CS 6101 MFCS - Test V, Sep.'17. Name:

1. (3 points) Let p, q be odd primes. Let i, j be elements in $\mathbf{Z}_{pq}$ and such that $(i \mod p) = 1$, $(i \mod q) = 0$, $(j \mod p) = 0$, $(j \mod q) = 1$. Find an expression in terms of i, j, p and q for all distinct solutions (upto congruence $\mod pq$) for the equation $x^2 = 1 \mod pq$.

   Soln: Assuming $p \neq q$, the possible solutions are those for which $x = \pm 1 \mod p$ and $x = \pm 1 \mod q$. It is not hard to see that $x = \pm i \pm j$ satisfies these conditions. (Chinese remainder Theorem shows that $i = q(q^{-1} \mod p)$ and $j = p(p^{-1} \mod q)$). if x is a solution, so is $x + pq$. Hence, the general solution is $\pm i \pm j + tpq$ for all integer t.

   if $p = q$, then $\mathbf{Z}^*_{p^2}$ is a cyclic group. Any solution to $x^2 = 1 \mod p^2$ must have order 2 or 1 (why?). There is $\phi(2) = 1$ element of order 2 (why?) and there are two solutions in total to $x^2 - 1 = 0$. (Full marks will be given if you solve the case $p \neq q$.)

2. (3 points) Let $I \neq \{0\}$ be an ideal in $\mathbf{Z}$. Let r be the least positive integer in I. Show that every element in I is an integer multiple of r.

   Soln: Suppose $i \in I$. Let $i = xr + y$ where $x = i$ div r and $y = i \mod r$. We have therefore, $y < r$. But by the absoption property of ideal, $xr \in I$ and hence $i - xr = y \in I$ (why?). This contradicts the assumption that r is the least positive integer in I.

3. (3 points) Let M_n be the set of all $n \times n$ non-singular real matrices. Let f be the map from M_n to $\mathbf{R}$ defined by $f(A) = det(A)$. Is f a ring homomorphism? if so find the kernel and image of f.

   Soln: f is not a ring homomorphism because $f(A+B) = det(A+B) \neq det(A) + det(B) = f(A) + f(B)$ in general. In fact, the set of non-singular real matrices do not even form a ring. (if A is non-singular, $A - A$ is singular etc.). However, the set of non-singular matrices form a (non-commutative) group with respect to multiplication and f is a group homomorphism onto non-zero real numbers (with multiplication).

4. (3 points) Let p, q be odd primes. What is the maximum order of an element in Z^*_{pq}?

   Soln: By Chinese remainder Theorem, $Z^*_{pq} \cong \mathbf{Z}^*_p \times \mathbf{Z}^*_q$. Since both $\mathbf{Z}^*_p$ and $\mathbf{Z}^*_q$ are cyclic with order $p-1$ and $q-1$, Let g_1 and g_2 be generators of $\mathbf{Z}^*_p$ and $\mathbf{Z}^*_q$ respectively. Every element in $\mathbf{Z}^*_p \times \mathbf{Z}^*_q$ is of the form (g_1^i, g_2^j) for some integers i, j. Let $t = LCM(p-1, q-1)$, then $(g_1^t, g_2^t) = (1, 1)$ in $\mathbf{Z}^*_p \times \mathbf{Z}^*_q$, it follows that any element of form (g_1^i, g_2^j) will have order at most t (why?).

   If $p = q$, $\mathbf{Z}^*_{p^2}$ is cyclic of order $p(p-1)$. Hence, generators of $\mathbf{Z}^*_{p^2}$ have order $p(p-1)$, which is the maximum possible (why?).

5. (3 points) Let p be an odd prime. Let g be a generator of $\mathbf{Z}^*_p$. Suppose g is not a generator of $Z^*_{p^2}$, what is the order of g. Give clear proof for your answer.

   Soln: $Z^*_{p^2}$ has order $p(p-1)$ and is cyclic. If $o(g)$ in this group is t, then $g^t = 1 \mod p^2$ and $g^t = 1 \mod p$ (why?). This implies that $p - 1 | t | p(p-1)$. The only possible value for t is $p - 1$.