MACM 401/MATH 701/MATH 801
Assignment 5, Spring 2023.

Michael Monagan

Due Monday March 2
Late Penalty: −20% ... e. Zero after that.

Question 1: Fact... (20 marks)

(a) Factor the following polynomials over $\mathbb{Z}_{11}$ using the Cantor-Zassenhaus algorithm.

$$\begin{aligned} a_1 &= x^4 + 8\,x^2 + 6\,x + 8, \\ a_2 &= x^6 + 3\,x^5 - x^4 + 2\,x^3 - 3\,x + 3, \\ a_3 &= x^8 + x^7 + x^6 + 2\,x^4 + 5\,x^3 + 2\,x^2 + 8. \end{aligned}$$

Use Maple to do all polynomial arithmetic, that is, you can use the `Gcd(...) mod p` and `Powmod(...) mod p` commands etc., but not `Factor(...) mod p`.

(b) Compute the square-roots of the integers $a = 3, 5, 7$ in the integers modulo p, if they exist, for $p = 10^{20} + 129 = 100000000000000000129$ by factoring the polynomial $x^2 - a$ in $\mathbb{Z}_p[x]$ using the Cantor-Zassenhaus algorithm. Show your working. You will have to use `Powmod` here.

Question 2: Factorization in $\mathbb{Z}[x]$ (25 marks)

Factor the following polynomials in $\mathbb{Z}[x]$.

$$a_1 = x^{10} - 6\,x^4 + 3\,x^2 + 13$$

$$a_2 = 8\,x^7 + 12\,x^6 + 22\,x^5 + 25\,x^4 + 84\,x^3 + 110\,x^2 + 54\,x + 9$$

$$a_3 = 9\,x^7 + 6\,x^6 - 12\,x^5 + 14\,x^4 + 15\,x^3 + 2\,x^2 - 3\,x + 14$$

$$a_4 = x^{11} + 2\,x^{10} + 3\,x^9 - 10\,x^8 - x^7 - 2\,x^6 + 16\,x^4 + 26\,x^3 + 4\,x^2 + 51\,x - 170$$

For each polynomial, first compute its square free factorization. You may use the Maple command `gcd(...)` to do this. Now factor each non-linear square-free factor as follows. Use the Maple command `Factor(...) mod p` to factor the square-free factors over $\mathbb{Z}_p$ modulo the primes $p = 13, 17, 19, 23$. From this information, determine whether each polynomial is irreducible over $\mathbb{Z}$ or not. If not irreducible, try to discover what the irreducible factors are by considering combinations of the modular factors and Chinese remaindering (if necessary) and trial division over $\mathbb{Z}$.

Using Chinese remaindering here is not efficient in general. Why?

Thus for the polynomial a_4, use Hensel lifting instead; using a prime of your choice from 13, 17, 19, 23, Hensel lift each factor mod p, then determine the irreducible factorization of a_4 over $\mathbb{Z}$.

Question 3: A linear x-adic Newton iteration (15 marks)

Let p be an odd prime and let $a(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}_p[x]$ with $a_0 \neq 0$ and $a_n \neq 0$. Suppose $\sqrt{a_0} = \pm u_0 \bmod p$. The goal of this question is to design an x-adic Newton iteration algorithm that given u_0, determ $\mathbb{Z}_p[x]$ and if so computes u. Let

$$+ u_{k-1} x^{k-1} + ... + u_{n-1} x^{n-1}.$$

(a) Derive the New r u_k given $u^{(k)}$. Show your working.

(b) Now implement aple and test it on the two polynomials $a_1(x)$ and $a_2(x)$ below using p = Please print out the sequence of values of $u_0, u_1, u_2, ...$ that your progr one of the polynomials has a $\sqrt{}$ in $\mathbb{Z}_p[x]$, the other does not.

$$a_1 = 81\,x^6 + 16\,x^5 + 24\,x^4 + 89\,x^3 + 72\,x^2 + 41\,x + 25$$

$$a_2 = 81\,x^6 + 46\,x^5 + 34\,x^4 + 19\,x^3 + 72\,x^2 + 41\,x + 25$$

Question 5 (15 marks): Symbolic Integration

Implement a Maple procedure `INT` (you may use `Int` if you prefer) that evaluates antiderivatives $\int f(x)\mathrm{d}x$. For constants a, b, c and positive integer n your Maple procedure should apply

$$\int c\,dx = cx.$$

$$\int cf(x)\,dx \to c\int f(x)\,dx.$$

$$\int f(x) + g(x)\,dx \to \int f(x)\,dx + \int g(x)\,dx.$$

$$\int x^{-1}\,dx = \ln x \quad \text{and for } c \neq 1 \quad \int x^c\,dx = \frac{1}{c+1}x^{c+1}.$$

$$\int e^x\,dx = e^x \quad \text{and} \quad \int \ln x\,dx = x\ln x - x.$$

$$\int x^n e^x\,dx \to x^n e^x - \int n x^{n-1} e^x\,dx.$$

$$\int x^n \ln x\,dx = \frac{x^{n+1}}{n+1}\ln x - \frac{x^{n+1}}{(n+1)^2}.$$

$$\int e^{ax+b}\,dx = \frac{1}{a}e^{ax+b} \quad \text{and} \quad \int \frac{1}{ax+b}\,dx = \ln|ax+b|/a.$$

You may ignore the constant of integration. NOTE: e^x in Maple is `exp(x)`, i.e. it's a function not a power. HINT: use the `diff` command for differentiation to determine if a Maple expression is a constant wrt x. Test your program on the following.

```
> INT( x^2 + 2*x + 1, x );
> INT( x^(-1) + 2*x^(-2) + 3*x^(-1/2), x );
> INT( exp(x) + ln(x) + sin(x), x );
> INT( 2*f(x) + 3*y*x/2 + 3*ln(2), x );
> INT( x^2*exp(x) + 2*x*exp(x), x );
> INT( 4*x^3*ln(x), x );
> INT( 2*exp(-2*x) + 2/(3*x+1), x );
```