# Wolfgang K. Seiler: Finite fields

*Sommerschule Datensicherheit, Mannheim 2003*

Both cryptography and coding theory deal with message blocks, transforming them in such a way that either their meaning is hidden from eavesdroppers, or they contain redundancy that can be used to detect or even correct transmission errors.

Mathematically speaking therefore, in both cases we are looking for mappings between finite sets. For such maps there are no further requirements except the obvious one that they have to be injective. Since arbitrary maps are hard to deal with, however, in practical approaches, the sets of message blocks are given a mathematical structure, usually the simplest one from a computational viewpoint: They are made into vector spaces.

Vector spaces over the real numbers are, of course, useless as models for finite sets: Like the vector spaces themselves the scalar fields have to be finite. This introductory talk will summarize the principal facts about finite fields, as far as they will be needed in subsequent talks of this summer school.

## §1: The characteristic of a field

Let us first recall the definition of a field:

**Definition:** A field $F$ is a set together with two operations

$$+ : F \times F \to F \quad \text{and} \quad \cdot : F \times F \to F\,,$$

called *addition* and *multiplication,* obeying the following axioms:



I.1) Associativity of addition

$$(a+b)+c = a+(b+c) \qquad \text{for all } a,b,c \in F$$

I.2) There is an element $0 \in F$, such that

$$a+0 = 0+a = a \qquad \text{for all } a \in F$$

I.3) For each $a \in F$ there exists an $a' \in F$, such that

$$a + a' = a' + a = 0\,.$$

I.4) Commutativity of addition

$$a+b = b+a \qquad \text{for all } a,b \in F$$

II.1) Associativity of multiplication

$$(a \cdot b)\cdot c = a \cdot (b \cdot c) \qquad \text{for all } a,b,c \in F$$

II.2) There is an element $1 \neq 0$ in $F$, such that

$$a \cdot 1 = 1 \cdot a = a \qquad \text{for all } a \in F$$

II.3) For each $a \in F \setminus \{0\}$, there exists an $a'' \in F$, such that

$$a \cdot a'' = a'' \cdot a = 1\,.$$

II.4) Commutativity of multiplication

$$a \cdot b = b \cdot a \qquad \text{for all } a,b \in F$$

III.) Distributivity

$$a\cdot(b+c) = a\cdot b + a \cdot c \qquad \text{for all } a,b,c \in F$$

The element $a'$ from I.3.) is usually written $-a$, and $a''$ from II.3) $a^{-1}$; also $a+(-b)$ is usually shortened to $a-b$, and $a \cdot b^{-1}$ to $a/b$.

Informally speaking, we can say that a fields is a set, in which the usual operations of arithmetic are defined and obey the usual rules, or at least most of them.

There is, however, one big difference between the well known fields of real or rational numbers and a finite field: If we keep adding the element one to itself in $\mathbb{R}$ or $\mathbb{Q}$, all the numbers

$$n \cdot 1 \underset{\text{def}}{=} \underbrace{1 + \cdots + 1}_{n \text{ terms}}$$

are different; in the case of a finite field $F$, this is impossible, because there are only finitely many elements in $F$. Hence for every finite field there are positive integers $n < m$, such that

$$n \cdot 1 = m \cdot 1 \quad \text{or} \quad (m-n) \cdot 1 = 0\,.$$

**Definition:** The *characteristic* of a field $F$ is the smallest positive integer $p$ such that $p \cdot 1 = 0$. If no such positive integer exists, the characteristic of $F$ is zero.

If the characteristic of a field is nonzero, it is necessarily a prime number, because, if we could write it as $p = n \cdot m$ with integers $n, m > 1$, the product of $a = n \cdot 1$ and $b = m \cdot 1$ in $F$ were $p \cdot 1 = 0$. But then

$$\begin{aligned} m \cdot 1 = y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (xy) = x^{-1} \cdot 0 \\ = x^{-1} \cdot (1-1) = x^{-1} - x^{-1} = 0\,, \end{aligned}$$

contradicting the minimality of $p$. Thus $p$ must be prime.

The simplest field of characteristic $p > 0$ consists of nothing but the multiples of 1; we call this field $\mathbb{F}_p$. We can identify its elements with the numbers $0, 1, \ldots, p-1$, and its arithmetic operations are simply the usual ones performed modulo $p$.

All field axioms except the existence of multiplicative inverses are obviously satisfied; for multiplicative inverses and thus for the proof that $\mathbb{F}_p$ really is a field, we have to recall EUCLID's algorithm.

## §2: Euclid's algorithm

It computes the greatest common divisor (gcd) of two positive integers $a \ge b$ using the following observation: If

$$a : b = q \ \text{ remainder } r\,,$$

then

$$\gcd(a,b) = \begin{cases} a & \text{if } b = 0 \\ \gcd(b,r) & \text{if } b \ne 0 \end{cases}.$$

This holds, because the equations

$$a = bq + r \quad \text{and} \quad r = a - bq$$



show that every common divisor of $b$ and $r$ is also a divisor of $a$, and every common divisor of $a$ and $b$ is also one of $r$.

So, starting from $a, b$, EUCLID divides $a$ by $b$ and computes the remainder $r_1$; by definition, it is less than $b$. If $r_1 = 0$, then $b$ divides $a$ and therefore is the greatest common divisor of $a$ and $b$; if not,

$$\gcd(a,b) = \gcd(b, r_1)\,.$$

To compute the right hand side, divide $b$ by $r_1$:

$$b : r_1 = q_1 \ \text{ remainder } r_2$$

with $r_2 < r_1$, and so on. Since a sequence of positive integers cannot decrease indefinitely, after a finite number of steps we get some $r_n = 0$, and $\gcd(a,b) = r_{n-1}$, because we got $r_n$ as remainder of $r_{n-2}$ when divided by $r_{n-1}$, hence

$$\gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = r_{n-1}\,.$$

As EUCLID already observed in his *Elements,* this algorithms not only computes the greatest common divisor $d$ of any two positive integers $a, b$, but also leads to integers $\lambda, \mu$ such that

$$\lambda a + \mu b = d\,.$$

To see why this is the case, consider an intermediate step

$$r_{s-2} : r_{s-1} = q_{s-1} \ \text{ remainder } r_s\,.$$

This can also be written

$$r_s = r_{s-2} - q_{s-1} r_{s-1}\,,$$

giving $r_s$ as a linear combination of $r_{s-1}$ and $r_{s-2}$. The step before gave $r_{s-1}$ as a linear combination of $r_{s-2}$ and $r_{s-3}$; putting this into the equation above gives $r_s$ as a linear combination of $r_{s-2}$ and $r_{s-3}$, and so on, till it is written as a linear combination of $a$ and $b$.

Applying this to the last nonzero remainder $r_{n-1}$, we get the gcd of $a$ and $b$ as a linear combination of $a$ and $b$.

As an example, let's compute the gcd of 200 and 148. We first divide 200 by 148 getting quotient one and remainder

$$52 = 1 \cdot 200 - 1 \cdot 148\,.$$

In the next step we divide 148 by 52, which is two with remainder

$$44 = 148 - 2 \cdot 52 = 148 - 2 \cdot (1 \cdot 200 - 1 \cdot 148) = 3 \cdot 148 - 2 \cdot 200 .$$

Dividing 52 by 44 gives remainder

$$\begin{aligned} 8 &= 52 - 44 = (1 \cdot 200 - 1 \cdot 148) - (3 \cdot 148 - 2 \cdot 200) \\ &= 3 \cdot 200 - 4 \cdot 148 . \end{aligned}$$

44 divided by 8 is 5 with remainder 4 and

$$\begin{aligned} 4 &= 44 - 5 \cdot 8 = (3 \cdot 148 - 2 \cdot 200) - 5 \cdot (3 \cdot 200 - 4 \cdot 148) \\ &= 23 \cdot 148 - 17 \cdot 200 . \end{aligned}$$

In the next step we divide eight by four; since there is no remainder, the algorithm terminates with

$$\gcd(200, 148) = 4 = 23 \cdot 148 - 17 \cdot 200 .$$

As a first application, we now easily see that the integers modulo a prime number $p$ form a field: The only remaining problem is the existence of multiplicative inverses; so let $a \in \mathbb{F}_p \setminus \{0\} = \{1, \ldots, , p-1\}$ be an element different from zero. Since $p$ is a prime and $a < p$, the two numbers $a$ and $p$ cannot have any common divisor except one; hence $\gcd(a, p) = 1$. According to EUCLID we can write it as a linear combination

$$1 = \lambda a + \mu p \quad \text{with} \quad \lambda, \mu \in \mathbb{Z} .$$

Taking $a' = \lambda \bmod p$, we therefore get $a'a = 1$ in $\mathbb{F}_p$.

## §3: Fermat's theorem

Let $F$ be any finite field, and $q$ its cardinality (number of elements). Since $F$ is finite, the set of powers $x, x^2, x^3, \ldots$ of every element $x \in F$ must be finite. Hence there must be pairs of integers $m > n$ such that $x^n = x^m$. If $x \neq 0$ this implies that $x^{m-n} = 1$, so every $x \neq 0$ has a power equal to one.

**Definition:** The order of an element $x \neq 0$ of a finite field $F$ is the smallest positive integer $r$ such that $x^r = 1$.

EUCLID's algorithm immediately shows



**Lemma:** Let $x \neq 0$ be an element of order $r$ of the finite field $F$, and let $n$ be an integer. Then $x^n = 1$ if and only if $n$ is a multiple of $r$.

*Proof:* $d = \gcd(n, r)$ can be written as a linear combination $d = \lambda n + \mu r$ of $n$ and $r$; therefore

$$x^d = x^{\lambda n + \mu r} x^{\lambda n} x^{\mu r} = \left(x^n\right)^\lambda \left(x^r\right)^\mu = 1 .$$

Since $r$ is the smallest positive integer such that $x^r = 1$ and $d \leq r$, we have $d = r$, i.e. $r$ divides $n$.

■

**Fermat's theorem:** Let $F$ be a finite field with $q$ elements. Then

$$x^{q-1} = 1$$

for every $x \in F \setminus \{0\}$. In particular, the order of each $x \in F \setminus \{0\}$ divides $q - 1$.

*Proof:* Fix an $x \in F \setminus \{0\}$ and, for any $a \in F \setminus \{0\}$, let

$$M_a = \left\{ ax^n \in F \;\middle|\; n \in \mathbb{Z} \right\} = \left\{ ax^n \in F \;\middle|\; n = 0, \ldots, r-1 \right\} ,$$

where $r$ is the order of $x$. If for two elements $a, b \in F \setminus \{0\}$ the intersection $M_a \cap M_b$ contains some $c \in F$, there exist $n, m \in \mathbb{Z}$ such that $c = ax^n = bx^m$; since $x \neq 0$, this implies

$$a = bx^{m-n} \in M_b \quad \text{and} \quad b = ax^{n-m} \in M_a, \quad \text{hence} \quad M_a = M_b .$$

Thus either $M_a = M_b$ or $M_a \cap M_b = \emptyset$. On the other hand, each $M_a$ contains exactly $r$ different elements; so, if $s$ is the number of different sets $M_a$, we have $rs = q - 1$, the number of elements in $F \setminus \{0\}$. Thus $r$ divides $q - 1$, and $x^{q-1} = 1$ by the lemma.

■

**Corollary 1:** For every element $x$ in a finite field with $q$ elements, $x^q = x$.

*Proof:* This is obviously true for $x = 0$, and for $x \neq 0$, we have $x^{q-1} = 1$, hence $x^q = x$.

■

**Corollary 2:** Every finite field $F$ contains at least one element $x$ such that every element of $F \setminus \{0\}$ is a power of $x$, i.e.

$$F = \{0, 1 = x^0, x = x^1, x^2, \dots, x^{q-2}\},$$

where $q$ is the cardinality of $F$.

*Proof:* Let

$$q - 1 = p_1^{e_1} \cdots p_s^{e_s}$$

be the decomposition of $q-1$ into a product of prime numbers.

The order of $y \in F \setminus \{0\}$ divides an integer $r$ if and only if $y^r = 1$, i.e. $y$ is a zero of the polynomial $X^r - 1$. Thus there can be at most $r$ elements $y \in F$ for which $y^r = 1$, because a polynomial of degree $r$ has at most $r$ different zeroes.

In particular, for each $i = 1, \dots, s$, there are at most $\frac{q-1}{p_i}$ elements $y$ such that $y^{(q-1)/p_i} = 1$; hence there are elements $y_i$ such that

$$y_i^{(q-1)/p_i} \neq 1\,.$$

Let $x_i = y_i^{(q-1)/p_i^{e_i}}$; then

$$x_i^{p^{e_i}} = y_i^{q-1} = 1, \quad \text{but} \quad x_i^{p^{e_i-1}} = y_i^{(q-1)/p_i} \neq 1\,.$$

Therefore $x_i$ has order $p_i^{e_i}$.

Now consider the product $x = x_1 \cdots x_s$ of the $x_i$. By FERMAT, its order divides $q-1$; if it is smaller then $q-1$, it divides at least one of the numbers $h_i = \frac{q-1}{p_i}$. But

$$h_i = \frac{q-1}{p_i} = p_1^{e^1} \cdots p_{i-1}^{e_{i-1}} p_i^{e_i - 1} p_{i+1}^{e_{i+1}} \cdots p_s^{e_s}$$

is a multiple of all $p_j^{e_j}$ with $j \neq i$; hence $x_j^{h_i} = 1$ for all $j \neq i$, and

$$x^{h_i} = x_1^{h_i} \cdots x_s^{h_i} = x_i^{h_i}\,.$$

Since $x_i$ has order $p_i^{e_i}$, but $h_i = \frac{q-1}{p_i}$ is divisible only by $p_i^{e_i-1}$, the above lemma shows that $x^{h_i} \neq 1$; therefore the order of $x$ must be $q-1$. ■



**Definition:** An element $x \in F$ of a finite fields $F$ is called a *primitive root,* if every nonzero element of $F$ is a power of $x$.

Thus every finite field contains primitive roots. There is, however, no good formula to get a primitive root for a given finite field; the usual strategy is to take either random numbers or systematically to take all numbers and compute their order, until one has found a primitive root.

## §4: Existence of finite fields

From §2, we know that for every prime number $p$ we have exactly one field with $p$ elements, the field $\mathbb{F}_p$. We also know, that any field $F$ of characteristic $p$ contains $\mathbb{F}_p$ as a subfield and therefore is an $\mathbb{F}_p$-vector space.

If $F$ is a finite field of characteristic $p$, it is of course a finite dimensional vector space; by choosing a basis, we can identify it with $\mathbb{F}_p^n$ for some positive integer $n$, the dimension of $F$ over $\mathbb{F}_p$. The cardinality $q$ of $F$ is therefore $p^n$, hence the cardinality of any finite field must be a prime power.

In fact, it is not very difficult to show that for every prime power $q = p^n$, there is indeed a unique field $\mathbb{F}_q$ with $q$ elements: By a general theorem from algebra (the key point of whose proof will be outlined in the next paragraph), for any field $F$ and any polynomial $P$ over $F$, there exists a field $F'$ containing $F$, such that $P$ can be written as a product of linear polynomials over $F'$. Apply this to the polynomial $x^q - x$ over $\mathbb{F}_p$ and let $\mathbb{F}_q$ be the set of its zeroes in $F'$.

Since $F'$ contains $\mathbb{F}_p$, it is a field of characteristic $p$. For $x, y \in F'$, we have

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \binom{p}{2} x^{p-2} y^2 + \cdots + \binom{p}{p-1} x y^{p-1} + y^p\,,$$

and

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

is divisible by $p$ for $i = 1, \dots, p-1$, because the numerator, but not the denominator is a multiple of $p$. Hence

$$(x+y)^p = x^p + y^p \quad \text{for all} \quad x, y \in F' .$$

By induction we find that for each positive integer $r$

$$(x+y)^{p^r} = x^{p^r} + y^{p^r} \quad \text{for all} \quad x, y \in F' ,$$

so in particular $(x+y)^q = x^q + y^q$. For $x, y \in \mathbb{F}_q$, we have $x^q = x$ and $y^q = y$, hence

$$(x+y)^q = x + y \quad \text{for all} \quad x, y \in \mathbb{F}_q .$$

Similarly, we get that $(x-y)^q = x - y$. Thus, for $x, y \in \mathbb{F}^q$, also $x \pm y$ is an element of $\mathbb{F}_q$, the set of zeroes of the polynomial $X^q - X$. Of course, also $(xy)^q = x^q y^q = xy$, so that $xy \in \mathbb{F}_q$, and for $y \neq 0$ similarly $\left(\frac{x}{y}\right)^q = \frac{x^q}{y^q} = \frac{x}{y}$; hence the set $\mathbb{F}_q$ is in fact a subfield of $F'$ containing exactly the $q$ roots of $x^q - x$.

## §5: Computations in finite fields

As long as we are only interested in multiplication, computations in $\mathbb{F}_q$ are rather simple: We choose a primitive root $x$ and write all nonzero elements of $\mathbb{F}_q$ as powers of $x$; then $x^i \cdot x^j = x^{i+j} = x^{i+j \bmod (q-1)}$.

As soon as we also want to add, however, this approach is no longer practical for large values of $q$: The task of finding an exponent $k$ such that some element like $x^i + x^j$ is equal to $x^k$ turns out to be so difficult that, as we shall see in the next talk, several cryptosystems can be based on this problem.

Therefore we shall usually use a linear algebra approach: For prime numbers $p$, computing in $\mathbb{F}_p$ simply means ordinary arithmetic modulo $p$, which is quite easy. If $q = p^n$ is a prime power, then $\mathbb{F}_q \cong \mathbb{F}_p^n$ is an $n$-dimensional $\mathbb{F}_p$-vector space, and the conventional approach to computations in finite dimensional vector spaces is, first to choose a basis, and then to reduce everything to computations in the field of scalars.



Since $\mathbb{F}_q$ is not simply an $\mathbb{F}_p$-vector space, but also a field of its own, we should take a basis that is adapted to the multiplicative structure of $\mathbb{F}_q$, for example a basis of the form $\{1, x, x^2, \dots x^{n-1}\}$ for some element $x \in \mathbb{F}_q$. As we shall see soon, every primitive root $x \in \mathbb{F}_q$ gives rise to such a basis.

With respect to such a basis, we can write every element of $\mathbb{F}_q$ as a polynomial of degree at most $n-1$ in $x$. Addition of such polynomials is of course no problem, their product, however, will usually have a bigger degree than $n-1$. Nevertheless, as an element of $\mathbb{F}_q$, it can also be written as a polynomial of degree at most $n-1$ in $x$, and we have to find that polynomial.

Since $x^n \in \mathbb{F}_q$, it must be representable as a linear combination of the elements of the basis, i.e. there must exist elements $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{F}_p$, such that

$$x^n = \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0$$

or

$$x^n - \alpha_{n-1}x^{n-1} - \cdots - \alpha_1 x - \alpha_0 = 0 .$$

If $f$ denotes the polynomial

$$X^n - \alpha_{n-1}X^{n-1} - \cdots - \alpha_1 X - \alpha_0 = 0 ,$$

we therefore have $f(x) = 0$.

Now recall that for polynomials, just as for integers, we have a division algorithm: Whenever $s, f$ are two polynomials over a field $F$, we can divide $s$ by $f$ getting a quotient $q$ and a remainder $r$ such that

$$s = qf + r \quad \text{where} \quad \deg r < \deg f .$$

If $y, z \in \mathbb{F}_q$ are any two elements, we have unique polynomials $g, h$ of degree less than $n$ such that

$$y = g(x) \quad \text{and} \quad z = h(x) .$$

If $s$ is the product of the polynomials $g$ and $h$, we can divide $s$ by $f$ getting

$$s = qf + r \quad \text{where} \quad \deg r < \deg f = n ,$$

and

$$y \cdot z = g(x) \cdot h(x) = s(x) = q(x) \cdot f(x) + r(x) = r(x) ,$$

because $f(x) = 0$. Hence multiplication in $\mathbb{F}_q$ can be done with a multiplication and a division of polynomials over $\mathbb{F}_p$.

Division is no big problem either: Since we have a division algorithm for polynomials, EUCLID's algorithm can be generalized to polynomials, giving us inverse elements as in the case of $\mathbb{F}_p$.

In the case of $\mathbb{F}_p$, it was essential for this that the numbers $1, \dots, p-1$ are all coprime to $p$, so that we can write one as a linear combination of any such number and $p$. Similarly we need here, that no polynomial of degree less than $n$ has a common divisor with $f$, that is, $f$ must be irreducible in the following sense:

**Definition:** A polynomial $f$ over a field $F$ is called irreducible, if there do not exist polynomials $g, h$ over $F$ of positive degree such that $f = gh$.

Irreducible polynomials play the same rôle as prime numbers. In particular, it is a well known fact that every integer can be written as a product of primes in an essentially unique way. A straightforward modification of the (not so well known, but rather elementary) proof shows, that also every polynomial over a field $F$ can be written as a product of irreducible polynomials, and again in an essentially unique way. Here, the word *essentially* also means that we do not regard two irreducible polynomials as *essentially* different, if each one is a constant multiple of the other.

Since $\mathbb{F}_q$ is a field, it is clear, that the polynomial $f$ defined above must be irreducible: If $f = gh$ were a decomposition with both $g$ and $h$ of positive degree, both $\deg g$ and $\deg h$ were less than $n$ and would define nonzero elements of $\mathbb{F}_q$ with product zero, which is impossible in a field.

Therefore, for any polynomial $g$ of degree less than $n$, the greatest common divisor of $f$ and $g$ is one; hence we can find polynomials $\alpha, \beta$, such that

$$1 = \alpha f + \beta g \quad \text{and} \quad 1 = \alpha(x)f(x) + \beta(x)g(x) = \beta(x)g(x) ,$$

since $f(x) = 0$. Hence $\beta(x)$ is an inverse to $g(x)$.



In most applications, finite fields are not *given,* but have to be constructed. The discussion above shows how to make an $n$-dimensional vector space over $\mathbb{F}_p$ (or any other finite field $\mathbb{F}_q$) into a field: Choose an irreducible polynomial $f$ of degree $n$ over the field in question, and define a multiplication as above.

Suppose, for example, we want to make the vector space $\mathbb{F}_2^8$ into a field. Since $\mathbb{F}_2 = \{0, 1\}$ is simply the field of all bits, $\mathbb{F}_2^8$ is the vector space of all bytes.

We first have to find an irreducible polynomial of degree eight. This is not very difficult: We either take random polynomials and check whether or not they are irreducible, or we remember that the polynomial must divide $x^{255} - 1$, and factor that polynomial, looking for irreducible factors of degree eight. Computer algebra provides a rather efficient algorithm for factorization over finite fields (BERLEKAMP's algorithm), whose first step contains a very efficient check for irreducibility.

In our case, there are thirty irreducible polynomials of degree eight; the two most popular (because computationally efficient) ones are

$$f_1 = X^8 + X^4 + X^3 + X + 1 \quad \text{and} \quad f_2 = X^8 + X^4 + X^3 + X^2 + 1 .$$

$f_1$ is used for the Advanced Encryption Standard AES, $f_2$ for the REED-SOLOMON code which is one part of error correction on a compact disk.

We still don't know, why a primitive root $x$ of $\mathbb{F}_q$ leads to a basis $\{1, x, \dots, x^{n-1}\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. Assume not. Then these elements are linearly dependent, hence there is a polynomial $g$ of smaller degree than $n$ such that $g(x) = 0$, and there is also an irreducible such polynomial. This polynomial defines a proper subfield of $\mathbb{F}_q$ containing all powers of $x$. But this contradicts the assumption that every nonzero element of $\mathbb{F}_q$ is a power of $x$.