1. **Defina resumidamente, um grupo, um anel, um corpo.**
   R:
   Um grupo G, às vezes indicado por {G,}, é um conjunto de elementos com uma operação binária, sinalizada por *, que associa a cada par ordenado (a, b) de elementos em G um elemento (a b) em G, tal que os seguintes axiomas são obedecidos

   i) Fechamento: Se a e b pertencem a G, então a b também está em G.
   ii) Associativo: a(b * c) = (a * b)c para todo a, b, c em G.
   iii) Elemento identidade: Existe um elemento e em G, tal que a * e = e * a = a para todo a em G.
   iv) Elemento inverso: Para cada a em G existe um elemento a' em G, tal que a * a' = a' * a = e.
   Um grupo abeliano tem *v) comulativo:* a * b = b * a para todo a, b em G.

   Um anel R, às vezes indicado por {R, +, ×}, é um conjunto de elementos com duas operações binárias, chamadas adição e multiplicação, 6 de forma que, para todo a, b, c em R, os seguintes axiomas são obedecidos

   i) R é um grupo abeliano com relação à adição; ou seja, R satisfaz os axiomas de *i* a *v* de um grupo G. Para o caso de um grupo aditivo, indicamos o elemento de identidade como 0 e o inverso de a como -a.
   ii) Fechamento sob multiplicação: se a e b pertencem a R, então ab também está em R.
   iii) Associatividade da multiplicação: a (bc) = (ab)c, para todo a, b, c em R.
   iv) Leis distributivas: a (b + c) = ab + ac, para todo a, b, c em R. (a + b)c = ac + bc, para todo a, b, c em R.
   Um anel é comutativo se tem
   v) Comutatividade da multiplícação: ab = ba, para todo a, b em R.
   Um anel tem domínio integral se tem
   vi) Identidade multiplicativa: existe um elemento 1 em R, tal que a1 = 1a = a, para todo a em R.
   vii) Sem divisores de zero: se a, b em R e ab = 0, então a = 0 ou b = 0.

   Um corpo F, às vezes indicado por {F, +, ×}, é um conjunto de elementos com duas operações binárias, chamadas de adição e multiplicação, de modo que, para todo a, b, c em F, os seguintes axiomas são obedecidos

   i) F é um anel comulativo com domínio integral; ou seja, F satisfaz os axiomas de *i* a *v* de um grupo G e de *i* a *vii* de um anel R.
   ii) Inverso multiplicativo: para cada a em F, exceto 0, existe um elemento a^–1 em F, tal que aa^–1 = (a^–1)a = 1.

2. **O que significa dizer que b é um divisor de a?**
   R:
   Quando b divide a e tem resto 0 no processo de divisão. Por exemplo 3 é divisor de 12, pois quando dividimos 12 por 3 resultados em 4 e temos resto 0.

3. **Para cada uma das seguintes equações, encontre um inteiro x que satisfaça:**
   a) **5x ≡ 4 (mod 3)** R: Como 4 mod 3 ≡ 1 mod 3 então com x = 2 temos 5.2 = 10 = 1 mod 3.

b) **7x ≡ 6 (mod 5)** R: Como 6 mod 5 ≡ 1 mod 5 então com x = 3 temos 7.3 = 21 = 1 mod 5
c) **9x ≡ 8 (mod 7)** R: Como 8 mod 7 ≡ 1 mod 7 então com x = 4 temos 9.4 = 36 = 1 mod 7.

4. Encontre o inverso multiplicativo de cada elemento diferente de zero em Z_5.

R:

Para Z_5 temos {|0|, |1|, |2|, |3|, |4|} de possibilidades, dessa forma

1 * 1 = 1, logo 1^-1 = 1

2 * 3 = 6 ≡ 1 mod 5, logo 2^-1 = 3

3 * 2 = 6 ≡ 1 mod 5, logo 3^-1 = 2

4 * 4 = 16 ≡ 1 mod 5, logo 4^-1 = 4

5. Determine os MDC:

a) **mdc(24140, 16762)** = mdc(16762,24140 mod 16762) = mdc(16762,7378) = mdc(7378,16762 mod 7378) = mdc(7378,2006) = mdc(2006,7378 mod 2006) = mdc(2006,1360) = mdc(1360,2006 mod 1360) = mdc(1360,646) = mdc(646,1360 mod 646) = mdc(646,68) = mdc(68,646 mod 68) = mdc(68, 34) = mdc(34, 68 mod 34) = mdc(34, 0) = 34.
b) **mdc(4655, 12075)** = mdc(12075, 4655) = mdc(4655, 12075 mod 4655) = mod(4655,2765) = mod(2765,4655 mod 2765) = mdc(2765,1890) = mdc(1890, 2765 mod 1890) = mdc(1890,875) = mdc(875,1890 mod 875) = mdc(875,140) = mdc(140,875 mod 140) = mdc(140,35) = mdc(35, 140 mod 35) = mdc(35,0) = 35.

6. Usando o algoritmo de Euclides estendido, encontre o inverso multiplicativo de:

a) **1234 mod 4321**
   É necessário verificar se o mdc(1234, 4321) =? 1. Logo mdc(1234,4321) = mdc(4321,1234) = mdc(1234, 4321 mod 1234) = mdc(1234,619) = mdc(619,1234 mod 619) = mdc(619, 615) = mdc(615, 619 mod 615) = mdc(615, 4) = mdc(4, 615 mod 4) = mdc(4, 3) = mdc(3, 4 mod 3) = mdc(3, 1) = mdc(1, 3 mod 1) = mdc(1, 0) = 1
   Portanto é verdadeiro logo a equação *by mod a = 1* é satisfeita
   Dessa forma, o inverso de 1234 mod 4321 é 4321y mod 1234 = 1, portanto y = 309 que é o inverso de 4321. Para 1234y mod 4321 = 1, y = 3239 que é o inverso de 1234.

b) **24140 mod 40902**
   Verificando mdc(24140,40902) =? 1
   mdc(24140,40902) = mdc(40902,24140) = mdc(24140, 40902 mod 24140) = mdc(24140,16762) = mdc(16762, 24140 mod 16762) = mdc(16762,7378) = mdc(7378, 16762 mod 7378) = mdc(7378,2006) = mdc(2006,7378 mod 2006) = mdc(2006,1360) = mdc(1360, 2006 mod 1360) = mdc(1360,646) = mdc(646,1360 mod 646) = mdc(646,68) = mdc(68, 646 mod 68) = mdc(34, 68 mod 34) = mdc(68, 0) = 68
   Logo, não é possível encontrar o inverso multiplicativo utilizando a equação do algoritmo de euclides estendido.

c) **550 mod 1769**

Verificando mdc(550,1769) = 1
mdc(1769,550) = mdc(550, 1769 mod 550) = mdc(550,119) = mdc(119,550 mod 119) = mdc(119,74) = mdc(74,119 mod 74) = mdc(74,45) = mdc(45,74 mod 45) = mdc(45,29) = mdc(29, 45 mod 29) = mdc(29,16) = mdc(16, 29 mod 16) = mdc(16, 13) = mdc(13, 16 mod 13) = mdc(13, 3) = mdc(3, 13 mod 3) = mdc(3, 1) = mdc(1, 3 mod 1) = mdc(1, 0) = 1
Logo a equação 1769y mod 550 = 1 é válida e portanto y = 379 que é o inverso de 1769. Para 550y mod 1769 = 1, y = 550 que é o inverso de 550.

7. Determine o inverso multiplicativo de x^3 + x + 1 em GF(2^4), com m(x) = x^4 + x + 1.
R: Chamando a função *xgdc(a,b)* no SegeMath obtemos a dupla (1, x^2 + 1, 0). Dessa forma, como especificado temos que o mdc(a,b) = 1, u = x^2 + 1 e v = 0.
Sabemos pela fórmula do algoritmo de euclides estendido que mdc(a,b) = ua + vb, assim o u e v representam os inversos. Como u = a^-1 = x^2 + 1 e v = b^-1 = 0, logo não existem inverso de b.

8. Para a aritmética de polinômios com coeficientes em Z_{10}, realize os seguintes cálculos:
(a) (7x + 2) − (x^2 + 5) = 7x + 2 - x^2 - 5 = -x^2 + 7x + -3

(b) (6x^2 + x + 3) × (5x^2 + 2) = 30x^4 + 12x^2 + 5x^3 + 2x + 15x^2 + 6
= 30x^4 + 5x^3 + 15x^2 + 2x + 6