MACM 401, MATH 701, MATH 819, Assignment 3, Spring 2007.

Michael Monagan

This assignment is to be handed in by Tuesday February 27th. For problems involving Maple calculations and Maple programming, you should submit a printout of a Maple worksheet of your Maple session. Late Penalty: -10% for each day late.

Question 1 (20 marks): Symbolic Integration

Implement a Maple procedure `INT` that evaluates and simplifies indefinite integrals $\int f(x)\mathrm{d}x$. For constant c your Maple procedure should do the following

$$\int c\,\mathrm{d}x \to cx,$$

$$\int cf(x)\,\mathrm{d}x \to c\int f(x)\,\mathrm{d}x,$$

$$\int f(x)+g(x)\,\mathrm{d}x = \int f(x)\,\mathrm{d}x + \int g(x)\,\mathrm{d}x,$$

$$\text{for } n \neq -1,\ \int x^n\,\mathrm{d}x = 1/(n+1)x^{n+1},$$

$$\int x^{-1}\,\mathrm{d}x = \ln x,$$

$$\int e^x\,\mathrm{d}x = e^x,$$

$$\text{for } n > 0,\ \int x^n e^x\,\mathrm{d}x = x^n e^x - \int nx^{n-1}e^x\,\mathrm{d}x,$$

$$\int \ln x\,\mathrm{d}x = \ ?$$

$$\text{for } n > 0,\ \int x^n \ln x\,\mathrm{d}x = \ ?$$

You may ignore the constant of integration. You may use the `diff` command for differentiation if this would be useful. Test your program on the following.

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

Question 2: Polynomial Evaluation and Interpolation (10 marks)

(a) Let R be a ring and $\alpha \in R$. Let $\phi_{x=\alpha} : R[x] \to R$ denote the evaluation function: $\phi_{x=\alpha}(f(x)) = f(\alpha)$. Show that $\phi_{x=\alpha}$ is a ring morphism.

(b) By hand, using Newton's method, find $f(x) \in \mathbb{Q}[x]$ such that $f(0) = 1, f(1) = -2, f(2) = 4$ such that $\deg_x f < 3$. Now repeat the calculations this time in the ring $\mathbb{Z}_5[x]$.

Question 2: Chinese Remaindering (10 marks)

(a) By hand, find $0 \leq u < 5 \times 7 \times 9$ such that

$$u \equiv 3 \bmod 5, \quad u \equiv 1 \bmod 7, \quad \text{and} \quad u \equiv 3 \bmod 9,$$

using firstly the "mixed radix representation" for $\mathbb{Z}$ and also using the "Lagrange representation". The answer you should obtain is 183.

(b) Consider the following recursive algorithm for finding the integer u in the Chinese remainder theorem. For n moduli $m_1, m_2, ..., m_n$, to find $0 \leq u < \Pi_{i=1}^{n} m_i$, first find $0 \leq \bar{u} < \Pi_{i=1}^{n-1} m_i$, satisfying $\bar{u} \equiv u_i \bmod m_i$ for $i = 1, 2, \ldots, n-1$, *recursively*. Using this result and $u \equiv u_n \bmod m_n$ now find u. Work out the details of the method and apply it by hand to the problem in part (a). Now write a recursive Maple procedure which implements the method and test your procedure on the problem in part (a). Note, you can compute the inverse of a in $\mathbb{Z}_m$ in Maple using `1/a mod m`.

Question 4: Homomorphic Imaging (10 marks)

Given $a, b \in \mathbb{Z}[y][x]$ where

$$\begin{aligned} a &= (9y-7)x + 12, \\ b &= (13y+23)x^2 + (21y-11)x + (11y-13), \end{aligned}$$

compute the product $a \times b$ using modular homomorphisms ϕ_{p_i} then evaluation homomorphisms $\phi_{y=\beta_j}$ and $\phi_{x=\alpha_k}$ so that you end up multiplying in $\mathbb{Z}_p$. The Maple command `Eval(a,x=2) mod p` can be used to evaluate the polynomial $a(x)$ at $x = 2$ modulo p. Then use polynomial interpolation and Chinese remaindering to reconstruct the product in $\mathbb{Z}[y][x]$.

First determine how many primes you need and compute them in a list. Use $p = 23, 29, 31, 37, ...$ Then determine how many evaluation points for x and y you need. Use $x = 0, 1, 2, ...$ and $y = 0, 1, 2, ...$ Now do the computations using three loops, one for the primes one for the evaluation points in y and one for the evaluation points in x. The Maple command for interpolation modulo p is `Interp(...) mod p` and the Maple command for Chinese remaindering is `chrem(...)`.

Question 5: The Modular GCD Algorithm (10 marks)

Consider the following pairs of polynomials in $\mathbb{Z}[x]$.

$$\begin{aligned} a_1 &= 58\,x^4 - 415\,x^3 - 111\,x + 213 \\ b_1 &= 69\,x^3 - 112\,x^2 + 413\,x + 113 \\ a_2 &= x^5 - 111\,x^4 + 112\,x^3 + 8\,x^2 - 888\,x + 896 \\ b_2 &= x^5 - 114\,x^4 + 448\,x^3 - 672\,x^2 + 669\,x - 336 \\ a_3 &= 396\,x^5 - 36\,x^4 + 3498\,x^3 - 2532\,x^2 + 2844\,x - 1870 \\ b_3 &= 156\,x^5 + 69\,x^4 + 1371\,x^3 - 332\,x^2 + 593\,x - 697 \end{aligned}$$

Compute the GCD(a_i, b_i) via multiple modular mappings and Chinese remaindering. Use primes $p = 23, 29, 31, 37, 43, ...$ Explain which primes are bad primes, and which are unlucky primes. Use the Maple routine `Gcd(...) mod p` to compute a GCD modulo p and the Maple routine `chrem` to put the modular images together, the `mods` routine to put the coefficients in the symmetric range,

and `divide` for testing if the calculated GCD g_i divides a_i and b_i, and any other routines that you need.

PLEASE make sure you input the polynomials correctly!

Question 6: The Fast Fourier Transform (10 marks)

Let $a(x) = -x^3 + 3x + 1$ and $b(x) = 2x^4 - 3x^3 - 2x^2 + x + 1$ be polynomials in $\mathbb{Z}_{17}[x]$. Calculate the product of $c(x) = a(x)b(x)$ using the FFT. To do this you will need an 8th root of unity since $deg(c) = 7$. Determine the Fourier transform of $a(x)$ by hand using the FFT. For the forward transform of $b(x)$ and the inverse transform of $c(x)$ you may use ordinary evaluation and interpolation (mod 17).

Question 7: (10 marks) (MACM 401 students only)

For the Sparse Multivariate Polynomial data structure that you designed and implemented in the last assignment, if you didn't get it working, get it working now! Now implement a Maple procedure `SMPdiv(A,B,'Q')` that has the same functionality as Maple's `divide` command. Test your routine on the examples in Question 6 below.

Question 7: (30 marks) (MATH 819 students only)

If you used a recursive form for the SMP polynomial data structure on your last assignment, use a distributed form this time. And if you used a distributed form on your last assignment use a recursive form this time. Implement the same 5 Maple procedures

- `Maple2SMP` - to convert from Maple's expanded form to SMP,
- `SMP2Maple` - to convert from SMP to Maple's expanded form,
- `SMPadd` - to add two polynomials,
- `SMPmul` - to multiply two SMP polynomials,
- `SMPdiv` - to divide two SMP polynomials.

Use Maple to do coefficient and exponent arithmetic. Test your routine on the following

```
> a := randpoly([x,y,z],degree=6,terms=15);
> b := randpoly([x,y,z],degree=6,terms=15);
> A := Maple2SMP(a);
> B := Maple2SMP(b);
> C := SMPadd(A,B);
> a+b - SMP2Maple(C));
> C := SMPmul(A,B);
> expand(a*b - SMP2Maple(C));
> SMPdiv(A,B); # should output false
> SMPdiv(C,B); # should output true
> if SMPdiv(C,A,'Q') then expand(b-SMP2Maple(Q)) else buginyourcode fi;
```