7. Finite fields

CS-E4500 Advanced Course on Algorithms
Spring 2019

Petteri Kaski
Department of Computer Science
Aalto University

Lecture schedule

Tue 15 Jan:	1. Polynomials and integers
Tue 22 Jan:	2. The fast Fourier transform and fast multiplication
Tue 29 Jan:	3. Quotient and remainder
Tue 5 Feb:	4. Batch evaluation and interpolation
Tue 12 Feb:	5. Extended Euclidean algorithm and interpolation from erroneous data
Tue 19 Feb:	*Exam week — no lecture*
Tue 27 Feb:	6. Identity testing and probabilistically checkable proofs
Tue 5 Mar:	*Break — no lecture*
Tue 12 Mar:	7. Finite fields
Tue 19 Mar:	8. Factoring polynomials over finite fields
Tue 26 Mar:	9. Factoring integers

CS-E4500 Advanced Course in Algorithms (5 ECTS, III–IV, Spring 2019)

2019	KALENTERI	2019

Tammikuu	Helmikuu	Maaliskuu	Huhtikuu	Toukokuu	Kesäkuu
1 Ti Uudenvuodenpäivä	1 Pe	1 Pe	1 Ma Vk 14 T9	1 Ke Vappu	1 La
2 Ke	2 La	2 La	2 Ti	2 To	2 Su
3 To	3 Su D3	3 Su	3 Ke	3 Pe	3 Ma Vk 23 ●
4 Pe	4 Ma Vk 06 T3 ●	4 Ma Vk 10 Break	4 To	4 La	4 Ti
5 La	5 Ti L4	5 Ti Laskiainen	5 Pe ●	5 Su ●	5 Ke
6 Su Loppiainen	6 Ke	6 Ke ●	6 La	6 Ma Vk 19	6 To
7 Ma Vk 02	7 To Q4	7 To	7 Su	7 Ti	7 Pe
8 Ti	8 Pe	8 Pe	8 Ma Vk 15	8 Ke	8 La
9 Ke	9 La	9 La	9 Ti	9 To	9 Su Helluntaipäivä
10 To	10 Su D4	10 Su D6	10 Ke	10 Pe	10 Ma Vk 24 ◐
11 Pe	11 Ma Vk 07 T4	11 Ma Vk 11 T6	11 To	11 La	11 Ti
12 La	12 Ti L5	12 Ti L7	12 Pe ◐	12 Su Äitienpäivä	12 Ke
13 Su	13 Ke ◐	13 Ke	13 La	13 Ma Vk 20	13 To
14 Ma Vk 03 ◐	14 To Q5	14 To Q7 ◐	14 Su Palmusunnuntai	14 Ti	14 Pe
15 Ti L1	15 Pe	15 Pe	15 Ma Vk 16	15 Ke	15 La
16 Ke	16 La	16 La	16 Ti	16 To	16 Su
17 To Q1	17 Su	17 Su D7	17 Ke	17 Pe	17 Ma Vk 25 ○
18 Pe	18 Ma Vk 08 Exam	18 Ma Vk 12 T7	18 To	18 La	18 Ti
19 La	19 Ti ○	19 Ti L8	19 Pe Pitkäperjantai	19 Su Kaatuneiden muistopäivä	19 Ke
20 Su D1	20 Ke	20 Ke Kevätpäiväntasaus	20 La	20 Ma Vk 21	20 To
21 Ma Vk 04 T1 ○	21 To week	21 To Q8 ○	21 Su Pääsiäispäivä	21 Ti	21 Pe Kesäpäivänseisaus
22 Ti L2	22 Pe	22 Pe	22 Ma 2. pääsiäispäivä	22 Ke	22 La Juhannus
23 Ke	23 La	23 La	23 Ti	23 To	23 Su
24 To Q2	24 Su D5	24 Su D8	24 Ke	24 Pe	24 Ma Vk 26
25 Pe	25 Ma Vk 09 T5	25 Ma Vk 13 T8	25 To	25 La	25 Ti ◑
26 La	26 Ti L6 ◑	26 Ti L9	26 Pe	26 Su ◑	26 Ke
27 Su D2 ◑	27 Ke	27 Ke	27 La ◑	27 Ma Vk 22	27 To
28 Ma Vk 05 T2	28 To Q6	28 To Q9 ◑	28 Su	28 Ti	28 Pe
29 Ti L3		29 Pe	29 Ma Vk 18	29 Ke	29 La
30 Ke		30 La	30 Ti	30 To Helatorstai	30 Su
31 To Q3		31 Su Kesäaika alkaa D9		31 Pe	

L = Lecture; hall T5, Tue 12–14

Q = Q & A session; hall T5, Thu 12–14

D = Problem set deadline; Sun 20:00

T = Tutorial (model solutions); hall T6, Mon 16–18

Recap of last week

- We look at yet further applications of the evaluation–interpolation duality and randomization in algorithm design
- Randomized **identity testing** for polynomials and matrices (exercise)
- **Delegating computation** and **proof systems**
- **Completeness** and **soundness** of a proof system,
  cost of **preparing** a proof, cost of **verifying** a proof
- Williams's (2016) [30] probabilistic proof system for #CNFSAT
- Coping with **errors in computation** using error-correcting codes with multiplicative structure (Reed–Solomon codes revisited)
- Proof systems that tolerate errors during proof preparation (Björklund & K. 2016) [3]
- An extension of Shamir's secret sharing to delegating a computation to multiple counterparties (delegating matrix multiplication, exercise)

Motivation for this week

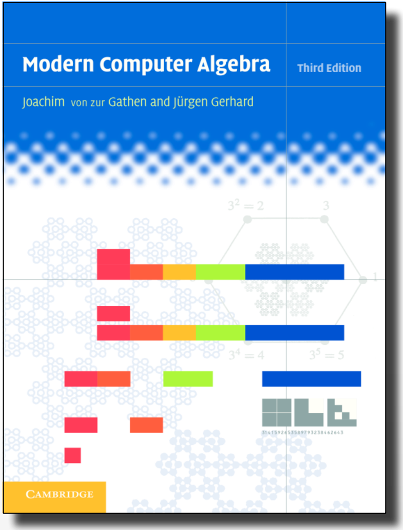
- This week we switch topic somewhat compared with earlier weeks (which focused on the near-linear-time toolbox and its applications)
- Namely, our goal is to develop our understanding of finite fields further
- We proceed from prime fields (finite fields of prime order, that is $\mathbb{Z}_p$ for p prime) to finite fields of prime power order, that is, $\mathbb{F}_q$ for $q = p^d$ with p prime and $d \in \mathbb{Z}_{\geq 1}$
- We develop some structure theory for finite fields to enable our subsequent study of factoring algorithms for univariate polynomials with coefficients in a finite field

Further motivation for this week and what follows

- A tantalizing case where the connection between polynomials and integers apparently breaks down occurs with **factoring**
- Namely, it is known how to efficiently factor a given univariate polynomial over a finite field into its irreducible components, whereas no such algorithms are known for factoring a given integer into its prime factors
- Indeed, the best known algorithms for factoring integers run in time that scales moderately exponentially in the number of digits in the input

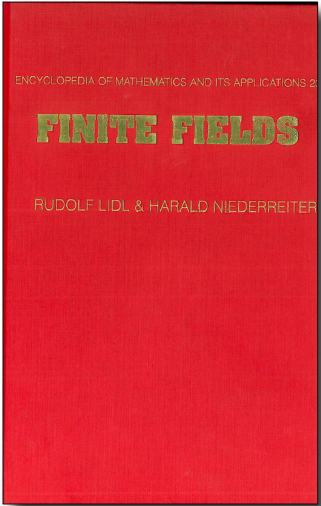
Finite fields

(von zur Gathen and Gerhard [11], Sections 14.1–2, 25.3–4)



Finite fields

(Lidl and Niedderreiter [19])



Key content for Lecture 7

- Prime fields (the integers modulo a prime)
- **Irreducible polynomial**, existence of irreducible polynomials
- **Fermat's Little Theorem** and its generalization (exercise)
- **Finite fields** of **prime power order** via irreducible polynomials (exercise)
- The **characteristic** of a ring; fields have either zero or prime characteristic
- **Extension field**, **subfield**, **degree** of an extension
- **Algebraic** and **transcendental** elements of a field extension;
  the **minimal polynomial** of an algebraic element
- **Multiplicative order** of a nonzero element in a finite field;
  the multiplicative group of a finite field is cyclic
- **Formal derivative** of a polynomial with coefficients in a field (exercise)

(Finite) prime field

- Let p be a prime
- $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ equipped with addition and multiplication modulo p is a field
- Indeed, since p is prime, we have that $\gcd(a, p) = 1$ for all $a \in \mathbb{Z}_p \setminus \{0\}$, and using the extended Euclidean algorithm we can recover Bézout coefficients $s, t \in \mathbb{Z}$ with $as + tp = 1$; reducing s modulo p, we have that every $a \in \mathbb{Z}_p \setminus \{0\}$ has a multiplicative inverse

Finite fields beyond prime fields?

- But are there other finite fields besides the fields of prime order?

Irreducible polynomial

- Let F be a field (for example, take $F = \mathbb{Z}_p$ for a prime p)
- We say that a polynomial $f \in F[x]$ is **irreducible** if $f \notin F$ and for any $g, h \in F[x]$ with $f = gh$ we have $g \in F$ or $h \in F$
- Let us also recall that we say that $f \in F[x]$ is **monic** if its leading coefficient is 1

Fermat's little theorem

Theorem 14 (Fermat's little theorem)

Let q be a prime power. For all $a \in \mathbb{F}_q$ it holds that $a^q = a$ and thus $a^{q-1} = 1$ whenever $a \neq 0$. Furthermore, we have

$$x^q - x = \prod_{a \in \mathbb{F}_q} (x - a) \in \mathbb{F}_q[x]$$

Proof of Fermat's little theorem

- Let us recall **Lagrange's theorem**: for a finite group G and a subgroup $H \leq G$ it holds that $|H|$ divides $|G|$; in particular, for any $g \in G$ we can consider the cyclic subgroup generated by g in G to conclude that $g^{|G|} = 1_G$, where 1_G is the identity of G
- The multiplicative group $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ has $|\mathbb{F}_q^\times| = q - 1$
- Thus, for all nonzero $a \in \mathbb{F}_q \setminus \{0\}$ it holds that $a^{q-1} = 1$
- Consequently, for all $a \in \mathbb{F}_q$ we conclude that $a^q = a$
- From $a^q = a$ it follows that $x - a$ divides $x^q - x$
- Since $\gcd(x - a, x - b) = 1$ for all distinct $a, b \in \mathbb{F}_q$, we have that $\prod_{a \in \mathbb{F}_q}(x - a)$ divides $x^q - x$
- Both $\prod_{a \in \mathbb{F}_q}(x - a)$ and $x^q - x$ are monic of degree q, so we must have $\prod_{a \in \mathbb{F}_q}(x - a) = x^q - x$

Extended Fermat's little theorem

- Fermat's little theorem is the $d = 1$ special case of the following theorem

Theorem 15 (Extended Fermat's little theorem)
Let q be a prime power and let $d \in \mathbb{Z}_{\geq 1}$. Then, $x^{q^d} - x \in \mathbb{F}_q[x]$ is the product of all monic irreducible polynomials in $\mathbb{F}_q[x]$ whose degree divides d

Proof.
Exercise □

Existence of irreducible polynomials

- The following lemma shows that irreducible polynomials exist for all prime powers $q \geq 2$ and $n \geq 2$, apart possibly from the case $q = 2$ and $n = 2$, where it is easily verified that $x^2 + x + 1 \in \mathbb{F}_2[x]$ is irreducible

Lemma 16 (Number of irreducible polynomials)

Let q be a prime power and $n \in \mathbb{Z}_{\geq 1}$. Then, the number $I(n, q)$ of monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$ satisfies

$$\frac{q^n - 2q^{n/2}}{n} \leq I(n, q) \leq \frac{q^n}{n}$$

Proof of Lemma 16 I

- Let f_n be the product of all monic irreducible polynomials of degree n in $\mathbb{F}_q[x]$
- Thus, $\deg f_n = n \cdot I(n, q)$
- From Theorem 15 we thus have

$$x^{q^n} - x = \prod_{d \mid n} f_d = f_n \prod_{d \mid n, d < n} f_d \tag{33}$$

- Taking degrees on both sides of (33), we have

$$q^n = \deg f_n + \sum_{d \mid n, d < n} \deg f_d$$

  and thus we have the upper bound

$$q^n \geq \deg f_n = n \cdot I(n, q) \tag{34}$$

Proof of Lemma 16 II

- To set up the lower bound, use (34) and $q \geq 2$ to observe that

$$\sum_{d|n, d<n} \deg f_d \leq \sum_{1 \leq d \leq n/2} \deg f_d \leq \sum_{1 \leq d \leq n/2} q^d < \frac{q^{n/2+1} - 1}{q - 1} \leq 2q^{n/2}$$

- Thus,

$$n \cdot I(n, q) = \deg f_n = q^n - \sum_{d|n, d<n} \deg f_d \geq q^n - 2q^{n/2},$$

which establishes the lower bound

Finite fields of prime power order

- Let p be a prime and let $d \in \mathbb{Z}_{\geq 1}$
- Let $f \in \mathbb{Z}_p[x]$ be an irreducible monic polynomial of degree d
- Then, $F = \mathbb{Z}_p[x]/\langle f \rangle$ is a finite field with p^d elements
- Indeed, we can identify the elements of F with the set of all polynomials of degree at most $d-1$ in $\mathbb{Z}_p[x]$
- Addition and multiplication in F are as in $\mathbb{Z}_p[x]$, except that multiplication is reduced by taking the polynomial remainder with respect to f so that the result has degree at most $d-1$
- Since f is irreducible, for every nonzero element $a \in F$ we have $\gcd(a, f) = 1$; accordingly, a has a multiplicative inverse $a^{-1} = s$ in F, which can be computed by running the extended Euclidean algorithm to obtain the Bézout coefficients $s, t \in \mathbb{Z}_p[x]$ with $as + ft = 1$

The characteristic of a ring

- Let R be a ring (commutative and nontrivial with $0_R \neq 1_R$)
- For $k \in \mathbb{Z}_{\geq 0}$, let us write $k \cdot 1_R$ for $k \cdot 1_R = 1_R + 1_R + \ldots + 1_R$, where we take the sum of k copies of 1_R, the multiplicative identity of R
- The **characteristic** of R is the minimum positive integer k such that $k \cdot 1_R = 0_R$
- When no such positive k exists for R, we define the characteristic of R to be 0

The characteristic of a field

- The characteristic of a field F is either zero (in which case F is infinite) or prime
- Indeed, suppose that F has characteristic n with $n = ab$ for $a, b \in \mathbb{Z}_{\geq 2}$
- Then $a \cdot 1_F \in F$ is a zero divisor since by definition of characteristic we have $a \cdot 1_F \neq 0_F$, $b \cdot 1_F \neq 0_F$, and $(a \cdot 1_F)(b \cdot 1_F) = (ab) \cdot 1_F = 0_F$
- But this is a contradiction since a zero divisor cannot be a unit (exercise), and all nonzero elements in a field are units
- Thus, we conclude that every finite field has prime characteristic

Extension field, subfield

- Let E and F be fields such that $F \subseteq E$
- We say that E is an **extension field** of F, and, conversely, that F is a **subfield** of E
- *Example:*
  Let F be a finite field. The set $P = \{k \cdot 1_F : k \in \mathbb{Z}_{\geq 0}\}$ is a subfield of F of order p, where p is the (prime) characteristic of F

Finite extension, degree of an extension

- Let E be an extension field of a field F
- We may view E as a vector space over F
- If the dimension of E as a vector space over F is finite, we say that E is a **finite extension** of F
- If E is a finite extension of F, we say that the **degree** of the extension is the dimension of E as a vector space over F
- Since every finite field has prime characteristic and a subfield of prime order, every finite field is a finite extension of a field of prime order
- Thus, for every finite field F there exists a prime p and an integer $d \in \mathbb{Z}_{\geq 1}$ such that $|F| = p^d$.

Algebraic and transcendental elements, algebraic extension

- Let E be an extension field of a field F
- We say that an element $\alpha \in E$ is **algebraic** over F if there exists a nonzero polynomial $f \in F[x]$ with coefficients in F such that $f(\alpha) = 0$
- Elements that are not algebraic are **transcendental**
- If all elements of E are algebraic over F, we say that E is an **algebraic extension** of F
- All finite extensions are algebraic (exercise)

Minimal polynomial of an algebraic element

- Let E be an extension field of a field F
- Let $\alpha \in E$ be algebraic over F
- Let $I = \{f \in F[x] : f(\alpha) = 0\}$ and observe that I is an ideal of $F[x]$
- Since $F[x]$ is an Euclidean domain, every ideal of $F[x]$ is generated by a single element
- The unique monic polynomial m_α of least degree in I is called the **minimal polynomial** of α
- m_α is irreducible in $F[x]$ (indeed, otherwise at least one of the nontrivial factors of m_α would have root α, contradicting the minimality of m_α)
- The **degree** of α is $\deg m_\alpha$

Existence of elements of maximum degree

- Let F be a finite field of order $q = p^d$ for p prime and $d \in \mathbb{Z}_{\geq 1}$
- Let P be a subfield of F of order p
- Then, F is an extension of degree d of P, and all elements of F are algebraic over P with degree at most d
- There always exists an element $\alpha \in F$ that is algebraic of degree d over P (exercise)

Uniqueness and characterization

- Let F and $\tilde{F}$ be finite fields of order $q = p^d$ for p prime and $d \in \mathbb{Z}_{\geq 1}$
- Then, F and $\tilde{F}$ are isomorphic (details omitted)

- Thus, we have a complete characterization of finite fields – all finite fields arise by extension of a prime-order field using an irreducible polynomial with coefficients in the prime-order field
- Up to isomorphism, only the degree of the irreducible polynomial matters; all irreducible polynomials of a particular degree give rise to the same field up to isomorphism
- Thus for a prime power q it makes sense to write $\mathbb{F}_q$ for the finite field of order q
- Let us next analyze the structure of $\mathbb{F}_q$ in somewhat more detail ...

Multiplicative order of a nonzero element

- Let q be a prime power
- For a nonzero $a \in \mathbb{F}_q \setminus \{0\}$ let us write $\mathrm{ord}(a)$ for the least positive integer k such that $a^k = 1$
- We say that $\mathrm{ord}(a)$ is the **multiplicative order** of a
- By Fermat's little theorem (Theorem 14) we have that $\mathrm{ord}(a)$ divides $q - 1$
- Indeed, suppose $ord(a)$ does not divide $q - 1$, and let $1 \leq r < \mathrm{ord}(a)$ be the remainder in the division of $q - 1$ by $\mathrm{ord}(a)$
- Then we have $a^r = a^{q-1-((q-1)\,\mathrm{quo}\,\mathrm{ord}(a))\,\mathrm{ord}(a)} = a^{q-1}(a^{\mathrm{ord}(a)})^{-(q-1)\,\mathrm{quo}\,\mathrm{ord}(a)} = 1 \cdot 1 = 1$, which contradicts the definition of $\mathrm{ord}(a)$ since $1 \leq r < \mathrm{ord}(a)$

The multiplicative group is cyclic

Theorem 17 (Structure of the multiplicative group)

Let q be a prime power and let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ divide $q - 1$ with $p_1, p_2, \ldots, p_k$ distinct primes and $e_1, e_2, \ldots, e_k \in \mathbb{Z}_{\geq 1}$. Then,

(i) *for all $a \in \mathbb{F}_q^\times$ we have $\operatorname{ord}(a) = n$ if and only if $a^n = 1$ and $a^{n/p_j} \neq 1$ for all $j = 1, 2, \ldots, k$*

(ii) *for all $j = 1, 2, \ldots, k$, there exists an $a \in \mathbb{F}_q^\times$ with $\operatorname{ord}(a) = p_j^{e_j}$*

(iii) *for all $a, b \in \mathbb{F}_q^\times$ with $\operatorname{ord}(a)$ and $\operatorname{ord}(b)$ coprime, we have $\operatorname{ord}(ab) = \operatorname{ord}(a) \operatorname{ord}(b)$*

(iv) *there exists an $a \in \mathbb{F}_q^\times$ with $\operatorname{ord}(a) = q - 1$*

(v) *the multiplicative group $\mathbb{F}_q^\times$ is cyclic*

Proof of Theorem 17 I

- To establish (i), we first observe that the “only if” direction is immediate from the definition of $\operatorname{ord}(a)$
- To show the “if” direction, let us assume that $\operatorname{ord}(a) \neq n$
- If $\operatorname{ord}(a) > n$, then we must have $a^n \neq 1$ by definition of $\operatorname{ord}(a)$
- So let us assume that $\operatorname{ord}(a) < n$
- Suppose that $a^n = 1$ holds (indeed, otherwise we are done)
- If $\operatorname{ord}(a)$ divides n, then since $\operatorname{ord}(a) < n$ there exists a $j = 1, 2, \ldots, k$ such that $\operatorname{ord}(a)$ divides n/p_j; thus $a^{n/p_j} = 1$
- If $\operatorname{ord}(a)$ does not divide n, then let $1 \leq r < \operatorname{ord}(a)$ be the remainder in the division of n by $\operatorname{ord}(a)$; in this case we have $a^r = a^{n-(n \operatorname{quo} \operatorname{ord}(a)) \operatorname{ord}(a)} = 1$, which contradicts the definition of $\operatorname{ord}(a)$ — this establishes (i)

Proof of Theorem 17 II

- To establish (ii), let us study the polynomial $x^{n/p_j} - 1 = 0$
- Since $n/p_j < q - 1$, we know that there is at least one $b \in \mathbb{F}_q^\times$ that is not a root of $x^{n/p_j} - 1 = 0$; that is, $b^{n/p_j} \neq 1$
- Take $a = b^{(q-1)/p_j^{e_j}}$; we claim that $\operatorname{ord}(a) = p_j^{e_j}$ holds
- Indeed, let us verify (i) for a and $n = p_j^{e_j}$; we have

$$a^{p_j^{e_j}} = \left(b^{(q-1)/p_j^{e_j}}\right)^{p_j^{e_j}} = b^{q-1} = 1$$

  and

$$a^{p_j^{e_j-1}} = \left(b^{(q-1)/p_j^{e_j}}\right)^{p_j^{e_j-1}} = b^{(q-1)/p_j} \neq 1$$

- To establish (iii), let us verify (i) for ab with $n = \operatorname{ord}(a)\operatorname{ord}(b)$

Proof of Theorem 17 III

- First, we have $(ab)^n = a^{\mathrm{ord}(a)\,\mathrm{ord}(b)} b^{\mathrm{ord}(a)\,\mathrm{ord}(b)} = 1^{\mathrm{ord}(b)} 1^{\mathrm{ord}(a)} = 1$
- Next, let p be a prime that divides n
- Since $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$ are coprime, we have that p divides exactly one of $\mathrm{ord}(a)$ or $\mathrm{ord}(b)$; by symmetry between a and b we can assume that p divides $\mathrm{ord}(a)$
- We thus have that $(ab)^{\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)} = a^{\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)} b^{\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)} = a^{\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)}$
- Suppose we have $a^{\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)} = 1$
- Then, we must have that $\mathrm{ord}(a)$ divides $\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)$ or otherwise we contradict the definition of $\mathrm{ord}(a)$; but we cannot have that $\mathrm{ord}(a)$ divides $\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)$ because $\mathrm{ord}(a)$ and $\mathrm{ord}(b)$ are coprime
- Thus, we have $a^{\frac{\mathrm{ord}(a)}{p}\,\mathrm{ord}(b)} \neq 1$ – this establishes (iii)

Proof of Theorem 17 IV

- To establish (iv), let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q - 1$ and use (ii) for each $j = 1, 2, \ldots, k$ to obtain an $a_j \in \mathbb{F}_q^\times$ with $\operatorname{ord}(a_j) = p_j^{e_j}$
- Then, use (iii) to conclude that $\operatorname{ord}(a_1 a_2 \cdots a_k) = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q - 1$; thus, setting $a = a_1 a_2 \cdots a_k$ establishes (iv)
- To establish (v), observe that the element a constructed in (iv) generates $\mathbb{F}_q^\times$ as a cyclic group since $\operatorname{ord}(a) = q - 1$

Recap of Lecture 7

- Prime fields (the integers modulo a prime)
- **Irreducible polynomial**, existence of irreducible polynomials
- **Fermat's Little Theorem** and its generalization (exercise)
- **Finite fields** of **prime power order** via irreducible polynomials (exercise)
- The **characteristic** of a ring; fields have either zero or prime characteristic
- **Extension field**, **subfield**, **degree** of an extension
- **Algebraic** and **transcendental** elements of a field extension;
  the **minimal polynomial** of an algebraic element
- **Multiplicative order** of a nonzero element in a finite field;
  the multiplicative group of a finite field is cyclic
- **Formal derivative** of a polynomial with coefficients in a field (exercise)