# Math 502
# Written Assignment No. 5

**due Monday, May 7, 2007**

## 1 Cryptography on Cubic Curves over $\mathbf{F}_\ell$

In the following $\ell$ will denote a prime greater than 2, and $\mathbf{F}_\ell \cong \mathbf{Z}/\ell\mathbf{Z}$ the field of integers modulo $\ell$. We will be talking about "addition", as previously studied, on a cubic curve $E$ given in Weierstrass form, i.e., $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with coefficients in $\mathbf{F}_\ell$, and points $(x, y)$ of $E$ will be pairs of elements $x, y$ in $\mathbf{F}_\ell$. A reference for this material is the book *A Course in Number Theory and Cryptography* by Neal Koblitz, published in 1987 by Springer. Some information may also be found online; for example, one might look at Wikipedia[1].

### 1.1 Representing characters by points on a curve

As before, characters may be represented by numbers; in particular, characters and standard symbols in U.S. English may be represented by their ASCII codes, which are integers from 0 to 127. The question here is how to represent a number $N$ in this range by a point of $E$. In the first place $l$ must be large enough that $E$ contains at least 127 points. Since for a point $(x, y)$ of $E$ the second coordinate $y$ is the root of a quadratic polynomial in the first coordinate $x$, letting $x$ be $N$ and then solving for $y$ will not lead to a root $y$ in $\mathbf{F}_\ell$ unless the discriminant of the corresponding quadratic equation is the square of an element of $\mathbf{F}_\ell$. Precisely half of the non-zero elements of $\mathbf{F}_\ell$ are squares, so the discriminant will be a square roughly half the time. Because of that $x$ cannot simply be $N$ but rather something determined by $N$ that offers a range of possible values of $x$.

One chooses an integer $m$ so that $1/2^m$ is an acceptably small probability of failure to find a $y$ for given $x$. The idea then is, for a given number $N$, to try as many as $m$ different values of $x$ until there is found a $y$ with $(x, y)$ on $E$. The values of $x$ one tries are

$$x = mN + j\,, \quad 1 \le j \le m \quad .$$

The event that one does not find a $y$ after trying all $m$ of these values has probability $1/2^m$. If a $y$ is found, then the point $p = (x, y)$ becomes the point of the curve representing the number $N$. There is no secrecy in this. The original number $N$ may be recovered from $p$ as the largest integer strictly smaller than $x/m$ or

$$N = \text{floor}(\frac{x-1}{m}) \quad .$$

It is necessary that $\ell \ge 128m$ if this method is to be viable for representing integers $0 \le N \le 127$ by a point on a given curve $E$ over $\mathbf{F}_\ell$.

[1] URI: http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

### 1.2 Encoding points on a curve

Here the question is encoding for secrecy the points on a curve. As with the earlier foray into cryptography the method discussed here – which is named El Gamal – involves public knowledge of how to encrypt with only secret knowledge of how to decrypt. One wants a curve having a base point $b$ of large order relative to the arithmetic on $E$. For example, if the number of all points $|E|$ of $E$ happens to be prime, which is far from always true, then there will be a point $b$ of $E$ having order $|E|$. As suggested above, for any $E$ the number $|E|$ of its points is usually somewhere around $\ell$ since there are two points on $E$ for each of the roughly $\ell/2$ values of $x$ for which there is a $y$ except for the case when $x$ leads to a quadratic equation for $y$ having discriminant 0. In this scheme a single point $p$ on $E$ will be encrypted by a pair $(q, r)$ where both $q$ and $r$ are points of $E$.

The designer of the scheme picks the prime $\ell$, the curve $E$, a "base point" $b$ on $E$ of large order, all of which are to be public, and a secret element $j$ of $\mathbf{F}_\ell$. With those items fixed, the designer publishes one more point $c$ on $E$ that is determined by the formula $c = jb$. For given $\ell$ and $E$, the scheme's "public key" is the pair of points $b$ and $c$ on $E$.

A user of this scheme may encode a point $p$ of $E$ as follows: (i) draw a non-zero random value $k$ mod $\ell$ and then (ii) produce the pair of points $(q, r)$ using the formulae:

$$\begin{aligned} q &= kb \\ r &= p + kc \end{aligned}$$

Anyone who knows the secret value $j$ as well as the published data may recover the original point $p$ from the pair $(q, r)$ using the simple formula

$$p = r - jq \quad .$$

Security for this system relies on it being difficult to ascertain $j$ even though $b$ and $c$ are both known.

## 2 Problems

**Directions:** Use *Maple* for assistance in responding to the following problems. **Please typeset** your solutions. Explain what you have done. *Maple* session details are not necessary unless you think it important to include them. Accuracy is important.

Although you may refer to books and notes, you may not seek help from others on this written assignment.

1. Let $E$ be the curve $y^2 = x^3 + 43x + 13$ over $\mathbf{F}_{1283}$.
   (a) Find the number of points on $E$.
   (b) Find a point on $E$ of largest order in the arithmetic of points on $E$ over $\mathbf{F}_{1283}$.
2. Let $E$, as above, be the curve $y^2 = x^3 + 43x + 13$ over $\mathbf{F}_{1283}$. Find $j$ in $\mathbf{F}_{1283}$ such that $(0, 1247) = j(1, 338)$, i.e.,

   $$(0, 1247) = \underbrace{(1, 338) + (1, 338) + \ldots + (1, 338)}_{j \text{ times}}$$

   relative to the arithmetic of points

3. Let $E$, as above, be the curve $y^2 = x^3 + 43x + 13$ over $\mathbf{F}_{1283}$. Assume that the sequence of ASCII codes (range 0 to 127) for a text string is to be converted to a sequence of points on $E$ as described in 1.1 above with conversion failure probability $1/2^m$ where $m = 10$. What text string is represented by the following sequence of points?

```
[ [ 871,  375], [1041,  866], [1013,  352], [1143, 1151],

  [1013,  352], [ 391,  259], [1151,  248], [ 321,  486],

  [1162,  391], [1041,  866], [1013,  352], [ 321,  486],

  [ 662,  150], [1013,  352], [1013,  352], [1022, 1227],

  [ 631,  897] ]
```

4. Now switch to the curve $y^2 = x^3 + 43x + 13$ over the field $\mathbf{F}_{40487}$, which may be seen to have 40611 points. Numbers from 0 to 127 are to be represented as points on this curve with conversion failure probability $1/2^{10}$.

   (a) As described in 1.2 above an encryption scheme owner has published $b = (144, 25562)$ and $c = (20489, 39430)$. Represent the string "ABC" as a sequence of 3 points on this curve and compute an encryption of it for delivery to this owner.

   (b) You own an encryption scheme for this same curve with secret key 257. You receive from someone else the following sequence of 3 pairs of points on this curve:

   ```
   [[21002, 35305], [32172, 29672]]
   [[28238, 39896], [18730,  4860]]
   [[15467, 39118], [30952, 38775]]
   ```

   What 3 character string lies behind it?