Analytic and Combinatorial Number Theory 2026

Martin Klazar

February 23, 2026

(lecture notes for the course in summer term 2026)

Contents

Introduction **ii**

1 Combinatorial applications of finite fields **1**
1.1 Finite fields 1
1.2 Sidon sets 4
1.3 The Chevalley–Warning theorem 4
1.4 The bound of Balogh, Füredi and Roy 4

2 Counting solutions of congruences **5**

References **6**

Introduction

These lecture notes

Notation.

Chapter 1

Combinatorial applications of finite fields

1.1 Finite fields

Recall that a field is an algebraic structure

$$F = \langle F,\, 0_F,\, 1_F,\, +,\, \cdot \rangle$$

such that $\langle F, 0_F, + \rangle$ and $\langle F \setminus \{0_F\}, 1_F, \cdot \rangle$ are Abelian groups, and that the multiplication $\cdot$ is distributive over the addition $+$. We write F^* for $F \setminus \{0_F\}$ and call the latter group $\langle F^*, 1_F, \cdot \rangle$ the *multiplicative group of* F. Examples of fields are $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers) and $\mathbb{C}$ (complex numbers). In this chapter, we are interested in finite fields, and we will eventually describe them all. Basic examples of such fields are provided by the next proposition.

Proposition 1.1 *Let p be a prime number. The algebraic structure*

$$\mathbb{Z}_p = \langle \{0,\, 1,\, \ldots,\, p-1\},\, 0,\, 1,\, +,\, \cdot \rangle\,,$$

where in the base set we add and multiply integers modulo p, is a field.

Proof. We take for granted that the structure of integers $\langle \mathbb{Z}, 0, 1, +, \cdot \rangle$ is a commutative ring with 1. It is easy to see that this is preserved in the arithmetic modulo p, and $\mathbb{Z}_p$ is a unital commutative ring as well. It remains to prove the existence of multiplicative inverses. Let $a \in \mathbb{Z}_p^*$. Then the map $f(x) = ax$ (multiplication modulo p) goes from $\mathbb{Z}_p^*$ to $\mathbb{Z}_p^*$ and is injective:

$$ax = ay \iff ax \equiv ay \iff a(x-y) \equiv 0 \iff x \equiv y \iff x = y \pmod{p}\,.$$

Since $\mathbb{Z}_p^*$ is a finite set, the map f is also surjective and $b := f^{-1}(1)$ is the multiplicative inverse of a. □

$\mathbb{Z}_p$ will also denote the base set $\{0, 1, \ldots, p-1\}$.

Let F be a field and $n \in \mathbb{N}_0$. We define the element

$$n_F = \underbrace{1_F + 1_F + \cdots + 1_F}_{n \text{ summands}} \ (\in F)\,.$$

For $n = 0$ we have, of course, $n_F = 0_F$. For $n \in \mathbb{Z}$ with $n < 0$ we define $n_F = -(-n)_F$. The map $n \mapsto n_F$ is a ring homomorphism from $\mathbb{Z}$ to F. If $n_F \neq 0_F$ for every $n \in \mathbb{N}$, we say that the field F has *characteristic* 0. Else, if $m \in \mathbb{N}$ is the minimum number such that $m_F = 0_F$, we say that the field F has *characteristic* m. The fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ have characteristic 0, and $\mathbb{Z}_p$ has characteristic p. I leave the proof of the next proposition to you as an exercise.

Proposition 1.2 *Let F be a finite field. Then F has characteristic p for some prime number p and for every $m, n \in \mathbb{Z}$,*

$$m_F = n_F \iff m \equiv n \pmod{p}\,.$$

Proposition 1.3 *Let F be a finite field with characteristic p. Then the field $\mathbb{Z}_p$ is isomorphic to a subfield of F.*

Proof. Indeed, $\mathbb{Z}_p \ni n \mapsto n_F \in F$ is such isomorphism. □

If F has characteristic p, we view $\mathbb{Z}_p$ simply as a subfield of F.

In the next proposition, linear algebra shows its power.

Proposition 1.4 *Let F be a finite field with characteristic p. Then $|F| = p^r$ for some number $r \in \mathbb{N}$.*

Proof. Since $\mathbb{Z}_p$ is a subfield of F, the field F is in fact a (finite) vector space over the field $\mathbb{Z}_p$. Let $B = \{b_1, \ldots, b_r\} \subset F$ with $|B| = r$ $(\in \mathbb{N})$ be one of its bases. We have the map $f\colon F \to (\mathbb{Z}_p)^r$, $f(a) = \langle c_1, \ldots, c_r \rangle$, given by

$$a = c_1 b_1 + \cdots + c_r b_r\,.$$

Since B is a basis, f is a bijection and $|F| = |\mathbb{Z}_p|^r = p^r$. □

We establish the basic result that the multiplicative group of every finite field is cyclic. A group is cyclic if it is generated by a single element, so called generator. For the proof we need a simple identity satisfied by Euler's *totient function* $\varphi\colon \mathbb{N} \to \mathbb{N}$. It is given by ($[n] = \{1, 2, \ldots, n\}$)

$$\varphi(n) = |\{m \in [n]\colon\ (m,\, n) = 1\}|\,.$$

The notation $(m, n) = 1$ means that m and n are coprime; no prime divides both m and n. For example, $\varphi(p) = p - 1$ and $\varphi(6) = 2$. Let $n = p_1^{a_1} \ldots p_k^{a_k}$ be the prime factorization of n $(\in \mathbb{N})$. The formula

$$\varphi(n) = n \cdot \textstyle\prod_{i=1}^{k} \left(1 - p_i^{-1}\right)$$

is well known.

Lemma 1.5 *Let $n \in \mathbb{N}$. Then*

$$\sum_{d \,|\, n} \varphi(d) = n\,.$$

Proof. For a divisor d of n, let $X_d = \{m \in [n]\colon\ \gcd(m,n) = d\}$. Then

$$X_d = \{dk\colon\ k \in [n/d] \wedge (k, n/d) = 1\}\,.$$

Since $\{X_d\colon\ d \,|\, n\}$ is a partition of $[n]$, we have

$$n = |[n]| = \sum_{d \,|\, n} |X_d| = \sum_{d \,|\, n} \varphi(n/d) = \sum_{d \,|\, n} \varphi(d)\,.$$

□

Theorem 1.6 *Let F with $|F| = p^r$ be a finite field. The multiplicative group $F^* = \langle F^*, 1_F, \cdot\rangle$ of F is cyclic and has exactly $\varphi(p^r - 1)$ generators.*

Proof. Recall that the order $\mathrm{ord}(a)$ ($\in \mathbb{N}$) of an element $a \in F^*$ in the group F^* is the minimum $n \in \mathbb{N}$ such that $a^n = 1_F$. As we know, $\mathrm{ord}(a)$ is a divisor of $|F^*| = p^r - 1$. We claim that, more generally, for every divisor $d \,|\, (p^r - 1)$ there are exactly $\varphi(d)$ elements $a \in F^*$ with $\mathrm{ord}(a) = d$; for $d = p^r - 1$ we get the stated result.

To prove the claim, we define for $d \,|\, (p^r - 1)$ the sets

$$R_d = \{a \in F^*\colon\ \mathrm{ord}(a) = d\} \ \text{ and } \ X_d = \{a \in F^*\colon\ a^d - 1_F = 0_F\}\,.$$

Suppose that $R_d \neq \emptyset$ and take any element $a \in R_d$. Then $X = \{a, a^2, \ldots, a^d\}$ has $|X| = d$ elements because $\mathrm{ord}(a) = d$. Clearly, $X \subset X_d$. The well known bound on the number of zeros of a polynomial over a field implies that $X = X_d$. However, it is also clear that $R_d \subset X_d$, and therefore $R_d \subset X$. For $i \in [d]$ we have $\mathrm{ord}(a^i) = d$ iff $(i, d) = 1$. Thus $|R_d| = \varphi(d)$.

We proved that for every divisor $d \,|\, (p^r - 1)$ either $R_d = \emptyset$ or $|R_d| = \varphi(d)$. Since $\{R_d\colon\ d \,|\, (p^r - 1)\}$ is a partition of F^* and $|F^*| = p^r - 1$, Lemma 1.5 proves the claim. □

Next we show that every finite field is determined, up to an isomorphism, by its number of elements. For the proof, we need some properties of polynomials over fields. Let $G \subset F$ be an extension of fields and let $a \in F$. We say that the element a is algebraic over G if $f(a) = 0_F$ for some nonzero polynomial $f(x)$ in $G[x]$. The minimal polynomial of a is then the (unique) monic $f(x) \in G[x]$ such that $f(a) = 0_F$. It is not hard to show that minimal polynomials are irreducible and that if $f(x) \in G[x]$ is a minimal polynomial of $a \in F$ and $g(x) \in G[x]$ is a polynomial such that $g(a) = 0_F$, then $f(x)$ divides $g(x)$.

Theorem 1.7 *Let F and G be finite fields such that $|F| = |G|$. Then F and G are isomorphic.*

Proof. Let $|F| = |G| = p^r = q$ and $\sigma \in F^*$ be a generator of the multiplicative group of F. First, we show that the set $\{\sigma^0, \sigma^1, \ldots, \sigma^{r-1}\}$ is a basis of F as a vector space over $\mathbb{Z}_p$. Let $i \in [r]$ be the minimum number such that the set of vectors

$$X = \{\sigma^0, \sigma^1, \ldots, \sigma^{i-1}\}$$

is linearly independent over $\mathbb{Z}_p$, but that $X \cup \{\sigma^i\}$ is linearly dependent. □

1.2 Sidon sets

$X \subset \mathbb{Z}$ (X may be finite or infinite) is a *Sidon set* if for every $d \in \mathbb{N}$ the equation $x - y = d$ has at most one solution $x, y \in X$. These sets are named after the Hungarian mathematician *Simon Sidon (Szidon) (1892–1941)* [5], not after the Czech–Jewish writer and rabbi *Karol Sidon (1942)* [2, 4].

1.3 The Chevalley–Warning theorem

1.4 The bound of Balogh, Füredi and Roy

Chapter 2

Counting solutions of congruences

Bibliography

[1] J. Balogh, Z. Füredi and S. Roy, An upper bound on the size of Sidon sets, *Amer. Math. Monthly* **130** (2023), 437–445

[2] Karol Sidon, Wikipedia article, `https://en.wikipedia.org/wiki/Karol_Sidon`

[3] S. Lang, *Algebra*, Springer, New York 2002

[4] K. Sidon, *Sen o mém otci. Sen o mně*, Akropolis, Praha 2016

[5] Simon Sidon, Wikipedia article, `https://en.wikipedia.org/wiki/Simon_Sidon`

[6] D. Stanovský, *Základy algebry*, MatfyzPress, Praha 2010