Math 3100 Test 02.

The test is due Monday July 21 before midnight. The test is open notes this includes my notes on the website. You may not receive any other outside assistance and may not discuss the test with anyone. **Please affirm at the beginning of your hand-in work that you have abided by these conditions.** (If you do not do so, you may be penalized.)

Email to me as an attachment your solutions to the problems as a pdf file with the file name beginning with your last name: e.g. LastName_test02.pdf. (If you do not do so, you may be penalized.)

Problem 1.

Use the method of the division algorithm to express the greatest common divisor $d = \gcd(70, 130)$ in the form $d = 70x + 130y$ for integers x and y.

Solution.

$$10 \quad = \quad 70(2) + 130(-1).$$

□

Problem 2.

Find integers x and y so that $1 = 36x + 101y$. Observe that this proves that 36 and 101 are relatively prime - which theorem in the notes tells us this?

Solution.

$$1 \quad = \quad 101(5) + 36(-14).$$

Theorem 4.8, 4.9 or 4.10 tells us that this means that 36 and 101 are relatively prime. □

Problem 3.

a.) Find the multiplicative inverse of $[36]_{101}$ in $\mathbb{Z}_{101}$.

Solution. From problem 2 we have,

$$1 \quad = \quad 101(5) + 36(-14).$$

This tells us that $[-14]_{101} = [87]_{101}$ is the multiplicative inverse we seek. □

b.) Argue that the function $F : \mathbb{Z}_{101} \to \mathbb{Z}_{101}$ defined by $F([x]_{101}) = [36x + 19]_{101}$ is one-to-one and onto.

Solution. Suppose $[36x + 19]_{101} = [36y + 19]_{101}$. Then,

$$\begin{aligned}
[36x + 19]_{101} &= [36y + 19]_{101} \\
[36x + 19]_{101} - [19]_{101} &= [36y + 19]_{101} - [19]_{101} \\
[36x]_{101} &= [36y]_{101} \\
[87]_{101} \cdot [36x]_{101} &= [87]_{101} \cdot [36y]_{101} \\
[87]_{101} \cdot [36]_{101} \cdot [x]_{101} &= [87]_{101} \cdot [36]_{101} \cdot [y]_{101} \\
[1]_{101} \cdot [x]_{101} &= [1]_{101} \cdot [y]_{101} \\
[x]_{101} &= [y]_{101}.
\end{aligned}$$

Therefore the function is one-to-one. Since $F : \mathbb{Z}_{101} \to \mathbb{Z}_{101}$ and $\mathbb{Z}_{101}$ is finite the function must also be onto. □

c.) For the element $[y]_{101} \in \mathbb{Z}_{101}$ find the element $[x]_{101} \in \mathbb{Z}_{101}$ that is mapped onto it by the function F of part (b).

Solution. First some scratch work:

$$\begin{aligned}
[36x + 19]_{101} &= [y]_{101} \\
[36x + 19]_{101} - [19]_{101} &= [y]_{101} - [19]_{101} = [y - 19]_{101} \\
[36x]_{101} &= [y - 19]_{101} \\
[87]_{101}[36x]_{101} &= [87]_{101}[y - 19]_{101} \\
[x]_{101} &= [87(y - 19)]_{101}.
\end{aligned}$$

Now we prove that this value is correct:

Proof.

$$\begin{aligned}
F([87(y - 19)]_{101}) &= [36(87(y - 19)) + 19]_{101} \\
&= [36(87(y - 19))]_{101} + [19]_{101} \\
&= [36 \cdot 87]_{101} \cdot [(y - 19)]_{101} + [19]_{101} \\
&= [1]_{101} \cdot [(y - 19)]_{101} + [19]_{101} \\
&= [(y - 19)]_{101} + [19]_{101} \\
&= [y]_{101} - [19]_{101} + [19]_{101} \\
&= [y]_{101}.
\end{aligned}$$

□

□

Problem 4.

Determine if the following functions are well defined. In each case, provide proofs for your conclusion:

$$\text{a.)} \quad F : \mathbb{Z}_5 \to \mathbb{Z}_{10} \quad \text{defined by } F([x]_5) = [3x+2]_{10}$$

Solution. If you try the standard technique to prove that it's well-defined, it doesn't work out; so you should suspect that it isn't well-defined. It turns out that most reasonable choices will show what we need. I chose 1 and 6.

$$\begin{aligned} 1 &\sim_5 6 \\ F([1]_5) &= [5]_{10} \\ F([1]_5) &= [20]_{10}. \end{aligned}$$

But $20 - 5 = 15$ is not divisible by 10 so the function is not well-defined. □

$$\text{b.)} \quad F : \mathbb{Z}_5 \to \mathbb{Z}_{10} \quad \text{defined by } F([x]_5) = [6x+4]_{10}$$

Solution. Suppose that $x \sim_5 y$; then $y - x = 5q$ for some integer q. So $y = x + 5q$, and we have:

$$\begin{aligned} (6y+4) - (6x+4) &= 6y - 6x \\ &= 6(x+5q) - 6x \\ &= 6x + 30q - 6x \\ &= 30q = 10(3q). \end{aligned}$$

So $(6y+4)-(6x+4)$ is divisible by 10, and so the function is well-defined. □

$$\text{c.)} \quad F : \mathbb{Z}_7 \to \mathbb{Z}_7 \quad \text{defined by } F([x]_7) = [3x^2 + x]_7.$$

Solution. Suppose that $x \sim_7 y$; then $y - x = 7q$ for some integer q. So $y = x + 7q$, and we have:

$$\begin{aligned}(3y^2 + y) - (3x^2 + x) &= (3(x + 7q)^2 + (x + 7q)) - (3x^2 + x) \\ &= 3(x + 7q)^2 - 3x^2 + 7q \\ &= 3(x^2 + 14q + 49q^2) - 3x^2 + 7q \\ &= 3 \cdot 14q + 3 \cdot 49q^2 + 7q \\ &= 7(6q + 21q^2 + q)\end{aligned}$$

So $(3y^2 + y) - (3x^2 + x)$ is divisible by 7 so the function is well-defined. □

Problem 5 a.

Suppose that we define the operation $\otimes$ on $\mathbb{Z}_{13}$ as follows:

$$[x]_{13} \otimes [y]_{13} = [7xy]_{13}.$$

Show that the operation $\otimes$ is well defined.

Solution. We assume that $x \sim_{13} a$ and $y \sim_{13} b$. So $13|(x - a)$ and $13|(y - b)$. So there are integers p and q so that $x = 13q + a$ and $y = 13p + b$. Then

$$\begin{aligned}7xy - 7ab &= 7(13q + a)(13p + b) - 7ab \\ &= 7(169qp + 13qb + 13ap + ab) - 7ab \\ &= 7(169qp + 13qb + 13ap) + 7ab - 7ab \\ &= 7(169qp + 13qb + 13ap) \\ &= 13(7 \cdot 13qp + 7qb + 7ap).\end{aligned}$$

Therefore $13|(7xy - 7ab)$, so the operation is well-defined. □

Problem 5 b.

Define the following relation on the integers:

$$x \sim y \quad \text{means that} \quad 11|(y + 10x).$$

Show that $\sim$ is an equivalence relation.

Solution. (1) Reflexive.

$$x + 10x = 11x.$$

Therefore $11|(x + 10x)$, so $x \sim x$.

(2) Symmetric.
Suppose $x \sim y$ then $11|(y + 10x)$ and there is an integer q so that $y + 10x = 11q$. Then we have $y = 11q - 10x$. So:

$$\begin{aligned} x + 10y &= x + 10(11q - 10x) \\ &= x + 110q - 100x) \\ &= 110q - 99x) \\ &= 11(10q - 9x). \end{aligned}$$

Therefore $11|(x + 10y)$, so $y \sim x$.

(3) Transitive.
Suppose $x \sim y$ and $y \sim z$ then $11|(y + 10x)$ and $11|(z + 10y)$ there are integers q and p so that $y + 10x = 11q$ and $z + 10y = 11p$. Then we have $y = 11q - 10x$ and $z = 11p - 10y$. So:

$$\begin{aligned} z + 10x &= 11p - 10y + 10x \\ &= 11p - 10(11q - 10x) + 10x \\ &= 11p - 110q + 100x + 10x \\ &= 11p - 110q + 110x \\ &= 11(p - 10q + 10x). \end{aligned}$$

Therefore $11|(z + 10x)$, so $x \sim z$. □

Problem 6.
Let $H = \{11n \mid n \in \mathbb{Z}\}$.
a.) Show that $(H, +)$ is a group (in other words, show that H with the usual addition of integers is a group).

Solution. (1. Associativity.) Since H is a subset of $\mathbb{Z}$ and we are using the same operation, the we have associativity.

(2. Closure.) If $x \in H$ and $y \in H$ then there are integers n_1 and n_2 so that $x = 11n_1$ and $y = 11n_2$. Then

$$\begin{aligned} x + y &= 11n_1 + 11n_2 \\ &= 11(n_1 + n_2). \end{aligned}$$

So $x + y \in H$ and we have closure.

(3. Identity.) If $h \in H$ then $h + 0 = h$ so 0 is the identity. Since $0 = 11 \cdot 0$ it follows that $0 \in H$. By commutativity of the integers $0 + h = h + 0 = h$. So H has an identity (namely $0 = 11 \cdot 0$).

(4. Inverse.) If $h \in H$ then $h = 11n$ for some $n \in \mathbb{Z}$. But then $-n \in \mathbb{Z}$ and so $11(-n) \in H$. And we have $h + 11(-n) = 11n + 11(-n) = 11n - 11n = 0$. By commutativity of the integers $11(-n) + h = h + 11(-n) = 0$. So each element has an inverse.

By conditions 1-4 the set H satisfies the condition to being a group.

□

b.) Consider the function $f(x) : \mathbb{Z} \to H$ defined by $f(x) = 11x$.

i.) Is f one-to-one? Why?

Solution. Yes. Suppose $f(x) = f(y)$

$$\begin{aligned} f(x) &= f(y) \\ 11x &= 11y \\ x &= y. \end{aligned}$$

where the last step follows from the fact that $11 \neq 0$ and we can use the cancellation property of the integers. □

ii.) Is f onto? Why?

Solution. Yes. Suppose $y \in H$. Then $y = 11n$ for some $n \in \mathbb{Z}$. Then pick $x = n$, and we have:

$$\begin{aligned} f(x) &= 11x \\ &= 11n \\ &= y. \end{aligned}$$

So the function is onto. □

c.) Show that $f(x+y) = f(x) + f(y)$.

Solution.

$$\begin{aligned} f(x+y) &= 11(x+y) \\ &= 11x + 11y \\ &= f(x) + f(y). \end{aligned}$$

□

d.) Define the relation $\sim$ on $\mathbb{Z}$ by $x \sim y$ if and only if $y - x \in H$. Show that $\sim$ is an equivalence relation.

Solution. (1) Reflexive. If x in $\mathbb{Z}$ then,

$$x - x = 0 \in H.$$

Therefore $x \sim x$.

(2) Symmetric.
Suppose $x \sim y$ then $y - x \in H$. Since H is a group, the inverse of $y - x$ is in H. So,

$$\begin{aligned} -(y-x) &\in H \\ -y + x &\in H \\ x - y &\in H. \end{aligned}$$

Therefore $y \sim x$.

(3) Transitive.
Suppose $x \sim y$ and $y \sim z$ then $y - x \in H$ and $z - y \in H$. Since $(H, +)$ is a group $(y - x) + (z - y) \in H$. So $z - x \in H$. $x \sim z$. □

Problem 7.

Suppose that G is an arbitrary group. Prove the following statements about G. Make sure to state the reasoning for each step.

Solution. Since a group is associative I will assume that abc means $(ab)c$ or $a(bc)$; since they are equal it doesn't make any difference which interpretation is assumed.

a.) Given $x, y, z \in G$. Then

$$(xyz)^{-1} = z^{-1}y^{-1}x^{-1}.$$

Solution.

$$\begin{array}{rcll}
(xyz)^{-1}(xyz) & = & e & \text{definition of inverse} \\
(xyz)^{-1}xyzz^{-1} & = & ez^{-1} & \text{closure} \\
(xyz)^{-1}xye & = & ez^{-1} & \text{def. of inverse} \\
(xyz)^{-1}xy & = & z^{-1} & \text{identity} \\
(xyz)^{-1}xyy^{-1} & = & z^{-1}y^{-1} & \text{closure} \\
(xyz)^{-1}xe & = & z^{-1}y^{-1} & \text{def. of inverse} \\
(xyz)^{-1}x & = & z^{-1}y^{-1} & \text{identity} \\
(xyz)^{-1}xx^{-1} & = & z^{-1}y^{-1}x^{-1} & \text{closure} \\
(xyz)^{-1}e & = & z^{-1}y^{-1}x^{-1} & \text{def. of inverse} \\
(xyz)^{-1} & = & z^{-1}y^{-1}x^{-1} & \text{identity.}
\end{array}$$

□

b.) If e is the identity element of G. Then

$$e^{-1} = e.$$

Solution.

$$\begin{array}{rcll}
e^{-1}e & = & e & \text{definition of inverse} \\
e^{-1}e & = & e^{-1} & \text{identity} \\
e & = & e^{-1} & \text{trancsitity property of } =.
\end{array}$$

□

c.) If $x \in G$ then x^2 is defined to be the element $x \cdot x$. Then show that

$$\left(x^{-1}\right)^2 = \left(x^2\right)^{-1}.$$

$$\begin{array}{rcll}
\left(x^{-1}\right)^2x^2 & = & x^{-1}x^{-1}xx & \text{definition of notation} \\
\left(x^{-1}\right)^2x^2 & = & x^{-1}ex & \text{def. of inverse} \\
\left(x^{-1}\right)^2x^2 & = & x^{-1}x & \text{identity} \\
\left(x^{-1}\right)^2x^2 & = & e & \text{def. of inverse} \\
\left(x^{-1}\right)^2x^2\left(x^2\right)^{-1} & = & e\left(x^2\right)^{-1} & \text{closure} \\
\left(x^{-1}\right)^2e & = & e\left(x^2\right)^{-1} & \text{closure} \\
\left(x^{-1}\right)^2 & = & \left(x^2\right)^{-1} & \text{identity.}
\end{array}$$

□