Public Key Cryptography (Spring 2003)

Instructor: Adi Shamir *Teaching assistant: Eran Tromer*

Note: Solving polynomial equations modulo prime powers

We have seen Berlekamp's algorithm for finding square roots modulo a prime. However, this algorithm cannot be used directly for finding roots modulo a prime power p^e ($e > 1$) because $a^{\frac{p^e-1}{2}} = 1$ only holds for a small fraction of $a \in \mathbb{Z}_{p^e}$. We thus proceed as follows.

Finding square roots modulo p^2

Given a prime p and $a \in \mathbb{Z}_{p^2}$ we wish to find the solutions of

$$x^2 \equiv a \pmod{p^2} \tag{1}$$

We begin by solving the following (e.g., using Berlekamp's algorithm):

$$y^2 \equiv a \pmod{p} \tag{2}$$

Each solution x of (1) is congruent modulo p to a solution y of (2). It thus suffices to find, for each y, the values $x = y + ip$ that fulfill (1). This is done as follows.

$$a \equiv (y + ip)^2 \equiv y^2 + 2yip + i^2p^2 \equiv y^2 + 2yip \pmod{p^2} \tag{3}$$

so we wish to say:

$$i \equiv \frac{a - y^2}{2yp} \pmod{p^2} \tag{4}$$

In general we cannot divide by a multiple of p, because it does not have an inverse modulo p^2. However, by (2) we have $a - y^2 \equiv 0 \pmod{p}$, so the p factors cancel out: $a - y^2 \equiv tp \pmod{p^2}$ for some t, so we can compute i:

$$i = t/2y \pmod{p^2}$$

This fails if $2y$ does not have an inverse modulo p^2, or equivalently, when $\gcd(2y, p^2) > 1$. This happens when either $p = 2$ (which is an easy special case) or y is a multiple of p. In the latter case, if there exists a corresponding solution $x = y + ip$ then $a \equiv x^2 \equiv 0 \pmod{p^2}$, so we merely need to consider the trivial case $a = 0$ separately.

To conclude, we saw that each root modulo p can be "lifted" into a root modulo p^2 by simple computation. This is a special case of "Hensel lifting".

Finding square roots modulo p^e for $e > 2$

To find roots modulo p^4, we first find roots modulo p and "lift" them into roots modulo p^2 as above. Then, we then "lift" the roots modulo p^2 to into roots modulo p^4. This can be similarly to the above, except we replace p by p^2, and p^2 by p^4. The handling of non-invertible denominators can be generalized.

By such repeated squaring, we can compute roots modulo p^e for any e which is a power of 2. To compute roots modulo p^e for other e, simply compute the roots modulo $p^{e'}$ where $e' \geq e$ is a power of 2, and reduce them modulo p^e.

Finding roots of polynomials modulo p^e

The above generalizes from the special case of solving $x^2 = a$ (i.e., extracting square roots) to finding roots of arbitrary polynomials. The essential points are that in (3) $f(y + ip) \mod p_i$ is linear for any polynomial f, and that the cancellation of p in (4) always occurs.

Finding roots modulo arbitrary integers

To compute roots modulo an arbitrary natural number n whose prime factorization is known to be $n = p_1^{e_1} p_2^{e} \cdots p_l^{e_l}$, first compute the roots modulo each of the $p_i^{e_i}$ $(i = 1, \ldots, l)$ and them combine them using the Chinese remainder theorem.