CIS 5371 Cryptography

5. Algebraic foundations

Groups

Group $(G,*)$

A set G with a binary operation "$*$" for which we have

- Closure
- Associativity
- An identity
- Each element has an inverse

Groups

Examples

- $(Z,+)$, $(Z_p^*, \cdot)$, $(Z_n^*, \cdot)$ are all groups

Here:

- $Z_n = \{0,1,2, \ldots , n\text{-}1\}$,
- $Z_p^* = \{1,2, \ldots , p\text{-}1\}$, for prime p,
- $Z_n^* = \{\text{all integers } k,\ 0 < k < n, \text{ with } gcd(k,n)=1\}$.

So: $Z_{15}^* = \{1,2,,4,7,8,11,13,14\}$.

We have, $|Z_n^*| = \phi(n)$

Lagrange's theorem

Lagrange's theorem

- *If H is a subgroup of G then:* $|H|$ *is a factor of* $|G|$
- *If G is a finite group and* $a \in G$ *then* $ord(a)$ *is a factor of* $|G|$.

Examples

$(\{1,2,4\},\cdot)$ is a subgroup of Z_7^*

The order of 2 in Z_7^* is 3: $2^3 \equiv 8 \equiv 1 \pmod{7}$

Cyclic groups

A group is *cyclic* if it has an element whose order is the same as the cardinality of the group.

Any such element is called a *generator* of the group.

Examples

Z_7^* is a cyclic group with generator 3.

In fact, it can be shown that any group Z_p^*, with p prime is cyclic.

Rings

Ring $(R,+,*)$

- Under addition R is a commutative group with identity 0
- Under multiplication we have:

  Closure, associativity, an identity $1 \neq 0$, commutativity and distributivity

Examples

$Z(+, *)$ and $Z_n(+,*)$

Finite Fields

Field $(F, +, *)$

F is a ring in which all non-zero elements have an inverse with respect to "$*$"

Examples

$Z_p(+, *)$, p a prime

Groups on the elliptic curve

An modular elliptic curve is defined by an equation of the form

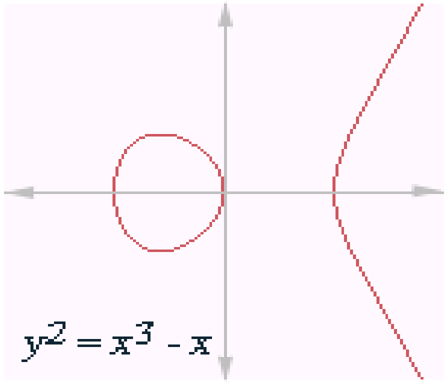
$$E: y^2 = x^3 + ax + b \pmod{p}$$

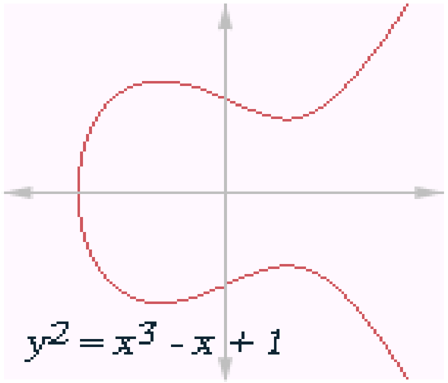
where a,b are constants in F_p satisfying

$$\Delta \text{ (descriminant)} = 4a^3 + 27b^2 \neq 0 \pmod{p}$$

We take p a prime greater than 3. To have the points on E to be a group we add an extra point at infinity:

$$O=(x,\infty).$$





Groups on the elliptic curve

The group law

See wikipedia diagrams.

http://en.wikipedia.org/wiki/Elliptic_curves

Groups on the elliptic curve

Elliptic Curve Discrete Logarithm problem

Point addition:

Let $P,Q \in E$, let ℓ be the line containing them (or the tangent if $P=Q$), and R the third point of intersection of with E.

Let ℓ' be the line connecting R and O. Then $P+Q$ is the point such that ℓ' intersects E at R, O and $P+Q$.

If P is a point: $nP = P + P + \cdots + P$ (n times)

The ECDL problem:

Given (P, nP) find n.

(In the EC group addition corresponds to multiplication in the field group).

Groups on the elliptic curve

Elliptic Curve Discrete Logarithm problem

- In general the cost of finding the order of an arbitrary point in a group is proportional to the order of the group.
- The best known algorithm give us O($\sqrt{q}$), where q is the order of the field. This exponential in q.
- In the case of the discrete logarithm problem there are algorithmic methods that sub-exponential in q.
- So if we take $q \approx 2^{160}$ we get difficulty 2^{80} in brute force attacks.
- To get similar protection in a finite field we need $q \approx 2^{1000}$