Wireless communication Security
無線通訊安全

Lecture II-2

May 7, 2009

洪國寶

Outline

- **Review**
- 橢圓曲線密碼技術
  - 基本代數概念
  - 橢圓曲線簡介
  - 基本橢圓曲線密碼協定
  - 橢圓曲線之其他性質與應用

Review of Lecture 1

- Algebraic structures
- Group
  - Additive group, Multiplicative group, cyclic group, subgroup, left/right coset, normal subgroup, quotient group
- Homomorphism
  - Isomorphism, epimorphism, endomorphism, automorphism, kernel
- Ring
  - Commutative ring, integral domain, characteristic, Frobenius endomorphism
- Field
  - Finite field, Modular arithmetic, modular inverse, Galois Fields GF(p)
- Diffie-Hellman Key Exchange, abstraction (generalization)

Diffie-Hellman Key Exchange

- all users agree on global parameters:
  - large prime integer p
  - α a primitive root mod p
- each user (eg. A) generates their key
  - chooses a secret key (number): $x_A < p$
  - compute their **public key**: $y_A = \alpha^{x_A} \bmod p$
- each user makes public that key y_A ■

Abstract (generalized) Diffie-Hellman Key Exchange

- General description of the Diffie-Hellman Key Exchange protocol:
  1. Alice and Bob agree on a finite cyclic group G and a generator g in G.
  2. Alice picks a random natural number a and sends g^a to Bob.
  3. Bob picks a random natural number b and sends g^b to Alice.
  4. Alice computes $(g^b)^a$.
  5. Bob computes $(g^a)^b$.
- Further generalization involves endomorphisms. ■

Galois Fields GF(p)

- GF(p) is the set of integers {0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field
  - since have **multiplicative inverses**
- hence arithmetic is "well-behaved" and can do addition, subtraction, multiplication, and division without leaving the field GF(p) ■

Finding Inverses

1. Construct a multiplicative table
2. **Use extended Euclid algorithm**
3. Apply Fermat's little theorem ■

Outline

Part II:

(d) 橢圓曲線密碼技術

- **基本代數概念 (continued)**
- **橢圓曲線簡介**
- 基本橢圓曲線密碼協定
- 橢圓曲線之其他性質與應用

(e) 無線感測網路安全

- 無線感測網路簡介
- 無線感測網路的安全議題
  - Key distribution/management
  - Secure routing

(f) 相關論文討論

Galois Fields

- We have shown how to construct GF(p)
- We will now show how to construct GF(p^n) for $n > 1$ ■

Polynomial arithmetic

- Virtually all encryption algorithms involve arithmetic operations on integers
- **If division is required then we need to work over a field**
- For convenience and for implementation efficiency, we work with integers in the range 0 through 2^n-1 (n-bit word)
- With 8 bit, Z_{256} is not a field,
  - the closest prime is 251
  - Z_{251} is a field (inefficient use of storage)
- How to construct field with 256 elements? (**How to construct GF(p^n) for n > 1 in general?**)
  - We need polynomial arithmetic ■

Polynomial arithmetic

- Let F be a field. If $a_m, a_{m-1}, \ldots, a_1, a_0 \in F$, then any expression of the form

$$a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0$$

is called a **polynomial over F** in the **indeterminate** x with coefficients $a_m, a_{m-1}, \ldots, a_0$. The set of all polynomials with coefficients in F is denoted by F[x].

- If n is the largest nonnegative integer such that $a_n \neq 0$, then we say that the polynomial

$$f(x) = a_n x^n + \cdots + a_0$$

has **degree** n, written deg(f(x)) = n, and a_n is called the **leading coefficient** of f(x). ■

Polynomial Arithmetic

- General form of polynomials

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

- Zeroth degree polynomials are called **constant polynomials**
- An nth degree polynomial is said to be a **monic polynomial** if $a_n = 1$
- several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coordinates mod p
  - poly arithmetic with coordinates mod p and polynomials mod M(x)
    ■

Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg
  - let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

  $f(x) + g(x) = x^3 + 2x^2 - x + 3$

  $f(x) - g(x) = x^3 + x + 1$

  $f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$ ■

Polynomial Arithmetic with Modulo Coefficients

- when computing value of each coefficient do calculation modulo some value
- could be modulo any prime p
- but we are most interested in **mod 2**
  - i.e. **all coefficients are 0 or 1** (i.e. over Z_2)
  - eg. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$f(x) + g(x) = x^3 + x + 1$

$f(x) \times g(x) = x^5 + x^2$ ■

Modular Polynomial Arithmetic

- [**Division Algorithm**] For any polynomials f(x) and g(x) in F[x], with $g(x) \neq 0$, there exist unique polynomials q(x), $r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$, where either $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.
- We can write any polynomial in the form:
  - $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- If have no remainder say $g(x)$ divides $f(x)$
- If $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- **arithmetic modulo an irreducible polynomial forms a field** ■

Galois Fields GF(p^n)

- Consider
  - polynomials with coefficients modulo p
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- They form a finite field.
- We can always find an inverse
  - can use extend Euclid's Inverse algorithm, or
  - **Calvez, Azou and Vilbé / Goupil and Palicot ■**

GF(2^n)

- Finite field GF(2^n)
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only) ■

$GF(2^n)$

- $GF(2^3)$

  $(\{000,001,010,011,100,101,110,111\}, +, \times)$

  – $(\{0, 1, 2, 3, 4, 5, 6, 7\}, +_{\text{mod } 8}, \times_{\text{mod } 8})$

    - Some non-zero elements have no multiplicative inverse
    - Does not form a finite field ■

Interpreted as binary integers

Modulo 8 Example

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

Modulo 8 Example (cont.)

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

(b) Multiplication modulo 8

Modulo 8 Example (cont.)

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

(c) Additive and multiplicative inverses modulo 8

$GF(2^n)$

Interpreted as coefficients of polynomials

- $GF(2^3)$

  $(\{000,001,010,011,100,101,110,111\}, +, \times)$

  – $(\{0, 1, x, x+1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}, +_{\text{mod } 2}, \times_{\text{mod } p(x)})$

    - $p(x) = x^3 + x + 1$
    - **Form a field**
    - **Table 4.6** (next slide) ■

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

Polynomial GCD

- A monic polynomial $d(x) \in F[x]$ is called the **greatest common divisor** of $f(x), g(x) \in F[x]$ if

  (i) $d(x) \mid f(x)$ and $d(x) \mid g(x)$, and

  (ii) if $h(x) \mid f(x)$ and $h(x) \mid g(x)$ for some $h(x) \in F[x]$, then $h(x) \mid d(x)$.

- The greatest common divisor of $f(x)$ and $g(x)$ is denoted by $\gcd(f(x),g(x))$.
  If $\gcd(f(x),g(x)) = 1$, then the polynomials $f(x)$ and $g(x)$ are said to be **relatively prime**. ■

Polynomial GCD

- can adapt Euclid's Algorithm to find it:

  EUCLID[$a(x)$, $b(x)$]

  1. A(x) = $a(x)$; B(x) = $b(x)$
  2. if B(x) = 0 **return** A(x) = gcd[$a(x)$, $b(x)$]
  3. R(x) = A(x) mod B(x)
  4. A(x) ← B(x)
  5. B(x) ← R(x)
  6. goto 2

Finding inverses (polynomials)

- For any nonzero polynomials $f(x), g(x) \in F[x]$ gcd(f(x),g(x)) exists and can be expressed as a linear combination of f(x) and g(x), in the form $\gcd(f(x),g(x)) = a(x)f(x) + b(x)g(x)$ for some $a(x),b(x) \in F[x]$.
- The polynomials a(x) and b(x) can be found just like extended Euclidean algorithm for integers. ■

Finding inverses (polynomials)

- **L.C. Calvez, S. Azou and P. Vilbé, Variation on Euclid's algorithm for polynomials, *Electron. Lett.* 33 (11) (1997), pp. 939–940.**
- **A. Goupil and J. Palicot, Variation on variation on Euclid's algorithm, IEEE Trans. Signal Process. Lett. 11 (5) (2004), pp. 457–458.**

Algorithm *(Euclidean Algorithm for Polynomials (EAP)).*
INPUT: Two polynomials $A(x)$ and $B(x)$ with degree a and b, respectively, where $a, b > 0$.
OUTPUT: $U(x)$, $V(x)$ and $G(x)$ such that $G(x) = \mathrm{GCD}(A(x), B(x)) = A(x)U(x) + B(x)V(x)$.

1. $R(x) \leftarrow x^{a+b}A(x) + x^a$; $R'(x) \leftarrow x^{a+b}B(x) + 1$;
2. **while** $\deg(R'(x)) > a + b$ **do**
3. $\quad T(x) \leftarrow R'(x)$; $R'(x) \leftarrow R(x) \bmod R'(x)$; $R(x) \leftarrow T(x)$;
4. Compute $U(x)$, $V(x)$ and $G(x)$ such that
   $\quad R(x) = x^{a+b}G(x) + x^aU(x) + V(x)$;
5. **return** $U(x)$, $V(x)$ and $G(x)$.

Computational Considerations

- If coefficients are 0 or 1 then we can represent any such polynomial as a bit string:
- addition becomes XOR of these bit strings
- multiplication is shift & XOR
  - cf long-hand multiplication
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also shift & XOR) ■

Example

- in GF(2^3) have (x^2+1) is 101_2 & (x^2+x+1) is 111_2
- so addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101 \text{ XOR } 111 = 010_2$
- and multiplication is
  - $(x+1).(x^2+1) = x.(x^2+1) + 1.(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011.101 = (101)\ll 1 \text{ XOR } (101)\ll 0 =$
    $1010 \text{ XOR } 101 = 1111_2$
- polynomial modulo reduction (get q(x) & r(x)) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1.(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111 \text{ XOR } 1011 = 0100_2$ ■

Using a Generator

- a **generator** g is an element whose powers generate all non-zero elements
  - in F have 0, g^0, g^1, …, g^{q-2}
- can create generator from **root** of the irreducible polynomial
- then implement multiplication by adding exponents of generator ■

More algebraic concepts

- Field extension
- Algebraic number fields
- Algebraic closure
- Galois group, Galois extension ■

Field extension

- It is possible to construct other examples of fields by means of extensions.
  - For example, given the field Q of rational numbers, we can augment the set Q with a particular number e that is not in Q, and this automatically implies that every rational function of e is also in the extended field.
- An important special case of a field extension is when the number e is algebraic, i.e., the root of a polynomial with coefficients in the base field. ■

Examples

- **C** is an **extension field** of **Q**.
- The set $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$ is an extension field of **Q.**

Field extension

- Let L be a field. If K is a subset of L which is also a field with respect to the field operations of addition and multiplication in L, then we say that **K is a subfield of L**, that **L is an extension field of K**, and that L /K, read as "L over K", is a field extension.
- Given a field extension L /K and a subset S of L, we denote by K(S) the smallest subfield of L which contains K and S.
  - We say K(S) is generated by the adjunction of elements of S to K.
  - If S consists of only one element s we often write K(s) instead of K({s}).
  - A field extension of the form L=K(s) is called a **simple extension** and s is called a **primitive element** of the extension. ■

Field extension

- Given a field extension L /K, then L can also be considered as a vector space over K.
  - The elements of L are the "vectors" and the elements of K are the "scalars".
  - We add the vectors just like we add elements in L, and scalar multiplication is multiplication of elements from L by elements from K.
  - The dimension of this vector space is called the degree of the extension, and is denoted by [L : K].
- Extensions of degree 2 and 3 are called **quadratic extensions** and **cubic extensions**, respectively. Depending on whether the degree is finite or infinite the extension is called a **finite extension** or **infinite extension**. ■

Examples

- The field of complex numbers C is an extension field of the field of real numbers R, and R in turn is an extension field of the field of rational numbers Q.
  - Clearly then, C/Q is also a field extension.
  - We have [C : R] = 2 because {1,i } is a basis, so the extension C/R is finite.
- If p is any prime number and n is a positive integer, we have a finite field GF(p^n) with p^n elements; this is an extension field of the finite field GF(p) = $\mathbf{Z}/p\mathbf{Z}$ with p elements. ■

Separable extension

- An algebraic field extension L/K is **separable** if it can be generated by adjoining to K a set each of whose elements is a root of a separable polynomial over K.
- A polynomial P(X) is **separable over a field K** if all of its irreducible factors have distinct roots in an algebraic closure of K - that is each irreducible factor of P(X) has distinct linear factors in some large enough field extension. ■

Normal extension

- An algebraic field extension L/K is said to be **normal** if L is the splitting field of a family of polynomials in K[X].
- The **splitting field** of a polynomial P(X) over a given field K is a field extension L of K, over which P factorizes into linear factors $X - a_i$, and such that the a_i generate L over K. ■

Algebraic number fields

- Finite extensions of Q are also called **algebraic number fields** and are important in number theory.
- An element x of the algebraic number field F is called an **algebraic integer** if it is a root of a monic polynomial with integer coefficients. ■

Algebraic closure

- A field F is said to be **algebraically closed** if every polynomial in one variable of degree at least 1, with coefficients in F, has a root in F.
- The field of rational numbers is not algebraically closed.
- Also, **no finite field F is algebraically closed**, because if $a_1, a_2, \ldots, a_n$ are the elements of F, then the polynomial $(x - a_1)(x - a_2) \cdots (x - a_n) + 1$ has no zero in F. ■

Algebraic closure

- An algebraic closure of a field K is an algebraic extension of K that is algebraically closed.
- The algebraic closure of a field *K* can be thought of as the largest algebraic extension of *K*. ■

Algebraic closure

The fundamental theorem of algebra states that

- The algebraic closure of the field of **real** numbers is the field of complex numbers.
- The algebraic closure of the field of **rational** numbers is the field of algebraic numbers.
- For a **finite field** of prime order p, the algebraic closure is a countably infinite field which contains a copy of the field of order p^n for each positive integer n (and is in fact the union of these copies). ■

Galois group

- A Galois group is a group associated with a certain type of field extension.
- Suppose that E is an extension of the field F Consider the set of all automorphisms of E/F. This set of automorphisms with the operation of function composition forms a group, sometimes denoted by Aut(E/F). ■

Galois extension

- An algebraic field extension E/F is Galois if it is normal and separable.
- If E/F is a Galois extension, then Aut(E/F) is called the Galois group of (the extension) E over F, and is usually denoted by Gal(E/F). ■

- Now we are ready for elliptic curves

Elliptic curve

Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field

Alfred Menezes & Scott Vanstone
Dept. of Combinatorics and Optimization, University of Waterloo
Waterloo, Ontario, Canada, N2L 3G1.

Tatsuaki Okamoto
NTT Laboratories
Take, Yokosuka-Shi, 238-03 Japan.

..\..\..\..\elliptic-curve\MOV.pdf

Elliptic Curve

- Elliptic Curve over K is the set of points (x,y), with x, y $\in$ K, which satisfy
  - $y^2 = x^3 + ax + b$, together with the point at infinity O, if characteristic of K > 3 and $4a^3 + 27b^2 \neq 0$
- If the characteristic of K is 2, than the elliptic curve is:
  - $y^2 + cy = x^3 + ax + b$ (1)
  - $y^2 + xy = x^3 + ax^2 + b$ (2)

Some Questions

- We usually need to specify that
  - The characteristic is not 2 or 3, and
  - $4a^3 + 27b^2 \neq 0$
  - Point at infinity O (or ∞)
  - If the characteristic of K is 2, than the elliptic curves have different forms.
- Why?
- What are j-invarant, n-torsion point, Weil pairing, and supersingular curves etc?

Notation

- K: field
- $\overline{\mathrm{K}}$: algebraic closure of K
- $GF(q)$ or F_q: finite field with q elements
  - typically, $q = p$ where p is prime, or 2^m
- $E(F_q)$: elliptic curve over F_q
- (x, y): point on $E(F_q)$
- $\boldsymbol{O}$: point at infinity

Weierstrass equation

- An elliptic curve E is the graph of the form $y^2 = x^3 + ax + b$ where a, b are constants
- We will need to specify what set a, b, x, and y belong to
- If K is a field with a, b \in K, then we say that E is **defined over** K
- If we want to consider points with coordinates in some field $L \supseteq K$, we write E(L). This set always contains the **point at infinity.**

Elliptic Curve

- In fact the elliptic curve is given by the generalized Weierstrass equation
  - $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
  - This is specialized with variable changes to the equations initially shown
- If the characteristic of K is not 2 then we can divide by 2 and complete the square
- If the characteristic of K is not 3 then we can further simplify (use blackboard)

Characteristic 3

- There are curves that are not of the form $y^2 = x^3 + ax + b$
- The general case for characteristic 3 is the form $y^2 = x^3 + Cx^2 + Ax + B$

Characteristic 2

- The curves of the form $y^2 = x^3 + ax + b$ are singular
- The equations for K of characteristic 2 come from:
  - Define $j(E) = (a_1)^{12}/\Delta$ then
    - if $j(E) \neq 0$ we get (2)
    - if $j(E) = 0$ we get (1)

j-invariant

- Define $j(E) = (a_1)^{12}/\Delta$

Discriminant

- In algebra, the discriminant of a polynomial is a certain expression in the coefficients of the polynomial which is equal to zero if and only if the polynomial has a multiple root.
- A nonsingular point in F(x,y) = 0 is a point in which one of the partial derivatives (over x or y) is non-zero
- The equation on the elliptic curve $x^3 + ax + b$ will not have multiple root if F(x,y) has only nonsingular points.
  - Using $\Delta = -16(4a^3 + 27b^2)$, F(x,y) will have only nonsingular points if $\Delta \neq 0$
- Singular point must be excluded.

Projective space

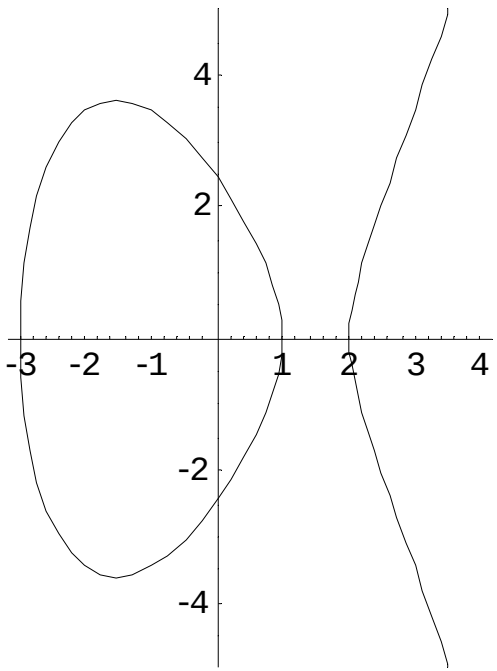
- Point of infinity

Supersingular curves

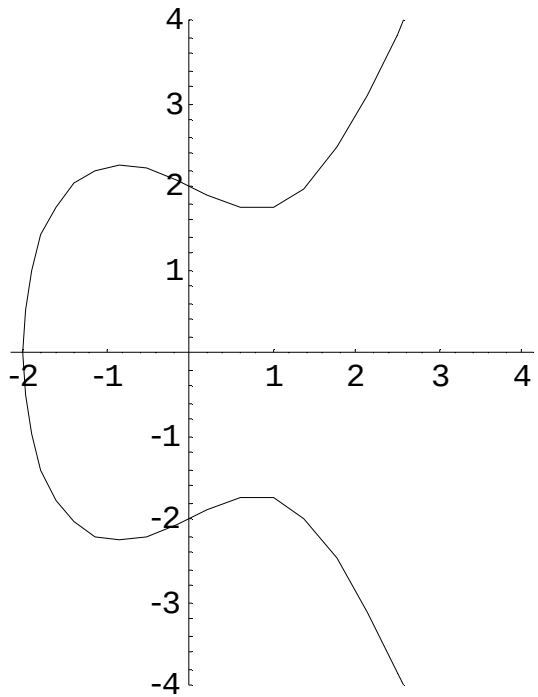
- An elliptic curve in characteristic p is called supersingular if E[p] = {O}.
- In other words, there are no points of oder p, even with coordinates in an algebraically closed field.
- An attractive feature of supersingular curves is that computations involving an integer times a point can sometimes be done faster than might be expected.

Examples of Elliptic Curves

- $y^2 = x^3-7x+6$



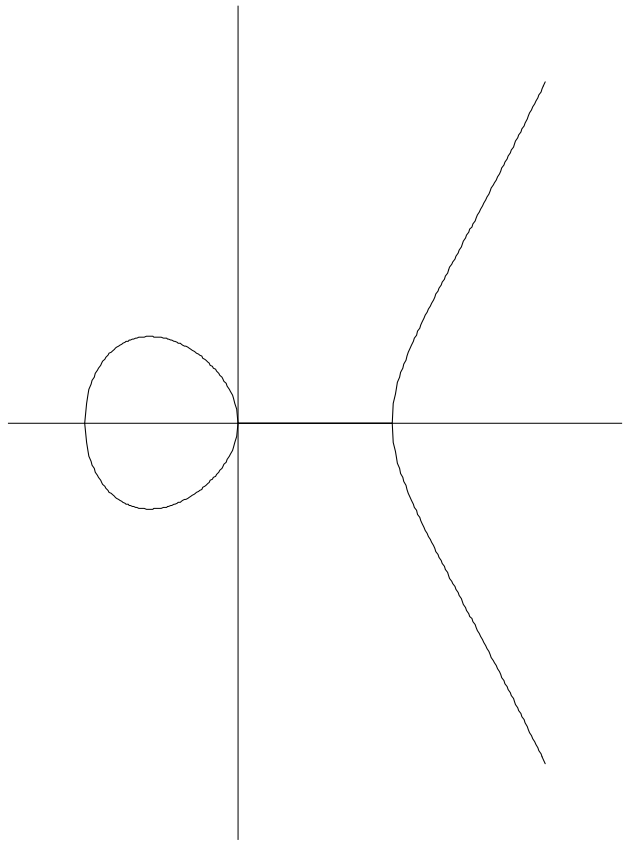
- $y^2 = x^3-2x+4$



Examples of Elliptic Curves

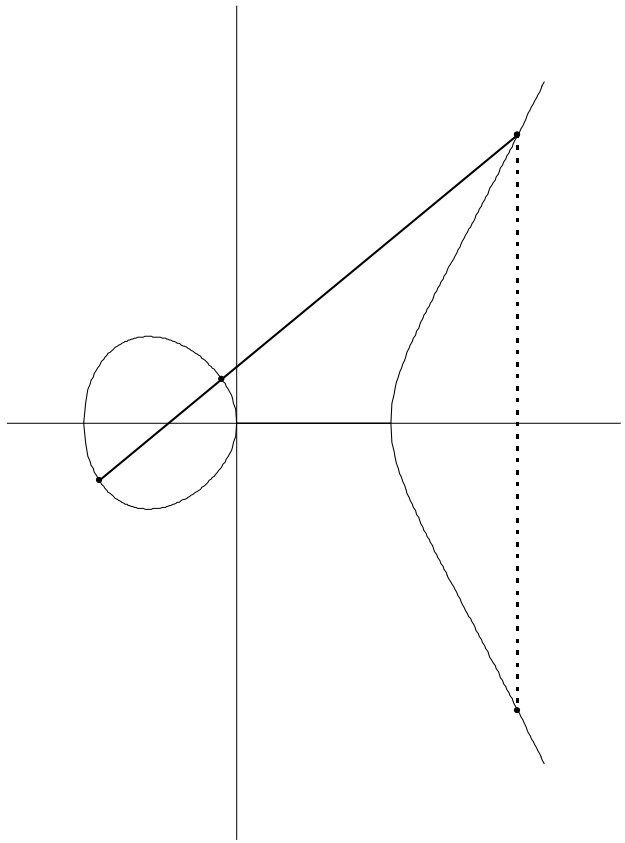
- Over the reals, the solutions form a curve with one or two components
- Example:

$$y^2 = x^3 - x$$



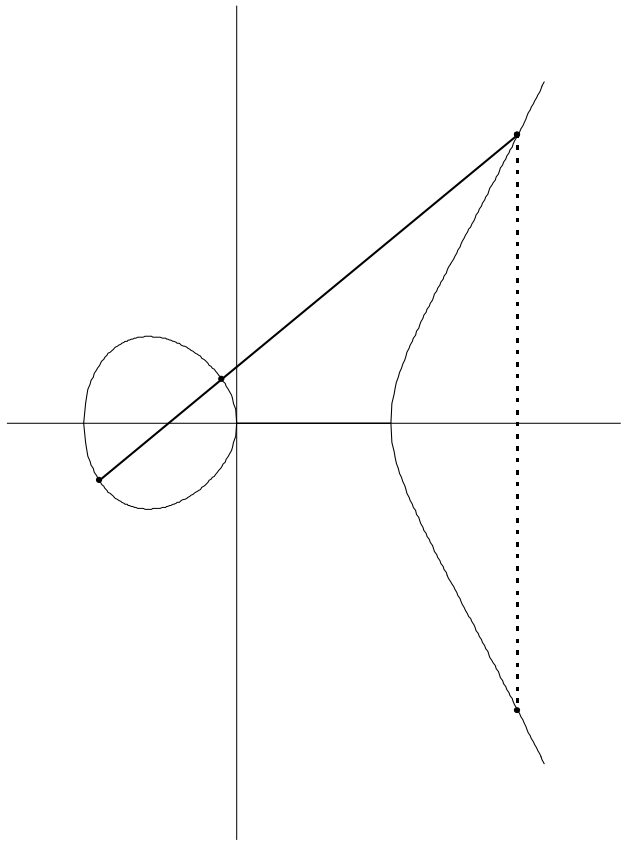
Elliptic Curve Arithmetic

- A group law may be defined where the sum of two points is the reflection across the *x*-axis of the third point on the same line
- "Chords and tangents"



Group Law Axioms

- Closure
- Identity:
  $P + \boldsymbol{O} = \boldsymbol{O} + P = P$
- Inverse:
  $(x, y) + (x, -y) = \boldsymbol{O}$
- Associativity
- Commutativity



Addition Formulae

- Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be non-inverses
- Then $P_1 + P_2 = (x_3, y_3)$ where

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda (x_1 - x_3) - y_1$$

and λ is the slope of the line:

  - $\lambda = (3x_1^2+a)/2y_1$ if $x_1 = x_2$
  - $\lambda = (y_2-y_1)/(x_2-x_1)$ otherwise

Addition Formulae

- Now we can show the formulas for adding points.
  - Assume $P = (x_1, y_1)$ and $Q = (x_2, y_2)$
- If the characteristic of K is > 3 than
  - $-P = (x_1, -y_1)$
  - $P + Q = (\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$
    - $\lambda = (y_2 - y_1)/(x_2 - x_1)$, if $P \neq Q$
      $= (3 x_1^2 + a)/2y_1$, if $P = Q$

Addition Formulae

- If the characteristic of K is 2, than
  - If $j(E) \neq 0$:
    - $-P = (x_1, y_1 + x_1)$
    - $P+Q = (x_3, y_3)$

    $x_3 = ((y_1+y_2)/(x_1+x_2))^2 + (y_1+y_2)/(x_1+x_2) + x_1+x_2 + a, \; P \neq Q$

    $= x_1^2 + b/ x_1^2, \; P = Q$

    $y_3 = ((y_1+y_2)/(x_1+x_2))(x_1+x_3) + x_3 + y_1, \; P \neq Q$

    $= x_1^2 + (x_1 + y_1/x_1)x_3 + x_3, \; P = Q$

Addition Formulae

- If the characteristic of K is 2, than
  - If j(E) = 0:
    - $-P = (x_1, y_1 + c)$
    - $P+Q = (x_3, y_3)$

    $x_3 = ((y_1+y_2)/(x_1+x_2))^2 + x_1+x_2,\ P \neq Q$

    $= (x_1^4 + a^2)/ c^2,\ P = Q$

    $y_3 = ((y_1+y_2)/(x_1+x_2))(x_1+x_3) + c + y_1,\ P \neq Q$

    $= ((x_1^2 + a)/c)(x_1+x_3) + c + y_1,\ P = Q$

Elliptic Curves over Finite Fields

- An elliptic curve may be defined over any finite field GF(q)
- For GF(2^m), the curve has a different form:

$$y^2 + xy = x^3 + ax^2 + b$$

  where $b \neq 0$
- Addition formulae are similar to those over the reals

Elliptic Curves over Finite Fields

Elliptic curve of finite field F_q:

- The number of points is given by
  - $q + 1 + \sum\chi(x^3 + ax + b)$, χ is the quadratic character of F_q
- Hasses's Theorem:
  - $| N - (q+1)| \leq 2\sqrt{q}$
- The abelian group over F_q does not need to be cyclic, but it can be decomposed on cyclic groups

Elliptic Curves over Finite Fields

- Let #E(F_q) denote the number of points on an elliptic curve $E(F_q)$, including $\boldsymbol{O}$
- Hasse bound: #E(F_q) = q+1-t, where

$$|t| \leq 2\sqrt{q}$$

- The group of points is either cyclic or a product of two cyclic groups

Example

- $y^2 = x^3 + 1$ / GF(5)

z	0	1	2	3	4
z^2	0	1	4	4	1

x	1	2	3	4	5
y	± 1	?	± 2	?	0

$E(\mathbf{F}_5) = \{\infty, (0, \pm 1), (2, \pm 2), (4, 0)\}$. Hence $\#E(\mathbf{F}_5) = 6$.

Scalar Multiplication

- *Scalar multiplication* is repeated group addition:

$$cP = P + \cdots + P \quad (c \text{ times})$$

  where c is an integer

- For all $P \in E(F_q)$,

$$nP = \boldsymbol{O}$$

  where $n = \#E(F_q)$

Analogy with Multiplicative Groups

Elliptic Curve Group	**Multiplicative Group**
point addition	multiplication
scalar multiplication	exponentiation
elliptic curve discrete logarithm	discrete logarithm