Ungraded

p. 174-3 $(1,1)(-1,-1) = -1 \equiv 1$ and 15

p. 174-5 $(2,3)(3,5) = (6, 15) \equiv (1,6)$.

$6 \equiv 1$ and 5, $15 \equiv 6$ and 9, so

p. 174-15 $(a,b)(c,d) = (ac, bd)$ in $\mathbb{Z} \times \mathbb{Z}$. If $|ac, bd| = (1,1)$, then $a, b, c, d = \pm 1$

so units are $(1,1), (1,-1), (-1,1), (-1,-1)$.

p. 182-3, 4 in $\mathbb{Z}/6\mathbb{Z}$

x	x^2+2x+2	x^2+2x+4 reduced mod 6
0	$2 \to 2+2 = 4$	
1	$5 \to 5+2 = 1$	
2	$10 \to 4+2 = 0$	
3	$17 \to 5+2 = 1$	
4	$26 \to 2+2 = 4$	
5	$37 \to 1+2 = 3$	

no sol. one sol $x = 2$.

Another way: $x^2+2x+1 = (x+1)^2$

so $x^2+2x+2 = 0 \iff (x+1)^2+1 = 0 \iff$

$(x+1)^2 = 5$ and $x^2+2x+4 = 0 \iff (x+1)^2 = 3$.

1a §18-23 R is idempotent if $a^2 = a$. A division ring [p. 175] is a ring with unit such that every non-zero element is a unit.

So. $a = 0 \Rightarrow 0^2 = 0$ ✓.

$a \neq 0 \Rightarrow \exists$ inverse a^{-1}, so

$a^2 = a \Rightarrow aa = a \Rightarrow (a \cdot a)a^{-1} = a \cdot a^{-1}$

$\Rightarrow a \cdot (aa^{-1}) = aa^{-1} \Rightarrow a \cdot 1 = 1 \Rightarrow$

$a = 1$. These are the solutions

Note: e.g. in $\mathbb{Z}/6\mathbb{Z}$ $a^2 = a$ has 4 solutions: $a = [0]_6, [1]_6, [3]_6, [4]_6$

The latter two don't have inverses

1b §18-46 Suppose R is a commutative ring and $a^n = 0$, $b^m = 0$ (Math 417 HW 8, Due 4/6/16)

Look at $(a+b)^{m+n-1}$

$$= \sum_{k=0}^{m+n-1} \binom{m+n-1}{k} a^k b^{m+n-1-k}.$$

If $k \geq n$ then $a^k = 0$

If $m+n-1-k \geq m$, then $b^{m+n-1-k} = 0$.

so if $k \geq n$, $a^k = 0$

$m+n-1-k \geq m \Rightarrow n-1 \geq k$, $n \geq k+1$

Since either $k \geq n$ or $k \leq n-1$, all terms in the sum are 0.

(you can take a big enough power of $(a+b)$, but this is the idea.

---

2. §18-1 R is a commutative ring & characteristic 3

$(a+b)^9 = ((a+b)^3)^3$

First. $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

but 3 times anything in a ring with characteristic 3 is 0, so

$(a+b)^3 = a^3 + b^3$

Thus $(a+b)^9 = ((a+b)^3)^3 = (a^3+b^3)^3$

$= a^9 + 3a^6b^3 + 3a^3b^6 + b^9 = a^9 + b^9$.

Note: It's ok to do directly:

$(a+b)^9 = a^9 + 9a^8b + 36a^7b^2 + 84a^6b^3 + 126a^5b^4$

$+ 126a^4b^5 + 84a^3b^6 + 36a^2b^7 + 9ab^8 + b^9$

and $3 \mid 9, 36, 84, 126$, so same answer.

---

3. Zero divisors in $\mathbb{Z}/10\mathbb{Z}$

2, 4, 5, 6, 8 $\quad 2 \cdot 5 = 4 \cdot 5 = 6 \cdot 5 = 8 \cdot 5 = 0$

3b. Units in $\mathbb{Z}/10\mathbb{Z}$

1, 3, 7, 9 $\quad 1 \cdot 1 = 9 \cdot 1 = 3 \cdot 7 = 7 \cdot 3 = 1$.

$1_{\mathbb{Z}/10\mathbb{Z}}$ is $[1]_{10}$ (put brackets if needed.)

4. $R = \mathbb{Z}/12\mathbb{Z}$

$x^2 = [1]_{12} x^2$

$(x+1)^2 = [1]_{12} x^2 + [2]_{12} x + [1]_{12}$

$(x+2)^2 = [1]_{12} x^2 + [4]_{12} x + [4]_{12}$

$(x+3)^2 = [1]_{12} x^2 + [6]_{12} x + [9]_{12}$.

$(x+4)^2 = [1]_{12} x^2 + [8]_{12} x + [4]_{12}$

because $4^2 \equiv 4 \bmod 12$

$(x+5)^2 = [1]_{12} x^2 + [10]_{12} x + [1]_{12}$

because $5^2 = 25 \equiv 1 \bmod 12$

$(x+6)^2 = [1]_{12} x^2 = x^2$

because $2 \cdot 6 = 12 \equiv 0 \bmod 12$, $6^2 = 36 \equiv 0 \bmod 12$

$(x+7)^2 = [1]_{12} x^2 + [2]_{12} x + [1]_{12}$

because $2 \cdot 7 = 14 \equiv 2 \bmod 12$, $7^2 = 49$

$\equiv 1 \bmod 12$. Thus, $x^2 = (x+7)^2$,

$(x+1)^2 = (x+5)^2$, etc. in $R[x]$

for $R = \mathbb{Z}/n\mathbb{Z}$

5, 6 $R = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

+	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,0)	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,1)	(0,1)	(0,2)	(0,3)	(0,0)	(1,1)	(1,2)	(1,3)	(1,0)
(0,2)	(0,2)	(0,3)	(0,0)	(0,1)	(1,2)	(1,3)	(1,0)	(1,1)
(0,3)	(0,3)	(0,0)	(0,1)	(0,2)	(1,3)	(1,0)	(1,1)	(1,2)
(1,0)	(1,0)	(1,1)	(1,2)	(1,3)	(0,0)	(0,1)	(0,2)	(0,3)
(1,1)	(1,1)	(1,2)	(1,3)	(1,0)	(0,1)	(0,2)	(0,3)	(0,0)
(1,2)	(1,2)	(1,3)	(1,0)	(1,1)	(0,2)	(0,3)	(0,0)	(0,1)
(1,3)	(1,3)	(1,0)	(1,1)	(1,2)	(0,3)	(0,0)	(0,1)	(0,2)

$0_R = (0,0)$ - you probably didn't need a table for that!

·	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,0)	(0,1)	(0,2)	(0,3)
(0,2)	(0,0)	(0,2)	(0,0)	(0,2)	(0,0)	(0,2)	(0,0)	(0,2)
(0,3)	(0,0)	(0,3)	(0,2)	(0,1)	(0,0)	(0,3)	(0,2)	(0,1)
(1,0)	(0,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)	(1,0)	(1,0)
(1,1)	(0,0)	(0,1)	(0,2)	(0,3)	(1,0)	(1,1)	(1,2)	(1,3)
(1,2)	(0,0)	(0,2)	(0,0)	(0,2)	(1,0)	(1,2)	(1,0)	(1,2)
(1,3)	(0,0)	(0,3)	(0,2)	(0,1)	(1,0)	(1,3)	(1,2)	(1,1)

$1_R = (1,1) = ([1]_2, [1]_4)$

Lots of zero divisors

$(0,1) \cdot (1,0) = (0,0)$

$(0,2) \cdot (1,2) = (0,0)$

$(0,3) \cdot (1,0) = (0,0)$

$(0,1), (0,2), (0,3), (1,0), (1,2)$

are zero divisors.

Only two units:

$(1,1) \cdot (1,1) = (1,1)$

$(1,3) \cdot (1,3) = (1,1)$

In general $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$(a,b)(c,d) = (ac, bd)$

So (a,b) is a unit $\iff$

There are c, d so that

$ac = 1$, $bd = 1$,

ie $ac \equiv 1 \bmod m$, $bd \equiv 1 \bmod n$.

We've seen that this occurs

$\iff \gcd(a,m) = 1$, $\gcd(b,n) = 1$

$m = 2 \Rightarrow a = 1$ $n = 4 \Rightarrow b = 1, 3$

in this case.