An Approach to Hensel's Lemma

GARY MCGUIRE

Abstract. Hensel's Lemma is an important tool in many ways. One application is in factoring polynomials over $\mathbf{Z}$. The computation in applying Hensel's Lemma proceeds by using the Euclidean algorithm. In this short article we present another approach to Hensel's Lemma, and we show that the lift of a polynomial can be calculated in another way. In some cases this is computationally faster. The proof is a connection between Hensel's Lemma and the polynomial whose roots are the p-th powers of the roots of a given polynomial.

1. Introduction

Let $h(x)$ be a polynomial with integer coefficients. In this article we will assume that all polynomials are monic. Hensel's Lemma begins with a factorisation $h(x) = f_1(x)g_1(x)$ over $\mathbf{Z}_p$, where p is a prime and $gcd(f_1, g_1) = 1$, and inductively constructs a factorisation $h(x) = f_k(x)g_k(x)$ over $\mathbf{Z}_{p^k}$ with the property that $f_k(x) \equiv f_1(x) \pmod p$ and $g_k(x) \equiv g_1(x) \pmod p$. This "Hensel lift" from $\mathbf{Z}_p$ to $\mathbf{Z}_{p^k}$ is accomplished by repeated use of the Euclidean algorithm. For more details, and applications, see [2], [3] or [4]. Here is an example where $p = 2$.

k	$\mathbf{Z}_{p^k}[x]$	$f_k(x)$	$g_k(x)$	$= h(x)$
1	$\mathbf{Z}_2[x]$	$(x^3 + x + 1)$	$(x^4 + x^2 + x + 1)$	$= x^7 - 1$
2	$\mathbf{Z}_4[x]$	$(x^3 + 2x^2 + x + 3)$	$(x^4 + 2x^3 + 3x^2 + x + 1)$	$= x^7 - 1$
3	$\mathbf{Z}_8[x]$	$(x^3 + 6x^2 + 5x + 7)$	$(x^4 + 2x^3 + 7x^2 + 5x + 1)$	$= x^7 - 1$
4	$\mathbf{Z}_{16}[x]$	$(x^3 + 6x^2 + 5x + 15)$	$(x^4 + 10x^3 + 15x^2 + 5x + 1)$	$= x^7 - 1$
5	$\mathbf{Z}_{32}[x]$	$(x^3 + 6x^2 + 5x + 31)$	$(x^4 + 26x^3 + 31x^2 + 5x + 1)$	$= x^7 - 1$
6	$\mathbf{Z}_{64}[x]$	$(x^3 + 38x^2 + 37x + 63)$	$(x^4 + 26x^3 + 63x^2 + 37x + 1)$	$= x^7 - 1$

In Section 2 we will give another method for accomplishing the lifting of a factorisation. Our method will lift either a single polynomial in the factorisation, or both factors, using only polynomial

multiplication. The procedure in the previous paragraph lifts both factors $f_1(x)$ and $g_1(x)$ simultaneously. The lifting of one factor is sometimes all that is required; for example, this occurs in the lifting of generator polynomials of cyclic codes over $\mathbf{Z}_2$ to $\mathbf{Z}_4$, or more generally from $\mathbf{Z}_p$ to $\mathbf{Z}_{p^k}$. Coding theorists have been using the method of this article, and although we have not seen anything in print, this article contains nothing new. In Section 3 we compare the computational complexities of both methods. Section 4 will provide full details of one of the proofs.

The Hensel lift of a factorisation is defined above. We will now define the *Hensel lift* of a single polynomial. First we define the Hensel lift of irreducible divisors of $x^n - 1$, and then proceed to define the Hensel lift for an arbitrary divisor of $x^n - 1$. Sometimes we will refer to the Hensel lift simply as the lift.

If $f(x) \in \mathbf{Z}_p[x]$ is a monic irreducible divisor of $x^n - 1$, the Hensel lift to $\mathbf{Z}_{p^k}$ of $f(x)$ is defined to be the unique monic irreducible polynomial $f_k(x) \in \mathbf{Z}_{p^k}[x]$ such that $f_k(x) \equiv f(x) \pmod{p}$ and $f_k(x)$ divides $x^n - 1$ in $\mathbf{Z}_{p^k}[x]$. For a proof of the existence and uniqueness of $f_k(x)$, see Theorem 1 below. With $g(x) = (x^n - 1)/f(x)$, this is the same result as would be found if we lifted the factorisation $h(x) = x^n - 1 = f(x)g(x)$ in $\mathbf{Z}_p[x]$ to $x^n - 1 = f_k(x)g_k(x)$ in $\mathbf{Z}_{p^k}[x]$, by uniqueness.

The Hensel lift of any monic $f(x) \in \mathbf{Z}_p[x]$ which divides $x^n - 1$ is obtained by factoring $f(x)$ into irreducible factors in $\mathbf{Z}_p[x]$, then lifting each irreducible factor to $\mathbf{Z}_{p^k}[x]$ and multiplying the lifts together.

We could even define the Hensel lift of any monic $f(x) \in \mathbf{Z}_p[x]$, by defining the lift to be the product of the lifts of the irreducible factors of $f(x)$, but we will not discuss this further.

2. The Results

Our method is based on finding the polynomial whose roots are the p-th powers of the roots of a given polynomial $a(x)$. Corollary C below can be seen as a generalisation of the familiar method of calculating a polynomial whose roots are the squares of a given $a(x)$, which is to replace x^2 by x in the polynomial $a(x)a(-x)$.

Theorem A. *Let $a(x)$ be a polynomial with rational coefficients. Let $\omega \neq 1$ be a complex n-th root of unity, for any integer $n > 1$.*

If $r \geq 1$ is relatively prime to n then the coefficient of x^r in the polynomial

$$b(x) = \prod_{j=1}^{n} a(\omega^j x)$$

is zero. All the coefficients of $b(x)$ are rational, and if $a(x)$ has integer coefficients, then so does $b(x)$.

Proof: It is clear that $b(x)$ has rational coefficients since it is fixed by the Galois group of the extension $\mathbf{Q}(\omega)/\mathbf{Q}$. If $a(x)$ has integer coefficients, then the coefficients of $b(x)$ are algebraic integers, and therefore rational integers.

If $a(x) = \sum a_i x^i$ then the coefficient of x^r in $b(x)$ is

$$\sum a_{i_0} a_{i_1} \cdots a_{i_{n-1}} \omega^{i_1+2i_2+3i_3+\cdots+(n-1)i_{n-1}}$$

where the sum is over all n-tuples $(i_0, i_1, i_2, \ldots, i_{n-1})$ such that each $i_j \geq 0$ and $i_0 + i_1 + i_2 + \cdots + i_{n-1} = r$. In this sum, consider the n terms arising from any particular n-tuple and its n cyclic shifts. If r is relatively prime to n, we will show that the sum of these n terms is zero. This will complete the proof.

Since the coefficients $a_{i_0} a_{i_1} \cdots a_{i_{n-1}}$ in the n terms are all equal, to show that the sum of these n terms is zero it will suffice to show that the n powers of ω are all distinct, and then use the fact that $1+\omega+\omega^2+\cdots+\omega^{n-1} = 0$. Suppose to the contrary that two of the powers are equal. By relabelling the i_j if necessary, we may assume that

$$\omega^{i_1+2i_2+3i_3+\cdots+(n-1)i_{n-1}} = \omega^{i_{k+1}+2i_{k+2}+3i_{k+3}+\cdots+(n-1)i_{k+n-1}}$$

(reading subscripts modulo n) for some k satisfying $0 < k < n$. If we consider the exponents, this implies

$$\sum_{m=0}^{n-1} m i_m \equiv \sum_{m=0}^{n-1} m i_{k+m} \pmod{n}.$$

But this righthand side is congruent modulo n to $\sum_{s=0}^{n-1}(s-k)i_s$, and so

$$\sum_{m=0}^{n-1} m i_m \equiv \sum_{s=0}^{n-1}(s-k)i_s \equiv \sum_{s=0}^{n-1} s i_s - \sum_{s=0}^{n-1} k i_s \pmod{n}$$

giving $\sum_{s=0}^{n-1} ki_s \equiv 0 \pmod{n}$. Now we use that fact that $i_0 + i_1 + i_2 + \cdots + i_{n-1} = r$ to conclude $kr \equiv 0 \pmod{n}$, which is impossible if r and n are relatively prime. □

Corollary B. *Let $a(x)$ be a polynomial with integer coefficients. Let $\omega \neq 1$ be a p-th root of unity, for any prime p. Then the integral polynomial*

$$b(x) = \prod_{j=1}^{p} a(\omega^j x)$$

is a polynomial in x^p.

Corollary C. *Let $a(x)$ be a monic polynomial with integer coefficients, and let p be a prime. Let $b(x)$ be as in Corollary B. Then the monic integral polynomial $c(x)$ whose roots are the p-th powers of the roots of $a(x)$ is*

$$c(x) = b(x^{1/p}).$$

Now that we have shown how to calculate the polynomial whose roots are the p-th powers of a given polynomial, we shall show that this polynomial is the lift that is produced by Hensel's Lemma. This will be shown in the course of the proof of Theorem 1, which is why we include the proof although the result is not new (see [1] for example—we will give their proof). Usually Theorem 1 is given as a corollary of Hensel's Lemma.

Theorem 1. *Let $f_k(x)$ be a monic irreducible divisor of $x^n - 1$ in $\mathbf{Z}_{p^k}[x]$ for any $k \geq 1$. Assume n and p are relatively prime. Then there exists a unique monic irreducible polynomial $f_{k+1}(x)$ which divides $x^n - 1$ in $\mathbf{Z}_{p^{k+1}}[x]$ and such that $f_{k+1}(x) \equiv f_k(x) \pmod{p^k}$.*

Proof: (Sketch—for full details see Section 4.) Let S_k be the set of n-th roots of unity in an extension ring of $\mathbf{Z}_{p^k}$. If $\alpha \in S_k$ is a root of $f_k(x)$, then in $\mathbf{Z}_{p^{k+1}}[S_{k+1}]$ we have $\alpha^n = 1 + p^k\delta$ for some $\delta \in S_{k+1}$. It follows that $\alpha^{np} = 1$. We conclude that the polynomial in $\mathbf{Z}_{p^{k+1}}[x]$ whose roots are the p-th powers of the roots of $f_k(x)$ is a lift of $f_k(x)$. For uniqueness see section 4. If $f_{k+1}(x)$ were reducible, then reduction modulo p^k would imply that $f_k(x)$ is reducible. □

Corollary 2. *Given $f_k(x)$, $f_{k+1}(x)$ can be calculated as follows:*
1. *Regard $f_k(x)$ as having integer coefficents.*
2. *Compute the polynomial $c(x)$ in Corollary C (with $f_k(x)$ in place of $a(x)$).*
3. *Reduce $c(x)$ modulo p^{k+1}.*

We can now summarise our approach.

INPUT: A monic polynomial $f(x) \in \mathbf{Z}_p[x]$ dividing $x^n - 1$.

WANTED: The Hensel lift of $f(x)$ to $\mathbf{Z}_{p^k}[x]$.

PROCEDURE: Factor $f(x)$ into irreducible factors. For each irreducible factor iterate Corollary 2 $k-1$ times, i.e., lift from $\mathbf{Z}_{p^m}$ to $\mathbf{Z}_{p^{m+1}}$ for $m = 1, 2, \ldots, k-1$. Then multiply the lifts of each factor together.

We remark that by iterating Corollary 2 indefinitely, we would get the p-adic lift of $f(x)$.

3. Computational Complexity

Here we (rather crudely) compare the complexity of using Corollary 2 to calculate the lift versus the usual method. The worst feature of the Corollary 2 method is that the given polynomial $f(x)$ to be lifted has to be factored into irreducible factors in $\mathbf{Z}_p[x]$.

Assume for the moment that $f(x)$ is a monic irreducible polynomial in $\mathbf{Z}_p[x]$, of degree r, say. In this case there is no factoring required. To calculate the lift of $f(x)$ to $\mathbf{Z}_{p^2}$, we must multiply p polynomials of degree r together. According to [2], multiplication of two degree r polynomials using the Fast Fourier Transform takes $O(r \log r)$ operations, so the multiplication of our p polynomials of degree r takes $O(pr \log pr)$ operations. However, this may not be strictly accurate in our case since the coefficients are not integers, and the simplification of these coefficients is not taken into account.

The Euclidean algorithm calculation in Hensel's Lemma takes $O(m(\log m)^2 \log\log m)$ operations where m is the largest of the degrees of the two polynomials, see [2]. If $f(x)$ has degree r then $m = n - r$ where n is the smallest n such that $f(x)$ divides $x^n - 1$.

In the case that $f(x)$ is a primitive irreducible polynomial, we have $n = p^r - 1$ and $m = p^r - 1 - r$, so in this crude comparison we see that using Corollary 2 is faster for large r and fixed p. This was

borne out by *Mathematica* experiments. For example, if $p = 3$ and $r = 30$ then $pr = 120$, but $m = p^r - 1 - r = 3^{30} - 31$ is much larger than pr.

For small r we tested some examples on *Mathematica* and the Euclidean algorithm method was faster, as one might expect.

4. Technical Details

In this section we give a more complete proof of Theorem 1. The complications arise from the fact that we are dealing with polynomials which have coefficients in a ring (with zero-divisors), and not a field. We would like to know that extension rings always exist containing the roots of these polynomials, as happens with a field. Since we are always working with monic polynomials within the roots of unity, this is true.

The proper framework is really the field of p-adic numbers Q_p. If S is the set of n-th roots of unity in an extension field of Q_p, then we consider the ring $Z_p[S]$ where Z_p is the ring of p-adic integers. For each k there is the reduction modulo p^k homomorphism $\phi_k \colon Z_p \longrightarrow \mathbf{Z}_{p^k}$ and this can be extended to $Z_p[S]$. Let $S_k = \phi_k(S)$. For example, S_1 is the set of n-th roots of unity in an extension field of $\mathbf{Z}/p\mathbf{Z}$.

There are also homomorphisms $\psi_k \colon \mathbf{Z}_{p^{k+1}} \longrightarrow \mathbf{Z}_{p^k}$ which are reduction modulo p^k. For example,

$$\psi_k^{-1}(1) = \{1 + p^k\delta : \delta \in S\}.$$

This set has n elements, but note that all n elements have the same p-th power, namely 1.

To prove Theorem 1, let $T \subseteq S_k$ be the set of roots of $f_k(x)$. Take the p-th powers of the elements of $\psi_k^{-1}(T)$. If $\alpha_k \in T$ then a pre-image of α_k in $\psi_k^{-1}(T)$ looks like $\alpha_{k+1} = \alpha_k + p^k\delta$ so that $\alpha_{k+1}^p = \alpha_k^p$. This gives us $\deg(f_k)$ elements of $\mathbf{Z}_{p^{k+1}}[S_{k+1}]$ each of whose n-th power is 1. Clearly their reduction modulo p^k gives the roots of $f_k(x)$, i.e., $\psi_k(\psi_k^{-1}(T)^p) = T$. These two properties mean that we can take the p-th powers of the elements of $\psi_k^{-1}(T)$, and form the polynomial with these as roots, and this polynomial will be $f_{k+1}(x)$.

To prove uniqueness, suppose there are two polynomials $g(x)$ and $g'(x)$ in $\mathbf{Z}_{p^{k+1}}[x]$ which divide $x^n - 1$ and reduce modulo p^k to $f_k(x)$.

Let β and β' be roots of $g(x)$ and $g'(x)$ respectively, both of which reduce modulo p^k to α. Then $\beta^n = 1 = \beta'^n$ of course, so $(\beta/\beta')^n = 1$. But also $\beta^p = \beta'^p$ so $(\beta/\beta')^p = 1$. Since n and p are relatively prime we get $\beta = \beta'$ and therefore $g(x) = g'(x)$.

References

[1] A. R. Calderbank and N. J. A. Sloane, Modular and p-adic cyclic codes, *Designs Codes and Cryptography* **6** (1995), 21–35.
[2] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, 1999.
[3] K. O. Geddes, S. R. Czapor, G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic Publishers, 1992.
[4] B. L. van der Waerden, *Algebra Volume II*, Springer-Verlag, 1991.

Gary McGuire,
Department of Mathematics,
National University of Ireland,
Maynooth, Co. Kildare, Ireland
gmg@maths.may.ie

Received 2 November 2000 and in revised form on 23 November 2001.