Hensel Interpolation

Lecture 9

Recall our typical mapping from GCD

$$\begin{tikzcd}
\mathrm{GCD}(F(x,y,z),G(x,y,z)) \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & H(x,y,z) \\
\mathrm{GCD}(F_p(x,y,z),G_p(x,y,z)) \arrow[d, shift left=3] \arrow[d, shift left=1] \arrow[d, shift right=1] \arrow[d, shift right=3] & H_p(x,y,z) \arrow[u, shift left] \arrow[u, shift right] \\
\mathrm{GCD}(F_p(x,0,0),G_p(x,0,0)) \arrow[r, shift left] \arrow[r, shift right] & H_p(x,0,0) \arrow[u, shift left=3] \arrow[u, shift left=1] \arrow[u, shift right=1] \arrow[u, shift right=3]
\end{tikzcd}$$

Start in the lower right corner of this diagram with some image of a factorization

- c(x)*h(x)=f(x) mod p
- ... we have c mod p, h mod p.   (and f mod p)
- ... we want to know c and h over Z [x], in fact, over Z[x,y,z,...] as many variables as are necessary.

- note that here c(x) is the cofactor of f, (c=f/h), and h is the gcd(f,g).
- ALSO we'll sometimes need to trump up these --otherwise in general --false assumptions..
- f(x) and h(x) are monic [leading coeff 1]
- f(x) and h(x) are "square-free". That is, $f(x)=k^2(x)$*... is forbidden.

Aside..

- Removing squared factors takes some effort, but not as much as factoring generally, so this is a good move if the problem is to find factors. Compared to taking a GCD, it is not such a clear win, but still, it must be done.
- Making the input monic by separating the content and primitive part, then dividing (in a finite field) by the leading coefficient; we must replace these factors, perhaps at considerable cost (the leading coefficient may be a polynomial in other variables!)

Recall p-adic notation

If p and N are integers, then the p-adic representation of N is

(a_0, a_1, ..., a_m) where for i = 1, ...,m = we have

$(-p+1)/2 \leq ai < (p-1)/2$ or here we will use.. $0 \leq a_i < p$

$N = a_0 p^0 + a_1 p^1 + \ldots + a_m p^m$

For instance, the 3-adic representation of the integer 65 is (2,0,1,2).= $2+0*3+1*3^2+2*3^3 = 2+9+54 = 65$

p-adic notation for polynomials

We can extend this notion to polynomials. If p(x) and q(x) are polynomials (in x), then the p-adic representation of q is $(a_1, a_2, ..., a_m)$ where for i=1, ..., m-1, a_i is in an integer, a_m is a nonzero integer and

$q(x) = a_0p(x)^0 + a_1p(x)^1 + ... +a_mp(x)^m$

For instance the (x-1)-adic representation of x^3 is (1,3,3,1) $= 1+ 3*(x-1)+3(x-1)^2+1*(x-1)^3 = 1+3x-3+3x^2-6x+3+x^3-3x^2+3x-1 = x^3$

Hensel Algorithms

Start with a p-adic approximate and compute ever more accurate versions. When we get a high enough approximation p^r we hope (or prove) it will be good over the integers.

The original linear Hensel Construction lifts a factorization

from mod p^i to mod p^{i+1} at the ith step

while the quadratic construction due to Zassenhaus lifts a factorization from mod $(p^2)^i$ to mod $(p^2)^{i+1}$

That is, twice as many terms instead of one more term. Nevertheless, the linear version may require so much less computation at each step that it may be the algorithm of choice in lifting to a given power of a modulus.

Starting up.. Algorithm

Let $u(x)$ be a monic polynomial . (As previously noted, this assumption is, in general, unwarranted. Since overcoming it makes the algorithm messy, we ignore it.)

in $Z[x]$ and assume $v_1(x)$ ¢ $w_1(x) = u(x) \bmod p$ and GCD $(v_1,w_1) = 1 \bmod p$ where p is a prime.

The algorithm computes a sequence of pairs of polynomials

$\{(v_i,w_i)\}$ such that

$v_i(x)$ ¢ $w_i(x) = u(x) \bmod p^i$

Step I

Compute by means of the Extended Euclidean Algorithm

generalized to polynomials, two polynomials $a(x)$ and $b(x)$ in $Z_p[x]$ such that

(i) $\deg(a) < \deg(w_1)$

(ii) $\deg(b) < \deg(v_1)$

(iii) $(a(x)v_1 + b(x)w_1 = 1) \bmod p$

Step II

Now suppose we are given (v_i, w_i) and we wish to compute (v_{i+1},w_{i+1}). Compute a polynomial c_i such that

$(p^i c_i(x) = v_i(x) w_i(x) - u(x)) \bmod p^{i+1}$

How hard is this? a multiply, subtraction, and division with remainder

Step III

Compute (by polynomial division of $a(x)c_i(x)$ by $w_1(x)$) the quotient $q_i(x)$ and remainder $a_i(x)$ such that

$a(x)c_i(x) = q_i(x)w_1(x) + a_i(x) \bmod p$

and set

$b_i(x) := (b(x)c_i(x) + q_i(x)v_1(x)) \bmod p$

Observe that $\deg(a_i)<\deg(w_1)$, $\deg(b_i)<\deg(v_i)$

and mod p,

$a_i v_1 + b_i w_1 = (a ¢ c_i - w_1 q_i)v_1 + (b ¢ c_i + v_1 q_i)w_1$

$= c_i(a ¢ v_1 + b ¢ w_1)$

$= c_i$

Step III- observation

{so in Z[x] , (or $Z_{p2}[x]$)

$a_i v_1 + b_i w_1 = c_i + p$ ¢ $d_i(x)$ for some $d_i(x)$ in Z[x]

Step IV

Set

$v_{i+1}(x) \quad := \quad v_i(x)-p^i b_i(x) \bmod p^{i+1}$

$w_{i+1}(x) \quad := \quad w_i(x)-p^i a_i(x) \bmod p^{i+1}$

Observe that, over the integers

$v_{i+1}(x)w_{i+1}(x) \quad = \quad v_i(x)w_i(x)- p^i[a_i(x)v_i(x)+b_i(x)w_i(x)] + p^{2i} \text{¢} a_i(x)b_i(x)$

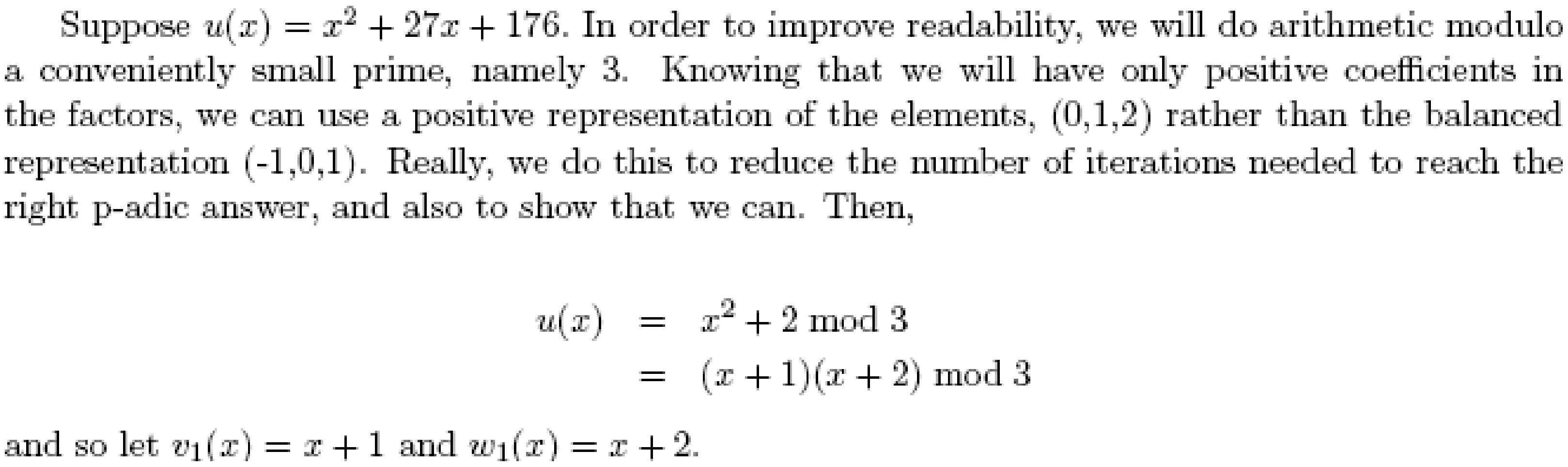
$= u(x) + p^i \text{¢} c_i(x) - p^i[c_i(x) +p \text{¢} d_i(x)] + p^{2i} \text{¢} a_i(x)b_i(x)$

$= u(x) - p^{i+1}[d_i(x)-p^{i-1} \text{¢} a_i(x)b_i(x)$

that is,

$v_{i+1}(x)w_{i+1}(x) = u(x) \bmod p^{i+1}$ (QED)

An Example (see online notes “Hensel.pdf”)

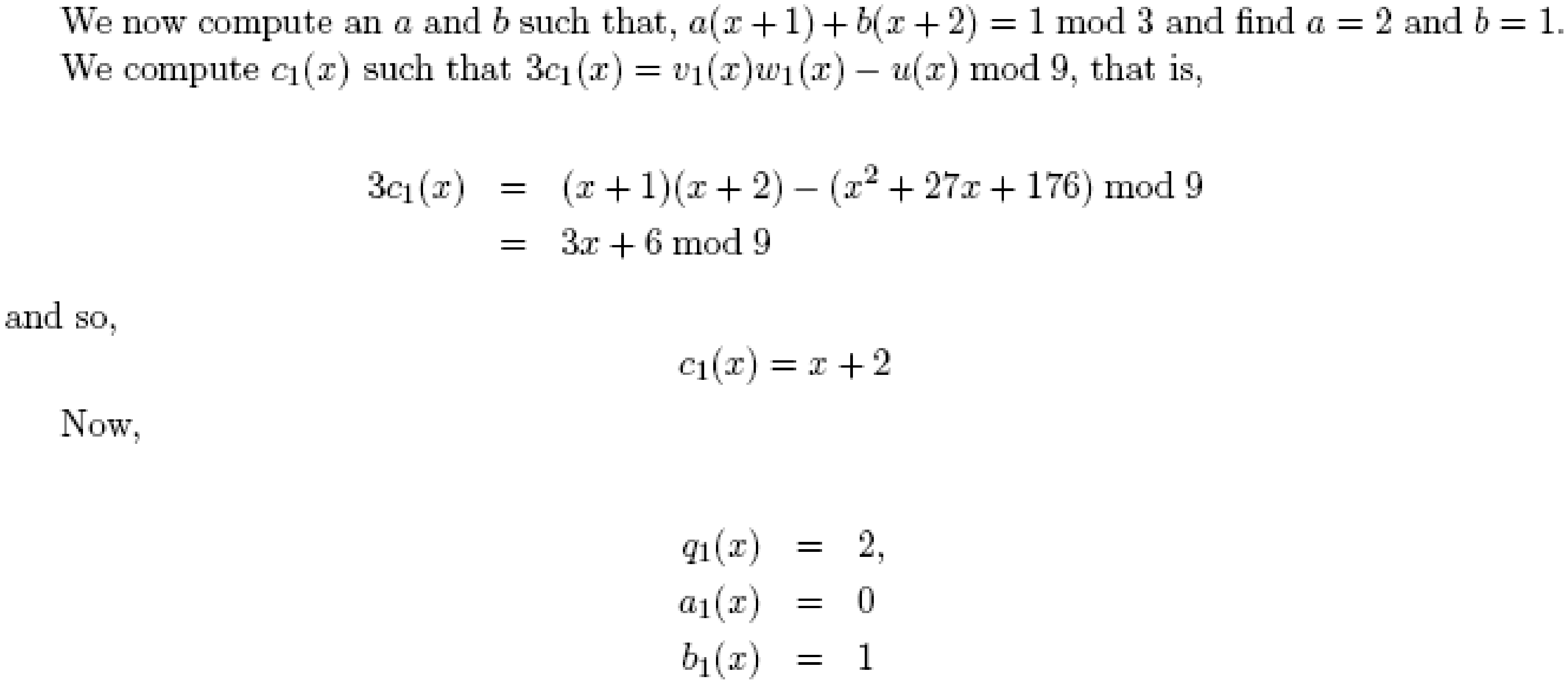


Suppose $u(x) = x^2 + 27x + 176$. In order to improve readability, we will do arithmetic modulo a conveniently small prime, namely 3. Knowing that we will have only positive coefficients in the factors, we can use a positive representation of the elements, (0,1,2) rather than the balanced representation (-1,0,1). Really, we do this to reduce the number of iterations needed to reach the right p-adic answer, and also to show that we can. Then,

$$\begin{aligned} u(x) &= x^2 + 2 \bmod 3 \\ &= (x+1)(x+2) \bmod 3 \end{aligned}$$

and so let $v_1(x) = x + 1$ and $w_1(x) = x + 2$.

Continuing…



We now compute an a and b such that, $a(x+1)+b(x+2)=1 \bmod 3$ and find $a=2$ and $b=1$. We compute $c_1(x)$ such that $3c_1(x)=v_1(x)w_1(x)-u(x) \bmod 9$, that is,

$$\begin{aligned} 3c_1(x) &= (x+1)(x+2)-(x^2+27x+176) \bmod 9 \\ &= 3x+6 \bmod 9 \end{aligned}$$

and so,

$$c_1(x)=x+2$$

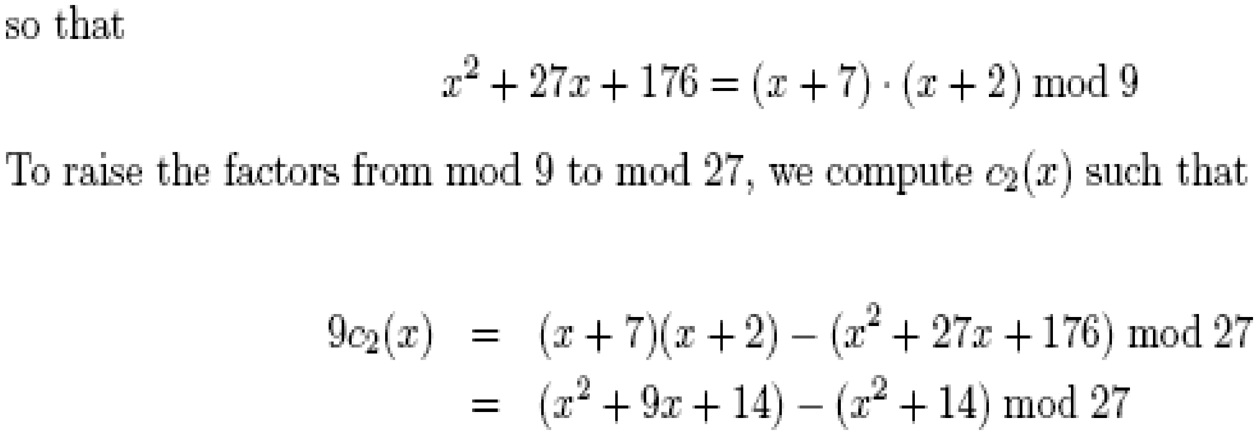
Now,

$$\begin{aligned} q_1(x) &= 2, \\ a_1(x) &= 0 \\ b_1(x) &= 1 \end{aligned}$$

Result Modulo 9

$$\begin{aligned} v_2(x) &= (x+1) - (3)\cdot(1) \bmod 9 \\ &= x+7 \\ w_2(x) &= (x+2) - (3)\cdot(0) \bmod 9 \\ &= x+2 \end{aligned}$$

We must go further, to mod 3^3



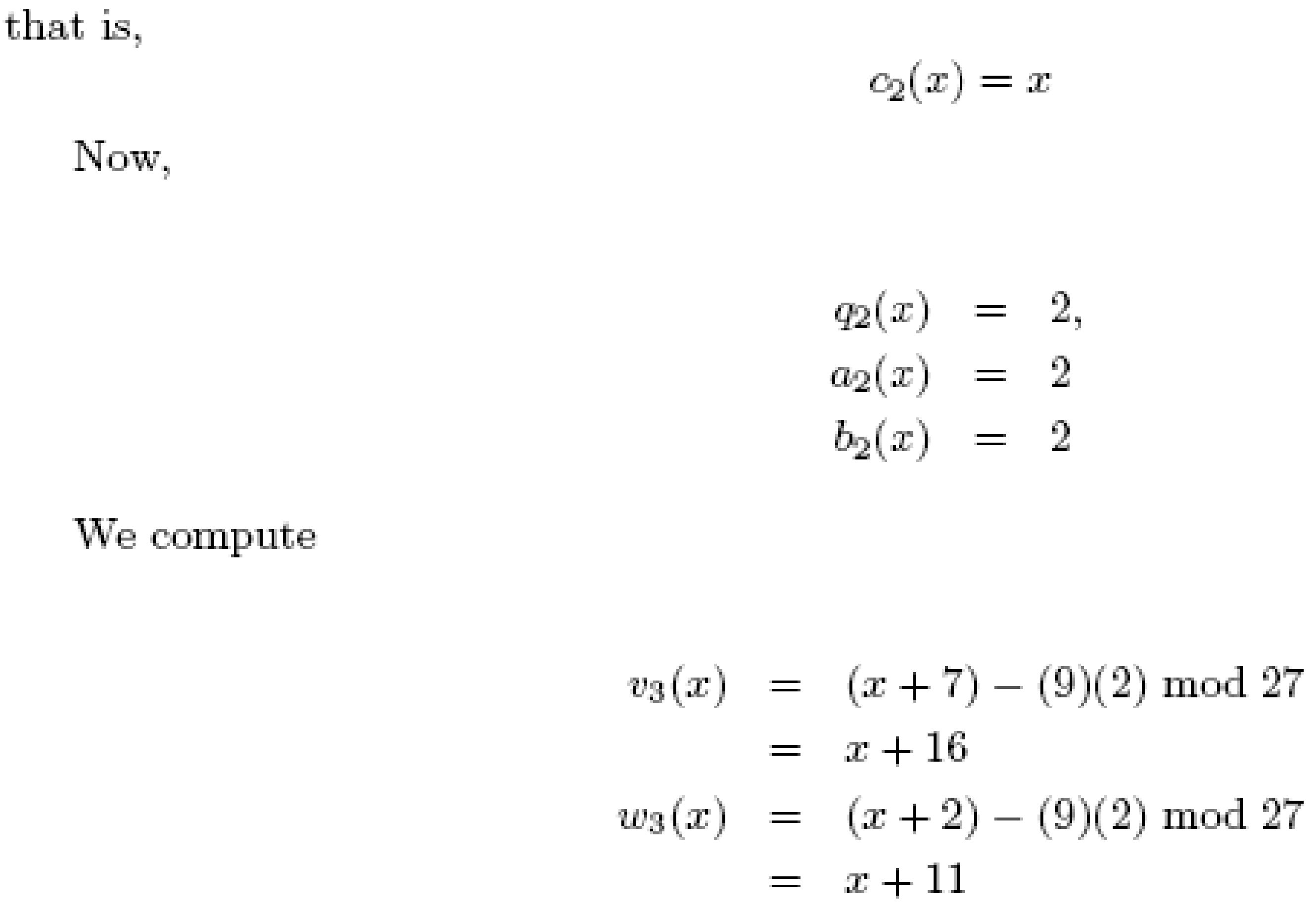
so that

$$x^2 + 27x + 176 = (x + 7) \cdot (x + 2) \bmod 9$$

To raise the factors from mod 9 to mod 27, we compute $c_2(x)$ such that

$$\begin{aligned} 9c_2(x) &= (x + 7)(x + 2) - (x^2 + 27x + 176) \bmod 27 \\ &= (x^2 + 9x + 14) - (x^2 + 14) \bmod 27 \end{aligned}$$

Here are the steps



that is,

$$c_2(x) = x$$

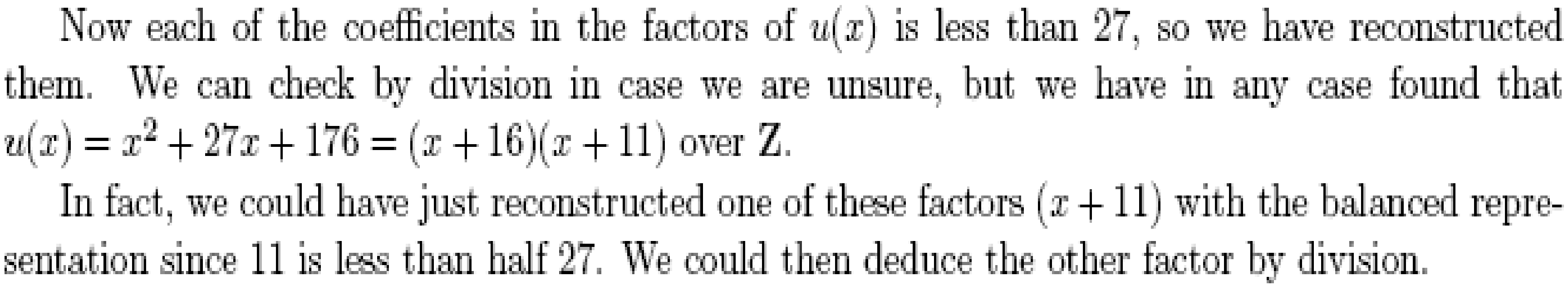
Now,

$$\begin{aligned} q_2(x) &= 2, \\ a_2(x) &= 2 \\ b_2(x) &= 2 \end{aligned}$$

We compute

$$\begin{aligned} v_3(x) &= (x+7) - (9)(2) \bmod 27 \\ &= x + 16 \\ w_3(x) &= (x+2) - (9)(2) \bmod 27 \\ &= x + 11 \end{aligned}$$

Check (x+16)*(x+11)



Now each of the coefficients in the factors of $u(x)$ is less than 27, so we have reconstructed them. We can check by division in case we are unsure, but we have in any case found that $u(x) = x^2 + 27x + 176 = (x + 16)(x + 11)$ over **Z**.

In fact, we could have just reconstructed one of these factors $(x + 11)$ with the balanced representation since 11 is less than half 27. We could then deduce the other factor by division.

end