Newton iteration for simultaneous algebraic equations

Abstract:
Various problems in computational number theory can be represented by simultaneous algebraic equations, often involving the coefficients of polynomials satisfying some identity. For exmaple, if N is an odd prime then an elliptic curve

$$(1) \quad E : Y^2 = P(X) = X^3 + aX^2 + bX + c$$

has an N-torsion point with X = x if and only if there exists a Weil function A(X) + Y B(X) of degree N whose N-th order zero has X-coordinate x; equivalently, if and only if the identity

$$(2) \quad A^2 - PB^2 = (X - x)^N$$

holds for some polynomials A,B of degree $(N-1)/2, (N-3)/2$ respectively, with $A(x)$ nonzero. Thus finding the N-torsion points on E amounts to finding all such identities (2) with P prescribed, and parametrizing all identities of that form with P varying as well amounts to finding equations for the modular curve $X_1(N)$ and certain rational functions on that curve.
The standard technique for solving simultaneous algebraic equations is to use Groebner bases, but this often takes infeasibly long even when one knows or expects that the answer will be reasonably simple, say with coefficients in a low-degree number field or a parametrizing curve of low genus. While our illustrative problems of computing torsion points and modular functions can be solved much more efficiently using division polynomials and q-expansions, one cannot expect such tools to be available in general.
We outline an alternative general approach, using multivariate Newton iteration. In practice, this approach often produces good enough approximations (either Archimedean or p-adic) that the exact solution can be surmised. We illustrate with two examples that lead to elliptic K3 surfaces of Neron-Severi rank 19 or 20. These surfaces and others like them were used in the computation of elliptic curves over Q of prescribed torsion with record Mordell-Weil rank; more structurally, in the case of rank 19 the parametrization also yields explicit formulas and other previously inaccessible information for certain Shimura modular curves.