# Selected Topics in Finite Fields

David Thomson
dthomson@math.carleton.ca

Carleton University

September 8, 2013

# How this will work

1. How this class came to be.

# How this will work

1. How this class came to be.
2. Expectations and goals.

# How this will work

1. How this class came to be.
2. Expectations and goals.
3. Syllabus.

# How this will work

1. How this class came to be.
2. Expectations and goals.
3. Syllabus.
4. The project.

# How this will work

1. How this class came to be.
2. Expectations and goals.
3. Syllabus.
4. The project.
   `http://cms.math.ca/Events/winter13/students`

# How this will work

1. How this class came to be.
2. Expectations and goals.
3. Syllabus.
4. The project.
   `http://cms.math.ca/Events/winter13/students`
5. Reschedule November 26, December 3.
   `http://www.ricam.oeaw.ac.at/specsem/specsem2013/`

# How this will work

1. How this class came to be.
2. Expectations and goals.
3. Syllabus.
4. The project.
   `http://cms.math.ca/Events/winter13/students`
5. Reschedule November 26, December 3.
   `http://www.ricam.oeaw.ac.at/specsem/specsem2013/`
6. Reviewing some factoids about finite fields.
7. Bird's eye view of cryptography.
8. Computational complexity (blackboard).

# Review about finite fields

Recall. A field $(\mathbb{F}, +, *)$ is an Abelian group under $+$, and the non-zero elements of $\mathbb{F}$ form an Abelian group under $*$.

The characteristic of a field is the smallest positive number $n$ such that the sum $1 + 1 + \cdots + 1 = 0$ ($n$ times). If no such number exists, the characteristic is defined to be 0.

Proposition. If a field has positive characteristic $n$, then $n$ is prime.

# Review about finite fields

Recall. A field $(\mathbb{F}, +, *)$ is an Abelian group under $+$, and the non-zero elements of $\mathbb{F}$ form an Abelian group under $*$.

The characteristic of a field is the smallest positive number $n$ such that the sum $1 + 1 + \cdots + 1 = 0$ ($n$ times). If no such number exists, the characteristic is defined to be 0.

Proposition. If a field has positive characteristic $n$, then $n$ is prime.
Proof. Suppose $n = pq$, where $1 < p \leq q$. Then $n = 1 + 1 + \cdots + 1 = (1 + 1 + \cdots + 1)_p(1 + 1 + \cdots + 1)_q = 0$, where the subscript indicates the number of sums. Thus $p = 0$ or $q = 0$, contradicting that $n$ is minimal.

Proposition. A finite field has non-zero characteristic.

# Review about finite fields

Recall. A field $(\mathbb{F}, +, *)$ is an Abelian group under $+$, and the non-zero elements of $\mathbb{F}$ form an Abelian group under $*$.

The characteristic of a field is the smallest positive number $n$ such that the sum $1 + 1 + \cdots + 1 = 0$ ($n$ times). If no such number exists, the characteristic is defined to be 0.

Proposition. If a field has positive characteristic $n$, then $n$ is prime.
Proof. Suppose $n = pq$, where $1 < p \leq q$. Then $n = 1 + 1 + \cdots + 1 = (1 + 1 + \cdots + 1)_p(1 + 1 + \cdots + 1)_q = 0$, where the subscript indicates the number of sums. Thus $p = 0$ or $q = 0$, contradicting that $n$ is minimal.

Proposition. A finite field has non-zero characteristic.
Proof. A finite field has a characteristic, since $1, 1 + 1, 1 + 1 + 1, \cdots$ must repeat (Pigeon hole). If the characteristic is equal to 0, then $1 + 1 + 1 + \cdots$ never repeats. So a finite field has prime characteristic.

# Building finite fields

Definition. The prime subfield of a finite field is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Theorem. Let $q$ be a power of a prime $p$. There is a unique finite field with $q^n$ elements (up to isomorphism), denoted $\mathbb{F}_{q^n}$. Moreover, $\mathbb{F}_{q^n}$ is a vector space over $\mathbb{F}_q$.

Theorem. The most common way of building a finite field is with a polynomial basis. Let $\mathbb{F}_q$ be a finite field and let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree $n$. Then,

$$\mathbb{F}_{q^n} \cong \mathbb{F}_q[x]/(f) \cong \mathbb{F}_q(\alpha),$$

where $\alpha$ is a root of $f$ (in some algebraic closure of $\mathbb{F}$).

Therefore $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

# An example

Let $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$. If $f$ is reducible, then it must have a root, but $f(0) = f(1) = 2$ and $f(2) = 1$, so $f$ is irreducible.

Any element of $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2 + 2x + 2)$ can be written as $a + b\alpha$, where $a, b \in \mathbb{F}_3$ and $\alpha$ is a root of $f$ in some extension.

Addition is performed term-wise, and multiplication is performed modulo $f$. For example

$$(x + 2)(2x + 1) = 2x^2 + 5x + 2 =$$

# An example

Let $f(x) = x^2 + 2x + 2 \in \mathbb{F}_3[x]$. If $f$ is reducible, then it must have a root, but $f(0) = f(1) = 2$ and $f(2) = 1$, so $f$ is irreducible.

Any element of $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2 + 2x + 2)$ can be written as $a + b\alpha$, where $a, b \in \mathbb{F}_3$ and $\alpha$ is a root of $f$ in some extension.

Addition is performed term-wise, and multiplication is performed modulo $f$. For example

$$(x + 2)(2x + 1) = 2x^2 + 5x + 2 = 2(x + 1) + 2x + 2 = x + 1.$$