MATH 340 Bonus Assignment, Fall 2007

Michael Monagan

Each question is worth a 1% bonus towards your final mark.
This assignment is due Monday December 10th at 1:00pm.
Late penalty: −20% for up to 24 hours late. Zero for more than 24 hours late.
For problems involving Maple please submit a printout of a Maple worksheet.

Question 1: The Extended Euclidean Algorithm

Let F be a field and $a(x)$ and $b(x)$ be non-zero polynomials in $F[x]$.
The Euclidean Algorithm computes the sequence of polynomials

$$r_0 = a, r_1 = b, r_i = r_{i-2} - r_{i-1}q_i \text{ for } i = 2, 3, ..., n+1$$

where q_i is the quotient of r_{i-2} divided r_{i-1} and $r_{n+1} = 0$.
The Extended Euclidean Algorithm also computes the polynomials

$$\lambda_0 = 1, \lambda_1 = 0, \lambda_i = \lambda_{i-2} - \lambda_{i-1}q_i \text{ for } i = 2, 3, ..., n+1 \text{ and}$$

$$\mu_0 = 0, \mu_1 = 1, \mu_i = \mu_{i-2} - \mu_{i-1}q_i \text{ for } i = 2, 3, ..., n+1.$$

Prove, by induction on i, that $\lambda_i(x)a(x) + \mu_i(x)b(x) = r_i(x)$ for $0 \le i \le n+1$.

Question 2: Cyclotomic Polynomials

Let ω be a primitive n'th root of unity in $\mathbb{C}$. The minimial polynomial for ω is called the n'th cyclotomic polynomial. It is denoted by $\Phi_n(x)$. For example, since $x^3-1 = (x-1)(x^2+x+1)$, we have $\Phi_1(x) = x - 1$ and $\Phi_3(x) = x^2 + x + 1$.

Apply the theorem in the handout to compute $\Phi_n(x)$ for $n = 6, 10, 15, 21, 35$, and 105. Do the divisions in Maple using the `divide` command.

Check that $\Phi_n(x)$ is irreducible – it should be one of the irreducible factors of $x^n - 1$. It may be helpful to factor the polynomial $x^n - 1$ so that you can check your results.

Question 3: Primitive n'th roots of unity in finite fields.

Let α be a primitive element in the finite field GF(q) with q elements.
In Assignment 7 you proved that α^j is a primitive element $\Leftrightarrow$ $\gcd(j, q-1) = 1$.

(a) Suppose $n \in \mathbb{N}$ and $n|q-1$. Prove that α^j has order $n \Leftrightarrow \gcd(j, q-1) = (q-1)/n$.

This result gives us a simple way to determine all elements in GF(q) of a given order n once we have a primitive element α. Now, if $\beta \in GF(q)$ has order n, this means $\beta^n = 1$ hence β is a root of $x^n - 1$ and hence β is an n'th *root of unity*. And since $\beta^j \neq 1$ for $0 < j < n$, β is a *primitive* n'th root of unity in the finite field $GF(q)$.

(b) Recall that $x^8 - 1 = (x^4 - 1)(x^4 + 1)$ and hence the four primitive 8'th roots of unity are the roots of $x^4 + 1$. Using the result above, find the four primitive 8'th roots of unity in the following finite fields by first finding a primitive element α in the field and then computing the appropriate powers of α. Use Maple where appropriate.

1. $\mathbb{Z}_{17}$,
2. $GF(25) = \mathbb{Z}_5[y]/(y^2 + 2)$ and
3. $GF(81) = \mathbb{Z}_3[y]/(y^4 + y + 2)$.

Question 4: The Quaternion Group

The quaternion group Q_8 is the subset of 2 by 2 invertible matrices over $\mathbb{C}$ generated by

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

Find the 8 elements of Q_8 by multiplying the above matrices (repeatedly) and calculate the order of all elements of Q_8. Explain why Q_8 is not isomorphic to $\mathbb{Z}_8(+)$ and why Q_8 is not isomorphic to D_4 the set of rotational symmetries of the square.

Note, you can create the two matrices in Maple by doing

```
> A := Matrix([[0,+1],[-1,0]]);
> B := Matrix([[0,+I],[+I,0]]);
```

and multiply matrices using

```
> A.B;
```