Course 374 (Cryptography)
Sample Paper 1

Dr Timothy Murphy

GMB ?? Friday, ?? 2007 ??:00–??:00

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

Part B

9. Prove that the multiplicative group $F^\times$ of a finite field F is cyclic.

   Find all the primitive roots mod17, ie the generators of $(\mathbb{Z}/17)^\times$.

   How many primitive elements does $\mathbb{F}_{3^3}$ possess?

   Answer:

   (a) *Let*
$$\|F\| = q.$$

   Lemma 1. *The exponent of $F^\times$ is $q - 1$.*

   Proof. By Lagrange's Theorem,
$$e \mid q - 1$$

   On the other hand, since the equation
$$x^e - 1 = 0$$

has at most e roots in F,

$$q - 1 \leq e.$$

Hence

$$e = q - 1.$$

$\square$

Lemma 2. *If A is an abelian group, and $g, h \in A$ are of orders m, n, where*

$$\gcd(m, n) = 1,$$

then gh is or order mn.

Proof. Suppose the order of gh is d. Then

$$d \mid mn,$$

since

$$(gh)^{mn} = g^{mn} h^{mn} = 1,$$

On the other hand,

$$(gh)^d = 1 \implies (gh)^{md} = h^{md} = 1.$$

Thus

$$n \mid md \implies n \mid d,$$

since $\gcd(m, n) = 1$. Similarly

$$m \mid d.$$

Hence

$$mn \mid d,$$

since $\gcd(m, n) = 1$; and so

$$d = mn.$$

$\square$

Lemma 3. *A finite abelian group A of exponent e contains an element of order e.*

Proof. Suppose

$$e = p_1^{e_1} \cdots p_r^{e_r}.$$

For each $i \in [1, r]$, A contains an element α_i of order divisible by $p_i^{e_i}$, say of order $p_i^{e_i} q_i$. But then

$$\beta_i = \alpha_i^{q_i}$$

is of order $p_i^{e_i}$.

Hence by the previous Lemma,

$$\beta = \beta_1 \cdots \beta_r$$

is of order

$$e = p_1^{e_1} \cdots p_r^{e_r}.$$

□

It follows from this Lemma that $F^\times$ *contains an element of order* $e = q - 1$*, and so is cyclic.*

(b) $(\mathbb{Z}/17)^\times$ *is a cyclic group of order 16. So each element has order 1,2,4,8 or 16.*

There is 1 element of order 1, namely 1; 1 element of order 2, namely -1; $\phi(4) = 2$ *elements of order 4;* $\phi(8) = 4$ *elements of order 8; and* $\phi(16) = 8$ *elements of order 28,*

If x *has order 16 then*

$$x^8 = -1.$$

Hence

$$(-x)^8 = -1,$$

and so the 4 elements $\pm x, \pm x^{-1}$ *all have order 16.*

Since

$$2^4 = -1 \bmod 17$$

it follows that 2 has order $8 \bmod 17$*.*

Since

$$(-2)^4 = 2^4 = -1 \bmod 17$$

it follows that the 4 elements of order 8 are

$$\pm 2, \pm 2^{-1},$$

ie

$$2, 15, 9, 8.$$

Also, since 2 is of order 8, $4 = 2^2$ *is of order 4. Thus the 2 elements of order 4 are*

$$\pm 4,$$

ie

$$4, 13.$$

Thus the 8 elements of order 16 (ie the primitive roots) are:

$$3, 5, 6, 7, 10, 11, 12, 14.$$

(c) *The number of primitive elements in* $\mathbb{F}_{3^3}$ *is*

$$\begin{aligned} \phi(3^3 - 1) &= \phi(26) \\ &= \phi(2)\phi(13) \\ &= 1 \cdot 12 \\ &= 12. \end{aligned}$$

10. Explain what is meant by a *singular point* on a curve, and show that the curve

$$y^2 = x^3 + ax^2 + bx + c$$

is always singular over a field of characteristic 2.

What is the condition for the curve to be singular over a field of characteristic $\neq 2$?

Determine whether the equation

$$y^2 = x^3 + x^2 + x + 1$$

defines an elliptic curve over each of the fields $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7, \mathbb{F}_8$; and in those cases where it does, determine the group on the curve (as eg $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$).

Answer:

(a) *Suppose the curve is given by*

$$F(X, Y, Z) = 0$$

in homogeneous coordinates. Then the point $P = [X_0, Y_0, Z_0]$ *on the curve is said to be singular if*

$$\partial F/\partial X = \partial F/\partial Y = \partial F/\partial Z = 0$$

at P. *[In other words,* P *is singular if the tangent at* P *is undefined.]*

(b) *In homogeneous coordinates the curve is given by*

$$F(X, Y, Z) \equiv Y^2Z + X^3 + aX^2Z + bXZ^2 + cZ^3 = 0.$$

Thus

$$\partial F/\partial X = X^2 + bZ^2,$$
$$\partial F/\partial Y = 0 \partial F/\partial Z \qquad = aX^2 + cZ^2.$$

It follows that the point $O = [0, 1,]$, *which is on the curve, is singular. Hence the curve is singular.*

(c) *If* $\operatorname{char} k \neq 2$ *then the curve*

$$y^2 = x^3 + ax^2 + bx + c$$

is singular if and only if the polynomial

$$p(x) = x^3 + ax^2 + bx + c$$

has a multiple root.
The condition for this is that

$$\gcd(p(x), p'(x)) \neq 1.$$

$k = \mathbb{F}_3$ *Then*

$$p(x) = x^3 + x^2 + x + 1, \quad p'(x) = 2x + 1.$$

Since

$$p'(x) = 0 \implies x = -1/2 = 1$$

and

$$p(1) = 1 \neq 0,$$

the curve is non-singular, and so is an elliptic curve.
The quadratic residues mod3 *are* $\{0, 1\}$.
Let us draw up a table for $x, p(x), y$:

x	$p(x)$	y
0	1	± 1
1	1	± 1
-1	0	0

We deduce that the curve has 6 points: $(0, \pm 1)$, $(1, \pm 1)$, $(0, 0)$ *and the point* $[0, 1, 0]$ *at infinity.*
There is only 1 abelian group of order 6, namely $\mathbb{Z}/(6) = \mathbb{Z}/(2) \oplus \mathbb{Z}/(3)$, *so we deduce that*

$$\mathcal{E}(\mathbb{F}_3) \cong \mathbb{Z}/(6).$$

$k = \mathbb{F}_5$ *Then*

$$p(x) = x^3 + x^2 + x + 1, \quad p'(x) = 3x^2 + 2x + 1.$$

Now

$$3p(x) - xp'(x) = x^2 + 2x + 3,$$

while

$$3(x^2 + 2x + 3) - p(x) = 4x + 8.$$

Thus

$$\gcd(p(x), p'(x)) = 1 \iff p(-2) \neq 0.x = -2.$$

In fact

$$p(-2) = -8 + 4 - 2 + 1 = 2 - 1 - 2 + 1 = 0.$$

Thus the curve is singular in this case, and so is not an elliptic curve.

$k = \mathbb{F}_7$ *As before,*

$$3p(x) - xp'(x) = x^2 + 2x + 3,$$
$$3(x^2 + 2x + 3) - p(x) = 4x + 8.$$

But in this case

$$p(-2) = -8 + 4 - 2 + 1 = -1 - 3 - 2 + 1 = 2 \neq 0.$$

Thus the curve is non-singular, ie it is an elliptic curve.
The quadratic residues $\bmod 7$ *are* $\{0, 1, 2, 4\} = \{0, 1, 2, -3\}$.
We draw up the table for $x, p(x), y$*:*

x	$p(x)$	y
0	1	± 1
1	-3	± 3
2	1	± 1
3	-2	$-$
-3	1	± 1
-2	2	± 3
-1	0	0

We deduce that the curve has 12 points: $(0, \pm 1),\ (1, \pm 3),\ (2, \pm 1),\ (-3, \pm 1),\ (-2, \pm$
and the point $[0, 1, 0]$ *at infinity.*

There are 2 abelian groups of order 12, namely $\mathbb{Z}/(4)\oplus\mathbb{Z}/(3) = \mathbb{Z}/12$ *and* $\mathbb{Z}/(2) \oplus \mathbb{Z}(2) \oplus \mathbb{Z}(3) = \mathbb{Z}/(6) \oplus \mathbb{Z}/(2)$.
The first of these has just 1 element of order 2, while the second has 3 elements of order 2.
But if $P = (x, y)$ *then*

$$-P = (x, -y).$$

It follows that P *is of order 2 if and only if* $y = 0$. *Since* $(-1, 0)$ *is the only such point in this case, we deduce that*

$$\mathcal{E}(\mathbb{F}_3) \cong \mathbb{Z}/(12).$$

$\mathbb{F}_8$ *The curve in this case is singular.*
[More generally, the curve

$$y^2 = f(x),$$

where $f(x)$ *is a cubic, is always singular in characteristic 2. To get an elliptic curve in characteristic 2, there must be a term in* xy *or* y*, or both, on the left. If the characteristic is not 2 then one can complete the square on the left,*

$$y^2 + Axy + By = (y + Ax/2 + B/2)^2 + g(x).]$$

To verify singularity in this case, we write the equation in projective form:

$$F(X, Y, Z) \equiv Y^2Z + X^3 + X^2Z + XZ^2 + Z^3 = 0.$$

Now

$$\begin{aligned}\partial F/\partial X &= X^2 + Z^2,\\ \partial F/\partial Y &= 0,\\ \partial F/\partial Z &= Y^2 + X^2 + Z^2.\end{aligned}$$

The fact the $\partial F/\partial Y$ *vanishes identically means that a singular point can be found by solving 2 equations in 3 unkowns, which is always possible.*
In general the solution does not lie in the ground field, but in this case it does: $(1, 0) = [1, 0, 1]$ *is a singular point on the curve.*

11. Show that a polynomial $f(x)$ of degree n over the finite field $\mathbb{F}_p$ is irreducible if and only if

$$\gcd(f(x), x^{p^m} - x) = 1$$

for $m = 1, 2, \ldots, [n/2]$.

Find an irreducible polynomial $p(x)$ of degree 6 over $\mathbb{F}_2$.

Show that

$$y^2 + y = x^3 + 1$$

defines an elliptic curve over $\mathbb{F}_{2^6}$, and determine the group on this curve.

Answer:

(a) If $f(x)$ is composite, it must have a factor $g(x)$ of degree $m \le [n/2]$.

Recall that

$$U_m(x) = x^{p^m} - x = \prod \pi(x)$$

where $\pi(x)$ runs over all irreducible polynomials of degree $d \mid m$.

In particular

$$g(x) \mid U_m(x)$$

and so

$$\gcd(f(x), U_m(x)) \neq 1.$$

Conversely, suppose

$$\gcd(f(x), U_m(x)) \neq 1.$$

Then some irreducible factor $\pi(x)$ of $U_m(x)$ must divide $f(x)$. This factor has degree $d \le m$, and so is not $f(x)$. Hence $f(x)$ is composite.

(b) Consider the polynomial

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

in $\mathbb{F}_2[x]$.

Since x is not a factor of $f(x)$, this will be irreducible if and only if

$$\gcd(f(x), x^{2^m - 1} - 1) = 1$$

for $m = 2, 3$.

Now

$$x^6 \equiv 1 \bmod x^3 - 1,$$

and so

$$f(x) \equiv x \bmod x^3 - 1.$$

Hence

$$\gcd(f(x), x^3 - 1) = 1$$

Also

$$xf(x) = x^7 + x^2 + x \equiv x^2 + x + 1 \bmod x^7 - 1,$$

while

$$x^3 - 1 = (x - 1)(x^2 + x + 1) \equiv 0 \bmod x^2 + x + 1.$$

Hence

$$x^6 \equiv 1 \bmod x^2 + x + 1,$$

and so

$$x^6 + x + 1 \equiv x^2 \bmod x^2 + x + 1.$$

Thus

$$\gcd(f(x), x^7 - 1) = 1.$$

We conclude that

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

is irreducible over $\mathbb{F}_2$.

(c) The curve

$$y^2 + y = x^3 + 1$$

takes homogeneous form

$$F(X, Y, Z) = Y^2 Z + Y Z^2 + X^3 + Z^3.$$

Now

$$\begin{aligned} \partial F/\partial X &= X^2, \\ \partial F/\partial Y &= Z^2, \\ \partial F/\partial Z &= Y^2 + Z^2. \end{aligned}$$

Thus

$$\partial F/\partial X = \partial F/\partial Y = \partial F/\partial Z = 0 \implies X = Y = Z = 0.$$

Hence the curve is non-singular (since $[0, 0, 0]$ *is not a point in the projective plane).*

(d) *We want to determine the number of points, N say, on the curve $\mathcal{E}(\mathbb{F}_{2^6})$.*

Note first that the left-hand side of the equation, $y^2+y = y(y+1)$, is invariant under $y \mapsto y+1$. Thus

$$(x, y) \in \mathcal{E}(\mathbb{F}_{2^6}) \iff (x, y+1) \in \mathcal{E}(\mathbb{F}_{2^6}).$$

[In fact, since the line $x = c$ passing through these two points also passes through $O = [0, 1, 0]$, these points are the negatives of each other:

$$-(x, y) = (x, y+1).]$$

On adding the point $[0, 1, 0]$ at infinity on the curve, it follows that N is odd.

The points defined over $\mathbb{F}_2$, $\mathbb{F}_{2^2}$, $\mathbb{F}_{2^3}$ give subgroups of $\mathcal{E}(\mathbb{F}_{2^6}$:

$$\mathcal{E}(\mathbb{F}_2) \subset \mathcal{E}(\mathbb{F}_{2^2}) \subset \mathcal{E}(\mathbb{F}_{2^6}), \ \mathcal{E}(\mathbb{F}_2) \subset \mathcal{E}(\mathbb{F}_{2^3}) \subset \mathcal{E}(\mathbb{F}_{2^6}).$$

We start by looking at the smaller groups, since this will probably give useful information about the large group.

$\mathbb{F}_2$ *By inspection the curve $\mathcal{E}(\mathbb{F}_2)$ contains the points $(1, 0)$, $(1, 1)$, together with the point at infinity. Thus*

$$\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(3).$$

$\mathbb{F}_{2^2}$ *If $x = 0$ the equation becomes*

$$y^2 + y + 1 = 0.$$

This polynomial is irreducible over $\mathbb{F}_2$, but has two roots in $\mathbb{F}_{2^2}$, since we could take

$$\mathbb{F}_{2^2} = \mathbb{F}_2[x]/(x^2 + x + 1).$$

We know that the number of points on the curve is divisible by 3 (since $\mathcal{E}(\mathbb{F}_2) = \mathbb{Z}/(3)$ is a subgroup). So there is at least one more point, with $x \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$.

But in fact, as we have seen, if there is one such point for a given x then there are two.

This implies that both values of x must provide 2 new points, giving 9 points in all.

[Concretely, the elements of $\mathbb{F}_{2^2} \setminus \mathbb{F}_2$ are the roots of

$$x^2 + x + 1 = 0.$$

If one root is ω *then the other is* ω^2*.*
The 9 points on the curve are:

$$(0,\omega),\ (0,\omega^2),\ (1,0),\ (1,1),\ (\omega,0),\ (\omega,1),\ (\omega^2,0),\ (\omega^2,1),$$

together with the point $[0,1,0]$ *at infinity.]*
It follows that

$$\mathcal{E}(\mathbb{F}_{2^2}) = \mathbb{Z}/(9) \textit{ or } \mathbb{Z}/(3) \oplus \mathbb{Z}/(3).$$

To distinguish between these, we use a little geometry to identify the points of order 3 on the curve.
A point P *on an elliptic curve has order 3 if and only if it is* a point of inflexion, *ie the tangent at* P *meets the curve in 3 points* P, P, P*. For* $2P = -Q$*, where* Q *is the point where the tangent meets the curve again. Thus*

$$3P = 0 \iff 2P = -P \iff Q = P,$$

ie the tangent meets the curve again at P*.*
The tangent at $P = (x, y)$ *is*

$$y = mx + c,$$

where $m = dy/dx$*. In our case*

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

ie

$$m = x^2.$$

This meets the curve where

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

If the roots of this cubic are x_1, x_2, x_3 *then*

$$x_1 + x_2 + x_3 = m^2.$$

Thus

$$\begin{aligned} 3P = 0 &\iff 3x = m^2 \\ &\iff x = x^4 \\ &\iff x^3 = 1, \end{aligned}$$

if we ignore the case $x = 0$ *(which we know from* $\mathcal{E}(\mathbb{F}_2)$ *does actually give 2 points of order 3).*
But we know (from Lagrange's Theorem) that

$$x \in \mathbb{F}_{2^3}^\times \implies x^3 = 1.$$

We conclude that all the points on $\mathcal{E}(\mathbb{F}_{2^2})$ *are of order 3, and so*

$$\mathcal{E}(\mathbb{F}_{2^2}) = \mathbb{Z}/(3) \oplus \mathbb{Z}(3).$$

$\mathbb{F}_{2^3}$ *The map*

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

has $\ker \theta = \{1\}$ *(since the group has order 8). Thus each element of* F_{2^3} *has a unique cube root.*
It follows that the equation, which can be written

$$x^3 = y^2 + y + 1,$$

has a unique solution for each y*. Thus there are* $8 + 1 = 9$ *points on the curve; and so*

$$\mathcal{E}(\mathbb{F}_{2^3}) = \mathbb{Z}/(9) \text{ or } \mathbb{Z}/(3) \oplus \mathbb{Z}/(3).$$

But as we saw in the case $\mathbb{F}_{2^2}$*, the point* $P = (x, y)$ *is of order 3 if and only if* $x = 0$ *or* $x^3 = 1$*.*
As we just saw, if $x \in \mathbb{F}_{2^3}^\times$ *then*

$$x^3 = 1 \implies x = 1 \implies y = 0 \text{ or } 1.$$

Thus there are just 2 points of order 3 on $\mathcal{E}(\mathbb{F}_{2^3})$*, namely* $\mathcal{E}(\mathbb{F}_2) \setminus O$*, and so*

$$\mathcal{E}(\mathbb{F}_{2^3}) = \mathbb{Z}/(9).$$

Now let us turn to $\mathcal{E}(\mathbb{F}_{2^6})$*. Since*

$$\mathcal{E}(\mathbb{F}_{2^2}) \cap \mathcal{E}(\mathbb{F}_{2^2}) = \mathcal{E}(\mathbb{F}_2)$$

it follows that the subgroup

$$\mathcal{E}(\mathbb{F}_{2^2}) + \mathcal{E}(\mathbb{F}_{2^2}) = \mathbb{Z}/(3) \oplus \mathbb{Z}/(9).$$

(This is the only one of the 3 abelian groups of order 3^3 *with subgroups* $\mathbb{Z}/(9)$ *and* $\mathbb{Z}/(3) \oplus \mathbb{Z}/(3)$*).*
In particular, if $\mathcal{E}(\mathbb{F}_{2^6}$ *has* N *points then*

$$27 \mid N.$$

Also, by Hasse's theorem,

$$|N - 65| \leq 2\sqrt{64} = 16,$$
$$49 \leq N \leq 81.$$

ie

Since N is odd, it follows that

$$N = 81 = 3^4.$$

There are three possibilities:

$\mathcal{E}(\mathbb{F}_{2^6}) = \mathbb{Z}/(27) \oplus \mathbb{Z}/(3)$ *or* $\mathbb{Z}/(9) \oplus \mathbb{Z}/(9)$ *or* $\mathbb{Z}/(9) \oplus \mathbb{Z}/(3) \oplus \mathbb{Z}/(3)$.

The first two of these groups have $3^2 - 1$ elements of order 3, while the last has $3^3 - 1 = 26$.
As we have seen, if $P = (x, y)$ then

$$3P = 0 \iff x = 0 \text{ or } x^3 = 1.$$

Thus the only points of order 3 are the 8 in $\mathcal{E}(\mathbb{F}_{2^2})$, ruling out the third group.
To distinguish between the first 2 cases, let us determine the number of points of order 9.
We have seen that if $P = (x, y) \in \mathcal{E}(\mathbb{F}_{2^6})$ then

$$\begin{aligned} 2P = (x^4, y_1) &\implies 4P = (x^{16}, y_2) \\ &\implies 8P = (x^{64}, y_3). \end{aligned}$$

But

$$x^64 = x$$

for all $x \in \mathbb{F}_{2^6}$. Hence

$$8P = \pm P$$

for all points on the curve. Now

$$8P = P \implies 7P = 0$$

is impossible (since the group has order 3^4). We conclude that

$$9P = 0$$

for all $P \in \mathcal{E}(\mathbb{F}_{2^5})$.
Hence

$$\mathcal{E}(\mathbb{F}_{2^6}) = \mathbb{Z}/(9) \oplus \mathbb{Z}/(9).$$

[That was much more difficult than intended!]