CS 6101 MFCS Final Exam, Nov. 2017. Name:

Answer STRICTLY in the space provided. Answers written elsewhere may not be valued. Brief and precise justification to your answer to each question is ABSOLUTELY NECESSARY and shall be given on the **reverse side** of the sheet containing the question.

1. Let p be an odd prime. How many solutions are there for the equation $x^2 = 1 \mod 2p$. $\boxed{2}$

   Soln: By Chinese remainder theorem, $\mathbf{Z}_{2p}^* \equiv \mathbf{Z}_2^* \times \mathbf{Z}_p^*$. Hence, it sufficies to count solutions of the form $(a, b) \in \mathbf{Z}_2^* \times \mathbf{Z}_p^*$ such that $(a, b)^2 = (a^2, b^2) = (1, 1)$ (why?). The possible solutions are only $(1, 1)$ and $(1, -1)$ (why?). Thus here are exactly 2 solutions.

2. Let p be an odd prime. Consider the homomorphism $f : \mathbf{Z}_p^* \mapsto \mathbf{R}$ defined by $f(a) = a^{\frac{p-1}{2}} \mod p$. How many elements are there in $\ker(f)$? (Hint: Let α be a generator of $\mathbf{Z}_p^*$. Try evaluating $f(\alpha), f(\alpha^2), \ldots$) $\boxed{2}$

   Soln: Let g be a generator of $\mathbf{Z}_p^*$. Hence, every element in $\mathbf{Z}_p^*$ must be of the form g^i for some positive integer i, $1 \leq i \leq p-1$. $f(g^i) = 1$ if and only if i is even ($f(g^i) = -1$ when i is odd - why?). Thus, there are $\frac{p-1}{2}$ elements in $\mathbf{Z}_p^*$ whose image under f is 1. Since 1 is the multiplicative identify in $\mathbf{R}$, and f is a group homomorphism from $\mathbf{Z}_p^*$ to $\mathbf{R}^*$, $\ker(f)$ has $\frac{p-1}{2}$ elements.

3. Let n be a positive integer. Let $0 \neq d \in \mathbf{Z}_n$. Consider the ideal $I = d\mathbf{Z}_n$. How many elements $d' \in \mathbf{Z}_n$ satisfy $I = d'\mathbf{Z}_n$? $\boxed{2}$

   Soln: I consists of all elements of the form $dx \mod n$ for various values of x. In other words, I consists of elements $I = \{b \in \mathbf{Z}_n : dx = b \mod n \text{ has a solution}\}$. In other words, I is the cyclic subgroup of the additive group $\mathbf{Z}_n$ of n generated by d. Yet another way to look at this is that $I = \{b \in \mathbf{Z}_n : \text{there exists integers } x, y \text{ such that } dx + ny = b\}$. Consequently we see that $I = \{b : \mathrm{GCD}(n, d) | b\}$ (why?). Thus d' generates I if and only if GCD(n, d')=GCD(n, d). But the order of GCD(n, d) is $\frac{n}{\mathrm{GCD}(n,d)}$ in $\mathbf{Z}_n$ (why?). Consequently, the question is to find how many elements of order $\frac{n}{\mathrm{GCD}(n,d)}$ present in the cyclic subgroup generated by GCD(n, d) (why?). We have seen in the class that this is given by $\varphi(\frac{n}{\mathrm{GCD}(n,d)})$, where φ is the Euler's tautient function.

4. Let p, q be distinct odd primes. For how many values a in $\{1, 2, \ldots, pq-1\}$, the system of equations $ax = 1 \mod p$ and $ay = -1 \mod q$ have no solution? $\boxed{2}$

   Soln: $ax = 1 \mod p$ fails to have a solution if and only if a is a multiple of p and $ay = -1 \mod q$ fails to have a solution if and only if a is a multiple of q (why?). Hence, any a which a "non-solution" in $\mathbf{Z}_{pq}$ must be either a multiple of p or q. In other words, non-solutions are precisely those elements in $\mathbf{Z}_{pq} \setminus \{0\}$ satisfying GCD$(a, pq) \neq 1$. Hence, there are $(pq-1) - \varphi(pq) = (pq-1) - (p-1)(q-1) = p + q - 2$ non-solutions.

5. If n is a Carmichael number. For how many $a \in \mathbf{Z}_n$, $a \neq 0$ such that $a^{n-1} \neq 1 \mod n$? $\boxed{2}$

   Soln: If n is Carmichael, every element in $\mathbf{Z}_n^*$ will satisfy $a^{n-1} = 1 \mod n$. All the remaining $n - \varphi(n)$ elements of $\mathbf{Z}_n$ are not co-prime to n and hence cannot satisfy $a^{n-1} = 1 \mod n$ (why?).

6. How many elements $a \in \mathbf{Z}_{121}^*$ satisfy $a^{11} \neq 1 \mod 121$ and $a^{10} \neq 1 \mod 121$? $\boxed{2}$

   Soln: For any odd prime p, Any element in $\mathbf{Z}_{p^2}^*$ that satifies $a^{p-1} \neq 1 \mod p^2$ and $a^p \neq 1 \mod p^2$ must have order $p(p-1)$ and Consequently must be a generator of $\mathbf{Z}_{p^2}^*$. Since $\mathbf{Z}_{p^2}^*$ is a cyclic group of $\varphi(p^2)$ elements, it must have $\varphi(\varphi(p^2))$ generators. Here $p = 11$, hence $\varphi(\varphi(121)) = \varphi(110) = 40$.

7. For what values of d, $0 < d < 121$, the equation $3x + 4y = d$ have no solution? $\boxed{2}$

   Soln: As GCD$(3, 4)$=1, the equation $3x + 4y = d$ has a solution for every integer value of d. Hence, the answer to the question is zero.

8. Consider the system of equations, $ax^2 + bx = p \mod (x-1)$ and $ax^2 + bx = q \mod (x+1)$. Solve for a and b in terms of p and q. $\boxed{2}$

   Soln: By remainder theorem, the remainder of dividing any polynomial $Q(x)$ by $(x-\alpha)$ is obtained by evaluating $Q(x)$ at $px = \alpha$. The two equations given above corresponds to setting $Q(x) = ax^2 + bx$, with $\alpha = 1$ and $\alpha = -1$ respectively. From these, we get $a + b = p$ and $a - b = q$. Consequently $a = \frac{p+1}{2}$, $b = \frac{p-q}{2}$ is one possible solution. (Note that other solutions exist. For example, if $Q(x)$ is one solution, so is $Q(x) + S(x)(x^2 - 1)$ for any polynomial $S(x)$).

9. Let $b_1, b_2, \ldots, b_n$ and $c_1, c_2, \ldots, c_n$ be two distinct basis for a vector space V over a field F. Let B be the matrix of basis translation satisfying $[b_1, b_2, \ldots, b_n] = [c_1, c_2, \ldots, c_n]B$. Show that for any $\vec{x} = [x_1, x_2, \ldots, x_n] \in F^n$, $B\vec{x} = 0$ only if $\vec{x} = 0$. $\boxed{2}$

   Soln: Suppose $B\vec{x} = 0$, then $[c_1, c_2, \ldots, c_n]B\vec{x} = 0$. i.e., $[b_1, b_2, \ldots, b_n]\vec{x} = 0$, which is possible if and only if $\vec{x} = 0$, as $\{b_1, b_2, \ldots, b_n\}$ is a linearly independent set.

10. Let V, W be a vector spaces over a field F. Let $b_1, b_2, \ldots, b_n$ be a basis of V. Let $T : V \mapsto W$ be a linear transformation. Suppose $T(b_1), T(b_2), \ldots, T(b_n)$ are linearly dependent, is it always the case that T is not injective? Prove/disprove. $\boxed{2}$

    Soln: If $T(b_1), T(b_2), \ldots, T(b_n)$ are linearly dependent, then there exists $x_1, x_2, \ldots x_n \in F$, not all zero, such that $\sum_{i=1}^{n} x_i T(b_i) = T(\sum_{i=1}^{n} x_i b_i) = 0$. As $b_1, b_2 \ldots, b_n$ are linearly independent, $\sum_{i=1}^{n} x_i b_i \neq 0$, and Consequently T cannot be injective.

11. Consider the vector space F^4 over the field $F = \mathbf{Z}_2$. write down all vectors in two distinct 2 dimensional subspaces of F^4. $\boxed{2}$

    Soln: Any two linearly independent vectors in F^4 will generate a subspace of dimension 2. For instance, if we take 0110 and 1001, we get the subspace $\{0000, 0110, 1001, 1111\}$. If we take 0001 and 1000, we get the subspace $\{0000, 0001, 1000, 1001\}$. There are several other possibilities as well.

12. Let $b_1, b_2, \ldots, b_n$ be a basis for a vector space V over a field F. Is $(b_1 - b_2), (b_2 - b_3), \ldots,$ $(b_{n-1} - b_n), (b_n - b_1)$ a basis for V? $\boxed{2}$

    Soln: The sum of the vectors $(b_1 - b_2), (b_2 - b_3), \ldots (b_n - b_1)$ is zero, and hence they cannot be linearly independent.

13. Consider the vector space V over $\mathbf{R}$ consisting of all polynomials (with real coefficiants) of degree less than n . Find a basis for this spaces such that the polynomial $f(x) = 1 + x + x^2 + \cdots + x^{n-1}$ has cordinates $(1, 0, 0, 0, \ldots, 0)$. $\boxed{2}$

    Soln: Any basis $b_1, b_2, \ldots b_n$ with $b_1 = 1 + x + x^2 + \cdots + x^{n-1}$ suffices. For instance, we may set $b_2 = 1, b_3 = x, b_4 = x^2, \ldots, b_{n-1} = x^{n-3}, b_n = x^{n-2}$.

14. Let A be a real symmetric postive definite matrix. Show that $\det(A) \neq 0$. $\boxed{2}$

    Soln: Given, for any $\vec{x} \in \mathbf{R}^n$, $\vec{x}^T A \vec{x} > 0$. Hence $Ax \neq 0$ whenever $x \neq 0$, consequently A is non-singular and $det(A) \neq 0$.

15. Let V be an inner-product space over $\mathbf{R}$. Let $b_1, b_2, \ldots, b_n$ and $c_1, c_2 \ldots, c_n$ be two orthonormal basis with translation matrix B satisfying $[b_1, b_2, \ldots, b_n] = [c_1, c_2, \ldots, c_n]B$. Show that B satisfy $B^T B = I$. $\boxed{2}$

    Soln: Let u, v be arbitrary vectors in V. Let $\vec{x}, vecy$ be cordinates of u, v with respect to $[b_1, b_2 \ldots b_n]$. The cordinates of u, v w.r.t $[c_1, c_2, \ldots, c_n]$ will be $B\vec{x}, B\vec{y}$. Since both $[b_1, b_2, \ldots, b_n]$ and $[c_1, c_2, \ldots, c_n]$ are orthonormal, we have $(u, v) = \vec{x}^T \overline{\vec{y}} = (B\vec{x})^T \overline{B\vec{y}} = \vec{x}^T B^T \overline{B\vec{y}}$. Since u, v were arbitrary, the equality remains true for all $\vec{x}, \vec{y}$ in $\mathbf{R}^n$, which is possible only if $B^T \overline{B} = I$.

16. Find the matrix B for an orthonormal basis translation from $\mathbf{R}^2$ to $\mathbf{R}^2$ (w.r.t. the standard inner product) satisfying $B \neq \pm I$ where I is the 2×2 identify matrix, such that B has **real** Eigen values. $\boxed{2}$

Soln: $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ are two possibilities. In both cases, $[1, 0]^T$ and $[0, 1]^T$ are Eigen vectors. In the first case, the corresponding Eigen values are -1 and 1. In the second case, the Eigen values are 1 and -1. Note that these are "flip" operations around an axis.

17. Find the point nearest to the vector $[1, 1, 1]^T$ in the plane $x + y + z = 0$. $\boxed{2}$

Soln: Since the vector $[1, 1, 1]^T$ is perpendicular to the plance $x + y + z = 0$, its projection to any vector in the plane is zero. Consequently, the point nearest to the vector in the plane is the origin, $[0, 0, 0]^T$.

18. Let u, v be vectors in a real inner product space V such that $(u, v) = 0$. Show that $||u + v||^2 = ||u||^2 + ||v||^2$. $\boxed{2}$

Soln: $||u + v||^2 = (u + v, u + v) = (u, u) + (u, v) + (v, u) + (v, v) = ||u||^2 + ||v||^2$.

19. Find a 2×2 Hermitian matrix A such that $[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]^T, [-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]^T$ are Eigen vectors of A with Eigen values $+1$ and -1 respectively. $\boxed{2}$

Soln: It is easy to see that the matrix $A = 1[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]^T[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}] - 1[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]^T[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}]$ suffices.

i.e., $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

20. Find the cordinates x_1, x_2, x_3 and x_4 of the point $[1, 2, 3, 4]^T$ with respect to the basis $b_1 = \frac{1}{2}[1, 1, 1, 1]^T$, $b_2 = \frac{1}{2}[1, -1, 1, -1]^T$, $b_3 = \frac{1}{2}[1, 1, -1, -1]^T$, $b_4 = \frac{1}{2}[-1, 1, 1, -1]^T$ of $\mathbf{R}^4$. $\boxed{2}$

Soln: The given basis is orthonormal. Hence, the cordinates are obtained by projections. Let $v = [1, 2, 3, 4]$. We have $(v, b_1) = 5, (v, b_2) = -1, (v, b_3) = -2, (v, b_4) = 0$.