Graduate Study in algebra and combinatorics at Tohoku University

Akihiro Munemasa

Graduate School of Information Sciences
Tohoku University

November 5, 2018
Institut Teknologi Bandung

Prime Numbers

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

- for abstract algebra, these are the source of finite prime fields, finite (abelian) simple groups.
- for combinatorics, these are the source of constructing some combinatorial objects, such as graphs, designs, codes.
- for number theorists, not individual prime numbers, but the set of all prime numbers, is of the primary interest.

Abstract algebra

The only prime fields, that is, a field which contains no proper subfield, are:

$$\mathbb{Q}, \quad \mathbb{F}_p = \mathrm{GF}(p) \quad (p : \text{ prime}),$$

where

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{[0], [1], \ldots, [p-1]\},$$

$$\begin{aligned}[a] &= \{mp + a \mid m \in \mathbb{Z}\} \\ &= \{n \in \mathbb{Z} \mid n \equiv a \pmod{p}\}.\end{aligned}$$

Fields

Definition

A field is a set K equipped with addition $+$ and multiplication, such that

- K is an abelian group with respect to addition,
- $K \setminus \{0\}$ is an abelian group with respect to multiplication, where 0 denotes the identity of K as an abelian group with respect to addition,
- distributive law holds:

$$a(b+c) = ab + ac \quad (a, b, c \in K).$$

Fields

Definition

A field is a set K equipped with addition $+$ and multiplication, such that

- K is an abelian group with respect to addition,
- $K \setminus \{0\}$ is an abelian group with respect to multiplication, where 0 denotes the identity of K as an abelian group with respect to addition,
- distributive law holds:

$$a(b+c) = ab + ac \quad (a, b, c \in K).$$

Exercise: Give a reason why $K = \mathbb{F}_p$ is a field, especially describe how to find the multiplicative inverse of $[a] \in \mathbb{F}_p \setminus \{[0]\}$ (what is $[3]^{-1}$ in $\mathbb{F}_7$?).

Polynomials

For a field K, the univariate polynomial ring with indeterminate x is denoted by $K[x]$. It consists of all polynomials in x with coefficients in K:

$$K[x] = \{\sum_{i=0}^{n} a_i x^i \mid n \in \mathbb{Z}_{\geq 0},\ a_0, \ldots, a_n \in K\}.$$

Here x is not considered to be an element of K, rather, it is a formal symbol. However, we allow the operation "substitution $x = b$," where $b \in K$:

$$\text{for } f(x) = \sum_{i=0}^{n} a_i x^i \in K[x], \quad f(b) = \sum_{i=0}^{n} a_i b^i \in K.$$

If $a_n \neq 0$, then n is called the degree of $f(x)$ and is denoted by $\deg f$.

Factorization of polynomials

Let K be a field, and let $K[x]$ be the univariate polynomial ring with indeterminate x. Exercise: Prove the following:

Lemma

If $f(x), g(x) \in K[x] \setminus \{0\}$, then $\deg(fg) = \deg f + \deg g$.

Lemma

If $f(x) \in K[x]$, $b \in K$ and $f(b) = 0$, then there exists $g(x) \in K[x]$ such that $f(x) = (x - b)g(x)$.

Lemma

If $f(x) \in K[x] \setminus \{0\}$, then

$$|\{b \in K \mid f(b) = 0\}| \leq \deg f.$$

Finite fields

If K is a finite field with q elements, then $K^\times = K \setminus \{0\}$ is an abelian group of order $q - 1$. This is known to be cyclic. We illustrate the proof by means of example.

Finite fields

If K is a finite field with q elements, then $K^\times = K \setminus \{0\}$ is an abelian group of order $q - 1$. This is known to be cyclic. We illustrate the proof by means of example.

The order of an element $a \in K^\times$ is the smallest positive integer n such that $a^n = 1$ holds. It follows from finite group theory that the order of an element is a divisor of $q - 1$.

Finite fields

If K is a finite field with q elements, then $K^\times = K \setminus \{0\}$ is an abelian group of order $q-1$. This is known to be cyclic. We illustrate the proof by means of example.

The order of an element $a \in K^\times$ is the smallest positive integer n such that $a^n = 1$ holds. It follows from finite group theory that the order of an element is a divisor of $q-1$.

For $K = \mathbb{F}_7$, divisors of $q-1=6$ are $1,2,3,6$. Elements of order $1,2,3$ should be roots of x^1-1, $(x^2-1)/(x-1) = x+1$, and $(x^3-1)/(x-1) = x^2+x+1$, respectively, so there are (at most) $1,1,2$ such elements. The remaining $6-(1+1+2)=2$ elements must have order 6.

Exercise: Give a proof for an arbitrary odd prime p.

Primitive elements

If K is a finite field with q elements, then $K^\times$ is a cyclic group of order $q-1$.

A generator, that is, an element of order $q-1$, of this cyclic group is called a primitive element of K.

Primitive elements

If K is a finite field with q elements, then $K^\times$ is a cyclic group of order $q-1$.

A generator, that is, an element of order $q-1$, of this cyclic group is called a primitive element of K.

For $K = \mathbb{F}_7$, 2 is not a primitive element: $2^3 = 1$, while 3 is a primitive element: $3^2 \neq 1$, $3^3 \neq 1$.

Artin's conjecture: there are infinitely many primes p for which 2 is a primitive element.

Quadratic residues

Fix an odd prime p, and let $K = \mathbb{F}_p$. Let α be a primitive element of K, so that

$$K^\times = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-2}\}.$$

The set of quadratic residues Q and that of quadratic nonresidues and N are defined as

$$Q = \{1, \alpha^2, \alpha^4, \ldots, \alpha^{p-3}\},$$
$$N = \{\alpha, \alpha^3, \ldots, \alpha^{p-2}\}.$$

The quadratic residue character χ of K is

$$\chi(a) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a \in Q, \\ -1 & \text{if } a \in N. \end{cases}$$

Abstract algebra

Fields: other than prime fields $\mathbb{Q}$, $\mathbb{F}_p$. A quadratic extension $\mathbb{F}_3[i]$, $i^2 = -1$, and a transcendental extension $K(x)$, the field of all rational functions in a formal variable x with coefficients in a field K.

Groups: The only finite groups which possess no nontrivial subgroups are cyclic groups of prime order. Finite groups which possess no nontrivial normal subgroups are called simple, and they are classified after huge amount of effort.

Rings: noncommutative rings are closely related to representation theory (of groups). Typical examples of commutative rings are multivariate polynomial rings.

Abstract algebra

Fields: other than prime fields $\mathbb{Q}$, $\mathbb{F}_p$. A quadratic extension $\mathbb{F}_3[i]$, $i^2 = -1$, and a transcendental extension $K(x)$, the field of all rational functions in a formal variable x with coefficients in a field K.

Groups: The only finite groups which possess no nontrivial subgroups are cyclic groups of prime order. Finite groups which possess no nontrivial normal subgroups are called simple, and they are classified after huge amount of effort.

Rings: noncommutative rings are closely related to representation theory (of groups). Typical examples of commutative rings are multivariate polynomial rings.

Abstract algebra

Fields: other than prime fields $\mathbb{Q}$, $\mathbb{F}_p$. A quadratic extension $\mathbb{F}_3[i]$, $i^2 = -1$, and a transcendental extension $K(x)$, the field of all rational functions in a formal variable x with coefficients in a field K.

Groups: The only finite groups which possess no nontrivial subgroups are cyclic groups of prime order. Finite groups which possess no nontrivial normal subgroups are called simple, and they are classified after huge amount of effort.

Rings: noncommutative rings are closely related to representation theory (of groups). Typical examples of commutative rings are multivariate polynomial rings.

Abstract algebra

Fields: other than prime fields $\mathbb{Q}$, $\mathbb{F}_p$. A quadratic extension $\mathbb{F}_3[i]$, $i^2 = -1$, and a transcendental extension $K(x)$, the field of all rational functions in a formal variable x with coefficients in a field K.

Groups: The only finite groups which possess no nontrivial subgroups are cyclic groups of prime order. Finite groups which possess no nontrivial normal subgroups are called simple, and they are classified after huge amount of effort.

Rings: noncommutative rings are closely related to representation theory (of groups). Typical examples of commutative rings are multivariate polynomial rings.

Applied, or not so abstract, algebra

Fields: algorithmic aspects in finite fields. Extensions of $K(x)$ of finite degree are called algebraic function fields, and it has applications to algebraic geometry and codes.

Finite groups: permutation groups, or more generally group action on combinatorial objects. Isomorphisms and automorphisms of graphs.

Representation theory: combinatorial representation theory, symmetric groups.

Gröbner bases for ideals in multivariate polynomial rings.

Applied, or not so abstract, algebra

Fields: algorithmic aspects in finite fields. Extensions of $K(x)$ of finite degree are called algebraic function fields, and it has applications to algebraic geometry and codes.

Finite groups: permutation groups, or more generally group action on combinatorial objects. Isomorphisms and automorphisms of graphs.

Representation theory: combinatorial representation theory, symmetric groups.

Gröbner bases for ideals in multivariate polynomial rings.

Group action on combinatorial objects

A combinatorial object E is a subset of X^n where X is a finite set and n is a positive integer.

A graph is a subset E of X^2 satisfying

$$(x, y) \in E \implies x \neq y \text{ and } (y, x) \in E.$$

Group action on combinatorial objects

A combinatorial object E is a subset of X^n where X is a finite set and n is a positive integer.

A graph is a subset E of X^2 satisfying

$$(x, y) \in E \implies x \neq y \text{ and } (y, x) \in E.$$

A hypergraph can be defined by replacing 2 by some integer $k \geq 2$.

Group action on combinatorial objects

A combinatorial object E is a subset of X^n where X is a finite set and n is a positive integer.

A graph is a subset E of X^2 satisfying

$$(x, y) \in E \implies x \neq y \text{ and } (y, x) \in E.$$

A hypergraph can be defined by replacing 2 by some integer $k \geq 2$.

The automorphism group of a combinatorial object E is the subgroup of the symmetric group on X whose induced action on X^n preserves E.

A circulant graph

Let $X = \mathbb{F}_p$, where p is a prime with $p \equiv 1 \pmod 4$. Then $-1 \in Q$ (quadratic residue), so $Q = -Q$. This implies

$$E = \{(x, y) \mid x, y \in X,\ x - y \in Q\}$$

defines a graph, that is,

$$(x, y) \in E \implies x \neq y \text{ and } (y, x) \in E.$$

The additive group X preserves E:

$$z \in X,\ (x, y) \in E \implies (x + z, y + z) \in E.$$

For example, $p = 5$, $Q = \{1, -1\}$, E consists of the set of edges of a pentagon.

A conference graph

Let $X = \mathbb{F}_p$, where p is a prime with $p \equiv 1 \pmod 4$. Consider the graph G with vertex set X, and edge set

$$E = \{(x, y) \mid x, y \in X,\ x - y \in Q\}.$$

Then for $x, y \in X$,

$$\#\{\text{common neighbors of } x, y\} = \begin{cases} \frac{p-1}{2} & \text{if } x = y, \\ \frac{p-5}{4} & \text{if } (x, y) \in E, \\ \frac{p-1}{4} & \text{otherwise.} \end{cases}$$

A graph on p (not necessarily prime) vertices satisfying the above condition is called a conference graph.
It is unknown whether a conference graph on 65 vertices exists.

An incidence structure

Let $X = \mathbb{F}_p$, where p is a prime. Recall that, if $p \equiv 1 \pmod 4$, then $-1 \in Q$, so $-Q = Q$.

Now assume $p \equiv -1 \pmod 4$, then $-1 \notin Q$. In this case

$$-Q = N \text{ (quadratic nonresidue)}.$$

Exercise: Prove this.

(For $p = 7$, $Q = \{1, 2, 4\}$, $-Q = N = \{3, 5, 6\}$).

Let

$$\mathcal{B} = \{Q + a \mid a \in \mathbb{F}_p\}.$$

Then for any distinct $x, y \in K$,

$$|\{B \in \mathcal{B} \mid x, y \in B\}| = \frac{p-3}{4}.$$

Exercise: Prove this.

A symmetric $(4m-1, 2m-1, m-1)$ design

Let $X = \mathbb{F}_p$, where p is a prime of the form $p = 4m-1$, where $m \in \mathbb{Z}$. Let

$$\mathcal{B} = \{Q + a \mid a \in \mathbb{F}_p\}.$$

Then for any distinct $x, y \in K$,

$$|\{B \in \mathcal{B} \mid x, y \in B\}| = \frac{p-3}{4} = m-1.$$

A family $\mathcal{B}$ of $(2m-1)$-element subsets of an $(4m-1)$-element set is called a symmetric $(4m-1, 2m-1, m-1)$ design if the above condition is satisfied.
The existence is unknown for $m = 47$ ($p = 187$ is not a prime).

A skew Hadamard matrix

Let $X = \mathbb{F}_p$, where p is a prime with $p \equiv -1 \pmod 4$. Let C be the matrix whose rows and columns are indexed by X, and whose entries are defined by

$$C_{xy} = \chi(x - y) \quad (x, y \in X),$$

where χ denotes the quadratic residue character. Define a $(p+1) \times (p+1)$ matrix

$$H = \begin{bmatrix} 1 & 1 \cdots 1 \\ -1 & \\ \vdots & C + I \\ -1 & \end{bmatrix}$$

Then

$$HH^\top = (p+1)I.$$

A Hadamard matrix

A square matrix H of order n is called a Hadamard matrix if all of its entries are ± 1, and

$$HH^\top = nI.$$

For example,

$$\begin{bmatrix} 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

If H is a Hadamard matrix of order n, then $n = 1, 2$ or n is divisible by 4.

It is unknown whether a Hadamard matrix of order 668 exists ($p = 667$ is not a prime).

Summary

Prime numbers can be used to construct graphs, designs and Hadamard matrices.

A straightforward method using prime numbers are not sufficient to produce all possible combinatorial objects.

Summary

Prime numbers can be used to construct graphs, designs and Hadamard matrices.

A straightforward method using prime numbers are not sufficient to produce all possible combinatorial objects.

Similar situations arise in spectral graph theory, algebraic coding theory.

Related areas: extremal set theory (Turán graphs), enumerative combinatorics (Catalan numbers).