Early Termination I

Andrew Novocin & Mark van Hoeij
Department of Mathematics, Florida State

Summary of Zassenh

Let $f \in \mathbb{Z}[x]$ be separable and monic with degree N. **Goal:** the factors of

Idea 1: If $g \in \mathbb{Z}[x]$ divides f then the coefficients of g are smaller than so

Idea 2: If $g \in \mathbb{Z}[x]$ divides f then g can be **reconstructed** when $g \bmod p^a$

Idea 3: Factor $f = f_1 \cdots f_r$ over $\mathbb{Z}_p$ (the p-adic integers). There are only **f** of f in $\mathbb{Z}_p[x]$. Each is of the form

$$g_{v_1,\ldots,v_r} := \prod f^{v_i}$$