Some combinatorial aspects of cyclotomic polynomials

Richard P. Stanley University of Miami and M.I.T

A theorem of Schur (1926) states that the number of partitions of n for which no part appears exactly once equals the number of partitions of n into parts $\equiv \pm 1 \pmod 6$. The key fact behind this identity is that the numerator of the rational function $\frac{1}{1-x} - x$ is a product of cyclotomic polynomials $\phi_j(x)$, in this case just the single cyclotomic polynomial $\Phi_6(x)$. This leads to asking for what subsets S of the positive integers is the power series $N_S(x) = \frac{1}{1-x} - \sum_{i \in S} x^i$ a product of cyclotomic polynomials divided by a product of cyclotomic polynomials. We then call S a *cyclotomic set*. If S is cyclotomic, then we get a partition identity analogous to Schur's, but in general the parts of the partition might be weighted by integers, sometimes negative. Thus we can also ask when we have a "clean" identity, i.e., no weighted parts.

One source of cyclotomic sets comes from numerical semigroups, i.e., a submonoid M of the nonnegative integers $\mathbb{N}$ (under addition) such that $\mathbb{N} - M$ is finite. If the monoid algebra $\mathbb{Q}M$ is a complete intersection (meaning in this case that if M has k generators, then all the relations among the generators are consequences of $k-1$ relations, the minimum possible), then $\mathbb{N} - M$ is a cyclotomic set.

For any subset S of the positive integers, we can also ask for the number $f_S(n)$ of monic polynomials of degree n over the finite field $\mathbb{F}_q$ that have no irreducible factors whose multiplicity belongs to S. If S is a cyclotomic set, then we can write an explicit formula (in general quite lengthy) for the numbers $f_S(n)$.

For instance, if $S = \{1\}$ then we are counting (monic) *powerful polynomials* of degree n, i.e., those with no irreducible factor of multiplicity one. We get

$$f_S(n) = q^{\lfloor n/2 \rfloor} + q^{\lfloor n/2 \rfloor - 1} - q^{\lfloor (n-1)/3 \rfloor}.$$

For another example, take $S = \{2, 3, 4, \ldots\}$. Then we are counting squarefree polynomials, and we obtain the well-known result

$$f_S(n) = q^{n-1}(q-1).$$

This is a kind of analogue (though not a q-analogue in the usual sense) of Euler's result that the number of partitions of n into distinct parts is equal to the number of partitions of n into odd parts.