

FIELDS OF ORDER 2^n

Let F be a field, and let $F[x]$ be the ring of polynomials with coefficients in F . This ring admits a division with remainder, similar to the Euclidean algorithm for integers. More precisely, if $a(x)$ and $b(x) \neq 0$ are two polynomials, then there exist polynomials $q(x)$ and $r(x)$ such that

$$a(x) = q(x)b(x) + r(x)$$

where $r(x) = 0$ or $\deg(r) < \deg(b)$. If $r(x) = 0$ then we say that $b(x)$ divides $a(x)$. This algorithm is particularly easy to perform if $F = \mathbb{F}_2$, which we assume in the rest of this section. Take for example $a(x) = x^6 + x^3 + x$ and $b(x) = x^3 + x + 1$. Then the remainder $r(x)$ can be determined by the following steps. The leading terms of $a(x)$ and $b(x)$ are x^6 and x^3 . Then $x^6/x^3 = x^3$ and we can subtract $x^3b(x)$ from $a(x)$:

$$x^6 + x^3 + x - x^3(x^3 + x + 1) = x^4 + x.$$

Repeating the same procedure with $x^4 + x$ (instead of $x^6 + x^3 + x$) gives

$$x^4 + x - x(x^3 + x + 1) = x^2.$$

Since the degree of x^2 is smaller than the degree of $x^3 + x + 1$, this is the remainder. Indeed, adding the two equations gives

$$x^6 + x^3 + x = (x^3 + x)(x^3 + x + 1) + x^2.$$

The greatest common divisor of $a(x)$ and $b(x)$ is defined to be the common divisor of $a(x)$ and $b(x)$ with the greatest degree. If $d(x) = \gcd(a(x), b(x))$ then there exist polynomials $\alpha(x)$ and $\beta(x)$ such that

$$\alpha(x)a(x) + \beta(x)b(x) = d(x)$$

This is proved using the division algorithm, essentially in the same way as the proof of the fundamental theorem of arithmetic. For example, assume that $a(x) = x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^2$. Then

$$a(x) = (x^2 + x + 1)b(x) + (x + 1)$$

and dividing $b(x)$ by $r(x) = x + 1$ gives

$$b(x) = (x + 1)r(x) + 1.$$

This shows that $\gcd(x^4 + x^3 + x^2 + x + 1, x^2) = 1$ and, by substituting $r(x) = a(x) - (x^2 + x + 1)b(x)$ in the second equation, we get

$$(x + 1)a(x) + x^3b(x) = 1.$$

Fix a polynomial $p(x)$. We say that $a(x)$ and $b(x)$ are congruent modulo $p(x)$ and write $a(x) \equiv b(x) \pmod{p(x)}$ if $p(x)$ divides $a(x) - b(x)$. Every polynomial $a(x)$ is congruent to its remainder $r(x)$ when divided by $p(x)$. Thus the congruence classes (modulo $p(x)$) are represented by all polynomials of degree strictly smaller than the degree of $p(x)$. This is a finite set whose cardinality can be easily determined. Assuming that the degree of $p(x)$ is n then any polynomial of degree $n - 1$ or less can be written as

$$a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

where $a_i = 0$ or 1 for every i since $\mathbb{F}_2 = \{0, 1\}$. In particular, we have 2 choices for each of n coefficients. Thus the number of all polynomials of degree $n - 1$ or less is equal to 2^n . For example, if $p(x) = x^3 + x + 1$ then the possible remainders are the following eight polynomials

$$0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1.$$

We can add and multiply polynomials modulo $p(x)$. The addition, in terms of the eight remainders, is trivial and amounts to adding coefficients as usual. The multiplication is more interesting. For example, we have

$$x \cdot x^2 = x^2 \cdot x = x^3 \equiv x + 1 \pmod{x^3 + x + 1}$$

and

$$x^2 \cdot x^2 = x^4 \equiv x^2 + x \pmod{x^3 + x + 1}$$

From these we can easily work out the whole multiplication table modulo $x^3 + x + 1$.

| | | | | | | | |
|---------------|---------------|---------------|---------------|---------------|---------------|---------------|---------------|
| \cdot | 1 | x | $x + 1$ | x^2 | $x^2 + 1$ | $x^2 + x$ | $x^2 + x + 1$ |
| 1 | 1 | x | $x + 1$ | x^2 | $x^2 + 1$ | $x^2 + x$ | $x^2 + x + 1$ |
| x | x | x^2 | $x^2 + x$ | $x + 1$ | 1 | $x^2 + x + 1$ | $x^2 + 1$ |
| $x + 1$ | $x + 1$ | $x^2 + x$ | $x^2 + 1$ | $x^2 + x + 1$ | | | |
| x^2 | x^2 | $x + 1$ | $x^2 + x + 1$ | $x^2 + x$ | x | $x^2 + 1$ | 1 |
| $x^2 + 1$ | $x^2 + 1$ | | | | $x^2 + x + 1$ | | |
| $x^2 + x$ | $x^2 + x$ | $x^2 + x + 1$ | | | | | |
| $x^2 + x + 1$ | $x^2 + x + 1$ | | | | | | |

If you complete this table, you will see that any polynomial not divisible by $x^3 + x + 1$ has a multiplicative inverse modulo $x^3 + x + 1$. (For example, the table tells you that the inverse of x is $x^2 + 1$.) Thus the set of congruence classes of polynomials in $\mathbb{F}_2[x]$ modulo $x^3 + x + 1$ is a field of order 8.

We say that a polynomial $p(x)$ in $F[x]$ (F is now any field) is irreducible or prime if it cannot be factored into a product of two or more polynomials of smaller degrees. We claim that $x^3 + x + 1$ is irreducible, in $\mathbb{F}_2[x]$. If not then it has to be a product of two polynomials of degrees 1 and 2, as $1 + 2 = 3$ is the only way to write 3 as a sum of two smaller positive integers:

$$x^3 + x + 1 = (x - c)(x^2 + px + q).$$

But then $c \in \mathbb{F}_2$ would have to be a root of $x^3 + x + 1$. This is a contradiction since neither 0 nor 1 is a root of $x^3 + x + 1$. Now, if $p(x)$ is prime, then the ring of polynomials modulo $p(x)$ is a field. This is a consequence of the division algorithm for polynomials. It is proved in the same way as the corresponding fact(s) for $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Indeed, if $a(x)$ is a polynomial of degree less than the degree of $p(x)$ then $\gcd(a(x), p(x)) = 1$ since $p(x)$ is prime and it clearly does not divide $a(x)$. Then

$$\alpha(x)a(x) + \beta(x)p(x) = 1$$

for some polynomials $\alpha(x)$ and $\beta(x)$. In particular $\alpha(x)$ is the inverse of $a(x)$ modulo $p(x)$.

In particular, in order to construct a field of order 2^n we need to find an irreducible polynomial in $\mathbb{F}_2[x]$ of degree n . For example, $x^4 + x^3 + x^2 + x + 1$ is irreducible (see the exercise), therefore we have an explicit construction of a finite field of order 16. For every n there is unique field of order 2^n denoted by \mathbb{F}_{2^n} . We shall not prove this fact.

HW due 02/09/2009

1) Complete the above multiplication table for the field \mathbb{F}_8 realized as polynomials in $\mathbb{F}_2[x]$ modulo $x^3 + x + 1$.

2) Show that the polynomial $x^4 + x^3 + x^2 + x + 1$ cannot be factored into two degree 2 polynomials

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

in $\mathbb{F}_2[x]$. (This is the hardest part to show that $x^4 + x^3 + x^2 + x + 1$ is irreducible.)