

7-2 Let $\alpha = s+ti$. Then $\alpha - s = ti$
 $(\alpha - s)^2 = -t^2$
 $\alpha^2 - 2\alpha s + s^2 + t^2 = 0$

Thus α is a root of $X^2 - 2sX + s^2 + t^2 = p(X)$

Substituting shows $s-ti$ is also a root.

$p(X)$ must be irreducible since it is degree 2 w/ no roots in \mathbb{Q} .

Thus $s+ti$ and $s-ti$ are conjugates.

If $t=0$, s is a root of $X-s$ so s is conjugate only to itself.

7-3 $p(X) = X^2 + \frac{1}{3}X - 1$

Let $q_1(X) = X^3 + 1$ $q_2(X) = -\frac{1}{3}X^2 + X + 1$ $q_3(X) = \frac{10}{9}X + \frac{2}{3}$

Notice $q_1 - q_2 = X^3 + \frac{1}{3}X^2 - X = X \cdot p(X)$ so $q_1 \sim q_2$

$q_2 - q_3 = -\frac{1}{3}X^2 - \frac{1}{9}X + \frac{1}{3} = -\frac{1}{3} \cdot p(X)$ so $q_2 \sim q_3$

Also $(X^4 + X^2 + 1) - (-\frac{28}{27}X + \frac{28}{9}) = X^4 + X^2 + \frac{28}{27}X - \frac{28}{9}$

$= p(X) \cdot (X^2 - \frac{47}{27}X + \frac{19}{9})$
 $X^2 - \frac{1}{3}X + \frac{19}{9}$

7-4 $p(X) = X^2 + \frac{1}{3}X - 1$ so $X^2 \equiv 1 - \frac{1}{3}X$

$X^3 \equiv X \cdot X^2 \equiv X(1 - \frac{1}{3}X) = X - \frac{1}{3}X^2 \equiv X - \frac{1}{3}(1 - \frac{1}{3}X)$

$\equiv X - \frac{1}{3} + \frac{1}{9}X \equiv \frac{10}{9}X - \frac{1}{3} \equiv X^3$

$X^4 = X^2 \cdot X^2 \equiv (1 - \frac{1}{3}X)^2 = \frac{1}{9}X^2 - \frac{2}{3}X + 1$

$\equiv \frac{1}{9} - \frac{1}{27}X - \frac{2}{3}X + 1 = \frac{-19}{27}X + \frac{10}{9} \equiv X^4$

7-4 (cont)

$$\text{Thus } 3x^4 + x^3 - \frac{2}{3}x^2 + x + 1 \equiv 3\left(\frac{-14}{27}x + \frac{10}{9}\right) + \left(\frac{10}{9}x - \frac{1}{3}\right) - \frac{2}{3}\left(1 - \frac{1}{3}x\right) + x + 1$$

7-7 1

$$\text{7-8 } (x + \frac{1}{2}) \mid (-\frac{4}{5}x + \frac{2}{5}) = -\frac{4}{5}x^2 + \frac{1}{5}$$

$$\text{but } x^2 \equiv -1 \text{ so } \equiv -\frac{4}{5}(-1) + \frac{1}{5} = 1.$$

7-9

inverse of x is $-x$ since $x \cdot -x = -x^2 \equiv 1$.

7-10, Goal: Find inverse of $s+tx$ in $\mathbb{Q}[x]/x^2+1$

$$\begin{array}{r} \frac{\frac{1}{c}x - \frac{s}{c^2}}{tx+s} \mid \frac{x^2+1}{x^2 + \frac{s}{c}x} \\ \underline{-\frac{s}{c}x + 1} \\ -\frac{s}{c}x - \frac{s^2}{c^2} \\ \underline{\phantom{-\frac{s}{c}x} + \frac{s^2}{c^2}} \\ 1 + \frac{s^2}{c^2} \end{array}$$

$$\text{Thus } x^2 + 1 = (tx + s)\left(\frac{1}{c}x - \frac{s}{c^2}\right) + 1 + \frac{s^2}{c^2}$$

$$\text{Hence } (tx + s) \mid \left(\frac{1}{c}x - \frac{s}{c^2}\right) \equiv -1 - \frac{s^2}{c^2} \pmod{x^2 + 1}$$

$$\text{Thus } (tx + s) \mid \frac{\left(\frac{1}{c}x - \frac{s}{c^2}\right)}{-1 - \frac{s^2}{c^2}} \equiv 1 \pmod{x^2 + 1}$$

7-10 Thus the inverse of $tX + s$ is

$$\frac{\frac{1}{t}X - \frac{s}{t^2}}{-1 - s^2/t^2} = \frac{1}{t(-1 - s^2/t^2)} X - \frac{s}{t^2(-1 - s^2/t^2)}$$
$$= \boxed{\frac{-t}{t^2 + s^2} X + \frac{s}{t^2 + s^2}}$$

This is the corresponding formula to

$$\frac{1}{ax + b} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

HW # 18

7.12 From the calculation we see

$$\mathcal{O}(\mathcal{O}^4 - 4\mathcal{O}^3 + 2) \cong -2 \text{ in the field } \mathbb{C}$$

$$\boxed{\mathcal{O}^{-1} = -\frac{1}{2}\mathcal{O}^4 + 2\mathcal{O}^3 - 1}$$

7.14

If $p_0 = 0$ then $p(x) = p_1x + p_2x^2 + \dots + p_nx^n = x(p_1 + p_2x + \dots + p_nx^{n-1})$

so p is not irreducible. In general

$$-p_0 = \mathcal{O}(p_1 + p_2\mathcal{O} + \dots + p_n\mathcal{O}^{n-1})$$

$$\text{so } \mathcal{O}^{-1} = \frac{-1}{p_0}(p_1 + p_2\mathcal{O} + \dots + p_n\mathcal{O}^{n-1}) \quad \text{For example } \mathcal{O} = i, p = x^2 + 1$$

$$\text{so } \mathcal{O}^{-1} = -1(0 + i) = -i$$

2. a. $(x^2 + 1)$

b. ~~$(x^2 + 1)$~~ $x = \sqrt{7} \quad (x^2 - 7)$

c. $(x^2 - x - 1)$

d. $\alpha = \sqrt{3} + \sqrt{5} \quad \alpha^2 = 8 + 2\sqrt{15}$

$$\alpha^2 - 8 = 2\sqrt{15}$$

$$(\alpha^2 - 8)^2 = 60$$

$$\alpha^4 - 16\alpha^2 + 4 = 0$$

$$\boxed{x^4 - 16x^2 + 4}$$

3. a. x^2+1 is irreducible in $\mathbb{Z}_3[x]$ since $0^2+1 \equiv 1, 1^2+1 \equiv 2, 2^2+1 \equiv 2$

Thus let $p(x) = x^2+1$

b.

x	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
2	2	0	1	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
α	α	$1+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+\alpha$	2α	0	1	2
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+\alpha$	2α	$1+\alpha$	1	2	0
2α	2α	$1+\alpha$	$2+\alpha$	0	1	2	2	0	1
$2\alpha+1$	$2\alpha+1$	$2+\alpha$	α	1	2	0	α	$1+\alpha$	$2+\alpha$
$2\alpha+2$	$2\alpha+2$	α	$1+\alpha$	2	0	1	$1+\alpha$	$2+\alpha$	α

For multiplication we use $\alpha^2 \equiv -1 \equiv 2$ and of course $0 \equiv 3$

\cdot	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
α	0	α	$1+\alpha$	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
$1+\alpha$	0	$1+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$
$2+\alpha$	0	$2+\alpha$	α	$1+\alpha$	$2+\alpha$	2α	$2\alpha+1$	$2\alpha+2$	α
2α	0	2α	α	1	$2\alpha+1$	$2+\alpha$	2	$2\alpha+2$	2α
$2\alpha+1$	0	$2\alpha+1$	$2+\alpha$	α	2	2α	$2\alpha+2$	α	1
$2\alpha+2$	0	$2\alpha+2$	α	$1+\alpha$	$2\alpha+1$	$2+\alpha$	2	1	2α

$x+1$ divide by $x-\alpha$ in $\mathbb{F}_3[\alpha]$

$$\begin{array}{r} x+\alpha \\ x-\alpha \overline{) x^2+1} \\ \underline{x^2-\alpha x} \\ \alpha x+1 \\ \underline{\alpha x-\alpha^2} \\ 1+\alpha^2 \leftarrow \equiv 0 \end{array}$$

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

d. x^3+x+1 is an irreducible cubic. Thus
your field will be:

$$\{0, 1, \alpha, 1+\alpha, \alpha^2, \alpha^2+\alpha, \alpha^2+1, \alpha^2+\alpha+1\}$$

to add remember $1+1 \equiv 0$

to multiply you use $\alpha^3+\alpha+1=0$
 $\alpha^3 \equiv 1+\alpha$