Arithmetic Algorithms 2014: HW2 Revised

Taylor Lee

March 24, 2014

Problem 1

Part A:

First, since a has an inverse $\mod p$, we know that it has an inverse $\mod p^k$. Because of this, we know that the function $f(x) = a - \frac{1}{x} \mod p^k$ will have a root in $\mod p^k$. We can find it using Newton Iteration:

$$x_{i+1} = x_i - \frac{f_i(x_i)}{f_i'(x_i)} \Rightarrow x' = x - \frac{a - \frac{1}{x}}{\frac{1}{x^2}}$$

which in turn gives us:

$$x' = x - \left(a x^2 - x\right) = 2x - a x^2 = x(2 - a x)$$

Thus, by Hensel's lemma, if x_0 is a solution to $f(x) \mod p^k$, then $x_0' = x_0(2 - a x_0)$ will be a solution to $f(x) \mod p^{2k}$.

This can be further seen, since if we multiply both sides by a, we see a multiple of p^{2k} emerge:

$$a x' = 1 - 1 + 2xa - a^2 x^2 = 1 - (1 - a x)^2 \equiv 0 \pmod{p^{2k}}.$$

This is since $a x - 1 \equiv 0 \pmod{p^k} \Rightarrow (1 - a x)^2 \equiv 0 \pmod{p^{2k}}$. Thus we are left with:

$$a x' \equiv 1 \pmod{p^{2k}}.$$

Part B:

Here, we can not show that there will be a solution for $f(x) = a - \frac{1}{x^2} \pmod{p^k}$, since that would take the knowledge that a^{-1} is a quadratic residue, which is not given. However, since we know that a is invertible, we know that x^2 has an inverse (a), and that a solution to $f(x) = a - \frac{1}{x^2} \pmod{p^k}$ will also be a solution to our given congruence. Hence, with Newton iteration, by Hensel's lemma, we can show that, given x_0 is a solution to $f(x) \pmod{p^k}$, that

$$x_0' = x_0 - \frac{f(x_0)}{f'(x_0)} \Rightarrow x_0' = x_0 - \frac{a - \frac{1}{x^2}}{\frac{2}{x^3}}$$

which in turn gives us:

$$x_0' = x_0 - \left(\frac{a x_0^3 - x_0}{2}\right) = \left(\frac{x_0}{2}\right)\left(3 - a x_0^2\right) \pmod{p^{2k}}$$

Which will be a solution to our congruence, $\pmod{p^k}$.

This can be further seen:

We can slightly modify the previous right hand side to get:

$$x' = x + \frac{x}{2}\left(1 - a x^2\right)$$

And so after we square both sides and multiply through by a we get:

$$a x'^2 = a x^2 + a x^2\left(1 - a x^2\right) + \frac{a x^2}{4}\left(1 - a x^2\right)^2 \pmod{p^{2k}}.$$

Now we can see that the term on the far right is equivalent to $0 \pmod{p^{2k}}$, since $1 - a x^2 \equiv 0 \pmod{p^k}$. This last congruence also tells us that $1 - a x^2 \equiv c p^k \pmod{p^k}$, for some $c \in \{c : 0, 1, \ldots, p^k - 1\}$. Hence, our equality above becomes:

$$a x'^2 = 1 - c p^k + \left(1 - c p^k\right) c p^k = 1 - c p^k + c p^k + c^2 p^{2k} \equiv 1 \pmod{p^{2k}}.$$

Problem 2

Part A:

$L_t(a)$ is clearly linear, since whenever a polynomial is squared, all possible pairs of terms are multiplied together and added to the new sum, and the only time there are

not two copies of a these new terms in the new sum is when a term is paired with itself: hence for any $a \in R/[t]$, sending it through the map will only double the degrees of the terms of a, before finally subtracting at from this new term, $a^2 \pmod{\mathbb{Z}_2}$. In other words, if $a, b \in R/[t]$, then:

$$L_t(a+b) = (a+b)^2 - t(a+b) \pmod{\mathbb{Z}_2} = a^2 + b^2 - ta - tb \pmod{\mathbb{Z}_2}.$$

And hence $L_t(a)$ is $\mathbb{Z}_2$ linear.

Part B:

First, suppose that $a \in \ker(L_x)$, then $a^2 \equiv aX \pmod{f}$, and hence this congruency must hold for all $f_1, f_2, \ldots f_i$ irreducible factors of f. Since we have

$$a^2 \equiv ax \pmod{f_i}$$

for all f_i irreducible factors of f, we can make an observation regarding the form of the a in our congruences. Namely, since f_i is irreducible, it forms a field when it's quotient is taken from the polynomial ring $\mathbb{Z}_2[x]$. Hence, either a must have an inverse in $\mathbb{Z}[x]/(f)$, which would imply $a = X \pmod{f_i}$, or a must be zero $\pmod{f_i}$, which concludes our proof from left to right.

Now if a is congruent to $0, X \pmod{f_i}$, for some f_i, we can use the Chinese Remainder Theorem to create a solution to this system of congruences which will be unique $\pmod{f}$. To do this, we create a sum $\pmod{f}$ which is a chain of terms of the form $g_i = e_i f_i' a \pmod{f_i}$, where f_i' is the product of all the other irreducible f_j which divide f, besides f_i and e_i is the inverse of $f_i' \pmod{f_i}$. We can simply let $g_i = 0$ for i where $a \equiv 0 \pmod{f_i}$. Each of these terms g_i will sort of stick out at f_i by being congruent to $a \pmod{f_i}$ and zero everywhere else.

Now, if we only concentrate on g_i where $a \equiv X \pmod{f}_i$, this term is only congruent to $X \pmod{f_i}$ and zero everything else and hence is congruent to $X \pmod{f}$, and hence will be in the kernel of L_X, since $X^2 - X^2 = 0 \pmod{f}$.

Since L_X is $\mathbb{Z}_2$ linear, the sum all of the individual terms $G = \sum g_i$ that are added together to mimic the behavior of a single polynomial a over the smaller congruences will be mapped as if they were sent through the function individually and added together in the image. Since each one on its own is sent to zero, their sum in the image will be zero, which means their sum, if taken before the function, is in the kernel. Symbolically,

$$L_X(G) = L_X(g_1) + L_X(g_2) + \ldots + L_X(g_{i-1}) + L_X(g_i) = 0 + 0 + \ldots + 0 + 0 = 0.$$