Finding the multiplicative inverse in $GF(p)$

If $\gcd(m, b) = 1$, then b has a multiplicative inverse modulo n. In other words, for positive integer $b < m$, there exists $b^{-1} < m$ such that $b.b^{-1} = 1 \pmod{m}$, where 1 is the multiplicative identity in $GF(p)$.

Algorithm: EXTENDED EUCLID(m, b)

1: Initialize: $(A1, A2, A3) \leftarrow (1, 0, m)$ and $(B1, B2, B3) \leftarrow (0, 1, b)$
2: **if** $B3 = 0$ **then**
3:     **return** $A3 = \gcd(m, b)$; no inverse
4: **end if**
5: **if** $B3 = 1$ **then**
6:     **return** $B3 = \gcd(m, b)$; $B2 = b^{-1} \pmod{m}$
7: **end if**
8: Set $Q = \lfloor \frac{A3}{B3} \rfloor$, quotient when $A3$ is divided by $B3$
9: Set $(T1, T2, T3) \leftarrow (A1 - Q.B1, A2 - Q.B2, A3 - Q.B3)$
10: Set $(A1, A2, A3) \leftarrow (B1, B2, B3)$
11: Set $(B1, B2, B3) \leftarrow (T1, T2, T3)$
12: goto Step 2

Ring and Field

Problem: Find the multiplicative inverse of 550 in $GF(1759)$.

Here, $m = 1759$ and $b = 550$. We need to find $b^{-1} \pmod{m}$, i.e., $550^{-1} \pmod{1759}$.
Applying the extended Euclid's gcd algorithm, we have the following table.

Q	$A1$	$A2$	$A3$	$B1$	$B2$	$B3$	$T1$	$T2$	$T3$
–	1	0	1759	0	1	550	–	–	–
3	0	1	550	1	-3	109	1	-3	109
5	1	-3	109	-5	16	5	-5	16	5
21	-5	16	5	106	-339	4	106	-339	4
1	106	-339	4	-111	355	$\boxed{1}$	-111	355	1

Since $B3 = 1$, so $\gcd(m, b) = B3 = 1$ and multiplicative inverse will be $b^{-1} \pmod{m} = B2 = 355$.
Verification: $b.b^{-1} \pmod{m} = 550.355 \pmod{1759} = 1$.

Ring and Field

Definition (Irreducible Polynomial)

A polynomial $f(x)$ of degree $n > 0$ over the field K is *irreducible* over K if and only if there do not exist polynomials $g(x)$ and $h(x)$ of degree > 0 over K such that

$$f(x) = g(x).h(x),$$

where multiplication is ordinary polynomial multiplication with coefficients operations in K.

- In other words, a polynomial $f(x)$ is said to be irreducible if it can not be factored into non-trivial polynomials over the same field K. 1 and $f(x)$ are trivial factors of $f(x)$.
- A polynomial $f(x)$ is irreducible over K if and only if there does not exist a polynomial $d(x)$, $0 < deg.d(x) < deg.f(x)$, where $deg.f(x)$ means the degree of the polynomial $f(x)$, such that $d(x)|f(x)$ over K.

Ring and Field

Problem: Determine which of the following are reducible over the Galois (finite) field $GF(2)$:

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

Ring and Field

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Lemma

A polynomial $p(x)$ is irreducible over a field K if and only if $k.p(x)$ is also irreducible over K, $\forall k \in K$.

Proof.

$(\Rightarrow)$: Given that $p(x)$ is irreducible over K.
RTP: $k.p(x)$ is irreducible over K, $\forall k \in K$.
If possible, let $k.p(x)$ be reducible over K.
Then, there exist $f(x), g(x) \in \mathcal{P}_K^n$, the set of all polynomials of degree $< n$ over the field K, such that

$$k.p(x) = f(x).g(x).$$

Since $k^{-1} \in K$ exists, we have:

$$p(x) = (k^{-1}.f(x)).g(x) = f'(x).g(x),$$

where $f'(x) = k^{-1}.f(x) \in \mathcal{P}_K^n$.

This shows that $p(x)$ is is reducible polynomial. Hence, it is a contradiction. Consequently, $k.p(x)$ must be irreducible over K.
$(\Leftarrow)$: Given $k.p(x)$ is irreducible, $\forall k \in K$.
RTP: $p(x)$ is irreducible.
If possible, assume that $p(x)$ is reducible one.
Then, there exist $f(x), g(x) \in \mathcal{P}_K^n$, the set of all polynomials of degree $< n$ over the field K, such that

$$p(x) = f(x).g(x).$$

Now,

$$k.p(x) = k.f(x).g(x) = f'(x).g(x),$$

where $f'(x) = k.f(x) \in \mathcal{P}_K^n$.
It shows that $k.p(x)$ is reducible polynomial over the finite field K. But, it is a contradiction from the given condition. Hence, $p(x)$ must be irreducible polynomial over K.

Ring and Field

Modular Polynomial Arithmetic

- Consider the set S of all polynomials of degree $n-1$ or less over a finite field (Galois field) $Z_p = GF(p)$.
- Each polynomial has the following form:

$$\begin{aligned} f(x) &= a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0 \\ &= \sum_{i-0}^{n-1} a_i x^i, \end{aligned}$$

  where $a_i \in Z_p = \{0, 1, 2, \cdots, p-1\}$.
- There are a total of p^n different polynomials is S.

Problem: Find all polynomials in the field $GF(3^2)$

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Here, we have the extended Galois field $GF(p^n)$, where $p = 3$ and $n = 2$.
Then, $S = \{f(x) | f(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{1} a_i x^i = a_1 x + a_0\}$ where $a_i \in Z_p = Z_3 = \{0, 1, 2\}$.
Therefore, there are a total of $3^2 = 9$ polynomials in the set S, which are given below.

a_1	a_0	$f(x) = a_1 x + a_0$
0	0	0
0	1	1
0	2	2
1	0	x
1	1	$x + 1$
1	2	$x + 2$
2	0	$2x$
2	1	$2x + 1$
2	2	$2x + 2$

Problem: Find all polynomials in the field $GF(2^3)$

Here, we have the extended Galois field $GF(p^n)$, where $p = 2$ and $n = 3$.
Then, $S = \{f(x) | f(x) = \sum_{i=0}^{n-1} a_i x^i = \sum_{i=0}^{2} a_i x^i = a_2 x^2 + a_1 x + a_0\}$ where $a_i \in Z_p = Z_2 = \{0, 1\}$. Therefore, there are a total of $2^3 = 8$ polynomials in the set S, which are given below.

a_2	a_1	a_0	$f(x) = a_2x^2 + a_1x + a_0$
0	0	0	0
0	0	1	1
0	1	0	x
0	1	1	$x + 1$
1	0	0	x^2
1	0	1	$x^2 + 1$
1	1	0	$x^2 + x$
1	1	1	$x^2 + x + 1$

Finding the Greatest Common Divisor (gcd)

The polynomial $c(x)$ is said to be the greatest common divisor of the polynomials $a(x)$ 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 $c(x)$, that is,

$$\gcd[a(x), b(x)] = \gcd[b(x), a(x) \bmod b(x)]$$

Algorithm: EUCLID$(a(x), b(x))$

1: Set $A(x) \leftarrow a(x)$; $B(x) \leftarrow b(x)$
2: **if** $B(x) = 0$ **then**
3:     **return** $A(x) = \gcd[a(x), b(x)]$
4: **end if**
5: Compute $R(x) = A(x) \bmod B(x)$
6: Set $A(x) \leftarrow B(x)$
7: Set $B(x) \leftarrow R(x)$
8: goto Step 2

Finding the multiplicative inverse of a polynomial $b(x)$ modulo $m(x)$ in $GF(p^n)$

If $\gcd(m(x), b(x)) = 1$, then $b(x)$ has a multiplicative inverse $b(x)^{-1}$ modulo $m(x)$, where $m(x)$ is irreducible polynomial over $GF(p^n)$.

Algorithm: EXTENDED EUCLID$(m(x), b(x))$

1: Initialize: $(A1(x), A2(x), A3(x)) \leftarrow (1, 0, m(x))$ and $(B1(x), B2(x), B3(x)) \leftarrow (0, 1, b(x))$
2: **if** $B3(x) = 0$ **then**
3:     **return** $A3(x) = \gcd[m(x), b(x)]$; no inverse
4: **end if**
5: **if** $B3 = 1$ **then**
6:     **return** $B3(x) = \gcd[m(x), b(x)]$; $B2(x) = b(x)^{-1} \pmod{m(x)}$
7: **end if**
8: Set $Q(x) = \lfloor \frac{A3(x)}{B3(x)} \rfloor$, quotient when $A3(x)$ is divided by $B3(x)$
9: Set $[T1(x), T2(x), T3(x)] \leftarrow [A1(x) - Q(x).B1(x), A2(x) - Q(x).B2(x), A3(x) - Q(x).B3(x)]$
10: Set $[A1(x), A2(x), A3(x)] \leftarrow [B1(x), B2(x), B3(x)]$
11: Set $[B1(x), B2(x), B3(x)] \leftarrow [T1(x), T2(x), T3(x)]$
12: goto Step 2

Ring and Field

Problem: Find the multiplicative inverse of $(x^7 + x + 1)$ modulo an irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$ in $GF(2^8)$.

- **Initialization:**

$$A1(x) = 1; A2(x) = 0; A3(x) = m(x) = x^8 + x^4 + x^3 + x + 1$$

$$B1(x) = 0; B2(x) = 1; B3(x) = x^7 + x + 1$$

- **Iteration 1:**

$$\begin{aligned} Q(x) &= \left\lfloor \frac{A3(x)}{B3(x)} \right\rfloor = x \\ T1(x) &= A1(x) - Q(x).B1(x) = 1 \\ T2(x) &= A2(x) - Q(x).B2(x) = -x = x \pmod 2 \\ T3(x) &= A3(x) - Q(x).B3(x) = x^4 + x^3 + x^2 + 1 \end{aligned}$$

Ring and Field

- **Iteration 1 (Continued...):**

$$
\begin{aligned}
A1(x) = B1(x) = 0; A2(x) = B2(x) = 1; \\
A3(x) = B3(x) = x^7 + x + 1 \\
B1(x) = T1(x) = 1; B2(x) = T2(x) = x; \\
B3(x) = T3(x) = x^4 + x^3 + x^2 + 1
\end{aligned}
$$

- **Iteration 2:**

$$
\begin{aligned}
Q(x) &= \left\lfloor \frac{A3(x)}{B3(x)} \right\rfloor = x^3 + x^2 + 1 \\
T1(x) &= A1(x) - Q(x).B1(x) = x^3 + x^2 + 1 \\
T2(x) &= A2(x) - Q(x).B2(x) = x^4 + x^3 + x + 1 \\
T3(x) &= A3(x) - Q(x).B3(x) = x
\end{aligned}
$$

Ring and Field

- **Iteration 2 (Continued...):**

$$\begin{aligned} A1(x) &= B1(x) = 1; A2(x) = B2(x) = x; \\ A3(x) &= B3(x) = x^4 + x^3 + x^2 + 1 \\ B1(x) &= T1(x) = x^3 + x^2 + 1; \\ B2(x) &= T2(x) = x^4 + x^3 + x + 1; \\ B3(x) &= T3(x) = x \end{aligned}$$

- **Iteration 3:**

$$\begin{aligned} Q(x) &= \left\lfloor \frac{A3(x)}{B3(x)} \right\rfloor = x^3 + x^2 + x \\ T1(x) &= A1(x) - Q(x).B1(x) = x^6 + x^2 + x + 1 \\ T2(x) &= A2(x) - Q(x).B2(x) = x^7 \\ T3(x) &= A3(x) - Q(x).B3(x) = 1 \end{aligned}$$

- **Iteration 4:** Since $B3(x) = 1$, so

$$\gcd[m(x), b(x)] = B3(x) = 1$$

and

$$\begin{aligned} b(x)^{-1} \bmod m(x) &= B2(x) \\ &= (x^7 + x + 1)^{-1} \bmod x^8 + x^4 + x^3 + x + 1 \\ &= x^7. \end{aligned}$$