Assignment IV

1. Find all the elements in $\mathbf{Z_{561}}$ satifying $x^2 = 1 \mod n$ using the Chinese remainder theorem. (use Euclid's algorithm for modular inversion). □

2. When $n = 561$, suppose $a = 35$ is the element in $\mathbf{Z^*_{561}}$ chosen randomly by the Miller Rabin test, will the test return prime or composite? □

3. Let p, q be odd prime numbers. Let $n = pq$, $m = (p-1)(q-1)$ and $e \in \mathbf{Z^*_m}$. Let d be the multiplicative inverse of e in $\mathbf{Z^*_m}$. □

   1. For any $x, y \in \mathbf{Z^*_n}$ show that $x^e \neq y^e \mod n$ unless $x = y$.
   2. For all $x \in \mathbf{Z^*_n}$, show that $(x^e)^d = x^{ed} = x \mod n$.

   (Note: What we have set up is the RSA cryptosystem. Part I established the injectivity of the encryption function (so that two different messages doesn't get mapped to the same cyphertext) and Part II how the original message can be recovered from the cyphertext).

4. Let p be an odd prime. Let g be a generator of $\mathbf{Z^*_p}$ and $d \in \mathbf{Z^*_p}$. Given any (message) x, the El-Gamal encryption scheme picks a random $r \in \mathbf{Z^*_p}$ and sends the pair $(\alpha = g^r \mod p, \beta = x(g^d)^r \mod p)$. (It is assumed that the sender knows p, g and g^d, but only the receiver knowns d.) At the receving show that the message x can be recovered from α and β by computing $(\alpha^d)^{-1}\beta \mod p$. □

5. Let $(R, +, .)$ be a (commutative) ring with unity. $S \subseteq R$ is called an *Ideal* in R if S is a subring of R and S has the property that if $a \in R$ and $s \in S$, then $as \in S$. That is, if you multiply any ring element with an element in S, the resultant element is in S. □

   1. If $a, b \in \mathbf{Z}$, Show that $S = \{ax + by : x, y \in \mathbf{Z}\}$ is an ideal.
   2. Let S be any ideal in $\mathbf{Z}$, show that there exists an element d in S such that $S = d\mathbf{Z}$.
   3. Find all the ideals in the ring $\mathbf{Z_{10}}$.

6. Let G, H be (commutative) rings (with unity). A function $f : G \longrightarrow H$ is a ring homomorphism if f satisfies for all $a, b \in G$, $f(a+b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$ and $f(1) = 1$. Define $ker(f) = \{a \in G : f(a) = 0\}$ and $Img(f) = \{f(a) : a \in G\}$. In each of the following maps, first verify that f is a ring homomorphism and find $ker(f)$ and $img(f)$.
   a) $f(x) = x \mod n$ from $\mathbf{Z}$ to $\mathbf{Z_n}$. b) $f(x) = x \mod 5$ from $\mathbf{Z_{10}}$ to $\mathbf{Z_5}$. □

7. This question develops the notion of quotient ring. Suppose S is an ideal in a ring R. Since S is an additive subgroup of R, we can define addition of cosets in the way developed in last question of Assignment II. Thus, we define $(a + S) + (b + S) = (a + b) + S$. We now extend the system to accomodate multiplication as well with the rule $(a + S)(b + S) = ab + S$. Show that with this definition of multiplication of cosets, the set of cosets form a ring. (Critically observe where in the proof you are using the assumption that S is an ideal and not just a sub-ring). This ring is called the **quotient ring** of R defined by S, denoted by R/S. Which coset is the multiplicative identity in the ring? □

8. The last Question of Assignment IV developed the homomorphism theorem for groups. We now extend this to rings. Let f be a homomorphism from a ring G to a ring H. Let $S = ker(f)$. □

   1. Show that $ker(f)$ is an ideal in G and $Img(f)$ is a subring of H.
   2. Define the map $\Phi : G/S \longrightarrow Img(f)$ as follows: $\Phi(a+S) = f(a)$. (The map simply associates the coset $a + S$ in G/H to the element $f(a)$ in $Img(f)$).
   3. Show that $\Phi((a+S)+(b+S)) = \Phi(a+S)+\Phi(b+S) = f(a)+f(b)$, $\Phi((a+S)(b+S)) = \Phi(a+S)\Phi(b+S)$ and $\Phi(1+S) = 1$. Since bijectivity of the map Φ was proved already in Assignment IV, Φ defines an isomorphism between G/S and $img(f)$. This observation is known as the homomorphism theorem for rings.