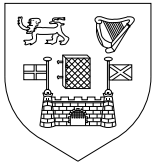

Course 374 (Cryptography)

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

7. 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)

8. 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 mod11 *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.

9. 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* mod3. *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

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