#3 continue $(x^2+x+1)(x+1)(x^3+x^2+x+1) + (x^2+x+1)(x^4+x+1) + (x^3+x^2+x+1)$

$(x^2+x+1)(x+1)(x^3+x^2+x+1) + (x^3+x^2+x+1) + (x^2+x+1)(x^4+x+1)$

$1 = (x^3+x^2+x+1)[(x^2+x+1)(x+1) + \square] + (x^2+x+1)(x^4+x+1)$

$x^3+2x^2+2x+1+1$

$1 = [(x^3+x^2+x+1)(x^3) + (x^2+x+1)(x^4+x+1)] \bmod (x^4+x+1)$

$1 = (x^3+x^2+x+1)(x^3) \bmod (x^4+x+1) + 0$

answer $= x^3$

#4 $n = p \cdot q$ | $d = e^{-1} \bmod \phi(n)$, $\phi(n) = (p-1)(q-1)$ | encrypt $y = x^e \bmod n$, decrypt $x = y^d \bmod n$ | $e > 1$ & $e <$

$p = 367$

1) $q = 373$ $n = (367)(373) = 136,891$ $\phi(n) = (367-1)(373-1) = 136,152$

2) $136,152 \to 68,256 \to 22,752$ has remander so $e = 5$ (/2, /3, /5)

3) $d = 5^{-1} \bmod 136,512$ egcd $(136,512, 5) \to$ egcd $(5, 136,512 \bmod 5)$

$136,512 = (27302)(5) + 2$

$2 = -(27302)(5) + (136,512)(1)$

egcd $(5, 2) \to (2, 5 \bmod 2)$

$5 = (2)(2) + 1 \Rightarrow 1 = -(2)(2) + 5 \Rightarrow 1 = -2((-27305)(5) + (136$

$1 = [(54460)(5) - (2)(136512) + 5] \bmod 136512$

$1 = (54460)(5) \bmod 136512 - 0 + 5$

$1 = 5(54460 + 1)$ ← factor out 5

$1 = 5(54461)$ so $d = 54461$

encrypt $y = 5^5 \bmod 136,891 = 3125$

decrypt $x = 3125^{54461} \bmod 136891 = 5$ ✓

#5 $13 \Rightarrow 1101$

$12^0 \Rightarrow 1$

$12^{01} \Rightarrow (1)^2 \cdot 12 = 12 \bmod 13 = 12$

$12^{011} \Rightarrow (12)^2 \cdot 12 = 1728 \bmod 13 = 12$

$12^{0110} \Rightarrow (12)^2 \Rightarrow 144 \bmod 13 = 1$

$12^{01101} \Rightarrow (1)^2 \cdot 12 = 12 \bmod 13 = 12$

$= 12$

$12^{13} \bmod 13 = \boxed{12}$

Homework 5

#1) egcd (59, 55) -> egcd (55, 59 mod 55)

$59 = (1)(55) + 4$

$4 = -(1)(55) + (59)(1)$

egcd (55, 4) -> egcd (4, 55 mod 4)

$55 = (13)(4) + 3$

$3 = -(13)(4) + (55)(1)$

$3 = -13[-(1)(55) + (59)(1)] + (55)(1)$

$3 = (13)(55) - (59)(13) + (55)(1)$

$3 = (14)(55) - (59)(13)$

egcd (4, 3) -> egcd (3, 4 mod 3)

$4 = (1)(3) + 1 \Rightarrow 1 = -(1)(3) + (4)(1)$

$1 = -1[(14)(55) - (59)(13)] + (1)[-(1)(55) + (59)(1)]$

$1 = (-14)(55) + (59)(13) + (-1)(55) + (59)(1)$

$1 = (-15)(55) + (14)(59)$

egcd (3, 1) -> egcd (1, 3 mod 1)

$3 = 3(1) + 0$

$3 = 3$

#2) $55^{-1} \bmod 59$ -> egcd (59, 55)

$(1) = [(-15)(55) + (14)(59)] \bmod 59$

$1 = (-15)(55) \bmod 59 + 0$

$1 = (-15) \bmod 59 \ (55) + 0$

$1 = (44)(55)$ $\quad A A^{-1} \bmod n = 1 \quad 55^{-1} \bmod 59 = 44$

#3) egcd $(x^4 + x + 1, x^3 + x^2 x + + 1)$

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

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

egcd $(x^3 + x^2 + x + 1, x)$

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

$1 = -(x^2 + x + 1)(x) + (x^3 + x^2 + x + 1)(1) \bmod 2$ * get rid of negative

$1 = (x^2 + x + 1)[(x+1)(x^3 + x^2 + x + 1) + (1)(x^4 + x + 1)] + (x^3 + x^2 + x + 1)(1)$