THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 | **Exercises for Week 9** | 2004

Recall that the cyclotomic polynomials are defined in terms of the factorizations of $x^N - 1$

$$x^N - 1 = \prod_{m|N} \Phi_m(x).$$

For a particular m and q, you can construct the m-th cyclotomic polynomial in $\mathbb{F}_q[x]$ using the `Magma` commands:

```
P<x> := PolynomialRing(FiniteField(q));
Phi := P!CyclotomicPolynomial(m);
```

1. **a.** What is the factorization of $\Phi_{26}(x)$ in $\mathbb{F}_3[x]$? How many factors are there of each degree? What are the numbers of factors of each degree in the factorizations of $\Phi_m(x)$ for m dividing 26 dividing 80? Carry out a similar analysis for m dividing 63 and $\Phi_m(x)$ in $\mathbb{F}_2[x]$ and for m dividing 124 and $\Phi_m(x)$ in $\mathbb{F}_5[x]$.

b. Show that r divides $\varphi(p^r - 1)$. Give an example of a p, r, and an m, such that m divides but is not equal to $p^r - 1$, and such that r divides the degree of every factor of $\Phi_m(x)$ in $\mathbb{F}_p[x]$.

c. Let r be the order of p in $\mathbb{Z}/m\mathbb{Z}^*$. Show that r is the degree of every irreducible factor of $\Phi_m(x)$

2. Let $\mathbb{F}_q$ be a finite field of q elements.

a. What is the number of elements in $\mathbb{F}_q^*$ of each order dividing $q - 1$? Do this count for $q = 27$, $q = 64$, $q = 81$, and $q = 125$.

b. Consider the finite fields $K = \mathbb{F}_3[x]/(x^3 - x + 1)$ and $L = \mathbb{F}_3[y]/(y^3 - y^2 + 1)$. Define isomorphisms $K \to L$ and $L \to K$. What is the compositum of the two isomorphism you chose?

N.B. A finite field in `Magma` can be created using the default constructor, or as an explicit quotient of a polynomial ring:

```
p := 3;
F := FiniteField(p);
P<x> := PolynomialRing(F);
K<t> := FiniteField(p,3);
L<u> := quo< P | x^3 - x^2 + 1 >;
```

The defining polynomial in the former case, K, is arbitrarily set to be $x^3 - x + 1$, while we choose the defining polynomial to be $x^3 - x^2 + 1$ in the latter. Note that in both cases the resulting rings are fields of size 27, hence isomorphic. Necessarily, these minimal polynomials of t and u must then divide $x^{27} - x$.