[1] Find a pair of inverse ring isomorphisms between $\mathbb{Z}/91\mathbb{Z}$ and $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$. Show that your maps are in fact inverse to each other. Using these maps, compute 5^{26} mod 91.

$$\begin{array}{c|ccc} & a & b & c \\ \hline ① & 13 & 0 & 1 \\ ② & 7 & 1 & 0 \\ & 1 & 2 & -1 \end{array} \Big\} \; a = 7b + 13c \quad \Rightarrow \quad 1 = 2\cdot 7 - 1\cdot 13$$

$2② - ①$

$$\mathbb{Z}/91\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$$

$$m \xmapsto{f} (m, m) \bmod (7, 13)$$

$$-1\cdot 13 \longleftarrow (1, 0)$$

$$2\cdot 7 \qquad (0, 1)$$

$$1 \qquad (1, 1)$$

$$-13x + 2\cdot 7y \bmod 91 \xleftarrow{g} (x, y)$$

$$g(f(m)) = g(m, m) = -13m + 2\cdot 7m = m$$

$$f(g(x, y)) = f(-13x + 2\cdot 7y) = (-13x, 2\cdot 7y) = (x, y)$$

$(\mathbb{Z}/7\mathbb{Z})^* \cong C_6 \quad 5^6 \equiv 1 \quad 5^{26} \equiv 5^2 \equiv 4$

$(\mathbb{Z}/13\mathbb{Z})^* \cong C_{12} \quad 5^{12} \equiv 1 \quad 5^{26} \equiv 5^2 \equiv -1$

$$5^{26} = (4, -1) \xmapsto{g} -13\cdot 4 - 2\cdot 7 = -52 - 14 = -66$$

$$\boxed{5^{26} \equiv 25 \bmod 91}$$

5^{26} mod 7 = 4

5^{26} mod 13 = 12

5^{26} mod 91 = 25

[2] Find a pair of inverse ring isomorphisms between $\mathbb{Z}/187\mathbb{Z}$ and $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$. Show that your maps are in fact inverse to each other. Using these maps, compute 3^{32} mod 187.

	a	b	c	
①	17	0	1	
②	11	1	0	
③	6	-1	1	①−②
④	1	-3	2	2③−②

$a = 11b + 17c \Rightarrow 1 = -3\cdot 11 + 2\cdot 17$

$-33 + 44$ ✓

$$\mathbb{Z}/187\mathbb{Z} \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$$

$$m \xmapsto{f} (m, m) \bmod (11, 17)$$

$$2\cdot 17 \longleftarrow (1, 0)$$

$$-3\cdot 11 \qquad (0, 1)$$

$$1 \qquad (1, 1)$$

$$2\cdot 17x - 3\cdot 11y \bmod_{187} \xleftarrow{g} (x, y)$$

$$g(f(m)) = g(m, m) = 2\cdot 17m - 3\cdot 11m = m \quad ✓$$

$$f(g(x,y)) = f(2\cdot 17x - 3\cdot 11y) = (2\cdot 17x, -3\cdot 11y)$$

$$\equiv (x, y) \quad ✓$$

$(\mathbb{Z}/11\mathbb{Z})^* \cong C_{10} \quad 3^{10} \equiv 1 \quad 3^{32} \equiv 3^2 = 9$

$(\mathbb{Z}/17\mathbb{Z})^* \cong C_{16} \quad 3^{16} = 1 \quad 3^{32} = 1$

$$3^{32} = (9, 1) \xmapsto{g} 2\cdot 17\cdot 9 - 3\cdot 11\cdot 1$$

$$18\cdot 17 - 33$$

$$16\cdot 17 + 1$$

$$16\cdot 16 + 16 + 1$$

$$256 + 16 + 1$$

$$-187$$

$$69 + 16 + 1 = \boxed{86}$$

3^{32} mod 11 = 9

3^{32} mod 17 = 1

3^{32} mod 187 = 86

[3] Find a pair of inverse ring isomorphisms between $\mathbb{Z}/144\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$. Show that your maps are in fact inverse to each other. Using these maps, compute 5^{25} mod 144.

$$\begin{array}{llll} & a & b & c \\ ① & 16 & 0 & 1 \\ ② & 9 & 1 & 0 \\ ③ & 2 & 2 & -1 & 2②-① \\ ④ & 1 & -7 & 4 & ②-4③ \end{array} \quad \left.\right\} a = 9b + 16c \Rightarrow 1 = -7\cdot 9 + 4\cdot 16 = -63 + 64 \checkmark$$

$$\mathbb{Z}/144\mathbb{Z} \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$$

$$m \xmapsto{f} (m, m)$$

$$4\cdot 16 \longleftarrow (1,0)$$

$$\begin{array}{r} 4\cdot 16 \\ -7\cdot 9 \\ \hline 1 \end{array} \qquad \begin{array}{c} (1,0) \\ (0,1) \\ \hline (1,1) \end{array}$$

$$+4\cdot 16x - 7\cdot 9y \text{ mod } 144 \xleftarrow{g} (x, y)$$

$$g(f(m)) = g(m,m) = 4\cdot 16m - 7\cdot 9m = m \checkmark$$

$$f(g(x,y)) = f(4\cdot 16x - 7\cdot 9y) = (4\cdot 16x, -7\cdot 9y) \checkmark$$
$$\equiv (x, y) \text{ mod } (9,16)$$

$$(\mathbb{Z}/9\mathbb{Z})^* = \{1,2,4,5,7,8\} \cong C^6 \qquad 5^6 = 1, \quad 5^{25} = 5$$

$$(\mathbb{Z}/16\mathbb{Z})^* = \{1,3,5,7,9,11,13,15\} \quad \text{order } 8, \ 5 \text{ has order } 2,4 \text{ or } 8 \ (\text{so } 5^8 = 1)$$

$$5^2 = 9 \quad 5^4 = 9^2 = 1 \quad 5^{25} = 5$$

$$5^{25} = (5,5) = 5(1,1) \xmapsto{g} 5\cdot 1 = \boxed{5}$$

(lucky break)

5^{25} mod 9 = 5

5^{25} mod 16 = 5

5^{25} mod 144 = 5

[4] A message is represented as an integer a mod 55. You receive the encrypted message $a^7 \equiv 13 \mod 55$. What is a?

$$\underbrace{\mathbb{Z}/55\mathbb{Z}}_{\substack{x^e = x \text{ for} \\ e \equiv 1 \bmod 20}} \cong \underbrace{\mathbb{Z}/5\mathbb{Z}}_{x^5 = x} \times \underbrace{\mathbb{Z}/11\mathbb{Z}}_{x^{11} = x}$$

$x^e = x$ for $e \equiv 1 \mod 20$ $\Longleftarrow$ $x^e = x$ for $e \equiv 1 \mod 4$, $x^e = x$ for $e \equiv 1 \mod 10$

$20 = \text{lcm}(4, 10)$

Want ℓ so $7\ell \equiv 1 \mod 20$.
Then $(x^7)^\ell = x$ and ℓ^{th} power decodes 7^{th} power

$$\begin{array}{cccc} ① & 20 & 0 & 1 \\ ② & 7 & 1 & 0 \\ & 1 & 3 & -1 \end{array} \quad a = 7b + 20c \qquad 3②-①$$

$\Rightarrow \; 1 = 3 \cdot 7 - 20$

$1 \equiv 3 \cdot 7 \mod 20$

$7^{-1} = \boxed{3} \mod 20$

$(a^7)^3 = a \qquad 13^3 = a \qquad 13 \cdot 13 = 169 = 4 \mod 55$

$13 \cdot 4 = 52$

$\boxed{a = 52}$ is original message

Check $52^7 = 13$? $\qquad 7 = 4 + 2 + 1 \qquad x^7 = x^4 x^2 x$

$= (x^2)^2 x^2 x$

$52 = -3$

$52^2 = 9$

$52^4 = 81 - 55 = 26$

$52^7 = -3 \cdot 9 \cdot 26 = 9 \cdot (-3 \cdot 26 + 55) = 9(-23) = -207$

$+220 = \boxed{13}$ ✓

[5] A message is represented as an integer a mod 91. You receive the encrypted message $a^{17} \equiv 61 \mod 91$. What is a?

$$\mathbb{Z}/91\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$$

$x^7 = x \mod 7$

$x^{13} = x \mod 13$ $\quad 17 \equiv -1 \mod 6 \Rightarrow (x^{17})^6 = (x^{-1})^{-1} = x \mod 7$ (if $\neq 0$)

$17 \equiv 5 \mod 12$

$5 \cdot 5 \equiv 1 \mod 12 \Rightarrow (x^{17})^5 = (x^5)^5 = x \mod 13$

$1 = 2 \cdot 7 - 1 \cdot 13$ from [1]

$m \xmapsto{f} (m, m) \mod (7, 13)$

$(x, y) \xmapsto{g} -13x + 14y \mod 91$

$61 \longmapsto (5, 9) \mod (7, 13)$

$5^{-1} = 3 \mod 7 \quad (5 \cdot 3 = 15 = 1$ ✓$)$

$9^5 = 9 \cdot 81 \cdot 81 = 9 \cdot 3 \cdot 3 = 81 = 3 \mod 13 \quad (78 = 6 \cdot 13)$

and $(3, 3) = 3(1, 1) \xmapsto{g} \boxed{3}$

check $3^{17} \stackrel{?}{=} 61 \mod 91$

$3^{17} = 3^{-1} = 5 \equiv 61 \mod 7$ ✓

$3^{17} = 3^5 = 9 \cdot 9 \cdot 3 = -4 \cdot (-4) \cdot 3 = 48 = 9 \equiv 61 \mod 13$

check $3^{17} \stackrel{?}{=} 61 \mod 91$

$3^{17} = 3 \cdot 3^{16} = 3(((3^2)^2)^2)^2$

$= -3 \cdot 10 = 61$ ✓

$3^2 = 9$

$9^2 = 81 = -10$

$(-10)^2 = 100 = 9$

$9^2 = -10$

[6] A message is represented as an integer a mod 187. You receive the encrypted message $a^9 \equiv 60$ mod 187. What is a?

$$\mathbb{Z}/187\mathbb{Z} \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/17\mathbb{Z}$$

$x^{11} = x$ mod 11, exponents mod 10

$x^{17} = x$ mod 17, exponents mod 16

$9 \cdot 9 = 81 = 1$ mod 10 $\Rightarrow (x^9)^9 = x$ mod 11

$= 1$ mod 16 $\quad$ " $\quad$ " $\quad$ mod 17

so $(x^9)^9 = x$ mod 187

$60 = -6$ mod 11 $\qquad x^9 = x \cdot ((x^2)^2)^2$

$(-6)^2 = 36 = 3 \quad 3^2 = 9 \quad 9^2 = 81 = 4 \quad -6 \cdot 4 = -24 = 9$

$60 = -8$ mod 17

$(-8)^2 = 64 = -4 \quad (-4)^2 = 16 = -1 \quad (-1)^2 = 1 \quad -8 \cdot 1 = -8$

$60^9 = (9, -8)$ mod $(11, 17)$ $\qquad \left(\begin{array}{l} 1 = -3 \cdot 11 + 2 \cdot 17 \text{ from [2]} \\ (x, y) \mapsto 2 \cdot 17x - 3 \cdot 11y \end{array} \right)$

$\mapsto 2 \cdot 17 \cdot 9 + 3 \cdot 11 \cdot 8$

$= 17 \cdot 18 + 11 \cdot 24$

$= 17 \cdot (18 - 11) + 11 \cdot (24 - 17) = 17 \cdot 7 + 11 \cdot 7 = 28 \cdot 7$

$= 210 - 14$

$= 196 = \boxed{9}$

---

check $9^9 \stackrel{?}{=} 60$ mod 187 $\qquad 3 \cdot 187 = 600 - 3 \cdot 13 = 561$

$9^2 = 81 \quad 9^3 = 9 \cdot 81 = 729 - 561 = 168 = -19$

$(-19)^2 = (20-1)^2 = 400 - 40 + 1 = 361 - 374 = -13$

$(-19)(-13) = (20-1)13 = 260 - 13 = 247 = 187 + \boxed{60}$

✓

[7] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)(x-3) = 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

$$\mathbb{R}[x]/((x-2)(x-3)) \cong \mathbb{R}[x]/(x-2) \times \mathbb{R}[x]/(x-3)$$

$$\begin{array}{ccc} x-2 & 1 & 0 \\ x-3 & 0 & 1 \\ 1 & 1 & -1 \end{array} \quad \Rightarrow \quad 1 = (x-2) - (x-3)$$

$$\underset{\text{mod } (x-2,\, x-3)}{(f,g)} \longmapsto \underset{\text{mod } (x-2)(x-3)}{-(x-3)f + (x-2)g}$$

$$e^{xt} = e^{2t} \text{ mod } x-2$$
$$e^{xt} = e^{3t} \text{ mod } x-3$$

$$(e^{2t}, e^{3t}) \mapsto -e^{2t}(x-3) + e^{3t}(x-2)$$

so $$\boxed{e^{At} = -e^{2t}(A-3I) + e^{3t}(A-2I)}$$

check $A = \begin{bmatrix} 2 & \\ & 3 \end{bmatrix}$ $\quad e^{At} = \begin{bmatrix} e^{2t} & \\ & e^{3t} \end{bmatrix}$

$$-e^{2t}\left(\begin{bmatrix} 2 & \\ & 3 \end{bmatrix} - \begin{bmatrix} 3 & \\ & 3 \end{bmatrix}\right) + e^{3t}\left(\begin{bmatrix} 2 & \\ & 3 \end{bmatrix} - \begin{bmatrix} 2 & \\ & 2 \end{bmatrix}\right)$$

$$= e^{2t}\begin{bmatrix} 1 & \\ & 0 \end{bmatrix} + e^{3t}\begin{bmatrix} 0 & \\ & 1 \end{bmatrix} \quad ✓$$

[8] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)^2 = 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

$\mathbb{R}[x]/(x-2)^2$

$$e^{xt} = 1 + xt + x^2t^2/2 + \ldots$$

$$e^{xt} = e^{2t} e^{(x-2)t}$$

$$= e^{2t}(1 + (x-2)t)$$

mod $(x-2)^2$

so $\boxed{e^{At} = e^{2t}(I + (A-2I)t)}$

check: $A = \begin{bmatrix} 2 & 1 \\ & 2 \end{bmatrix}$ $\quad e^{At} = \begin{bmatrix} e^{2t} & te^{2t} \\ & e^{2t} \end{bmatrix}$

$$e^{2t}(I + (A-2I)t)$$

$$= e^{2t} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + te^{2t} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$ ✓

[9] Let A be an $n \times n$ matrix with entries in $\mathbb{R}$, satisfying the polynomial relation

$$(x-2)^2(x-3) = 0$$

Find a formula for e^{At} as a polynomial expression in A. Give an example of a matrix A for which this is the minimal polynomial relation, and check your formula using this matrix.

$$\mathbb{R}[x]/(x-2)^2(x-3) \cong \mathbb{R}[x]/(x-2)^2 \times \mathbb{R}[x]/(x-3)$$

$$\begin{array}{ll|ll} ① & x^2-4x+4 & 0 & 1 \\ ② & x-3 & 1 & 0 \\ & 1 & -x+1 & 1 \end{array} \qquad ①-(x-1)②$$

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

$$\Longrightarrow \quad 1 = -(x-1)(x-3) + (x-2)^2$$

so $\quad (f,g) \bmod (x-2)^2, (x-3)$

$$\longmapsto -(x-1)(x-3)f + (x-2)^2 g$$

$$e^{xt} = e^{2t}(1+(x-2)t) \bmod (x-2)^2$$
$$e^{xt} = e^{3t} \qquad \text{''} \quad (x-3)$$

$$(e^{2t}(1+(x-2)t), e^{3t}) \longmapsto -(x-1)(x-3)e^{2t}$$
$$-(x-1)(x-3)(x-2)te^{2t}$$
$$+(x-2)^2 e^{3t}$$

$$\boxed{e^{At} = -(A-I)(A-3I)\left[e^{2t} + (A-2I)te^{2t}\right] + (A-2I)^2 e^{3t}}$$

check: $A = \begin{bmatrix} 2 & 1 & \\ & 2 & \\ & & 3 \end{bmatrix}$ $A-I = \begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 2 \end{bmatrix}$ $A-2I = \begin{bmatrix} 0 & 1 & \\ & 0 & \\ & & 1 \end{bmatrix}$ $A-3I = \begin{bmatrix} -1 & 1 & \\ & -1 & \\ & & 0 \end{bmatrix}$

$$e^{At} = \begin{bmatrix} e^{2t} & te^{2t} & \cdot \\ \cdot & e^{2t} & \cdot \\ \cdot & \cdot & e^{3t} \end{bmatrix} \overset{?}{=} \begin{bmatrix} 1 & 0 & \\ 0 & 1 & \\ & & 0 \end{bmatrix}\left(e^{2t} + \begin{bmatrix} 0 & 1 & \\ & 0 & \\ & & 1 \end{bmatrix} te^{2t}\right) + \begin{bmatrix} 0 & & \\ & 0 & \\ & & 1 \end{bmatrix} e^{3t}$$

✓

[10] Construct the finite field $\mathbb{F}_4$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_2$. What are the two roots of your irreducible polynomial?

$\mathbb{F}_4 = \mathbb{F}_2[x]/f(x)$ for $f(x) = x^2+ax+b$ irreducable.

(for deg ≤ 3, $\Leftrightarrow$ no roots)

poly	coefs	x=0	x=1
x^2	1 0 0	0	1
$x^2 + 1$	1 0 1	1	0
$x^2 + x$	1 1 0	0	0
$x^2 + x + 1$	1 1 1	1	1

$\Rightarrow$ x^2+x+1 irred

$\mathbb{F}_4 = \mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$

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

$f(\alpha) = 0$ by construction

$\mathbb{F}_4$ α $\alpha+1$

$\mathbb{F}_2$ 0 1

$= \{0, 1, \alpha, \alpha+1\}$

so $f(\alpha+1)=0$ must be other root

check: $(x-\alpha)(x-(\alpha+1))$

$= (x+\alpha)(x+\alpha+1)$ (no signs in char 2)

$= x^2 + (\alpha+\alpha+1)x + \alpha(\alpha+1)$

$= x^2 + x + 1$ ✓

$\alpha(\alpha+1)$ add twice

$= \cancel{\alpha^2+\alpha+1}+1$

cross out $\alpha^2+\alpha+1$

$= 1$

we also know Frobenius $x \mapsto x^2$ circles through roots

$\alpha^2 = \cancel{\alpha^2+\alpha^2}+\alpha+1 = \alpha+1$ ✓

[11] Construct the finite field $\mathbb{F}_8$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 3 with coefficients in $\mathbb{F}_2$. What are the three roots of your irreducible polynomial?

$\mathbb{F}_8 = \mathbb{F}_2[\alpha]/(f(\alpha))$ where $f(x) = x^3 + ax + by + c$ irreducible. Deg 3, so $\Leftrightarrow$ no roots

$$f(0) = 0 \Leftrightarrow \text{const term} = 0$$
$$f(1) = 1 \Leftrightarrow \text{even \# terms.}$$

So irred $f(x)$ is $f(x) = x^3 + \underbrace{ax + by}_{\text{choose one}} + 1$, odd # terms.

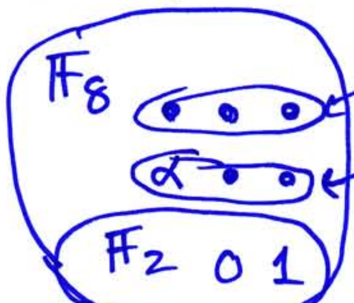
$f(x) = \begin{matrix} x^3 + x^2 + 1 \\ x^3 + x + 1 \end{matrix}$ two choices.

---

we choose $f(x) = x^3 + x + 1$

$$\mathbb{F}_8 = \mathbb{F}_2[\alpha]/(\alpha^3 + \alpha + 1) = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

Picture:



roots of $x^3 + x^2 + 1 = 0$

roots of $x^3 + x + 1 = 0$

And Frobenius $x \mapsto x^2$ fixes $\mathbb{F}_2$, moves $\mathbb{F}_8$ in orbits of size 3

$((x^2)^2)^2 = x^8 = x$ on $\mathbb{F}_8$

We use Frobenius to find the other roots of $x^3 + x + 1 = 0$.

$$\alpha^2 = \alpha^2$$
$$(\alpha^2)^2 = \alpha^4 = \alpha \cdot \alpha^3 = \alpha(\alpha+1) = \alpha^2 + \alpha \quad (\text{because } \alpha^3 = \alpha + 1)$$
$$(\alpha^2+\alpha)^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + \alpha^2 = \alpha \quad \text{☑ cycle closes up}$$

So

$$\boxed{x^3 + x + 1 = (x+\alpha)(x+\alpha^2)(x+\alpha^2+\alpha)}$$

[11.11] Before checking, we learn shorter notation for $\mathbb{F}_8$

$000 = 0$	$100 = \alpha^2$
$001 = 1$	$101 = \alpha^2+1$
$010 = \alpha$	$110 = \alpha^2+\alpha$
$011 = \alpha+1$	$111 = \alpha^2+\alpha+1$

Write bit vector of $\mathbb{F}_2$ coefficients of any polynomial in α, use $\alpha^3 = \alpha+1$ to reduce to deg ≤ 2

Redo earlier work for practice:

$$\alpha^4 = \begin{array}{r} 10000 \\ +\ 1011 \\ \hline 110 \end{array} = \alpha^2+\alpha$$

add $\alpha(\alpha^3+\alpha+1) = 0$ (our defining relation)

$$(\alpha^2+\alpha)^2 \qquad \begin{array}{c|ccc} & \alpha^2 & \alpha & 0 \\ \hline \alpha^2 & \alpha^4 & \alpha^3 & 0 \\ \alpha & \alpha^3 & \alpha^2 & 0 \\ 0 & 0 & 0 & 0 \end{array} = \alpha^4+\alpha^2$$

(sum diagonals)

do as

$$\begin{array}{c|ccc} & 1 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} = \begin{array}{r} 10100 \\ 1011 \\ \hline 011 \end{array} = \alpha$$

$$(x+010)(x+100)(x+110)$$

$$= (x^2 + \underbrace{(010+100)}_{110}x + 010 \cdot 100)(x+110)$$

just add mod 2

$$\begin{array}{c|ccc} & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array} = \begin{array}{r} 1000 \\ 1011 \\ \hline 011 \end{array}$$

$$= (x^2 + 110\,x + 011)(x+110)$$

$$\begin{array}{c|cc} & 1\cancel{x} & 110 \\ \hline 1 & 1 & 110 \\ 110 & 110 & 110 \cdot 110 \\ 011 & 011 & 011 \cdot 110 \end{array} = \begin{array}{|cc|} \hline 1 & 110 \\ 110 & 010 \\ 011 & 001 \\ \hline \end{array}$$

(sum diagonals)

$$= x^4 + 001\,x + 001$$

$$= \boxed{x^4 + x + 1}$$

✓

$$\begin{array}{c|ccc} & 1 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array} = \begin{array}{r} 10100 \\ 1011 \\ \hline 010 \end{array} \qquad \begin{array}{c|ccc} & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{array} = \begin{array}{r} 01010 \\ 1011 \\ \hline 001 \end{array}$$

(some people may prefer inventing notation like this, to condense a problem. Others may prefer writing everything out longhand in $(\alpha^2+\alpha)x$, etc...)

[11] Construct the finite field $\mathbb{F}_8$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 3 with coefficients in $\mathbb{F}_2$. What are the three roots of your irreducible polynomial?

$\mathbb{F}_8 = \mathbb{F}_2[\alpha]/f(\alpha)$ for $f(x) = x^3 + ax^2 + bx + c$ irred

$\iff$ no roots, (deg = 3)

		$x=0$	$x=1$
x^3	1 0 0 0	~~0~~	~~1~~
$x^3 \quad +1$	1 0 0 1	~~1~~	~~0~~
$x^3 \quad +x$	1 0 1 0	~~0~~	~~0~~
$x^3 \quad +x+1$	1 0 1 1	1	1
x^3+x^2	1 1 0 0	~~0~~	~~0~~
$x^3+x^2 \quad +1$	1 1 0 1	1	1
x^3+x^2+x	1 1 1 0	~~0~~	~~1~~
x^3+x^2+x+1	1 1 1 1	~~1~~	~~0~~

$f(x) = x^3 + x + 1$ or

$x^3 + x^2 + 1$

(deg 3, odd # terms, const term)

use $f(x) = x^3 + x + 1$, simpler

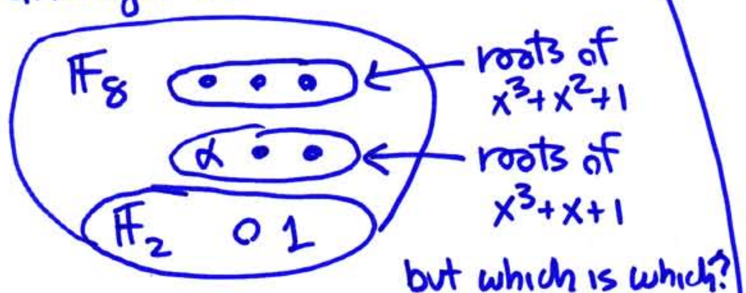
$\mathbb{F}_8 = \mathbb{F}_2[\alpha]/\alpha^3+\alpha+1$

$\mathbb{F}_8$ α^2 α^2+1 $\alpha^2+\alpha$ $\alpha^2+\alpha+1$

α $\alpha+1$

$\mathbb{F}_2$ 0 1

arranged as



Use Frobenius to find roots

$f(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)$

$\alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha+1) = \alpha^2 + \alpha$

$f(\alpha) = 0$ by construction

~~f(α²) =~~

$f(\alpha^2) = \alpha^6 + \alpha^2 + 1$

$= (\alpha+1)^2 + \alpha^2 + 1$

$= \alpha^2 + 1 + \alpha^2 + 1 = 0$ ✓

$f(\alpha^2+\alpha) = (\alpha^2+\alpha)^3 + \alpha^2 + \alpha + 1$

$= \alpha^6 + 3\alpha^5 + 3\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1$

$= \cancel{\alpha^6} + \cancel{\alpha^5} + \cancel{\alpha^4} + \cancel{\alpha^3} + \cancel{\alpha^2} + \cancel{\alpha} + \cancel{1}$

$\cancel{\alpha^3} \qquad + \cancel{\alpha} + \cancel{1}$

0 ✓

(add multiples of $\alpha^3+\alpha+1$ to aid in crossing out)

$\boxed{\text{roots are } \alpha, \alpha^2, \alpha^2+\alpha}$

[12] Construct the finite field $\mathbb{F}_9$ as an extension of $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, by finding an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_3$. What are the two roots of your irreducible polynomial?

$\mathbb{F}_9 = \mathbb{F}_3[\alpha]/f(\alpha)$ for $f(x) = x^2 + ax + b$ irred (no roots) deg=2

		0 1 2
x^2	1 0 0	~~0~~
$x^2 + 1$	1 0 1	1 2 2
$x^2 + 2$	1 0 2	~~2 0~~
$x^2 + x$	1 1 0	~~0~~
$x^2 + x + 1$	1 1 1	~~1 0~~
$x^2 + x + 2$	1 1 2	2 1 2
$x^2 + 2x$	1 2 0	~~0~~
$x^2 + 2x + 1$	1 2 1	1 1 0
$x^2 + 2x + 2$	1 2 2	2 2 1
$x=0$	0 0 1	
$x=1$	1 1 1	
$x=2$	1 2 1	

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

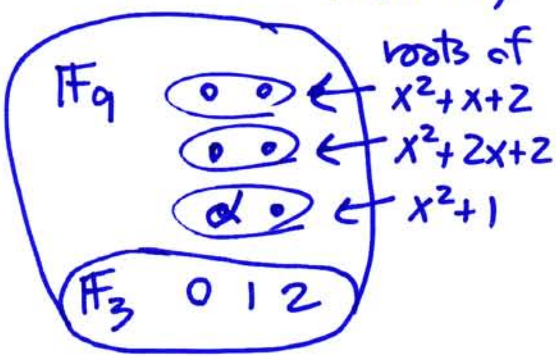
$x^2 + x + 2$

$x^2 + 2x + 2$

- const term $\neq 0$
- coefs add $\neq 0$
- " + twice middle coef $\neq 0$

use x^2+1, easiest

$\mathbb{F}_9 = \mathbb{F}_3[\alpha]/(\alpha^2+1) = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$



other root is α^3

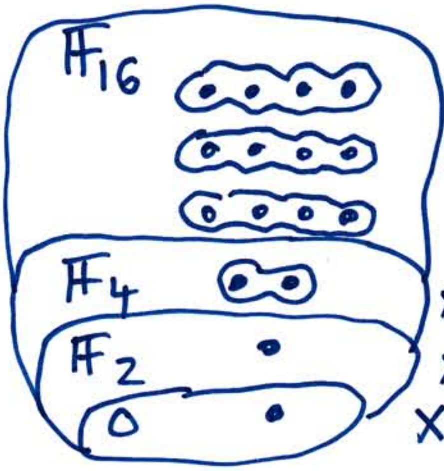
$\alpha^3 = \alpha(\alpha^2) = \alpha(+2) = +2\alpha$

$(x-\alpha)(x-2\alpha) = x^2 - 3\alpha x + 2\alpha^2$

$= x^2 + 1$ ✓

[13] Construct the finite field $\mathbb{F}_{16}$ as an extension of $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, by finding an irreducible polynomial of degree 4 with coefficients in $\mathbb{F}_2$. What are the four roots of your irreducible polynomial?

$$\mathbb{F}_{16} = \mathbb{F}_2[\alpha]/(f(\alpha)) \quad \text{for } \underbrace{f(x) = x^4 + ax^3 + bx^2 + cx + 1}_{\text{irreducible}}$$



$$\left.\begin{matrix} x^{15} = 1 \\ x^3 = 1 \end{matrix}\right\} x^{16} - x = 0 \qquad \left.\begin{matrix} x^3 = 1 \\ x = 1 \end{matrix}\right\} x^4 - x = 0 \qquad \left.\begin{matrix} x = 1 \\ x = 0 \end{matrix}\right\} x^2 - x = 0$$

$$16 = 1 + 1 + \underbrace{2 + 4 + 4 + 4}_{\text{irred polys of these degs}}$$

$f(0) \neq 0 \iff$ constant term 1

$f(1) \neq 0 \iff$ odd # terms

also $g(x) = x^2 + x + 1$ irred deg 2

$f(x) = g(x)^2$ also irreducible

	x^2	x	1
x^2	x^4	x^3	x^2
x	x^3	x^2	x
1	x^2	x	1

$= x^4 + x^2 + 1$

quicker:

	1	1	1
1	1	1	1
1	1	1	1
1	1	1	1

$= 10101$

but of course $y \mapsto y^2$ is Frobenius, linear:

$(x^2 + x + 1)^2 = (x^2)^2 + (x)^2 + (1)^2 = x^4 + x^2 + 1$ in char 2.

This leaves 3 irred polys of deg 4, as expected by above diagram:

$$\boxed{\begin{matrix} x^4 + x^3 + 1 \\ x^4 + x + 1 \\ x^4 + x^3 + x^2 + x + 1 \end{matrix}}$$

we choose easiest, for relation $x^4 = x + 1$

So $\boxed{\mathbb{F}_{16} = \mathbb{F}_2[\alpha]/(\alpha^4 + \alpha + 1) \quad \text{or } \alpha^4 = \alpha + 1}$

α is a root of $f(x) = x^4 + x + 1$ by design. Iterate Frobenius: $\alpha^2, \alpha^4, \alpha^8$ are other roots, and $\alpha^{16} = \alpha$

$$\boxed{f(x) = x^4 + x + 1 = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8)}$$

[..13] Check: α^2 doesn't reduce, it is deg < 4

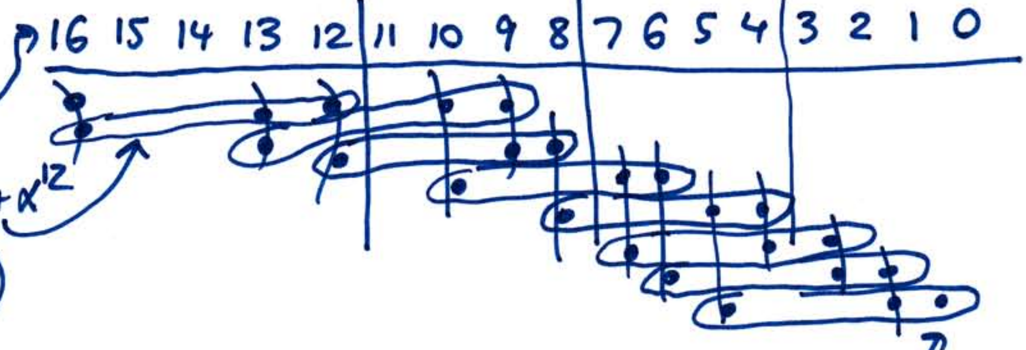
$\alpha^4 = \alpha + 1$ is our basic relation

$$\alpha^8 = (\alpha^4)^2 = (\alpha+1)^2 = \alpha^2+1$$

$$\alpha^{16} = (\alpha^8)^2 = (\alpha^2+1)^2 = (\alpha^2)^2 + (1)^2 = \alpha^4+1 = (\alpha+1)+1 = \alpha \;\boxed{\checkmark}$$

Or make a game

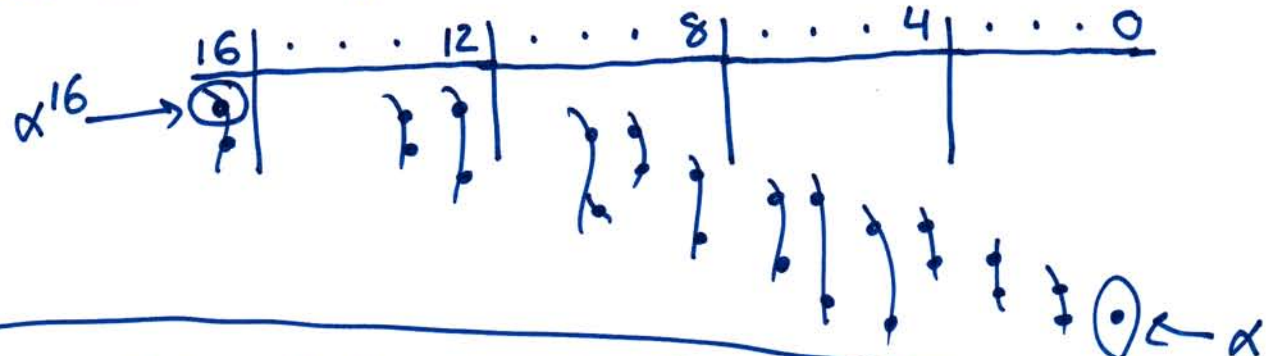
power of α



$\alpha^{12}(\alpha^4+\alpha+1) = \alpha^{16}+\alpha^{13}+\alpha^{12}$

(relation slides over by mult by α^n)

redo more succintly:



$$(x+\alpha)(x+\alpha^2)(x+\alpha+1)(x+\alpha^2+1)$$

$$= (x+0010)(x+0100)(x+0011)(x+0101)$$

(write $a\alpha^3+b\alpha^2+c\alpha+d$ = abcd in binary)

add mod 2, multiply as polys

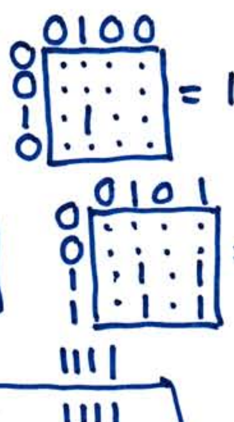
	1	0100
1	1	0100
0010	0010	0010 · 0100

$0010 \cdot 0100 = 1000$ → $x^2 + 0110\,x + 1000$

	1	0101
1	1	0101
0011	0011	0011·0101

$0011 \cdot 0101 = 1111$ → $x^2 + 0110\,x + 1111$

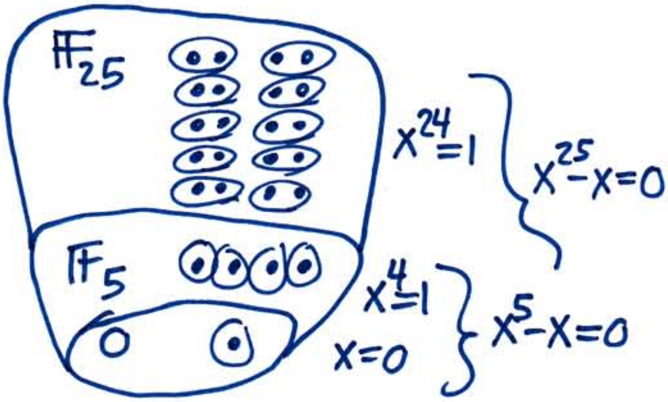
	1	0110	1111
1	1	0110	1111
0110	0110	0110·0110	0110·1111
1000	1000	1000·0110	1000·1111



$$x^4 + \left[\begin{array}{r}0010100\\1111\\1000\\\hline 10011\\1\;\;11\\\hline 0\end{array}\right]0x^2 + \begin{array}{r}0110000\\0100010\\\hline 10010\\1\end{array}\,x + \begin{array}{r}1111000\\1000\\\hline 1\end{array}\,1$$

$$= \boxed{x^4 + x + 1} \quad \checkmark$$

[14] Construct the finite field $\mathbb{F}_{25}$ as an extension of $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$, by finding an irreducible polynomial of degree 2 with coefficients in $\mathbb{F}_5$. What are the two roots of your irreducible polynomial?



$$\mathbb{F}_{25} = \mathbb{F}_5[\alpha]/f(\alpha)$$

$$f(x) = x^2 + ax + b$$

$a \in \{0,1,2,3,4\}$

$b \in \{1,2,3,4\}$

20 choices, 10 are irreducible
other 10 have a root

so probability ½ we find irred by guessing.

poly	1	2	3	4
x^2+1	2	0	0	2
x^2+2	3	1	1	3

study, add 1

(why?
$\{1,4\} = \{1,-1\} \subseteq \{1,2,3,4\}$
is order 2 subgroup of $C_4 = \mathbb{F}_5^*$
squaring sends everyone to this subgp.)

so $\boxed{\mathbb{F}_{25} = \mathbb{F}_5[\alpha]/(\alpha^2+2)}$ (so $\mathbb{F}_{25} = \mathbb{F}_5(\sqrt{3})$)

$\alpha^2+2=0 \iff \alpha^2=3$

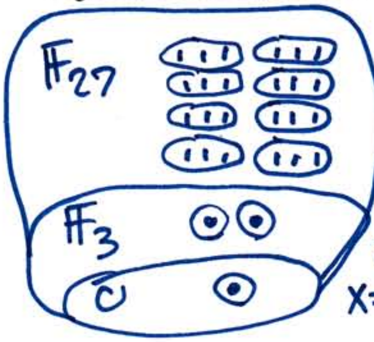
$$x^2+2 = (x-\alpha)(x-\alpha^5)$$

$$= x^2 - \underbrace{(\alpha^5+\alpha)}_{0}x + \underbrace{\alpha^6}_{3^3=27=2 \text{ mod } 5}$$

$$= x^2+2 \quad \boxed{\checkmark}$$

$\alpha^5 = \alpha(\alpha^2)^2$
$= \alpha \cdot 3^2$
$= -\alpha$
$\text{mod}(\alpha^2+2, 5)$

[15] Construct the finite field $\mathbb{F}_{27}$ as an extension of $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$, by finding an irreducible polynomial of degree 3 with coefficients in $\mathbb{F}_3$. What are the three roots of your irreducible polynomial?



$x^{26}=1 \Big\} \; x^{27}=x$

$\left.\begin{array}{l} x^2=1 \\ x=0 \end{array}\right\} x^3=x$

of course

x	0	1	2
x^3	0	1	2
x^3-x	0	0	0
x^3-x+1	1	1	1

no roots

$\mathbb{F}_{27} = \mathbb{F}_3[\alpha]/(f(\alpha))$

$f(\alpha) = x^3 + ax^2 + bx + c$

$18 = 3\cdot 3\cdot 2$ choices with $c \neq 0$

8 irred, so roughly half, try guessing

$\mathbb{F}_{27} = \mathbb{F}_3[\alpha]/(\alpha^3-\alpha+1)$

or $\alpha^3 = \alpha - 1$

$$\mathbb{F}_3 = \{0,1,2\} = \{0,1,-1\} = \{0 + -\}$$

$$\mathbb{F}_{27} = \{a\alpha^2 + b\alpha + c\} = \{abc\}$$ use $0,+,-$ base 3

$$x^3 - x + 1 = (x-\alpha)(x-\alpha^3)(x-\alpha^9) \quad \text{where } \alpha^3 = \alpha - 1$$

$$\alpha^3 = \alpha - 1 = 0{+}{-}$$

$$\alpha^9 = (\alpha-1)^3 = \alpha^3 - 1 = \alpha - 1 - 1 = \alpha + 1 = 0{+}{+}$$

$$(x - 0{+}0)(x - 0{+}{-})(x - 0{+}{+})$$

$$= (x + 0{-}0)(x + 0{-}{+})(x + 0{-}{-})$$

$$= \left(x^2 + \frac{\begin{array}{c}0{-}0\\0{-}{+}\end{array}}{0{+}{+}}\,x + {+}{-}0\right)(x + 0{-}{-})$$

$$= \begin{array}{c|cc} & 1 & 0{-}{-} \\ \hline 1 & 1 & 0{-}{-} \\ 0{+}{+} & 0{+}{+} & {-}{+}{-} \\ {+}{-}0 & {+}{-}0 & {-}0{+}0 \end{array} = x^3 + \left(\frac{\begin{array}{c}{+}{-}0\\{-}{+}{-}\end{array}}{00{-}}\right)x + \left(\frac{\begin{array}{c}{-}0{+}0\\{+}\;{-}{+}\end{array}}{+}\right)$$

$$= \boxed{x^3 - x + 1}$$ ✓

[**16**] Let $\mathbb{Z}[x]$ be the ring of polynomials in x with coeficients in $\mathbb{Z}$. Give an example of a maximal ideal $I \subset \mathbb{Z}[x]$. Give an example of an ideal I which is prime but not maximal. Are there any ideals I such that the quotient $\mathbb{Z}[x]$ is a field not of the form $\mathbb{Z}/p\mathbb{Z}$ for a prime p?

$I = (x,2)$ is maximal $\Leftrightarrow$ $\mathbb{Z}[x]/(x,2) \cong \mathbb{Z}/2\mathbb{Z}$ is a field ✓

$I = (x)$ is prime $\Leftrightarrow$ $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is a domain ✓

$$\mathbb{Z}[x]/(2, x^2+x+1) \cong \mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$$

$$\cong \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$$

$|\mathbb{F}_4| = 4$, and 4 isn't prime, so $\mathbb{F}_4 \neq \mathbb{Z}/p\mathbb{Z}$ for any prime p