MACM 401/MATH 701/MATH 801
Assignment 4, Spring 2023.

Michael Monagan

Due Monday March 13th at 11pm. You may use Maple for all calculations unless asked to do the question by hand. For problems involving Maple calculations and Maple programming, please upload a printout of a Maple worksheet.
Late Penalty: -20% for up to 24 hours late. Zero after that.

Question 1: P-adic Lifting (20 marks)

Reference: Section 6.2 and 6.3.

(a) By hand, determine the p-adic representation of the integer $u = 116$ for $p = 5$, first using the positive representation, then using the symmetric representation for $\mathbb{Z}_5$.

(b) Theorem 2: Let $u, p \in \mathbb{Z}$ with $p > 2$. For simplicity assume p is odd.
If $-\frac{p^n}{2} < u < \frac{p^n}{2}$ there exist unique integers $u_0, u_1, \ldots, u_{n-1}$ such that $u = u_0 + u_1 p + \cdots + u_{n-1}p^{n-1}$ and $-\frac{p}{2} < u_i < \frac{p}{2}$.

Prove uniqueness.

(c) Determine the cube-root, *if it exists*, of the following polynomials

$$\begin{aligned} a(x) &= x^6 - 531x^5 + 94137x^4 - 5598333x^3 + 4706850x^2 - 1327500x + 125000, \\ b(x) &= x^6 - 406\,x^5 + 94262\,x^4 - 5598208\,x^3 + 4706975\,x^2 - 1327375\,x + 125125 \end{aligned}$$

using reduction mod 5 and linear p-adic lifting. You will need to derivive the update formula by modifying the update formula for computing the $\sqrt{a(x)}$.

Factor the polynomials so you know what the answers are. Express your the answer in the p-adic representation. To calculate the initial solution $u_0 = \sqrt[3]{a} \bmod 5$ use any method. Use Maple to do all the calculations.

Question 2: Hensel lifting (15 marks)

Reference: Section 6.4 and 6.5.

(a) Given

$$a(x) = x^4 - 2\,x^3 - 233\,x^2 - 214\,x + 85$$

and image polynomials

$$u_0(x) = x^2 - 3\,x - 2 \quad \text{and} \quad w_0(x) = x^2 + x + 3,$$

satisfying $a \equiv u_0\,w_0 \pmod 7$, lift the image polynomials using Hensel lifting to find (if there exist) u and w in $\mathbb{Z}[x]$ such that $a = uw$.

(b) Given

$$b(x) \;=\; 48\,x^4 - 22\,x^3 + 47\,x^2 + 144$$

and an image polynomials

$$u_0(x) = x^2 + 4\,x + 2 \quad \text{and} \quad w_0 = x^2 + 4\,x + 5$$

satisfying $b \;\equiv\; 6\,u_0\,w_0 \pmod 7$, lift the image polynomials using Hensel lifting to find (if there exist) u and w in $\mathbb{Z}[x]$ such that $b \;=\; uw$.

Question 3: Determinants (25 marks)

Consider the following 3 by 3 matrix A of polynomials in $\mathbb{Z}[x]$ and its determinant d.

```
> P := () -> randpoly(x,degree=2,dense):
> A := Matrix(3,3,P);
```

$$A := \begin{bmatrix} -55 - 7\,x^2 + 22\,x & -56 - 94\,x^2 + 87\,x & 97 - 62\,x \\ -83 - 73\,x^2 - 4\,x & -82 - 10\,x^2 + 62\,x & 71 + 80\,x^2 - 44\,x \\ -10 - 17\,x^2 - 75\,x & 42 - 7\,x^2 - 40\,x & 75 - 50\,x^2 + 23\,x \end{bmatrix}$$

```
> d := LinearAlgebra[Determinant](A);
```

$$d := -224262 - 455486\,x^2 + 55203\,x - 539985\,x^4 + 937816\,x^3 + 463520\,x^6 - 75964\,x^5$$

(a) (15 marks) Let A by an n by n matrix of polynomials in $\mathbb{Z}[x]$ and let $d = \det(A)$. Develop a modular algorithm for computing $d = \det(A) \in \mathbb{Z}[x]$. Your algorithm will compute determinants of A modulo a sequence of primes and apply the CRT. For each prime p it will compute the determinant in $\mathbb{Z}_p[x]$ by evaluation and interpolation. In this way we reduce computation of a determinant of a matrix over $\mathbb{Z}[x]$ to many computations of determinants of matrices over $\mathbb{Z}_p$, a field, for which ordinary Gaussian elimination, which does $O(n^3)$ arithmetic operations in $\mathbb{Z}_p$, may be used.

You will need bounds for $\deg d$ and $||d||_\infty$. Use primes $p = [101, 103, 107, ...]$ and use Maple to do Chinese remaindering. Use $x = 1, 2, 3, ...$ for the evaluation points and use Maple for the interpolations.

Present your algorithm as a homomorphism diagram.
Implement your algorithm in Maple and test it on the above example.

To reduce the coefficients of the polynomials in A modulo p in Maple use

```
> B := A mod p;
```

To evaluate the polynomials in B at $x = \alpha$ modulo p in Maple use

```
> C := Eval(B,x=alpha) mod p;
```

To compute the determinant of a matrix C over $\mathbb{Z}_p$ in Maple use

```
> Det(C) mod p;
```

(b) (10 marks) Suppose A is an n by n matrix over $\mathbb{Z}[x]$ and $A_{i,j} = \sum_{k=0}^{d} a_{i,j,k}x^k$ and $|a_{i,j,k}| < B^m$. That is A is an n by n matrix of polynomials of degree at most d with coefficients at most m base B digits long. Assume the primes satisfy $B < p < 2B$ and that arithmetic in $\mathbb{Z}_p$ costs $O(1)$. Estimate the time complexity of your algorithm in big O notation as a function of n, m and d. Make reasonable simplifying assumptions such as $n < B$ and $d < B$ as necessary. State your assumptions. Also helpful is

$$\ln n! < n \ln n \quad \text{for} \quad n > 1.$$

Question 4: Lagrange Interpolation (20 marks)

In class we stated the following theorem for polynomial interpolation.

> Theorem: Let F be a field. Let $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ be n points in F^2. If the x_i are distinct there exists a unique polynomial $f(z)$ in $F[z]$ satisfying $\deg(f) \le n-1$ and $f(x_i) = y_i$ for $1 \le i \le n$.

Lagrange interpolation is an $O(n^2)$ algorithm for computing $f(z)$. It does

1. Expand the product $M(z) = \prod_{i=1}^{n}(z - x_i)$.
2. Set $L_i(z) = M(z)/(z - x_i)$ for $1 \le i \le n$.
3. Set $\alpha_i = L_i(x_i)$ for $1 \le i \le n$.
4. Set $\beta_i = y_i \cdot \alpha_i^{-1}$ for $1 \le i \le n$.
5. Set $f = \sum_{i=1}^{n} \beta_i L_i(z)$.

(a) For $F = \mathbb{Z}_7$, $x = [1, 2, 3, 4]$ and $y = [0, 5, 5, 0]$, use Maple's `Interp(x,y,z) mod p;` command to find $f(z)$. Now, using Maple as a calculator, execute Steps 1 to 5 to find the interpolating polynomial $f(z)$. I suggest you use Arrays for L, α and β.

(b) Write a Maple procedure `INTERP(x,y,z,p)` that uses Lagrange interpolation to interpolate $f(z)$ for the field $F = \mathbb{Z}_p$, that is, for the integers modulo p. Please print out the L_i polynomials. Test your Maple procedure on the example in part (a).

(c) Show that Steps 1,2,3, and 5 do $O(n^2)$ multiplications in F. Since Step 4 does n multiplications and n inverses in F, conclude that Lagrange interpolation does $O(n^2)$ multiplications in F. Please note the following. An obvious way to code Step 1 in Maple for $F = \mathbb{Z}_7$

```
> M := z-x[1] mod p;
> for i from 2 to n do M := Expand((z-x[i])*M) mod p; od;
```

In the loop, at step i, this multiplies $(z-x_i)$ by M where $M = \prod_{k=1}^{i-1}(z-x_k) = z^{i-1} + \sum_{k=0}^{i-2} b_k z^k$ for some coefficients $b_k \in F$. This multiplication is special because the factors $(z - x_k)$ and M are both monic. To minimize the number of multiplications in F we can use

$$(z - x_k)(z^{i-1} + \sum_{k=0}^{i-2} b_k z^k) = z^i + \sum_{k=0}^{i-2} b_k z^{k+1} - x_k z^{i-1} - \sum_{k=0}^{i-2}(x_k \cdot b_k) z^k$$

which needs only $i - 1$ multiplications $x_k \cdot b_k$ in F.