1. (a) i. State and prove Wilson's Theorem.

   ii. Show that, if p is a prime number congruent to 1 modulo 4, then there exists a solution to the congruence $x^2 \equiv -1 \mod p$.

   (b) i. Let $p(x)$, $q(x)$ be polynomials in $\mathbb{Z}_3[x]$, given by $p(x) = x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1$ and $q(x) = x^5 + 2x^3$. Find all gcds of $p(x)$ and $q(x)$ in $\mathbb{Z}_3[x]$.
   Solution: Using long division of polynomials, the Euclidean algorithm gives:

$$\begin{array}{rcccc} x^6+2x^5+2x^4+2x^2+x+1 & = & (x+2) & (x^5+2x^3) & + & (2x^3+2x^2+x+1) \\ (x^5+2x^3) & = & (2x^2+x+2) & (2x^3+2x^2+x+1) & + & (2x^2+1) \\ (2x^3+2x^2+x+1) & = & (x+1) & (2x^2+1) & + & 0 \end{array}$$

   Hence the gcds are $2x^2 + 1$, $x^2 + 2$.

   ii. Is $\mathbb{Z}_3[x]$ a principal ideal domain? Is $\mathbb{Z}_3[x]/_{\langle p(x)\rangle}$ a field? Justify your answers.
   Solution: Since $\mathbb{Z}_3$ is a field, $\mathbb{Z}_3[x]$ is a Euclidean ring and therefore a PID.
   Since $(x^2 + 2)|p(x)$, $p(x)$ is not irreducible; hence $\mathbb{Z}_3[x]/_{\langle p(x)\rangle}$ is not a field.

   iii. Give a single generator for the ideal $\langle p(x), q(x)\rangle$.
   Solution: $x^2 + 2$

   iv. Give a brief explanation as to why the Euclidean algorithm is guaranteed to terminate.
   Solution: The norm of the remainder, which is non-negative integer, is strictly decreasing at every step.

2. (a) Find a gcd of $x^3 - 2x$ and $x^2 - 2x + 1$ in $\mathbb{Q}[x]$.
   Solution: Using long division of polynomials, the Euclidean algorithm gives:

$$\begin{array}{rcccc} x^3-2x & = & (x-2) & (x^2-2x+1) & + & (x-2) \\ x^2-2x+1 & = & (x-4) & (x+2) & + & 9 \\ (x+2) & = & (\frac{1}{9}x+\frac{2}{9}) & (9) & + & 0 \end{array}$$

   Hence 9 (or 1) is a gcd of the two polynomials. In other words, the two polynomials are relatively prime.

Alternatively, one can spot that $x^2 - 2x + 1 = (x-1)^2$ and then it is sufficient to show that $(x-1) \not| (x^2 - 2)$.

(b) State and prove one of the following:

- Gauss' Lemma
- Eisenstein Criterion

Note: *In the literature "Gauss' Lemma" can refer to various (related) results. Here we mean that, for a UFD R, if f, g are primitive in $R[x]$, then so is fg. This is the simplest version.*

The version of the Eisenstein Criterion as we saw it in class was the following:

Suppose R is a unique factorization domain with quotient field F. Let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a polynomial of degree at least 1 with coefficients in R. Suppose there exists an irreducible element p of R such that:

$$\forall i = 0, 1, \ldots n-1, \quad p | a_i; p \not| a_n, \ p^2 \not| a_0.$$

Then $f[x]$ is irreducible in $F[x]$.

(c) State what it means for a field $\mathbb{F}$ to be a *field of fractions* of an integral domain R.

(d) Show that the polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$.

Solution: We have $x^2 - 2 \in \mathbb{Z}[x]$, and $\mathbb{Q}$ is the field of quotients of the UFD $\mathbb{Z}$. Clearly 2 is a prime integer which divides all the coefficients (0,-2) except the leading coefficient (1), and 2^2 does not divide -2. Hence by the Eisenstein criterion $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$.

(e) Show that

i. the polynomial $(p(x,y))^2$ is primitive in $(\mathbb{Q}[x])[y]$

ii. the polynomial $p(x,y)$ is irreducible in $\mathbb{Q}[x,y]$

where $p(x,y) =$

$$(x^2 - 2x + 1)y^4 + (x^3 - 2x)y^3 + (x^2 - 2)y^2 + (x^2 - 2)y + \frac{1}{2}(x^2 - 2)$$

Solution: (i): The first two coefficients of $p(x,y)$ are the polynomials of part 2a. Since they are coprime, the polynomial is primitive. Hence by Gauss' Lemma, so is $p(x,y)^2$ (since $\mathbb{Q}$ is a field, $\mathbb{Q}[x]$ is a Euclidean ring, and therefore a UFD, so Gauss' Lemma indeed does apply).

(ii) We apply the Eisenstein Criterion to $p(x,y)$, seen as an element of $(\mathbb{Q}[x])[y]$, with $R = \mathbb{Q}[x]$ (which is a UFD, as above). We take the

irreducible $p = x^2 - 2$ (from part 2d). This clearly divides all the coefficients apart from the leading coefficient. From part 2a, it does *not* divide the leading coefficient (otherwise the gcd in part 2a would not be 1). Moreover, since $\deg((x^2-2)^2) = 4 > 2 = \deg\left(\frac{1}{2}(x^2-2)\right)$ and in $\mathbb{Q}[x]$ the degree of a product is the sum of the degrees ($\mathbb{Q}$ being an integral domain), $(x^2-2)^2$ does not divide the constant term.

Thus we may apply the Eisenstein Criterion to obtain that $p(x,y)$ is irreducible in $F[y]$, where F is the field of fractions of $\mathbb{Q}[x]$. In class we saw a Lemma stating that

Lemma: Let F be the field of fractions of the unique factorization domain R, and suppose $f(x) \in R[x]$ is primitive. Then $f(x)$ is irreducible in $R[x]$ iff $f(x)$ is irreducible in $F[x]$.

Since the polynomial is primitive, the Lemma applies; hence $p(x,y)$ is irreducible in $R[y] = (\mathbb{Q}[x])[y] \cong \mathbb{Q}[x,y]$.

Note: *In class (as here) we identified, without proof, $R[x,y]$ with $(R[x])[y]$. We also saw in an exercise an application of the Eisenstein Criterion to $(\mathbb{Q}[x])[y]$.*

3. (a) Let D be an integral domain with multiplicative identity, and suppose the element $a \in D$ has a factorization into irreducibles. Prove that this factorization is unique up to associates, assuming *one* of the following:
   - D is a Euclidean Ring;
   - D is principal ideal domain;
   - $D = R[x]$ for some unique factorization domain R.

   (b) Consider the subring E of the field of complex numbers given by

$$E = \left\{ \frac{1}{2}(a+bi) \mid a,b \in \mathbb{Z},\ a-b \text{ is even} \right\}.$$

   In other words, E consists of the complex numbers $x + y\sqrt{-3}$ such that x and y are either both integers or both odd multiples of $\frac{1}{2}$. For example, $\frac{1}{2} - \frac{3}{2}\sqrt{-3}$ and $-2 + 3\sqrt{-3}$ are both in E, but $1 + \frac{1}{2}\sqrt{-3}$ is not.

   i. Find the units of E.
   Solution: Suppose

$$\frac{(x+y\sqrt{-3})}{2}\frac{(z+t\sqrt{-3})}{2} = 1$$

where x, y, z, t are integers such that $x-y$ and $z-t$ are both even.

$$\begin{array}{lrcl} \text{Then} & (x+y\sqrt{-3})(z+t\sqrt{-3}) & = & 4 \\ \text{whence} & \left|x+y\sqrt{-3}\right|\left|z+t\sqrt{-3}\right| & = & |4| \\ & \left|x+y\sqrt{-3}\right|^2\left|z+t\sqrt{-3}\right|^2 & = & 16 \\ & (x^2+3y^2)(z^2+3t^2) & = & 16. \end{array}$$

The positive factors of 16 are 1,2,4,8,16. However, $x^2+3y^2=1$ can only be achieved with $|x|=1, |y|=0$, which is to be discarded because $x-y$ should be even. Also, $x^2+3y^2=2$ has no solutions at all for integer values of x, y. Similarly $z^2+3t^2=1$ and $z^2+3t^2=2$ can be discarded. The only way of factorizing 16 avoiding 1 and 2 is $16=4\cdot 4$.
Now $x^2+3y^2=4$ is has 6 solutions in integers:
$(x,y)=(1,1),(-1,1),(1,-1),(-1,-1),(2,0),(-2,0)$. Note that in all cases $x-y$ is even. Thus the units are to be found among $\frac{1}{2}(\pm 1\pm\sqrt{-3}),\pm 1$. Simple computations show that

$$\frac{(1+\sqrt{-3})}{2}\frac{(1-\sqrt{-3})}{2}=1$$

$$\frac{(-1-\sqrt{-3})}{2}\frac{(-1+\sqrt{-3})}{2}=1$$

and 1 and -1 are clearly their own inverses. Hence the units are precisely the 6 elements $\frac{1}{2}(\pm 1\pm\sqrt{-3}),\pm 1$.

ii. State whether the following argument is correct:
In E, we have that $2.2=4=(1+\sqrt{-3})(1-\sqrt{-3})$. *Therefore, E is not a unique factorization domain.*
If correct, fill in the missing details. If not, explain why.
Solution: The reasoning is incorrect, because multiplying the factors $1\pm\sqrt{-3})$ on the right hand side by the units $\frac{1}{2}(\pm 1\mp\sqrt{-3})$ we obtain the factors on the left hand side, 2 and 2. Thus the factorizations are the same up to units.

iii. State whether 13 is irreducible in E or not, and justify your answer (if irreducible, give a proof; if not, give a non-trivial factorization).
Solution: Suppose

$$\frac{(x+y\sqrt{-3})}{2}\frac{(z+t\sqrt{-3})}{2}=13$$

$$\begin{array}{lrcl} \text{Then} & (x+y\sqrt{-3})(z+t\sqrt{-3}) & = & 4\cdot 13 \\ \text{whence} & \left|x+y\sqrt{-3}\right|\left|z+t\sqrt{-3}\right| & = & |4\cdot 13| \\ & \left|x+y\sqrt{-3}\right|^2\left|z+t\sqrt{-3}\right|^2 & = & 4^2\cdot 13^2 \\ & (x^2+3y^2)(z^2+3t^2) & = & 4^2\cdot 13^2. \end{array}$$

One way of achieving the above is $|x| = 2 = |z|, |y| = |t| = 4$. Note $x - y$ and $z - t$ are both even. Moreover, taking $x = 2 = z$, $y = 4 = -t$, we obtain the factorization

$$(1+2\sqrt{-3})(1-2\sqrt{-3}) = 13.$$

Since $1 \pm 2\sqrt{-3}$ are non-units (by part 3(b)i), this is a non-trivial factorization. This shows that 13 is not irreducible.

4. (a) Let D be an integral domain with multiplicative identity, and suppose the element $a \in D$ is not 0 and is not a unit. Show that a can be expressed as a finite product of irreducibles, assuming *one* of the following.
   - D is a Euclidean Ring;
   - D is principal ideal domain;
   - $D = R[x]$ for some unique factorization domain R.

   (b) Let a, b be Gaussian integers given by $a = 1 + 12i$ and $b = 3 + 6i$. Find a gcd of a, b in the ring of Gaussian integers, and Gaussian integers x, y such that this gcd can be expressed in the form $xa + yb$.

   Solution:

$$\begin{array}{rcllll} 1+12i & = & q_0 & (3+6i) & + & (1-3i) \\ (3+6i) & = & q_1 & (1-3i) & + & (1+2i) \\ (1-3i) & = & q_2 & (1+2i) & + & 0 \end{array}$$

   where $q_0 = (2+i), q_1 = (-1+i), q_2 = (-1-i)$. Thus 1+2i is a gcd and we may take $x = -q_1 = (1-i)$ and $y = 1 + q_0 q_1 = (-2+i)$.

   (c) Show that, if m, n are relatively prime positive integers, then m is invertible in $\mathbb{Z}_n$. (You may assume $m < n$.)

   Solution: There exist integers a, b such that $am + bn = 1$. Hence $am \equiv 1 \mod n$.

   (d) Give an example of a unique factorization domain which is not a Euclidean ring. (You do not need to prove that your example is as claimed).

   Solution: We saw in class that $\mathbb{Z}[x]$ is a UFD but not a PID. Since PID $\Rightarrow$ ER, $\mathbb{Z}[x]$ is an example of a UFD which is not an ER.

(e) Find a gcd of $x^4 + 4x^3 + 6x^2 + 4x + 1$ and $x^4 - 4x^3 + 6x^2 - 4x + 1$ in $\mathbb{Z}[x]$.

Solution: The numbers 1 4 6 4 1 constitute the fifth line of Pascal's Triangle, that is, they are the binomial coefficients $\binom{4}{i}$, $i = 0, 1, \ldots, 4$. Hence the two polynomials are $(1 + x)^4$ and $(1 - x)^4$. We saw that, for an integral domain R with 1 (such as $\mathbb{Z}$) and a unit a of R, any polynomial $ax+b$ is irreducible in $R[x]$. Thus $1 \pm x$ are both irreducible. Since they are coprime, the two polynomials are coprime; one gcd is 1.

5. (a) Let R be a commutative ring with multiplicative identity. Show that R is a field if and only if it has no proper ideals.

(b) State the Second Isomorphism Theorem.

(c) Let S be a commutative ring with multiplicative identity. Let $a, b \in S$ be such that $\langle b \rangle \subseteq \langle a \rangle$. Show that $b|a$.

(d) Let T be the ring $\mathbb{Z}_{24}$. Apart from the empty ideal and T itself, how many ideals are there in T?

Solution: By the Second Isomorphism Theorem, there is a bijection between the ideals of T and the ideals of $\mathbb{Z}$ containing $\langle 24 \rangle$. Thus it is sufficient to count the ideals in $\mathbb{Z}$ which are strictly in between T and $\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, these ideals are of the form $\langle b \rangle$ for some $b \in \mathbb{Z}$. By part 5c, $b|24$. Thus $|b| \in \{2, 3, 4, 6, 8, 12\}$. Moreover, by an exercise from class (essentially the converse of part 5c), for any such b we have $\langle 24 \rangle \subsetneq \langle b \rangle \subsetneq \mathbb{Z}$. Clearly if $b_1 = -b_2$, then $\langle b_1 \rangle = \langle b_2 \rangle$ while if $|b_1| \neq |b_2|$ then $\langle b_1 \rangle \neq \langle b_2 \rangle$. Thus there are 6 proper ideals in T.

(e) Give a positive integer n such that $\mathbb{Z}_n$ is not a field, but has precisely one non-trivial factor ring (that is, only one factor ring apart from $\mathbb{Z}_n$ itself and $\{0\}$). Show that this factor ring is a field. (Note that there are various possibilities for n).

Solution: The factor rings are in one-to-one correspondence with the ideals of $\mathbb{Z}_n$. From part 5d it should be clear that the proper ideals of $\mathbb{Z}_n$ are in one-to-one correspondence with the non-trivial positive integer divisors of n. Looking at the factorization of n into primes, we see that this can only be achieved by taking $n = p^2$ for some prime p. The simplest example is thus $n = 4$.

Whatever the choice of p, the unique ideal in $\mathbb{Z}_n$ is maximal, hence the factor ring is a field.

(f) Let J be a proper ideal in a principal ideal domain Y. Show that J is contained in a maximal ideal. Hence, or otherwise, show that there

exists a factor ring F which is a field and such that the elements of Y/J (seen as cosets of Y) partition the elements of F.

Solution: If J is maximal, we have the required maximal ideal containing J. Otherwise, there exists an ideal J_1 such that $J \subsetneq J_1 \subsetneq Y$. Again, we may assume J_1 is not maximal (otherwise we are done). In this way we obtain a chain of ideals

$$J \subsetneq J_1 \subsetneq J_2 \subsetneq \cdots$$

By the following Lemma seen in class:

Lemma: Suppose

$$I_1 \subsetneq I_2 \subsetneq I_2 \subsetneq \cdots$$

is a strictly increasing chain of ideals in a PID. Then the chain is finite

at some point we must obtain a maximal ideal J_k containing J. We take the field Y/J_k for F.

If x, y belong to the same coset with respect to J, then $x - y \in J$. Since $J \subseteq J_k$, $x - y \in J_k$, and x, y belong to the same coset with respect to J_k. Thus the partition of Y into cosets with respect to J is a refinement of the partition into cosets with respect to J_k, which are the elements of F.