Math 021 Fundamentals of Math Fall 2005 Worksheet IV Name:_____
(please print legibly)

MODULAR ARITHMETIC.

As discussed in the previous section, we count in other ways besides just base ten. The illustration that I alluded to was time, weight, distance, etc. that we in the United States follow rather than as most humans where they have acclimated to a decimal system for all but time. Nonetheless, there is something really odd about our system. Think about the following: Start with 1 minim. After a while we get 60 minims which is one dram. Later we finally have 8 drams which is an ounce. Sixteen ounces and we have a pint. Two pints and we have a quart. Four quarts and we have a gallon, and so for and so on.

What of drams, ounces, pounds, tons, etc. not to mention inches, feet, yards, miles, etc.? Why measure time as 60 seconds for one minute, sixty minutes for an hour, but twenty-four hours for a day; and more preposterous months with 28, 29, 30, or 31 days but there are twelve of them so a year has 365, 366, or 367 days?[1]

Well, it is convention and sometimes ten is not always the best under any and all circumstances, eh? So, what of these systems? They illustrate modular arithmetic (some with changes in the place values). Consider 11 + 5 = 4. Note it is nonsense since the universe was not defined and it leads on to assume it is referencing real arithmetic. We are *not* in the business to play games and attempt to fool others, each other, or ourselves.

So, let us define modular arithmetic as follows. Let $U = \mathbb{N}^*_p$ and $D = \mathbb{N}^*_{(p-1)}$ Where $p \in \mathbb{N}$.

Let $a \in D$ and $b \in D$. Let $a +_p b$ be $z \in D$ where z is the remainder from the division of p into (a + b) under ordinary addition for the natural numbers.

So, for example let us see what $+_4$ is. $0 +_4 0 = 0$, $0 +_4 1 = 1$, $0 +_4 2 = 2$, $0 +_4 3 = 3$, $1 +_4 0 = 0$, $2 +_4 0 = 2$, $3 +_4 0 = 3$ all because 4 divided into any of these is zero with remainder whatever the non-zero constant was. Consider $1 +_4 1 = 2$, $2 +_4 1 = 3$, $1 +_4 2 = 3$ for the same reasons.

So, we are left with the other possibilities:

$1 +_4 3 = 0$ since $4 \div 4 = 1$ with remainder 0.
$2 +_4 2 = 0$ since $4 \div 4 = 1$ with remainder 0.
$2 +_4 3 = 1$ since $5 \div 4 = 1$ with remainder 1.
$3 +_4 2 = 1$ since $5 \div 4 = 1$ with remainder 1.
$3 +_4 3 = 2$ since $6 \div 4 = 1$ with remainder 2.

Note that this is all good and well but it can be confusing. So, let us note the results in tabular form:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

This should look strikingly familiar (see the text).

[1] Check this out – hint: years ending with '00' but not divisible by 400.

You should be comfortable with defining the same for other mods (modular arithmetic operations with some natural number) such as:

$+_3$	0	1	2
0	0	1	2
1	1	2	3
2	2	3	0

and:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

We can also define modular multiplication: Let $U = \mathbb{N}_p^*$ for some $p \in \mathbb{N}$.

Let $a \in \mathbb{N}_p^*$ and $b \in \mathbb{N}_p^*$. Let $a \times_p b$ be $z \in \mathbb{N}_p^*$ where z is the remainder from the division of p into $(a \times b)$ under ordinary multiplication for the natural numbers. Do the arithmetic in your head for mod 4 multiplication to get the following:

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Now reconsider 11 + 5 = 4. Recall we are *not* in the business to play 'games.'
Consider $+_{12}$. Note it is fine to consider $U = \mathbb{N}_{12}^*$ and let the set of digits be $\mathbb{N}_{11}^*$.
$11 +_{12} 5 = 4$ is understandable from the applied problem of 11 a.m. and 5 hours is 4 p.m. (5 hours after 11 a.m. is 4 p.m.). Notice we do not use the universe $D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, T, E\}$ as with base arithmetic. Also, note that commutativity and associativity hold.

Now, does there exist a distributive property of modular multiplication over modular addition? If so, how would you prove it; if not, can you devise a counterexample?

It is perfectly acceptable to define a system of modular arithmetic that includes $p \in \mathbb{N}$ for $U = \mathbb{N}_p^*$ as with time. Hence, in modular 12 arithmetic, $7 +_{12} 5 = 0$ but in practical applications most would say it is 12 Since $12 \Leftrightarrow 0$ in the sense of time (in hours). Once again defining the domain of discourse for the discussion (logic) and noting the universe (sets) is paramount to clearly and objectively investigating, understanding, and applying the mathematical system.

§ 3.5 EXERCISES.

1. Construct the table for addition and multiplication mod 5.

2. Construct the table for addition and multiplication mod 8.

3. Calculate the following

A.	$8 +_9 1 +_9 3$	G.	$7 +_9 7 +_9 7$	N.	$7 +_8 5 +_8 6$
B.	$8 \times_9 1 \times_9 3$	H.	$7 \times_9 7 \times_9 7$	O.	$6 +_8 5 +_8 7$
C.	$1 +_2 1 +_2 1$	I.	$7 +_8 7 +_8 7$	N.	$(7 +_8 5) +_8 6$
D.	$0 \times_2 1 \times_2 1$	J.	$7 \times_8 7 \times_8 7$	O.	$5 \times_8 7 \times_8 6$
E.	$4 +_5 3 +_5 1$	K.	$3 +_5 3 +_5 1$	N.	$5 +_{12} 5 +_{12} 5$
F.	$4 \times_5 3 \times_5 1$	L.	$4 \times_5 3 \times_5 3$	O.	$5 \times_8 6 \times_8 7$

4. What is incorrect (if anything) about the following claims?

A. $9 \times_8 7 = 7 \times_8 9$ B. $2 \times_8 7 = 7 \times_8 2$ C. $11 +_2 10 = 10 +_2 11$

5. Compute the following:

A.	$813_{(9)} + 712_{(9)}$	I.	$110101_{(2)} + 1111_{(2)}$	Q.	$1101_{(2)} \times 1001_{(2)}$
B.	$8 +_9 7$	J.	$1 +_{12} 1$	R.	$1 \times_2 1$
C.	$1 +_9 1$	K.	$3 +_6 1$	S.	$8 \times_9 7$
D.	$103_{(4)} \times 212_{(4)}$	L.	$3 +_6 3$	T.	$3 \times_9 2$
E.	$11 +_{12} 9$	M.	$3 \times_6 3$	U.	$10 \times_{12} 11$
F.	$8 +_{12} 7$	N.	$3 \times_6 5$	V.	$11 \times_{60} 30$
G.	$8 +_{60} 7$	O.	$3 \times_{60} 5$	W.	$21 \times_{60} 35$
H.	$38 +_{60} 47$	P.	$48 +_{60} 47$	X.	$58 +_{60} 47$

6. Compare the results of exercise 5 with exercise 7 of worksheet 3. What patterns (if any) exist and can they be explained or an hypothesis formed as to the relationship between modular arithmetic and arithmetic of natural numbers in different bases?