Lecture 3

Elliptic curves over finite fields

First steps

College of Sciences
Department of Mathematics
University of Salahaddin,
Erbil, Kurdistan December 4th, 2014

Francesco Pappalardi
Dipartimento di Matematica e Fisica
Università Roma Tre

Proto–History (from WIKIPEDIA)

Giulio Carlo, Count Fagnano, and Marquis de Toschi (December 6, 1682 – September 26, 1766) was an Italian mathematician. He was probably the first to direct attention to the theory of *elliptic integrals*. Fagnano was born in Senigallia.

He made his higher studies at the *Collegio Clementino* in Rome and there won great distinction, except in mathematics, to which his aversion was extreme. Only after his college course he took up the study of mathematics.

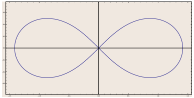
Later, without help from any teacher, he mastered mathematics from its foundations.

Some of His Achievements:

- $\pi = 2i \log \frac{1-i}{1+1}$
- Length of *Lemniscate*

Carlo Fagnano

Collegio Clementino



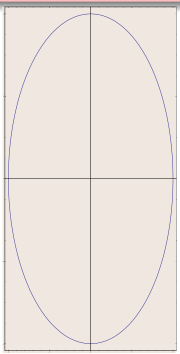
Lemniscate

$(x^2 + y^2)^2 = 2a^2(x^2 - y^2)$

$$\ell = 4 \int_0^a \frac{a^2\,dr}{\sqrt{a^4 - r^4}} = \frac{a\sqrt{\pi}\,\Gamma(\frac{5}{4})}{\Gamma(\frac{3}{4})}$$

Length of Ellipses

$$\mathcal{E} : \frac{x^2}{4} + \frac{y^2}{16} = 1$$



The length of the arc of a plane curve $y = f(x)$, $f : [a, b] \to \mathbb{R}$ is:

$$\ell = \int_a^b \sqrt{1 + (f'(t))^2} dt$$

Applying this formula to $\mathcal{E}$:

$$\ell(\mathcal{E}) = 4 \int_0^4 \sqrt{1 + \left(\frac{d\sqrt{16(1 - t^2/4)}}{dt} \right)^2} dt$$

$$= 4 \int_0^1 \sqrt{\frac{1 + 3x^2}{1 - x^2}} dx \qquad x = t/2$$

If y is the integrand, then we have the identity:

$$y^2(1 - x^2) = 1 + 3x^2$$

Apply the invertible change of variables:

$$\begin{cases} x = 1 - 2/t \\ y = \frac{u}{t-1} \end{cases}$$

Arrive to

$$u^2 = t^3 - 4t^2 + 6t - 3$$

What are Elliptic Curves?
Reasons to study them

Elliptic Curves

1. are curves and finite groups at the same time
2. are non singular projective curves of *genus* 1
3. have important applications in Algorithmic Number Theory and Cryptography
4. are the topic of the Birch and Swinnerton-Dyer conjecture (one of the seven Millennium Prize Problems)
5. have a group law that is a consequence of the fact that they intersect every line in exactly three points (in the projective plane over $\mathbb{C}$ and counted with multiplicity)
6. represent a mathematical world in itself ... Each of them does!!

Notations

Fields of characteristics 0

1. $\mathbb{Q}$ is the field of rational numbers
2. $\mathbb{R}$ and $\mathbb{C}$ are the fields of real and complex numbers
3. $K \subset \mathbb{C}$, $\dim_{\mathbb{Q}} K < \infty$ is a *number field*
   - $\mathbb{Q}[\sqrt{d}]$, $d \in \mathbb{Q}$
   - $\mathbb{Q}[\alpha]$, $f(\alpha) = 0$, $f \in \mathbb{Q}[X]$ irreducible

Finite fields

1. $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ is the prime field;
2. $\mathbb{F}_q$ is a finite field with $q = p^n$ elements
3. $\mathbb{F}_q = \mathbb{F}_p[\xi]$, $f(\xi) = 0$, $f \in \mathbb{F}_p[X]$ irreducible, $\partial f = n$
4. $\mathbb{F}_4 = \mathbb{F}_2[\xi]$, $\xi^2 = 1 + \xi$
5. $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, $\alpha^3 = \alpha + 1$ but also $\mathbb{F}_8 = \mathbb{F}_2[\beta]$, $\beta^3 = \beta^2 + 1$, $(\beta = \alpha^2 + 1)$
6. $\mathbb{F}_{101^{101}} = \mathbb{F}_{101}[\omega], \omega^{101} = \omega + 1$

Notations

Algebraic Closure of $\mathbb{F}_q$

- $\mathbb{C} \supset \mathbb{Q}$ satisfies that *Fundamental Theorem of Algebra*! (i.e. $\forall f \in \mathbb{Q}[x], \partial f > 1, \exists \alpha \in \mathbb{C}, f(\alpha) = 0$)
- We need a field that plays the role, for $\mathbb{F}_q$, that $\mathbb{C}$ plays for $\mathbb{Q}$. It will be $\overline{\mathbb{F}}_q$, called *algebraic closure of* $\mathbb{F}_q$
-
  1. $\forall n \in \mathbb{N}$, we fix an $\mathbb{F}_{q^n}$
  2. We also require that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if $n \mid m$
  3. We let $\overline{\mathbb{F}}_q = \bigcup_{n \in \mathbb{N}} \mathbb{F}_{q^n}$
- **Fact:** $\overline{\mathbb{F}}_q$ is *algebraically closed* (i.e. $\forall f \in \mathbb{F}_q[x], \partial f > 1, \exists \alpha \in \overline{\mathbb{F}}_q, f(\alpha) = 0$)

If $F(x, y) \in \mathbb{Q}[x, y]$ a *point of the curve* $F = 0$, means $(x_0, y_0) \in \mathbb{C}^2$ s.t. $F(x_0, y_0) = 0$.

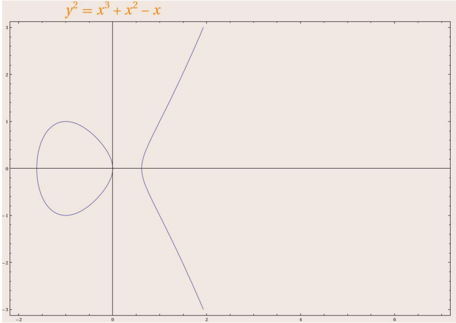
If $F(x, y) \in \mathbb{F}_q[x, y]$ a *point of the curve* $F = 0$, means $(x_0, y_0) \in \overline{\mathbb{F}}_q^2$ s.t. $F(x_0, y_0) = 0$.

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$



The equation should not be *singular*

Tangent line to a plane curve

Given $f(x,y) \in \mathbb{F}_q[x,y]$ and a point (x_0,y_0) such that $f(x_0,y_0)=0$, the *tangent line* is:

$$\frac{\partial f}{\partial x}(x_0,y_0)(x-x_0)+\frac{\partial f}{\partial y}(x_0,y_0)(y-y_0)=0$$

If

$$\frac{\partial f}{\partial x}(x_0,y_0)=\frac{\partial f}{\partial y}(x_0,y_0)=0,$$

such a tangent line cannot be computed and we say that (x_0,y_0) is *singular*

Definition

A non singular curve is a curve without any singular point

Example

The tangent line to $x^2+y^2=1$ over $\mathbb{F}_7$ at $(2,2)$ is

$$x+y=4$$

Singular points
The classical definition

Definition

A *singular* point (x_0, y_0) on a curve $f(x, y) = 0$ is a point such that

$$\begin{cases} \frac{\partial f}{\partial x}(x_0, y_0) = 0 \\ \frac{\partial f}{\partial y}(x_0, y_0) = 0 \end{cases}$$

So, at a singular point there is no (unique) tangent line!! In the special case of Weierstraß equations:

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

we have

$$\begin{cases} \partial_x = 0 \\ \partial_y = 0 \end{cases} \longrightarrow \begin{cases} a_1 y = 3x^2 + 2a_2 x + a_4 \\ 2y + a_1 x + a_3 = 0 \end{cases}$$

We can express this condition in terms of the coefficients a_1, a_2, a_3, a_4, a_5.

The Discriminant of an Equation

The condition of absence of singular points in terms of a_1, a_2, a_3, a_4, a_6

With a bit of `Mathematica`

```
Ell:=-a_6-a_4x-a_2x^2-x^3+a_3y+a_1xy+y^2;
SS := Solve[{D[Ell,x]==0,D[Ell,y]==0},{y,x}];
Simplify[ReplaceAll[Ell,SS[[1]]]*ReplaceAll[Ell,SS[[2]]]]
```

we obtain

$$\Delta'_E := \frac{1}{2^4 3^3}\big(-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16a_1 a_2^2 a_3 a_4 + 36a_1^2 a_3^2 a_4 - a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16a_2^2 a_4^2 + 96a_1 a_3 a_4^2 + 64a_4^3 + a_1^6 a_6 + 12a_1^4 a_2 a_6 + 48a_1^2 a_2^2 a_6 + 64a_2^3 a_6 - 36a_1^3 a_3 a_6 - 144a_1 a_2 a_3 a_6 - 72a_1^2 a_4 a_6 - 288a_2 a_4 a_6 + 432a_6^2\big)$$

Definition

The *discriminant* of a Weierstraß equation over $\mathbb{F}_q$, $q = p^n$, $p \geq 5$ is

$$\Delta_E := 3^3 \Delta'_E$$

The discriminant of $E/\mathbb{F}_{2^\alpha}$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{F}_{2^\alpha}$$

If $p = 2$, the singularity condition becomes:

$$\begin{cases} \partial_x = 0 \\ \partial_y = 0 \end{cases} \longrightarrow \begin{cases} a_1y = x^2 + a_4 \\ a_1x + a_3 = 0 \end{cases}$$

Classification of Weierstraß equations over $\mathbb{F}_{2^\alpha}$

- Case $a_1 \neq 0$:

```
El:=a6+a4x+a2x^2+x^3+a3y+a1xy+y^2;
Simplify[ReplaceAll[El,{x→a3/a1,y→((a3/a1)^2+a4)/a1}]]
```

  we obtain

$$\Delta_E := (a_1^6a_6 + a_1^5a_3a_4 + a_1^4a_2a_3^2 + a_1^4a_4^2 + a_1^3a_3^3 + a_3^4)/a_1^6$$

- Case $a_1 = 0$ and $a_3 \neq 0$: curve non singular ($\Delta_E := a_3$)
- Case $a_1 = 0$ and $a_3 = 0$: *curve singular*
  (x_0, y_0), $(x_0^2 = a_4, y_0^2 = a_2a_4 + a_6)$ is the singular point!

Special Weierstraß equation of $E/\mathbb{F}_{p^\alpha}, p \neq 2$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in \mathbb{F}_{p^\alpha}$$

If we “complete the squares“ by applying the transformation:

$$\begin{cases} x \leftarrow x \\ y \leftarrow y - \frac{a_1x+a_3}{2} \end{cases}$$

the Weierstraß equation becomes:

$$E' : y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

where $a_2' = a_2 + \frac{a_1^2}{4}, a_4' = a_4 + \frac{a_1a_3}{2}, a_6' = a_6 + \frac{a_3^2}{4}$
If $p \geq 5$, we can also apply the transformation

$$\begin{cases} x \leftarrow x - \frac{a_2'}{3} \\ y \leftarrow y \end{cases}$$

obtaining the equations:

$$E'' : y^2 = x^3 + a_4''x + a_6''$$

where $a_4'' = a_4' - \frac{a_2'^2}{3}, a_6'' = a_6' + \frac{2a_2'^3}{27} - \frac{a_2'a_4'}{3}$

Special Weierstraß equation for $E/\mathbb{F}_{2^\alpha}$

Case $a_1 \neq 0$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in \mathbb{F}_{2^\alpha}$$
$$\Delta_E := \frac{a_1^6a_6+a_1^5a_3a_4+a_1^4a_2a_3^2+a_1^4a_4^2+a_1^3a_3^3+a_3^4}{a_1^6}$$

If we apply the affine transformation:

$$\begin{cases} x \longleftarrow a_1^2x + a_3/a_1 \\ y \longleftarrow a_1^3y + (a_1^2a_4 + a_3^2)/a_1^2 \end{cases}$$

we obtain

$$E' : y^2 + xy = x^3 + \left(\frac{a_2}{a_1^2} + \frac{a_3}{a_1^3}\right)x^2 + \frac{\Delta_E}{a_1^6}$$

Surprisingly $\Delta_{E'} = \Delta_E/a_1^6$

With Mathematica

```
El:=a6+a4x+a2x^2+x^3+a3y+a1xy+y^2;
Simplify[PolynomialMod[ReplaceAll[El,
  {x->a1^2 x+a3/a1, y->a1^3y+(a1^2a4+a3^2)/a1^3}],2]]
```

Special Weierstraß equation for $E/\mathbb{F}_{2^\alpha}$

Case $a_1 = 0$ and $\Delta_E := a_3 \neq 0$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad a_i \in \mathbb{F}_{2^\alpha}$$

If we apply the affine transformation:

$$\begin{cases} x \longleftarrow x + a_2 \\ y \longleftarrow y \end{cases}$$

we obtain

$$E : y^2 + a_3y = x^3 + (a_4 + a_2^2)x + (a_6 + a_2a_4)$$

With Mathematica

```
El:=a6+a4x+a2x^2+x^3+a3y+y^2;
Simplify[PolynomialMod[ReplaceAll[El,{x->x+a2,y->y}],2]]
```

Definition

Two Weierstraß equations over $\mathbb{F}_q$ are said (affinely) equivalent if there exists a (affine) change of variables that takes one into the other

Fact:

Necessarily the change of variables has form

$$\begin{cases} x \longleftarrow u^2x + r \\ y \longleftarrow u^3y + u^2sx + t \end{cases} \qquad r, s, t, u \in \mathbb{F}_q$$

The Weierstraß equation
Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/\mathbb{F}_q(q = p^n)$ has a Weierstraß equation of the following form

Example (Classification)

E	p	Δ_E
$y^2 = x^3 + Ax + B$	≥ 5	$4A^3 + 27B^2$
$y^2 + xy = x^3 + a_2x^2 + a_6$	2	a_6^2
$y^2 + a_3y = x^3 + a_4x + a_6$	2	a_3^4
$y^2 = x^3 + Ax^2 + Bx + C$	3	$4A^3C - A^2B^2 - 18ABC$ $+4B^3 + 27C^2$

Definition (Elliptic curve)

An elliptic curve is the data of a non singular Weierstraß equation (i.e. $\Delta_E \neq 0$)

Note: If $p \geq 3$, $\Delta_E \neq 0 \Leftrightarrow x^3 + Ax^2 + Bx + C$ has no double root

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Weierstraß equations over $\mathbb{F}_2$

1. $y^2 + xy = x^3 + x^2 + 1$
2. $y^2 + xy = x^3 + 1$
3. $y^2 + y = x^3 + x$
4. $y^2 + y = x^3 + x + 1$
5. $y^2 + y = x^3$
6. $y^2 + y = x^3 + 1$

However the change of variables $\begin{cases} x \leftarrow x + 1 \\ y \leftarrow y + x \end{cases}$ takes the sixth curve into the fifth. Hence we can remove the sixth from the list.

Fact:

There are 5 affinely inequivalent elliptic curves over $\mathbb{F}_2$

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Weierstraß equations over $\mathbb{F}_3$

1. $y^2 = x^3 + x$
2. $y^2 = x^3 - x$
3. $y^2 = x^3 - x + 1$
4. $y^2 = x^3 - x - 1$
5. $y^2 = x^3 + x^2 + 1$
6. $y^2 = x^3 + x^2 - 1$
7. $y^2 = x^3 - x^2 + 1$
8. $y^2 = x^3 - x^2 - 1$

Fact:

1. Over $\mathbb{F}_5$ there are 12 elliptic curves
2. Compute all of them
3. How many are there over $\mathbb{F}_4$, over $\mathbb{F}_7$ and over $\mathbb{F}_8$?

The projective Plane

Definition (Projective plane)

$$\mathbb{P}_2(\mathbb{F}_q) = (\mathbb{F}_q^3 \setminus \{\mathbf{0}\})/\sim$$

where $\mathbf{0} = (0,0,0)$ and

$$\mathbf{x} = (x_1, x_2, x_3) \sim \mathbf{y} = (y_1, y_2, y_3) \quad \Leftrightarrow \quad \mathbf{x} = \lambda \mathbf{y}, \exists \lambda \in \mathbb{F}_q^*$$

Basic properties of the projective plane

1. $P \in \mathbb{P}_2(\mathbb{F}_q) \Rightarrow P = [\mathbf{x}] = \{\lambda \mathbf{x} : \lambda \in \mathbb{F}_q^*\}, \mathbf{x} \in \mathbb{F}_q^3, \mathbf{x} \neq 0;$
2. $\#[\mathbf{x}] = q - 1$. Hence $\#\mathbb{P}_2(\mathbb{F}_q) = \frac{q^3-1}{q-1} = q^2 + q + 1;$
3. $P \in \mathbb{P}_2(\mathbb{F}_q)$, $P =: [x, y, z]$ with $(x, y, z) \in \mathbb{F}_q^3 \setminus \{\mathbf{0}\};$
4. $[x, y, z] = [x', y', z'] \iff \text{rank} \begin{pmatrix} x & y & z \\ x' & y' & z' \end{pmatrix} = 1$
5. $\mathbb{P}_2(\mathbb{F}_q) \longleftrightarrow \{\text{lines through } \mathbf{0} \text{ in } \mathbb{F}_q^3\} = \{V \subset \mathbb{F}_q^3 : \dim V = 1\}$
6. $\mathbb{P}_2(\mathbb{F}_q) \longleftrightarrow \{\text{lines in } \mathbb{F}_q^2\}, [a, b, c] \mapsto aX + bY + cZ = 0$

The projective Plane

Infinite and Affine points

- $P = [x, y, 0]$ *is a point at infinity*
- $P = [x, y, 1]$ *is an affine point*
- $P \in \mathbb{P}_2(\mathbb{F}_q)$ is either affine or at infinity
- $\mathbb{A}_2(\mathbb{F}_q) := \{[x, y, 1] : (x, y) \in \mathbb{F}_q^2\}$ *set of affine points*
  $\#\mathbb{A}_2(\mathbb{F}_q) = q^2$
- $\mathbb{P}_1(\mathbb{F}_q) := \{[x, y, 0] : (x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\}$ *line at infinity*
  $\#\mathbb{P}_1(\mathbb{F}_q) = q + 1$
- $\mathbb{P}_2(\mathbb{F}_q) = \mathbb{A}_2(\mathbb{F}_q) \sqcup \mathbb{P}_1(\mathbb{F}_q)$ disjoint union
- $\mathbb{P}_1(\mathbb{F}_q)$ can be thought as *set of directions of lines in* $\mathbb{F}_q^2$

General construction

- $\mathbb{P}_n(K)$, K field, $n \geq 3$ is similarly defined;
- $\mathbb{P}_n(K) = \mathbb{A}_n(K) \sqcup \mathbb{P}_{n-1}(K)$
- $\#\mathbb{P}_n(\mathbb{F}_q) = q^n + \cdots + q + 1$
- $\mathbb{P}_n(K) \longleftrightarrow \{\text{lines in } K^n\}$

Homogeneous Polynomials

Definition (Homogeneous polynomials)

$g(X_1, \dots, X_m) \in \mathbb{F}_q[X_1, \dots, X_m]$ is said *homogeneous* if all its monomials have the same degree. i.e.

$$g(X_1, \dots, X_m) = \sum_{j_1+\cdots+j_m=\partial g} a_{j_1,\dots,j_m} X_1^{j_1} \cdots X_m^{j_m}, \; a_{j_1,\dots,j_m} \in \mathbb{F}_q$$

Properties of homogeneous polynomials - Projective Curves

- $\forall \lambda, F(\lambda X, \lambda Y, \lambda Z) = \lambda^{\partial F} F(X, Y, Z)$
- If $P = [X_0, Y_0, Z_0] \in \mathbb{P}_2(\mathbb{F}_q)$, then $F(X_0, Y_0, Z_0) = 0$ depends only on P, not on X_0, Y_0, Z_0
- $F(P) = 0 \Leftrightarrow F(X_0, Y_0, Z_0) = 0$ is well defined
- *Projective curve* $F(X, Y, Z) = 0$ the set of $P \in \mathbb{F}_2(\mathbb{F}_q)$ s.t. $F(P) = 0$

Example

Projective line $aX + bY + cZ = 0$; $Z = 0$, line at infinity

Points at infinity of a plane curve

Definition (Homogenized polynomial)

if $f(x, y) \in \mathbb{F}_q[x, y]$,

$$F_f(X, Y, Z) = Z^{\partial f} f(\frac{X}{Z}, \frac{Y}{Z})$$

- F_f is homogenoeus, the homogenized of f
- $\partial F_f = \partial f$
- if $f(x_0, y_0) = 0$, then $F_f(x_0, y_0, 1) = 0$
- the points of the curve $f = 0$ are the affine points of the projective curve $F_f = 0$

Example (homogenized curves)

curve	affine curve	homogenized (projective curve)
line	$ax + by = c$	$aX + bY = cZ$
conic	$ax^2 + by^2 = 1$	$aX^2 + bY^2 = Z^2$

$Z = 0$ (line at infinity) Not the homogenized of anything

Points at infinity of a plane curve

Definition

If $f \in \mathbb{F}_q[x, y]$ then

$$\{[\alpha, \beta, 0] \in \mathbb{P}_2(\mathbb{F}_q) : F_f(\alpha, \beta, 0) = 0\}$$

is the set of *points at infinity* of $f = 0$.
(i.e. the intersection of the curve and $Z = 0$, the line at infinity)

The points of $Z = 0$ are directions of lines in $\mathbb{F}_q^2$

Example (point at infinity)

- line: $ax + by + c = 0 \quad \rightsquigarrow \quad [b, -a, 0]$
- hyperbola: $x^2/a^2 - y^2/b^2 = 1 \quad \rightsquigarrow \quad [a, \pm b, 0]$
- parabola: $y = ax^2 + bx + c \quad \rightsquigarrow \quad [0, 1, 0]$
- elliptic curve:
  $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad \rightsquigarrow \quad [0, 1, 0]$

$E/\mathbb{F}_q$ elliptic curve, $\infty := [0, 1, 0]$

Further Reading...

- Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, Advances in elliptic curve cryptography, London Mathematical Society Lecture Note Series, vol. 317, Cambridge University Press, Cambridge, 2005.
- J. W. S. Cassels, Lectures on elliptic curves, London Mathematical Society Student Texts, vol. 24, Cambridge University Press, Cambridge, 1991.
- John E. Cremona, Algorithms for modular elliptic curves, 2nd ed., Cambridge University Press, Cambridge, 1997.
- Anthony W. Knapp, Elliptic curves, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992.
- Neal Koblitz, Introduction to elliptic curves and modular forms, Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1984.
- Joseph H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
- Joseph H. Silverman and John Tate, Rational points on elliptic curves, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.
- Lawrence C. Washington, Elliptic curves: Number theory and cryptography, 2nd ED. Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2008.
- Horst G. Zimmer, Computational aspects of the theory of elliptic curves, Number theory and applications (Banff, AB, 1988) NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 279–324.