wins is equal to $(x \mid k)_n$. Our main combinatorial result is the following (see the Section 2. for detailed definitions).

Theorem 1.1. *Let $y, z \in \mathbf{N}$ such that $m = z - y > 0$. Then the difference $(z \mid k)_n - (y \mid k)_n$ counts the number of winning cases in an n-round-altered game on a z-wheel with at least one landing in a safe zone of size m.*

In fact, this game is still valid if x is allowed to be a rational number. Returning to the Diophantine problem, we can then try to find all rational solutions to Equation (1.1). As in [G], the interesting case occurs when $n = 3$ and (1.1) defines an elliptic curve:

$$(x \mid k)_3 + (y \mid k)_3 = (z \mid k)_3 \,. \tag{1.2}$$

Our approach is to translate the rational solutions to (1.2) to those on an elliptic curve E defined over the function field $\mathbf{Q}(\lambda)$ and then use techniques of arithmetic geometry to determine all solutions. Our main number-theoretic result is the following.

Theorem 1.2. *With all notation as above, we have $E(\mathbf{Q}(\lambda)) \simeq \mathbf{Z} \times \mathbf{Z}$ with generators*

$$P \stackrel{\text{def}}{=} (3, -9/2) \qquad \textit{and} \qquad Q \stackrel{\text{def}}{=} (3 - 3\lambda, 9\lambda - 9/2).$$

Moreover, the rank r_λ of any specialization is $\geqslant 2$ unless $\lambda = 0$ or $\pm 1/2$. In those exceptional cases the Mordell-Weil groups are isomorphic to $\mathbf{Z}/3$ and $\mathbf{Z}/2 \times \mathbf{Z}/2 \times \mathbf{Z}$, respectively.

It is easy to pass from the λ-parameterization back to the k-parameterization, hence Theorem 1.2 describes all parametric solutions to (1.2). We note that there will be additional rational solutions not covered by Theorem 1.2 at specializations for which $r_\lambda > 2$. This project falls naturally into a larger class of problems where techniques of elliptic curves are used to solve combinatorial problems. We point out [BCN] and [BG] as two particular examples where the rational points on certain elliptic curves over function fields are used to parameterize rational 4- and 5-tilings of the unit square.

The layout of the paper is as follows. We begin with the game-interpretation of Equation (1.1). Then in Section 3. we give an alternative formulation in terms of elliptic curves over function fields. Finally, we give some concluding remarks and further directions for research.

2.. A Combinatorial Game

Recall the initial setup of the Introduction. We define an x-*wheel* to be a wheel with x slots, as above. Note that the game still makes sense on a continuous x-wheel, *i.e.* if $x, k \in \mathbf{R}_{>0}$ and at each round, arcs of total length k are declared toxic. In the continuous version we assume that the ball lands on the wheel uniformly at random. The probability of winning is still $(x \mid k)_n / x^n$. We start by rewriting Equation (1.1) with $n = 3$ as $(x \mid k)_3 = (z \mid k)_3 - (y \mid k)_3$ and focus on the right side. Each of these terms represent the number of winning cases on a z- and y-wheel, respectively. To have a combinatorial interpretation of this difference, we look at the game from a new perspective and alter the rules slightly.

Write $z = y + m$ with $m > 0$ and on a z-wheel declare m consecutive slots as a safe zone. If the ball lands in one of the remaining y slots these m would be skipped over. If the ball lands in one of the m slots, the player is safe for that round and k available non-toxic slots following the safe zone would be declared toxic. The rest of the rules are as before. We define this to be an n-*round-altered game*. We will start by showing that the number of winning games in an 3-round-altered game is equal to $(z \mid k)_3$.

Since $z = y + m$ we can write $(z \mid k)_3 = (y \mid k)_3 + 3my^2 + (3m^2 - 6km)y + (m^3 - 3km^2 + 2k^2m)$. A straightforward argument based on the number of landings in the safe zone shows the number of winning cases in the n-round-altered game is equal to

$$y(y-k)(y-2k) + m((y-k)(y-2k) + y(y-2k) + y(y-k)) + m^2((y-2k) + (y-k) + y) + m^3 =$$

$$(y \mid k)_3 + m(3y^2 - 6ky + 2k^2) + m^2(3y - 3k) + m^3 =$$

$$(y \mid k)_3 + 3my^2 + (3m^2 - 6km)y + (m^3 - 3km^2 + 2k^2) = (z \mid k)_3 .$$

Thus $(z \mid k)_3 - (y \mid k)_3$ counts the number of winning cases with at least one landing in the safe zone in the n-round-altered game. To establish this in general, we will use the well-known identity

$$(x \mid k)_n = \sum_{j=1}^{n} \begin{bmatrix} n \\ j \end{bmatrix} (-k)^{n-j} x^j \tag{2.1}$$

(see [AS, 24.1.3]) where $\begin{bmatrix} n \\ j \end{bmatrix}$ is the notation for the unsigned Stirling numbers of the first kind.

Lemma 2.1. *For $n \geqslant 1$ and $1 \leqslant i \leqslant n$,*

$$\sum_{j=i}^{n} \begin{bmatrix} n \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-j} y^{j-i} = \sum_{0 \leqslant a_1 < \cdots < a_i \leqslant n-1} \frac{(y \mid k)_n}{(y - a_1 k) \cdots (y - a_i k)}.$$

Proof. We will prove this lemma by induction on n, where $n = 1$ and 2 are trivial to check and $n = 3$ was shown above. Recall $\begin{bmatrix} n \\ j \end{bmatrix} = (n-1)\begin{bmatrix} n-1 \\ j \end{bmatrix} + \begin{bmatrix} n-1 \\ j-1 \end{bmatrix}$ and $\binom{j}{i} = \binom{j-1}{i} + \binom{j-1}{i-1}$. Therefore, for $1 \leqslant i \leqslant n$ we have

$$\begin{aligned}
&\sum_{j=i}^{n} \begin{bmatrix} n \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-j} y^{j-i} = \sum_{j=i}^{n} \left((n-1) \begin{bmatrix} n-1 \\ j \end{bmatrix} + \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \right) \binom{j}{i} (-k)^{n-j} y^{j-i} \\
&= (n-1)(-k) \sum_{j=i}^{n} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-1-j} y^{j-i} + \sum_{j=i}^{n} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \binom{j}{i} (-k)^{n-j} y^{j-i} \\
&= (-nk+k) \sum_{j=i}^{n-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-1-j} y^{j-i} + \sum_{j=i}^{n} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \binom{j-1}{i} (-k)^{n-j} y^{j-i} \\
&\quad + \sum_{j=i}^{n} \begin{bmatrix} n-1 \\ j-1 \end{bmatrix} \binom{j-1}{i-1} (-k)^{n-j} y^{j-i} \\
&= (-nk+k) \sum_{j=i}^{n-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-1-j} y^{j-i} + \sum_{j=i}^{n-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-1-j} y^{j-i+1} \\
&\quad + \sum_{j=i-1}^{n-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i-1} (-k)^{n-1-j} y^{j-(i-1)}
\end{aligned}$$

$$
\begin{aligned}
&= (y - nk + k) \sum_{j=i}^{n-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-1-j} y^{j-i} \\
&\quad + \sum_{j=i-1}^{n-1} \begin{bmatrix} n-1 \\ j \end{bmatrix} \binom{j}{i-1} (-k)^{n-1-j} y^{j-(i-1)} \\
&= (y - nk + k) \left(\sum_{0 \leqslant a_1 < \cdots < a_i \leqslant n-2} \frac{(y \mid k)_{n-1}}{(y - a_1 k) \cdots (y - a_i k)} \right) \\
&\quad + \left(\sum_{0 \leqslant a_1 < \cdots < a_{i-1} \leqslant n-2} \frac{(y \mid k)_{n-1}}{(y - a_1 k) \cdots (y - a_{i-1} k)} \right) \\
&= \sum_{0 \leqslant a_1 < \cdots < a_i \leqslant n-2} \frac{(y \mid k)_n}{(y - a_1 k) \cdots (y - a_i k)} \\
&\quad + \sum_{0 \leqslant a_1 < \cdots < a_{i-1} \leqslant n-2} \frac{(y \mid k)_{n-1} \, (y - nk + k)}{(y - a_1 k) \cdots (y - a_{i-1} k)(y - nk + k)} \\
&= \sum_{0 \leqslant a_1 < \cdots < a_i \leqslant n-2} \frac{(y \mid k)_n}{(y - a_1 k) \cdots (y - a_i k)} \\
&\quad + \sum_{0 \leqslant a_1 < \cdots < a_{i-1} \leqslant n-2, a_i = n-1} \frac{(y \mid k)_n}{(y - a_1 k) \cdots (y - a_i k)} \\
&= \sum_{0 \leqslant a_1 < \cdots < a_i \leqslant n-1} \frac{(y \mid k)_n}{(y - a_1 k) \cdots (y - a_i k)}. \qquad \square
\end{aligned}
$$

We are now ready to prove Theorem 1.1.

Theorem 2.1 (Theorem 1.1 in Section 1.)**.** *Let* $y, z \in \mathbf{N}$ *such that* $m = z - y > 0$*. Then the difference* $(z \mid k)_n - (y \mid k)_n$ *counts the number of winning cases in an* n*-round-altered game on a* z*-wheel with at least one landing in a safe zone of size* m*.*

Proof. Using identity (2.1) and applying Lemma 2.1, we have

$$\begin{aligned}
(y+m \mid k)_n - (y \mid k)_n &= \sum_{j=1}^{n} \begin{bmatrix} n \\ j \end{bmatrix} (-k)^{n-j} \left((y+m)^j - y^j \right) \\
&= \sum_{j=1}^{n} \begin{bmatrix} n \\ j \end{bmatrix} (-k)^{n-j} \left(\sum_{i=1}^{j} \binom{j}{i} m^i y^{j-i} \right) \\
&= \sum_{j=1}^{n} \sum_{i=1}^{j} \begin{bmatrix} n \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-j} m^i y^{j-i} \\
&= \sum_{i=1}^{n} \sum_{j=i}^{n} \begin{bmatrix} n \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-j} m^i y^{j-i} \\
&= \sum_{i=1}^{n} m^i \left(\sum_{j=i}^{n} \begin{bmatrix} n \\ j \end{bmatrix} \binom{j}{i} (-k)^{n-j} y^{j-i} \right) \\
&= \sum_{i=1}^{n} m^i \left(\sum_{0 \leqslant a_1 < \cdots < a_i \leqslant n-1} \frac{(y \mid k)_n}{(y-a_1 k) \cdots (y-a_i k)} \right).
\end{aligned}$$

A straightforward counting argument shows that the terms in this last sum counts the number of cases in an n-round-altered game with exactly i landing landings in the safe zone and $a_1, \ldots, a_i$ indicate the rounds in which the ball lands in the safe zone. □

Even though the above interpretation of $(z \mid k)_n - (y \mid k)_n$ seems *ad hoc* at first, there is in fact a good intuitive argument. In order that $(z \mid k)_n$ and $(y \mid k)_n$ be positive integers and count the number of winning cases for wheels of size z and y, respectively, we need to assume that $z \geqslant y \geqslant (n-1)k$. To avoid trivial cases, we need to make a slightly stronger assumption that $z > y > (n-1)k$. Note that at the end of any winning case using the z-wheel, there are $z-(n-1)k-1$ unused slots. But this is greater than $z-y-1 = m-1$. This shows that at least m slots are not used at the end of each winning case. Even though the position of these slots varies from case to case, their existence explains why the above argument should work: for every winning case there is a given set of safe slots. If we give *a priori* safe status to m fixed slots at the beginning the n-round-altered game, we should get the same number of winning cases, i.e., $(z \mid k)_n$. Removing the cases that never use the safe zone, i.e., $(y \mid k)_n$ results in the cases that use the safe zone at least once.

In the final section of the paper we will present additional combinatorial interpretations and identities related to Equation (1.1). In the next section we take a different approach to the equation and describe its rational solutions in the context of elliptic curves over function fields.

3.. Elliptic Curves

Fix $k \in \mathbf{Z}$ and note that for any integral solution (x, y, z) to (1.2) we may write $z = y + m$ for some $m \in \mathbf{Z}$. Then (1.2) reduces to

$$3my^2 + (3m^2 - 6km)y = x^3 - 3kx^2 + 2k^2x - (m^3 - 3km^2 + 2k^2m). \tag{3.2}$$

This defines (an affine patch of) a genus 1 curve over the function field $\mathbf{Q}(m, k)$; under the standard embedding into $\mathbf{P}^2$, the point $[0 : 1 : 0]$ is a $\mathbf{Q}(m, k)$-rational point on this curve. Thus, (3.2) defines an elliptic curve $E(m, k)$ over the function field $\mathbf{Q}(m, k)$.

From the point of view of elliptic curves, there is a convenient reparameterization of $E(m, k)$ that will ease computations. Let $\lambda \in \mathbf{Q}$ and write $k = \lambda m$. Then the elliptic curve

$E(m, \lambda m)$ may be put into short Weierstrass form through the substitutions

$$X = 3x/m - 3\lambda \qquad \text{and} \qquad Y = 9y/m + 9/2 - 9\lambda.$$

In fact, these substitutions show that the curve $E(m, \lambda m)$ is constant with respect to m. We therefore set the following notation that we will use for the rest of the paper. Let $E/\mathbf{Q}(\lambda)$ be the elliptic curve with Weierstrass equation

$$E: \qquad Y^2 = X^3 - 9\lambda^2 X + 27\lambda^2 - 27/4,$$

given by the above substitutions. By the Mordell-Weil theorem, the $\mathbf{Q}(\lambda)$-rational points of E form a finitely generated abelian group. That is, there is an isomorphism

$$E(\mathbf{Q}(\lambda)) \simeq \text{Tors} \times \mathbf{Z}^r,$$

where Tors is a finite abelian group and r is a non-negative integer. The main purpose of this section is to prove that Tors is trivial and that $r = 2$.

Some of our proofs rely on Silverman's Specialization Theorem [Si, Thm. III.11.4] for elliptic curves over function fields. To describe it, we begin by noting that E corresponds to an elliptic fibration $\mathscr{E} \to \mathbf{P}^1$ with generic fiber isomorphic to E. We write $\mathscr{E}_\lambda$ for the fiber above $\lambda \in \mathbf{P}^1(\mathbf{Q})$ and so $\mathscr{E}_\lambda$ defines an elliptic curve over $\mathbf{Q}$ for all but finitely many λ. For good specializations we set

$$\mathscr{E}_\lambda(\mathbf{Q}) \simeq \text{Tors}_\lambda \times \mathbf{Z}^{r_\lambda}.$$

In this context, the specialization theorem tell us $E(\mathbf{Q}(\lambda)) \leqslant \mathscr{E}_\lambda(\mathbf{Q})$ for all but finitely many $\lambda \in \mathbf{Q}$. That is, for all but finitely many λ we have $\text{Tors} \leqslant \text{Tors}_\lambda$ and $r \leqslant r_\lambda$. For completeness, note that the discriminant and j-invariant of E are given by

$$\Delta = 3^6(64\lambda^6 - 432\lambda^4 + 216\lambda^2 - 27) \qquad \text{and} \qquad j = 2^{12}3^9\lambda^6/\Delta,$$

respectively. We write Δ_λ and j_λ for the discriminant and j-invariants of the specializations $\mathscr{E}_\lambda$. Note that Δ, viewed as a polynomial over $\mathbf{Q}$, is irreducible. Thus $\mathscr{E}_\lambda$ is non-degenerate for *every* $\lambda \in \mathbf{Q}$. We are now prepared to prove Theorem 1.2.

Theorem 1.2 shows that the parametric solutions to (1.2) are generated by $\mathbf{Q}(\lambda)$-rational points on E. Tracing back through the substitutions, we find that the generators of $E(\mathbf{Q}(\lambda))$ give rise to the "obvious" solutions of (1.2)

$$P \mapsto (\lambda m + m, \lambda m - m) \text{ and}$$
$$Q \mapsto (m, 2\lambda m - m).$$

Any other parametric solution to (1.2) comes from an E-linear combination of P and Q. In terms of the original m and k, P and Q may be written as

$$(3m^2, -9m^3/2) \qquad \text{and} \qquad (3m^2 - 3km, -9m^2(m - 2k)/2),$$

respectively. We now prove Theorem 1.2 via a series of lemmas and propositions.

Lemma 3.2. *The torsion subgroup* Tors *of* $E(\mathbf{Q}(\lambda))$ *is trivial.*

Proof. If E had a non-trivial $\mathbf{Q}(\lambda)$-rational torsion point, then so would $\mathscr{E}_\lambda(\mathbf{Q})$ for all $\lambda \in \mathbf{Q}$ (of possibly different order). It is routine to check that $\mathscr{E}_1(\mathbf{Q})$ has trivial torsion, hence Tors is trivial. □

Lemma 3.3. *The points* P *and* Q *are independent on* E.

To prove Lemma 3.3 we will use the height pairing to show that P and Q are independent. Briefly, recall [Si, III.7], [Sh] that if E is an elliptic curve over a function field $k(\lambda)$ and

$P, Q \in E(k(\lambda))$, then the height pairing $\langle\ ,\ \rangle : E \times E \to \mathbf{Z}$ is a bilinear form on $E(k(\lambda))$ given by

$$\langle P, Q\rangle = \chi + P\cdot\mathcal{O} + Q\cdot\mathcal{O} - P\cdot Q - \sum_{\text{bad }\lambda} (P\cdot Q)_\lambda,$$
$$\langle P, P\rangle = 2\chi + 2\cdot P\cdot\mathcal{O} - \sum_{\text{bad }\lambda} (P\cdot P)_\lambda$$

where χ is the arithmetic genus of E, $P\cdot Q$ is the intersection number of the *divisors* P and Q, and $(P\cdot Q)_\lambda$ is the local intersection index at λ (the possible values can be found in the table in [Sh] preceding Theorem 8.7), where the sum is over the singular fibers. A collection of points $\{P_i\}_{i=1}^n \subset E(k(\lambda))$ spans a rank-n sublattice of the Mordell-Weil group precisely when the determinant $\det\left(\langle P_i, P_j\rangle\right)_{ij}$ is non-zero. We now apply this formalism in the context of our elliptic curve.

Proof of Lemma 3.3. It suffices to show that the determinant $\det\left(\begin{smallmatrix}\langle P,P\rangle & \langle P,Q\rangle\\ \langle Q,P\rangle & \langle Q,Q\rangle\end{smallmatrix}\right)$ is non-zero. Since E is a rational elliptic surface (the coefficients a_i of a minimal model have degree $\leqslant i$), we know that $\chi = 1$. We now compute

$$\langle P, P\rangle = 2 + 0 - 1 = 1,$$
$$\langle P, Q\rangle = \langle Q, P\rangle = 1 + 0 + 0 - 1 - 1/2,$$
$$\langle Q, Q\rangle = 2 + 0 - 1 = 1.$$

Substituting these values into the height pairing matrix shows the determinant equals $3/4$, whence P and Q are independent. □

The most difficult part of the proof of Theorem 1.2 is showing that $r = 2$. Our approach is via the Shioda-Tate formula, which relates the Mordell-Weil rank of an elliptic curve over a function field to the number and type of singularities of the bad fibers. The Shioda-Tate formula tells us the rank of the Mordell-Weil group $E(\overline{\mathbf{Q}}(\lambda))$, while Theorem 1.2 concerns that of $E(\mathbf{Q}(\lambda))$. To establish the latter we will need to find explicit $\overline{\mathbf{Q}}(\lambda)$-points on E and show they are independent, which we will do through the height pairing. Before we prove Theorem 1.2, we give a brief recap of the background in the context of our specific example E. For general details, see the original paper of Shioda [Sh]. Our approach to Theorem 1.2 follows that of [TZ].

The fibration $\mathscr{E} \to \mathbf{P}^1$ defines a rational elliptic surface, hence the Shioda-Tate formula [Sh] reduces to

$$\operatorname{rank} E(\overline{\mathbf{Q}}(\lambda)) = 8 - \sum_{\text{bad }\lambda} (m_\lambda - 1),$$

where the sum is taken over the singular fibers and m_λ denotes the geometric multiplicity of the fiber. Because Δ_λ is nonzero for all $\lambda \in \mathbf{Q}$, the only contribution to the sum comes from $\lambda = \infty$. Changing variables, let $t = 1/\lambda$ and take $z = t^2X$ and $w = t^3Y$ so that the fiber over ∞ is given by

$$w^2 = z^3 - 9t^2z - (27/4)t^6 + 27t^4$$

with discriminant $3^6t^6(27t^6 - 216t^4 + 432t^2 - 64)$. By the Kodaira classification of singularities, it follows that ∞ is a singularity of type I_0^* with 5 components. Hence the Mordell-Weil rank of $E(\overline{\mathbf{Q}}(\lambda))$ equals 4.

Shioda-Tate and Lemma 3.3 together show that $r \in \{2, 3, 4\}$. To prove $r = 2$ is more difficult, so we first give evidence for the equality. In [RS] it was shown for elliptic

fibrations satisfying the Tate conjecture that the rank r can be computed via

$$r = \operatorname{rank} E(\mathbf{Q}(\lambda)) = \operatorname*{Res}_{s=1} \sum_p \frac{\log p}{p^{s+1}} \sum_{\lambda \in \mathbf{P}^1(\mathbf{F}_p)} -a_p(\overline{\mathscr{E}_\lambda}).$$

Since E is a rational surface, the Tate conjecture holds and we may estimate the residue using the limit

$$\lim_{x\to\infty} \frac{1}{x} \sum_{p \leqslant x} \frac{\log p}{p} \left(\sum_{\lambda=0}^{p-1} -a_p(\overline{E_\lambda}) \right),$$

where $\overline{E_\lambda}$ denotes the reduction modulo p of E_λ at a good prime p and we define $a_p(\overline{E_\lambda}) = 0$ for singular fibers. Let $\delta(x) = \frac{1}{x} \sum_{p\leqslant x} \frac{\log p}{p} \left(\sum_{\lambda=0}^{p-1} -a_p(\overline{E_\lambda}) \right)$. Computations performed in PARI/GP suggest $r = 2$:

x	100	500	5000	10000	50000
$\delta(x)$	1.454	1.911	1.944	1.973	1.990

To show the rank of $E(\mathbf{Q}(\lambda))$ equals 2, we employ the following strategy: search for all points of $E(\mathbf{C}(\lambda))$ of the form

$$(a\lambda^2 + b\lambda + c, A\lambda^3 + B\lambda^2 + C\lambda + D),$$

where $a, b, c, A, B, C, D \in \mathbf{C}$ and show that there are four independent points on E. This amounts to computing the ideal I of the polynomial ring $\mathbf{C}[a, b, c, A, B, C, D]$ defined by the relations

$$\begin{aligned}
&-a^3 + A^2, -3ba^2 + 2BA, -3ca^2 - 3b^2 + 9a + 2CA + B^2,\\
&-6cba - b^3 + 9b + 2DA + 2CB, -3c^2a - 3cb^2 + 9c + 2DB + C^2 - 27, -3c^2b + 2DC,\\
&-c^3 + D^2 + 27/4,
\end{aligned}$$

and then computing the variety $V(I)$. One checks by computer algebra (we used Magma) that $V(I)$ is 0-dimensional and consists of 48 septuples of the form (a, b, c, A, B, C, D). We select two of these points and set

$$\begin{aligned}
R &\stackrel{\text{def}}{=} \left(-3\lambda + u/3 - 3/2, \left(-u^2/27 + u + 9/4\right)\lambda + u\right)\\
S &\stackrel{\text{def}}{=} ((-v^4/2187 + v^2/27)\lambda^2 - v^4/2916 - v^2/18 + 3/4,\\
&\qquad (-v^5/6561 + 2v^3/243 - v/3)\lambda^3 + v\lambda))
\end{aligned}$$

where u and v satisfy

$$2u^3 - 18u^2 + 243 = 0 \qquad \text{and} \qquad v^4 - 81v^2 + 6561 = 0,$$

respectively (with this information, one can easily show that $R, S \in E(\overline{\mathbf{Q}}(\lambda))$). At this point it is a computation (which we omit) to show that the height pairing matrix for the four points P, Q, R, S has non-zero determinant. From this we may conclude that the points P, Q, R, S generate a rank-4 sublattice of $E(\overline{\mathbf{Q}}(\lambda))$.

To see that $\operatorname{rank} E(\mathbf{Q}(\lambda)) = 2$ it is not sufficient simply to observe that R and S are not $\mathbf{Q}(\lambda)$-rational. Instead, we appeal to the fact that for good primes p, the reduction mod p map $E(\mathbf{Q}(\lambda)) \to \overline{E}(\mathbf{F}_p(\lambda))$ is injective [L, Proposition 6.2]. The prime $p = 7$ is good for E and one checks that $\overline{E}(\mathbf{F}_7(\lambda)) = \mathbf{Z} \times \mathbf{Z}$; this is easily performed in Magma via the command

```
k<t>:=FunctionField(GF(7));
E:=EllipticCurve([-9t^2,27t^2-27/4]);
MordellWeilGroup(E);
```

Moreover, the height pairing computed in Lemma 3.3 is invertible modulo 7. Altogether, this shows $\operatorname{rank} E(\mathbf{Q}(\lambda)) \leqslant 2$ and we knew *a priori* that $\operatorname{rank} E(\mathbf{Q}(\lambda)) \in \{2,3,4\}$. Therefore $\operatorname{rank} E(\mathbf{Q}(\lambda)) = 2$. □

To finish the proof of Theorem 1.2, we must show that P and Q generate the Mordell-Weil group $E(\mathbf{Q}(\lambda))$, rather than simply generate a sublattice. We use the same reasoning as in [L]: if P and Q generated an index-n sublattice of $E(\mathbf{Q}(\lambda))$, then the height pairing determinant would equal $3/(4n^2)$. But the denominator of a determinant of two points can be at most 4 because the singularity is of type I_0^* and the rest of the entries of the matrix are integral. Thus, $n = 1$. This finishes the proof of Theorem 1.2. □

4.. Conclusion

We conclude with some final observations on the combinatorial properties of the solutions to Equation (1.1) for general n and offer other avenues into enumerating the integral solutions. Let $S(z, m \mid k)_n$ denote the number of winning cases on a z-wheel with a safe zone of size m, increments of size k and playing n rounds (including the 0th round). We have already established that $S(y+m, m \mid k)_n = (y+m \mid k)_n - (y \mid k)_n$. It is easy to see that for fixed z, m and k

$$S(z, m \mid k)_n = \underbrace{\boxed{(z-m)S(z-k, m \mid k)_{n-1}}}_{\text{First landing is not in the safe zone}} + \underbrace{\boxed{m(z-m-k \mid k)_{n-1} + mS(z-k, m \mid k)_{n-1}}}_{\text{First landing is in the safe zone}}$$

$$= m(z-m-k \mid k)_{n-1} + zS(z-k, m \mid k)_{n-1}. \tag{4.3}$$

Note that $(z \mid k)_0 = 1$ and $S(z, m \mid k)_0 = 0$ and $S(z, m \mid k)_n = 0$ when $m + k > z > 0$ and $n \geqslant 1$. Using the recursion above it is easy to show that

$$S(z, m \mid k)_n = m\left[\sum_{i=1}^{N} (z \mid k)_{i-1} (z-m-ik \mid k)_{n-i}\right] + (z \mid k)_N S(z-Nk, m \mid k)_{n-N}$$

where $N = \min\{n-1, \lfloor (z-m)/k \rfloor\}$. For the game interpretation, we assumed that $z - m = y$ to be strictly greater than $(n-1)k$; hence, $N = n-1$ and we have

$$\begin{aligned} S(z, m \mid k)_n &= m\left[\sum_{i=1}^{n-1} (z \mid k)_{i-1} (z-m-ik \mid k)_{n-i}\right] + (z \mid k)_{n-1} S(z-(n-1)k, m \mid k)_1 \\ &= m\left[\sum_{i=1}^{n-1} (z \mid k)_{i-1} (z-m-ik \mid k)_{n-i}\right] + (z \mid k)_{n-1} m[z \geqslant m+nk]_\delta \\ &= m\left[\sum_{i=1}^{n-1} (z \mid k)_{i-1} (y-ik \mid k)_{n-i}\right] + (z \mid k)_{n-1} m[y \geqslant nk]_\delta, \end{aligned}$$

where $[\quad]_\delta$ is the Iverson bracket (*i.e.* $[X]_\delta$ equals 1 if X is true and equals 0 otherwise). Assuming that $y \geqslant nk$, we have

$$S(z, m \mid k)_n = \sum_{i=1}^{n} (z \mid k)_{i-1} m (y-ik \mid k)_{n-i}.$$

There is a combinatorial argument for the validity of this identity which is based on at which round the last landing in the safe zone happens. If we use a combinatorial argument

based on when the first landing the safe zone occurs, we have

$$S(z, m \mid k)_n = m \sum_{i=1}^{n} (y \mid k)_{i-1} (z - ik \mid k)_{n-i}.$$

Hence, we have the following proposition:

Proposition 1. *Let $n, k \in \mathbf{N}$. If y and z are positive integers such $z \geqslant y \geqslant nk$, then*

$$\sum_{i=1}^{n} (y \mid k)_{i-1} (z - ik \mid k)_{n-i} = \sum_{i=1}^{n} (z \mid k)_{i-1} (y - ik \mid k)_{n-i}. \qquad \square$$

Remark. It is easy to show that in fact Proposition 1 holds for y, z arbitrary integers.

Given $y, z \in \mathbf{Z}$, define $\mathfrak{S}(z, m \mid k)_n \stackrel{\text{def}}{=} (z \mid k)_n - (y \mid k)_n$ where $m = z - y$. Using the recursive relation

$$\mathfrak{S}(\zeta, m \mid k)_n = m(\zeta - m - k \mid k)_{n-1} + \zeta \mathfrak{S}(\zeta - k, m \mid k)_{n-1} \tag{4.4}$$

we will find the ordinary generating function $f_{\zeta,m,k}(t)$ for $\mathfrak{S}(\zeta, m \mid k)_n$ for fixed ζ, m and k, and $n \geqslant 1$. However, we first need to find $g_{\xi,k}(t)$ the ordinary generating function for $(\xi \mid k)_n$ for fixed ξ and k and $n \geqslant 1$. As shown in the previous section using techniques from algebraic number theory, finding the solutions to Equation (1.1) is an intricate problem. These intricacies will be reaffirmed below using techniques from algebraic combinatorics. To start, the generating function $g_{\xi,k}(t)$ satisfies the following linear differential equation:

$$g_{\xi,k}(t) = 1 + \xi t g_{\xi,k}(t) - kt^2 \frac{d}{dt} g_{\xi,k}(t),$$

whence $g_{\xi,k}(t) = e^{1/(kt)} t^{\xi/k} \left[k^{\xi/k} \Gamma\left(1 + \frac{\xi}{k}, \frac{1}{kt}\right) + C_{\xi,k} \right]$, where $\Gamma(a, x) = \int_x^\infty t^{a-1} e^{-t}\, dt$ is the incomplete gamma function. One can show

$$\lim_{t \to 0^+} e^{1/(kt)} t^{\xi/k} k^{z/k} \Gamma(1 + \xi/k, 1/(kt)) = 1;$$

so that $\lim_{t\to 0^+} e^{1/(kt)} t^{\xi/k} C_{\xi,k} = 0$. Moreover, since $\lim_{t\to 0^+} e^{1/(kt)} t^{\xi/k} = \infty$ we conclude that $C_{\xi,k} = 0$ and so

$$g_{\xi,k}(t) = e^{1/(kt)} t^{\xi/k} k^{\xi/k} \Gamma\left(1 + \frac{\xi}{k}, \frac{1}{kt}\right).$$

To derive an expression for $f_{\zeta,m,k}(t)$, one can directly use (4.4), or use its rewritten form as a sum

$$\mathfrak{S}(\zeta, m \mid k)_n = m \sum_{i=1}^{n} (\zeta \mid k)_{i-1} (\zeta - m - ik \mid k)_{n-i}. \tag{4.5}$$

We omit the details and conclude that

$$f_{\zeta,m,k}(t) = m \sum_{i=1}^{\infty} (\zeta \mid k)_{i-1}\ t^i\, g_{\zeta - m - ik,k}(t).$$

Using the closed formula for $g_{\zeta,k}(t)$, we have

$$f_{\zeta,m,k}(t) = m e^{1/(kt)} t^{(\zeta-m)/k} k^{(\zeta-m)/k} \sum_{i=1}^{\infty} \frac{(\zeta \mid k)_{i-1}}{k^i} \Gamma\left(\frac{\zeta - m}{k} - i + 1, \frac{1}{kt}\right).$$

With the assumption that $(\zeta - m)/k = \nu \in \mathbf{N}$, the above identity can be simplified further to

$$f_{\zeta,m,k}(t) = m \sum_{i=1}^{\infty} \sum_{j=0}^{\nu-i} (\zeta \mid k)_{i-1}\ \frac{(\nu - i)!}{j!} k^{\nu-i-j} t^{\nu-j} \tag{4.6}$$

using the fact that for $n \in \mathbf{N}$ and $x \in \mathbf{R}$, $\Gamma(n,x) = (n-1)!e^{-x}\sum_{j=0}^{n-1}\frac{x^j}{j!}$. (N.B. we cannot use this to tackle the general problem, as expected, since the coefficient of t^n in (4.6) leads us back to (4.5).) Finally, the fact that $(\zeta \mid k)_n = \sum_{i=0}^{\infty} \mathfrak{S}(\zeta - im, m \mid k)_n$ gives us

$$\sum_{n=0}^{\infty} (\zeta \mid k)_n t^n = \sum_{n=0}^{\infty}\sum_{i=0}^{\infty} \mathfrak{S}(\zeta - im, m \mid k)_n t^n = \sum_{i=0}^{\infty}\sum_{n=0}^{\infty} \mathfrak{S}(\zeta - im, m \mid k)_n t^n;$$

hence,

$$g_{\zeta,k}(t) = \sum_{i=0}^{\infty} f_{\zeta - im,m,k}(t).$$

In the aforementioned combinatorial game, instead of considering the special case discussed in this paper where $k_i = k$ for $1 \leqslant i \leqslant n-1$, one can consider the general case and see whether there is a combinatorial interpretation for the difference

$$\prod_{i=0}^{n-1}(z - s_i) - \prod_{i=0}^{n-1}(y - s_i).$$

This consideration motivates the following number theoretic problem: For $k_1, k_2 \in \mathbf{N}$, determine the non-trivial integer solutions to the equation

$$x(x-k_1)(x-(k_1+k_2)) + y(y-k_1)(y-(k_1+k_2)) = z(z-k_1)(z-(k_1+k_2)).$$

Another direction is determining non-trivial integer solutions to the (probabilistic) equation

$$\frac{(x \mid k)_n}{x^n} + \frac{(y \mid k)_n}{y^n} = \frac{(z \mid k)_n}{z^n}, \tag{4.7}$$

where $k, n \in \mathbf{N}$. This equation can be rewritten as

$$y^{n-1}z^{n-1}(x-k \mid k)_{n-1} + x^{n-1}z^{n-1}(y-k \mid k)_{n-1} = x^{n-1}y^{n-1}(z-k \mid k)_{n-1};$$

in particular, when $n = 2$, we have $yz(x-k) + xz(y-k) = xy(z-k)$ or equivalently, $xyz = k(yz + xz - xy)$.

Since $(x \mid k)_n$ is the number of favorable outcomes in the above variant of roulette on an x-wheel where the ball is equiprobable to land in any of the slots, one can consider an x-wheel where the ball lands in the ith slot with probability π_i and find the probability that the player survives n rounds of the game on this biased wheel. If $X_{\pi,k,n}$ is the Bernoulli random variable for player's success (surviving n rounds) on a biased x-wheel where $\pi = (\pi_1, \ldots, \pi_x)$, (4.7) can be generalized to

$$\mathbb{P}(X_{\pi,k,n} = 1) + \mathbb{P}(Y_{\pi,k,n} = 1) = \mathbb{P}(Z_{\pi,k,n} = 1).$$

Acknowledgements. We would like to thank Carl Pomerance, Peter Winkler, and Siman Wong for helpful comments and the referees for their careful reading of the manuscript.

References

[AS] M. Abramowitz, I.A. Stegun. *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables.* Dover, New York, 1972.

[BCN] J. Brady, G. Campbell, A. Nair. *Tiling the unit square with 5 rational triangles.* Rocky Mountain J. Math. **37** (2007), no. 2, 399–418.

[BG] A. Bremner, R.K. Guy. *The delta-lambda configurations in tiling the square.* J. Number Theory **32** (1989), no. 3, 263–280.

[G] M. Green. *A factorial power variation of Fermat's equation.* Rose-Hulman Undergrad. Math J. **13** (2012), no. 1, 43–51.

[L] R. van Luijk. *An elliptic K3 surface associated to Heron triangles.* J. Number Theory **123** (2007), no. 1, 92–119.

[RS] M. Rosen, J. Silverman. *On the rank of an elliptic surface.* Invent. Math. **133** (1998), no. 1, 43–67.

[Sh] T. Shioda. *On the Mordell-Weil lattices.* Comment. Math. Univ. St. Pauli. **39** (1990), no. 2, 211–240.
[Si] J. Silverman. *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, **151** Springer-Verlag, New York, 1994.
[TZ] J. Top, F. De Zeeuw. *Explicit elliptic K3 surfaces with rank 15.* Rocky Mountain J. Math. 39 (2009), no. 5, 1689–1697.

E-mail address: abarghi@bard.edi, cullinan@bard.edu