1. The easiest (but not only) way to show that $\mathbb{Z}[i]$ is an integral domain is to use the fact that it is a subring of the field $\mathbb{C}$

If $a, b \in \mathbb{Z}[i]$ satisfy $ab = 0$ but $a \neq 0$, then take the multiplicative inverse of a in $\mathbb{C}$

In $\mathbb{C}$, $a^{-1}ab = 1 \cdot b = 0$

$\Rightarrow b = 0$.

We claim that the field of fractions of $\mathbb{Z}[i]$ is $\mathbb{Q}(i)$

To see this, think of $\mathbb{Z}[i]$ as a subring of $\mathbb{C}$ again. for $a, b, c, d \in \mathbb{Z}$ $c+di \neq 0$,

$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2} i \in \mathbb{Q}(i)$$

and any element $\alpha + \beta i$ in $\mathbb{Q}(i)$ can be written in this form,

– if $a, b, c, d \in \mathbb{Z}$ then $\frac{a}{b} + \frac{c}{d} i = \frac{ad + bci}{bd + 0i}$

2. The field of fractions of $2\mathbb{Z}$ is the set of equivalence classes $\frac{n}{d} = \{ (a,b) \mid a \in 2\mathbb{Z}, b \in 2\mathbb{Z} \setminus \{0\} \text{ and } rb = ad. \}$.

Define

$\phi : \mathbb{Q} \to F$

by $\phi\left(\frac{a}{b}\right) = \frac{2a}{2b}$.

This is well defined, since if $\frac{a}{b} = \frac{c}{d}$, then $\frac{2a}{2b} = \frac{2c}{2d}$ in the field of fractions of $2\mathbb{Z}$.

By definition of addition and multiplication in the field of fractions,

$$\phi\left(\frac{a}{b} + \frac{a'}{b'}\right) = \phi\left(\frac{ab' + ba'}{bb'}\right) = \frac{2ab' + 2ba'}{2bb'} = \frac{4ab' + 4ba'}{4bb'}$$

$$= \frac{2a}{2b} + \frac{2a'}{2b'}$$

$$= \phi\left(\frac{a}{b}\right) + \phi\left(\frac{a'}{b'}\right)$$

and $\phi\left(\frac{a}{b} \cdot \frac{a'}{b'}\right) = \frac{2aa'}{2bb'} = \frac{4aa'}{4bb'} = \frac{2a}{2b} \cdot \frac{2a'}{2b'} = \phi\left(\frac{a}{b}\right)\phi\left(\frac{a'}{b'}\right)$.

So ϕ is a homomorphism.

Finally, ϕ is an isomorphism since $\ker(\phi) = \left\{ \frac{a}{b} \in \mathbb{Q} \mid \frac{2a}{2b} = 0 \right\}$

$$= \left\{ \frac{a}{b} \in \mathbb{Q} \mid a = 0 \right\} = \{0\}.$$

4. DF 7.6 #4.

Let R and S be nonzero rings. $(0, a) \in R \times S$ is not the additive identity for any $a \in S$, $a \neq 0$. But for any $(r, s) \in R \times S$, $(r, s)(0, a) = (0, sa)$. If $R \times S$ were a field, it would have to have identity $(1, 1)$, and $(0, a)$ would have a multiplicative inverse (r, s) such that $(r, s)(0, a) = (1, 1)$. This is impossible.

5. In this example, $n = 5 \cdot 8 \cdot 9 = 360$, $\frac{n}{5} = 72$, $\frac{n}{8} = 45$, $\frac{n}{9} = 40$.

Inverses mod n: $(72)^{-1}$ mod 5 is $(2)^{-1}$ mod 5 (since $72 \equiv 2 \bmod 5$) which is 3.

$(45)^{-1}$ mod 8 is 5

$(40)^{-1}$ mod 9 is 7.

A solution is $x = 4 \cdot 72 \cdot 3 + 6 \cdot 45 \cdot 5 + 8 \cdot 40 \cdot 7$

$= 134$.

Solutions are unique mod 360, so 134 is the smallest positive integer solution.

6. a) We need to show that $1 \in A + B$. This will imply that $A + B = R$.

$1 = \frac{-1}{2}(x+3) + \frac{1}{2}(x+5)$ and $\frac{-1}{2}(x+3) \in A$, $\frac{1}{2}(x+5) \in B$.

b) We need to find a polynomial $p(x)$ such that

$p(x) - x^2 = g(x)(x+3)$ for some polynomial $g(x)$, and

$p(x) - 3x = f(x)(x+5)$ for some polynomial $f(x)$.

If $p(x) = ax + b$, then $p(x) - x^2 = -x^2 + ax + b$

and $p(x) - 3x = (a-3)x + b$ so f has degree 0,

asome $f = c$. Then $(a-3)x + b = c(x+5) \Rightarrow$ $a - 3 = c$, $b = 5c$

substituting this in, we have

$$-x^2 + (c+3)x + 5c = g(x)(x+3)$$

So g has degree 1, and is of the form $g(x) = -x + d$.

$$-x^2 + (c+3)x + 5c = (-x+d)(x+3) = -x^2 + (-3+d)x + 3d$$

$\Rightarrow c + 3 = d - 3$ so $c = d - 6$

and $5c = 3d = 3(c+6)$

$\Rightarrow 2c = 18$ and $c = 9$ so $a = 12$, $b = 45$

$$p(x) = 12x + 45.$$

c) The chinese remainder theorem says that the kernel of $\phi: R \to R/A \times R/B$ is AB, since A and B are relatively prime.

In this case $AB = \{ p(x)q(x) \mid p(x) \in A,\ q(x) \in B \}$ since A and B are principal ideals in a commutative ring.

So AB is the set of polynomials with $(x+5)(x+3)$ as a factor, i.e. $AB = (x^2+8x+15)$.

If $p(x)$ and $q(x)$ are two solutions, then $p(x) - q(x)$ is an elemt of $\ker(\phi)$, so a multiple of $x^2+8x+15$.

d). Solutions are unique mod $(x^2+8x+15)$. By DF section 7.4 problem 14, every elemt of $R/(x^2+8x+15)$ can be represented as a polynomial of degree <2.

7 a) The Chinese remainder theorem says that $\phi: \mathbb{Z} \to \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$ has kernel $(p_1 \cdots p_k)\mathbb{Z} = n\mathbb{Z}$. (you should say why $p_1\mathbb{Z}\, p_2\mathbb{Z} \cdots p_k\mathbb{Z} = p_1p_2\cdots p_k\mathbb{Z}$).

By the first isomorphism theorem for rings,

$$\mathbb{Z}/\ker(\phi) = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$$ since ϕ is surjective (by the C.R.T.)

b) $(a_1, a_2, \dots a_k) \in \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$ is a unit if and only if a_i is a unit in $\mathbb{Z}/p_i\mathbb{Z}$ for each i, i.e. if and only if each a_i is nonzero. (you can check this!)

c) Since $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$, they have the same number of units, which is