Course 374 (Cryptography)

Sample Paper 3

Dr Timothy Murphy

GMB ??　　Friday, ?? 2007　　??:00–??:00

Attempt 4 questions from Part A, and 2 questions from Part B.

Part B

9. Let the number of irreducible polynomials of degree d over $\mathbb{F}_p$ be denoted by $N(d)$. Show that

$$p^n = \sum_{d|n} dN(d).$$

Hence or otherwise show that there is at least one irreducible polynomial of each degree d.

How many irreducible polynomials are there of degree 6 over $\mathbb{F}_2$? How many of these polynomials are primitive?

Find one such primitive polynomial (of degree 6 over $\mathbb{F}_2$).

Answer:

(a) *We assume the following result:*

Lemma 1. *Let*

$$U_n(x) = x^{p^n} - x \in \mathbb{F}_p[x].$$

Then

$$U_n(x) = \prod f(x)$$

where the product extends over all irreducible polynomials $f(x) \in \mathbb{F}_p[x]$ of degree $d \mid n$.

[I think in this case one could state the Lemma without proof. The proof is fairly long, depending on the following ideas:

- *$U_n(x)$ factorises completely in $\mathbb{F}_{p^n}$;*
- *If $f(x) \mid U_n(x)$ then $f(x)$ must have a root $\alpha \in \mathbb{F}_{p^n}$, and then $\mathbb{F}_p[\alpha]$ will be a subfield of $\mathbb{F}_{p^n}$, and so $d \mid n$.*
- *Conversely, if $f(x)$ is irreducible of degree $d|n$ then $\mathbb{F}_p[x]/(f(x))$ is a field of order p^d, which can be identified with the field $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^n}$.*

Remember, stating a Lemma like this clearly and correctly, but without proof, is likely to get full or nearly full marks.]

Comparing degrees on each side of the identity, on the left $U_n(x)$ has degree p^n, while on the right if there are $N(d)$ polynomials of degree $d \mid n$ they will contribute $dN(d)$ to the degree. Hence

$$p^n = \sum_{d|n} dN(d).$$

(b) It follows from the formula that

$$dN(d) \le p^d.$$

Hence

$$\begin{aligned} nN(n) &= p^n - \sum_{d|n,\ d<n} dN(d) \\ &\ge p^n - \sum_{d|n,\ d<n} p^d \\ &\ge p^n - \sum_{d<n} p^d \\ &= p^n - \frac{p^n - 1}{p - 1} \\ &> 0. \end{aligned}$$

Thus

$$N(n) > 0.$$

(c) *We have*

$$2^6 = 6N(6) + 3N(3) + 2N(2) + N(1).$$

But

$$\begin{aligned} 2^3 = 3N(3) + N(1) &\implies 3N(3) = 8 - 2 \\ &\implies N(3) = 2, \end{aligned}$$

while

$$\begin{aligned} 2^2 = 2N(2) + N(1) &\implies 2(2) = 4 - 2 \\ &\implies N(2) = 1. \end{aligned}$$

Hence

$$\begin{aligned} 2^6 = 6N(6) + 3 \cdot 2 + 2 \cdot 1 + 2 &\implies 6N(6) = 64 - 10 \\ &\implies N(6) = 9; \end{aligned}$$

there are 9 irreducible polynomials of degree 6 over $\mathbb{F}_2$.

(d) *The number of primitive elements in* $\mathbb{F}_{2^6}$ *is*

$$\begin{aligned} \phi(2^6 - 1) &= \phi(63) \\ &= \phi(3^2 7) \\ &= \phi(3^2)\phi(7) \\ &= 3 \cdot 2 \cdot 6 \\ &= 36. \end{aligned}$$

Each primitive polynomial of degree 6 has 6 primitive elements as roots. Hence the number of primitive polynomials of degree 6 is

$$\frac{36}{6} = 6.$$

(e) *Let us try the polynomial*

$$f(x) = x^6 + x + 1.$$

First we must see if it is irreducible.
Since $f(0) = f(1) = 1$, $f(x)$ *does not have a factor of degree 1.*
Thus if $f(x)$ *factorizes, it is either the product of 3 factors of degree 2, or 2 factors of degree 3.*

We have seen that there is one irreducible polynomial of degree 2, namely

$$h(x) = x^2 + x + 1.$$

Now

$$x^3 \equiv 1 \implies x^6 \equiv 1 \bmod h(x).$$

Hence

$$x^6 + x + 1 \equiv x \bmod h(x),$$

and so

$$\gcd(f(x), h(x)) = 1.$$

There are 2 irreducible polynomials of degree 3, namely

$$u(x) = x^3 + x + 1,\ v(x) = x^3 + x^2 + 1.$$

Now

$$u(x)^2 = x^6 + x^2 + 1,\ v(x)^2 = x^6 + x^4 + 1,$$

while

$$u(x)v(x) = x^6 + x^5 + x^4 + x^2 + x + 1.$$

We conclude that $f(x)$ is irreducible.

To see if it is primitive we must determine the order of $x \bmod f(x)$; if this is $2^6 - 1 = 63$ then $f(x)$ is primitive.

The order divides 63; so it is sufficient to consider $x^7,\ x^9$ and $x^{21} \bmod f(x)$. We have

$$\begin{aligned}
x^7 &\equiv x^2 + x \not\equiv 1,\\
x^9 &\equiv x^4 + x^3 \not\equiv 1,\\
x^{21} &\equiv (x^2 + x)^3\\
&\equiv x^3(x+1)^3\\
&\equiv x^3(x^3 + x^2 + x + 1)\\
&\equiv x^6 + x^5 + x^4 + x^3\\
&\equiv x^5 + x^4 + x^3 + x + 1\\
&\not\equiv 1.
\end{aligned}$$

We conclude that the order of $x \bmod f(x)$ is 63, and so $f(x)$ is primitive.

10. Explain how points on an elliptic curve are added.

Show that
$$y^2 = x^3 + x + 1$$
defines an elliptic curve over $\mathbb{F}_{11}$, and find the order of the group on the curve.

Find points on the curve of each possible order.

Answer:

(a) *The quadratic residues* $\bmod 11$ *are* $0, 1, 4, -2, 5, 3$. *We draw up a table showing* x, $x^3 + x + 1$ *and the possible values for* y*:*

x	$x^3 + x + 1$	y
0	1	± 1
1	3	± 5
2	0	0
3	-2	± 3
4	3	± 5
5	-1	$-$
-5	3	$pm5$
-4	-1	$-$
-3	4	± 2
-2	2	$-$
-1	-1	$-$

Taking the point at infinity into account, the curve has 14 points. It follows that the group on the curve is $\mathbb{Z}/(14)$*, with elements of order 1,2,7,14.*

We know that if $d \mid n$ *then there are just* $\phi(d)$ *elements of order* d *in* $\mathbb{Z}/(n)$*. Thus there is 1 element of order 1, 1 element of order 2, and 6 elements each of orders* 7 *and* 14*.*

The zero element $[0, 1, 0]$ *has order 1. If* $P = (x, y)$ *then* $-P = (-x, y)$*. Thus* P *has order 2 if and only if* $y = 0$*. We see from the table above that* $A = (2, 0)$ *is such a point.*

If P *has order 7 then* $-P$ *has order 14; and since there are the same number of points of orders 7 and 14, the converse is also true: if* P *has order 14 then* $-P$ *has order 7.*

Take the point $B = (0, 1)$*. Recall that* $P + Q + R = 0$ *if the points* P, Q, R *on the curve are collinear. Thus the tangent at* B *meets the curve again in the point* $-2B$*.*

We have

$$2y\frac{dy}{dx} = 3x^2 + 1,$$

ie

$$\frac{dy}{dx} = \frac{3x^2 + 1}{2y}$$

In particular, at B

$$m = \frac{dy}{dx} = 1/2 = -5.$$

Thus the tangent at B is

$$y - 1 = -5(x - 0),$$

ie

$$y = -5x + 1.$$

This meets the curve where

$$(mx + c)^2 = x^3 + x + 1.$$

If the roots of this are x_0, x_1, x_2 *then*

$$x_0 + x_1 + x_2 = m^2.$$

We know that two of the roots, say x_0, x_1*, are* $0, 0$*. Hence the third root is*

$$x = m^2 - 2x_0 = 25 - 0 = 3.$$

From the equation for the tangent,

$$y = -14 = -3.$$

Thus the tangent at B meets the curve again in the point $C = (3, -3)$*:*

$$2B = -C.$$

Applying the same argument with C in place of B, we now have

$$m = -28/6 = -1.$$

Thus the tangent at C is

$$y + 3 = -(x - 3),$$

ie

$$y = -x.$$

This meets the curve again where

$$x = (-1)^2 - 2 \cdot 3 = -5.$$

From the equation for the tangent,

$$y = 5.$$

Thus the tangent at C meets the curve again in the point $D = (-5, 5)$:

$$4B = -2C = D.$$

Repeating yet again, at D

$$m = 76/10 = 1.$$

Thus the tangent at D is

$$y - 5 = x + 5,$$

ie

$$y = x - 1.$$

This meets the curve again where

$$x = 1^2 + 2 \cdot 5 = 0.$$

From the equation for the tangent,

$$y = -1.$$

Thus the tangent at D meets the curve again in the point $E = (0, -1)$:

$$8B = -4C = 2D = -E = B.$$

In other words, the order of the point $B = (0, 1)$ is 7.
Finally, the point $-B = (0, -1)$ has order 14.

11. Show that the polynomial

$$x^2 + 1$$

is irreducible over $\mathbb{F}_3$. Is it primitive?

Find the group on the elliptic curve

$$y^2 = x^3 + x$$

over $\mathbb{F}_{3^2}$.

Sketch the proof that the addition on an elliptic curve is associative.

Answer:

(a) *If the polynomial*

$$p(x) = x^2 + 1$$

were not irreducible, it would have a root in $\mathbb{F}_3$. *But none of* $0, \pm 1$ *are roots* $\bmod 3$. *Hence* $p(x)$ *is irreducible.*

(b) *To determine if it is primitive, we must find the order* d *of* $x \bmod p(x)$. *We know that*

$$d \mid 3^2 - 1 = 8.$$

The order of x *is not 2, since*

$$x^2 - 1 \not\equiv 0 \bmod p(x),$$

But

$$x^2 \equiv -1 \implies x^4 \equiv 1 \bmod p(x).$$

Hence x *is of order 4, and so is not primitive.*

(c) *The elements of* $\mathbb{F}_{3^2}$ *are represented by the polynomials*

$$at + b \bmod p(t),$$

where $a, b \in \{0, \pm 1\}$. *(We have changed the variable to* t *to avoid confusion with the* x*-coordinate.)*

The homomorphism

$$\theta : x \mapsto x^2 : \mathbb{F}_{3^2}^\times \to \mathbb{F}_{3^2}^\times$$

has

$$\ker \theta = \{\pm 1\}.$$

It follows that there are just 4 squares in $\mathbb{F}_{3^2}^{\times}$*, and it is easy to see that these are*

$$1, t^2 = -1, (t+1)^2 = -t, (t-1)^2 = t.$$

ie

$$[0,1],\ [0,-1],\ [1,0],\ [-1,0].$$

We draw up a table for the 9 values $x \in \mathbb{F}_{3^2}$ *together with* $x^3 + x$ *and possible values for* y*:*

x	$x^3 + x$	y
0	0	0
1	-1	$\pm t$
-1	1	± 1
t	0	0
$t+1$	$-t+1$	$-$
$t-1$	$-t-1$	$-$
$-t$	0	0
$-t+1$	$t+1$	$-$
$-t-1$	$t-1$	$-$

Thus there are 8 points on the curve (including the point at infinity).
Also, there are 3 points of order 2 (with $y = 0$*).*
There are 3 abelian groups of order 8:

$$\mathbb{Z}/(8),\ \mathbb{Z}/(4) \oplus \mathbb{Z}/(2),\ \mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(2).$$

These have, respectively, $1, 3, 7$ *elements of order 2.*
We conclude that the group on the curve is

$$\mathbb{Z}/(4) \oplus \mathbb{Z}/(2).$$