Polynomials over Galois Field

- Consider polynomials whose coefficients are taken from prime-order finite fields.

Primitive polynomials and Galois fields of order p^m

- Let $\mathrm{GF}(q)[x]$ denote the collection of all polynomials $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ of arbitrary degree with coefficients $\{a_i\}$ in the finite field $\mathrm{GF}(q)$.
  - $(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) + (b_0 + b_1x + b_2x^2 + \cdots + b_nx^n)$
    $= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_n + b_n)x^n$.
  - $(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n)\cdot(b_0 + b_1x + b_2x^2 + \cdots + b_mx^m)$
    $= (a_0 \cdot b_0) + [a_1 \cdot b_0 + a_0 \cdot b_1]x^1 + [a_2 \cdot b_0 + a_1 \cdot b_1 + a_0 \cdot b_2]x^2 + \cdots + (a_n \cdot b_m)x^{n+m}$.

  The coefficient operations are performed using the operations for the field from which the coefficients were taken.
  - Such a collection of polynomials forms a **<u>commutative ring with identity</u>**.
  - Nonzero field elements are considered to be zero-degree polynomials.

    The zero element, however, is not considered a polynomial at all, because most metrics used with Euclidean rings of polynomials are undefined for the zero element.
- Let α be a root of *f*(*x*). Then, $f(x) \mid x^n - 1 \Rightarrow \mathrm{ord}(\alpha) \mid n$.

- A polynomial *f*(*x*) is **<u>irreducible</u>** in $\mathrm{GF}(q)[x]$ if *f*(*x*) cannot be factored into a product of <u>lower-degree</u> polynomials in $\mathrm{GF}(q)[x]$.
  - All of the roots have the same order.
  - The set of all roots of $f(x)$ is one conjugacy class with respect to $\mathrm{GF}(q)$.
  - $f(x) \mid x^{\mathrm{ord}(\alpha)} - 1$, where $\mathrm{ord}(\alpha)$ is the order of any root of *f*(*x*).

- A polynomial *f*(*x*) is **<u>irreducible</u>** in $\mathrm{GF}(q)$ if *f*(*x*) cannot be factored into a product of <u>lower-degree</u> polynomials in $\mathrm{GF}(q)[x]$.
  - A polynomial may be irreducible in one ring of polynomials, but reducible in another.
  - In fact, every polynomial is reducible in some ring of polynomials. The term irreducible must thus be used only with respect to a specific ring of polynomials.
  - **<u>Remark</u>**: In $\mathrm{GF}(2)[x]$, if *f*(*x*) has degree > 1 and has an even number of terms, then it can't be irreducible. Because 1 is its root, and hence *x* + 1 is one of its factor.
- Irreducible polynomials of degree *n* in GF(2)[*x*]

Degree	Irreducible polynomials
1	x, $x+1$
2	x^2+x+1
3	$x^3+0+x+1$, x^3+x^2+0+1
4	$x^4+0+0+x+1$, $x^4+x^3+0+0+1$, $x^4+x^3+x^2+x+1$
5	$x^5+0+0+x^2+0+1$, $x^5+0+x^3+0+0+1$, $x^5+\underbrace{x^4+x^3+x^2+x}+1$ where exactly one of the 4 middle terms is deleted.

- Any irreducible m^{th}-degree polynomial $f(x)\in \mathrm{GF}(p)[x]$ must divide $x^{p^m-1}-1$.
- Remark for binary polynomials:
  - $x^{n+1}+1=(x+1)\left(\sum_{i=0}^{n} x^i\right)$
  - For n odd, $\sum_{i=0}^{n} x^i = \left(x^n+x^{n-1}\right)+\cdots+(x+1)=(x+1)\left(x^{n-1}+x^{n-3}+\cdots+1\right)$. It is clear that $(x+1)$ is a factor because $\left.\sum_{i=0}^{n} x^i\right|_{x=1}=0$. Also, observe that $\sum_{i=0}^{2k+1} x^i=(x+1)\left(\sum_{i=0}^{k} x^{2i}\right)$.
  - Binary polynomials that miss alternate terms are not irreducible
    - Lowest degree term is $x \Rightarrow x$ is a factor.
    - Lowest degree term is 1: $\sum_{i=0}^{k} x^{2k}$
      - $x^2+1=(x+1)^2$, $x^4+x^2+1=\left(x^2+x+1\right)^2$. $\left(\sum_{i=0}^{n} x^i\right)^2=\sum_{k=0}^{n} x^{2k}$.

        To see this, consider, $\left(x^{n+1}+1\right)^2=(x+1)^2\left(\sum_{i=0}^{n} x^i\right)^2$. Also,

        $\left(x^{n+1}+1\right)^2=x^{2n+2}+1=(x+1)\left(\sum_{i=0}^{2n+1} x^i\right)=(x+1)^2\left(\sum_{i=0}^{n} x^{2k}\right)$.

- $x^4 + \underbrace{x^3 + x^2 + x} + 1$ can't take just one of the middle terms because we left with even number of terms.
- $x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$

- All roots of an irreducible polynomial have the same order.

- Primitive polynomials: An irreducible polynomial $p(x) \in \mathrm{GF}(p)[x]$ of degree *m* is said to be **primitive** if $\min_{n \in \mathbb{N}} \{n : p(x) | x^n - 1\} = p^m - 1$.
  - There are $\frac{\phi(2^n - 1)}{n}$ binary primitive polynomials of degree *n*.

- Primitive polynomials: An irreducible polynomial $p(x) \in \mathrm{GF}(p)[x]$ of degree *m* is said to be **primitive** if $\min_{n \in \mathbb{N}} \{n : p(x) | x^n - 1\} = p^m - 1$.
  - There are $\frac{\phi(2^n - 1)}{n}$ binary primitive polynomials of degree *n*.

  - Given an irreducible polynomial of degree *m*, to test whether it is primitive, divide it from $x^n - 1$ where $m < n < p^m - 1$. If no such *n* gives 0 remainder, then it is primitive. (The case when $n = p^m - 1$ is guaranteed to have 0 remainder.). If there exists *n*, $m < n < p^m - 1$, such that the remainder is not 0, then it is not primitive.
  - Primitive polynomials are the minimal polynomials for primitive elements in a Galois field.

- Primitive polynomials of degree *n* in GF(2)[*x*]

Degree	Primitive polynomials
2	$x^2 + x + 1$
3	$x^3 + 0 + x + 1$, $x^3 + x^2 + 0 + 1$
4	$x^4 + 0 + 0 + x + 1$, $x^4 + x^3 + 0 + 0 + 1$
5	$x^5 + 0 + 0 + x^2 + 0 + 1$, $x^5 + 0 + x^3 + 0 + 0 + 1$, $x^5 + \underbrace{x^4 + x^3 + x^2 + x} + 1$ where exactly one of the 4 middle terms is deleted.

- Remark:

- A primitive polynomial $p(x) \in \mathrm{GF}(p)[x]$ is always irreducible in $\mathrm{GF}(p)[x]$ (by definition), but irreducible polynomials are not always primitive.
- All irreducible polynomials in $\mathrm{GF}(2)[x]$ of degree 2, 3, 5 are primitive.
- $x^4 + x^3 + x^2 + x + 1$ is irreducible but not primitive in $\mathrm{GF}(2)[x]$.

  $\min_{n \in \mathbb{N}} \left\{ n : x^4 + x^3 + x^2 + x + 1 \middle| x^n - 1 \right\} = 5$.

- The root α of an m^{th}-degree primitive polynomial $p(x) \in \mathrm{GF}(p)[x]$
  - Is also be a root of $x^{p^m - 1} - 1$
  - have order $p^m - 1$. (and hence, is a primitive element in $\mathrm{GF}(p^m)$)
  - $p^m - 1$ consecutive powers of α form a multiplicative group of order $p^m - 1$.

- Let α be a nonzero root of $f(x)$. Then, $f(x) | x^n - 1 \Rightarrow \mathrm{ord}(\alpha) | n$.

  Proof. Because α be a root of $f(x)$, we have $f(\alpha) = 0$. Because $f(x) | x^n - 1$, we also have $\alpha^n - 1 = 0$. Recall that $\alpha^n = 1 \Leftrightarrow \mathrm{ord}(\alpha) | n$.

- Let α_i's be roots of an irreducible polynomial $f(x)$, then $f(x) | x^{\mathrm{ord}(\alpha)} - 1$, where $\mathrm{ord}(\alpha)$ is the order of any root of $f(x)$.

  Proof. Because all roots of an irreducible polynomial have the same order, $\forall i$ $(\alpha_i)^{\mathrm{ord}(\alpha)} = 1$. So, all roots of $f(x)$ are also roots of $x^{\mathrm{ord}(\alpha)} - 1$.

- If α is a root of an m^{th}-degree primitive polynomial $p(x) \in \mathrm{GF}(p)[x]$, then
  - α must also be a root of $x^{p^m - 1} - 1$ and $\mathrm{ord}(\alpha) | p^m - 1$.

    Proof. By definition, $p(x) | x^{p^m - 1} - 1$.

  - Let β be any root of $x^{\mathrm{ord}(\alpha)} - 1$, then β is a root of $x^{p^m - 1} - 1$.

    Proof. We have $\beta^{\mathrm{ord}(\alpha)} = 1$. Next, note that $\beta^{p^m - 1} = \left(\beta^{\mathrm{ord}(\alpha)}\right)^k$ where $k \in \mathbb{N}$ because $\mathrm{ord}(\alpha) | p^m - 1$. Hence, $\beta^{p^m - 1} = 1^k = 1$.

  - $x^{\mathrm{ord}(\alpha)} - 1 | x^{p^m - 1} - 1$

    Proof. Because all roots of $x^{\mathrm{ord}(\alpha)} - 1$ are the roots of $x^{p^m - 1} - 1$.

- The root α of an m^{th}-degree primitive polynomial $p(x) \in \mathrm{GF}(p)[x]$ have order $p^m - 1$. (and hence, is a primitive element in $\mathrm{GF}(p^m)$)

Proof. Let α be an arbitrary root of $p(x)$. We know that $x^{\operatorname{ord}(\alpha)}-1 \mid x^{p^m-1}-1$. We also have $p(x) \mid x^{\operatorname{ord}(\alpha)}-1$ because $p(x)$ is irreducible. Because $p(x)$ is primitive, $p^m-1 = \min_{n\in\mathbb{N}}\left\{n : p(x) \mid x^n-1\right\}$. So, $\operatorname{ord}(\alpha) \geq p^m-1$. But from $x^{\operatorname{ord}(\alpha)}-1 \mid x^{p^m-1}-1$, we have $\operatorname{ord}(\alpha) \leq p^m-1$. So, $\operatorname{ord}(\alpha) = p^m-1$.

- Given that α has order p^m-1, then the p^m-1 consecutive powers of α form a multiplicative group of order p^m-1.

  The multiplication operation is performed by adding the exponents of the powers of α modulo $\left(p^m-1\right)$.

- Let $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ be primitive in $\mathrm{GF}(p)[x]$. If α is a root of $p(x)$, it must satisfy $p(\alpha) = \alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$. It follows that

  $$\alpha^m = \left(-a_{m-1}\right)\alpha^{m-1} + \cdots + \left(-a_1\right)\alpha + \left(-a_0\right)1.$$

  The individual powers of α of degree greater than or equal to m can be reexpressed as polynomials in α of degree (m – 1) or less.

  Since $\operatorname{ord}(\alpha) = p^m-1$, the distinct powers of α must have p^m-1 distinct nonzero polynomial representations of the form $b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$. The coefficients $\{b_i\}$ are taken from $\mathrm{GF}(p)$. So, there are p^m-1 distinct nonzero polynomial representations available. A bijective mapping is then defined between the distinct powers of α and the set of polynomials in α of degree less than or equal to (m – 1) with coefficients in GF(p).

- **Construction** of $\mathrm{GF}\left(p^m\right)$:

  Let α be a root of an m^{th}-degree primitive polynomial $p(x) \in \mathrm{GF}(p)[x]$. Then $\operatorname{ord}(\alpha) = p^m-1$ and the p^m-1 consecutive powers of α $\left(\alpha^0, \alpha^1, \ldots, \alpha^{\operatorname{ord}(\alpha)-1}\right)$ are the nonzero elements of the field $\mathrm{GF}\left(p^m\right)$. Also, can express any power of α (exponential representation) (or even any polynomials in α) as $b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$ (polynomial representation).

- $\operatorname{ord}\left(\alpha^i\right) = \dfrac{q-1}{\gcd(i, q-1)}$, $q = p^m$.

- Construction of $\mathrm{GF}\left(p^m\right)$:

  Let α be a root of an m^{th}-degree primitive polynomial $p(x) \in \mathrm{GF}(p)[x]$. Then

  - $\operatorname{ord}(\alpha) = p^m-1$.

- The $p^m - 1$ consecutive powers of α $\left(\alpha^0, \alpha^1, \ldots, \alpha^{\mathrm{ord}(\alpha)-1}\right)$ are the nonzero elements of the field $\mathrm{GF}\left(p^m\right)$.
- Can express $\alpha^m = \left(-a_{m-1}\right)\alpha^{m-1} + \cdots + \left(-a_1\right)\alpha + \left(-a_0\right)1$. ⇒ Can express any power of α (exponential representation) (or even any polynomials in α) as $b_{m-1}\alpha^{m-1} + \cdots + b_1\alpha + b_0$ (polynomial representation).
- Can define bijective mapping between the distinct powers of α and the set of nonzero polynomials in α of degree less than or equal to (m – 1) with coefficients in GF(p).
- Addition is performed using the polynomial representation. One begins by substituting the polynomial representations for the exponential representations. The polynomials are then summed to obtain a third polynomial representation, which may then be reexpressed as a power of α.
- Multiplication is performed through the use of exponential representation. The exponents of the two elements being multiplied together are added together modulo $p^m - 1$.
- Multiplication can also be performed through the polynomial representation. If α^a and α^b have the polynomial representations $p_a(\alpha)$ and $p_b(\alpha)$, respectively, then $\alpha^{(a+b)\bmod\left(p^m-1\right)}$ has polynomial representation $p_a(\alpha)\,p_b(\alpha)$ modulo $p(\alpha)$.

- The polynomial representation for a finite field $\mathrm{GF}\left(p^m\right)$ has coefficients in the "ground field" GF(p). Clearly $\mathrm{GF}\left(p^m\right)$ can thus be interpreted as a vector space over $\mathrm{GF}(p)$. The set $\left\{1, \alpha, \ldots, \alpha^{m-1}\right\}$ can be used as a basis for the vector space.
- Let $\beta \in \mathrm{GF}\left(2^m\right)$, then $-\beta = \beta$.

  Proof. $\beta + \beta = \beta(1+1)$. Note that $1 \in \mathrm{GF}(2)$, hence $1+1=0$. Therefore, $\beta + \beta = \beta 0 = 0$.

Zech's logarithms

- Except in the prime-order field case, GF(q) addition is not as easy to implement as multiplication. The simplest (though least efficient) approach is to construct a ($q \times q$) look-up table. A more efficient use of memory can be obtained through the use of Zech's logarithms, also known as "add-one tables."
- An add-one tables has two columns:

  The first contains the logarithm of each element with respect to a primitive element α. $\left(\log_\alpha(x)\right)$

  The second column contains the logarithm to the base α of the corresponding element in the first column after it has been incremented by one. $\left(\log_\alpha(x+1)\right)$

- $* \to 0$: $\log_\alpha 0 = *$. $\log_\alpha(0+1) = \log_\alpha 1 = 0$.

  In $\mathrm{GF}(2^m)$: $0 \leftrightarrow *$. (1 + 1 = 0)
- $\log_\alpha \alpha^i \equiv i \bmod \mathrm{ord}(\alpha)$
- Check:
  - For $\mathrm{GF}(2^m)$, note that $\alpha^j + 1 = \alpha^k \Leftrightarrow \alpha^k + 1 = \alpha^j$ because $-1 = 1$. So, also works in pair $j \leftrightarrow k$.
  - We stop at α^{q-2}. But can check by calculate whether $\alpha\alpha^{q-2} = \alpha^{q-1} = 1$.
- Addition in $\mathrm{GF}(p^m)$ is then performed using the following scheme:
  - Combine all terms that have the same exponent using modular addition of the exponents (i.e., $\mathrm{GF}(p)$ addition of the "coefficients")
  - Arrange the resulting expression $\alpha^a + \alpha^b + \cdots + \alpha^z$ in order of decreasing exponents.
  - Factor the expression into the form $\left(\cdots\left(\left(\left(\alpha^{a-b}+1\right)\alpha^{b-c}+1\right)\alpha^{c-d}+1\right)\cdots\right)\alpha^z$.

    The summation can now be performed as a series of add-one operations and Galois field multiplications.
- $\alpha^a + \alpha^b + \alpha^c + \alpha^d = \left(\alpha^{a-b}+1\right)\alpha^b + \alpha^c + \alpha^d = \left(\left(\alpha^{a-b}+1\right)\alpha^{b-c}+1\right)\alpha^c + \alpha^d$

  $$= \left(\left(\left(\alpha^{a-b}+1\right)\alpha^{b-c}+1\right)\alpha^{c-d}+1\right)\alpha^d$$
- $\alpha^a + \alpha^b + \alpha^c + 1 = \left(\left(\alpha^{a-b}+1\right)\alpha^{b-c}+1\right)\alpha^{c-d}+1$
- **<u>Example</u>**: The construction of GF(4)

  Because 4 = 2^2, we seek a primitive polynomial in GF(2)[x] of degree 2. Let $p(x) = x^2 + x + 1$. Let α be a root of $p(x)$. This implies that $\mathrm{ord}(\alpha) = 3$ and $\alpha^2 + \alpha + 1 = 0$, i.e., $\alpha^2 = \alpha + 1$. Then,

Exp. Rep.	Poly. Rep.	Vector-space Rep. $(1,\alpha)$	Order	$\log_\alpha(x)$	$\log_\alpha(x+1)$
α^0	1	(1, 0)	1	0	*
α^1	α	(0, 1)	3	1	2
α^2	$\alpha+1$	(1, 1)	3	2	1
0	0	(0, 0)	-	*	0

- **<u>Example</u>**: The construction of GF(8)

  Because 8 = 2^3, we seek a primitive polynomial in $\mathrm{GF}(2)[x]$ of degree 3. Let $p(x) = x^3 + x + 1$. Let α be a root of $p(x)$. This implies that $\mathrm{ord}(\alpha) = 7$ and $\alpha^3 + \alpha + 1 = 0$, i.e., $\alpha^3 = \alpha + 1$. Then,

$\alpha^4 = \alpha^3 \cdot \alpha = \alpha^2 + \alpha$

$\alpha^5 = \alpha^4 \cdot \alpha = \alpha^3 + \alpha^2 = \alpha + 1 + \alpha^2$

$\alpha^6 = \alpha^5 \cdot \alpha = \alpha^3 + \alpha^2 + \alpha = \alpha + 1 + \alpha^2 + \alpha = \alpha^2 + 1$.

Exp. Rep.	Poly. Rep.	Vector-space Rep. $(1, \alpha, \alpha^2)$	Order	$\log_\alpha(x)$	$\log_\alpha(x+1)$
α^0	1	(1, 0, 0)	1	0	*
α^1	α	(0, 1, 0)	7	1	3
α^2	α^2	(0, 0, 1)	7	2	6
α^3	$1+\alpha$	(1, 1, 0)	7	3	1
α^4	$\alpha+\alpha^2$	(0, 1, 1)	7	4	5
α^5	$1+\alpha+\alpha^2$	(1, 1, 1)	7	5	4
α^6	$1+\alpha^2$	(1, 0, 1)	7	6	2
0	0	(0, 0, 0)	-	*	0

Note also that α is a primitive element in $\mathrm{GF}(2^3)$ = GF(8). $\alpha^7 = 1$.

- **<u>Example</u>**: The construction of GF(8)

  Let $p(x) = x^3 + x^2 + 1$. Let α be a root of $p(x)$. This implies that $\mathrm{ord}(\alpha) = 7$ and $\alpha^3 = \alpha^2 + 1$.

Exp. Rep.	Poly. Rep.	Order	$\log_\alpha(x)$	$\log_\alpha(x+1)$
α^0	1	1	0	*
α^1	α	7	1	5
α^2	α^2	7	2	3
α^3	α^2+1	7	3	2
α^4	$\alpha^2+\alpha+1$	7	4	6
α^5	$\alpha+1$	7	5	1
α^6	$\alpha^2+\alpha$	7	6	4
0	0	-	*	0

Note also that α is a primitive element in $\mathrm{GF}(2^3)$ = GF(8). $\alpha^7 = 1$.

- **<u>Example</u>**: The construction of GF(16)

  Let $p(x) = x^4 + x + 1$.

Exp. Rep.	Poly. Rep.	Vector-space Rep. $(1, \alpha, \alpha^2, \alpha^3)$	Order	$\log_\alpha(x)$	$\log_\alpha(x+1)$
0	0	(0, 0, 0, 0)	-	*	0
α^0	1	(1, 0, 0, 0)	1	0	*
α^1	α	(0, 1, 0, 0)	15	1	4

α^2	α^2	(0, 0, 1, 0)	15	2	8
α^3	α^3	(0, 0, 0, 1)	5	3	14
α^4	$\alpha+1$	(1, 1, 0, 0)	15	4	1
α^5	$\alpha^2+\alpha$	(0, 1, 1, 0)	3	5	10
α^6	$\alpha^3+\alpha^2$	(0, 0, 1, 1)	5	6	13
α^7	$\alpha^3+\alpha+1$	(1, 1, 0, 1)	15	7	9
α^8	α^2+1	(1, 0, 1, 0)	15	8	2
α^9	$\alpha^3+\alpha$	(0, 1, 0, 1)	5	9	7
α^{10}	$\alpha^2+\alpha+1$	(1, 1, 1, 0)	3	10	5
α^{11}	$\alpha^3+\alpha^2+\alpha$	(0, 1, 1, 1)	15	11	12
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	(1, 1, 1, 1)	5	12	11
α^{13}	$\alpha^3+\alpha^2+1$	(1, 0, 1, 1)	15	13	6
α^{14}	α^3+1	(1, 0, 0, 1)	15	14	3

Remark: the order is easily find by $\operatorname{ord}\left(\alpha^k\right)=\dfrac{15}{\gcd(k,15)}$.

This follows from a theorem, or can be intuitively shown here as follows: Consider, for example, α^9. We want to find $\min_i\left\{\left(\alpha^9\right)^i=1\right\}$. This happens iff $9i\equiv 0 \bmod 15$ i.e. $15|9i$. But 3 = $\gcd(15,9)$ which is a factor of 9 already divide 15. So we only need $5=\dfrac{15}{\gcd(15,9)}$ to divide *i*. The minimum of *i* for this to occur is *i* = 5.

In this representation, the nonzero elements α^i which are also in $\mathrm{GF}(4)$ is the elements which satisfy $3i\equiv 0 \bmod 15$, i.e., $15|3i$. So, they are $\alpha^0,\alpha^5,\alpha^{10}$. Hence, $\mathrm{GF}(4)=\left\{0,1,\alpha^5,\alpha^{10}\right\}$.

Euclidean Domains

- A Euclidean domain is a set *D* with two binary operations "+" and "$\cdot$" that satisfy the following:
  1. *D* forms a commutative ring with identity.
  2. Cancellation: if *ab* = *bc*, *b* ≠ 0, then *a* = *c*.
  3. Every element *a* ∈ *D* has an associated metric *g*(*a*) such that
     a) *g*(*a*) ≤ $g(a\cdot b)$ for all nonzero *b* ∈ *D*.
     b) For all nonzero *a*, *b* ∈ *D*, *g*(*a*) > *g*(*b*), there exist *q* and *r* such that *a* = *qb* + *r* with *r* = 0 or *g*(*r*) < *g*(*b*).

  - *q* is called the **quotient** and *r* the **remainder**.

    - $g(0)$ is generally taken to be undefined, though a value of $-\infty$ can be assigned if desired.
- Examples of Euclidean Domains
    - The ring of integers under addition and multiplication with metric $g(n) = |n|$ (absolute value).
    - $\mathrm{GF}(q)[x]$: the ring of polynomials over a finite field with metric $g(f(x)) = \mathrm{degree}(f(x))$.
- a is said to be a **divisor** of b (written $a|b$) if there exists $c \in D$ such that $a \cdot c = b$.
- An element a is said to be a **common divisor** of a collection of elements $\{b_1, b_2, \ldots, b_n\}$ if $a|b_i$ for $i = 1, \ldots, n$.
- If d is a common divisor of the $\{b_i\}$ and all other common divisors are less than d, then d is called the **greatest common divisor** (GCD) of the $\{b_i\}$.
    - $g = \gcd(a,b) \Leftrightarrow g$ is a common divisor of a and b, and $\forall d$ common divisor of a and b, $d|g$.

Euclid's Algorithm

- Euclid's algorithm is a very fast method for finding the GCDs of sets of elements in Euclidean domains.
- **Euclid's Algorithm**:
  Let a, b be a pair of elements contained in a Euclidean domain D, where $g(a) > g(b)$
  Let the indexed variable r_i take on the initial values $r_{-1} = a$ and $r_0 = b$.
  Proceed by using the following recursion formula

  If $r_{i-1} \neq 0$, the define r_i using $r_{i-2} - q_i r_{i-1} = r_i$ where $g(r_i) < g(r_{i-1})$.

  Repeat until $r_i = 0$.

  If $r_i = 0$, then $r_{i-1} = \mathrm{GCD}(a,b)$.
- Recursive system of equations:

$a = q_1 b + r_1$	$0 < r_1 < b$
$b = q_2 r_1 + r_2$	$0 < r_2 < r_1$
$r_1 = q_3 r_2 + r_3$	$0 < r_3 < r_2$
$\vdots$	$\vdots$
$r_{n-2} = q_n r_{n-1} + r_n$	$0 < r_n < r_{n-1}$

  $\mathrm{GCD}(a,b) = r_n$.
- Example

- GCD(336,54)

  336 = 6(54) + 12

  54 = 4(12) + 6

  12 = 2(6) + 0

  GCD(336, 54) = 6

- $\mathrm{GCD}\left(x^5+x^3+x+1, x^4+x^2+x+1\right)$

  $x^5+x^3+x+1 = x\left(x^4+x^2+x+1\right)+\left(x^2+1\right)$

  $x^4+x^2+x+1 = x^2\left(x^2+1\right)+\left(x+1\right)$

  $x^2+1 = \left(x+1\right)\left(x+1\right)+0$

  $\mathrm{GCD}\left(x^5+x^3+x+1, x^4+x^2+x+1\right) = x+1$

- $D^m+1=\left(D+1\right)\left(D^{m-1}+D^{m-2}+\cdots+D+1\right)$.
- In a Euclidean domain, the remainder r_i will always take on the value zero after a finite number of steps.

  The worst case: Euclid's algorithm requires a maximal number of steps to complete when a and b are consecutive Fibonacci numbers.
- $\mathrm{GCD}\left(a,b,c\right)=\mathrm{GCD}\left(\mathrm{GCD}\left(a,b\right),c\right)$.
- If $B=\left\{b_1,b_2,\ldots,b_n\right\}$ is any finite subset of elements from a Euclidean domain D, then B has a GCD d which can be expressed as a linear combination $\sum_k \lambda_k b_k$, where the coefficients $\left\{\lambda_i\right\}\subset D$.

- **The extended Version of Euclid's Algorithm**
  - $r_{i-2}=q_i r_{i-1}+r_i \Leftrightarrow r_i=r_{i-2}-q_i r_{i-1} \quad g\left(r_i\right)<g\left(r_{i-1}\right)$
  - $s_i=s_{i-2}-q_i s_{i-1}$, $t_i=t_{i-2}-q_i t_{i-1}$.

i	r_i	q_i	s_i	t_i	
-1	a	-	1	0	
0	b	-	0	1	
1	r_1	q_1	1	$-q_1$	
2					
	$\mathrm{GCD}\left(a,b\right)$		s	t	
	0				

  - Check: $\mathrm{GCD}\left(a,b\right)=sa+tb$.
  - Check: for all j, $s_j a+t_j b=r_j$.

- The extended Version of Euclid's Algorithm

  We wish to find *s* and *t* such that $\text{GCD}(a,b) = sa + tb$.

  1. A set of indexed variables $\{r_i, s_i, t_i\}$ is given the following initial conditions:

     $r_{-1} = a$, $r_0 = b$, $s_{-1} = 1$, $s_0 = 0$, $t_{-1} = 0$, $t_0 = 1$.
  2. If $r_{i-1} \neq 0$, then define r_i using $r_i = r_{i-2} - q_i r_{i-1}$, $g(r_i) < g(r_{i-1})$.
  3. Compute s_i using $s_{i-2} - q_i s_{i-1}$, where q_i is from step 2.
  4. Compute t_i using $t_i = t_{i-2} - q_i t_{i-1}$.
  5. Repeat steps 2 through 4 until $r_i = 0$.

  At this point $r_{i-1} = \text{GCD}(a,b)$ and $s_{i-1}a + t_{i-1}b = r_{i-1}$.

i	r_i	q_i	s_i	t_i
-1	a	-	1	0
0	b	-	0	1
1	r_1	q_1	1	$-q_1$
2				

  - Remark:
    - for all *j*, $s_j a + t_j b = r_j$.
    - $a = bq_1 + r_1$, $s_1 = s_{-1} - q_1 s_0 = 1 - q_1 0 = 1$, $t_1 = t_{-1} - q_1 t_0 = 0 - q_1 1 = -q_1$.
    - Observe that the initial conditions for s_i and t_i is the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

- If $B = \{b_1, b_2, \ldots, b_n\}$ is any finite subset from a Euclidean domain *D*, then *B* has a gcd *d* which can be expressed as a linear combination $\sum \lambda_k b_k$ where the coefficients $\{\lambda_i\} \subset D$

  Proof. Let $S = \left\{\sum \lambda_k b_k : \{\lambda_i\} \subset D\right\}$. Let *d* be the element in *S* with the smallest metric $(g(d))$. By definition, $d \in S \Rightarrow d = \sum \lambda_i b_i$. We will show that *d* is the GCD of the elements in *B*.
  If *d* does not divide some element $b_i \in B$, then we can write $b_i = qd + r$ where $g(r) < g(d)$. But $r = b_i - qd$ must be in *S*, since b_i and *d* are in *S*. This contradicts the minimality of the metric of *d* in *S*. Thus, *d* is a common divisor of all the elements in *B*.

Now let e by any other common divisor of the elements in B. We can then write $b_i = q_i' e$ for each $b_i \in B$. Then, $d = \sum \lambda_i b_i = \sum \lambda_i q_i' e = e \sum \lambda_i q_i'$. So, d is a multiple of every common divisor and thus the GCD of all of the elements in B.

- Let D be a Euclidean domain. Suppose that for $a, b, c \in D$, $a \mid (bc)$, but a and b are relatively prime. Show that $a \mid c$.

  Proof. $\gcd(a,b) = 1 \Rightarrow \exists\ s,t \in D\ \ sa + tb = 1$. $a \mid (bc) \Rightarrow bc = aq$ for some $q \in D$. $sa + tb = 1 \Rightarrow sac + tbc = c \Rightarrow sac + taq = c \Rightarrow a(sc + tq) = c$.

- All finite Euclidean domains are fields.

  Proof. D forms a commutative <u>ring</u> with identity. Hence, only need to show the existence of unique multiplicative inverse. Let $x \in D$. $|D|$ is finite; hence, the sequence $x, x^2, x^3, \ldots$ must repeat. $\Rightarrow \exists\ p,q\ \ q > p$ such that $x^p = x^q$ $\Rightarrow x^p = x^p \left(x^{q-p}\right) \Rightarrow$ by cancellation, $x^{q-p} = 1$. $\Rightarrow x\left(x^{q-p-1}\right) = 1$, thus x has an inverse.

- **<u>Example</u>**: $\text{GCD}(256,108)$

r_i	q_i	s_i	t_i
256	-	1	0
108	-	0	1
140	2	1	-2
28	2	-2	5
12	1	3	-7
4	2	-8	19
0			

$\text{GCD}(256,108)$ = 4 = 256(-8) + 108(19)

- **<u>Examples</u>**: $\text{GCD}\left(x^5 + x^3 + x + 1, x^4 + x^2 + x + 1\right)$

r_i	q_i	s_i	t_i
$x^5 + x^3 + x + 1$	-	1	0
$x^4 + x^2 + x + 1$	-	0	1
$x^2 + 1$	x	1	x
$x + 1$	x^2	x^2	$x^3 + 1$
0			

$$\begin{aligned}\mathrm{GCD}\left(x^5+x^3+x+1, x^4+x^2+x+1\right) &= x+1 \\ &= x^2\left(x^5+x^3+x+1\right)+\left(x^3+1\right)\left(x^4+x^2+x+1\right)\end{aligned}$$