

Math 819 course project list: Spring 2007

Instructor: Michael Monagan

Please submit the project by 5pm Friday April 15th.

The modular GCD algorithm and Hensel lifting algorithm.

REFERENCE: Sections 6.5 and 7.4 of the Geddes et. al. text.

Consider the problem of computing GCDs in $\mathbb{Z}_q[t][x]$, q a prime. If q is large then we can use evaluation and interpolation, i.e., we can evaluate at $t = 0, 1, 2, \dots$. If q is small, e.g. $q = 2$, this will not work as there will be insufficient evaluation points to interpolate the gcd. Moreover, $t = 0$ and $t = 1$ may be bad or unlucky.

But $\mathbb{Z}_q[t]$ is a Euclidean domain and there are an infinite number of primes (irreducibles) in $\mathbb{Z}_q[t]$ which can play the role of primes in the modular GCD algorithm and the prime p in the univariate Hensel lifting algorithm for computing GCDs in $\mathbb{Z}_q[t][x]$.

This project is to first modify the modular GCD algorithm to compute a gcd in $\mathbb{Z}_q[t][x]$ by using irreducibles $p_1, p_2, \dots \in \mathbb{Z}_q[t]$. To do this we need a source of primes in $\mathbb{Z}_q[t]$ and we need to solve the Chinese remainder problem in $\mathbb{Z}_q[t]$.

The second part of the project is to modify the Hensel lifting algorithm to work in $\mathbb{Z}_q[t][x]$ by choosing one irreducible $p \in \mathbb{Z}_q[t][x]$ and lifting mod p^k (not difficult) and to make it efficient (you need to think).

1. Restate and prove the Chinese remainder theorem for $\mathbb{Z}_q[t]$.
Now modify the Chinese remainder algorithm for \mathbb{Z} to work for $\mathbb{Z}_q[t]$. To make sure you understand it correctly, implement it and test your algorithm on the following problem: find $u \in \mathbb{Z}_2[t]$ such that

$$u \equiv t^2 \pmod{t^3 + t + 1} \quad \text{and} \quad u \equiv t^2 + t + 1 \pmod{t^3 + t^2 + 1}.$$

For the extended Euclidean algorithm in $\mathbb{Z}_q[t]$, use Maple's `Gcdex(...)` mod q command to compute the required inverses.

2. Modify the modular GCD algorithm for $\mathbb{Z}[x]$ to work in $\mathbb{Z}_p[t][x]$. Test your algorithm on the following inputs $a, b \in \mathbb{Z}_3[t][x]$ where $a = g\bar{a}, b = g\bar{b}$ where

$$g = (t^3 - t)x^5 - t^{11}x^3 + t^7x + t^9 + 1, \bar{a} = tx^5 - t^6x^2 + 1, \bar{b} = tx^4 + x^2 + t^7.$$

3. Modify the linear-Hensel lifting algorithm to work modulo p where p is an irreducible in $\mathbb{Z}_q[t]$. Test your algorithm on the above inputs using $p = t^3 + 2t + 1$. This irreducible is not unlucky.
4. The expensive part of the Hensel lifting is computing the error $e_k = a - u^{(k)}w^{(k)}$ at each step (the multiplication is expensive) and dividing the error by p^k which is polynomial in t . Assuming classical algorithm for polynomial multiplication and division in $\mathbb{Z}_p[t]$, if $\deg_x a = n$ and $\deg_t a = m$ then calculating e_k is $O(n^2k^2)$ and dividing e_k by p^k is $O(n^2(m - k + 1)k)$ which leads to a total cost of $O(n^2m^3)$. Modify the Hensel lifting to reduce the cost of computing the error to $O(n^2m^2)$. Hint:

$$\begin{aligned} a - u^{(k)}w^{(k)} &= a - (u^{(k-1)} + u_{k-1}p^{k-1})(w^{(k-1)} + w_{k-1}p^{k-1}) \\ &= [a - u^{(k-1)}w^{(k-1)}] - [u^{(k-1)}w_{k-1} + u_{k-1}w^{(k-1)}]p^{k-1} - u_{k-1}w_{k-1}p^{2k-2} \\ &= e_{k-1} - [u^{(k-1)}w_{k-1} + u_{k-1}w^{(k-1)}]p^{k-1} - u_{k-1}w_{k-1}p^{2k-2}. \end{aligned}$$

5. Finally, identify the unlucky irreducibles for the above GCD problem.

Notes: (1) For a source of primes in $\mathbb{Z}_3[t]$ use the `Nextprime(...)` mod 3 command. (2) To compute a GCD of two polynomials $f_1, f_2 \in \mathbb{Z}_q[t][x]$ modulo an irreducible polynomial $m(x)$, use the following Maple command:

```
> alias(a=RootOf(m) mod q);
> g := subs(a=t, subs(t=a, Gcd(f1, f2) mod q));
```