Math 310-010 - Spring 2014 - Test 1 - Part 1

Instructor: Dr. Francesco Strazzullo My Name KEY

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.
   Compute $3[2]_{16} + [4]_{16} - 2[23]_{16} + [17]_{16}$. =

$= [6]_{16} + [4]_{16} - [46]_{16} + [1]_{16}$

$= [10]_{16} + [1]_{16} - [14]_{16}$

$= [11-14]_{16} = [-3]_{16} = [13]_{16}$

2. Use mathematical induction to prove that for every natural number n we have

$$\sum_{i=1}^{n} (2i-1) = n^2,$$

that is $1+3+5+\ldots+(2n-1) = n^2$, the sum of the first n odd integers is n^2.

$P(n)$: $1+3+\ldots+(2n-1) = n^2$

BASE: $P(1)$: $1 = 1^2$ ✓ AND $P(2)$: $1+3 = 2^2$ ✓

STEP: HYPOTHESIS OF INDUCTION: $P(n)$ TRUE. WE MUST PROVE $P(n+1)$: $1+3+\ldots+(2n-1)+(2(n+1)-1) = (n+1)^2$

LHS $= \underbrace{1+3+5+\ldots+(2n-1)}_{\text{HYP. INDUC.}} + (2n+1) = n^2+2n+1$ ($P(n)$)

RHS $= (n+1)^2 = n^2+2n+1$

LHS = RHS ✓ $P(n+1)$ IS TRUE

Math 310-010 - Spring 2014 - Test 1 - Part 2

Instructor: Dr. Francesco Strazzullo My Name Kelsey

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).

1. Use both the Euclidean algorithm and Proposition 1.2.10 (a corollary to Fundamental Theorem of Arithmetic) to compute the greatest common divisor of 49000 and 420.

Euclidean algorithm

$49000 = 420 \cdot 116 + 280$

$420 = 280 \cdot 1 + \boxed{140}$ ← GCD

$280 = 140 \cdot 2 + 0$ STOP

Proposition 1.2.10

$49000 = 7^2 \cdot 10^3$

$= 7^2 \cdot 5^3 \cdot 2^3$

$420 = 6 \cdot 7 \cdot 10$

$= 7 \cdot 5 \cdot 3 \cdot 2^2$

$GCD = 7 \cdot 5 \cdot 2^2$

$= 140$

2. Compute the addition table of $\mathbb{Z}_7$.

WRITE $[a]_7 = \bar{a}$, THEN WRITE $\bar{a} + \bar{b} = \overline{a+b}$,

LIKE $\bar{5} + \bar{3} = \overline{5+3} = \bar{8} = \bar{1}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

3. Compute the multiplication table of $\mathbb{Z}_8^*$ (called *set of units* $\mathbb{Z}_8^\times$).

$\mathbb{Z}_8^\times = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$

NOTATION AS IN #2

$\bar{a} \cdot \bar{b} = \overline{ab}$, LIKE

$\bar{4} \cdot \bar{6} = \overline{24} = \bar{0}$ (mod 8)

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

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 class.

(a) $[52]_{2197}$

NOTE: $52 = 13 \cdot 2^2$ AND $2197 = 13^3$, THUS $GCD(52, 2197) = 13 \neq 1$ AND 52 IS NOT COPRIME WITH THE MODULUS 2197. THEREFORE $[52]_{2197}$ IS A DIVISOR OF ZERO AND HAS NONE MULTIPLICATIVE INVERSE.

BY E.D.: $2197 = 52 \cdot 42 + 13$ ← GCD

$52 = 13 \cdot 4 + 0$ ← STOP

(b) $[1435]_{3952}$

USING EUCLIDEAN DIVISION:

$3952 = 1435 \cdot 2 + 1082$ (F)

$1435 = 1082 \cdot 1 + 353$ (E)

$1082 = 353 \cdot 3 + 23$ (D)

$353 = 23 \cdot 15 + 8$ (C)

$23 = 8 \cdot 2 + 7$ (B)

$8 = 7 \cdot 1 + 1$ GCD (A)

$7 = 1 \cdot 7 + 0$

THERE IS RECIPROCAL

$1 \overset{(A)}{=} 8 - 7 \overset{(B)}{=} 8 - (23 - 8 \cdot 2) = 8 \cdot 3 - 23 \overset{(C)}{=}$

$= (353 - 23 \cdot 15) \cdot 3 - 23 = 353 \cdot 3 - (45+1) \cdot 23$

$= 353 \cdot 3 - 23 \cdot 46 \overset{(D)}{=}$

$= 353 \cdot 3 - (1082 - 353 \cdot 3) \cdot 46$

$= 353 \cdot 3 \cdot 47 - 1082 \cdot 46 \overset{(E)}{=} (1435 +$

$- 1082) \cdot 3 \cdot 47 - 1082 \cdot 46 = 1435 \cdot 141 +$

$- 1082 \cdot 187 \overset{(F)}{=} 1435 \cdot 141 - (3952 +$

$- 1435 \cdot 2) \cdot 187 = 1435 \cdot 515 - 3952 \cdot 374$

THEN $\overline{515} = \overline{1435}^{-1}$.

IMPLEMENT THE PSEUDO-CODE ↔

IN EXCELL: $n = 35$ AND

$\overline{515} = \overline{1435}^{35}$

```
n=0; p=1435;
DO{a=p
   p=(a·1435)%3952; //(MOD)
   n=n+1; }
WHILE (p ≠ 1);
PRINT (a, n); // a = 1435^n = 1435^-1
```