Assignment 1

1. Let p be an odd prime. Show that every $a \in Z_p*$ is a root of the equation $x^p - x = 0$. Hence conclude that $x^{p-1} - 1 = \prod_{a=1}^{p-1}(x-a)$ in Z_p. Comparing constant terms conclude that $(p-1)! = -1(\mod p)$. Prove that if $(p-1)! = -1(\mod p)$ for odd p then p is prime. This is called *Wilson's Theorem*. □

2. Let R be a commutative ring with unity. Let $I \subseteq R$ be a subring satisfying the additional property that for all $a \in R, i \in I, ai \in I$. □

   1. For each $n \in Z$, show that $nZ = \{ni, i \in Z\}$ is an ideal in Z, where Z denotes the set of integers.
   2. Let $m, n \in Z$, show that the set $S(m,n) = \{im + jn, i, j \in Z\}$ is an ideal in Z. Let $GCD(m,n) = d$. Show that $S(m,n) = GCD(m,n)$.
   3. For each $a \in R$ define $a + I = \{a + i : i \in I\}$. For $a, b \in R$, define the equivalance relation $T \subseteq R \times R$ by $(a,b) \in T$ if and only if $a + I = b + I$. Define the set $R/I = \{a + I, a \in R\}$. Now Show the following:
      (a) T is an equivalance relation. Thus R/I is a partition of R and in fact forms the partition defined by the equivalance relation T.
      (b) Define addition and multiplication between elements of R/I as $(a+I)+(b+I) = ((a+b)+I)$ and $(a+I)(b+I) = (ab+I)$. Prove that the operations are well defined. (i.e., if $(a+I) = (a'+I), (b+I) = (b'+I)$ then $((a+b)+I) = ((a'+b')+I)$ and $(ab+I) = (a'b'+I)$ etc.). Which element is the unity?
      (c) Show that R/I with the above addition and multiplication is a commutative ring with unity. This ring is called the **quotient ring defined by the ideal** I.
   4. Let R, R' be commutative rings with unity. A map $f : R \longrightarrow R'$ is a ring homomorphism between R and R' if $f(1) = 1$, $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$. If the map is also bijective, then it is called an isomorphism. Let f be a ring homomorphism from R to R'. Define $ker(f) = \{a \in R : f(a) = 0\}$ and let $img(f) = \{f(a) : a \in R\}$, the image of f
      (a) Show that $ker(f)$ is an ideal in R.
      (b) Show that $img(f)$ is a subring of R'
      (c) Define the map $\overline{f} : R/ker(f) \longrightarrow img(f)$ by $f(a+I) = f(a)$. Show that $\overline{f}$ is a homomorphism from $R/ker(f)$ to $img(f)$. Show that $\overline{f}$ is an isomorphism.
   5. Show that Z/nZ is isomorphic to the ring Z_n. (In fact this is the algebraist's way to define the ring Z_n).

3. Let $Z_p[X]$ denote the set of polynomial with coefficients in Z_p. Let $f, g \in Z_p[X]$. (Let $deg(f) = m$, $deg(g) = n$ denote their degrees) Then we can write $f = qg + r$ where $deg(r) < deg(g)$ by normal division by remainder. This yields the Euclid's algorithm for division of polynomials in any field (not necessary finite). □

   1. Show that $F_p[X]$ is a commutative ring with unity (in fact an integral domain).
   2. Define $GCD(\alpha, \beta)$ in $F_p[X]$.
   3. Find $GCD(x^3+1), x^4+1)$ in $F_2[X]$.
   4. Let $g \in F_p[X]$. Define $gF_p[X] = \{gf : f \in F_p[X]\}$ show that $gF_p[X]$ is an ideal in $F_p[X]$.
   5. The quotient ring $F_p[X]/gF_p[X]$ is (just like the quotient ring Z/nZ in Z) is denoted by $F_p[X]/ < g(x) >$
   6. How many elements will the quotient ring $F_p[X]/gF_p[X]$ contain? Which among those elements are invertable. (The answers are exactly akin to the answers in the ring Z_n).

7. Show that the ring $F_p[X]/ < g(x) >$ is a field if and only if g is irreducible (i.e. if $g(x) = \alpha(x)\beta(x)$ then one of the factors is a constant, ie., memeber of Z_p). (Hint: Recall the proof showing that Z_n is a field iff n is prime). This gives as a way of starting from a field of p elements (viz. Z_p) and construct a field of size p^n using an irreducible polynomial of degree n.
8. Show that Z_p is a subfield of $Z_p[X]/ < g(x) >$.
9. Show that elements of $Z_p[X]/ < g(x) >$ over the field Z_p forms a vector space (with polynomial addition and multiplication defined by the field itself). What is the dimension of the vector space?
10. Recall that any finite field of dimension n over Z_p is isomorphic to Z_p^n. In this case, as each element in $Z_p[X]/ < g(x) >$ is a polynomial of degree atmost $n - 1$ the coefficiant vector of the polynomial gives a natural vector representation for each element in the field w.r.t the basis $\{1, x, x^2, ...x^{n-1}\}$
11. Consider any $\alpha \in Z_p[X]/ < g(x) >$. Consider the elements $1, \alpha, \alpha^2, ...\alpha^n$. Show that these elements are linearly dependent (in the above vector space). This means there exists a $a_0, a_1, ..a_n \in Z_p$ such that $\sum_{i=0}^{n} a_i\alpha^i = 0$. Hence conclude that every element in $Z_p[X]/ < g(x) >$ is a root of some polynomial of degree atmost $n = (deg(g))$ with coefficients in Z_p. Show that every $\alpha \in Z_p[X]/ < g(x) >$ is a root of the polynomial $y^{p^n} - y = 0 \in Z_p[Y]$. (The indeterminate has been changed from x to y only to avoid confusion with the elements in $Z_p[X]/ < g(x) >$ that are themselves polynomials in variable x.)