Math 801 course project list: Spring 2019

Instructor: Michael Monagan
Due 4pm Tuesday April 16th.

If you get stuck, please do come and ask for help any time.
You can call me at (778) 782 4279 to see if I am in my office.

The modular GCD algorithm and Hensel lifting algorithm.

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 then apply Hensel lifting to compute a GCD in $\mathbb{Z}_q[t][x]$.

For both algorithms, after choosing an irreducible $p(t)$ in $\mathbb{Z}_q[t]$, we need to compute a GCD in $F[x]$ where F is the quotient ring $\mathbb{Z}_q[t]/\langle p(t)\rangle$ which is finite field. Maple has a routine for doing this.

The help page for `?mod` has many commands for computing modulo a prime q that will be useful.

Question 1 (10 marks)

We have seen the Chinese remainder theorem for $\mathbb{Z}$. Assignment 3 question 4 asked you to prove the following Chinese remainder theorem for $\mathbb{Z}_q[t]$.

> Theorem: Let F be any field (e.g. $\mathbb{Z}_q$) and let $m_1, m_2, \ldots, m_n$ and $u_1, u_2, \ldots, u_n$ be polynomials in $F[y]$ with $deg(m_i) > 0$ for $1 \le i \le n$. If $\gcd(m_i, m_j) = 1$ for $1 \le i < j \le n$ then there exists a unique polynomial u in $F[y]$ s.t.
> (i) $u \equiv u_i \pmod{m_i}$ for $1 \le i \le n$ and
> (ii) $u = 0$ or $\deg u < \sum_{i=1}^{n} \deg m_i$.

Write a Maple procedure `CRT(u,m,y,q)` that outputs (U, M) such that $M = \prod_{i=1}^{n} m_i$ and $U \equiv u_i \pmod{m_i}$. The easiest way to do this is to do it recursively. Then you only need to solve the Chinese remainder problem for two congruences $\{\, u \equiv u_1 \pmod{m_1},\ u \equiv u_2 \pmod{m_2}\,\}$. Test your procedure on the following problem in $\mathbb{Z}_2[t]$.

```
> u1,m1 := t^2, t^3+t+1;
> u2,m2 := t^2+t+1, t^3+t^2+1;
> u3,m3 := t^3,t^4+t+1;
> CRT([u1,u2,u3],[m1,m2,m3],t,2);
```

To divide $a \div b$ in $\mathbb{Z}_q[t]$ use `Rem(a,b,t) mod q`.
To multiply $a \times b$ in $\mathbb{Z}_q[t]$ use `Expand(a*b) mod q`.
To solve $sa + tb = 1$ for $s, t \in \mathbb{Z}_q[t]$ use `Gcdex(a,b,t,'s','t') mod q`.

Question 2 (25 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

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

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

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

To compute a GCD of two polynomials $f_1, f_2 \in \mathbb{Z}_q[t][x]$ modulo an irreducible polynomial $p(t) \in \mathbb{Z}_q[t]$, that is, in the quotient ring $F[x]$ where $F = \mathbb{Z}_q[t]/\langle p(t)\rangle$, 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;
```

For a source of irreducibles in $\mathbb{Z}_q[t]$ see the `Nextprime` command under ?mod .
To test if $g|a$ in $\mathbb{Z}_q[t, x]$ use `Divide(a,g) mod q`.
To compute the content of $a \in \mathbb{Z}_q[t][x]$ use `Content(a,x) mod q`.

Question 3 (25 marks)

Modify the linear Hensel lifting algorithm to work modulo p where p is an irreducible in $\mathbb{Z}_q[t]$. Program the algorithm in Maple. Test your Maple code on the GCD problem from Question 2 using $p(t) = t^3 + 2t + 2$. This irreducible is not unlucky and it satisfies the other requirements for Hensel lifting to work.

You will need to solve $SA + TB = 1$ in $F[x]$ where F is the quotient ring $\mathbb{Z}_q[t]/p(t)$ using the extended Euclidean algorithm in order to solve the polynomial diophantine equation that arise in Hensel lifting. Use the following Maple commands to do this:

```
> 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 := subs(a=t,G);
     S := subs(a=t,S);
     T := subs(a=t,T);
  fi;
```

You can use the same approach to divide $A \div B$ in $F[x]$.

```
> a := RootOf(p) mod q;
> R := Rem(subs(t=a,A),subs(t=a,B),x,'Q') mod q;
> if not type(a,integer) then
     R := subs(a=t,R);
     Q := subs(a=t,Q);
  fi;
```

You will also need to multiply a polynomial $f \in \mathbb{Z}_q[t, x]$ by polynomials in $\alpha \in \mathbb{Z}_q[t]$ mod p^k. Use `Rem(alpha*h,p^k,t) mod q` to do this. This multiplies $\alpha \times h$ mod q first.

I suggest you start by first writing a Maple procedure to solve the polynomial Diophantine equation $\sigma A + \tau B = C$ in $F[x]$ needed for Hensel lifting. Test your procedure on input polynomials A, B, C of your choice.