How to build GF(p^n)

José Angel de Bustos Pérez

Contents

Chapter 1

Introduction

1.1 How many digits do we need in base n to write m numbers?

To write m numbers in base n the digits we need:

$$[\log_n(m)]$$

Example 1.1 *How many digits do we need in base* 2 *to write* 16 *numbers?*

$$[\log_2(16)] = 4$$

So we need 4 *digits to write* 16 *numbers in base* 2*:*

$$a_3a_2a_1a_0 = \sum_{i=0}^{3} a_i \cdot 2^i \qquad a_i \in \mathbb{F}_2$$

1.2 Irreducible or prime polynomial

Let $f(x)$ a polynomial over a field $\mathbb{K}$:

$$f(x) \in \mathbb{K}[x]$$

Definition 1.1 (Irreducible or prime polynomial)
$f(x)$ is said to be an irreducible or prime polynomial in $\mathbb{K}[x]$ when the polynomial cannot be written as a product of two polynomials of smaller degree with coefficients over the field $\mathbb{K}$.

1.3 Primitive-part and content of a polynomial

Definition 1.2 (Integral domain)
Is a non-zero commutative ring in which the product of non-zero elements is non-zero.

Definition 1.3 (Unique Factorization Domain (UFD))
A UFD is a integral domain in which every non-zero non-unit element can be written as a product of prime elements (or irreducible elements) uniquely up to order and units.

Definition 1.4 (Content of a polynomial with integer coefficients)
The content of a polynomial with integer coefficients (or, more generally, with coefficients in a unique factorization domain) is the greatest common divisor of its coefficients.

Example 1.2 *The content of the polynomial* $p(x) = -60+36\cdot x-24\cdot x^2+4\cdot x^3$ *is* 4*:*

$$\mathrm{mcd}(-60, 36, -24, 4) = 4$$

so $p(x) = 4 \cdot (-15 + 8 \cdot x - 6 \cdot x^2 + x^3)$*.*

Definition 1.5 (Primitive part of a polynomial with integer coefficients)
The primitive part of a polynomial with integer coefficients is the quotient of the polynomial by its content. Thus a polynomial is the product of its primitive part and its content, and this factorization is unique up to the multiplication of the content by a unit of the ring of the coefficients (and the multiplication of the primitive part by the inverse of the unit).

Example 1.3 *As the content of the polynomial* $p(x) = -60 + 36 \cdot x - 24 \cdot x^2 + 4 \cdot x^3$ *is* 4 *then the primitive-part for the polynomial is:*

$$-15 + 8 \cdot x - 6 \cdot x^2 + x^3$$

1.4 Primitive polynomials

Definition 1.6 (Primitive polynomial)
A polynomial is primitive if its content equals 1 *so the primitive-part and the polynomial are the same.*

Lemma 1.1 (Gauss's lemma (primitivity))
If $p(x)$ and $q(x)$ are primitive polynomials in $\mathbb{Z}[x]$ then $p(x) \cdot q(x)$ is also a primitive polynomial.

Lemma 1.2 (Gauss's lemma (irreducibility))
A non-constant polynomial in $\mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ if and only if it is both irreducible in $\mathbb{Q}[x]$ and primitive in $\mathbb{Z}[x]$.

1.5 Eisenstein's irreductible criterion

Let $p(x) \in \mathbb{Z}[x]$ a polynomial with integer coefficients:

$$p(x) = \sum_{i=0}^{n} a_i \cdot x^i \qquad a_i \in \mathbb{Z} \quad \forall i$$

If there is a prime number $p \in \mathbb{Z}$ such the following three conditions are all true:

- p divides each a_i when $0 \leq i < n$.
- p does not divide a_n.
- p^2 does not divide a_0.

then $p(x)$ is irreducible over the rational numbers[1].

1.6 Cyclotomic polynomials

Cyclotomic polynomials are a class of polynomials whose irreducibility can be established using Eisenstein's criterion (section (1.5)) is that of the cyclotomic polynomials for prime numbers p.

[1]It will also be irreducible over the integers, unless all its coefficients have a nontrivial factor in common (in which case $p(x)$ as integer polynomial will have some prime number, necessarily distinct from p, as an irreducible factor). The latter possibility can be avoided by first making $p(x)$ primitive, by dividing it by the greatest common divisor of its coefficients (the content of $p(x)$). This division does not change whether $p(x)$ is reducible or not over the rational numbers (see Primitive part–content factorization for details), and will not invalidate the hypotheses of the criterion for p (on the contrary it could make the criterion hold for some prime, even if it did not before the division).

Definition 1.7 (Cyclotomic polynomial)
Such a polynomial is obtained by dividing the polynomial $x^p - 1$ by the linear factor $x - 1$, corresponding to its obvious root 1 (which is its only rational root if $p > 2$):

$$\frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i$$

Chapter 2

Polynomials over Finite Fields

Let $f(x)$ a polynomial in $\mathbb{F}_p[x]$:

$$f(x) = \sum_{i=0}^{n} a_i \cdot x^i \qquad a_i \in \mathbb{F}_p \quad \forall i$$

2.1 How many polynomials of degree n exist in $\mathbb{F}_p[x]$?

A polynomial of degree n in $\mathbb{F}_p[x]$ can be expressed as:

$$(1, a_{n-1}, a_{n-2}, \ldots, a_1, a_0) \qquad a_i \in \mathbb{F}_p \quad \forall i$$

So with n digits m numbers can be written[1] in base p:

$$[\log_p(m) = n]$$

Example 2.1 *How many polynomials of degree 4 exist in $\mathbb{F}_2[x]$?*

A polynomial of degree 4 has 5 coefficients so:

$$p(x) = x^4 + \sum_{i=0}^{3} a_i \cdot x^i \qquad a_i \in \mathbb{F}_2 \quad \forall i$$

As the coefficient for the $4th$ power is always 1 there are 4 coefficients available:

$$[\log_2(16)] = 4$$

There are 16 polynomials of degree 4 in $\mathbb{F}_2[x]$.

[1] See section (1.1)

2.2 Irreducible polynomials in $\mathbb{F}_p[x]$

Polynomial	**Factorization**	**Irreducible**	**Primitive**
x^4	$x \cdot x \cdot x \cdot x$	No	No
x^4+1	$(x+1)^4$	No	No
x^4+x	$x \cdot (x^3+1)$	No	No
x^4+x+1	(x^4+x+1)	Yes	Yes
x^4+x^2	$x^2 \cdot (x+1)^2$	No	No
x^4+x^2+1			No
x^4+x^2+x			No
x^4+x^2+x+1			No
x^4+x^3	$x^3 \cdot (x+1)$	No	No
x^4+x^3+1			No
x^4+x^3+x			No
x^4+x^3+x+1			No
$x^4+x^3+x^2$			No
$x^4+x^3+x^2+1$			No
$x^4+x^3+x^2+x$			No
$x^4+x^3+x^2+x+1$			No

Table 2.1: Polynomials of degree 4 in $\mathbb{F}_2[x]$.