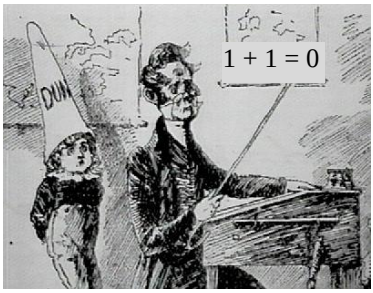
11. $\mathbb{Z}_2$ POLYNOMIALS AND CRYPTOGRAPHY

§11.1. $\mathbb{Z}_2$ The Fool's Field

The field $\mathbb{Z}_2$, of integers modulo 2, has been called the "fool's field". That's because $\mathbb{Z}_2$ arithmetic is ridiculously simple and 'forgives' many blunders that cause problems in ordinary arithmetic.



There are just two numbers in $\mathbb{Z}_2$: 0 and 1. Arithmetic in $\mathbb{Z}_2$ works just as in ordinary arithmetic except that 1 + 1 = 0. If you let 0 represent the even numbers and 1 the odd numbers, $\mathbb{Z}_2$ is just the odd-even system where 1 + 1 = 0 reflects the fact that odd + odd = even.

Anyone can learn his tables in the $\mathbb{Z}_2$ system because they are simply:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Because 2 = 0 in this system, –1 = 1, so subtraction is the same as addition. Errors in signs which plague many students' work, simply cannot arise in $\mathbb{Z}_2$. And if in doubt

about the answer to an arithmetic calculation you can always guess and have a 50-50 chance of being correct!

The dunce who believes that $(a + b)^2$ is just $a^2 + b^2$ is actually correct if the arithmetic is being done in $\mathbb{Z}_2$ because the missing term of $2ab$ is equal to zero in $\mathbb{Z}_2$.

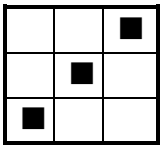
Induction, that often difficult process by which we can prove that something is true for all integers is totally unnecessary in $\mathbb{Z}_2$ because to prove something for all $n \in \mathbb{Z}_2$ you only need to check $n = 0$ and $n = 1$. For example if k is a positive integer, $n^k = n$ for all $n \in \mathbb{Z}_2$ simply because $0^k = 0$ and $1^k = 1$. Consequently the binomial theorem collapses to $(a + b)^n = a + b$ in $\mathbb{Z}_2$.

Is $\mathbb{Z}_2$ just a baby arithmetic for the fool who can't cope with the ordinary one? In fact $\mathbb{Z}_2$, for all its simplicity, leads to some powerful, and very useful, mathematical systems. The field $\mathbb{Z}_2$ is a model for any device that's capable of being in one of two possible states, just as a light globe can be either on or off.

The memory of a computer is made up of millions of tiny devices, each of which can store a 0 or a 1. The word that's used to refer to one of these indivisible atoms of memory is the **bit**. Using blocks of bits the computer memory can store numbers, text and even pictures.

A block of memory can store a sequence of 0's and 1's which, depending on the context, can represent a number, a fragment of text or a piece of graphics. And a sequence of 0's and 1's can be considered to be a $\mathbb{Z}_2$ polynomial.

For example the sequence 001010100 could be the binary representation of the number 84, or the code that represents a capital T, and it could represent the graphics pattern:



This sequence 001010100 could also be considered as representing the polynomial $0x^8 + 0x^7 + 1x^6 + 0x^5 + 1x^4 + 0x^3 + 1x^2 + 0x + 0$, or more simply, $x^6 + x^4 + x^2$. Polynomials have a richer algebraic structure than just sequences and this richer structure has be exploited in the science of cryptography.

Cryptography, the science of secret codes, has been around for centuries as a military tool but in the last couple of decades it has become of vital concern to the business world. Large volumes of sensitive data is now piped around computer networks, along telephone optical fibres and into the aether via sattelite connections.

Various branches of algebra, combinatorics and number theory have been drawn upon to create cryptographic systems. One such area is the algebra of polynomials over finite fields such as $\mathbb{Z}_2$.

§11.2. Irreducible $\mathbb{Z}_2$ Polynomials

With so few coefficients available it's a feasible task to enumerate all $\mathbb{Z}_2$ polynomials up to a certain degree.

Zero Polynomial: 0
Non-Zero Constant Polynomials: 1
Linear Polynomials: x, $x+1$
Quadratics: x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$.
Cubics: x^3, $x^3 + 1$, $x^3 + x$, $x^3 + x + 1$,
$x^3 + x^2$, $x^3 + x^2 + 1$, $x^3 + x^2 + x$, $x^3 + x^2 + x + 1$.

Finding the zeros of a polynomial in $\mathbb{Z}_2$[x] requires no special techniques or fancy formulae. After all there are only two possibilities: 0 and 1. Just try them both!

Example 1: Find the zeros of $f(x) = x^5 + x^4 + x + 1$ in $\mathbb{Z}_2$.
Solution: $f(0) = 1$; $f(1) = 1 + 1 + 1 + 1 = 0$. So 1 is the only zero for f.

NOTE: Testing for $x = 0$ means just looking to see whether the constant term is zero and testing for $x = 1$ simply means counting the number of terms and deciding whether it's even or odd.

A non-constant polynomial is **irreducible**, or **prime**, if it can't be factorised as a product of polynomials of lower degree. (It's **reducible**, or **composite**, if no such factorisation is possible.)

In a more general context the meanings of prime and irreducible are distinct and it's a theorem that for polynomials they are equivalent. Since polynomials are all we're concerned about here we'll use the words as synonyms.

Theorem 1: For any field of coefficients F, polynomials in F[x] are irreducible if:
(1) they are linear (i.e. have degree 1) or
(2) they are quadratics or cubics with no zeros in F.
Proof: Suppose that a(x) = b(x) c(x) where b and c have lower degrees than a.
Then deg a = deg b + deg c and so the degrees of b,c must be positive.
(1) If deg a = 1 we get a contradiction since 1 can't be written as the product of two positive integers.
(2) If deg a = 2 or 3 and a(x) has no zeros in F, then it has no factors of degree 1. This leads to a contradiction since neither 2 nor 3 can be written as the product of two integers which are both bigger than 1. ☺

NOTE: Once the degree of a polynomial is 4 or more it's no longer so easy to decide whether the polynomial is irreducible because a polynomial of degree 4 could be the

product of two irreducible quadratics. Having no zeros doesn't prove irreducibility unless the degree is 2 or 3.

Example 2: Does the real polynomial $x^4 + 2x^2 + 1$ have any (real) zeros? Is it irreducible?
Solution: Writing it as $(x^2 + 1)^2$ we can immediately see that although it has no zeros in **R**, it is not irreducible.

Example 3: Which of the $\mathbb{Z}_2$ polynomials listed above are irreducible?
Solution: Firstly we must eliminate the two constant polynomials 0 and 1 because being non-constant is a precondition for being irreducible. Since the remaining ones have degree no greater than 3 we can use Theorem 1 to eliminate those which either have zero constant term or have an even number of terms. This leaves:
x, $x+1$, $x^2 + x + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$
as the irreducibe $\mathbb{Z}_2$ polynomials up to degree 3.

Example 4:
Find the irreducible $\mathbb{Z}_2$ polynomials of degree 4.
Solution: As above we can eliminate those whose constant term is zero or which have an even number of terms. Those that remain are:
$x^4 + x + 1$, $x^4 + x^2 + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$.
But we must also eliminate those which are the product of two irreducible quadratics (or the square of one of them). Fortunately we already know about irreducible quadratics over $\mathbb{Z}_2$. There's only one of them: $x^2 + x + 1$.

So we must eliminate $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ (the other 3 terms can be ignored because they have a coefficient of 2). The irreducible $\mathbb{Z}_2$ quartics are thus:
$x^4 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x^3 + x^2 + x + 1$.

§11.3. Complex $\mathbb{Z}_2$ Numbers

Cast your mind back to the time when you first learnt about complex numbers. Your whole world of numbers up to then was the field of real numbers. There were many polynomial equations which had no solutions such as $x^2 + 1 = 0$. What we did was to invent solutions for this polynomial. A new 'imaginary' number i was introduced to provide a solution and we combined this number with the existing real numbers to form complex numbers $x + iy$. We were then able to do arithmetic in this larger system just using the relation $i^2 = -1$.

It turned out that this new system was extremely well behaved. Not only was it again a field, but we had somehow reached a state of algebraic perfection. Although in principle we could have repeated the process — finding yet another equation with no solutions and inventing further numbers, we cannot in fact find any polynomial equation that lacks solutions. The Fundamental Theorem of Algebra states that every non-constant polynomial over $\mathbb{C}$ has a solution in $\mathbb{C}$. This property of $\mathbb{C}$ is often referred to by saying that $\mathbb{C}$ is algebraically closed.

Our little field $\mathbb{Z}_2$ is pitifully small. Can we extend it in a way that is analogous to the creation of the complex numbers from the reals?

For a start there is no point in trying to introduce a square root of –1 because $\mathbb{Z}_2$ already has one. Remember that –1 = 1 in $\mathbb{Z}_2$ and $\mathbb{Z}_2$ has a square root of 1. So $x^2 + 1$ is the wrong polynomial to use.

But $\mathbb{Z}_2$ *does* have polynomials without zeros in $\mathbb{Z}_2$. The one of lowest degree is $x^2 + x + 1$. So we invent a new number that we'll call 't' for which $t^2 + t + 1 = 0$ and we'll combine this number t with the existing numbers 0 and 1 to obtain a system of $\mathbb{Z}_2$ 'complex' numbers. We carry out arithmetic on this system using the relation 1 + 1 = 0 for the coefficients and $t^2 + t + 1 = 0$. This last relation is perhaps more conveniently expressed as $t^2 = –1 – t = 1 + t$.

There are just four numbers we can produce in this way: 0, 1, t and 1+ t. We'll use the notation $\mathbb{Z}_2[t \mid t^2 = 1 + t]$ as the name of this system. Using this notation we could have written the complex number field as $\mathbb{R}[i \mid i^2 = –1]$ instead of $\mathbb{C}$.

Example 5: Simplify $(1 + t)^3$ in the system $\mathbb{Z}_2[t \mid t^2 = 1 + t]$.
Solution: $(1 + t)^2 = 1 + t^2$ (remember why we ignore the 2t term)

$$= 1 + 1 + t = t.$$

Hence $(1 + t)^3 = (1 + t)t = t + t^2 = t + 1 + t = 1$.

Example 6: Simplify $(1 + t)^{100}$ in the above system.
Solution: Since $(1 + t)^3 = 1$, $(1 + t)^{99} = 1$ and so $(1 + t)^{100} = 1 + t$.

Example 7: Construct the addition and multiplication tables for $\mathbb{Z}_2[t \mid t^2 = 1 + t]$.
Solution:

+	0	1	t	1+t
0	0	1	t	1+t
1	1	0	1+t	t
t	t	1+t	0	1
1+t	1+t	t	1	0

×	0	1	t	1+t
0	0	0	0	0
1	0	1	t	1+t
t	0	t	1+t	1
1+t	0	1+t	1	t

Like the system of ordinary complex numbers, this system is a field. You can see from the multiplication table that every non-zero element has a multiplicative inverse: 1 is its own inverse and t and 1 + t are inverses of each other. But $\mathbb{Z}_2[t \mid t^2 = 1 + t]$ is nowhere near as perfect as $\mathbb{C}$. It is not algebraically closed. Having provided $x^2 + x + 1$ with solutions we continue to have polynomial equations without any.

Example 8: Show that the equation $x^3 - t = 0$ has no solutions in $\mathbb{Z}_2[t \mid t^2 = 1 + t]$.
Solution: All we have to do is to cube each of the four elements in turn.
$0^3 = 0$; $1^3 = 1$; $t^3 = 1$; $(1 + t)^3 = 1$. In no case do we get t. Therefore $x^3 - t$ has no solution in $\mathbb{Z}_2[t \mid t^2 = 1 + t]$.

Of course we could extend $\mathbb{Z}_2[t \mid t^2 = 1 + t]$ by a new number s such that $s^3 = t$. This would be $\mathbb{Z}_2[t \mid t^2 = 1 + t][s^3 = t]$. We could write this as $\mathbb{Z}_2[s \mid s^6 = 1 + s^3]$. We could keep extending $\mathbb{Z}_2$ more and more but we would never reach an algebraically closed field. However if we took the union of an infinite tower of these extensions we would obtain an algebraically closed field.

Example 9: Show that $f(x) = x^3 + x + 1$ has no zeros in $\mathbb{Z}_2[t \mid t^2 = 1 + t]$.
Solution: Again we just check each possibility.
$f(0) = 1$; $f(1) = 1$; $f(t) = 1 + t + 1$; $f(1 + t) = 1 + (1 + t) + 1 = 1 + t$.

So it's not just the fact that extending the field gives us more polynomials to solve, but even ones that were already there fail to have solutions. $\mathbb{Z}_2[t \mid t^2 = 1 + t]$ has a long way to go before it becomes algebraically closed.

We could now take either of the above polynomials (any irreducible polynomial in fact) and extend the field

further by inventing more numbers. Or, we could go back to $\mathbb{Z}$ and seek to extend it in some other way.

$\mathbb{Z}_2[t \mid t^2 = 1 + t]$ is not the only extension of $\mathbb{Z}$ that we can obtain by the above process. Take any irreducible $\mathbb{Z}_2$ polynomial of degree n, invent a solution for it, combine it with 0, 1 in all possible ways, and hey presto! We will have constructed a field with 2^n elements.

Suppose we do this with the irreducible polynomial $x^3 + x + 1$. Let's invent the number 's' which satisfies the relation $s^3 + s + 1 = 0$, or equivalently, $s^3 = s + 1$. Combining this with 0 and 1 we get not only s and 1 + s but also s^2, $s^2 + 1$, $s^2 + s$ and $s^2 + s + 1$. Only when we get to s^3 can we break it down into lower powers. So this gives us a field of size 8.

§11.4. Extensions of $\mathbb{Z}_2$ and Cryptography

A piece of data can be encoded as a sequence of 0's and 1's which can be broken ino blocks of size n. Each of these blocks can be considered to be a $\mathbb{Z}_2$ polynomial of degree $\leq n$.

Example 10: Represent the sequence 11001001 as a sequence of $\mathbb{Z}_2$ polynomials using:
(a) blocks of size 8;
(b) blocks of size 4;
(c) blocks of size 2.
Solution:

(a) 11001001 can be represented by the $\mathbb{Z}_2$polynomial $x^7 + x^6 + x^3 + 1$.

(b) 11001001 can be broken into two blocks of length 4: 1100 1001 which can be represented by the pair of $\mathbb{Z}_2$ polynomials $x^3 + x^2$, $x^3 + 1$.

(c) Using blocks of size 2 we get the sequence of polynomials: $x + 1$, 0, x, 1.

There are many ways of using the algebra of finite fields in cryptography, some more sophisticated and complicated than others. To give the flavour of these techniques while avoiding the technicalities, we consider here a fairly unsophisticated technique.

Binary data is broken into blocks of length n. Two polynomials p(x) and e(x) are chosen. The first, p(x) has to be an irreducible polynomial of degree n while c(x) is a polynomial of degree less than n.
The arithmetic is carried out in the field $\mathbb{Z}_2[z \mid p(z) = 0]$. To encode a block we consider it to be a polynomial of degree less than n and substitute z to obtain m(z). Now we multiply m(z) by e(z) and simplify, ending up with a polynomial expression in z up to z^{n-1}. This is converted back to a sequence of 0's and 1's and it is this sequence which is transmitted as the coded text.

Example 11: Using a block size of 2, the irreducible polynomial $p(x) = x^2 + x + 1$ and the encoding polynomial $e(x) = x$, encode the binary message 11011100.

Solution: The arithmetic is performed in the field $\mathbb{Z}_2 [t \mid t^2 = 1 + t]$. (We shall use the symbol t to which we have become accustomed instead of the generic z.)

Breaking the message into blocks of length 2 we get 11 01 11 00. As polynomials, these become $x + 1$, 1, $x + 1$, 0. Substituting $x = t$ gives $1 + t$, 1, $1 + t$, 0. Multiplying by $e(t) = t$ gives: $t + t^2$, t, $t + t^2$, 0. Simplifying we get 1, t, 1, 0. Converting back to a binary sequence gives 01100100 which is the encoded message.