USE YOUR IMAGINATION™

Blue Book

EXAMINATION BOOK

BOX NO. ______

NAME Key - Test 1

SUBJECT ______

CLASS M 5420 F14

SECTION ______

INSTRUCTOR ______

DATE ______

11" x 8.5" 4 LEAVES 8 PAGES

1. $(282, 114) = 6$, by

$282 = 2 \cdot 114 + 54$ Then $6 = 114 - 2 \cdot 54$

$114 = 2 \cdot 54 + 6$ $= 114 - 2(282 - 2 \cdot 114)$

$54 = 9 \cdot 6$ $= 5 \cdot 114 - 2 \cdot 282$.

2. $13 \mid 3x - 9 \iff 3x - 9 \equiv 0 \ (13)$

$\iff 3x \equiv 9 \ (13)$

$\iff 4 \cdot 3x \equiv 4 \cdot 9 \equiv -3 \ (13)$

$\iff -x \equiv -3 \ (13)$

$\iff x \equiv 3 \ (13)$

So $x = 13q + 3$ for some $q \in \mathbb{Z} \iff 13 \mid 3x - 9$

Alternatively, $13 \mid 3x - 9 \iff 13 \mid 3(x-3) \iff 13 \mid x - 3$ since $(3, 13) = 1$. So $x = 13q + 3$.

3. Solve simultaneously $x \equiv 3 \ (5)$ and $x \equiv 6 \ (7)$. The first is true iff $x = 5q + 3$ for some q. Thus we need to solve

$5q + 3 \equiv 6 \ (7)$

or $5q \equiv 3 \ (7)$

or $3 \cdot 5q \equiv 3 \cdot 3 \ (7)$

i.e. $q \equiv 2 \ (7)$.

Then $q = 7r + 2$, so $x = 5(7r+2) + 3 = 35r + 13$ for some r iff $x \equiv 3 \ (5)$ and $x \equiv 6 \ (7)$.

9:45

4. $\mathbb{Z}_{12} \xrightarrow{f} \mathbb{Z}_{12}$ by $f[x] = [7x+3]$.

2 (a) $f(f([x])) = f([7x+3]) = [7(7x+3)+3] = [49x+24]_{12} = [x]$.

4 (3) (b) Since $f \circ f = 1_{\mathbb{Z}_{12}}$, f is one-to-one (1 is one-to-one)

4 (3) (c) Since $f \circ f = 1_{\mathbb{Z}_{12}}$, f is onto (1 is onto).

brute force

9:48

5. $f : \mathbb{Q} \to \mathbb{Q}$ by "$f\left(\frac{m}{n}\right) = \frac{n-m}{n^2}$". Is this well-defined?

No: $\frac{0}{1} = \frac{0}{2}$ but $\frac{1-0}{1^2} = 1$ while $\frac{2-0}{2^2} = \frac{1}{2}$.

9:50

6. $I = \{k \in \mathbb{Z} \mid [a]_n^k = [1]_n\}$ is closed under $+/-$.

If $x, y \in I$ then $[a]^x = [1] = [a]^y$ so

$$[a]^{x+y} = [a]^x[a]^y = [1][1] = [1], \text{ and } x+y \in I$$

while

$$[a]^{x-y} = [a]^x([a]^y)^{-1} = [1]([1])^{-1} = [1][1] = [1], \text{ so } x-y \in I.$$

9:52

7. (a) Since $|\mathbb{Z}_{18}^\times| = 18\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 18\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 6$,

5/5

$$[a]_{18}^6 = [1] \text{ for all } [a]_{18} \in \mathbb{Z}_{18}^\times$$

(b) $|\mathbb{Z}_{18}^\times| = 6 = |\{1, 5, 7, 11, 13, 17\}|$

(c) $5^2 = 25 \equiv 7$ so $[5]$ generates $\mathbb{Z}_{18}^\times$.

$5^3 \equiv 35 \equiv -1 \equiv 17$ (The other generator is $[11]$.)

$5^4 \equiv -5 \equiv 13$

$5^5 \equiv -25 \equiv -7 \equiv 11$

9:56

8. Suppose $[x]_n^{10} = [1]$ and $[x_n]^7 = [1]$.

We have $(10,7) = 1$ and $1 = 7 - 2\cdot 3 = 7 - 2\cdot(10 - 1\cdot 7)$

$10 = 1\cdot 7 + 3$ $\qquad = 3\cdot 7 - 2\cdot 10.$

$7 = 2\cdot 3 + 1$

So
$$\begin{aligned} [x]_n = [x]_n^1 &= [x]_n^{3\cdot 7 - 2\cdot 10} \\ &= \left([x]^7\right)^3 \left([x]^{10}\right)^{-2} \\ &= [1]^3 [1]^{-2} \\ &= [1]. \quad // \end{aligned}$$

9:58

9. $A \neq \emptyset$, $A \xrightarrow{f} B$

$$\begin{tikzcd} & A \\ A \arrow[ur, "p_1F"] \arrow[r, "F"] \arrow[dr, "p_2F"'] & A\times B \arrow[u, "p_1"'] \arrow[d, "p_2"] \\ & B \end{tikzcd}$$

$F(a) = (a, f(a))$

$p_1(a,b) = a$

$p_2(a,b) = b$

(a) $p_1F(a) = p_1(a, f(a))$
$\qquad = a$

so $p_1F = 1_A$. (1_A)

(b) $p_2F(a) = p_2(a, f(a)) = f(a)$ so $p_2F = f$.

(c) Suppose $F(a_1) = F(a_2)$. Then $(a_1, f(a_1)) = (a_2, f(a_2))$ so $a_1 = a_2$.
OR: Since $p_1F = 1_A$ is one-to-one, F is one-to-one

(d) For any $b \in B$, pick some $a \in A$ (since $A \neq \emptyset$)
and then $p_2(a,b) = b$.
OR: $p_2F = f$ ... oops! This is no help! //

10:02