The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Exercises and Solutions 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 $\Phi_m(x)$

Solution

a. The factorization of $\Phi_{26}(x)$ in $\mathbb{F}_3[x]$ can be determined in `Magma` with the following commands.

```
> P<x> := PolynomialRing(FiniteField(3));
> Factorization(P!CyclotomicPolynomial(26));
[
    <x^3 + 2*x + 1, 1>,
    <x^3 + x^2 + 2*x + 1, 1>,
    <x^3 + 2*x^2 + 1, 1>,
    <x^3 + 2*x^2 + x + 1, 1>
]
```

By its definition, we have that $\Phi_{26}(x) \,|\, x^{26} - 1$, and since $26 = 27 - 1$ the polynomial $x^{26} - 1$ factors completely over $\mathbb{F}_{27}$, but the only factors over $\mathbb{F}_3$ are $x + 1$ and $x + 2$. Therefore we could have predicted the factorization into degree 3 polynomials. Since the degree of this polynomial is $\varphi(26) = 12 = 3 \cdot 4$, there are 4 factors.

Similarly, the degrees r and number t of factors of other $\Phi_m(x)$ in $\mathbb{F}_p[x]$ are determined by the minimal r such that m divides $p^r - 1$. Complete data for p,

r, and m dividing 63, 26, 80, and 124 is given in the tables below.

m	$\varphi(m)$	p	r	t
63	36	2	6	6
9	6	2	6	1
7	6	2	3	2
3	2	2	2	1
1	1	2	1	1

m	$\varphi(m)$	p	r	t
26	36	3	3	4
13	6	3	3	4
2	6	3	1	2
1	1	3	1	1

m	$\varphi(m)$	p	r	t
80	32	3	4	8
40	16	3	4	4
20	8	3	4	2
16	8	3	4	2
10	4	3	4	1
8	4	3	2	2
5	4	3	4	1
4	2	3	2	1
2	1	3	1	1
1	1	3	1	1

p	m	$\varphi(m)$	r	t
5	124	60	3	20
5	62	30	3	10
5	31	30	3	10
5	4	2	2	1
5	2	1	1	1
5	1	1	1	1

b. The fact that r divides $\varphi(p^r - 1)$ could be inferred from the fact that all factors of $\Phi_{p^r-1}(x)$ in $\mathbb{F}_p[x]$ have degree r. A purely algebraic proof of this fact is derived from the expression $p^r \equiv 1 \bmod p^r - 1$, which says that p has order r in $\mathbb{Z}/(p-1)\mathbb{Z}$. Thus r divides the order, $\varphi(p^r - 1)$, of this group.

c. The powers of x in $\mathbb{F}_p[x]/(x^m - 1)$ form an abelian group isomorphic to $\mathbb{Z}/m\mathbb{Z}$. Since p has order r in $\mathbb{Z}/m\mathbb{Z}$, the r-th power of the Frobenius endomorphism π induces the identity on $\mathbb{F}_p[x]/(x^m - 1)$ because $\pi^r(x) = x^{p^r} = x$. Using the quotient homomorphism

$$\mathbb{F}_p[x]/(x^m - 1) \rightarrow \mathbb{F}_p[x]/(\Phi_m(x)),$$

the r-th power of the Frobenius endomorphism must also be the identity on the quotient $\mathbb{F}_p[x]/(\Phi_m(x))$. Since $\Phi_m(x)$ is squarefree, the latter quotient is isomorphic to a product of fields, each of which must have degree over $\mathbb{F}_p$ dividing r. On the other hand the degree of any quotient $\mathbb{F}_p[x]/(g(x))$ is a proper divisor s of r if and only if $g(x) | x^{p^s - 1} - 1$. But then $g(x)$ must be a divisor of $x^k - 1$, where $k = \mathrm{GCD}(m, p^s - 1)$. By construction, $g(x)$ then divides $\Phi_k(x)$ not $\Phi_m(x)$ as assumed.

Note that in this exercise, the main idea is that the subgroup $\langle x \rangle$ of $\mathbb{F}_p[x]/(x^m - 1)^*$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$, that this group is mapped injectively into $\mathbb{F}_{p^r}^* = \mathbb{F}_p[x]/(g(x))^*$, and that the elements of $\mathbb{Z}/m\mathbb{Z}^*$ are in bijection with the elements of exact order m in $\mathbb{F}_{p^r}^*$, which in turn are precisely the roots of $\Phi_m(x)$ in $\mathbb{F}_{p^r}$.

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 $K \rightarrow L$ and $L \rightarrow K$. What is the compositum of the two isomorphism you chose?

Solution

a. The number of each element in $\mathbb{F}_q^*$ of each order m dividing $q-1$ is $\varphi(m)$, as determined in the tables of the previous exercise.

b. There are four irreducible polynomials

$$x^3 - x + 1 \qquad x^3 + x^2 - x + 1 \qquad x^3 - x^2 + 1 \qquad x^3 - x^2 + x + 1$$

dividing $\Phi_{26}(x)$ in $\mathbb{F}_3[x]$. For each such $g(x)$, there exists a field extension $\mathbb{F}_3[x]/(g(x))$ of 27 elements, each isomorphic. For each k in $\mathbb{Z}/m\mathbb{Z}^*$, the map $x \mapsto x^k$ determines a ring homomorphism of $\mathbb{F}_3[x]/(\Phi_{26}(x))$ to itself. If we write this ring as a product of fields:

$$\frac{\mathbb{F}_3[x]}{(\Phi_{26}(x))} \cong \frac{\mathbb{F}_3[x]}{(x^3-x+1)} \times \frac{\mathbb{F}_3[x]}{(x^3+x^2-x+1)} \times \frac{\mathbb{F}_3[x]}{(x^3-x^2+1)} \times \frac{\mathbb{F}_3[x]}{(x^3-x^2+x+1)}$$

one makes the following observations. The Frobenius homomorphism $\pi(a) = a^3$ induces an automorphism of each factor, so that if $x^3 - x + 1 = 0$ then

$$\pi(x^3 - x + 1) = (x^3)^3 - (x^3) + 1 = 0,$$

but for each other k in $\mathbb{Z}/m\mathbb{Z}^*$, the homomorphism sending $x \mapsto x^k$ must permute the factors by taking a root of $x^3 - x + 1$ to a root of one of the other divisors of $\Phi_{26}(x)$. In particular we can verify that the map $x = y^{-1} = y^{25}$ and conversely $y = x^{-1} = x^{25}$ determine isomorphisms between K and L. Composite with any power of the Frobenius automorphism gives the two other possible isomorphisms.

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 $x^{27} - x$.