1. Show that if \( n \in \mathbb{Z} \) then for every integer \( a \) with \( \gcd(a, n) = 1 \), there exists a unique \( x \) mod \( n \) such that \( ax = 1 \) mod \( n \).

By the definition of \( \gcd \), for a given \( a, n \) and \( d \), \( \gcd(a, n) = d = xa + yn \) where \( x, y \in \mathbb{Z} \). In our case, \( xa + yn = 1 = \gcd(a, n) \).

In the ring \( \mathbb{Z}_n \) \( xa = 1 \) \( \Rightarrow \) \( x \) is unique.

2. Here is an age-guessing game you might play at a party. You ask a fellow party-goer to divide his age by each of the numbers \( a, 4 \) and \( 5 \) and tell you the remainders. Show how to use this information to determine the age.

Let the party goer’s age be \( x \). Then we have

\[
x = r_3 \text{ mod } 3, \quad x = r_4 \text{ mod } 4, \quad x = r_5 \text{ mod } 5.
\]

This means

\[
x = (r_3m_3 + r_4m_4 + r_5m_5) \text{ mod } 60 \quad \text{where:}
\]

\[
m_3 = s_3 \times 20 \quad \text{where } s_3 = 20^{-1} \text{ mod } 3 = 2
\]

\[
m_4 = s_4 \times 15 \quad \text{where } s_4 = 15^{-1} \text{ mod } 4 = 3
\]

\[
m_5 = s_5 \times 12 \quad \text{where } s_5 = 12^{-1} \text{ mod } 5 = 3
\]

\[
\Rightarrow m_3 = 40, \quad m_4 = 45, \quad m_5 = 36
\]

\[
\Rightarrow x = (40r_3 + 45r_4 + 36r_5) \text{ mod } 60
\]

3. For any integer \( n > 1 \), let \( \phi(n) \) denote the number of positive integers less than \( n \) and coprime to \( n \). If \( m, n \) are coprime then \( \phi(m, n) = \phi(m) \cdot \phi(n) \). If \( n \) is a prime power, \( n = p^e \) where \( \phi(n) = (p^e - p^{e-1}) \). Use the two results above to deduce a formula for \( \phi(n) \) in terms of the prime factorization of \( n \).

Let \( p_1, \ldots, p_k \) be the set of unique prime factors of \( n \), then we have \( n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k} \) where \( e_i \) us the appropriate power for the prime factor \( p_i \).

\[
\phi(n) = \phi(p_1^{e_1}) \cdot \ldots \cdot \phi(p_k^{e_k}) = \prod_{i=1}^{k} \phi(p_i^{e_i}) = \prod_{i=1}^{k} [p_i^{e_i} - p_i^{e_i-1}].
\]

4. For each pair of rings below, determine if they are isomorphic. If they are not isomorphic prove it, else provide an isomorphism.

4-1: \( R_1 = \mathbb{Z}_{15}, \ R_2 = \mathbb{Z}_3 \oplus \mathbb{Z}_5 \)

\( R_1 \cong R_2 \). Let \( \phi \) be the isomorphism. For \( a \in \mathbb{Z}_{15} \), \( \phi(a) = (a \mod 3, a \mod 5) \). For \( \phi^{-1}(\alpha, \beta) = \alpha(5(5^{-1} \mod 3)) + \beta(3(3^{-1} \mod 5)) = 10\alpha + 6\beta \).

The above definition of the isomorphism is bijective since \( \phi^{-1}(\alpha, \beta) \mod 3 = \alpha \mod 5, \ \phi^{-1}(\alpha, \beta) \mod 5 = \beta \).

By the properties of modulo we have \( \phi(ab) = (ab \mod 3, ab \mod 5) = (a \mod 3, a \mod 5) \ast (b \mod 3, b \mod 5) \).

1
mod 3, b mod 5) = \phi(a)\phi(b).
Similarly \( \phi(a + b) = (a + b \mod 3, a + b \mod 5) = (a \mod 3, a \mod 5) + (b \mod 3, b \mod 5) = \phi(a) + \phi(b). 
4-2: \( R_1 = \mathbb{Z}_{25}, \ R_2 = \mathbb{Z}_5 \oplus \mathbb{Z}_5 \)

\( R_1 \not\cong R_2. \) If \( R_1 \) and \( R_2 \) are isomorphic, then corresponding elements must have the same order. Note that in \( \mathbb{Z}_5 - \{0\} = \{1, 2, 3, 4\} \) each element \( x \) has \( x^4 = 1 \). Then if we look at the set \( \mathbb{Z}_5 \oplus \mathbb{Z}_5 \) without any elements containing 0, then we have that every \( (a, b)^4 = (1, 1) \). However, this does not hold true for \( \mathbb{Z}_{25} \). 2 mod 25 in \( \mathbb{Z}_{25} \), for example, does not match this expectation. \( (2 \mod 25)^4 = 16 \mod 25 \) which does not equal 1 mod 25.

4-3: \( R_1 = \mathbb{Q}[x]/\langle x^2 - 7 \rangle, \ R_2 = \mathbb{Q}[y]/\langle y^2 - 2 \rangle \)

\( R_1 \not\cong R_2. \) Both \( x^2 - 7 \) and \( y^2 - 2 \) are irreducible over \( \mathbb{Q}[x] \). Note that all elements in \( R_1 \) with \( x = 0 \) must map to those in \( R_2 \) with \( y = 0 \).
In \( R_1 \), \( x^2 - 7 = 0 \), this implies that there is an element, \( g \in R_1 \) such that \( g^2 = 7 \). In order for \( R_1 \cong R_2 \), one such element must exist in \( R_2 \) as well. Let that element be \( (a + by) \), then we have \( 7 = (a + by)^2 = a^2 + b^2y^2 + 2aby = (a^2 + 2b^2) + (2ab) \cdot y \). This means that \( a^2 + 2b^2 = 7 \) and that \( 2ab = 0 \). Solving, we have \( b = \sqrt{7/2} \). Since the constants in \( R_2 \) are all in \( \mathbb{Q} \), \( b \) cannot exist. Therefore no element \( z \in R_2 \) exists such that \( z^2 = 7 \). Therefore \( R_1 \not\cong R_2 \).

4-4: \( R_1 = \mathbb{R}[x]/\langle x^2 - 1 \rangle, \ R_2 = \mathbb{R}[x]/\langle x^2 + 1 \rangle \)

\( R_1 \not\cong R_2. \) \( x^2 - 1 \) is reducible over \( \mathbb{R}[x] \) while \( x^2 + 1 \) is not reducible over \( \mathbb{R}[x] \). By CRT, \( R_1 \cong \mathbb{R}[x]/\langle x - 1 \rangle \oplus \mathbb{R}[x]/\langle x + 1 \rangle \). However, \( R_2 \) cannot be isomorphic to a similar direct sum of co-primes since \( x^2 + 1 \) is irreducible in \( \mathbb{R}[x] \). This is a fundamental property difference. Therefore \( R_1 \not\cong R_2 \).

4-5: \( R_1 = \mathbb{C}[x]/\langle x^2 - 1 \rangle, \ R_2 = \mathbb{C}[x]/\langle x^2 + 1 \rangle \)

\( R_1 \cong R_2. \) All constants in \( R_1 \) must map to constants in \( R_2 \). Lets map \( \varphi : x \mapsto ix \).
Then we have that following:
\( \varphi(a + bx) = a + ibx \)
\( \varphi((a + bx)(c + dx)) = \varphi(ac + bd + (ad + bc)x) = (ac + bd) + i(ad + bc)x = ac + i(ad + bc) - bdx^2 \)
\( = ac + iadx + ibcx - bdx^2 = (a + ibx)(c + idx) = \varphi(a + bx)\varphi(c + dx) \)

Similarly, \( \varphi((a + bx)+(c + dx)) = \varphi((a+c)+(b+d)x) = (a+c)+i(b+d)x = (a+ibx)+(c+idx) = \varphi(a + bx) + \varphi(c + dx) \).

With all the constants mapping to constants and \( \varphi : x \mapsto ix \), bijectivity is satisfied. Therefore \( R_1 \cong R_2 \).

4-6: \( R_1 = \mathbb{Q}[x]/\langle x^3 - 1 \rangle, \ R_2 = \mathbb{Q}[x]/\langle x^3 + x^2 - 2x \rangle \)

\( R_1 \not\cong R_2. \) Over \( \mathbb{Q}[x] \), \( x^3 - 1 \) has two irreducible factors, \( x - 1 \) and \( x^2 + x + 1 \). On the other hand, \( x^3 + x^2 - 2x \) has three irreducible factors \( x, x + 2 \) and \( x - 1 \). By the CRT, this implies that \( x^3 - 1 \) would be isomorphic to a direct sum of two co-prime rings while \( x^3 + x^2 - 2x \) would be isomorphic to a direct sum of three co-prime rings.
Since the co-rime ring $\mathbb{R}[x]/ < x - 1 >$ is common for both sets of direct sums, the problem reduces to showing that $\mathbb{R}[x]/ < x^2 + x + 1 >$ is isomorphic to $\mathbb{R}[x]/ < x > \oplus \mathbb{R}[x]/ < x - 2 >$. This is, however, not an isomorphism, since the direct sum would only contain constants. Therefore $R_1 \not\cong R_2$.

4-7: $R_1 = \mathbb{Z}_7/ < x^3 - 1 >$, $R_2 = \mathbb{Z}_7[x]/ < x^3 + x^2 - 2x >$

$R_1 \cong R_2$. In $\mathbb{Z}_7[x]$ we have three elements that satisfy the equation $x^3 - 1$. They are 1, 2 and 4. $x^3 + x^2 - 2x$ can be factored into $x(x - 1)(x - 5)$.

By CRT we have $\mathbb{Z}_7[x]/ < x^3 - 1 > \cong \mathbb{Z}_7[x]/ < x - 1 > \oplus \mathbb{Z}_7[x]/ < x - 2 > \oplus \mathbb{Z}_7[x]/ < x - 4 >$ and $\mathbb{Z}_7[x]/ < x^3 + x^2 - 2x > \cong \mathbb{Z}_7[x]/ < x > \oplus \mathbb{Z}_7[x]/ < x - 1 > \oplus \mathbb{Z}_7[x]/ < x - 5 >$.

Since all polynomial divisors are of order 1, the direct sums for both rings are simply linear transformations. Therefore $R_1 \cong R_2$.

Complexity Section

1. Show that if a function $f(x)$ can be computed in polynomial time using an oracle for another polynomial time computable function $g(x)$ then $f(x)$ can be computed in polynomial time without the use of oracles.

For a given string $\beta$ and a language $B$, oracles can tell if $\beta \in B$.

If $f(x)$ is using an oracle for $g(x)$ and is still a polynomial time function, then we must call any oracle at most polynomial number of times.

If all the calls within $f(x)$ using any result from the oracle were replaced directly with $g(x)$ and the resulting changed function evaluated at the necessary value, then the time taken would still be polynomial since the composition of two polynomial functions is still polynomial.

2. Show that if a function $f(x)$ has an NC algorithm using an oracle for another NC-computable function $g(x)$ then $f(x)$ itself can be computed in NC without using oracles.

Similar to problem 1, if all places in $f(x)$ using results from the oracle are replaced with $g(x)$ directly and then $f(x)$ would still have a polynomial size circuit because the sum of two polynomials is still a polynomial. Thus $f(x)$ would still be NC even if it did not use oracles. Note that the depth, however would increase by $k(|g(x)|)$ where $k$ is the number of places within $f(x)$ where $g(x)$ occurs and $|g(x)|$ is the size of the circuit for $g(x)$.

3. Solve the following recurrence relations in terms of $n$, expressing the resulting functions asymptotically:
3-1: \( T(n) = 2T(n/2) + cn \)
Answer to 3-1

3-2: \( T(n) = 3T(n/5) + cn \)
Answer to 3-2

3-3: \( T(n) = 2T(n-1) \)

\[ T(n) = 2T(n-1) = 2.2T(n-2) = 2.2.2T(n-3) = 2^4T(n-4) = \cdots. \] This continues until \( n-x = 0 \Rightarrow x = n. \) \( T(n) = 2^n \Rightarrow T(n) = O(2^n). \)

Algorithmic Algebra Section

1. Let \( a, b \in \mathbb{Z}. \) Recall that if \( \gcd(a, b) = d, \) then there exists integers \( x, y \) s.t. \( ax + by = d. \) Devise an algorithm that given an \( a \) and \( b \) with \( a > b, \) computes \( d \) and an \( x \) an \( a \ y \) in time \( O(|<a>||<b>| + |<b>|^3). \)

Given \( m_0 \) and \( m_1, \) the euclidean algorithm for the \( \gcd(m_0, m_1) \) proceeds by finding the remainder sequence \( m_0, m_1, m_2, \ldots, 0 \) where \( m_i = m_{i-2} \mod m_{i-1} \) for \( i > 1. \) Then \( \gcd(m_0, m_1) \) is the last non-zero \( m_i. \)

The extended euclidean algorithm works in the following manner:
Let \( q_i \) be the quotient of the \( i^{th} \) remaindering step. Then \( m_{i+1} = m_{i-1} - q_im_i (i = 2, \ldots, k-1). \)
Let \( (s_0, \ldots, s_k) \) and \( (t_0, \ldots, t_k) \) be two sequences such that \( m_i = s_im_0 + t_im_1 (i = 0, \ldots, k). \)
When \( i = k \) we have \( m_k = \gcd(m_0, m_1) = s_km_0 + t_km_1. \)
Let \( s_{i+1} = s_{i-1} - q_is_i \) and \( t_{i+1} = t_{i-1} - q_it_i (i = 2, \ldots, k-1). \)
Since \( m_0 = 1m_0 + 0m_1 \) and \( m_1 = 0m_0 + 1m_1, \) we have \( s_0 = 1, t_0 = 0, t_1 = 1 \) and \( s_1 = 0. \)
Inductively, \( m_{i+1} = m_{i-1} - q_im_i = (s_{i-1}m_0 + t_{i-1}m_i) - q_i(s_im_0 + t_im_1). \)

Time Taken:
To calculate the remainders and quotients for \( m_0, m_1 \) with \( m_0 = a \) and \( m_1 = b \) we take \(|<a>||<b>| + |<b>|^2 \) to do \( a \mod b \) and \( b \mod m_2, m_2 \mod m_3 \) so on \(|<b>| \) number of times. This is because with each consecutive mod we lose at least 1 bit.
The above calculations also generate all the \( q_i \)s necessary to calculate all \( s_i \) and \( t_i \) values.
There are at most \(|<b>| \) number of \( s_i \) and \( t_i \) values each. Each \( s_i \) calculation takes \(|<b>|^2 + |<b>| \) for the one multiplication and one subtraction.
Similarly each \( t_i \) calculation takes \(|<b>|^2 + |<b>| \) time.
Together, all \( s_i \) and \( t_i \) calculations take \(|<b>|^2 + |<b>|^2 + |<b>| \). The total operation count: \(|<a>||<b>| + |<b>|^3 + |<b>|^3 + 2|<b>|^2 \).

1-1: Show that an analogous algorithm works for polynomials and assuming that all the underlying field operations are done in constant time, the time complexity for this is \( O(deg(a) * \)
2. Show that given integers $a, t, m$ we can compute $a^t \mod m$ in time $O(|a|, |m| + |t|)$. 

$a^t \mod m = (a \mod m)^t \mod m$.

The operation $a \mod m = r_0$ takes $|a| + |m|$ time. We now need to calculate $r_0^t \mod m$.

Note that $r_0 < m$. Without loss of generality, we can assume that $r_0^2 > m$. Then we have: $r_0^t \mod m = (r_0^2 \mod m)^{t/2} \mod m$.

Calculating $r_0^2 \mod m = r_1$ takes $|m| |t|^2$ operations. Now we have $t/2$ number of $r_1$ remainders. We can repeat the same process and calculate $(r_1^2 \mod m)^{t/4} \mod m$. $r_1^2 \mod m$ would once again take $|m| |t|^2$ operations.

Continuing this process we would have $t/2 + t/2 + t/8 + ...$ number of $|m| |t|^2$ sized operations for calculating $r_2^2 \mod m$. $t > t/2 + t/4 + t/8 + ...$. Therefore we have that the total for calculating $r_0^t \mod m = |m| |t|^2 |t|$. 

The total time taken for calculating $a^t \mod m$ is therefore $|a| + |m| + |m| |t|^2 |t|$. 

$deg(b) + deg(b)^3$.