Raising Polynomials to Powers

Alex Pan

April 2024

The problem

To determine properties about some invariant I don't understand yet, we need to compute the function: Given a polynomial $f = \mathbb{F}_p[x_1, x_2, ..., x_n]$ with homogeneous degree n, and a prime p, we need to compute $g = f^{p-1}$, lift g to $\mathbb{Z}[x_1, x_2, ..., x_n]$, and compute g^p.

Method 1: FLINT

Does $(numVars, prime) = (4, 5)$ in a worst-case time of around 800 ms, and does $(4, 7)$ in a worst case of 45 (I think) seconds.

Method 2: Multinomial Theorem

This method involves precomputing the multinomial coefficients for a certain number of terms. However, precomputing the multinomial coefficients is very slow, as well as not that parallelizable. Even for the lowest case of interest, being 4 variables and a prime of 5, we need to store $35 * \binom{20+35-1}{35-1} \approx 1.1 * 10^{16}$ integers, which corresponds to about 10 petabytes of storage. So, this is not a very viable solution

Though, I will mention that with pregenerated coefficients, multinomial theorem is by far the fastest method for the worst case of the first step $g = f^{p-1}$ at approximately 79 microseconds, though FFT does it in 1 millisecond anyways, basically making this method useless.

Method 3: Repeated Squaring with GPU-parallelized Trivial Multiplication

This just sucks, maybe its comparable when on a research cluster, since the results for all the steps on my machine are an order of magnitude behind the results for the same steps in the papers I've read about this method

Method 4: FFT

This method involves isomorphically mapping a n-variate polynomial, $\mathbb{Z}[x_1, x_2, ..., x_n]$, to a univariate polynomial $\mathbb{Z}[y]$ performing a slightly modified version of the well-known algorithm for using FFT to multiply polynomials, and mapping $\mathbb{Z}[y]$ back to $\mathbb{Z}[x_1, x_2, ..., x_n]$.

Mapping

Let $f = \mathbb{Z}[x_1, x_2, ..., x_n]$, and let $g = \mathbb{Z}[y]$. We want to compute f^p. Let k be an integer such that $k > p * maxdegree(f)$.

Let $\varphi : \mathbb{Z}[x_1, x_2, ..., x_n] \to \mathbb{Z}[y]$, defined by the following: Map each term $ax_1^{d_1}x_2^{d_2}...x_n^{d_n}$ of $f \in \mathbb{Z}[x_1, x_2, ..., x_n]$, to $ay^{d_1+d_2k+d_3k^2...d_nk^{n-1}}$.

Claim: φ is a ring isomorphism.

Proof: to be done

Proofs for correctness of computed numbers:

We are interested in bounds for two steps. The first, $g = f^{p-1}$, is an n-variate polynomial with homogeneous degree $n(p-1)$, and the second step, g^p, is another n-variate polynomial with homogeneous degree $np(p-1)$.

To compute the upper bound for the first step, take the initial condition that maximizes the resulting maximum coefficient:

$$f = (p-1) \sum_{\sum_n^{i=1} d=n} ax_1^{d_1}x_2^{d_2}...x_n^{d_n}$$

The notation overcomplicates things - f is just the polynomial with all possible n-homogeneous terms, and all coefficients are $p-1$.

Raising f^{p-1}, we get: $f^{p-1} = (p-1)^{p-1} \left(\sum_{\sum_n^{i=1} d=n} ax_1^{d_1}x_2^{d_2}...x_n^{d_n} \right)^{p-1}$

So, the question now is how we go about computing the maximum coefficient of the polynomial that contains every term, each having a coefficient of 1.

Consider any term of f^{p-1}. It will have degree $n(p-1)$. To make things easier, represent the exponents of the variables of a monomial with n-tuples $(d_1', d_2', ..., d_n')$

To find the coefficient of any term with degree tuple $D = (d_1', d_2', ..., d_n')$, we consider $\underbrace{f \cdot ... \cdot f}_{p-1 \text{ times}}$. Before combining like terms, and trying to FOIL everything out, we will end up with $\text{numTerms}(f)^{p-1}$ terms, which arise from choosing any one of the $\text{numTerms}(f)$ in each of the $p-1$ f's to get the product.

So, we need to count the number of ways to select a sequence of $p-1$ starting terms of f that multiply to D.

This has become a counting problem: How many lattice paths are there from the origin to a point D on the line/plane/hyperplane $x_1 + x_2 + ... + x_n = n(p-1)$ with $x_i \geq 0$, where the only steps allowed satisfy $x_1 + x_2 + ... + x_n = n$?

Let $WIC(d, n)$ denote the set of weak integer compositions of d into n parts, or

$\{(a_1, a_2, ..., a_n) | \sum_{i=1}^n a_i = d, a_i \geq 0\}$

Note that $WIC(n, n)$ represents the degrees of our starting terms of f.

We can now define a recurrence to compute the number of lattice paths to $D = (d_1, d_2, ..., d_n)$:

$(a_1, ..., a_n) \in WIC(n, n) \to \alpha(a_1, ..., a_n) = 1$

$$\alpha(d_1, d_2, ..., d_n) = \sum_{(a_1,...,a_n) \in WIC(n,n)} \alpha(d_1 - a_1, d_2 - a_2, ..., d_n - a_n)$$

So, we can now compute the coefficient of any term of our resulting expansion. But, we need the maximum coefficient, not just any coefficient.

Claim: The center coefficient of f^p for any integer p defined by the degree sequence $(p, p, ..., p)$ is greater than or equal to all other coefficients of f^p