Formal Power Series and Algebraic Combinatorics
Séries Formelles et Combinatoire Algébrique
San Diego, California 2006

Combinatorial aspects of elliptic curves

Gregg Musiker

Abstract. Given an elliptic curve C, we study here the number $N_k = \#C(\mathbb{F}_{q^k})$ of points of C over the finite field $\mathbb{F}_{q^k}$. We obtain two combinatorial formulas for N_k. In particular we prove that $N_k = -\mathcal{W}_k(q,t)|_{t=-N_1}$ where $\mathcal{W}_k(q,t)$ is a (q,t)-analogue for the number of spanning trees of the wheel graph.

Résumé. Étant donnée une courbe elliptique C on étudie le nombre $N_k = \#C(\mathbb{F}_{q^k})$ de points de C dans le corps fini $\mathbb{F}_{q^k}$. On obtient deux formules combinatoires pour N_k. En particulier on démontre que $N_k = -\mathcal{W}_k(q,t)|_{t=-N_1}$ oú $\mathcal{W}_k(q,t)$ est une (q,t)-extension du nombre des arbres recouvrants du graphe roue.

1. Introduction

An interesting problem at the cross-roads between combinatorics, number theory, and algebraic geometry, is that of counting the number of points on an algebraic curve over a finite field. Over a finite field, the locus of solutions of an algebraic equation is a discrete subset, but since they satisfy a certain type of algebraic equation this imposes a lot of extra structure below the surface. One of the ways to detect this additional structure is by looking at field extensions: the infinite sequence of cardinalities is only dependent on a finite set of data. Specifically the number of points over $\mathbb{F}_q$, $\mathbb{F}_{q^2}$, $\dots$, and $\mathbb{F}_{q^g}$ will be sufficient data to determine the number of points on a genus g algebraic curve over any other algebraic field extension. This observation begs the question of how the points over higher field extensions correspond to points over the first g extensions. To see this more clearly, we specialize to the case of elliptic curves, where $g = 1$. Letting N_k equal the number of points on C over $\mathbb{F}_{q^k}$, we find a polynomial formula for N_k in terms of q and N_1. Moreover, the coefficients in our formula have a combinatorial interpretation related to spanning trees of the wheel graph.

2. The Zeta Function of a Curve

The zeta function of a curve C is defined to be the exponential generating function

$$Z(C,T) = \exp\left(\sum_{k\geq 1} N_k \frac{T^k}{k}\right).$$

A result due to Weil [**7**] is that the zeta function of an elliptic curve, in fact for any curve, $Z(C,T)$ is rational, and moreover can be expressed as

$$Z(C,T) = \frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-T)(1-qT)} = \frac{1-(\alpha_1+\alpha_2)T+\alpha_1\alpha_2 T^2}{(1-T)(1-qT)}.$$

The inverse roots α_1 and α_2 satisfy a functional equation which reduces to

$$\alpha_1\alpha_2 = q$$

in the elliptic curve case.

2000 *Mathematics Subject Classification.* Primary 11G07; Secondary 05C05.
Key words and phrases. elliptic curves, finite fields, zeta functions, spanning trees, Lucas numbers, symmetric functions.
The author thanks the National Science Foundation for their generous support.

Among other things, rationality and the functional equation implies that $N_k = 1 + q^k - \alpha_1^k - \alpha_2^k$, which can be written in plethystic notation as $p_k[1 + q - \alpha_1 - \alpha_2]$. As a special case,

$$\alpha_1 + \alpha_2 = 1 + q - N_1.$$

Hence we can rewrite the Zeta function $Z(C, T)$ totally in terms of q and N_1, hence all the N_k's are actually dependent on these two quantities. The first few formulas are given below.

$$\begin{aligned}
N_2 &= (2 + 2q)N_1 - N_1^2 \\
N_3 &= (3 + 3q + 3q^2)N_1 - (3 + 3q)N_1^2 + N_1^3 \\
N_4 &= (4 + 4q + 4q^2 + 4q^3)N_1 - (6 + 8q + 6q^2)N_1^2 + (4 + 4q)N_1^3 - N_1^4 \\
N_5 &= (5 + 5q + 5q^2 + 5q^3 + 5q^4)N_1 - (10 + 15q + 15q^2 + 10q^3)N_1^2 \\
&+ (10 + 15q + 10q^2)N_1^3 - (5 + 5q)N_1^4 + N_1^5
\end{aligned}$$

This data gives rise to our first observation.

Theorem 2.1.

$$N_k = \sum_{i=1}^{k} (-1)^{i+1} P_{i,k}(q) N_1^i$$

where the $P_{i,k}$'s are polynomials with positive integer *coefficients.*

We will prove this in the course of the deriviations in Section 3. Also see [**3**] for a direct proof. This result motivates the combinatorial question: what are the objects that the family of polynomials, $\{P_{i,k}\}$ enumerate?

3. The Lucas Numbers and a (q, t)-analogue

Definition 3.1. We define the $(q, t)-$**Lucas numbers** to be a sequence of polynomials in variables q and t such that $L_n(q, t)$ is defined as

$$L_n(q, t) = \sum_{S \subseteq \{1,2,\ldots,n\} \;:\; S \cap S_1^{(n)} = \phi} q^{\#\text{ even elements in } S}\, t^{\lfloor \frac{n}{2} \rfloor - \#S}. \tag{3.1}$$

Here $S_1^{(n)}$ is the circular shift of set S modulo n, i.e. element $x \in S_1$ if and only if $x - 1 \pmod{n} \in S$. In other words, the sum is over subsets S with no two numbers circularly consecutive.

These polynomials are a generalization of the sequence of Lucas numbers L_n which have the initial conditions $L_1 = 1$, $L_2 = 3$ (or $L_0 = 2$ and $L_1 = 1$) and satisfy the Fibonacci recurrence $L_n = L_{n-1} + L_{n-2}$. The first few Lucas numbers are

$$1, 3, 4, 7, 11, 18, 29, 47, 76, 123, \ldots$$

As described in numerous sources, e.g. [**1**], L_n is equal to the number of ways to color an $n-$beaded necklace black and white so that no two black beads are consecutive. You can also think of this as choosing a subset of $\{1, 2, \ldots, n\}$ with no consecutive elements, nor the pair $1, n$. (We call this circularly consecutive.) Thus letting q and t both equal one, we get by definition that $L_n(1, 1,) = L_n$.

We will prove the following theorem, which relates our newly defined $(q, t)-$Lucas numbers to the polynomials of interest, namely the N_k's.

Theorem 3.2.

$$1 + q^k - N_k = L_{2k}(q, t)\Big|_{t=-N_1} \tag{3.2}$$

for all $k \geq 1$.

To prove this result it suffices to prove that both sides are equal for $k \in \{1, 2\}$, and that both sides satisfy the same three-term recurrence relation. Since

$$\begin{aligned}
L_2(q, t) &= 1 + q + t \qquad \text{and} \\
L_4(q, t) &= 1 + q^2 + (2q + 2)t + t^2
\end{aligned}$$

we have proven that the initial conditions agree. Note that the sets of (3.1) yielding the terms of these sums are respectively

$$\{1\},\ \{2\},\ \{\ \}\quad \text{and} \quad \{1,3\},\ \{2,4\},\ \{1\},\ \{2\},\ \{3\},\ \{4\},\ \{\ \}.$$

It remains to prove that both sides of (3.2) satisfy the recursion

$$G_{k+1} = (1+q-N_1)G_k - qG_{k-1}$$

for $k \geq 1$.

Proposition 3.1. *For the $(q,t)-$Lucas Numbers $L_k(q,t)$ defined as above,*

$$L_{2k+2}(q,t) = (1+q+t)L_{2k}(q,t) - qL_{2k-2}(q,t). \tag{3.3}$$

Proof. To prove this we actually define an auxiliary set of polynomials, $\{\tilde{L}_{2k}\}$, such that

$$L_{2k}(q,t) = t^k \tilde{L}_{2k}(q,t^{-1}).$$

Thus recurrence (3.3) for the L_{2k}'s translates into

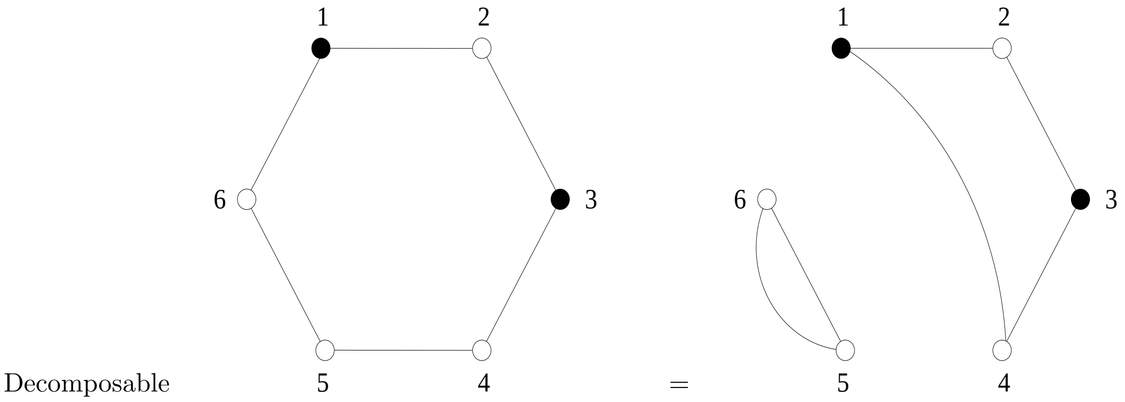
$$\tilde{L}_{2k+2}(q,t) = (1+t+qt)\tilde{L}_{2k}(q,t) - qt^2\tilde{L}_{2k-2}(q,t) \tag{3.4}$$

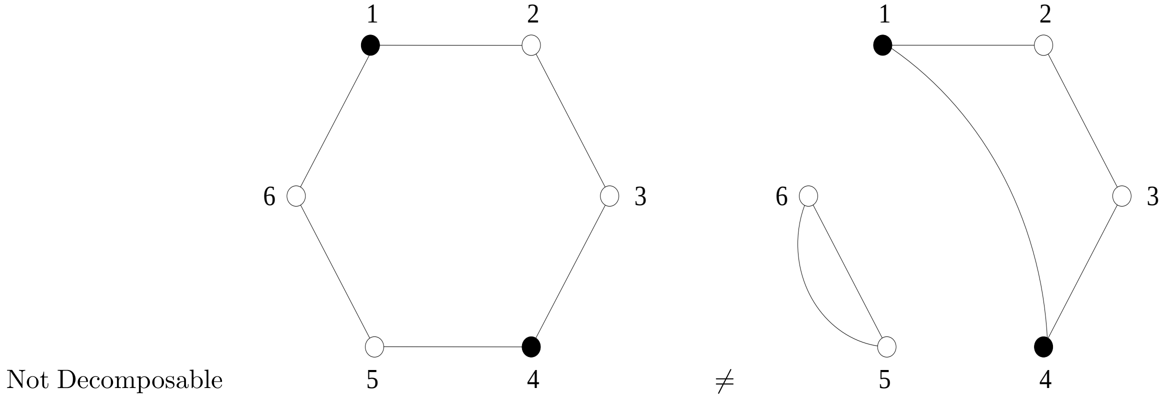
for the $\tilde{L}_{2k}$'s. The $\tilde{L}_{2k}$'s happen to have a nice combinatorial interpretation also, namely

$$\tilde{L}_{2k}(q,t) = \sum_{S\subseteq\{1,2,\ldots,2k\}\ :\ S\cap S_1^{(2k)}=\phi} q^{\#\text{ even elements in } S}\ t^{\#S}.$$

Recall our slightly different description which considers these as the generating function of 2-colored, labeled necklaces. We will find this terminology slightly easier to work with. We can think of the beads labeled 1 through $2k+2$ to be constructed from a pair of necklaces; one of length $2k$ with beads labeled 1 through $2k$, and one of length 2 with beads labeled $2k+1$ and $2k+2$.

Almost all possible necklaces of length $2k+2$ can be decomposed in such a way since the coloring requirements of the $2k+2$ necklace are more stringent than those of the pairs. However not all necklaces can be decomposed this way, nor can all pairs be pulled apart and reformed as a $(2k+2)$-necklace. For example, if $k=2$:





It is clear enough that the number of pairs is $\tilde{L}_2(q,t)\tilde{L}_{2k}(q,t) = (1+t+qt)\tilde{L}_{2k}(q,t)$. To get the third term of the recurrence, i.e. $qt^2\tilde{L}_{2k-2}$, we must define linear analogues, $\tilde{F}_n(q,t)$'s, of the previous generating function. Just as the $\tilde{L}_n(1,1)$'s were Lucas numbers, the $\tilde{F}_n(1,1)$'s will be Fibonacci numbers.

Definition 3.3. The (twisted) $(q,t)-$Fibonacci polynomials, denoted as $\tilde{F}_n(q,t)$, will be defined as

$$\tilde{F}_k(q,t) = \sum_{S\subseteq\{1,2,\ldots,k-1\}\ :\ S\cap(S_1^{(k-1)}-\{1\})=\phi} q^{\#\text{ even elements in } S}\ t^{\#S}.$$

The summands here are subsets of $\{1,2,\ldots,k-1\}$ such that no two elements are **linearly** consecutive, i.e. we now allow a subset with both the first and last elements. An alternate description of the objects involved are as (linear) chains of $k-1$ beads which are black or white with no two consecutive black beads. With these new polynomials at our disposal, we can calculate the third term of the recurrence, which is the difference between the number of pairs that cannot be recombined and the number of necklaces that cannot be decomposed.

Lemma 3.4. *The number of pairs that cannot be recombined into a longer necklace is $2qt^2\tilde{F}_{2k-2}(q,t)$.*

Proof. We have two cases: either both 1 and $2k+2$ are black, or both $2k$ and $2k+1$ are black. These contribute a factor of qt^2, and imply that beads 2, $2k$, and $2k+1$ are white, or that 1, $2k-1$, and $2k+2$ are white, respectively. In either case, we are left counting chains of length $2k-3$, which have no consecutive black beads. In one case we start at an odd-labeled bead and go to an evenly labeled one, and the other case is the reverse, thus summing over all possibilities yields the same generating function in both cases. □

Lemma 3.5. *The number of $(2k+2)$-necklaces that cannot be decomposed into a 2-necklace and a $2k$-necklace is $qt^2\tilde{F}_{2k-3}(q,t)$.*

Proof. The only ones the cannot be decomposed are those which have beads 1 and $2k$ both black. Since such a necklace would have no consecutive black beads, this implies that beads 2, $2k-1$, $2k+1$, and $2k+2$ are all white. Thus we are reduced to looking at chains of length $2k-4$, starting at an odd, 3, which have no consecutive black beads. □

Lemma 3.6. *The difference of the quantity referred to in Lemma 3.5 from the quantity in Lemma 3.4 is exactly $qt^2\tilde{L}_{2k-2}(q,t)$.*

Proof. It suffices to prove the relation

$$qt^2\tilde{L}_{2k-2}(q,t) = 2qt^2\tilde{F}_{2k-2}(q,t) - qt^2\tilde{F}_{2k-3}(q,t)$$

which is equivalent to

$$qt^2\tilde{L}_{2k-2}(q,t) = qt^2\tilde{F}_{2k-2}(q,t) + q^2t^3\tilde{F}_{2k-4}(q,t) \tag{3.5}$$

since

$$\tilde{F}_{2k-2}(q,t) = qt\tilde{F}_{2k-4}(q,t) + \tilde{F}_{2k-3}(q,t). \tag{3.6}$$

Note that identity (3.6) simply comes from the fact that the $(2k-2)$nd bead can be black or white. Finally we prove (3.5) by dividing by qt^2, and then breaking it into the cases where bead 1 is white or black. If bead 1 is white, we remove that bead and cut the necklace accordingly. If bead 1 is black, then beads 2 and $2k+2$ must be white, and we remove all three of the beads.

□

With this Lemma proven, the recursion for the $\tilde{L}_{2k}$'s, hence the L_{2k}'s follows immediately. □

PROPOSITION 3.2. *For an elliptic curve C with N_k points over $\mathbb{F}_{q^k}$ we have that*

$$1 + q^{k+1} - N_{k+1} = (1 + q - N_1)(1 + q^k - N_k) - q(1 + q^{k-1} - N_{k-1}).$$

PROOF. Recalling that for an elliptic curve C we have the identity $N_k = 1 + q^k - \alpha_1^k - \alpha_2^k$, we can rewrite the statement of this Proposition as

$$\alpha_1^{k+1} + \alpha_2^{k+1} = (\alpha_1 + \alpha_2)(\alpha_1^k + \alpha_2^k) - q(\alpha_1^{k-1} + \alpha_2^{k-1}). \tag{3.7}$$

Noting that $q = \alpha_1\alpha_2$ we obtain this Proposition after expanding out algebraically the right-hand-side of (3.7). □

With the proof of Proposition 3.1 and 3.2, we have proven Theorem 3.2.

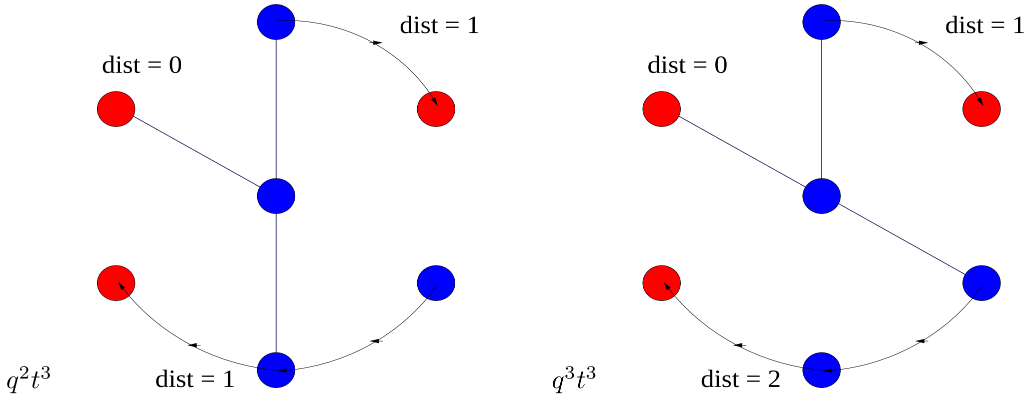
4. $(q,t)-$Wheel Numbers

Given that we found the Lucas numbers are related to the polynomial formulas $N_k(q, N_1)$, a natural question concerns how alternative interpretations of the Lucas numbers can help us better understand N_k. As noted in [**1**], [**4**], and [**5**, Seq. A004146], the sequence $\{L_{2n} - 2\}$ counts the number of spanning trees in the wheel graph W_n; a graph which consists of $n+1$ vertices, n of which lie on a circle and one vertex in the center, a hub, which is connected to all the other vertices. This combinatorial interpretation motivates the following definition.

DEFINITION 4.1.

$$\mathcal{W}_n(q,t) = \sum_{T \text{ a spanning tree of } W_n} q^{\text{sum of arc tail distance in } T}\, t^{\#\text{ spokes of } T}.$$

Here the exponent of t counts the number of edges emanating from the central vertex, and the exponent of q requires further explanation. We note that a spanning tree T of W_n consists of spokes and a collection of disconnected arcs on the rim. Further, since there are no cycles, each spoke will intersect exactly one arc. (An isolated vertex is considered to be an arc of length 1.) We imagine the circle being oriented clockwise, and imagine the tail of each arc being the vertex which is the sink for that arc. In the case of an isolated vertex, the lone vertex is the tail of that arc. Since the spoke intersects each arc exactly once, if an arc has length k, meaning that it contains k vertices, there will be k choices of where the spoke and the arc meet. We define the $q-$weight of an arc to be $q^{\text{ number of edges between the spoke and the tail}}$. We define the $q-$weight of the tree to be the product of the $q-$weights for all arcs on the rim of the tree.



This definition actually provides exactly the generating function that we desired, namely we have

Theorem 4.2 (Main Theorem).

$$N_k = -\mathcal{W}_k(q,t)\Big|_{t=-N_1}$$

for all $k \geq 1$.

Notice that this yields an exact interpretation of the $P_{i,k}$ polynomials as follows:

$$P_{i,k}(q) = \sum_{T \text{ a spanning tree of } W_n \text{ with exactly } i \text{ spokes}} q^{\text{sum of arc tail distance in } T}.$$

We will prove this Theorem in two different ways. The first method will utilize Theorem 3.2 and an analogue of the bijection given in [**1**] which relates perfect and imperfect matchings of the circle of length $2k$ and spanning trees of W_k. Our second proof will use the observation that we can categorize the spanning trees bases on the sizes of the various connected arcs on the rims. Since this categorization will correspond to partitions, this method will exploit formulas for decomposing p_k into a linear combination of h_λ's, as described in Section 6.

5. First Proof: Bijective

There is a simple bijection between subsets of $[2n]$ with no two elements circularly consecutive and spanning trees of the wheel graph W_n. We will use this bijection to give our first proof of Theorem 4.2. The bijection is as follows:

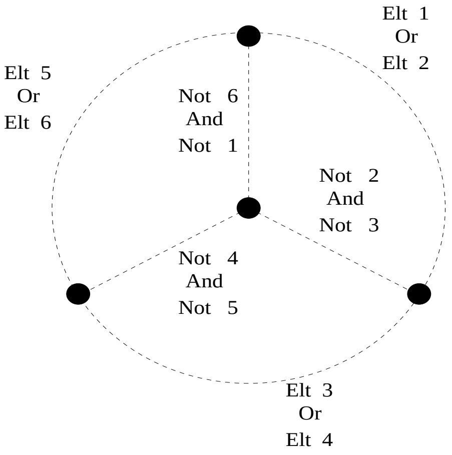
Given a subset S of the set $\{1, 2, \ldots, 2n-1, 2n\}$ with no circularly consecutive elements, we define the corresponding spanning tree T_S of W_n (with the correct q and t weight) in the following way:

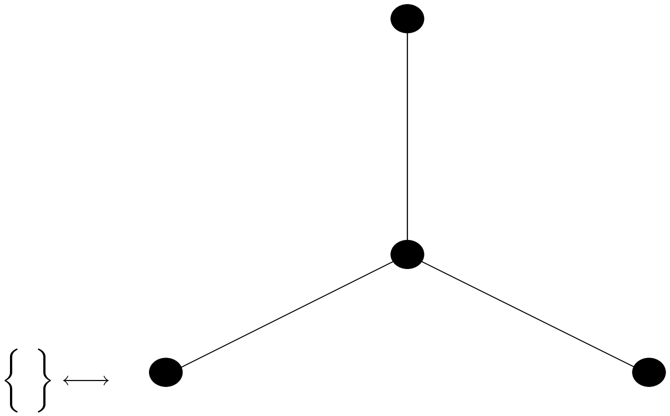
1) We will use the convention that the vertices of the graph W_n are labeled so that the vertices on the rim are w_1 through w_n, and the central vertex is w_0.

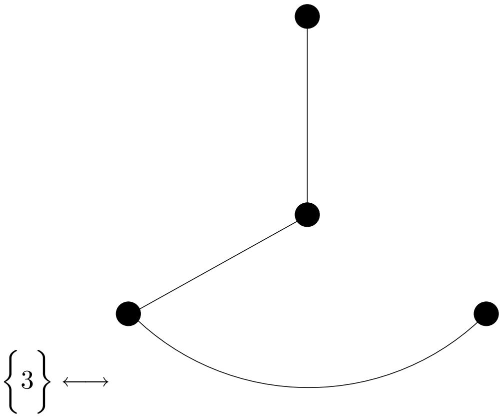
2) We will exclude the two subsets which consist of all the odds or all the evens from this bijection. Thus we will only be looking at subsets which contain $n-1$ or fewer elements.

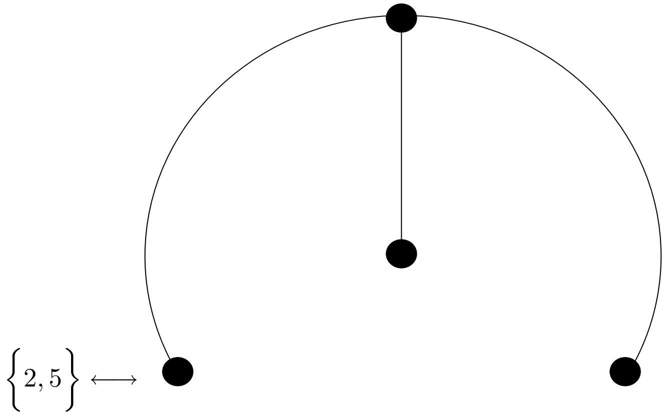
3) For $1 \leq i \leq n$, an edge exists from w_0 to w_i if and only if neither $2i-2$ nor $2i-1$ (element 0 is identified with element $2n$) is contained in S.

4) For $1 \leq i \leq n$, an edge exists from w_i to w_{i+1} (w_{n+1} is identified with w_1) if and only if element $2i-1$ or element $2i$ is contained in S.









Proposition 5.1. *Given this construction, T_S is in fact a spanning tree of W_n and further, tree T_S has the same $q-$ and $t-$weights as set S.*

Proof. Suppose that set S contains k elements. From our above restriction, we have that $0 \leq k \leq n-1$. Since S is a k-subset of a $2n$ element set with no circularly consecutive elements, there will be $n-k$ pairs $\{2i-2, 2i-1\}$ with neither element in set S, and k pairs $\{2i-1, 2i\}$ with one element in set S. Consequently, subgraph T_S will consist of exactly $(n-k)+k = n$ edges. Since $n = (\#\text{ vertices of } W_n) - 1$, to prove T_S is a spanning tree, it suffices to show that each vertex of W_n is included. For every oddly-labeled element of $\{1, 2, \ldots, 2n\}$, i.e. $2i-1$ for $1 \leq i \leq n$, we have the following rubric:

1) If $(2i-1) \in S$ then the subgraph T_S contains the edge from w_i to w_{i+1}.

2) If $(2i-1) \notin S$ and additionally $(2i-2) \notin S$, then T_S contains the spoke from w_0 to w_i.

3) If $(2i-1) \notin S$ and additionally $(2i-2) \in S$, then T_S contains the edge from w_{i-1} to w_i.

Since one of these three cases will happen for all $1 \leq i \leq n$, vertex w_i is incident to an edge in T_S. Also, the central vertex, w_0, has to be included since by our restriction, $0 \leq k \leq n-1$ and thus there are $n-k \geq 1$ pairs $\{2i-2, 2i-1\}$ which contain no elements of S.

The number of spokes in T_S is $n-k$ which agrees with the $t-$weight of a set S with k elements. Finally, we prove that the q-weight is preserved by induction on the number of elements in the set S. If set S has no elements, the $q-$weight should be q^0, and spanning tree T_S will consist of n spokes which also has $q-$weight q^0.

Now given a k element subset S $(0 \leq k \leq n-2)$, it is only possible to adjoin an odd number if there is a sequence of three consecutive numbers starting with an even, i.e. $\{2i-2, 2i-1, 2i\}$, which is disjoint from S. Such a sequence of S corresponds to a segment of T_S where a spoke and tail of an arc intersect. (Note this includes the case of vertex w_i being an isolated vertex.)

In this case, subset $S' = S \cup \{\text{odd}\}$ corresponds to $T_{S'}$, which is equivalent to spanning tree T_S except that one of the spokes w_0 to w_i has been deleted and replaced with an edge from w_i to w_{i+1}. The arc corresponding to the spoke from w_i will now be connected to the next arc, clockwise. Thus the distance between the spoke and the tail of this arc will not have changed, hence the $q-$weight of $T_{S'}$ will be the same as the $q-$weight of T_S.

Alternatively, it is only possible to adjoin an even number to S if there is a sequence $\{2i-1, 2i, 2i+1\}$ which is disjoint from S. Such a sequence of S corresponds to a segment of T_S where a spoke meets the *end* of an arc. (Note this includes the case of vertex w_i being an isolated vertex.)

Here, subset $S'' = S \cup \{\text{even}\}$ corresponds to $T_{S''}$, which is equivalent to spanning tree T_S except that one of the spokes w_0 to w_{i+1} has been deleted and replaced with an edge from w_i to w_{i+1}. The arc corresponding to the spoke from w_{i+1} will now be connected to the *previous* arc, clockwise. Thus the cumulative change to the total distance between spokes and the tails of arcs will be an increase of one, hence the $q-$weight of $T_{S''}$ will be q^1 times the $q-$weight of T_S.

Since any subset S can be built up this way from the empty set, our proof is complete via this induction. □

Since the two sets we excluded, of size k had $(q,t)-$weights q^0t^0 and q^kt^0 respectively, we have proven Theorem 4.2.

6. Brick Tabloids and Symmetric Function Expansions

Recall that we wrote N_k plethystically as $p_k[1+q-\alpha_1-\alpha_2]$. One advantage of plethystic notation is that we can exploit the following symmetric function identity [**6**, pg. 21]:

$$\sum_{n=0}^{\infty} h_n T^n = \prod_{k\in\mathcal{I}} \frac{1}{1-t_kT} = \exp\left(\sum_{n=1} p_n \frac{T^n}{n}\right) \tag{6.1}$$

where h_n and p_n are symmetric functions in the variables in $\mathcal{I}$. We note that $Z(C,T)$ resembles the right-hand-side of this identity, and consequently, if we had written $Z(C,T)$ as an ordinary power series

$$Z(C,T) = \sum_{k\geq 0} H_k T^k$$

we obtain that $H_k = h_k[1+q-\alpha_1-\alpha_2]$, where h_k denotes the kth homogeneous symmetric function.

Remark 6.1. In fact H_k has an algebraic geometric interpretation also, just as the N_k's did. H_k equals the number of positive divisors of degree k on curve C.

For a general curve we can thus, by plethysm, write cardinalities N_k in terms of H_1 through H_k, using the same coefficients as those that appear in the expansion of p_k in terms of h_1 through h_k:

$$N_k = \sum_{\lambda\vdash k} c_\lambda H_{\lambda_1} H_{\lambda_2} \cdots H_{\lambda_{|\lambda|}} \tag{6.2}$$

where the c_λ can be written down concisely as

$$c_\lambda = (-1)^{l(\lambda)-1} \frac{k}{l(\lambda)} \binom{l(\lambda)}{d_1, d_2, \dots, d_k} \tag{6.3}$$

where $l(\lambda)$ denotes the length of λ, which is a partition of k with type $1^{d_1}2^{d_2}\cdots k^{d_k}$.

We give one proof of this using Egecioglu and Remmel's interpretation involving weighted brick tabloids [**2**]. We will give another proof of this, involving a *possibly new* combinatorial interpretation for these coefficients, further on, in Section 7.

A brick tabloid [**2**] of type $\lambda = 1^{d_1}2^{d_2}\cdots k^{d_k}$ and shape μ is a filling of the Ferrers' Diagram μ with bricks of various sizes, d_1 which are 1×1, d_2 which are 2×1, d_3 which are 3×1, etc. The weight of a brick tabloid is the product of the lengths of all bricks at the end of the rows of the Ferrers' Diagram. We let $w(B_{\lambda,\mu})$ denote the weighted-number of brick tabloids of type λ and shape μ, where each tabloid is counted with multiplicity according to its weight.

Proposition 6.1 (Egecioglu-Remmel 1991, [**2**]).

$$p_\mu = \sum_\lambda (-1)^{l(\lambda)-l(\mu)} w(B_{\lambda,\mu})$$

and in particular

$$p_k = \sum_{\lambda} (-1)^{l(\lambda)-1} w(B_{\lambda,(k)}).$$

Brick tabloids of type λ and shape (k) are simply fillings of the $k \times 1$ board with bricks as specified by λ. Thus if divide these tabloids into classes based on the size of the last brick, we obtain, by counting the number of rearrangements, that there are

$$\binom{l(\lambda)-1}{d_1, \ldots, d_i - 1, \ldots, d_k}$$

brick tabloids of type (k) and shape $\lambda = 1^{d_1} 2^{d_2} \cdots k^{d_k}$ which have a last brick of length i.

Since each of these tabloids has weight i, summing up over all possible i, we get that (by abusing multinomial notation slightly)

$$\begin{aligned} w(B_{\lambda,(k)}) &= \sum_{i=0}^{k} i \cdot \binom{l(\lambda)-1}{d_1, \ldots, d_i - 1, \ldots, d_k} \\ &= \left(\sum_{i=0}^{k} i d_i\right) \cdot \binom{l(\lambda)-1}{d_1, \ldots, d_i, \ldots, d_k} \\ &= k \cdot \binom{l(\lambda)-1}{d_1, d_2, \ldots, d_k} = \frac{k}{l(\lambda)} \cdot \binom{l(\lambda)}{d_1, d_2, \ldots, d_k} \end{aligned}$$

Thus after comparing signs, we obtain that c_λ equals exactly the desired expression.

We now specialize to the case of $g = 1$. Here we can write H_k in terms of N_1 and q. We expand the series

$$Z(C,T) = \frac{1 - (1 + q - N_1)T + qT^2}{(1-T)(1-qT)}$$

with respect to T, and obtain $H_0 = 1$ and $H_k = N_1(1 + q + q^2 + \cdots + q^{k-1})$ for $k \geq 1$. Plugging these into formula (6.2), and using (6.3), we get polynomial formulas for N_k in terms of q and N_1, which in fact are an alternative expression for the formulas found in section 2.

$$N_k = \sum_{\lambda \vdash k} (-1)^{l(\lambda)-1} \frac{k}{l(\lambda)} \binom{l(\lambda)}{d_1,\ d_2,\ \ldots\ d_k} \left(\prod_{i=1}^{l(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_i - 1})\right) N_1^{l(\lambda)}.$$

Thus using these alternative expressions for N_k, we have that Theorem 4.2 is equivalent to the statement

$$\mathcal{W}_k = \sum_{\lambda \vdash k} \frac{k}{l(\lambda)} \binom{l(\lambda)}{d_1,\ d_2,\ \ldots\ d_k} \left(\prod_{i=1}^{l(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_i - 1})\right) t^{l(\lambda)}.$$

7. Second Proof: Via Symmetric Functions

For our second proof of Theorem 4.2, we start with the observation that the sequence of lengths of all disjoint arcs on the rim of W_n corresponds to a partition of n. We will construct a spanning tree of W_n from the following choices:

First we choose a partition $\lambda = 1^{d_1} 2^{d_2} \cdots k^{d_k}$ of n. We let this dictate how many arcs of each length occur, i.e. we have d_1 isolated vertices, d_2 arcs of length 2, etc. Note that this choice also dictates the number of spokes, which is equal to the number of arcs, i.e. the length of the partition.

Second, we pick an arrangement of $l(\lambda)$ arcs on the circle. After picking one to start with, without loss of generality since we are on a circle, we have

$$\frac{1}{l(\lambda)} \binom{l(\lambda)}{d_1,\ d_2,\ \ldots\ d_k}$$

choices for such an arrangement.

Third, we pick which vertex w_i of the rim to start with. There are n such choices.

Fourth, we pick where the $l(\lambda)$ spokes actually intersect the arcs. There will be |arc| choices for each arc, and the $q-$weight of this sum will be $(1 + q + q^2 + \cdots + q^{|\text{arc}|})$ for each arc.

Summing up all the possibilities yields

$$\mathcal{W}_n = \sum_{\lambda \vdash n} \frac{n}{l(\lambda)} \binom{l(\lambda)}{d_1,\ d_2,\ \dots\ d_k} \Bigg(\prod_{i=1}^{l(\lambda)} (1 + q + q^2 + \cdots + q^{\lambda_i - 1}) \Bigg) t^{l(\lambda)}.$$

As noted in Section 6, these coefficients are exactly the correct expansion coefficients by identities (6.1), (6.3), and plethysm. Thus we have given a second proof of Theorem 4.2.

Remark 7.1. We note that in the course of this second proof we have obtained a combinatorial interpretation for the c_λ's that is distinct from the one given in Egecioglu and Remmel's paper [**2**]. In particular this interpretation does not require weighted counting, only signed counting. Instead of defining c_λ as $(-1)^{l(\lambda)-1} w(B_{\lambda,(k)})$, we could define it as

$$(-1)^{l(\lambda)-1} |CB_{\lambda,(k)}|$$

where we define a new combinatorial class of **circular brick tabloids** which we denote as $CB_{\lambda,\mu}$. We define this for the case of $\mu = (k)$ just as we defined the usual brick tabloids, except we are not filling a $k \times 1$ rectangle, but are filling an annulus of circumference k and width 1 with curved bricks of sizes designated by λ. In this way we mimic our construction of the spanning trees.

Additionally, by using the fact that the power symmetric functions are multiplicative, i.e. $p_\lambda = p_{\lambda_1} p_{\lambda_2} \cdots p_{\lambda_r}$, we are able to generalize our definition of circular brick tabloids to allow μ to be any partition. We simply let λ designate what collection of bricks we have to use, and μ determines the filling: we are trying to fill $l(\mu)$ concentric circles where each circle has μ_i spaces. To summarize,

$$p_\mu = \sum_\lambda (-1)^{l(\lambda)-l(\mu)} |CB_{\lambda,\mu}| h_\lambda.$$

Consequently, all identities of [**2**] now involve *cardinalities* of $B_{\lambda,\mu}$, $OB_{\lambda,\mu}$ (Ordered Brick Tabloids), or $CB_{\lambda,\mu}$ and signs depending on $l(\lambda)$ and $l(\mu)$, with no additional weightings needed.

8. Conclusion

The new combinatorial formula for N_k presented in this write-up appears fruitful. It leads one to ask how spanning trees of the wheel graph are related to points on elliptic curves. For instance, is there an involution on (weighted) spanning trees whose fixed points enumerate points on $C(\mathbb{F}_{q^k})$? The fact that the Lucas numbers also enter the picture is also exciting since the Fibonacci numbers and Lucas numbers have so many different combinatorial interpretations, and there is such an extensive literature about them. Perhaps these combinatorial interpretations will lend insight into why N_k depends only on the finite data of N_1 and q for an elliptic curve, and how we can associate points over higher extension fields to points on $C(\mathbb{F}_q)$.

9. Ackowledgements

The author would like to thank Adriano Garsia for his support and many helpful conversations.

References

[1] A. Benjamin and C. Yerger, Combinatorial Interpretations of Spanning Tree Identities, *Bulletin of the Institute for Combinatorics and its Applications*, to appear.

[2] O. Egecioglu and J. Remmel, Brick Tabloids and the Connection Matrices Between Bases of Symmetric Functions, *Disc. Appl. Math.*, **34** (1991), 107-120.

[3] A. Garsia and G. Musiker, *Basics on Hyperelliptic Curves over Finite Fields*, in progress.

[4] B. R. Myers, Number of Spanning Trees in a Wheel, *IEEE Trans. Circuit Theory*, **18** (1971), 280-282.

[5] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/index.html.

[6] R. P. Stanley, *Enumerative Combinatorics Vol. 2, volume 62 of Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge (1999).

[7] A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris (1948).

Department of Mathematics, UCSD, San Diego, USA, 92037
E-mail address: gmusiker@math.ucsd.edu