A Johnston* (jannaston@gmail.com), 2003 Smith Ave, Baltimore, MD 21209. Exponential Hensel Lifting.

Traditional Hensel lifting finds roots for polynomials modulo $p^n$ given its roots modulo $p$, where $p$ is a prime integer. In other words, given $f(x) \in \mathbb{Z}[x], r_1 \in \mathbb{Z}/(p)$ such that $f(r_1) \equiv 0 \mod p$, and an integer $n > 1$, Hensel lifting finds $r_n \in \mathbb{Z}/(p^n)$ such that $f(r_n) \equiv 0 \mod p^n$.

This talk describes an exponential version of Hensel lifting. It details a method for finding discrete logarithms modulo $p^n$ given a discrete log modulo $p$: Given $\gamma, \sigma \in \mathbb{Z}, a_1 \in \mathbb{Z}/(p - 1)$ such that $\gamma^{a_1} \equiv \sigma \mod p$, and an integer $n > 1$, exponential Hensel lifting returns $a_n$ such that $\gamma^{a_n} \equiv \sigma \mod p^n$. (Received September 16, 2011)