1. (10 pts) Solve the following congruences. If there are multiple solutions, be sure to find all of them. If there is no solution, say so, and be sure to justify your answer.

(a) (5 pts) $8x \equiv 11 \pmod{30}$

$8x \equiv 11 \pmod{30} \iff 30 \mid 8x - 11 \iff 8x - 11 = 30k$ for some $k \in \mathbb{Z}$.

$\iff 8x - 30k = 11$ for some $k \in \mathbb{Z}$.

But $2 \mid 8x - 30k$ and $2 \nmid 11$, so there is no solution.

Another explanation:

$(8, 30) = 2$, and $2 \nmid 11$, so by Theorem 2.11, there is no solution.

(b) (5 pts) $8x \equiv 11 \pmod{31}$

$(8, 31) = 1$, so there must be a unique solution (modulo 31), namely $x \equiv 11 \cdot 8^{-1} \pmod{31}$, so we must compute $8^{-1} \pmod{31}$.

$31 = 8 \cdot 3 + 7$

$8 = 7 \cdot 1 + 1 \implies 1 = 8 - 7 \cdot 1 = 8 - (31 - 8 \cdot 3) \cdot 1 = 8 \cdot 4 - 31$, so

$8 \cdot 4 \equiv 1 \pmod{31}$, so $8^{-1} \equiv 4 \pmod{31}$.

$x \equiv 11 \cdot 8^{-1} \equiv 11 \cdot 4 \equiv 44 \equiv 13 \pmod{31}$

$\boxed{x \equiv 13 \pmod{31}}$

2. (10 pts) Let $a = 3X^2 + X + 2 \in \mathbb{Z}_7[X]$. Compute the inverse of $[a]$ in $\mathbb{Z}_7[X]/(p)$ where $p = X^3 + 4$.

Euclidean Algorithm: $p = a \cdot (5X+3) + (X+5)$

$a = (X+5)(3X) + 2$

↑ This is a unit, so we're done. (The gcd of a and p is 1.)

Working backwards:

$2 = a - (X+5)(3X)$

$X+5 = p - a(5X+3)$

$2 = a - (p - a(5X+3)) \cdot (3X)$

$= a - p(3X) + a(5X+3)(3X)$

$= a(X^2+2X+1) - p(3X)$

Now multiply by $2^{-1}=4$ to get

$1 = 2 \cdot 2^{-1} = 2 \cdot 4 = (a(X^2+2X+1) - p(3X)) \cdot 4 = a(4X^2+X+4) - p(5X)$

So $a(4X^2+X+4) \equiv 1 \pmod{p}$, so $[a]^{-1} = [4X^2+X+4]$

Scratch work:

$$\begin{array}{r} 5X+3 \\ 3X^2+X+2 \overline{)\, X^3 \quad\quad +4} \\ X^3+5X^2+3X \\ \hline 2X^2+4X+4 \\ 2X^2+3X+6 \\ \hline X+5 \end{array}$$

$$\begin{array}{r} 3X \\ X+5 \overline{)\, 3X^2+X+2} \\ 3X^2+X \\ \hline 2 \end{array}$$

3. (10 pts) Give an example of a field of order 125. Be sure to explain why your example is a field. *(Hint:* $125 = 5^3$*)*

If $p \in \mathbb{Z}_5[X]$ is an irreducible polynomial of degree 3, then $\mathbb{Z}_5[X]/(p)$ will be a field of order 5^3. So we just need to find an irreducible polynomial of degree 3 in $\mathbb{Z}_5[X]$. A degree 3 polynomial is irreducible over a field if and only if it has no roots in the field.

$p = X^3, X^3+1, X^3+2, X^3+3, X^3+4$ don't work...

$p = X^3+X+1$ works:

$p(0)=1$
$p(1)=3$
$p(2)=1$
$p(3)=1$
$p(4)=4$

$\mathbb{Z}_5[X]/(X^3+X+1)$ is one correct answer.

$p = X^3+X^2+1$ also works:

$p(0)=1$
$p(1)=3$
$p(2)=3$
$p(3)=2$
$p(4)=1$

$\mathbb{Z}_5[X]/(X^3+X^2+1)$ is also a correct answer.

Etc...

(There are a total of 40 different monic polynomials that you could use for this problem.)

4. (10 pts) Let R be a commutative ring with identity. Prove that R is an integral domain if and only if the ideal (0) is prime.

($\Rightarrow$) Assume R is an integral domain. WTS $(0) \neq R$ and for any $a, b \in R$, $ab \in (0) \Rightarrow a \in (0)$ or $b \in (0)$.
Since $1_R \neq 0_R$, $1_R \notin (0)$, so $(0) \neq R$.
Suppose $ab \in (0)$. Then $ab = 0$, so since R is an integral domain, $a = 0$ or $b = 0$. Thus either $a \in (0)$ or $b \in (0)$.
Hence (0) is a prime ideal.

($\Leftarrow$) Assume (0) is prime. WTS $1_R \neq 0_R$ and if $ab = 0$ then either $a = 0$ or $b = 0$.
If $1_R = 0_R$, then $r = r \cdot 1 = r \cdot 0 = 0$ for all $r \in R$, so $R = \{0\} = (0)$.
Since (0) is prime, $(0) \neq R$, so $1_R \neq 0_R$.
Suppose $ab = 0$. Then $ab \in (0)$, so since (0) is prime, either $a \in (0)$ or $b \in (0)$, so either $a = 0$ or $b = 0$.
Thus R is an integral domain.

Alternate proof:

Let $f : R \to R$ be the identity map: $f(r) = r$ $\forall r \in R$.
Then f is clearly a surjective homomorphism, and $\ker(f) = (0)$, so by the 1st Isomorphism Theorem, $R/(0) \cong R$.
Now by Theorem 6.14, $R/(0)$ is an integral domain iff (0) is prime, so R is an integral domain iff (0) is prime.

5. (a) (6 pts) Let R be a ring and let I and J be ideals in R. Let

$$I + J = \{i + j \mid i \in I \text{ and } j \in J\}.$$

Show that $I + J$ is an ideal in R.

We must show that $I+J$ (1) is nonempty, (2) is closed under subtraction, and (3) absorbs products.

1. $0 \in I$ and $0 \in J$, so $0 = 0+0 \in I+J$, so $I+J$ is nonempty.

2. Let $a, b \in I+J$. Then $a = i_1 + j_1$ and $b = i_2 + j_2$ for some $i_1, i_2 \in I$, $j_1, j_2 \in J$. So
$$a - b = (i_1 + j_1) - (i_2 + j_2)$$
$$= (i_1 - i_2) + (j_1 - j_2) \in I+J$$
because $i_1 - i_2 \in I$ and $j_1 - j_2 \in J$.
So $I+J$ is closed under subtraction.

3. Let $a \in I+J$, $r \in R$. Then $a = i + j$ for some $i \in I$, $j \in J$.
So $ar = (i+j)r = ir + jr \in I+J$ because $ir \in I$, $jr \in J$, and
$ra = r(i+j) = ri + rj \in I+J$ because $ri \in I$, $rj \in J$.
Thus $I+J$ absorbs products.

Therefore $I+J$ is an ideal.

(b) (7 pts) Let $a, b \in \mathbb{Z}$ with a and b not both 0, and let d be the gcd of a and b. Show that

$$(a) + (b) = (d).$$

(Note: Here (n) refers to the principal ideal in $\mathbb{Z}$ generated by the integer n, and $(a) + (b)$ refers to the sum of the ideals (a) and (b) as defined on the previous page.)

Since $(a) = \{ar \mid r \in \mathbb{Z}\}$ and $(b) = \{bs \mid s \in \mathbb{Z}\}$,
$(a)+(b) = \{ar+bs \mid r, s \in \mathbb{Z}\}$.

We will show that $(a)+(b) \subset (d)$ and $(a)+(b) \supset (d)$.

($\subset$): Let $x \in (a)+(b)$. Then $x = ar+bs$ for some $r, s \in \mathbb{Z}$.
Since $d|a$ and $d|b$, $d|ar$ and $d|bs$, so $d|ar+bs$,
so $d|x$. Thus $x \in (d)$. Hence $(a)+(b) \subset (d)$.

($\supset$): Since there exist $r, s \in \mathbb{Z}$ such that $d = ar+bs$
(by Theorem 1.3), $d \in (a)+(b)$. Now let $x \in (d)$.
Then $x = dk$ for some $k \in \mathbb{Z}$. Since $d \in (a)+(b)$ and
$(a)+(b)$ is an ideal, $dk \in (a)+(b)$, so $x \in (a)+(b)$.
Thus $(a)+(b) \supset (d)$.

Therefore $(a)+(b) = (d)$.

(c) (7 pts) Let F be a field, and let p and q be relatively prime polynomials in $F[X]$. Show that

$$(p) \cap (q) = (pq).$$

(Note: Here (f) refers to the principal ideal in $F[X]$ generated by the polynomial f.)

We will show $(p) \cap (q) \subset (pq)$ and $(p) \cap (q) \supset (pq)$.

($\subset$): Let $a \in (p) \cap (q)$. Then $a = pr$ for some $r \in F[X]$, and $a = qs$ for some $s \in F[X]$. Thus $p \mid a$, so $p \mid qs$, and since $(p,q) = 1$, we must have $p \mid s$.
Thus $s = pt$ for some $t \in F[X]$, so $a = qs = qpt = (pq)t$, so $a \in (pq)$.
Thus $(p) \cap (q) \subset (pq)$.

($\supset$): Let $a \in (pq)$. Then $a = pqt$ for some $t \in F[X]$, so $p \mid a$ and $q \mid a$. Thus $a \in (p)$ and $a \in (q)$, so $a \in (p) \cap (q)$.
Thus $(p) \cap (q) \supset (pq)$.

Therefore $(p) \cap (q) = (pq)$.

6. (20 pts) Recall that $M_2(\mathbb{Z})$ denotes the ring of 2×2 matrices with integer coefficients. Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z} \right\}.$$

(a) (5 pts) Show that R is a commutative subring of $M_2(\mathbb{Z})$.

Letting $a=b=0$ shows $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$, so R is nonempty.

$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ 0 & a-c \end{pmatrix} \in R$, so R is closed under subtractio

$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in R$, so R is closed under multiplicatio

$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}$ ↺ equal, so R is commutative.
$\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} ca & cb+da \\ 0 & ca \end{pmatrix}$

(b) (5 pts) Define a function $f : R \to \mathbb{Z}$ by $f(\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)) = a$. Show that f is a surjective homomorphism.

$f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = f\begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix} = a+c = f\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + f\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}$

$f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = f\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} = ac = f\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot f\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}$

So f preserves addition and multiplication, and thus is a homomorphism.

Let $a \in \mathbb{Z}$. Then $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in R$, and $f\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a$, so f is surjective.

(c) (3 pts) What is the kernel of f?

$$\text{Ker}(f) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R \;\middle|\; f\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = 0 \right\} = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in R \;\middle|\; a = 0 \right\}$$

$$= \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in R \right\} = \boxed{\left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \;\middle|\; b \in \mathbb{Z} \right\}}$$

(d) (3 pts) Prove that $R/\text{Ker}(f) \cong \mathbb{Z}$.

Since f is a surjective ring homomorphism, by the 1st Isomorphism Theorem, $R/\text{Ker}(f) \cong \mathbb{Z}$.

(e) (4 pts) Is $\text{Ker}(f)$ a prime ideal? Is it a maximal ideal? (Justify your answers.)

Since R is a commutative ring with identity (note that $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in R$), $\text{Ker}(f)$ is prime iff $R/\text{Ker}(f)$ is an integral domain, and $\text{Ker}(f)$ is maximal iff $R/\text{Ker}(f)$ is a field.

Since $R/\text{Ker}(f) \cong \mathbb{Z}$ is an integral domain but <u>not</u> a field,

$\boxed{\text{Ker}(f) \text{ is a prime ideal, but is } \underline{\text{not}} \text{ maximal.}}$