Math 310-010 - Spring 2016 - Test 1 - Part 1/2 -SOLUTIONS

Instructor: Dr. Francesco Strazzullo My Name____________________

I certify that I did not receive third party help in completing this test. (*sign*)____________________

Instructions. SHOW YOUR WORK neatly, please. Each exercise is worth 10 points. If using a result from the book, make a reference to it (using the page number as well). **Note:**When possible, the notation $\bar{a} = [a]_m$ is used.

1. Use the Euclidean algorithm to compute the greatest common divisor of 1739 and 9923.

Solution

$$\begin{array}{rcl|rcl} 9923 & = & 5 \cdot 1739 + 1228 & 99 & = & 12 \cdot 8 + 3 \\ 1739 & = & 1 \cdot 1228 + 511 & 8 & = & 2 \cdot 3 + 2 \\ 1228 & = & 2 \cdot 511 + 206 & 3 & = & 1 \cdot 2 + 1 \\ 511 & = & 2 \cdot 206 + 99 & 2 & = & 2 \cdot 1 + 0 \\ 206 & = & 2 \cdot 99 + 8 & \gcd(1739, 9923) & = & 1 \end{array}$$

2. Compute the addition (Cayley) table of $\mathbb{Z}_6$.

Solution The operation is commutative, therefore we don't need to write the lower triangular part of the table.

$(\mathbb{Z}_6, +)$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$		$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$			$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$
$\bar{3}$				$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$					$\bar{2}$	$\bar{3}$
$\bar{5}$						$\bar{4}$

3. Compute the multiplication (Cayley) table of $\mathbb{Z}_{12}^*$ (called *set of units* $U(12)$).

Solution The operation is commutative, therefore we don't need to write the lower triangular part of the table. Moreover, $\bar{a} \in \mathbb{Z}_m^*$ if and only if $\gcd(a, m) = 1$, therefore $\mathbb{Z}_{12}^* = \{\bar{1}, \bar{5}, \bar{7}, \bar{1}\bar{1}\}$.

$(\mathbb{Z}_{12}^*, \cdot)$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{1}\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{1}\bar{1}$
$\bar{5}$		$\bar{1}$	$\bar{1}\bar{1}$	$\bar{7}$
$\bar{7}$			$\bar{1}$	$\bar{5}$
$\bar{1}\bar{1}$				$\bar{1}$

4. Find, if possible, the multiplicative inverse of the following congruence classes. You get **5 extra points** if you express the inverse as a power of the given classes.

   (a) $[5]_{11}$

   (b) $[3]_{17}$

Solution One can implement the C++ code

```
int power = a, n=0;
do
{
    power = (a*power)%m;
    n=n+1;
}
while (power != 1);
```

in order to find the exponent n such that $([a]_m)^{n+1} = [1]_m$, that is $([a]_m)^n = ([a]_m)^{-1}$.

(a) $([5]_{11})^{-1} = ([5]_{11})^4 = [9]_{11}$.

(b) $([3]_{17})^{-1} = ([3]_{17})^{15} = [6]_{17}$.

Only for Math 310-02H

5. Prove that for all $n \in \mathbb{Z}$ the set $n\mathbb{Z} = \{na \in \mathbb{Z} \,|\, a \in \mathbb{Z}\}$ is a **subgroup** of $(\mathbb{Z}, +)$, by proving the following.

   (a) $n\mathbb{Z} = (-n)\mathbb{Z}$;

   (b) $n\mathbb{Z}$ is closed under sum, that is if $x, y \in n\mathbb{Z}$ then $x + y \in n\mathbb{Z}$;

   (c) $0 \in n\mathbb{Z}$;

   (d) if $x \in n\mathbb{Z}$ then $-x \in n\mathbb{Z}$.

Solution Let's fix an element $n \in \mathbb{Z}$.

(a) $n\mathbb{Z} = (-n)\mathbb{Z}$, because x is an element of $n\mathbb{Z}$ if and only if x is and element of $(-n)\mathbb{Z}$. Indeed:

$$x \in n\mathbb{Z} \Leftrightarrow x = nq \Leftrightarrow x = (-n)(-q) \Leftrightarrow x \in (-n)\mathbb{Z}$$

(b) $n\mathbb{Z}$ is closed under sum, that is if $x, y \in n\mathbb{Z}$ then $x + y \in n\mathbb{Z}$:

$$x, y \in n\mathbb{Z} \Leftrightarrow x = nq, \quad y = np \Leftrightarrow x + y = nq + np = n(q + p) \Leftrightarrow x + y \in n\mathbb{Z}$$

(c) $0 \in n\mathbb{Z}$ because $0 = n \cdot 0$.

(d) if $x \in n\mathbb{Z}$ then $-x \in n\mathbb{Z}$:

$$x \in n\mathbb{Z} \Rightarrow x = nq \Rightarrow -x = -nq = n(-q) \Rightarrow -x \in n\mathbb{Z}$$

Math 310-010 - Spring 2016 - Test 1 - Part 2/2

Instructor: Dr. Francesco Strazzullo My Name____________________________

Instructions. SHOW YOUR WORK neatly, please. Each exercise is worth 10 points. If using a result from the book, make a reference to it (using the page number as well).

1. Let m be a natural number, $\equiv_m$ be the congruence modulo m, and $[a]_m$ be the congruence class of an integer a with respect to m. By the Euclidean Division Algorithm, for every $a \in \mathbb{Z}$ there is a unique $r \in \mathbb{Z}$ such that $0 \leq r \leq m-1$ and $[a]_m = [r]_m$: accordingly, $[r]_m$ is called the standard form of $[a]_m$. For instance, the standard form of $[7]_3$ is $[1]_3$.
   Compute the standard form of $2[3]_{15} + [5]_{15} - 2\left([7]_{15} \cdot [8]_{15}\right)$.

Solution $2 \cdot \bar{3} + \bar{5} - 2\left(\bar{7} \cdot \bar{8}\right) = \bar{6} + \bar{5} - 2 \cdot \bar{56} = \bar{11} - 2 \cdot \bar{11} = -\bar{11} = \bar{4}$.

2. Use mathematical induction to prove that for every natural number n it is true that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution $P(n): \quad 1^2 + 2^2 + \ldots + n^2 = \sum_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$

Base $P(1)$: $LHS = 1^2$ and $RHS = \dfrac{1(1+1)(2+1)}{6} = 1 = LHS \checkmark$.

Step Assume $P(n)$ true, that is the Hypothesis of Induction (HI): $\sum_{i=1}^{n} i^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Prove the formula true for $n+1$: $\sum_{i=1}^{n+1} i^2 = \dfrac{(n+1)((n+1)+1)(2(n+1)+1)}{6}$.

$$RHS = \frac{(n+1)((n+1)+1)(2(n+1)+1)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

$$\begin{aligned} LHS &= \sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2 \overset{HI}{=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1)\frac{n(2n+1)+6(n+1)}{6} = (n+1)\frac{(2n^2+7n+6)}{6} \\ &= (n+1)\frac{(2n^2+4n+3n+6)}{6} = (n+1)\frac{(2n(n+2)+3(n+2))}{6} \\ &= (n+1)\frac{(n+2)(2n+3)}{6} = RHS\checkmark. \end{aligned}$$