MACM 401/MATH 701/MATH 819/CMPT 881, Assignment 3, Spring 2011.

Michael Monagan

This assignment is to be handed in by Monday February 28th at the beginning of class.
Late Penalty: −20% for up to 24 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: Homomorphic Imaging (10 marks)

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 3: The Fast Fourier Transform (15 marks)

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

(b) Let $M(n)$ be the number of multiplications that the FFT does. A naive implementation of the algorithm would lead to this recurrence:

$$M(n) = 2M(n/2) + n + 1 \text{ for } n > 1$$

with initial value $M(1) = 0$. In class we said that if we pre-compute the powers ω^i for $0 \le i \le n/2$ and store them in an array W, we can save half the multiplications in the transform so that

$$M(n) = 2M(n/2) + \frac{n}{2} \text{ for } n > 1.$$

Solve this recurrence and show that $M(n) = \frac{n}{2} \log_2 n + o(n)$.

(c) 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 Maple's `Eval(a,x=w) mod p` command to calculate $a(w) \mod p$. If you prefer, you may program the FFT in Maple and use your program instead.

Question 4: The Modular GCD Algorithm (10 marks)

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

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

Compute the GCD(a_i, b_i) via multiple modular mappings and Chinese remaindering. Use primes $p = 23, 29, 31, 37, 43, \ldots$. Identify 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: Resultants (15 marks)

(a) Calculate the resultant of $A = 3x^2 + 3$ and $B = (x-2)(x+5)$ by hand.

(b) Let A, B be non-constant polynomials in $\mathbb{Z}[x]$ and $c \in \mathbb{Z}$. Let $\mathrm{res}(A, B)$ denote the resultant of A and B. From the definition, determine $f(c)$ so that

$$\mathrm{res}(cA, B) = \quad f(c)\ \mathrm{res}(A, B).$$

(c) Let A, B be two non-zero polynomials in $\mathbb{Z}[x]$. Let $A = G\bar{A}$ and $B = G\bar{B}$ where $G = \gcd(A, B)$. Recall that a prime p in the modular gcd algorithm is unlucky iff $p|R$ where $R = \mathrm{res}(\bar{A}, \bar{B}) = 0$ is the resultant of $\bar{A}$ and $\bar{B}$, an integer.

Consider the following pair of polynomials from question 4.

$$A = 58\,x^4 - 415\,x^3 - 111\,x + 213, \quad \text{and}$$
$$B = 69\,x^3 - 112\,x^2 + 413\,x + 113.$$

They are relatively prime, i.e., $G = 1$, $\bar{A} = A$ and $\bar{B} = B$. Using Maple, compute the resultant R and identify all unlucky primes. For each unlucky prime p compute the gcd of the polynomials A and B modulo p to verify that the primes are indeed unlucky.