# Finite Fields and AES

Nicolas T. Courtois
- University College of London

# Rings

# Rings

“When two operations work together nicely” like + and *.

(R,+,*,0,1) is a Ring if:

- $0 \neq 1$ (avoids a “trivial” ring {0},+,*)
- R,+ is an Abelian group
- R\{0}, * is a monoid with identity element 1.
- * distributes over +:

$$a(b+c)=ab+ac$$

$$(b+c)a=ba+ca$$

# Fields

# Fields

- $R\backslash\{0\}, *$ is a monoid with identity element 1.

BECOMES

- $R\backslash\{0\}, *$ is a group with identity element 1.

Added requirement: each element $a\neq0$ has an inverse.

Corollary: When $p$ is prime, $Z_p$ is a field.

# Example 2.B.

({1,2,3}, + mod 4, * mod 4) is a ring.

It is NOT a field.

Why ?

# Example 2.B.

({1,2,3}, + mod 4, * mod 4) is a ring.

It is NOT a field.

Why ?

Proof: 2 has no inverse.

# Example 3

Let K[X] be the set of all polynomials in one variable X. K[X] is a ring.

Let P(X) be a polynomial of degree n.

Exactly as we reduce integers modulo p, we can reduce all polynomials modulo P(X).

Fact: Residue classes modulo P(X) also form a ring.

We call it K[X] / P(X).

Representative elements: all polynomials in K[X] of degree up to n-1.

# Example 3

Example: $K=Z_3$. Let $P(X)=X^3+1$.

$(X+1) * (2X^2 +X) = ?$

# Question:

At which moment the residue classes modulo $P(X)$ give a field ?

For what polynomials, $Z_n[X] / P(X)$ is a field ?

Theorem: If and only $K=Z_p$, $p$ prime and $P(X)$ is an irreducible polynomial.

Irreducible == has no proper divisor of lower degree.

Proof: DIY, the same as before. Irreducible is the equivalent of prime numbers.

Note: $p$ is called the characteristic of this field.
$x+x+\ldots$ p times $= 0$.

# Finite Fields

# Theorem:

ALL FINITE FIELDS are of the form $Z_p[X] / P(X)$, with $p$ prime.

Corollary: the number of elements of a finite field is always $q=p^n$:

They are represented by all polynomials

$$a_0 + a_1 X^1 + \ldots + a_{n-1} X^{n-1}.$$

corresponds to all possible n-tuples

$$(a_0, a_1, \ldots, a_{n-1}).$$

# Moreover

ALL FINITE FIELDS are of the form $Z_p[X] / P(X)$, with $p$ prime. There isn’t any more.

There is only “one” field that has $q=p^n$ elements: means that all finite fields that have $q$ elements are isomorphic (and therefore have exactly the same properties).

# Theorem:

The multiplicative group of a finite field F is cyclic.

Means that there is a single element g, called primitive element, such that every element of the field F\{0} is a power of g.

We call P(X) primitive polynomial (must be irreducible) such that X is a primitive element in $Z_p[X] / P(X) \setminus \{0\}$.

In other words, every element of $Z_p[X]$ is equal to a power of X modulo P(X).

# Corollary:

In $Z_p$ we had $a^p = a$ [Fermat's Little Thm.]

In any finite field $F$ that has $q$ elements

$a^q = a$.

This is called the equation of a finite field.