MATH 497, MATH 895, CMPT 894.
Assignment 5, Summer 2007

Instructor: Michael Monagan

Please hand in the assignment by 2:30pm on Thursday August 9th.
Late Penalty -20% off for each day late.

Question 1: Minimal Polynomials

Let α be algebraic over $\mathbb{C}$. Let $m(z) \in \mathbb{Q}[z]$ be a non-zero monic polynomial of minimal degree such that $m(\alpha) = 0$. Prove that $m(z)$ is irreducible over $\mathbb{Q}$ and unique.

Using resultants, find the minimal polynomial $m_\alpha(z) \in \mathbb{Q}[z]$ for

(a) $\alpha = 1 + \sqrt{2}$,

(c) $\alpha = 1 + \sqrt{2} + \sqrt[4]{2}$, and

(b) $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$.

Question 2: Cyclotomic Polynomials

For $n = 1, 2, 3, ..., 12$, factor the polynomial $x^n - 1$ over $\mathbb{Q}$ using the factor command and identify the cyclotomic polynomials $\Phi_n(x)$ for $n = 1, 2, 3, ..., 12$. Determine an algorithm for computing $\Phi_n(x)$ that does not do any polynomial factorization. Using your algorithm, find the first n such that the largest coefficient of $\Phi_n(x)$ is 3 in magnitude.

Note: if α is an n'th root of unity, but NOT a primitive n'th root of unity, that is, $\alpha^m = 1$ for some $m < n$ and $m|n$, then $\gcd(\Phi_n(x), x^m - 1) = 1$ so $\Phi_n(x)$ divides $(x^n - 1)/(x^m - 1)$.

Question 3: Solving Linear Systems over Number Fields

I've put three linear systems on the web under

`http://www.cecm.sfu.ca/~mmonagan/teaching/TopicsInCA07/`

They are the files `sys49.txt`, `sys100.txt` and `sys196.txt`.
The systems have dimension n = 49, 100, and 196 respectively.

They are over the cyloctomic fields of order $k = 5$, 3, and 24 respectively. Each file contains Maple code that creates a matrix A, a vector b, and defines the minimal polynomial $M = \Phi_k(e)$. The entries in the matrix A and vector b are in $\mathbb{Q}[e]$. Note, they have fractions and are not reduced modulo $M(e)$.

You can read the files into Maple using the `read` command.
You can solve the linear systems in Maple by doing

```
> with(LinearAlgebra):
> e := RootOf(M,e);
> x := LinearSolve(A,b);
> x[1]; # look at the first component of the solution
```

Maple does not use a clever algorithm. It took almost one minute to solve the 49 by 49 system on my computer. Implement two algorithms for solving $Ax = b$ for $x \in \mathbb{Q}[e]$ and use your algorithms to solve the given three linear systems.

The first algorithm should be ordinary Gaussian elimination with back substitution. I've coded Gaussian elimination over $\mathbb{Q}$ in the notes. You will need to multiply, subtract and compute inverses in the field $\mathbb{Q}[e]/M(e)$. The second algorithm is to be a modular algorithm.

A Modular Algorithm (Graduate Students Only)

You will solve $Ax = b$ modulo a sequence of primes $p_1, p_2, ...$, and apply Chinese remaindering to obtain the solution modulo $m = p_1 \times p_2 \times ...$ then recover the rationals in x using rational number reconstruction modulo m. For this use the Maple library routines `chrem` and `iratrecon`. See the notes.

For each prime p, solve the linear system $Ax = b \bmod p$ as follows. The idea is to solve $Ax = b$ modulo p at the roots of $M(e)$ modulo p. Pick the primes p such that $M(e)$ splits into distinct linear factors modulo p. For this, the following lemma will be helpful.

Lemma. If $M(e) = \Phi_k(e)$, the cyclotomic polynomial of order k, then $M(e)$ splits into $d = \phi(k)$ distinct linear factors modulo p if and only if $p \equiv 1 \bmod k$.
Example. For $p = 11$, $k = 5$,

$$M(e) = e^4 + e^3 + e^2 + e + 1 = (e + 7)(e + 6)(e + 8)(e + 2) \bmod 11.$$

Use the Maple library routine `Roots` to compute the roots of $M(e)$ modulo p. See the notes. For each root β of $M(e) \bmod p$ solve $A(\beta)x = b(\beta)$ modulo p using the `Linsolve(...) mod p` command. See notes. Now interpolate $x(e) \in \mathbb{Z}_p[e]$ from $x(\beta_j), \beta_j$ using the `Interp(...) mod p` command.

A detailed description of this algorithm may be found in the paper `Solving Linear Systems over Cyclotomic Fields` by Chen and Monagan on the course website.