INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECANICA Y ELECTRICA
UNIDAD CULHUACAN

MAESTRÍA EN INGENIERÍA EN SEGURIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN

IMPLEMENTACIÓN DEL ALGORITMO EXTENDIDO DE EUCLIDES PARA POLINOMIOS DE ORDEN Z2

Presenta:

Jonathan Eduardo Garcíá García

jgarciag1404@alumno.ipn.mx

Profesor:

Dr. Eduardo Vázquez Fernández

Fecha:

25/02/2022

https://jon2g.github.io/EuclidsPolynomialsEqSolver/theory

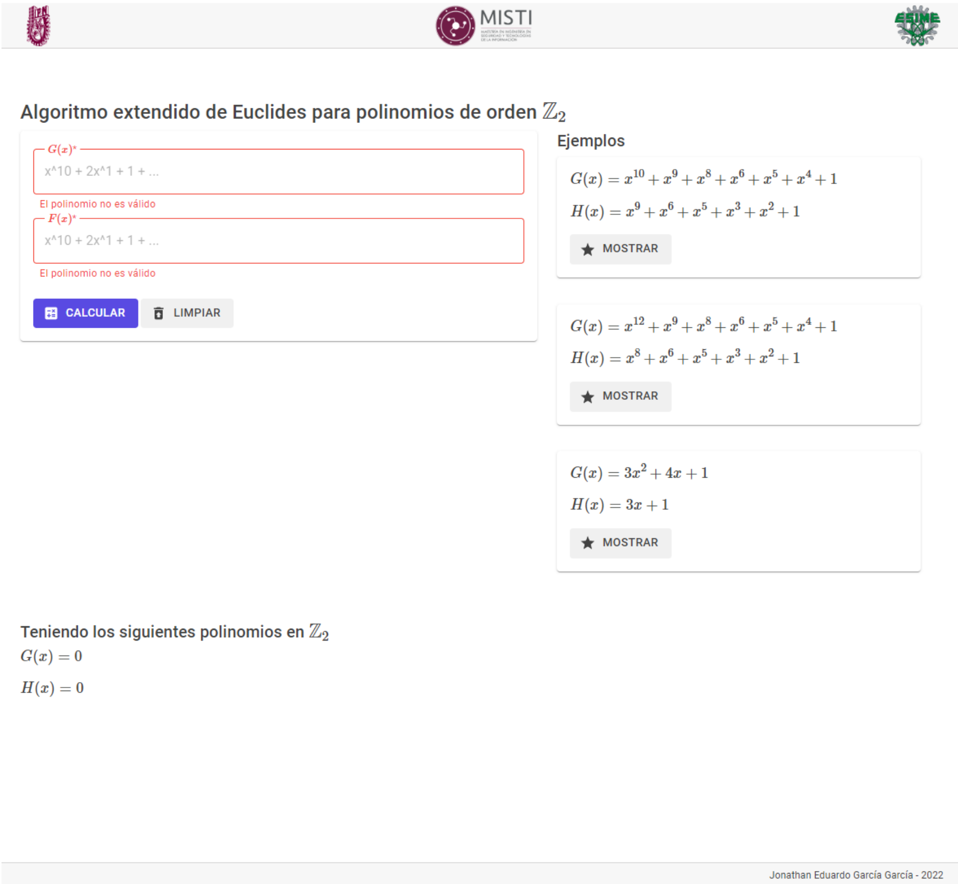
NOTA:

El programa esta publicado en la siguiente dirección:
https://jon2g.github.io/EuclidsPolynomialsEqSolver/theory

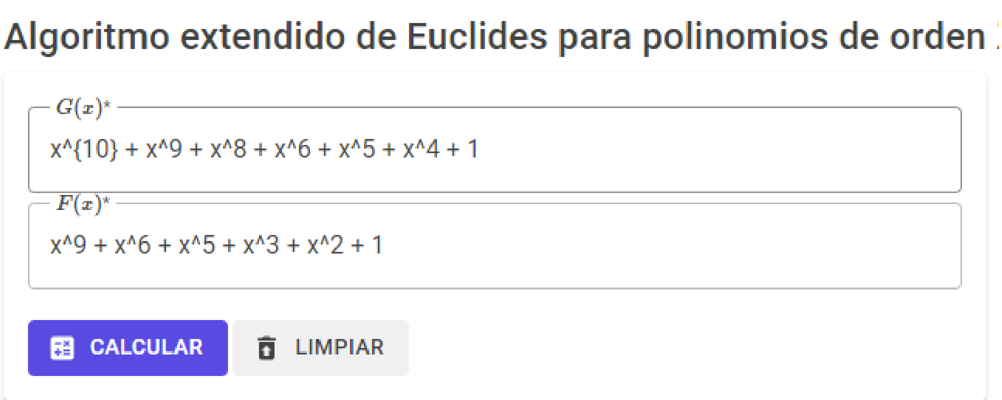
El código fuente puede consultarse en:

https://github.com/Jon2G/EuclidsPolynomialsEqSolver

Capturas de pantalla del programa en funcionamiento:



1) Procedemos a ingresar los polinomios ó podemos seleccionar un de los ejemplos:



Nota: Los polinomios deben ingresarse con formato de latex, no soporta otro tipo de ecuaciones

2) Presionamos calcular y se nos mostrará el resultado paso por paso.

a. Polinomio A)

Teniendo los siguientes polinomios en $\mathbb{Z}_2$

$G(x) = x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$

$H(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$

Calcular

$D(x) = gcd(G(x), H(x), S(x), T(x)$

$S_2(x) = 1$

$S_1(x) = 0$

$T(x) = 0$

$T_1(x) = 1$

Teniendo que $H(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$ **es diferente de cero**

Dividimos $G(x)$ **entre** $H(x)$

$$\frac{x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + 1}{x^9 + x^6 + x^5 + x^3 + x^2 + 1}$$

Resultado de la división:

$Q(x) = x + 1$

Resusido de la división:

$R(x) = x^8 + x^7 + x^6 + x^2 + x$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (1 - (x + 1 * 0))$

$S(x) = 1$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (0 - (x + 1 * 1))$

Hacemos a $G(x) = H(x), H(x) = R(x)$

$G(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$

$H(x) = x^8 + x^7 + x^6 + x^2 + x$

Hacemos a $S_2 = S_1, S_1 = S(x), T_2 = T_1, T_1 = T(x)$

$S_2(x) = 0$

$S_1(x) = 1$

$T_2(x) = 1$

$T_1(x) = x + 1$

2

Teniendo que $H(x) = x^8 + x^7 + x^6 + x^2 + x$ **es diferente de cero**

Dividimos $G(x)$ **entre** $H(x)$

$$\frac{x^9 + x^6 + x^5 + x^3 + x^2 + 1}{x^8 + x^7 + x^6 + x^2 + x}$$

Resultado de la división:

$Q(x) = x + 1$

Resusido de la división:

$R(x) = x^5 + x^2 + x + 1$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (0 - (x + 1 * 1))$

$S(x) = x + 1$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (1 - (x + 1 * x + 1))$

Hacemos a $G(x) = H(x)\,, H(x) = R(x)$

$G(x) = x^8 + x^7 + x^6 + x^2 + x$

$H(x) = x^5 + x^2 + x + 1$

Hacemos a $S_2 = S_1\,, S_1 = S(x)\,, T_2 = T_1\,, T_1 = T(x)$

$S_2(x) = 1$

$S_1(x) = x + 1$

$T_2(x) = x + 1$

$T_1(x) = x^2$

3

Teniendo que $H(x) = x^5 + x^2 + x + 1$ **es diferente de cero**

Dividimos $G(x)$ **entre** $H(x)$

$$\frac{x^8 + x^7 + x^6 + x^2 + x}{x^5 + x^2 + x + 1}$$

Resultado de la división:

$Q(x) = x^3 + x^2 + x + 1$

Resusido de la división:

$R(x) = x^3 + x + 1$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (1 - (x^3 + x^2 + x + 1 * x + 1))$

$S(x) = x^4$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (x + 1 - (x^3 + x^2 + x + 1 * x^2))$

Hacemos a $G(x) = H(x)\,, H(x) = R(x)$

$G(x) = x^5 + x^2 + x + 1$

$H(x) = x^3 + x + 1$

Hacemos a $S_2 = S_1\,, S_1 = S(x)\,, T_2 = T_1\,, T_1 = T(x)$

$S_2(x) = x + 1$

$S_1(x) = x^4$

$T_2(x) = x^2$

$T_1(x) = x^5 + x^4 + x^3 + x^2 + x + 1$

Teniendo que $H(x) = x^3 + x + 1$ es diferente de cero

Dividimos $G(x)$ entre $H(x)$

$$\frac{x^5 + x^2 + x + 1}{x^3 + x + 1}$$

Resultado de la división:

$$Q(x) = x^2 + 1$$

Resusido de la división:

$$R(x) = 0$$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$$S(x) = (x + 1 - (x^2 + 1 * x^4))$$

$$S(x) = x^6 + x^4 + x + 1$$

Hacemos a $T(x) = (s2 - qx * s1)$

$$T(x) = (x^2 - (x^2 + 1 * x^5 + x^4 + x^3 + x^2 + x + 1))$$

Hacemos a $G(x) = H(x)$, $H(x) = R(x)$

$$G(x) = x^3 + x + 1$$

$$H(x) = 0$$

Hacemos a $S_2 = S_1$, $S_1 = S(x)$, $T_2 = T_1$, $T_1 = T(x)$

$$S_2(x) = x^4$$

$$S_1(x) = x^6 + x^4 + x + 1$$

$$T_2(x) = x^5 + x^4 + x^3 + x^2 + x + 1$$

$$T_1(x) = x^7 + x^6 + x^2 + x + 1$$

H(x)=0 es cero por lo tanto hemos terminado ...

Resultado

$$G(x) = x^3 + x + 1$$

$$H(x) = x^9 + x^6 + x^5 + x^3 + x^2 + 1$$

$$S_2(x) = x^4$$

$$T_2(x) = x^5 + x^4 + x^3 + x^2 + x + 1$$

b) Polinomio b

Teniendo los siguientes polinomios en $\mathbb{Z}_2$

$G(x) = x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$

$H(x) = x^8 + x^6 + x^5 + x^3 + x^2 + 1$

Calcular

$D(x) = gcd(G(x), H(x), S(x), T(x)$

$S_2(x) = 1$

$S_1(x) = 0$

$T_(x) = 0$

$T_1(x) = 1$

Teniendo que $H(x) = x^8 + x^6 + x^5 + x^3 + x^2 + 1$ **es diferente de cero**

Dividimos $G(x)$ **entre** $H(x)$

$$\frac{x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 + 1}{x^8 + x^6 + x^5 + x^3 + x^2 + 1}$$

Resultado de la división:

$Q(x) = x^4 + x^2$

Resusido de la división:

$R(x) = x^4 + x^2 + 1$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (1 - (x^4 + x^2 * 0))$

$S(x) = 1$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (0 - (x^4 + x^2 * 1))$

Hacemos a $G(x) = H(x), H(x) = R(x)$

$G(x) = x^8 + x^6 + x^5 + x^3 + x^2 + 1$

$H(x) = x^4 + x^2 + 1$

Hacemos a $S_2 = S_1, S_1 = S(x), T_2 = T_1, T_1 = T(x)$

$S_2(x) = 0$

$S_1(x) = 1$

$T_2(x) = 1$

$T_1(x) = x^4 + x^2$

2

Teniendo que $H(x) = x^4 + x^2 + 1$ **es diferente de cero**

Dividimos $G(x)$ **entre** $H(x)$

$$\frac{x^8 + x^6 + x^5 + x^3 + x^2 + 1}{x^4 + x^2 + 1}$$

Resultado de la división:

$Q(x) = x^4 + x + 1$

Resusido de la división:

$R(x) = x$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (0 - (x^4 + x + 1 * 1))$

$S(x) = x^4 + x + 1$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (1 - (x^4 + x + 1 * x^4 + x^2))$

Hacemos a $G(x) = H(x)$, $H(x) = R(x)$

$G(x) = x^4 + x^2 + 1$

$H(x) = x$

Hacemos a $S_2 = S_1$, $S_1 = S(x)$, $T_2 = T_1$, $T_1 = T(x)$

$S_2(x) = 1$

$S_1(x) = x^4 + x + 1$

$T_2(x) = x^4 + x^2$

$T_1(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

3

Teniendo que $H(x) = x$ **es diferente de cero**

Dividimos $G(x)$ **entre** $H(x)$

$$\frac{x^4 + x^2 + 1}{x}$$

Resultado de la división:

$Q(x) = x^3 + x$

Resusido de la división:

$R(x) = 1$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (1 - (x^3 + x * x^4 + x + 1))$

$S(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (x^4 + x^2 - (x^3 + x * x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1))$

Hacemos a $G(x) = H(x)$, $H(x) = R(x)$

$G(x) = x$

$H(x) = 1$

Hacemos a $S_2 = S_1$, $S_1 = S(x)$, $T_2 = T_1$, $T_1 = T(x)$

$S_2(x) = x^4 + x + 1$

$S_1(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$

$T_2(x) = x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1$

$T_1(x) = x^{11} + x^8 + x^2 + x$

4

Teniendo que $H(x) = 1$ es diferente de cero

Dividimos $G(x)$ entre $H(x)$

$$\frac{x}{1}$$

Resultado de la división:

$Q(x) = x$

Resusido de la división:

$R(x) = 0$

Hacemos a $S(x) = (S_2 - Q(x) * S_1)$

$S(x) = (x^4 + x + 1 - (x * x^7 + x^5 + x^4 + x^3 + x^2 + x + 1))$

$S(x) = x^8 + x^6 + x^5 + x^3 + x^2 + 1$

Hacemos a $T(x) = (s2 - qx * s1)$

$T(x) = (x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 - (x * x^{11} + x^8 + x^2 + x))$

Hacemos a $G(x) = H(x)$, $H(x) = R(x)$

$G(x) = 1$

$H(x) = 0$

Hacemos a $S_2 = S_1$, $S_1 = S(x)$, $T_2 = T_1$, $T_1 = T(x)$

$S_2(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$

$S_1(x) = x^8 + x^6 + x^5 + x^3 + x^2 + 1$

$T_2(x) = x^{11} + x^8 + x^2 + x$

$T_1(x) = x^{12} + x^9 + x^8 + x^6 + x^5 + x^4 + 1$

H(x)=0 es cero por lo tanto hemos terminado ...

R

Resultado

$G(x) = 1$

$H(x) = x^8 + x^6 + x^5 + x^3 + x^2 + 1$

$S_2(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$

$T_2(x) = x^{11} + x^8 + x^2 + x$

3) Teoría

Campos finitos

Un campo finito consiste de un conjunto finito de elementos F sobre el cual se definen un par de operaciones binarias + y ·, las cuales satisfacen las siguientes propiedades aritméticas:

1. (F, +) es un grupo abeliano, denominado el grupo aditivo del campo.
2. (F ∗ = F − 0, ·) es un grupo abeliano, al que se denomina grupo multiplicativo del campo.
3. El producto tiene la propiedad distributiva respecto de la suma, esto es, a · (b + c) = a · b + a · c.

El orden de un campo finito es el número de elementos en el campo. Existe un campo finito de orden q si y solo si q es la potencia de un número primo. Si q es la potencia de un primo, existe esencialmente un solo campo finito de orden q al cual denotaremos como GF(q). Existen, sin embargo, varias maneras de representar a los elementos de GF(q). Algunas de estas representaciones darán origen a implementaciones más eficientes de la aritmética del campo.
Si q = p m donde p es un primo y m un entero positivo, entonces p es denominado la característica del campo GF(q) y m es denominado el grado de extensión de GF(q).

Campo finito GF(2m)

El campo GF(2m), denominado un campo finito de característica dos o campo finito binario, puede ser visto como un espacio vectorial de dimensión m sobre el campo GF(2). Esto es, existen m elementos α0, α1, . . . , αm−1 en GF(2m) tales que cada elemento α ∈ GF(2m) puede ser escrito en forma única como: α = a0α0 + a1α1 + · · · + am−1αm−1, donde ai ∈ {0, 1}. Al conjunto {α0, α1, . . . , αm−1} se le denomina una base de GF(2m) sobre GF(2). Dada una base tal, un elemento α del campo puede ser representado por la cadena de bits (a0a1 · · · am−1). La adición de elementos en el campo se realiza mediante el XOR bit a bit de sus representaciones vectoriales. Existen diferentes bases de GF(2m) sobre GF(2). Algunas bases dan origen a implementaciones más eficientes en hardware o software de la aritmética sobre GF(2m). El estándar ANSI X9.62 permite dos tipos de bases: las bases polinomiales y las bases normales.

Algoritmo Extendido de Euclides

Se tiene dos polinomios a y b, ambos diferentes de cero. El Maximo Común Divisor (MCD) de a y b, denotado por MCD (a, b), es el polinomio d del grado más alto que divide ambos polinomios a y b. Existen algoritmos para el cálculo del MCD(a, b) basados en el siguiente teorema.

Teorema 1. *Se tiene dos polinomios a y b. Entonces MCD = (a, b) = MCD(b − ca, a) para cualquier polinomio c.*

En el Algoritmo de Euclides clásico para el cálculo del MCD de dos polinomios a y b, cuando el grado(b) ≥ grado(a), b es divido por a para obtener un cociente q y un residuo r, que satisfacen la ecuación b = qa + r y grado(r) < grado(a). Por el Teorema 1, el MCD(a, b) = MCD(r, a). Así, el problema de determinar el MCD(a, b) es reducido a calcular MCD(r, a) donde los argumentos (r, a) tienen un grado menor que el grado de los argumentos originales (a, b). Este proceso es repetido hasta que uno de los argumentos es cero. El resultado obtenido inmediatamente de MCD(0, d) es d. Por otro lado, este algoritmo es eficiente porque el número de divisiones enteras es a lo más k, donde k = grado(a). En una variante del algoritmo clásico de Euclides, solamente un paso en cada división entera es modificado. Esto es, si el grado(b) ≥ grado(a) y j = grado(b) − grado(a) entonces sólo se calcula u ← u + v, g1 ← g1 + g2. Por el Teorema 1, MCD(a, b) = MCD(r, a). Este proceso es repetido hasta encontrar un residuo igual a cero. Si el grado(r) < grado(b), el número de divisiones enteras es a lo más k, en donde k = max {grado(a), grado(b)}.

Entrada: A y B.
Salida: $d = gcd(A, B)$, $x = (A^{-1} \bmod B)$ y $y = (B^{-1} \bmod A)$

si $B = 0$ **entonces**
  $d = A; x = 1; y = 0;$
en otro caso
  $x_1 = 0; x_2 = 1;$
  $y_1 = 1; y_2 = 0;$
  mientras $B > 0$ **hágase**
    $q = A \operatorname{div} B;$
    $r = A \bmod B;$
    $x = x_2 - q \cdot x_1;$
    $y = y_2 - q \cdot y_1;$
    $A = B;$
    $B = r;$
    $x_2 = x_1; x_1 = x;$
    $y_2 = y_1; y_1 = y;$
  $d = A;$
  $x = x_2;$
  $y = y_2;$
regresa d, x y y

Algoritmo Extendido de Euclides

Implementación propuesta:

```
PolynomialEq gx = this.Gx.Clone();
PolynomialEq hx = this.Hx.Clone();
PolynomialEq s2 = new PolynomialEq("S_2", XTerm.One);
PolynomialEq s1 = new PolynomialEq("S_1", XTerm.Zero);
PolynomialEq t2 = new PolynomialEq("T_", XTerm.Zero);
PolynomialEq t1 = new PolynomialEq("T_1", XTerm.One);
while (hx.IsNotZero)
{
    //Linea 9
    PolynomialDivisionResult qxDiv = gx / hx;
    PolynomialEq qx = qxDiv.Result.Mod().SetLetter('q');
    PolynomialEq rx = qxDiv.Remainder.Mod().SetLetter('r');
    //Linea 10
    PolynomialEq sx = (s2 - (qx * s1)).Mod().SetLetter('s');
    PolynomialEq tx = (t2 - (qx * t1)).Mod().SetLetter('t');
    //Linea 11
    gx = hx.Clone().SetLetter('g');
    hx = rx.Clone().SetLetter('h');
    //Linea 12
    s2 = s1.Clone().SetLetter("s2");
    s1 = sx.Clone().SetLetter("s1");
    t2 = t1.Clone().SetLetter("t2");
    t1 = tx.Clone().SetLetter("t1");
}
//Linea 14
Dx = gx;
Sx = s2;
Tx = t2;;
```