Annoying Precision

"A good stack of examples, as large as possible, is indispensable for a thorough understanding of any concept, and when I want to learn something new, I make it my first job to build one." – Paul Halmos

Newton’s sums, necklace congruences, and zeta functions

August 23, 2009 by Qiaochu Yuan

The goal of this post is to give a purely combinatorial proof of Newton’s sums which would have interrupted the flow of the previous post (https://qchu.wordpress.com/2009/08/20/introduction-to-symmetric-functions/). Recall that, in the notation of the previous post, Newton’s sums (also known as the first Newton-Girard identity) state that

$$p_k - e_1 p_{k-1} \pm ... = (-1)^{k+1} k e_k.$$

One way to motivate a combinatorial proof is to recast the generating function interpretation appropriately. Given a polynomial $C(t)$ with non-negative integer coefficients and $C(0) = 0$, let $r_1, ... r_n$ be the reciprocals of the roots of $C(t) - 1 = 0$. Then

$$\frac{tC'(t)}{1 - C(t)} = \sum_{k \ge 1} p_k(r_1, ... r_n) t^k.$$

The left hand side of this identity suggests a particular interpretation in terms of the combinatorial species described by $C(t)$. Today we’ll describe this species when $C(t)$ is a polynomial with non-negative integer coefficients and then describe it in the general case, which will handle the extension to the symmetric function case as well.

The method of proof used here is closely related to a post I made previously about the properties of the Frobenius map, and at the end of the post I’ll try to discuss what I think might be going on.

Tilings and closed walks on graphs

The simplest way to set up the combinatorics of the proof is as follows. Suppose one has a collection, not necessarily finite, of tiles of various lengths and colors such that the number of colors of tile of a particular length is finite. Let c_k denote the number of colors of tiles of size k in this collection. This information can be organized in a generating function

$$C(t) = \sum_{k \ge 1} c_k t^k$$

and then one can place the tiles in various orders. Then the generating function $\frac{1}{1-C(t)}$ counts the number of tilings of a strip of length n by the above collection of tiles, since $C(t)^r$ counts the number of ways to place r tiles in linear order by the total length of the tiles involved.

What we need is a corresponding combinatorial interpretation of the generating function $\frac{tC'(t)}{1-C(t)}$. The operation of sending $C(t)$ to $tC'(t)$ is known as **pointing**. It sends a sequence c_k to the sequence kc_k and has the following combinatorial interpretation: if we think of a tile of size k as being composed of k segments, then $tC'(t)$ describes the "pointed tiles," where one of these square segments has been distinguished, or pointed to. $\frac{tC'(t)}{1-C(t)}$ then counts the number of ways to pick out a pointed tile, then a sequence of regular tiles.

I claim that this description is equivalent to counting the number of **circular tilings**, defined as follows: distinguish a "starting tile" on a circle composed of n segments and place tiles from the collection $C(t)$ on this circle of total length n. This is equivalent to allowing the last tile in a regular tiling to "wrap around." The starting tile on the circle then points to a unique pointed tile, and counting counterclockwise from that tile one obtains a unique sequence of regular tiles. This construction might be familiar if you've ever encountered it in the case $C(t) = t + t^2$, where it gives a combinatorial description of the Lucas numbers (http://en.wikipedia.org/wiki/Lucas_number). Let a_k denote the number of circular tilings of length k; by definition, $a_0 = 0$. The equivalence of pointing and circularity implies the following result, which we re-prove for the sake of clarity.

Proposition: $a_k - c_1 a_{k-1} - ... - c_{k-1} a_1 = kc_k$.

Proof. Consider a circular tiling of length k and consider the first non-pointed tile in counterclockwise order. If it exists and has some length i, it has one of c_i colors and removing it produces a circular tiling of length $k - i$. The only tilings not of this form are the tilings with only one (pointed) tile of size k, of which there are kc_k.

In order to describe the connection to power sums, we now give a description of circular tilings in terms of closed walks on a certain directed graph G_C associated to any collection $C(t)$ of tiles, which is the final ingredient of the proof. The graph G_C consists of vertices $0, 1, 2, ...$ and edges defined as follows: there are edges $1 \to 0, 2 \to 1, 3 \to 2, ...$ and an additional c_i edges $0 \to i - 1$ for every i. Then we have the following result.

Proposition: For a fixed length, the number of closed walks in G_C from 0 to 0 is the number of regular tilings and the total number of closed walks is the number of circular tilings.

Corollary: If $C(t)$ is a polynomial, then a_k is the sum of the k^{th} powers of the reciprocals of the roots of $1 - C(t)$.

Proof. Choosing a vertex to step to from 0 is equivalent to choosing the length of a tile, and choosing an edge to use is equivalent to choosing its color. Once you are at vertex $i-1$, the only way to continue the walk is to take $i-1$ steps back to 0, so in total you have taken i steps corresponding to a particular color of tile of length i. Thus walks from 0 to 0 of a particular length are in one-to-one correspondence with tilings of the same length. Similarly, arbitrary closed walks start at some intermediate vertex which is not necessarily 0, and this is equivalent to pointing to a particular segment of the first tile.

To show that this implies the corollary, the first result implies that the eigenvalues of G_C are, at least in the generic case, identical to the reciprocals of the roots of $1-C(t)$. Arbitrary closed walks are then counted by traces of powers of the adjacency matrix of G_C, so they are power sums in the eigenvalues. One can also show the first part of the corollary by observing that the adjacency matrix of G_C is a companion matrix (http://en.wikipedia.org/wiki/Companion_matrix).

As stated, we have only proven Newton's sums for roots of polynomials with a restriction on their coefficients. This restriction can be removed by regarding c_i as a weight, i.e. a formal variable, and weighting a walk by the product of the weights of the edges involved. One can then regard the roots of the polynomial $1-C(t)$ also as formal variables which determine the formal variables c_i; the proof still carries through because all of the counting above can be done in a weighted fashion, and because we can regard the roots of $1-C(t)$ as formal, we can also allow countably many of them (hence tiles of arbitrary size) and prove Newton's sums in the full ring of symmetric functions.

Necklace congruences

From here on the graph G_C above is to replaced by an arbitrary directed graph G, and instead of circular tilings we will consider more general closed walks. a_k will still denote the number of closed walks of length k. More generally we can take $a_k = \text{tr } \mathbf{A}^k$ where $\mathbf{A}$ is a square matrix with integer entries (and not necessarily finite-dimensional, as long as all but finitely many of the diagonal entries of $\mathbf{A}^k$ are nonzero for every k.)

As I remarked in a previous post (https://qchu.wordpress.com/2009/06/09/the-magic-of-the-frobenius-map-ii/), the cyclic group C_n acts on closed walks of length n in the obvious way, and the fixed points of an element of order $\frac{n}{d}$ consist precisely of $\frac{n}{d}$ copies of a closed walk of length d. There are $\varphi\left(\frac{n}{d}\right)$ such elements, so by Polya's theorem the number of orbits of closed walks is

$$o_n = \frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) a_d.$$

Thinking of this result as a significant generalization of Fermat's little theorem, we will refer to the congruence $\sum_{d|n} \varphi\left(\frac{n}{d}\right) a_d \equiv 0 \bmod n$ as the **first** necklace congruence, since one can interpret it as talking about circular tilings, which generalize necklaces (http://en.wikipedia.org/wiki/Necklace_%28combinatorics%29).

When $n = p^k$ is a power of a prime, the first necklace congruence implies what Richard Lipton calls Fermat's little theorem for matrices (http://rjlipton.wordpress.com/2009/08/07/fermats-little-theorem-for-matrices/), which states that

$$a_{p^k} \equiv a_{p^{k-1}} \bmod p^k.$$

Using the Frobenius map appears to get you at best $a_{p^k} \equiv a_1 \bmod p$. I don’t know an algebraic proof of the stronger statement. A remarkable corollary of this result is that $\lim_{k \to \infty} a_{p^k}$ is a well-defined p-adic number (http://en.wikipedia.org/wiki/P-adic_number). This fact appears to be related to taking the algebraic closure of a variety over $\mathbb{F}_p$, which I’ll attempt to discuss later.

Instead of counting orbits, we may consider the following property of closed walks: each has a unique fundamental period, and a closed walk of length n and period $d, d|n$ consists precisely of $\frac{n}{d}$ copies of an *aperiodic* closed walk of length d. The aperiodic closed walks of length d are precisely those in full orbits under the group action of C_d, and we cannot count them directly using Polya theory; however, we can use Mobius inversion (http://en.wikipedia.org/wiki/M%C3%B6bius_inversion_formula). Let b_d denote the number of full orbits of closed walks under the group action of C_d; then db_d denotes the number of closed walks in all such orbits, and since every closed walk consists of copies of some such walk, we obtain

$$\sum_{d|n} db_d = a_n.$$

By Mobius inversion, it follows that

$$b_n = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d.$$

Because the case n prime here also implies Fermat’s little theorem, we will refer to the congruence $\sum_{d|n} \mu\left(\frac{n}{d}\right) a_n \equiv 0 \bmod n$ as the **second** necklace congruence.

We have just proven the necklace congruences for a fairly general class of sequences a_n. It’s a good exercise to show that they imply each other, but that fact won’t be necessary for our next application.

Zeta functions

As we have seen, Newton’s sums is equivalent to the identity

$$\frac{1}{1 - C(t)} = \exp\left(\sum_{k \ge 1} p_k(r_1, ...r_n) \frac{t^k}{k}\right)$$

which can be seen by dividing the first statement by t, integrating, and then exponentiating. The graph-theoretic argument above shows that this identity can be phrased as follows: if G is a graph with adjacency matrix $\mathbf{A}$ and $\mathbf{I}$ denotes the corresponding identity matrix, then

$$\det(\mathbf{I} - t\mathbf{A})^{-1} = \exp\left(\sum_{k \ge 1} \left(\text{tr } \mathbf{A}^k\right) \frac{t^k}{k}\right).$$

This identity is in turn equivalent to Jacobi’s identity $\det \exp \mathbf{M} = \exp \text{tr } \mathbf{M}$ with $\mathbf{M} = \log(\mathbf{I} - t\mathbf{A})^{-1}$. Introducing a second matrix $\mathbf{B}$, we now obtain

$$\frac{\det(\mathbf{I} - t\mathbf{B})}{\det(\mathbf{I} - t\mathbf{A})} = \exp\left(\sum_{k \ge 1} \left(\text{tr } \mathbf{A}^k - \text{tr } \mathbf{B}^k\right) \frac{t^k}{k}\right).$$

Of course a similar result is true if the determinants are replaced by power series, but we won't need that result for now.

Corollary: Let a_n be an integer sequence such that $\exp \left(\sum_{k \ge 1} a_k \frac{t^k}{k} \right)$ is a rational function with integer-coefficient numerator and denominator $P(t), Q(t) \in \mathbb{Z}[t]$ satisfying $P(0) = Q(0) = 1$. Then a_n satisfies the necklace congruences.

As a special case, this is known to be true for varieties over finite fields (http://en.wikipedia.org/wiki/Local_zeta-function), where a_k denotes the number of points on a variety V over the finite field $\mathbb{F}_{p^k}$, and the corresponding function is called a local zeta function in part because it satisfies an analogue of the Riemann hypothesis.

What's the connection between local zeta functions and our discussion? Well, at the heart of the construction of the local zeta function is the action of the Frobenius map $f : x \mapsto x^p$ on the points of a variety V over $\overline{\mathbb{F}_p}$. The fixed points of f^k are precisely the points of V over $\mathbb{F}_{p^k}$, so the local zeta function can be written

$$\zeta_V(t) = \exp \left(\sum_{k \ge 1} \left(\text{Fix } f^k \right) \frac{t^k}{k} \right).$$

And the fixed-point function is a trace, since f acts as a linear operator on $\overline{\mathbb{F}_p}$ as a vector space over $\mathbb{F}_p$. Under a suitable choice of basis, f acts by permutation, and then $\text{Fix } f^k = \text{tr } f^k$ as desired.

I may not know anything about fancy things like the Lefschetz zeta function (http://en.wikipedia.org/wiki/Lefschetz_zeta_function), but from my perspective it seems to me that the general idea is that given a dynamical system (http://en.wikipedia.org/wiki/Dynamical_system) consisting of a set X, a weighting $w : X \to \mathbb{C}$, and a function $f : X \to X$ one is interested in establishing rationality or a Riemann hypothesis for the associated dynamical zeta function (http://www.ams.org/notices/200208/fea-ruelle.pdf)

$$\zeta_X(t) = \exp \left(\sum_{k \ge 1} \left(\sum_{x \in \text{Fix } f^k} \prod_{i=0}^{k-1} w(f^i x) \right) \frac{t^k}{k} \right)$$

since these properties are associated with good regularity phenomena, which I referred to above as local finiteness. As the article above indicates, dynamical zeta functions have a very general notion of Euler product which I am still trying to digest.

It's interesting that the theory of zeta functions focuses so much on fixed points. From a purely combinatorial perspective, fixed points of f^k are precisely closed walks of length k on the functional graph (http://mathworld.wolfram.com/FunctionalGraph.html) associated to f acting on X, so there's no reason not to consider closed walks on more general graphs than functional graphs and define something like the Ihara zeta function (http://en.wikipedia.org/wiki/Ihara_zeta_function) in a general context, which is closely related, but apparently not identical, to the function $\frac{1}{\det(\mathbf{I} - t\mathbf{A})}$ defined earlier. From the example of the Lefschetz zeta function, however, it seems as if when X is infinite and carries additional structure this viewpoint may no longer be feasible. I would very much appreciate it if someone could clarify the situation here for me.

Edit, 8/24/2009: There is a fairly simple result that might clarify this situation.

Proposition: A sequence a_n of integers satisfies the necklace congruences if and only if there exist two functions $f, g : X \to X$ on a set X of at most countable cardinality such that $a_n = \text{Fix } f^n - \text{Fix } g^n$.

Proof. The left implication follows from arguments above. For the right implication, recall that a sequence satisfies the necklace congruences if and only if there exists an integer sequence b_n such that $\sum_{d|n} db_d = a_n$. Let p_n, q_n be sequences of non-negative integers such that $b_n = p_n - q_n$; if we require that one of p_n, q_n always be equal to zero, these sequences are unique.

Let $f : X \to X$ be a permutation with p_n cycles of length n for all n, and similarly let $g : X \to X$ be a permutation with q_n cycles of length n for all n. Clearly one only needs X at most countable to achieve this. Then a cycle of length d contains fixed points of f^n if and only if $d|n$, in which case every element of the cycle is a fixed point. It follows that $\text{Fix } f^n = \sum_{d|n} dp_d, \text{Fix } g^n = \sum_{d|n} dq_d$ as desired.

Applied to the case of walks on graphs, the set X is the set of closed walks and f is the permutation that takes a given closed walk to the same closed walk, but starting on the next vertex. So in a sense I had my order of inclusion wrong: as long as one isn't too picky about finiteness, closed walks are a special case of fixed points and not the other way around.

Remark

My combinatorics teacher, Gregg Musiker, gave a talk (http://www.crm.umontreal.ca/Words07/pdf/musikerslides.pdf) whose slides inspired much of the second half of this post. Instead of discussing closed walks on graphs he discusses the more-or-less equivalent notion of **cyclic language**, i.e. a language on which the cyclic group can act. He then goes on to discuss a specific connection between zeta functions of elliptic curves and certain sequences of chip-firing games, both of which are distinguished by the existence of group structure. I would love to see all of this stuff fit into a cohesive framework someday.

Thinking of a dynamical system as a category with object set X and morphisms determined by the iterates of f, one might hope that there is a meaningful definition of the zeta function of a category (http://www.projecteuclid.org/DPubS?verb=Display&version=1.0&service=UI&handle=euclid.pja/1195510168&page=record). My big hope is that this definition, or a modification thereof, somehow subsumes both the definition of the zeta function of a dynamical system and the zeta function of a poset (http://en.wikipedia.org/wiki/Incidence_algebra#Special_elements). At the moment, I have no idea if this is true.

Questions

1. Based on the above arguments, I am reasonably certain the following is true: an integer sequence a_n satisfies the necklace congruences if and only if $\exp\left(\sum_{k \geq 1} a_k \frac{t^k}{k}\right)$ is a power series with integer coefficients. I'd be interested in seeing a proof involving the Mellin transform (http://en.wikipedia.org/wiki/Mellin_transform) and Dirichlet series, as well as a more direct combinatorial proof.
2. If $\mathbf{A}$ is the adjacency matrix of a finite directed graph G, what combinatorial interpretation do the coefficients of $\frac{1}{\det(\mathbf{I} - t\mathbf{A})}$ have? (I am convinced that one exists because these coefficients are precisely the complete homogeneous symmetric polynomials of the eigenvalues of $\mathbf{A}$, but for some reason I'm just not seeing it.) This combinatorial interpretation should be closely related to the symmetric function identity

$$h_n = \frac{1}{n!} \sum_{\sigma \in S_n} p_\sigma$$

since $p_\sigma = p_{\lambda_1} p_{\lambda_2} \cdots p_{\lambda_n}$ counts the number of n-tuples of closed walks of prescribed lengths. Alternately, one might proceed via the second Newton-Girard identity.

If your interpretation is really good, it should also somehow explain Molien’s theorem (http://rigtriv.wordpress.com/2008/02/12/invariants-of-finite-groups-i/), at least for permutation representations.

Posted in math.CO, math.NT | Tagged finite fields, generating functions, group actions, species theory, symmetric functions, walks on graphs, zeta functions | 6 Comments

6 Responses

dt *on August 27, 2009 at 1:42 pm* | *Reply*

How’s this for your question 2. Say a directed graph is smooth if each vertex has one incoming and one outgoing vertex, or in other words if it’s a cycle, or a disjoint union of cycles. The coefficient of t^n in 1/det(1 – t A) is the number of equivalence classes of maps from a smooth graph with n vertices into G. (The equivalence relation is given by relabeling the vertices in the domain of the map.)

Here is an argument. The trace of A^n is (as you point out) the number of loops in A^n with a specified start-and-end vertex. The trace of A^n/n feels like the number of loops in G with no such specified vertex, but A^n/n can fail to be an integer. A more careful way to put it is: A^n * (n-1)! is the number of structures of the form

– cyclic ordering of {1,…,n}
– map from {1…n} to G preserving the cyclic ordering.

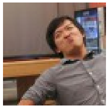
The exponential generating function of this is the logarithm of 1/det(1 – t A) (the second displayed formula in your “Zeta functions” section). A standard argument about exp-of-an-exponential-generating-function says that the coefficients of t^n/n! in 1/det(1 – t A) itself count structures of the form

a- decomposition of {1,…,n} into pieces, and a cyclic ordering of each piece
b- map from each cyclically-ordered piece into G preserving the order

Or “maps from a smooth graph with n vertices into G” for short. (a- can be recast as “total ordering of {1…n}” using the cycle notation for permutations)

Can you expand your comment about the symmetric function identity? Molien’s theorem?

Qiaochu Yuan *on August 30, 2009 at 11:51 am* | *Reply*



This sounds close to what I want. Let me explain the symmetric function idea, although it doesn’t work: ideally the sum on the RHS should result from an application of Burnside’s lemma, but this doesn’t actually work out since the term corresponding to the identity is smaller than the other terms in general. Even if that's not the case, there should be some way to explain why dividing by $n!$ on the RHS gives an integer.

As for the other idea, for a permutation representation $\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - \lambda g)}$ is an average over a bunch of terms coming from adjacency matrices of functional graphs describing the action of G on some finite set. Molien's theorem relates these to homogeneous invariants, so at least for this case one should be able to give a basis for these invariants which is in bijection with whatever it is $\frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - \lambda g)}$ counts.

The cyclotomic identity and Lyndon words « Annoying Precision *on November 3, 2009 at 11:12 am* | *Reply*

[…] theory and implies that the dynamical zeta function (which we first encountered when talking about Newton's sums) is equal […]

Newton's sums, necklace congruences, and zeta functions II « Annoying Precision *on November 9, 2010 at 5:02 pm* | *Reply*

[…] sums, necklace congruences, and zeta functions II November 4, 2009 In a previous post I gave essentially the following definition: given a discrete dynamical system, i.e. a space and a […]

The p-group fixed point theorem | Annoying Precision *on July 9, 2013 at 11:23 am* | *Reply*

[…] length on letters. (Orbits of this group action are sometimes called necklaces; see, for example, this previous blog post.) This set has cardinality and its fixed point set has cardinality , since a function is fixed if […]

gorofir *on February 8, 2015 at 11:40 am* | *Reply*

Here's a solution to your first question – it is simple than you'd expect. I'm sure it is known, but didn't find a reference (I came up with it reading a chapter in Alain Robert's "A Course in p-adic Analysis", where surprisingly, similar ideas are discussed, see Dieudonné-Dwork Criterion and Hazewinkel Theorem):

If a_n satisfies the necklace congruence, you can verify that $\exp \left(\sum_{k \ge 1} a_k \frac{t^k}{k} \right) = \prod_{n \ge 1} (1-x^n)^{-\frac{b_n}{n}}$, where b_n is an integer sequence given by $b := a * \mu$, and so $b(n) \equiv 0 \mod n$ and the product must have integer coefficients.

Other direction: Assume $\exp \left(\sum_{k \ge 1} a_k \frac{t^k}{k} \right)$ has integral coefficients. Again, one can write it as $\prod_{n \ge 1} (1-x^n)^{-\frac{b_n}{n}}$ where $b = a * \mu$. Because the coefficient of x^n is $\frac{b_n}{n}+$ a sum consisting of binomial coefficients depending on $\{ \frac{b_i}{i} \}_{i<n}$, an induction arguments shows that $\frac{b_n}{n}$ must be integral for all n, and so a_n satisfies the necklace congruence.

Comments RSS

Blog at WordPress.com.

The MistyLook Theme.