Ghosts and Necklaces

Barry Dayton

January, 1994

Mathematics is not self evident. The ancient Greeks wanted it to be so, but they missed the interplay between different branches of mathematics and the surprising consequences of this. This is an account of such a phenomena. The story starts with an observation in 1629 about roots of polynomials, touches the modern ideas of Witt vectors and Grothendieck groups and suddenly we are able to easily obtain some formulas from the classical theory of counting necklaces. The ideas, and connections, presented here are not new, (see, for example [9, 5, 6]) and maybe not even of practical value, but the connection between these seemingly unrelated ideas is another example of the amazing subtlety and consistency of mathematics.

Newton's Identities

In his 1629 work *L'invention nouvelle en l'algèbre* the Dutch mathematician Albert Girard noted that there was a connection between the coefficients of the equation $t^n = at^{n-1} - bt^{n-2} + ct^{n-3} - dt^{n-4} + \cdots$ and the sums of the kth powers of the roots $x_1, x_2, .., x_n$, i.e.

$$\begin{aligned}
x_1 + x_2 + \cdots x_n &= a \\
x_1^2 + x_2^2 + \cdots x_n^2 &= a^2 - 2b \\
x_1^3 + x_2^3 + \cdots x_n^3 &= a^3 - 3ab + 3c \\
x_1^4 + x_2^4 + \cdots x_n^4 &= a^4 - 4a^2b + 4ac + 2b^2 - 4d
\end{aligned}$$

(see, for example, [10, p. 86]).

A few years later in his *Arithmetica universalis* (again see [10, p. 95]) Isaac Newton discovered that the generalization of Girard's equations was the recursive series of identities

Theorem 1 (Newton's Identities) *Let $x_1, x_2, x_3, ..., x_n$ be the roots, counted according to multiplicity, of the polynomial equation*

$$t^n + p_1t^{n-1} + p_2t^{n-2} + \cdots + p_{n-1}t + p_n = 0$$

and let

$$s_k = x_1^k + x_2^k + \cdots + x_n^k$$

for $k = 1, 2, 3, \ldots$. *Then for each* $k \geq 1$

$$s_k + p_1 s_{k-1} + p_2 s_{k-2} + \cdots + p_{k-1} s_1 + k p_k = 0$$

Newton did not provide a proof, nor shall I at the present. Of course Newton was thinking about the case where the coefficients p_j were real, but this works equally well in any algebraically closed field of characteristic 0. Note also we are assuming that the coefficient $p_j = 0$ for $j > n$.

Newton's identities allow one to calculate the s_k recursively and his application was to estimate the largest positive real root (assuming multiplicity 1 and that it is actually the largest complex root in modulus) by $\sqrt[k]{s_k}$ for moderately large k. This is, of course, not useful today. A more interesting application is to calculate the characteristic polynomial $f(\lambda) = \det(\lambda I - A)$ of a $n \times n$ matrix A. If the eigenvalues of A are $x_1, \ldots, x_n$ then the eigenvalues of A^k are $x_1^k, \ldots, x_n^k$ and thus $s_k = \text{trace}(A^k)$, which is easily calculated. Knowing the $s_k,\ k = 1, \ldots, n$ one can work backwards in Newton's identities to find the coefficients of the characteristic polynomial.

There are similar classical identities to find $s_k = x_1^k + \cdots + x_n^k$ for negative values of k which are more to the point of this article.

Theorem 2 (Newton's Identities) *Let* $x_1, x_2, ..., x_n$ *be the roots (in an algebraically closed field of characteristic 0) of the unitary polynomial* $a(t) = 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n$. *Assume* $a_j = 0$ *for* $j > n$ *and let* $s_j = x_1^j + \cdots x_n^j$ *for* $j = -1, -2, -3, \ldots$. *Then for all* $k > 0$

$$k a_k + a_{k-1} s_{-1} + a_{k-1} s_{-2} + \cdots + a_1 s_{k-1} + s_{-k} = 0$$

Proof: From the factorization

$$a(t) = (1 - x_1^{-1} t)(1 - x_2^{-1} t) \cdots (1 - x_n^{-1} t)$$

it follows that the logrithmic derivative

$$\frac{a'(t)}{a(t)} = \frac{-x_1^{-1}}{1-x_1^{-1}t} + \cdots + \frac{-x_n^{-1}}{1-x_n^{-1}t}$$

Multiplying by $-t$ gives

$$-t\frac{a'(t)}{a(t)} = \frac{x_1^{-1}t}{1-x_1^{-1}t} + \cdots + \frac{x_n^{-1}t}{1-x_n^{-1}t}$$

Now by the geometric series there is the formal series expansion

$$\frac{1}{1-x_j^{-1}t} = 1 + x_j^{-1}t + x_j^{-2}t^2 + \cdots$$

or

$$\frac{x_j^{-1}t}{1-x_j^{-1}t} = x_j^{-1}t + x_j^{-2}t^2 + x_j^{-3}t^3 + \cdots$$

Summing over all j gives the formal power series

$$-t\frac{a'(t)}{a(t)} = s_{-1}t + s_{-2}t^2 + s_{-3}t^3 + \cdots \tag{1}$$

Multiplying both sides of this last equation by $a(t)$ and equating the coefficients of t^k on both sides gives the identities of the theorem.

I remark that a proof of Theorem 1 can be obtained as above by expanding $t\frac{a'(t)}{a(t)}$ as a formal power series in powers of t^{-1}. I would also remark that using a computer algebra system it is often easiest to calculate the s_{-k} by using Equation (1), i.e. by expanding the left hand side as a power series.

Now using the identities of Theorem 2 one can calculate the s_k from the coefficients a_j or vice versa. Thus the sequence $s_{-1}, s_{-2}, \ldots$ gives an alternate representation of the polynomial $a(t)$. I will call these the *ghost coefficients* of the polynomial and write $\mathrm{gh}_k(a(t)) = s_{-k}$.

It then makes sense given a unitary formal power series $a(t) = 1 + a_1t + a_2t^2 + \cdots$ to define ghost components $\mathrm{gh}_k(a(t)) = s_{-k}$ by means of the identities in Theorem 2. Of course, one can not then assume that the s_{-k} are sums of the kth powers of the roots. Euler, however, did just that when he calculated, correctly, the sums of the series

$$\zeta(k) = \sum_{n=1}^{\infty} \frac{1}{n^k}$$

for even integers k (see, for example, [7, p. 449]).

The ghost components, or more precisely the ghost series (i.e. the right hand of Equation (1)) acts somewhat like a logarithm. One can see this either from the equation

$$-t\frac{a'(t)}{a(t)} = -t\frac{d}{dt}\log a(t)$$

or by noting that the roots of the product $a(t)b(t)$ are the elements of the "disjoint union" of the roots of the two polynomials ("disjoint" so that multiplicities are counted correctly). From either point of view one gets $\mathrm{gh}_k(a(t)b(t)) = \mathrm{gh}_k(a(t)) + \mathrm{gh}_k(b(t))$.

I end this section with the following idea. Suppose that R is a subring of an algebraically closed field of characteristic 0, i.e. an integral domain of characteristic 0. Let $a(t), b(t) \in R[t]$ be unitary polynomials with coefficients in R. I claim that there is a polynomial $c(t) \in R[t]$ so that $\mathrm{gh}_k(c(t)) = \mathrm{gh}_k(a(t))\mathrm{gh}_k(b(t))$ for each $k > 0$. From a practical standpoint one can calculate the ghost components of $a(t), b(t)$ and then work backwards using the identity of Theorem 2, but it is not clear that only finitely many coefficients c_j will be non-zero nor is it clear that, if R does not contain all rational numbers, that the coefficents will be in R. Instead the argument is to let $x_1, \ldots, x_m$ be the roots of $a(t)$, $y_1, \ldots, y_n$ be the roots of $b(t)$ in both cases counted according to multiplicity. Now consider the polynomial $c(t)$ of degree mn whose roots are $\{x_iy_j | 1 \leq i \leq m, 1 \leq j \leq n\}$. This clearly satisfies the correct identities on the ghost components. But the coefficients of $c(t)$ are symmetric polynomials in the roots x_iy_j. Now in these symmetric polynomials the coefficient of any particular monomial in $y_1, \ldots, y_n$ is a symmetric polynomial in $x_1, \ldots, x_m$ and hence, by the Fundamental Theorem on Symmetric polynomials (eg. [8, Thm. 11, p133]) a polynomial in the coefficients of $a(t)$, i.e. an element of R. But, since the order in which we wrote down the y_j's clearly doesn't matter, the resulting polynomial in $R[y_1, \ldots, y_n]$ is again symmetric and hence a polynomial in the coefficients of $b(t)$, hence an element of R.

Witt Vectors

The preceding classical ideas can be axiomatized by the modern idea of (big) Witt vectors. It is generally accepted that these Witt vectors made their official debut in the paper by Cartier [4] even though they appear to have been discovered much earlier by E. Witt, for instance they had previously appeared in print in the form of a series of exercises in S. Lang's textbook [8].

Let R be a commutative ring with unit, which I will view as a commutative **Z**-algebra. As a set we define $W(R)$ to be the set of unitary power series in R, i.e $W(R) = \{a(t) = 1 + a_1 t + a_2 t^2 + \cdots \in R[[t]]\}$. The addition in $W(R)$ will be the usual multiplication of power series. I will use the usual multiplicative notation, so that for $a(t), b(t) \in W(R)$, $a(t)b(t)$ is the "sum", $\frac{a(t)}{b(t)}$ is the "difference", and in an expression such as $(1-t)^r$, r is the "coefficient".

Central to this is the *ghost map*. This is the map $W(R) \to tR[[t]]$ given by

$$\mathrm{gh}(a(t)) = -t\frac{a'(t)}{a(t)} = \frac{d}{dt}\log a(t)$$

If $\mathrm{gh}(a(t)) = f_1 t + f_2 t^2 + \cdots$ it is customary to call f_i the ith ghost component of $a(t)$ or $\mathrm{gh}_i(a(t))$.

The ghost map is a homomorphism of the additive groups of $W(R)$ and $tR[[t]]$ but rather than viewing $tR[[t]]$ as an ideal of $R[[t]]$ I will view it as the product $\prod_{i=1}^{\infty} R$ via the map $f_1 t + f_2 t^2 + \cdots \mapsto (f_1, f_2, f_3, \ldots)$ and thus addition is the same but multiplication is given by

$$(f_1 t + f_2 t^2 + \cdots) * (g_1 t + g_2 t^2 + \cdots) = (f_1 g_1)t + (f_2 g_2)t^2 + \cdots \tag{2}$$

If R has no **Z**-torsion (i.e. $nr = 0$ implies $r = 0$ for $n \in \mathbf{Z}, n \neq 0, r \in R$) then it is easily seen from Newton's Identities that gh is injective and if R contains the rationals **Q** then gh is bijective. In this latter case the ring structure on $tR[[t]]$ given by (2) determines a ring structure on $W(R)$ so that $\mathrm{gh} : W(R) \to tR[[t]]$ is an isomorphsim.

It is in fact true in general that there is a multiplication in $W(R)$ which makes gh a homomorphism of rings. There are probably more arguments for this than there are authors who have written about Witt vectors (see, for example, [1, 2, 3]) but I must stick in my own two cents worth with a sketch of my own favorite argument. It is clearly enough to establish this for the ring $\mathbf{Z}[\{a_i\}_{i=1}^{\infty}, \{b_i\}_{i=1}^{\infty}, \{c_i\}_{i=1}^{\infty}]$ of polynomials in infinitely many indeterminants so we can assume that R is an integral domain with no **Z**-torsion. Thus gh is injective and one only needs to show that if f, g are in the image of gh then fg is also in the image. Now Newton's Identities tell us that the nth ghost component $\mathrm{gh}_n(a)$ depends only on the first n components of a and thus by a limit argument in the appropriate topology the result follows from my remark at the end of the last section that given $a, b \in W(R)$ and any positive integer n there is a $c \in W(R)$ with $\text{gh}_i(c) = \text{gh}_i(a)\text{gh}_i(b)$ for $i \leq n$.

Denoting our multiplication by $*$ it is seen that

$$(1 - rt^m) * (1 - st^n) = (1 - r^{n/d}s^{m/d}t^{mn/d})^d, d = (m, n) \tag{3}$$

where (m, n) is the greatest common divisor of m, n. This can be checked by noting that

$$\text{gh}(1 - rt^m) = mrt^m + mr^2t^{2m} + mr^3t^{3m} + \cdots$$

In particular $1 - t$ is the multiplicative identity. (The astute reader will note that this differs from some authors such as [9, 2] where $(1 - t)^{-1}$ is the multiplicative identity.)

In general $W(R)$ is not an R-algebra, however there is a fairly common type of ring for which $W(R)$ is an R-algebra. This is a *binomial ring*, i.e. a ring with no **Z**-torsion in which for each $r \in R$ and positive integer n,

$$\left(\begin{array}{c} r \\ n \end{array} \right) = \frac{r(r-1)\cdots(r-n+1)}{n!}$$

is an element of R. For example the ring of integers and any ring containing **Q** is a binomial ring. For a binomial ring there is a map $\lambda : R \to W(R)$ given by

$$\lambda(r) = (1 - t)^r = \sum_{n=0}^{\infty} (-1)^n \left(\begin{array}{c} r \\ n \end{array} \right) t^n$$

which imbeds R as a subring of $W(R)$. More generally

$$(1 - t^m)^r = \sum_{n=0}^{\infty} (-1)^n \left(\begin{array}{c} r \\ n \end{array} \right) t^{mn}$$

is an element of $W(R)$. We note that

$$\text{gh}((1 - t^m)^r) = mrt^m + mrt^{2m} + mrt^{3m} + \cdots$$

which, incidentally, gives a proof (letting $m = 1$) that λ is an injective ring homomorphism.

The main result of this section is essentially the first proposition of [9, p. 113]. I remind the reader that $\prod$ below refers to the "sum" in $W(R)$. Also, at this point I will start writing a instead of $a(t)$.

Proposition 3 *Let R be a binomial ring. Then each $a \in W(R)$ can be written uniquely in the form*

$$a = \prod_{m=1}^{\infty} (1 - t^m)^{r_m}$$

for appropriate $r_1, r_2, \ldots \in R$.

Sketch of Proof: Suppose $\mathrm{gh}(a) = f_m t^m + f_{m+1} t^{m+1} + \cdots$ for some $m \geq 1$. It follows easily from Newton's identities that f_m is divisible by m in R so then $a(1 - t^m)^{-(f_m/m)} \in W(R)$ and $\mathrm{gh}_i(a(1 - t^m)^{-(f_m/m)}) = 0$ for all $i \leq m + 1$. Thus successively "subtracting" Witt vectors of the form $(1 - t^m)^{r_m}$ from a produces a sequence of elements in $W(R)$ converging to the zero Witt vector. An appropriate limit argument would clean up the details.

Example 4 I illustrate the constructive approach above by calculating the decomposition of the Witt vector $a = 1 - 5t \in W(\mathbf{Z})$. I first calculate

$$\mathrm{gh}(a) = 5t + 25t^2 + 125t^3 + 625t^4 + 3125t^5 + 15625t^6 + \cdots$$

I now note that $\mathrm{gh}((1 - t)^5) = 5t + 5t^2 + 5t^3 + \cdots$ so

$$\mathrm{gh}(a(1 - t)^{-5}) = 20t^2 + 120t^3 + 620t^4 + 3120t^5 + 15620t^6 + \cdots$$

But $\mathrm{gh}((1 - t^2)^{10}) = 20t^2 + 20t^4 + 20t^6 + \cdots$ so

$$\mathrm{gh}(a(1 - t)^{-5}(1 - t^2)^{-10}) = 120t^3 + 600t^4 + 3120t^5 + 15600t^6 + \cdots$$

Next $\mathrm{gh}((1 - t^3)^{40} = 120t^3 + 120t^6 + \cdots$ so

$$\mathrm{gh}(a(1 - t) {-} 5(1 - t^2)^{-10}(1 - t^3)^{-40}) = 600t^4 + 3120t^5 + 15480t^6 + \cdots$$

Finally as $600/4 = 150, 3120/5 = 624$ and $15480/6 = 2580$ I conclude that

$$a = (1 - t)^5(1 - t^2)^{10}(1 - t^3)^{40}(1 - t^4)^{150}(1 - t^5)^{624}(1 - t^6)^{2580} \cdots$$

Assuming that $a \in W(R)$ has the factorization $a = \prod_{m=1}^{\infty}(1 - t^m)^{r_m}$ then it is seen that the nth ghost component is

$$\mathrm{gh}_n(a) = \sum_{d|n} d r_d$$

A straightforward application of the Möbius inversion formula gives

Proposition 5 *Let $a \in W(R)$ where R is a binomial ring. Suppose*

$$gh(a) = g_1 t + g_2 t^2 + g_3 t^3 + \cdots$$

Then $a = \prod_{m=1}^{\infty}(1 - t^m)^{r_m}$ where

$$r_m = \frac{1}{m} \sum_{d|m} \mu \left(\frac{m}{d} \right) g_d$$

where μ is the Möbius function.

The Grothendieck – Burnside ring

In this section I construct the Grothendieck – Burnside ring of [5] in the special case of the infinite cyclic group. In [5, 6] this is constructed for any profinite group G, but I prefer to avoid all the technicalities involved. Thus let G denote the infinite cyclic group.

A (finite) G-space (S, σ) then consists simply of a finite set S together with a permutation σ of S. Thus G acts on S by $n \in G$ acting on $x \in S$ by $\sigma^n(x)$. Two G-spaces $(S, \sigma), (T, \tau)$ are isomorphic if there is a bijection $u : S \to T$ with $\tau u = u\sigma$. If $(S, \sigma), (T, \tau)$ are two G-spaces then there is a join $(S \bigsqcup T, \sigma \sqcup \tau)$ given by $S \bigsqcup T$ being the the disjoint union of S and T and

$$\sigma \sqcup \tau(x) = \begin{cases} \sigma(x) & \text{if } x \in S \\ \tau(x) & \text{if } x \in T \end{cases}$$

There is also the cartesian product G-space $(S \times T, \sigma \times \tau)$ where, of course, $\sigma \times \tau(x, y) = (\sigma(x), \tau(y))$.

I now let Ω be the Grothendieck group of the class of these (finite) G-spaces, i.e. Ω is the free abelian group generated by isomorphism classes $[S, \sigma]$ of G-spaces modulo the relation $[S \bigsqcup T, \sigma \sqcup \tau] = [S, \sigma] + [T, \tau]$. It is easily seen that the cartesian product operation induces a product on Ω so that Ω is a commutative ring.

Once again we have a ghost map. Here we define $\mathrm{Gh} : \Omega \to t\mathbf{Z}[[t]]$ by $\mathrm{Gh}([S, \sigma] = \sum_{n=1}^{\infty} \mathrm{Gh}_n([S, \sigma])t^n$ where $\mathrm{Gh}_n([S, \sigma])$ is the number of elements of S left fixed by the action of the subgroup of G generated by n, i.e the number of elements of S left fixed by the permutation σ^n. This is well defined on isomorphism classes and is easily seen to be compatible with the ring structure on Ω and so factors as a ring homomorphism Gh $: \Omega \to t\mathbf{Z}[[t]]$ where the latter ring is viewed as the infinite product of the previous section.

The point is that this ghost map factors through the ghost map of the previous section, i.e. there is a map $\psi : \Omega \to W(\mathbf{Z})$ so that the diagram commutes.

$$\begin{tikzcd}
 & W(R) \arrow[dd, "\text{gh}"] \\
\Omega \arrow[ru, "\psi"] \arrow[rd, "\text{Gh}"'] & \\
 & t\mathbf{Z}[[t]]
\end{tikzcd}$$

To see this, I first consider the case when (S, σ) is a transitive G-space, i.e. σ has only one orbit, i.e. σ is a cycle. Suppose that S has m elements. It is easily seen that σ^n has fixed points only if $m|n$, i.e. σ^n is the identity, in which case σ^n has m fixed points. Thus

$$\text{Gh}([S, \sigma]) = mt^m + mt^{2m} + mt^{3m} + \cdots = \text{gh}(1 - t^m)$$

But every permutation is the product of disjoint cycles so in Ω each class $[S, \sigma]$ is a sum of transitive G-spaces. It follows that if σ factors as a product of r_m cycles of length m for $m = 1, 2, 3, \ldots$ then ψ should be given by

$$\psi([S, \sigma]) = (1 - t)^{r_1}(1 - t^2)^{r_2}(1 - t^3)^{r_3} \cdots$$

It is easily checked that this does in fact work. It should be noted that since we are working with finite G-spaces that this “sum” is in fact finite, i.e. $r_m = 0$ for large m.

As a consequence of the above description of ψ one obtains

Proposition 6 *Let (S, σ) be a finite G-space with $\psi([S, \sigma]) = \prod_{m=1}^{\infty}(1 - t^m)^{r_m}$. Then the number of distinct orbits of elements of S of length n under the permutation σ is r_n and the total number of distinct orbits is $\sum_{m=1}^{\infty} r_m$.*

Necklaces

In this section I apply the preceding results to counting necklaces. It should be emphasized that all the results here are classical, none-the-less I find the connection between these classical results and the ideas presented above to be striking.

By a necklace with n beads in c colors, I mean an arrangement of n objects (beads) of c different colors around a circle. If the circle is rotated the resulting necklace is considered to be the same as the original, however a flip may produce a different necklace.

A more formal way of describing this is the following: let B be a set of n objects (the beads) and C be a set of c elements (the colors). Then consider the set S of all functions $f : B \to C$. Now let γ be a cyclic permutation of the set B, i.e. γ has order n. Then there is a permutation σ of S given by $\sigma(f) = f \circ \gamma$. A necklace is an orbit in S of the permutation σ.

Thus (S, σ) is a G-space, so by Proposition 6 to count necklaces one need only calculate $\psi([S, \sigma])$. But since gh : $W(\mathbf{Z}) \to t\mathbf{Z}[[t]]$ is an injection, the strategy is to first calculate Gh$([S, \sigma])$ and lift.

Now the main observation is that f is a fixed point of σ^k if and only if f is constant on each orbit of γ^k. If k is relatively prime to n then γ^k again has only one orbit so f must be constant, i.e. $\text{Gh}_k([S, \sigma]) = c$. More generally, if $(k, n) = d$, (here and below (k, n) is the greatest common divisor) then γ^k has d orbits, on each of which f must be constant. Thus $\text{Gh}_k([S, \sigma]) = c^d$.

Example 7 Suppose I wish to know the number of necklaces with 6 beads of 5 possible colors. By the above paragraph

$$\text{Gh}([S, \sigma]) = 5t + 25t^2 + 125t^3 + 25t^4 + 5t^5 + 15625t^6 + \cdots$$

and is periodic of period 6. Using the technique of Example 4 (note even that the first 3 terms are the same) I easily calculate

$$\psi([S, \sigma)] = (1 - t)^5(1 - t^2)^{10}(1 - t^3)^{40}(1 - t^6)^{2580}$$

It follows from Proposition 6 that there are $5 + 10 + 40 + 2580 = 2635$ such necklaces.

Generalizing from the above example I note that by Proposition 6 of the last section, since the order of each cycle of σ divides n, that $\psi([S, \sigma]) = \prod_{d|n}(1 - t^d)^{r_d}$. But $\text{gh}(1 - t^d) = dt^d +$

$dt^{2d} + \cdots + \frac{n}{d}t^n + \cdots$ so if we add the coefficients of t^i for $1 \le i \le n$ we get $\frac{n}{d}d = n$. Hence the coefficients of t^i, $1 \le i \le n$ in the expansion of $\text{gh}((1-t^d)^{r_d})$ add to nr_d and hence the coefficients of t^i, $1 \le i \le n$ of $\text{Gh}([S,\sigma]) = \text{gh}(\psi([S,\sigma])$ add to $n\left(\sum_{d|n} r_d\right)$. By Proposition 6 the sum in parentheses is the number of necklaces, and so one may conclude that the number of necklaces with n beads in c colors is

$$\frac{1}{n}\sum_{k=1}^{n} \text{Gh}_k([S,\sigma]) = \frac{1}{n}\sum_{k=1}^{n} c^{(k,n)}$$

But note that the number of times the term c^d appears in the last sum is $\phi(\frac{n}{d})$ where ϕ is Euler's ϕ function. And thus I have obtained the classical formula:

Theorem 8 *The number of necklaces with n beads and c colors is*

$$\frac{1}{n}\sum_{d|n} \phi\left(\frac{n}{d}\right) c^d$$

I now look at the problem of counting primitive necklaces with n beads in c colors, let $M(c,n)$ denote the number of these. A primitive necklace is one which is asymmetric under rotation, i.e. corresponds to an orbit of length n in S under σ. Thus we see from Proposition 6 $M(c,n) = r_n$ where $\psi([S,\sigma]) = \prod_{m=1}^{\infty}(1-t^m)^{r_m}$. And from this and Proposition 5 I immediately obtain the formula attributed to Col. Moreau (see [9]).

Theorem 9

$$M(c,n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right) c^d$$

where μ is the Möbius function.

Motivated by Examples 4,7 the reader might observe that the "coefficient" r_n in the expansion $(1-ct) = \prod_{m=1}^{\infty}(1-r^m)^{r_m}$ is also given by the same formula $\sum_{d|n} \mu(\frac{n}{d})c^d$ and hence

$$(1-ct) = \prod_{n=1}^{\infty}(1-t^n)^{M(c,n)}$$

This identity usually occurs in the literature by replacing each side by its "negative" as

Theorem 10 (The Cyclotomic Identity) *For each positive integer c*

$$\frac{1}{1-ct} = \prod_{n=1}^{\infty}\left(\frac{1}{1-t^n}\right)^{M(c,n)}$$

Thus from Example 4 one may conclude that $M(5,1)=5, M(5,2)=10, M(5,3)=40, M(5,4)=150, M(5,5)=624$ and $M(5,6)=2580$ etc.

So far the multiplicative structure of $W(\mathbf{Z})$ has not played much of a role. As my last result, I derive an identity from [9] using Witt vector multiplication.

Theorem 11 *For integers i,j let (i,j) denote the greatest common divisor and $[i,j]$ be the least common multiple. Then for all positive integers a,b,n,*

$$M(ab,n) = \sum_{[i,j]=n}(i,j)M(a,i)M(b,j)$$

Proof: $M(ab,n)$ is the "coefficient" of $(1-t^n)$ in the expansion $(1-abt) = \prod_{m=1}^{\infty}(1-t^m)^{M(ab,m)}$ by the previous theorem. But in $W(\mathbf{Z})$, $(1-abt)=(1-at)*(1-bt)$ so

$$(1-abt) = \left(\prod_{i=1}^{\infty}(1-t^i)^{M(a,i)}\right) * \left(\prod_{j=1}^{\infty}(1-t^j)^{M(b,j)}\right)$$

By virtue of Equation (3) the $(1-t^n)$ term in this last product will be the "sum" of all products

$$(1-t^i)^{M(a,i)} * (1-t^j)^{M(b,j)} = (1-t^{[i,j]})^{(i,j)M(a,i)M(b,j)}$$

where $[i,j]=n$. This finishes the proof.

References

[1] G.M. Bergman, Ring Schemes, in "Lectures on Curves on an Algebraic Surface"(D. Mumford, ed.), Princeton Univ. Press, 1966.

[2] S. Bloch, Algebraic K-theory and Crystalline Cohomology, Publ. Math. I.H.E.S. 47 (1978), 188–268.

[3] N. Bourbaki, Algèbra Commutative, Ch. 9, Masson, 1983.

[4] P. Cartier, Groups formels associés aux anneaux de Witt généralisés, C.R. Acad. Sci. Paris 265 (1967), 49-52.

[5] A.W.M. Dress and C. Siebeneicher, The Burnside Ring of Profinite Groups and the Witt Vector Construction, Advances in Math 70, (1988), 87–132.

[6] John Graham, Generalised Witt Vectors, Advances in Math 99 (1993), 248–263.

[7] Morris Kline, Mathematical Thought from ancient to modern times, Oxford University Press, 1972.

[8] S. Lang, Algebra, Addison-Wesley, 1965.

[9] N. Metropolis and G-C. Rota, Witt Vectors and the Algebra of Necklaces, Advances in Math 50 (1983), 95–125.

[10] D.J. Stuik, A Source Book in Mathematics 1200–1800, Princeton University Press, 1986.

Northeastern Illinois University
Chicago, IL 60625