CS 4031 **January, 2017**

Computational Algebra **Test I** **32 Marks**

1. Let a and b be generators of cyclic groups G_1 and G_2 respectively with p and q elements for some distinct odd primes p and q. Find all values of i, j for which (a^i, b^j) is not a generator of $G_1 \times G_2$, $1 \le i \le p, 1 \le j \le q$. $\boxed{4}$

   Soln: except when $i = p$ or $j = p$ or both. (total $p + q - 1$ possibilities).

2. Let F be a field and $\alpha \in F$ be an element. Let $m(x) \in F[x]$ be a polynomial of minimum degree that has α as a root. Show that $m(x)$ is irreducible. Is the claim true if F is an integral domain? $\boxed{4}$

   Soln: $(x - \alpha)$ is the minimum polynomial that has α as a root. Clearly, this is irreducible, irrespective of whether F is a field or an integral domain.

3. Let p, q be primes such that $p < q$. Suppose that Z^*_{pq} is cyclic. What are the possible values for p? Justify your answer. $\boxed{4}$

   Soln: $Z^*_{pq} \equiv Z^*_p \times Z^*_q$ by Chinese remainder theorem. The RHS is a product of two cyclic groups of order $p - 1$ and $q - 1$. Such a product is cyclic if and only if $GCD(p - 1, q - 1) = 1$. Since $p < q$ and p, q primes, this can happen if and only if $p = 2$.

4. Let $a(x)$ be a polynomal of degree at most $n - 1$ whose n-point FFT is $(0, 1, 0, 1, ..., 0, 1)$. Let $b(x)$ be a polynomal of degree at most $n - 1$ whose n-point FFT is $(1, 0, 1, 0, ..., 1, 0)$. Find $a(x)b(x) \mod (x^n - 1)$. Justify your answer. $\boxed{4}$

   Soln: Let ω be a primitive n^{th} root of unity. Then $FFT(a(x)b(x) \mod (x^n - 1))$
   $= (a(1)b(1), a(\omega)b(\omega), a(\omega^2)b(\omega^2), .., a(\omega^{n-1})b(\omega^{n-1})) = (0, 0, ...0)$. It follows that $a(x)b(x) \equiv 0 \mod (x^n - 1)$.

5. Let p be an odd prime. How many elements in Z^*_p has a square root? (That is, for how many values of a between 1 and $p - 1$ does the equation $x^2 = a \mod p$ has a solution?) $\boxed{4}$

   Soln: Let g be a generator of Z^*_p. All even powers of g must have exactly two square roots (why?). This gives us $\frac{p-1}{2}$ distinct elements in Z^*_p having square roots (how?) If a has a square root, then a must be a root of the polynomal $x^{\frac{p-1}{2}} - 1$ in Z^*_p (why?). Hence there can't be more than $\frac{p-1}{2}$ elements with square roots in Z^*_p (why?)

6. Given $n = 561 = 3 \times 11 \times 17$. Is it true that for each $a \in Z^*_{561}$, $a^{n-1} = 1 \mod n$? Justify. (Of course, not to be solved via brute force..). $\boxed{4}$

   Soln: By Chinese remainder theorem, $Z^*_{561} \equiv Z^*_3 \times Z^*_{11} \times Z^*_{17}$. Let $a \in Z^*_{561}$. Let $a = (a_1, a_2, a_3)$ on the RS of the Chinese remainder theorem. Applying Fermat's thereom, we have $a_1^2 = 1 \mod 3$, $a_2^{10} = 1 \mod 11$, $a_3^{16} = 1 \mod 17$. Hence $a_1^{560} = 1 \mod 3$, $a_2^{560} = 1 \mod 11$, $a_3^{560} = 1 \mod 17$ because 2, 10 and 16 divides 560.

7. A maximal ideal in a ring R is an ideal I such that 1) I is a *strict* subset of R and 2) any ideal of R *properly* containing I must be the whole R itself. Suppose I is a maximal ideal in a field F. What can you conclude about I? $\boxed{4}$

   Soln: If I contains any non zero element a, then since $aa^{-1} \in I$ and thus we have $1 \in I$. But then, for each $r \in R$, $1.r = r \in I$. Hence $I = R$. Hence, if $I \neq R$ then $I = \{0\}$.

8. Consider the linear transformation T from $\mathbf{R}^n$ to itself that transforms a vector $(a_0, a_1, ..., a_{n-1})$ to the vector $(a_1, 2a_2, 3a_3, .., (n-1)a_{n-1}, 0)$. Find all solutions to $T(x) = (1, 0, 0, ...0)$.

   Soln: Note that T is the derivative operator. It is easy to see that $ker(T) = \{(c, 0, 0, ...0) : c \in \mathbf{R}\}$. A particular solution to $T(x) = (1, 0, 0, .., 0)$ is $x_0 = (0, 1, 0, 0, ...0)$. Thus the general solution is $x_0 + ker(T) = (c, 1, 0, ...0)$.