

## FINITE FIELDS OF THE FORM GF(p)

Finite fields play crucial role in many crypto algorithms. It can be shown that the order of a finite field must be a power of a prime  $p^n$ , where  $n$  is a positive integer. Prime is an integer whose only positive integer factors are itself and 1. The finite field of order  $p^n$  is usually denoted by  $GF(p^n)$ ; GF stands for Galois field in honor of the French mathematician Evarist Galois (1811-1832, <http://scienceworld.wolfram.com/biography/Galois.html> ).

### Finite Fields of Order p

For a given prime  $p$ ,  $GF(p)$  is defined as the set  $Z_p = \{0, 1, \dots, p-1\}$  of integers together with arithmetic operations modulo  $p$ . For such prime numbers, holds (M7) - Multiplicative inverse axiom.

Because elements  $w$  of  $Z_p$  are relatively prime to  $p$ , if we multiply all the elements of  $Z_p$  by  $w$ , the resulting residues are all of elements  $Z_p$ , permuted. Thus, exactly one of the residues has the value 1, respective multiplier is just the inverse element for  $w$ , designated  $w^{-1}$ . Now, equation (4.2) can be written without condition:

$$\text{If } ab \equiv ac \pmod{p} \text{ then } b \equiv c \pmod{p} \quad (4.4)$$

Consequence is obtained by multiplication of both parts of (4.4) by  $a^{-1}$ .

The simplest finite field is  $GF(2)$ :

+	0	1
0	0	1
1	1	0

Addition

X	0	1
0	0	0
1	0	1

Multiplication

w	-w	$w^{-1}$
0	0	-
1	1	1

Inverses

## Finite Fields of Order p (CONT 1)

Next is for GF(7):

Table 4.3 Arithmetic in GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

	$w$	$-w$	$w^{-1}$
0	0	0	—
1	1	6	1
2	2	5	4
3	3	4	5
4	4	3	2
5	5	2	3
6	6	1	6

(c) Additive and multiplicative inverses modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

### Finding the Multiplicative Inverse in GF(p)

Table 4.3b may be used to find multiplicative inverse, but for large values of p it is not practical.

If  $\gcd(m,b)=1$ , then b has a multiplicative inverse modulo m. That is, for positive integer  $b < m$ , there exists a  $b^{-1} < m$  such that  $b b^{-1} = 1 \pmod m$ . Euclid's algorithm can be extended so that, in addition to finding  $\gcd(m,b)$ , if the gcd is 1, the algorithm returns the multiplicative inverse of b.

## Finding the Multiplicative Inverse in GF(p) (CONT 1)

EXTENDED EUCLID(m,b)

1.  $(A1,A2,A3):=(1,0,m)$ ;  $(B1,B2,B3):=(0,1,b)$ ;
2. if  $B3=0$  return  $A3=\text{gcd}(m,b)$ ; no inverse
3. if  $B3=1$  return  $B3 = \text{gcd}(m,b)$ ;  $B2= b^{-1} \text{ mod } m$
4.  $Q=\left\lfloor \frac{A3}{B3} \right\rfloor$
5.  $(T1,T2,T3):=(A1-QB1, A2-QB2, A3-QB3)$
6.  $(A1,A2,A3):= (B1,B2,B3)$
7.  $(B1,B2,B3):= (T1,T2,T3)$
8. goto 2

Throughout the computation, the following relationships hold:

$$mT1+bT2=T3 \quad mA1+bA2=A3 \quad mB1+bB2=B3$$

To see that algorithm correctly returns  $\text{gcd}(m,b)$ , note that if we equate A and B in Euclid's algorithm with  $A3$  and  $B3$  in the extended Euclid's algorithm, then the treatment of the two variables is identical. Note also that if  $\text{gcd}(m,b)=1$ , then on the final step we would have  $B3=0$  and  $A3=1$ . Therefore, on the preceding step,  $B3=1$ . But if  $B3=1$ , then we can say the following:

$$mB1+bB2=B3$$

$$mB1+bB2=1$$

$$bB2=1-mB1$$

$$bB2 \equiv 1 \pmod{m}$$

Hence,  $B2$  is the multiplicative inverse of  $b$ .

Table 4.4 is an example of the execution of the algorithm. It shows that  $\text{gcd}(550,1759)=1$  and that the multiplicative inverse of 550 is 355; that is,  $550 \times 355 \equiv 1 \pmod{1759}$ .

## Finding the Multiplicative Inverse in GF(p) (CONT 2)

Table 4.4 Finding the Multiplicative Inverse of 550 in GF(1759)

Q	A1	A2	A3	B1	B2	B3
—	1	0	1759	0	1	550
3	0	1	550	1	-3	109
5	1	-3	109	-5	16	5
21	-5	16	5	106	-339	4
1	106	-339	4	-111	355	1

## POLYNOMIAL ARITHMETIC

We are concerned with polynomials in a single variable  $x$ , and we can distinguish three classes of polynomial arithmetic:

- Ordinary polynomial arithmetic, using the basic rules of algebra
- Polynomial arithmetic in which the arithmetic on the coefficients is performed modulo  $p$ ; that is, coefficients are in  $\mathbb{Z}_p$
- Polynomial arithmetic in which the coefficients are in  $\mathbb{Z}_p$ , and the polynomials are defined modulo a polynomial  $m(x)$  whose highest power is some integer  $n$

We consider these variants below.

### Ordinary Polynomial Arithmetic

A polynomial of degree  $n$  (integer  $n \geq 0$ ) is an expression of the form

$$f(x) = \sum_{i=0}^n a_i x^i$$

where  $a_i$  are elements of some designated set of numbers  $S$ , called the coefficient set, and  $a_n \neq 0$ . We say that polynomials are defined over  $S$ .

## POLYNOMIAL ARITHMETIC (CONT 1)

A zeroth-degree is called a constant polynomial and is simply an element of  $S$ . An  $n$ -th degree polynomial is said to be a monic polynomial if  $a_n = 1$ .

In the context of abstract algebra, we are usually not interested in evaluating a polynomial for a particular value of  $x$  [e.g.,  $f(7)$ ]. To emphasize this point, the variable  $x$  is sometimes referred to as the indeterminate.

Polynomial arithmetic includes the operations of addition, subtraction, and multiplication:

$$f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^m b_i x^i, n \geq m,$$

$$f(x) + g(x) = \sum_{i=0}^n (a_i + b_i) x^i + \sum_{i=m+1}^n a_i x^i$$

$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i,$$

$$c_k = \sum_{i=0}^k a_i b_{k-i}$$

Division is similarly defined, but requires that  $S$  be a field. Examples of fields include the real numbers, rational numbers, and  $\mathbb{Z}_p$  for  $p$  prime. Note that the set of all integers is not a field and does not support polynomial division.

### Polynomial Arithmetic with Coefficients in $\mathbb{Z}_p$

Within a field, given two elements  $a$  and  $b$ , the quotient  $a/b$  is also an element of the field. However, in general division will result in quotient and remainder; that is, not exact division.

If the coefficient set  $S$  is integers, then  $(5x^2)/(3x)$  does not have a solution, because it would require a coefficient with the value of  $5/3$ , which is not

## Polynomial Arithmetic with Coefficients in $Z_p$

### (CONT 1)

in the coefficient set. Suppose, we perform the same polynomial division over  $Z_7$ . Then we have  $(5x^2)/(3x)=4x$ , which is a valid polynomial over  $Z_7$ .

However, in general, even if the coefficient set is a field, division will produce quotient and remainder:

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

$$f(x) = q(x)g(x) + r(x) \quad (4.5)$$

If the degree of  $f(x)$  is  $n$  and degree of  $g(x)$  is  $m$ , ( $m \leq n$ ), then the degree of the quotient  $q(x)$  is  $n-m$  and the degree of the remainder  $r(x)$  is at most  $m-1$ . With the understanding that remainders are allowed, we can say that the polynomial division is possible if the coefficient set is a field.

In an analogy to integer arithmetic, we can write  $f(x) \bmod g(x)$  for the remainder  $r(x)$  in (4.5), that is,  $r(x) = f(x) \bmod g(x)$ . If remainder  $r(x)=0$ , then we say that  $g(x)$  divides  $f(x)$ , written as  $g(x)|f(x)$ ; equivalently, we can say that  $g(x)$  is a factor of  $f(x)$  or  $g(x)$  is a divisor of  $f(x)$ .

If  $f(x) = x^3 + x^2 + 2$ ,  $g(x) = x^2 - x + 1$ ,  $f(x)/g(x)$  produces quotient  $q(x)=x+2$ , and remainder  $r(x)=x$ , as shown in Fig. 4.3d. This clearly verified by

$$q(x)g(x) + r(x) = (x+2)(x^2 - x + 1) + x = (x^3 + x^2 - x + 2) + x = x^3 + x^2 + 2 = f(x)$$

# Polynomial Arithmetic with Coefficients in $\mathbb{Z}_p$

## (CONT 2)

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ + (x^2 - x + 1) \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

(a) Addition

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ - (x^2 - x + 1) \\ \hline x^3 \quad + x + 1 \end{array}$$

(b) Subtraction

$$\begin{array}{r} x^3 + x^2 \quad + 2 \\ \times (x^2 - x + 1) \\ \hline x^3 + x^2 \quad + 2 \\ -x^4 - x^3 \quad - 2x \\ \hline x^5 + x^4 \quad + 2x^2 \\ \hline x^5 \quad + 3x^2 - 2x + 2 \end{array}$$

(c) Multiplication

$$\begin{array}{r} x^2 - x + 1 \overline{) x^3 + x^2 + 2} \\ \underline{x^3 + x^2 + x} \phantom{+ 2} \\ 2x^2 - x + 2 \\ \underline{2x^2 - 2x + 2} \\ x \end{array}$$

(d) Division

Figure 4.3 Examples of Polynomial Arithmetic

For our purposes, polynomials over  $\text{GF}(2)$  are of the most interest. Fig.4.4 shows an example of polynomial arithmetic over  $\text{GF}(2)$ :

# Polynomial Arithmetic with Coefficients in $\mathbb{Z}_p$

## (CONT 3)

$$\begin{array}{r}
 x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\
 \quad \quad \quad + (x^3 \quad + x + 1) \\
 \hline
 x^7 \quad + x^5 + x^4
 \end{array}$$

(a) Addition

$$\begin{array}{r}
 x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\
 \quad \quad \quad - (x^3 \quad + x + 1) \\
 \hline
 x^7 \quad + x^5 + x^4
 \end{array}$$

(b) Subtraction

$$\begin{array}{r}
 \quad \quad \quad x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\
 \quad \quad \quad \quad \quad \quad \times (x^3 \quad + x + 1) \\
 \quad \quad \quad \hline
 \quad \quad \quad x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1 \\
 \quad \quad \quad x^8 \quad + x^6 + x^5 + x^4 \quad + x^2 + x \\
 \quad \quad \quad \hline
 x^{10} \quad + x^8 + x^7 + x^6 \quad + x^4 + x^3 \\
 \hline
 x^{10} \quad \quad \quad + x^4 \quad + x^2 \quad + 1
 \end{array}$$

(c) Multiplication

$$\begin{array}{r}
 \quad \quad \quad \quad \quad \quad \quad \quad \quad x^4 + 1 \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \hline
 x^3 + x + 1 \overline{) x^7 \quad + x^5 + x^4 + x^3 \quad + x + 1} \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad x^7 \quad + x^5 + x^4 \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \hline
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad x^3 \quad + x + 1 \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \hline
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad x^3 \quad + x + 1 \\
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \hline
 \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad \quad 0
 \end{array}$$

(d) Division

Figure 4.4 Examples of Polynomial Arithmetic over  $\text{GF}(2)$

A polynomial  $f(x)$  over a field  $F$  is called irreducible if and only if  $f(x)$  cannot be expressed as a product of two polynomials, both over  $F$ , and both of degree lower than that of  $f(x)$ . By analogy to integers, an irreducible polynomial is also called a prime polynomial.

The polynomial  $f(x)=x^4+1$  over  $\text{GF}(2)$  is reducible, because  $x^4+1=(x+1)(x^3+x^2+x+1)$ .

Consider polynomial  $f(x)=x^3+x+1$ . It is clear by inspection that  $x$  is not a factor of  $f(x)$ . Also,  $x+1$  is not a factor of  $f(x)$ . Thus,  $f(x)$  has not factors of degree 1. But it is clear, that if  $f(x)$  is reducible then it must have one factor of degree 2 and one factor of degree 1. Therefore,  $f(x)$  is irreducible.



## Finding the Greatest Common Divisor

The polynomial  $c(x)$  is said to be the greatest common divisor of  $a(x)$  and  $b(x)$  if

1.  $c(x)$  divides both  $a(x)$  and  $b(x)$
2. any divisor of  $a(x)$  and  $b(x)$  is a divisor of  $c(x)$

An equivalent definition:  $\text{gcd}[a(x),b(x)]$  is the polynomial of maximum degree that divides both  $a(x)$  and  $b(x)$ .

We can adapt Euclid's algorithm to compute  $\text{gcd}$ . The equation (4.3) can be rewritten as the following theorem:

$$\text{gcd}[a(x),b(x)] = \text{gcd}[b(x), a(x) \bmod b(x)] \quad (4.6)$$

Euclid's algorithm below assumes that the degree of  $a(x)$  is greater than the degree of  $b(x)$ :

EUCLID[ $a(x),b(x)$ ]

1.  $A(x) := a(x); B(x) := b(x)$
2. if  $B(x) = 0$  return  $A(x) = \text{gcd}[a(x),b(x)]$
3.  $R(x) := A(x) \bmod B(x)$
4.  $A(x) := B(x)$
5.  $B(x) := R(x)$
6. goto 2

Find  $\text{gcd}[a(x),b(x)]$  for  $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$  and  $b(x) = x^4 + x^2 + x + 1$

$A(x) = a(x), B(x) = b(x)$

$R(x) = A(x) \bmod B(x) = x^3 + x^2 + 1$

$A(x) = x^4 + x^2 + x + 1, B(x) = x^3 + x^2 + 1$

$R(x) = A(x) \bmod B(x) = 0$

$A(x) = x^3 + x^2 + 1, B(x) = 0$

## Finding the Greatest Common Divisor (CONT 1)

$$\gcd[a(x),b(x)]=A(x)= x^3 + x^2 + 1$$

### Finite Fields of the Form $GF(2^n)$

Table 4.5 Arithmetic in  $GF(2^3)$

		000	001	010	011	100	101	110	111
+		0	1	2	3	4	5	6	7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

	w	-w	w <sup>-1</sup>
	0	0	—
	1	1	1
	2	2	5
	3	3	6
	4	4	7
	5	5	2
	6	6	3
	7	7	4

(a) Addition

(c) Additive and multiplicative inverses

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

(b) Multiplication

In Table 4.5, arithmetic operations are defined in special way, so, contrary to previously considered case of 8 elements, here we have multiplicative inverses for all non-zero values.

## Modular Polynomial Arithmetic

Let set  $S$  of polynomial coefficients is a finite field  $Z_p$ , and polynomials have degree from 0 to  $n-1$ . There are totally  $p^n$  different such polynomials. The definition consists of the following elements:

1. Arithmetic follows the ordinary rules of polynomial arithmetic using the basic rules of algebra, with the following two refinements
2. Arithmetic on the coefficients is performed modulo  $p$ . That is, we use the arithmetic for the finite field  $Z_p$
3. If multiplication results in polynomial of degree greater than  $n-1$ , then the polynomial is reduced modulo some irreducible polynomial  $m(x)$  of degree  $n$ . That is, we divide by  $m(x)$  and keep the remainder. For a polynomial  $f(x)$ , the remainder is expressed as  $r(x) = f(x) \bmod m(x)$

The AES algorithm uses arithmetic in the finite field  $GF(2^8)$ ,  $p=2$ ,  $n=8$ , with the irreducible polynomial  $m(x) = x^8 + x^4 + x^3 + x + 1$ .

It can be shown that the set of all polynomials modulo an irreducible  $n$ th degree polynomial  $m(x)$  satisfies the axioms in Fig. 4.1 and thus forms a finite field. Furthermore, all finite fields of a given order are isomorphic; that is, any two finite-field structures of a given order have the same structure, but the representation, or labels, of the elements may be different.

To construct the finite field  $GF(2^3)$ , we need to choose an irreducible polynomial of degree 3. There are only two such polynomials:  $x^3 + x^2 + 1$  and  $x^3 + x + 1$ . Using the latter, Table 4.6 shows the addition and multiplication tables for  $GF(2^3)$ :

# Modular Polynomial Arithmetic (CONT 1)

Table 4.6 Polynomial Arithmetic Modulo  $(x^3 + x + 1)$

		000	001	010	011	100	101	110	111
	+	0	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$
000	0	0	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$
001	1	1	0	$x+1$	$x$	$x^2+1$	$x^2$	$x^2+x+1$	$x^2+x$
010	$x$	$x$	$x+1$	0	1	$x^2+x$	$x^2+x+1$	$x^2$	$x^2+1$
011	$x+1$	$x+1$	$x$	1	0	$x^2+x+1$	$x^2+x$	$x^2+1$	$x^2$
100	$x^2$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$	0	1	$x$	$x+1$
101	$x^2+1$	$x^2+1$	$x^2$	$x^2+x+1$	$x^2+x$	1	0	$x+1$	$x$
110	$x^2+x$	$x^2+x$	$x^2+x+1$	$x^2$	$x^2+1$	$x$	$x+1$	0	1
111	$x^2+x+1$	$x^2+x+1$	$x^2+x$	$x^2+1$	$x^2$	$x+1$	$x$	1	0

(a) Addition

		000	001	010	011	100	101	110	111
	×	0	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$
000	0	0	0	0	0	0	0	0	0
001	1	0	1	$x$	$x+1$	$x^2$	$x^2+1$	$x^2+x$	$x^2+x+1$
010	$x$	0	$x$	$x^2$	$x^2+x$	$x+1$	1	$x^2+x+1$	$x^2+1$
011	$x+1$	0	$x+1$	$x^2+x$	$x^2+1$	$x^2+x+1$	$x^2$	1	$x$
100	$x^2$	0	$x^2$	$x+1$	$x^2+x+1$	$x^2+x$	$x$	$x^2+1$	1
101	$x^2+1$	0	$x^2+1$	1	$x^2$	$x$	$x^2+x+1$	$x+1$	$x^2+x$
110	$x^2+x$	0	$x^2+x$	$x^2+x+1$	1	$x^2+1$	$x+1$	$x$	$x^2$
111	$x^2+x+1$	0	$x^2+x+1$	$x^2+1$	$x$	1	$x^2+x$	$x^2$	$x+1$

(b) Multiplication

## Finding the Multiplicative Inverse

Just as Euclid's algorithm can be adapted to find gcd of two polynomials, the extended Euclid's algorithm can be also adapted to find the multiplicative inverse of a polynomial. The algorithm will find multiplicative inverse of  $b(x)$  modulo  $m(x)$  if the degree of  $b(x)$  is less than degree of  $m(x)$  and  $\gcd[m(x), b(x)] = 1$ . If  $m(x)$  is an irreducible polynomial, then it has no other factor than itself or 1, so that  $\gcd[m(x), b(x)] = 1$ . The algorithm follows:

## Finding the Multiplicative Inverse (CONT 1)

EXTENDED EUCLID[m(x),b(x)]

1. [A1(x), A2(x), A3(x)]:= [1,0,m(x)]; [B1(x), B2(x), B3(x)]:= [0,1,b(x)];
2. if B3(x)=0 return A3(x)= gcd[m(x),b(x)]; no inverse
3. if B3(x)=1 return B3(x)= gcd[m(x),b(x)]; B2(x)=b(x)<sup>-1</sup> mod m(x)
4. Q(x):= quotient of A3(x)/B3(x)
5. [T1(x), T2(x), T3(x)]:= [A1(x)-QB1(x), A2(x) -QB2(x), A3(x) - QB3(x)]
6. [A1(x), A2(x), A3(x)]:= [B1(x), B2(x), B3(x)]
7. [B1(x), B2(x), B3(x)]:= [T1(x), T2(x), T3(x)]
8. goto 2

Table 4.7 shows the calculation of the multiplicative inverse of  $x^7 + x + 1$  mod  $x^8 + x^4 + x^3 + x + 1$ . The result is that  $(x^7 + x + 1)^{-1} = x^7$ . That is  $(x^7 + x + 1)(x^7) \equiv 1 \pmod{x^8 + x^4 + x^3 + x + 1}$ .

**Table 4.7** Extended Euclid [( $x^7 + x + 1$ ), ( $x^8 + x^4 + x^3 + x + 1$ )]

<b>Initialization</b>	A1(x) = 1; A2(x) = 0; A3(x) = $x^8 + x^4 + x^3 + x + 1$ B1(x) = 0; B2(x) = 1; B3(x) = $x^7 + x + 1$
<b>Iteration 1</b>	Q(x) = x A1(x) = 0; A2(x) = 1; A3(x) = $x^7 + x + 1$ B1(x) = 1; B2(x) = x; B3(x) = $x^4 + x^3 + x^2 + 1$
<b>Iteration 2</b>	Q(x) = $x^3 + x^2 + 1$ A1(x) = 1; A2(x) = x; A3(x) = $x^4 + x^3 + x^2 + 1$ B1(x) = $x^3 + x^2 + 1$ ; B2(x) = $x^2 + 1$ ; B3(x) = x
<b>Iteration 3</b>	Q(x) = $x^3 + x^2 + x$ A1(x) = $x^3 + x^2 + 1$ ; A2(x) = $x^2 + 1$ ; A3(x) = x B1(x) = $x^6 + x^2 + x + 1$ ; B2(x) = $x^7$ ; B3(x) = 1
<b>Iteration 4</b>	B3(x) = gcd[( $x^7 + x + 1$ ), ( $x^8 + x^4 + x^3 + x + 1$ )] = 1 B2(x) = $(x^7 + x + 1)^{-1} \pmod{x^8 + x^4 + x^3 + x + 1} = x^7$

To get Table 4.5 a,b from Table 4.6 a,b it is sufficient to replace polynomials expressed as ordinary formulae by their codes (by sets of respective coefficients, for example,  $x^2 + 1$  - by 101).