Show all your work, and return this sheet with your exam. Name: _____

1. [12 points] Let A be a set with 7 elements, and let B be a set with 5 elements.

(a) Find the cardinality of the cartesian product $A \times B$.
$|A \times B| = |A||B| = 35$

(b) Find the cardinality of the power set $\mathcal{P}(B)$. Recall that $\mathcal{P}(X)$ is the set of all subsets of X.
$|\mathcal{P}(B)| = 2^{|B|} = 32$

(c) In how many ways can one choose 3 elements from A (without replacement)?
$\binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35$

(d) What is the smallest possible cardinality of the union $A \cup B$?
$|A \cup B| = |A| + |B| - |A \cap B| \geq 7 + 5 - 5 = 7$ the minimum is achieved when $B \subset A$

2. [16 points] For each positive integer n, let $S(n)$ be the sum $S(n) = 1 + 7 + 13 + \cdots + (6n - 5)$, that is, $S(n) = \sum_{i=1}^{n}(6i - 5)$.

(a) Compute $S(1)$ and $S(2)$.
$S(1) = 1 \quad S(2) = 1 + 7 = 8$

(b) Use mathematical induction to prove that $S(n) = n(3n - 2)$ for every positive integer n.
Let $\mathcal{S} \subset \mathbb{P}$ be the set of positive integers n for which $\mathcal{S}(n) = n(3n - 2)$,
that is $\sum_{i=1}^{n}(6i - 5) = n(3n - 2)$.
Since $S(1) = 1$ from part (a), we have $1 \in \mathcal{S}$.
Assume that $k \in \mathcal{S}$, so that $S(k) = k(3k - 2)$, that is $\sum_{i=1}^{k}(6i - 5) = k(3k - 2)$.
Then, $S(k+1) = \sum_{i=1}^{k+1}(6i - 5) = \sum_{i=1}^{k}(6i - 5) + (6(k+1) - 5) = S(k) + (6(k+1) - 5)$.
Since $S(k) = k(3k - 2)$, we have
$S(k+1) = k(3k - 2) + 6k + 1 = 3k^2 + 4k + 1 = (k+1)(3k+1) = (k+1)(3(k+1) - 2)$.
So $k \in \mathcal{S} \implies k + 1 \in \mathcal{S}$. Therefore, $\mathcal{S} = \mathbb{P}$ by mathematical induction,
and $S(n) = n(3n - 2)$ for every positive integer n.

3. [16 points]

(a) Use the Euclidean algorithm to find the greatest common divisor $d = (84, 360)$ of 84 and 360.
$\begin{bmatrix} 1 & 0 & 84 \\ 0 & 1 & 360 \end{bmatrix} \xrightarrow{R2-4R2} \begin{bmatrix} 1 & 0 & 84 \\ -4 & 1 & 24 \end{bmatrix} \xrightarrow{R3-3R2} \begin{bmatrix} 13 & -3 & 12 \\ -3 & 1 & 24 \end{bmatrix} \xrightarrow{R2-2R1} \begin{bmatrix} 13 & -3 & 12 \\ -30 & 7 & 0 \end{bmatrix}$ $d = 12$

(b) Express d as a linear combination of 84 and 360, that is, as $d = 84s + 360t$.
$d = 12 = 84(13) + 360(-3)$

(c) Find the least common multiple of $m = [84, 360]$ of 84 and 360.
$m = [84, 360] = \frac{84 \cdot 360}{(84, 360)} = \frac{84 \cdot 360}{12} = 2520$

4. [18 points] This problem concerns arithmetic modulo 15.
All answers should be expressed as $[a]_{15}$, where a is an integer with $0 \le a < 15$.

(a) Compute $[3]_{15} \cdot [9]_{15} + [12]_{15}^2$
$[3]_{15} \cdot [9]_{15} + [12]_{15}^2 = [27]_{15} + [144]_{15} = [12]_{15} + [9]_{15} = [21]_{15} = [6]_{15}$

(b) Compute $[13]_{15}^{-1}$
Use, for instance, the Euclidean algorithm to check that $13(7) + 15(-6) = 1$.
From this, we have $[13]_{15}[7]_{15} = [1]_{15}$, so $[13]_{15}^{-1} = [7]_{15}$.

(c) Find all elements $[a]_{15}$ in $\mathbb{Z}_{15}$ for which $[a]_{15} \cdot [10]_{15} = [0]_{15}$.
Check that $15 \mid 10a$ for $a = 0, 3, 6, 9, 12$, (and that $15 \not| 10a$ for $a = 1, 2, 4, 5, 7, 8, 10, 11, 13, 14$).
Consequently, the relevant elements in $\mathbb{Z}_{15}$ are $[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}$.

(d) List all units in $\mathbb{Z}_{15}$.
$[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}$ check that $(a, 15) = 1$ for each of these

(e) How many zero divisors are there in $\mathbb{Z}_{15}$?
Since $|\mathbb{Z}_{15}| = 15$, and there are $\varphi(15) = 8$ units, there are $15 - 8 = 7$ zero divisors.

5. [20 points] In this problem, you may use the equation $5 \cdot 41 - 12 \cdot 17 = 1$
(You do not need to verify this equation using the Euclidean algorithm.)

(a) Find the multiplicative inverse of $[12]_{41}$ in $\mathbb{Z}_{41}$. Express your answer as $[a]_{41}$, where $0 \le a < 41$.
From the equaltion, we have $[12]_{41}[-17]_{41} = [1]_{41}$, so $[12]^{-1} = [-17]_{41} = [24]_{41}$

(b) Solve the linear congruence $12x \equiv 11 (\mathrm{mod}\, 41)$.
Multiplying both sides by 24, we get $x \equiv 24 \cdot 11 (\mathrm{mod}\, 41) \equiv 18 (\mathrm{mod}\, 41)$, that is, $x = [18]_{41}$.

(c) Are there integers $a, b > 0$ for which the congruence $ax \equiv b (\mathrm{mod}\, 41)$ has no solution? Explain.
Yes. For instance, $82x \equiv b (\mathrm{mod}\, 41)$ has no solution if $b \not\equiv 0 (\mathrm{mod}\, 41)$.

(d) Find all solutions of the following system of congruences, and find the smallest positive solution.
$x \equiv 6 (\mathrm{mod}\, 41) \quad x \equiv 5 (\mathrm{mod}\, 17)$
Using the equation, we have $x \equiv (5{\cdot}5{\cdot}41 - 6{\cdot}12{\cdot}17) (\mathrm{mod}\, 41{\cdot}17) \equiv -199 (\mathrm{mod}\, 697) \equiv 498 (\mathrm{mod}\, 697)$
498 is the smallest positive solution

6. [18 points]

(a) Compute $\varphi(144)$. Here, $\varphi(n)$ is the Euler φ-function evaluated at n.
Since $144 = 12 \cdot 12 = 2^4 \cdot 3^2$, $\varphi(144) = 144\big(1 - \frac{1}{2}\big)\big(1 - \frac{1}{3}\big) = 48$

(b) State Euler's Theorem, and use it to compute $13^{100} (\mathrm{mod}\, 144)$.
If a, n are integers (with $n > 0$) and $(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.
Since $100 = 2 \cdot 48 + 4$, we have $13^{100} = 13^{2 \cdot 48 + 4} = (13^{48})^2 \cdot 13^4$.
So, $13^{100} (\mathrm{mod}\, 144) \equiv (13^{48})^2 \cdot 13^4 (\mathrm{mod}\, 144) \equiv 1^2 \cdot 13^4 (\mathrm{mod}\, 144) \equiv 169^2 (\mathrm{mod}\, 144) \equiv 49 (\mathrm{mod}\, 144)$

Spring 2013 Math 4023-1 Exam 1 Statistics

Score	Number
90 – 100	4
80 – 89	8
70 – 79	6
0 – 69	3
total	21

average: 76
median: 82