Math 801 course project list: Spring 2017

Instructor: Michael Monagan
Due 4pm Monday April 17th.
Late penalty: -20% for up to 48 hours late.

The modular GCD algorithm and Hensel lifting algorithm.

REFERENCE: Sections 6.5 and 7.4 of the Geddes 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 $t = 0, 1, 2, ...$ and interpolate the coefficients in $\mathbb{Z}_q[t]$. If q is small, e.g. $q = 2$, this will not work as there will be insufficient evaluation points in $\mathbb{Z}_q$ to interpolate t in the gcd. Moreover, $t = 0$ and $t = 1$ may be bad or unlucky, in which case we could not use Hensel lifting either.

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 $\mathbb{Z}_q[t][x]$. For example, here are the irreducibles in $\mathbb{Z}_2[t]$ up to degree 4.

$$t, t+1, t^2+t+1, t^3+t+1, t^3+t^2+1, t^4+t+1, t^4+t^3+1, t^4+t^3+t^2+t+1.$$

This project is to first modify the modular GCD algorithm to compute a gcd in $\mathbb{Z}_q[t][x]$ by using irreducibles $p_1, p_2, ... \in \mathbb{Z}_q[t]$. 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 $p \in \mathbb{Z}_q[t]$ and lifting mod p^k (not difficult) and to make it efficient (you need to think).

Question 1 (15 marks)

We have seen the Chinese remainder theorem for $\mathbb{Z}$. First state and prove a 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

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

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

Question 2 (15 marks)

Modify the modular GCD algorithm for $\mathbb{Z}[x]$ to work in $\mathbb{Z}_q[t][x]$. 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

$$g = (t^3 - t)\,x^5 - t^{11}x^3 + t^7x + t^9 + 1,$$

$$\bar{a} = tx^5 - t^6x^2 + 1, \text{ and}$$

$$\bar{b} = tx^4 + x^2 + t^7.$$

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

```
> a := RootOf(p) mod q;
> g := Gcd(subs(t=a,f1),subs(t=a,f2)) mod q;
> if not type(a,integer) then g := subs(a=t,g); fi;
```

Question 3 (15 marks)

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 inputs in question 2 using $p(t) = t^3 + 2t + 2$ in Maple. This irreducible is not unlucky and it satisfies the other requirements for Hensel lifting to work. You will need the extended Euclidean algorithm to solve $SA + TB = G$ over the finite field $\mathbb{Z}_q[t]/p(t)$. Use the following Maple commands:

```
> a := RootOf(p) mod q;
> G := Gcdex(subs(t=a,A),subs(t=a,B),x,'S','T') mod q;
> if not type(a,integer) then G,S,T := op(subs(a=t,[G,S,T])); fi;
```

Question 4 (15 marks)

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 polynomial multiplication, if $\deg_x a = n$ and $\deg_t a = m$ then calculating e_k costs $O(n^2k^2)$ arithmetic operations in $\mathbb{Z}_p$ 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: $a - u^{(k)}w^{(k)} = a - (u^{(k-1)} + u_{k-1}p^{k-1})(w^{(k-1)} + w_{k-1}p^{k-1})$.

Finally, for the GCD problem in question 2, identify which irreducibles in $\mathbb{Z}_q[t]$ are "unlucky" and also which other irreducibles cannot be used for Hensel lifting.