MACM 401/MATH 701/MATH 819, Assignment 3, Spring 2008.

Michael Monagan

This assignment is to be handed in by Thursday February 19th at the beginning of class.
Late Penalty: -20% for up to 30 hours late. Zero after that.
For problems involving Maple calculations and Maple programming, you should submit a printout of a Maple worksheet of your Maple session.

Question 1: 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 (15 marks)

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

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

using the "mixed radix representation" for $\mathbb{Z}$ AND also the "Lagrange representation". You should get $u = 183$.

(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 $0 \le u < \Pi_{i=1}^{n} m_i$, first find $0 \le \bar{u} < \Pi_{i=1}^{n-1} m_i$, 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. Apply the method by hand to the problem in part (a). Now write a Maple procedure which implements the method. 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 3: Homomorphic Imaging (15 marks)

(a) Let $\phi_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ denote the modular homomorphism. Let $\phi_{x=a}$ denote the evaluation homomorphism. Show that ϕ_n and $\phi_{x=a}$ commute, that is, $\phi_n \circ \phi_{x=a} = \phi_{x=a} \circ \phi_n$.

(b) Let $a = (9y-7)x + 12$ and $b = (13y+23)x^2 + (21y-11)x + (11y-13)$ be polynomials in $\mathbb{Z}[y][x]$. 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 $a(x,y)$ 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 4: 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 `Gcd(...) mod p` to compute a GCD modulo p in Maple and the Maple commands `chrem` to put the modular images together, `mods` 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 others that you need.

PLEASE make sure you input the polynomials correctly!

Question 5: The Fast Fourier Transform (10 marks)

(a) Let $n = 2m$ and let ω be a primitive n'th root of unity. To apply the FFT recursively, we used the fact that ω^2 is a primitive m'th root of unity. Prove this. See Lemma 4.3.

(b) 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 as follows. First, you will need a primitive 8th root of unity since $deg(c) = 7$. Find one. Now 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 6: The SDMP Data Structure

On assignment 2 you were asked to design and implement SMP, a Sparse Multivariate Polynomial data structure for $\mathbb{Z}[x_1, x_2, ..., x_n]$ and program addition, multiplication and (for graduate students) division. If you didn't get it working, do so now, and I will give you credit.