MACM 401/MATH 801/CMPT 891
Assignment 5, Spring 2021.

Michael Monagan

Due Monday March 29th at 11pm.
Late Penalty: -20% for up to 48 hours late. Zero after that.

Question 1: Factorization in $\mathbb{Z}_p[x]$ (20 marks)

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

$$a_1 = x^4 + 8\,x^2 + 6\,x + 8,$$

$$a_2 = x^6 + 3\,x^5 - x^4 + 2\,x^3 - 3\,x + 3,$$

$$a_3 = x^8 + x^7 + x^6 + 2\,x^4 + 5\,x^3 + 2\,x^2 + 8.$$

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: The linear x-adic Newton iteration (15 marks)

Let p be a prime and $a \in \mathbb{Z}_p[x]$ have degree $d \geq 0$. Let $u = \sqrt{a}$ and suppose $u \in \mathbb{Z}_p[x]$. Then for $\alpha \in \mathbb{Z}$ we may write

$$u = u_0 + u_1(x-\alpha) + \cdots + u_k(x-\alpha)^k + \cdots + u_{d/2}(x-\alpha)^{d/2}$$

where $u_0 = \sqrt{a(\alpha)}$. On assignment 4 you derived the following update formula for determining u_k given $u^{(k)} = \sum_{i=0}^{k-1} u_i(x-\alpha)^i$:

$$u_k = \frac{e_k}{(x-\alpha)^k}(2u_0)^{-1} \mod (x-\alpha) \text{ where } e_k = a - {u^{(k)}}^2.$$

If $a = \sum_0^d a_i x^i$ and $a_0 \neq 0$ then we can use $\alpha = 0$ since $a(0) = a_0$ so $u_0 = \sqrt{a_0} \neq 0$. Then the update formula simplifies: the quantity $e_k/x^k \mod x$ is just the coefficient of x^k of e_k. Here is my Maple code for implementing the algorithm for $a_0 \neq 0$.

```
XadicSqrt := proc(a,x::name,p::prime)
# Input a(x) in Zp[x]
# Output sqrt(a) if it is in Zp[x] else FAIL
local a0,u0,u,i,k,d,m,e,uk;
   if a=0 then return 0; fi;
   d := degree(a,x);
   if irem(d,2) <> 0 then return FAIL fi;
   a0 := coeff(a,x,0);
   if a0 = 0 then error "not implemented"; fi;
   u0 := numtheory[msqrt](a0,p);
   if u0 = FAIL then return FAIL; fi;
   i := modp(1/2/u0,p);
   u := u0;
   e := Expand( a-u^2 ) mod p;
   for k from 1 to d/2 do
       uk := coeff(e,x,k)*i mod p;
       u := u + uk*x^k;
       e := Expand( a-u^2 ) mod p;
   od;
   if e = 0 then u else FAIL fi;
end:
```


The algorithm is correct but not efficient. Let us find out why and then fix it. Let $\deg a = d$ and let $T(d)$ be the number of arithmetic operations algorithm XadicLift does in $\mathbb{Z}_p$. Assuming the polynomial multiplication u^2 uses a classical quadratic algorithm, show that $T(d)$ is cubic in d. You are to modify the computation of the error so that that $T(d) \in O(d^2)$. You must show that $T(d) \in O(d^2)$. Implement your modified algorithm in Maple – just modify my code appropriately. Finally make your Maple code work for inputs where $a_0 = 0$. Test your code on the following inputs for $p = 11$.

$$a = (9x^3 + 3x^2 + 5x + 6)^2, \quad a = x^3 + (9x^3 + 3x^2 + 5x + 6)^2, \quad a = (9x^3 + 3x^2 + 5x)^2.$$

Hint: The error $e_{k+1} = a - (u^{(k+1)})^2 = a - \left(u^{(k)} + u_k x^k\right)^2$. Use the error $e_k = a - {u^{(k)}}^2$ from the previous iteration to calculate e_{k+1} faster.

Question 4 (10 marks): Integration and Differentiation in Maple

(a) You were probably taught that the derivative of $\tan x$ is $\sec^2 x$. Differentiate $\tan x$ in Maple. Now use Maple to show that Maple's answer equals $\sec^2 x$.

(b) Evaluate the following antiderivatives in Maple.

$$\int (2x + \tan x) dx \quad \int \frac{\ln(x)}{x} dx \quad \int x^2 e^{-x} dx.$$

(c) Evaluate the following definite integrals in Maple where the parameters r and λ are positive.

$$\int_0^\pi \sin x \, dx \quad \int_{-r}^{r} \sqrt{r^2 - x^2} dx \quad \text{and} \quad \int_0^\infty \lambda e^{-\lambda x} dx.$$

You will need to tell Maple that $r > 0$ and $\lambda > 0$. See ?assume

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 a constant c and positive integer n your Maple procedure should apply

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

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

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

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

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

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

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

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(-x) + ln(2*x+1), x );
```