Basic Algebra and Number Theory

Nicolas T. Courtois
- University College of London

Integers

Number Theory

Not more than 30 years ago mathematicians used to say “Number Theory” will be probably last branch of mathematics that will ever find any practical application. Nevertheless large nations have invested considerable amounts of money into the development of it. The (research) money spend on proving the Last Fermat’s Theorem can be compared to the money spend on going to the moon.

Today each of you has a bank card AND does use secure TSL-like web connection every day.The security of these is based largely on number theory. The NSA is known to employ more mathematicians that any other company in the world. They don’t publish many papers.

Basic number theory (like we do here, related to RSA encryption) is easy and fun.

It is becoming worse: with elliptic curves, the potential number of people that understand the mathematics behind shrinks to a few dozen of elite academics worldwide.

Integers

Natural Integers - IN: [0],1,2,3…

Relative Integers - ZZ. -2,-1,0,1,2,3…

Prime number: has no “proper” divisor,

(means except 1 and itself.)

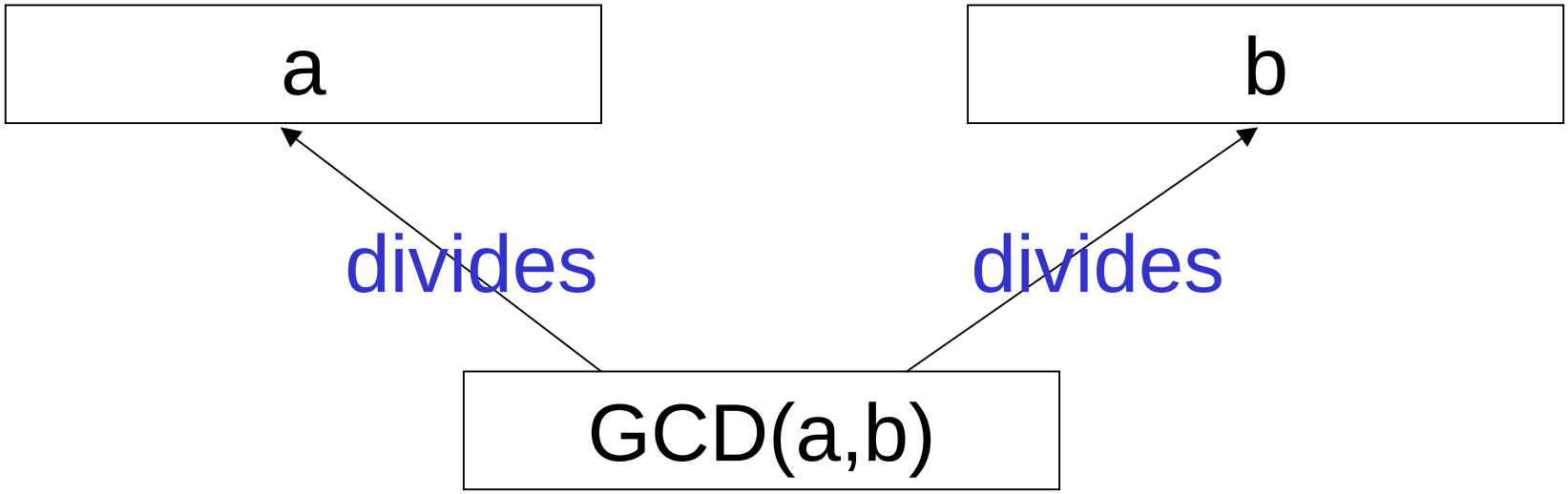
Thm. There is an infinite number of prime numbers.

Easy fact: Each number decomposes in prime factors.

Hard thing: to compute factors of a given number. Currently feasible up to some 600 bits.

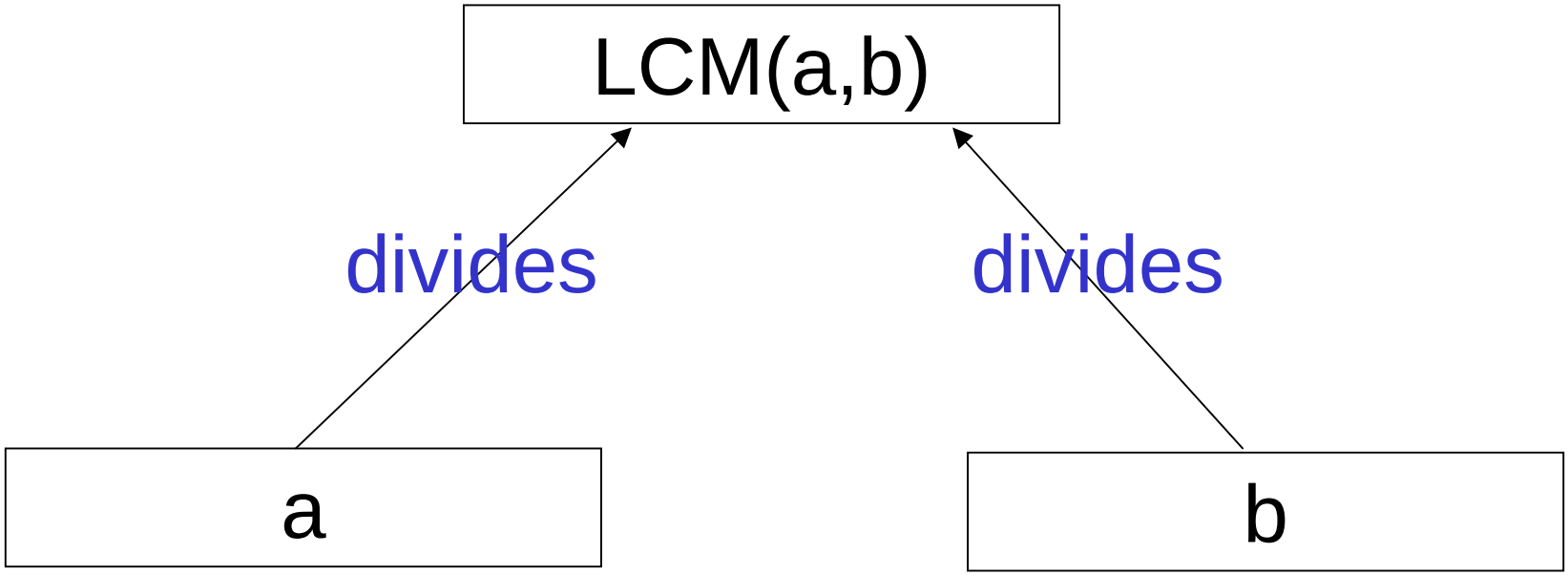
Greatest Common Divisor

the biggest such that



Least Common Multiple

the smallest such that



Bezout Theorem

1=GCD(a,b)

if and only if

∃ x and y such that

ax+by=1.

Proof:

<= easy

=> Let d be the smallest positive integer such that ax+by=d. We look at the sequence 0,d,2d,3d etc… d must divide a and the same for b. So GCD is equal at least d. Thus d=1.

Well-founded Orders

In this proof we used the following fact: for any subset $A \subseteq \mathbb{N}$, there exists the first (the smallest) element a in this set.

Doesn't work for real numbers…

Specialists say that $<$ in $\mathbb{N}$ is a well-founded order.

Bezout Theorem - Corollary

$d=GCD(a,b)$

Then $\exists$ x and y such that

$ax+by=d$.

Proof: Easy, put d as a factor…

Relatively Prime Numbers

1=GCD(a,b)

Theorem:

If d | a and d | b,
then d | GCD(a,b).

Proof:

By Bezout Corollary, GCD(a,b)=ax+by.

Essential Lemma [Euclid/Gauss]

If p is prime, and $p \mid ab$, then

Either $p \mid a$ or $p \mid b$.

Proof:

By Bezout. Either $p \mid a$ or $GCD(p,a)=1$.

Then $ax+py=1$ and $abx+pyb=b$.

Thus $p \mid b$.

Corollary ["Fundamental Theorem of Arithmetic"]

Every integer has a unique decomposition in prime factors.

$$n = p_1^{a\_1} * p_2^{a\_2} * \ldots * p_k^{a\_k}$$

with $p_1 < p_2 < \ldots$.

Proof 1: use the previous result.

Specialists's explanation:

ZZ is an Euclidian ring,
which implies it is
a unique factorisation domain.

Groups

Evariste Galois

Very famous French mathematician.

- At age of 14 started reading very serious books papers about algebra and mathematics.
- For reasons that are not fully explained failed all his exams to enter Ecole Polytechnique and most of his brilliant work was published and recognised only later.
- Did completely solve the problem of solvability of polynomial equations in one variable: “Galois Theory”.
- Was a political activist, against the king of France, frequently arrested and writing math papers while in prison.
- Died at the age of 20 after a fatal duel with an artillery officer, to some in the context of a broken love affair, to some stage-managed by the royalist fractions and the police.

He was the first to use the word Group.

Group - Definition

0. closure

A set M with an operation

•: MxM-> M such that:

1) Operation • is associative } semi-group
2) Has an identity element 1.

   $1 \bullet a = a \bullet 1 = a$

3) Each element a has an inverse called a^{-1}.

   $a^{-1} \bullet a = a \bullet a^{-1} = 1$

monoid

group

Pre-Cryptographic Interpretation of Groups and Monoids

One interpretation is as follows:

- Each element = transformation on the "message space" = a set M.
- Neutral element: transformation that does nothing.
- Inverse: decrypt a "scrambled" message. Don't call it encryption (would imply that this is actually somewhat "secure"…
- Group: we always have an inverse: every message can be decrypted.
  - (though in crypto we can relax/work around this requirement a lot…)

Question:

Is everything OK here?

Q1. How many multiplicative inverses has 2 modulo 2011?

Q2. How many multiplicative inverses has 2 modulo 2009?

Basic Results:

Thm:

In every Monoid,
the neutral element is unique.

Thm.

More generally, in every Monoid,
the inverse of an element (if exists) is unique.

Proof: easy.

A “CS-style” Example of a Monoid

A language L with concatenation of words.

When this will be a monoid?

Remark:

No element is invertible,

except the neutral element ε.

A “maths-style” example of a Monoid:

$(Z_m , * \bmod m)$ is a monoid.

Solution to Q2

2 is invertible mod 2009.

And the inverse is unique from the previous Theorem.

Group – additive convention

-operation is called

+

-the identity element is called 0.

-the inverse is called -a.

Abelian == Commutative Groups

$$a+b = b+a$$

Modular Addition - Congruencies

DEFINITION:

We say that $a \equiv b \bmod n$

if n divides $a-b$.

Congruencies - Properties

Equivalence Relation:

1. Reflexive: $a \equiv a$
2. Symmetric $a \equiv b$ if and only if $b \equiv a$
3. Transitive $a \equiv b$ and $b \equiv c$ implies $a \equiv c$.

Every equivalence relations partitions the set into equivalence classes.

Every congruence mod n partitions ZZ into classes == residues mod n usually represented by numbers {0,1,2,..,n-1}.

Congruencies - Properties

The set of residue classes modulo n is called
Z_n or ZZ / nZZ.

Elements of Z_n of are denoted {0,1,2,..,n-1}.
(This is possible because {0,1,2,..,n-1} is a complete set of representative elements.)

Fact:

Usual integer operations (+,*) and special elements (0,1) translate to the world of residue classes.

Example: if $a \equiv b \bmod n$ and $c \equiv d \bmod n$
THEN $a*c \equiv b*d \bmod n$.

Congruencies - Properties

Exercise:

What is the last decimal of 2^{2008} ?

Congruencies - Properties

Exercise:

What is the last decimal of 2^{2008} ?

Hint 1: what about computing 2^{2008} in Z_{10} ?

Modular Addition - Congruencies

$a \equiv b \bmod n$

Frequently we simply write

$a = b \bmod n$.

This "equality" is a real equality

in we think in terms of residues mod n and addition modulo n in the set of residues:

$\{0,1,2,\ldots,n-1\}$.

Group – Example 1

Let n>=2.

{0,1,2,…,n-1},+ mod n is a group.

The group of residue classes mod n
represented by {0,1,2,..,n-1}.

Group – Example 1.A.

{0,1},+ mod 2 is a group.

Proof:

-modular addition is always associative.

-identity element: a+0=0+a=a.

-we have -a = a here !

Group – Example 1.B.

{0,1,2},+ mod 3 is a group.

BTW: here -a=2a as we have: a+2a=0 mod 3.

Group ?

Fact:

{1,2,..,n-1},* mod n is a group IF AND ONLY IF n is a prime.

We call Z_n^* the set {1,2,..,n-1}.

Group – Example 2.A.

{1,2}, * mod 3 is a group.

Proof:

-associative.

-identity element $1*a=a*1=a \bmod 3$.

-inverse: $1^{-1}=1$, $2^{-1}=2$

- check that $2*2=4 \bmod 3 = 1$.

(Actually this group is the same (ISOMORPHIC) to {0,1},+.)

Order of a Group, Subgroups

We call order of G or ord(G) the number of elements in the group (its cardinality).

A sub-group: any subset closed under * that is a group for the same *.

Theorem [Lagrange]: Order of a subgroup $H \subseteq G$ divides the order of the group G.

Proof: All left cosets $x*H$ are of the same cardinality and they partition G.

Order of an Element

Order of an element g: $ord(g)$ =

- Cardinal of the sub-group generated by g: $g^1, g^2, g^3, \ldots g^{ord(g)-1}, 1$.
- It is also the smallest integer such that $g^{ord(g)}=1$.

Theorem: Order of an element divides the order of the group.

Proof: by Lagrange Theorem.

Fermat's Little Theorem

Pierre de Fermat [1601-1655]:

French lawyer and government official,
one of the fathers of number theory
(also involved in breaking enemy ciphers and codes).

Theorem: Let p be a prime.

For any integer $a^p = a \bmod p$.

Corollary: If $a \neq 0 \bmod p$, then $a^{p-1} = 1 \bmod p$.

Fermat's Little Thm. – Proof No 1.

Show that $a^p = a \bmod p$?

- Let $a \neq 0 \bmod p$.
- The set $\{0a, 1a, \ldots, (p-1)a\}$ mod p contains each element $\{0,1,2,\ldots,p-1\}$ exactly once.
- Remove 0 and multiply all these mod p:

$$a^{p-1}(p-1)! = (p-1)! \bmod p$$

- So that $p \mid (p-1)! \times (a^{p-1}-1)$.
- Since p is prime, must divide $(a^{p-1}-1)$ and thus also $p \mid (a^p - a)$.
- Works also when $a = 0 \bmod p$.

Fermat's Little Thm. – Proof No 2.

Z_p^*, * mod p is a group.

Finite group => each element has a finite order.

$a^{ord(a)} = 1$

The order of any element must divide the order of the group: $p - 1 = ord(a) * c$

Then $a^{p-1} = (a^{ord(a)})^c = 1^c = 1$.

Example 2.B.

{1,2,3}, * mod 4 is NOT a group.

Proof: 2 has no inverse.

Let $2a = 1 \bmod 4$.

We reduce the equation mod 2.

Can we ? YES: $4 \mid 2a-1$ then $2 \mid 2a-1$.

Thus $0 = 1 \bmod 2$.

Group ?

{1,2,..,n-1}, * mod n is a group IF AND ONLY IF n is a prime.

Proof:

=> If it is a group and p | n with p<n then p*a=1 mod n and thus 0=1 mod p, impossible.

<= If n=p be a prime, we put $a^{-1}=a^{p-2}$. This is an inverse of a by Fermat's Little Theorem.

Rings

Rings

"When two operations work together nicely" like + and *.

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

- $0 \neq 1$ (not serious, avoids one "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\{0}, * is a monoid with identity element 1.

BECOMES

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

Added requirement: each element $a \neq 0$ has an inverse.

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

Example 2.B.

({0,1,2,3}, + mod 4, * mod 4) is a ring.

It is NOT a field.

Why ?

Example 2.B.

({0,1,2,3}, + mod 4, * mod 4) is a ring.

It is NOT a field.

Why ?

Proof: 2 has no inverse.

Fields vs. Rings

- In a field we have all the 4 arithmetic operations +,-,*,/.
- In a ring we do not have /.

Obvious consequence:

- In a field a linear (affine) equation ax+b=0 has exactly 1 solution.
- False in a ring: Example: equation 2x=0 mod 6. has 2 solutions 0 and 3.
- Fact: ax=b mod n has 0 or GCD(a,n) solutions.

Fields vs. Rings

- In a field a linear (affine) equation $ax+b=0$ has exactly 1 solution.

Key Theorem:

more generally, in a field, a polynomial of degree k has AT MOST k roots.

Proof sketch: By induction of the degree. if a is a root, rewrite as a polynomial in $(X-a)$. Divide by $(X-a)$.

Fields vs. Rings – Root Theorem - Remarks

Root Theorem:

In a field, a polynomial of degree k has AT MOST k roots.

- Can have less.

[[why not exactly k ?
True in an “algebraically closed” field (will be infinite).]]

- False in a ring. And false already for degree 1, example is the same as before…

****Fields vs. Rings

Another important fact:

- In a field, every function is a polynomial. Allows to “Algebrize” anything…
- False in a ring…

Example 3

Let K be a field.

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

Let P(X) be a monic 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.

Polynomial Rings - Example 3

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

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

Show that P(X) is not irreducible.

Hint: find a root of it.

Polynomial Rings - Example 4

Example: $K=Z_3$. Let $P(X)=X^3+2X+1$.

Exercise:

Show that P(X) is irreducible.

Hint:

When a polynomial has no roots, IT DOES NOT IMPLY IT IS IRREDUCIBLE (!!!!).

However, one can show that for polynomial of degree 3 it does.

*Solving Equations in Rings

also appears in CNT_I0 part

Exercise[s]:

*How many multiplicative inverses has 2 modulo 2011?

*How many multiplicative inverses has 2 modulo 2009?

How many multiplicative inverses has 7 modulo 2009?

Solving Linear/Affine Equations mod n.

Only a ring, except when p prime.

Multiplicative structure: only a monoid, not a group.

ax+b=0 mod n

Solutions ? Theorem:

- If GCD(a,n)=1 then there is a exactly one solution modulo n. (a^-1 Can be found by E.Eu.A.)
- If GCD(a,n)=d > 1 then there is a solution IF AND ONLY IF d | b, and the congruence is equivalent to a congruence modulo n/d.
  - All solutions are congruent modulo n/d. There are exactly d solutions mod n.

Z_n^*

We call Z_n^* the set of the invertible elements mod n.

Theorem: it is a group under *.

When n is a prime, $Z_n^* = Z_n \backslash \{0\}$.

Otherwise it is even smaller set,
other elements are excluded.

How many?

Euler Totient φ Function

Swiss mathematician [1707-1783], 10 Swiss franks bills,
have published some 600 very clever papers.
Nobody has ever done that much…

Question 1: How many elements of Z_n are invertible ?

Question 2: Size of Z_n^* ?

Question 3: How many integers between 0 and n-1
are relatively prime with n ?

Answer: the same question.

Definition: this number is called φ(n).

Euler Totient φ Function

How many elements of Z_n are invertible ? $\varphi(n)$.

Examples:

$\varphi(1) = 1$. WHAT ??? By definition, it is so. Technically speaking $1|0$ (as any integer does) so $GCD(0,1)=1$ so 0 and 1 are relatively prime.

$\varphi(2) = 1$. WHAT ? 1 but not 0 anymore. $GCD(1,2)=1$ and $GCD(0,2)=2$.

$\varphi(3) = 2$. 1 and 2.

$\varphi(4) = 2$. 1 and 3.

$\varphi(6) = ?$.

Euler Totient φ Function

How many elements of Z_n are invertible ?

$\varphi(n)$.

- $\varphi(p) = p-1$. For ANY prime (even if $p=2$).

Proof: we did it. Z_p is a field.

- Prime powers:

$\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.

Proof: Count those that are NOT prime to p^a.

- Multiplicative property: later.

Chinese Remainder Theorem [very old]

Suppose we have several pairwise relatively prime moduli $n_1, n_2, \ldots, n_r$. How many solutions has the following system of equations with 1 variable x ?

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$
$$\ldots$$
$$x \equiv a_r \bmod n_r$$

Many but in a sense only ONE.

CRT Theorem:

All solutions are congruent mod $n_1 * n_2 * \ldots * n_r$.

Proof: Uniqueness and existence. DIY.

Chinese Remainder Theorem – Version 2.

[again, assume pairwise relatively prime]

The application:

product ring: component-wise + and x

$C: Z_{n1*n2*\ldots*nr} \rightarrow Z_{n1} \times Z_{n2*} \times \ldots \times Z_{nr}$

defined by:

$C(x) = (x \bmod n_1, x \bmod n_2, \ldots, x \bmod n_r)$

is a ring ISOMORPHISM

(bijective + preserves addition and multiplication)

CRT - Corollary

The Euler Totient $\varphi(n)$ is multiplicative.

More precisely,

$\varphi(m*n) = \varphi(m)\ \varphi(n)$ whenever $GCD(m,n)=1$.

Corollary:

And if $n = p_1^{a\_1} * \ldots p_r^{a\_r}$ with DISTINCT primes [as any integer is uniquely decomposed] then:

$\varphi(n) = \Pi\ p_i^{a\_i-1}(p_i-1)$.

Fermat's Little Theorem

Pierre de Fermat [1601-1655]:

French lawyer and government official,
one of the fathers of number theory
(also involved in breaking enemy ciphers and codes).

Theorem: p = prime.

Let $GCD(a,p)=1$.

Then $a^{p-1} \equiv 1 \bmod p$.

Re-formulation in Z_p:

for each $a \in Z_p^*$ we have $a^{\varphi(p)} = 1$.

Not accidentally, replaced by $\varphi(p) = |Z_p^*|$.

Euler-Fermat Theorem

Theorem: GCD(a,n)=1

$a^{\varphi(n)} \equiv 1 \bmod n$.

Re-formulation in Z_n:

for each $a \in Z_n^*$ we have $a^{\varphi(n)} = 1$.

Proof: by induction on prime factorisation of n.

Base step: $\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$.

This is proven in turn by induction on a.

Hint: raise a ^ $(p^{r-1}-p^{r-2})$ to the p-th power.

Lemma: $(1+x)^p = 1+x^p \bmod xp$.

(direct proof or multivariate linear in Zp).

Finite Fields

Question:

K=GF(p)=Zp, p prime.

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

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

Theorem: If and only if 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+… p times = 0.

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.
(in most cases false for Z_n^* in general)

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

Fact: g^j is a generator if and only if GCD(j,q-1)=1. There are exactly $\varphi(q-1)$ generators in GF(q).

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.

Why ?

The Equation of a Finite Field

Let L be a field and $K \subseteq L$ be another field.

It is called a sub-field of L when:

- [obvious] if is closed under + and *.
- It is a field.

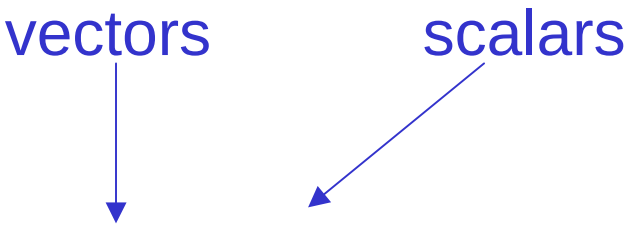
Assume that K has q elements.

Fact: The set of elements of L such that $a^q = a$. is exactly K.

Proof: Cannot have more roots, degree q.

Vector Spaces

Vector Space



An algebraic system

(V,+,x, F+,*) where:

- (F+,*) is a field
- (V,+) is an abelian group (additive notation)
- x is the ‘scaling’ by a scalar operation with:
  - closure
  - 1 x V =V
  - associative
  - distributive

Vector Space – key example

The

"vector space
of N-tuples":

F^N.

Interesting Mapping (general case):

"large" finite field ⟷ vector space over a "small" field

$GF(q^n)$ ⟷ $GF(q)^n$

or the set of all possible polynomials of the form

$a_0 + a_1 X^1 + \ldots + a_{n-1} X^{n-1}$ in $Z_q[X] / P(X)$,

⟷

or the set of all possible n-tuples

$(a_0, a_1, \ldots, a_{n-1})$ with $a_1 \in GF(q)$

Bijective and Additive

(Linear over GF(q), NOT linear over $GF(q^n)$)

Finite Fields and AES

See AES Spec

Publicly available on the Internet
(or buy the AES Book).