CHAPTER TWENTY-THREE

MODULAR ARITHMETIC

INTRODUCTION

What everyday way of thinking – familiar to each and every person on this planet (well, almost) – makes the following seemingly bizarre system of arithmetic absolutely meaningful and correct?

$3 + 4 = 7$	$5 + 6 = 11$
$6 + 8 = 2$	$8 + 10 = 6$
$9 + 4 = 1$	$9 + 10 = 7$
$10 + 10 = 8$	$2 + 9 = 11$
$3x5 = 5 + 5 + 5 = 3$	
$10x2 = 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 + 2 = 8$	
$5^2 = 1$	

Seriously think about this before reading on.

Can you correctly determine the answers to the following:

$$2 + 3 = ?$$
$$8 + 11 = ?$$
$$7 + 8 + 2 = ?$$
$$3 \times 7 = ?$$
$$5 \times 10 = ?$$

CURRICULUM CONNECTIONS
Modular arithmetic; Divisibility; Primes; Rings; Fields

ANSWER: We're looking at a clock!

If it is 3 o'clock and we wait 4 hours it will be 7 o'clock: $3+4=7$.

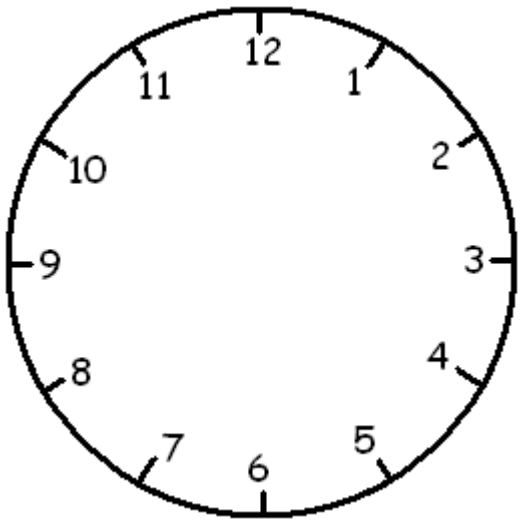
If it is 6 o'clock and we wait 8 hours it will be 2 o'clock: $6+8=2$.

If it is 9 o'clock and we wait 4 hours, it will be 1 o'clock: $9+4=1$.

and so on. As multiplication is repeated addition we can interpret $3\times 5=5+5+5$ as …

> If, starting at 5 o'clock, we wait 5 hours and then another 5 hours the time after this wait will be 3 o'clock: $3\times 5=3$

Can you now see that $5^2=5+5+5+5+5=1$?



In this system of clock-arithmetic, the number 12 behaves as zero:

If it is 3 o'clock and we wait 12 hours it will be 3 o'clock: 3 + 12 = 3.
If it is 7 o'clock and we wait 12 hours it will be 7 o'clock: 7 + 12 = 7.

It is convenient to deem the number 12 as equivalent to zero. We write:

$$12 \equiv 0 .$$

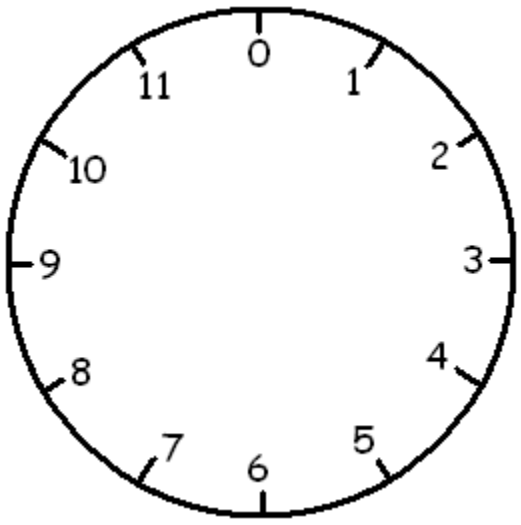
Doing this helps clarify the arithmetic of "12-clock math":

$$20 = 12 + 8 \equiv 0 + 8 = 8$$
$$50 = 12 + 12 + 12 + 12 + 2 \equiv 0 + 0 + 0 + 0 + 2 = 2$$

$$11 + 8 = 19 = 12 + 7 \quad \equiv \quad 0 + 7 = 7$$

$$3 \times 10 = 30 = 12 + 12 + 6 \equiv 6$$

$$7^2 = 49 = 48 + 1 \equiv 1$$



In 12-clock math one need only ever work with the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 and 11.

EXERCISE:

a) Complete the addition table for 12-clock math:

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3												
4												
5												
6												
7												
8												
9												
10												
11												

[This table isn't very exciting!]

b) Draw a multiplication table for 12-clock math.
[This is much more interesting.]

What number deserves to be called -3 in clock math?

There are at least three ways to think of this:

Answer 1: The number -3 is three units below zero. On the clock, the position three units to the left of zero is 9. Thus $-3 \equiv 9$.

Answer 2: In ordinary arithmetic, -3 is a number, which, when added to three, gives zero. Thus, in clock math we seek a number x such that $x + 3 = 0$. One sees that 9 does the trick. So $-3 \equiv 9$.

Answer 3: $-3 = -3 + 0 \equiv -3 + 12 = 9$. □

EXERCISE: What is -1000 in 12-clock math?

Consider the multiplication table for 12-clock math you computed on the previous page:

X	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

According to this table …

What is the square root of 9?

Answer: We see that there are two numbers *x* such that $x \times x = 9$, namely 3 and 9. Thus $\sqrt{9} = 3$ or 9. (Two square roots as expected, namely 3 and -3!) □

What is the square root of 4?

Answer: Looking at the table we see: $\sqrt{4} = 2$ or 4 or 8 or 10. (There are four square roots of four!) □

What is the square root of 1?

Answer: Your turn … $\sqrt{1}$ = ??

What is the square root of 10?

Answer: From the table we see that there is no square root of ten in 12-clock math.

What number in 12-clock math deserves to be called $\frac{2}{5}$?

Answer: In ordinary arithmetic, $\frac{2}{5}$ is a number, which, when multiplied by 5 gives the answer 2. According to the multiplication table, is there a number which when multiplied by 5 gives the answer 2? Yes! Looking at the fifth row we see that 10 does the trick: $10 \times 5 = 2$. Thus: $\frac{2}{5} \equiv 10$. □

What number deserves to be called $\frac{6}{7}$?

Answer: Your turn!

What number deserves to be called $\frac{1}{3}$?

Answer: This is troublesome. There is no number in 12-clock math which, when multiplied by three, gives the answer 1. The fraction $\frac{1}{3}$ does not exist! □

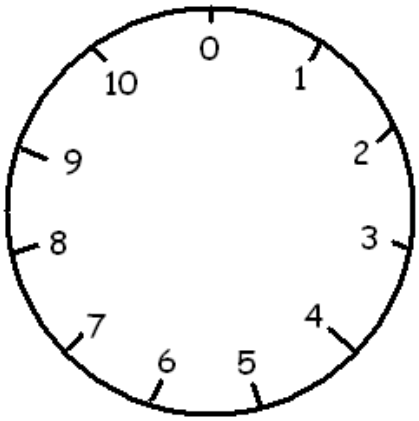
EXERCISE:
Which of the following fractions exist in 12-clock math?

$$\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}, \frac{1}{10}, \frac{1}{11}$$

Any patterns?

The fact that not all numbers 1, 2, …, 11 can be inverted in 12-clock math (that is, not all the fractions $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \frac{1}{8}, \frac{1}{9}, \frac{1}{10}, \frac{1}{11}$ exist) is a deficiency of the system. But we need not stick with the number 12 to play this arithmetic game.

Consider a clock with just 11 hours. In 11-clock math the number 11 is deemed equivalent to zero, $11 \equiv 0$, and the system of arithmetic obtained produces the following multiplication table:



X	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

We see that each and every number 0, 1, …, 10 appears in each and every (non-zero) row of the multiplication table. This means all "fractions" exist in 11-clock math.

EXERCISE: Draw multiplication tables for 4-clock, 5-clock, 6-clock, 7-clock, and 8-clock math. Which tables have each number appearing in each and every non-zero row? Do you have a conjecture?

Does you conjecture hold for 2-clock math and 3-clock math? How about 9-clock math?

Seriously play (or at least think) about this before reading on.

After playing with different examples of clock math one comes to realize the following:

Suppose we are working within N-clock math where N is a composite number: $N = ab$. Then some rows in the multiplication table for N will possess repeat entries.

Why? Because if $N = ab$ then the a-th row of the multiplication table will, at the very least, repeat the number zero since $a \times 0 = 0$ and $a \times b = 0$. There is not enough room then for all numbers to appear on that row.

This suggests:

Working with *p*-clock math, with *p* a prime, might be good. That is, all numbers might appear on each and every row of a mod p multiplication table.

This turns out to be true:

THEOREM: If *p* is prime, then no row (beyond the row that is identically zero) of the multiplication table for p-clock arithmetic repeats an entry. Thus each and every number appears and each and every row, and all "fractions" exist in p-clock arithmetic.

PROOF: Is it possible for a number to be repeated on, say, the *a*-th row of the multiplication table, beyond the zero-th row? That is, do we ever have: $a \times b_1 = a \times b_2$ for a non-zero *a* for two different values b_1 and b_2? (Note that the numbers here, a, b_1, b_2 are all between 0 and p-1, with *a* non-zero and b_1 and b_2 distinct.)

If $ab_1 = ab_2$ then $a(b_1 - b_2) = 0$ in the *p*-clock arithmetic system. This means that $a(b_1 - b_2)$ is a multiple of *p* in ordinary arithmetic. (Why?) By the key property of primes, either *a* is a multiple of *p* or $b_1 - b_2$ is a multiple of *p*. Since *a* is non-zero and smaller than *p* it is not. Thus $b_1 - b_2$ must be. But this means $b_1 = b_2$ in the *p*-clock system. Oops! Thus the situation $a \times b_1 = a \times b_2$ cannot happen if b_1 and b_2 are meant to be different values. □

EXERCISE: Let *p* be prime.

a) Show that "$\frac{1}{p-1}$" equals $p-1$ in *p*-clock math.

b) Prove that if $a^2 = 1$ in *p*-clock math, then $a = 1$ or $a = p-1$.

The second part of this question establishes that the only elements of *p*-clock math that are *self-inverse* (meaning that $\frac{1}{a} = a$) are 1 and $p-1$. Thus all other inverses come in distinct pairs.

For example, in 7-clock math we have:

$$\frac{1}{1} = 1$$
$$\frac{1}{2} = 4 \text{ and } \frac{1}{4} = 2 \text{ (because } 2 \cdot 4 = 1\text{)}$$
$$\frac{1}{3} = 5 \text{ and } \frac{1}{5} = 3 \text{ (because } 3 \cdot 5 = 1\text{)}$$
$$\frac{1}{6} = 6$$

Thus the product $6! = 6 \times 5 \times 4 \times 3 \times 2 \times 1 = 6 \times (2 \times 4) \times (3 \times 5) \times 1 \equiv 6 \times 1 \times 1 \times 1 \equiv -1$

In general:

WILSON'S THEOREM: For *p* prime we have:

$$(p-1)! \equiv -1$$

in *p*-clock arithmetic.

FERMAT'S LITTLE THEOREM

Prime clocks are "good": Every number appears in every row (except the zeroth row) of its multiplication table.

This means that the numbers in the *a*-th row (for $a \neq 0$), that is, the multiples of *a:*

$$a \cdot 1,\ a \cdot 2,\ a \cdot 3,\ \ \ldots, a \cdot (p-1)$$

are just the numbers 1, 2, 3, …, (p-1) rearranged in some order.

Let's multiply the two lists together. Since they are the same numbers (just in different orders) the two products must be the same:

$$a \cdot 1 \cdot a \cdot 2 \cdot a \cdot 3 \cdot \cdots \cdot a \cdot (p-1) = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$$

Rewriting:

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1)$$

Now … **EVERY FRACTION EXISTS IN PRIME CLOCKS,** which means we can multiply both sides by $\frac{1}{2}$ and by $\frac{1}{3}$ and by $\frac{1}{4}$ and so forth to establish:

$$a^{p-1} \equiv 1$$

in *p*-clock arithmetic.

This curious result is called Fermat's Little Theorem.

EXERCISE: a) Check that each of $1^4, 2^4, 3^4$ and 4^4 each leave a remainder of one when divided by five.
b) What are the values of $1^5, 2^5, 3^5, 4^5$ and 5^5 in 6-clock math?

THE JARGON AND THE FORMAL NOTATION

Mathematicians call a system of arithmetic for which a number *n* is deemed equivalent to zero *arithmetic modulo n*. If two numbers *a* and *b* are equivalent in this system, we write:

$$a \equiv b \pmod{n}$$

and say "*a* is *congruent* to *b* mod *n*."

For example, in "mod 12" arithmetic (that is, our 12-clock math) we have:

$$12 \equiv 0 \pmod{12}$$
$$15 \equiv 3 \pmod{12}$$
$$-3 \equiv 9 \pmod{12}$$

We also have:

$$65 \equiv 41 \pmod{12}$$

because $65 = 41 + 2 \times 12$ and twelve is equivalent to zero.

EXERCISE:

a) Explain the following: $a \equiv b \pmod{12}$ means $a - b$ is a multiple of 12.

b) Explain: $a \equiv b \pmod{n}$ means $n \mid (a - b)$

c) Explain: $a \equiv b \pmod{n}$ means *a* and *b* leave the same remainder when divided by *n*.

d) Explain: $a \equiv b \pmod{n}$ means $a = b + xn$ for some integer *x*.

COMMENT: Some texts in number theory use part b) or perhaps part c) or part d) as the first definition of modular arithmetic. Make sure you understand that these definitions really are equivalent.

EXERCISE: Explain the following:

a) Every number N is equivalent to its final digit mod 10.
b) Odd numbers are $\equiv 1 (\mathrm{mod}\, 2)$
c) Every number is congruent to its sum of digits mod 3.
d) Every fourth number is congruent to 3 mod 4.

In congruence notation we have:

WILSON'S THEOREM:
For *p* prime: $(p-1)! \equiv -1 \pmod{p}$

FERMAT'S LITTLE THEOREM:
For *p* prime: $a^{p-1} \equiv 1 \pmod{p}$ for $a = 1, 2, 3, \ldots, p-1$.

We've also established that all "fractions" exist in mod *p* arithmetic:

THEOREM: If *p* is prime and *a* is one of the numbers 1, 2, …, $p-1$, then the *inverse* a^{-1} exists mod *p*. That is, there is a number *c* such that $ca \equiv 1 (\mathrm{mod}\, p)$.

EXERCISE: Find 13^{-1} mod 17.

When you do, find a number *x* so that $13x \equiv 5 (\mathrm{mod}\, 17)$.

There are a number of basic properties of modular arithmetic one should confirm:

THEOREM: If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then one can add congruences to obtain:

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$$

One can also multiply congruences to obtain:

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$$

PROOF: Now $a_1 \equiv a_2 \pmod{n}$ means that a_1 and a_2 differ by a multiple of *n*, that is, $a_1 = a_2 + xn$ for some number *x*. Also, $b_1 \equiv b_2 \pmod{n}$ means $b_1 = b_2 + yn$ for some number *y*. Then:

$$a_1 + b_1 = a_2 + b_2 + xn + yn = a_2 + b_2 + (x + y)n$$

and so $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.

Also:

$$a_1 \cdot b_1 = (a_2 + xn)(b_2 + yn) = a_2 b_2 + \left(xb_2 + ya_2 + xyn\right)n$$

and so $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$. □

EXERCISE: If $a_1 \equiv a_2 \pmod{n}$ prove that $ka_1 \equiv ka_2 \pmod{n}$ for any number *k*.

For example, since $17 \equiv 5 \pmod{12}$ and $122 \equiv 2 \pmod{12}$ it must be true that $17 \times 122 = 2074$ is congruent to $5 \times 2 = 10$ mod 12. (Thus 2064 must be a multiple of 12. Is it?)

Another example: Since $316 \equiv 1 \pmod{9}$ (why?) we have that $316^{7002} \equiv 1^{7002} = 1 \pmod{9}$.

EXAMPLE: Compute 3^{75} mod 60

ANSWER: One has to build this up in stages.

Now $3^2 = 9, 3^3 = 27$ and $3^4 = 81 \equiv 21 (\text{mod}\, 60)$. So $3^5 \equiv 3 \times 21 = 63 \equiv 3 (\text{mod}\, 60)$.

Thus $3^{25} = \left(3^5\right)^5 \equiv 3^5 \equiv 3 \pmod{60}$.

So $3^{75} = \left(3^{25}\right)^3 = 3^3 = 27 (\text{mod}\, 60)$. □

EXAMPLE: Compute $1700^{90} (\text{mod}\, 31)$

ANSWER: Now $1700^{90} = \left(1700^3\right)^{30}$. And since, by Fermat's Little Theorem (using the fact that 31 is prime) we have $a^{30} \equiv 1 (\text{mod}\, 31)$ for any number *a* that is not zero, we have:

$$1700^{90} \equiv \left(1700^3\right)^{30} = 1 (\text{mod}\, 31).$$ □

EXAMPLE: Show that no non-zero integers *a*, *b* and *c* satisfy:

$$10^a + 4^b = 2c^2$$

ANSWER: Out of thin air … let's work $\text{mod}\, 5$.

Now $10 \equiv 0 (\text{mod}\, 5)$ so $10^a \equiv 0 \pmod{5}$.
$4 \equiv -1 (\text{mod}\, 5)$ so $4^b \equiv \pm 1 \pmod{5}$

Thus

$$10^a + 4^b \equiv \pm 1 (\text{mod}\, 5).$$

Now *c* is either 0, 1, 2, 3, or 4 $\text{mod}\, 5$, and so $2c^2$ is congruent to either 0, 2, 3, 3, or 2 $\text{mod}\, 5$, and never ± 1. □

COMMENT: There is nothing in the problem to suggest that working mod 5 will do the trick. Choosing this number was a matter of trial and error.

EXERCISE:

a) Prove, that for any number *n*, we have $n^2 \equiv 0 \text{ or } 1 \pmod 4$

b) Prove that there are no odd integers *a* and *b* so that $a^2 + b^2$ is a square number.

c) Prove that for any Pythagorean triple (a,b,c), that is, a set of integers satisfying $a^2 + b^2 = c^2$, at least one of *a*, *b* or *c* must be a multiple of 5.

d) Find an example of four positive integers that satisfy the relation $a^2 + b^2 + c^2 = d^2$.

e) Prove that for any set of positive integers satisfying $a^2 + b^2 + c^2 = d^2$ at least one of those integers must be a multiple of three. Also prove that at least two of the integers are even.

PSEUDO-PRIMES

Fermat's Little Theorem gives a test for whether or not a number is prime.

For example, suppose one suspects that 6 is prime. Then Fermat's Little Theorem insists that $a^5 \equiv 1 (\mathrm{mod}\, 6)$ for any number *a* between 1 and 5. Let's choose a number, say $a = 2$. We have:

$$2^5 = 32 \equiv 2 \ (\mathrm{mod}\, 6)$$

OOPS! This not 1. This means that 6 is not prime!

A prime number *p* will pass Fermat's test for all values *a* between 1 and p-1. However, some numbers can pass the test without being prime. For example, it turns out that $7^{24} \equiv 1 (\mathrm{mod}\, 25)$ even though 25 is not prime.

Definition: A composite number *n* is called *pseudoprime to base* $a \neq 1$ if $a^{n-1} \equiv 1 \ (\mathrm{mod}\, n)$.

For example,

$7^{24} \equiv 1 (\mathrm{mod}\, 25)$ so 25 is pseudoprime to base 7.

$2^{340} \equiv 1 (\mathrm{mod}\, 341)$ but $341 = 11 \times 31$. So 341 is pseudoprime to base 2.

Exercise:

a) Use the fact that $7^2 \equiv -1 (\mathrm{mod}\, 25)$ to verify that $7^{24} \equiv 1 (\mathrm{mod}\, 25)$.

b) Prove that $2^{340} \equiv 1 (\mathrm{mod}\, 341)$

If, however, for a fixed number *n* more and more values *a* are found for which $a^{n-1} \equiv 1 \ (\mathrm{mod}\, n)$, then this would be deemed accumulating evidence for *n* actually being prime.

Still warnings are to be had. For example, the number 561 = 3 x 11 x 17 satisfies $a^{560} \equiv 1 (\mathrm{mod}\, 561)$ for over half the different values of *a* between 1 and 560. (In fact for any *a* that is not a multiple of 3, 11, or 17.)

OPTIONAL EXERCISE: a) Find a website that allows you to enter a number and determine whether or not that number is prime. Is your phone number prime? Is your birth year prime? Find a large number meaningful in your life that is prime.

b) Is there any information on the website explaining whether or not the site is determining <u>for certain</u> that a given number is prime or is highly likely to be prime (meaning that it passes Fermat's test, or an equivalent test, a large number of times)?

EXERCISES

Question 1: a) Show that $3^{40,000}$ is congruent to 1 mod 10.
b) Compute the final digit of 13^{100}

Question 2: Find an efficient way to compute $2^{90} \pmod{91}$. Is 91 prime?

Question 3: Working mod 10 prove that no square number ends in an 8.

Question 4: Prove that no number that is a sum of two fourth powers ends in 3, 4, 8, or 9.

Question 5: By working mod 3 quickly explain why there are no integer solutions to the equation $21x + 15y = 77$.

Question 6: By working mod 8 …

a) Prove that there are no integers *a*, *b*, and *c* that satisfy:

$$a^2 + b^2 = 8c^2 + 11$$

b) Show that a number of the form $5^a + 3^a + 3$ is never a perfect square.

c) Prove that $8 \mid (n^{200} - 1)$ if *n* is odd.

Question 7: Suppose $\gcd(a, N) = 1$. Recall that the Euclidean algorithm shows that we can find numbers *x* and *y* so that $ax + yN = 1$.

a) Explain why a^{-1} exists mod N if $\gcd(a, N) = 1$.
b) List all the values *a* for which a^{-1} exists mod 12.
c) List all the values *a* for which a^{-1} exists mod 20.
d) Suppose $\gcd(a, N) = 1$. If $ar \equiv as \pmod{N}$ must $r \equiv s \pmod{N}$?
e) If $3r \equiv 3s \pmod{12}$ must $r \equiv s \pmod{12}$?
f) If $4r \equiv 4s \pmod{10}$ must $r \equiv s \pmod{10}$?
g) If $5r \equiv 5s \pmod{14}$ must $r \equiv s \pmod{14}$?

Question 8: Suppose $\gcd(a, N) = 1$. Prove that the *a*-th row of the multiplication table for *N*-clock math contains no repeat entries.

Question 9: Wilson's theorem states that if *p* is prime then $(p-1)! \equiv -1 \pmod{p}$.

Let's consider the corresponding congruence for numbers that are not prime:

a) Compute each of the following:

$3! \pmod{4}$
$5! \pmod{6}$
$7! \pmod{8}$
$8! \pmod{9}$
$9! \pmod{10}$
$11! \pmod{12}$
$99! \pmod{100}$
$7657909865871! \pmod{7657909865872}$

b) Make a conjecture about the value of $(n-1)! \pmod{n}$ for *n* a composite number.
c) Prove your conjecture.

Question 10:
a) Find a number $a \neq 1 \pmod{15}$ such that 15 is a pseudoprime base *a.*
b) Is 8 is a pseudoprime for some base?

Question 11:

a) Ten cups are placed upright in a circle. Jenny turns over every third cup, going around the circle multiple times. She stops when she first encounters a cup she has already turned over. How many cups are left upright when this occurs?
b) Twenty-two cups are placed upright in a circle. Sheena turns over every fifth cup and stop when she first encounters a cup already turned over. How many cups are left upright?
c) Twenty-seven cups are placed upright in a circle. Ava turns over every sixth cup and stops when she first encounters a cup already turned over. How many cups are left upright?
d) N cups are placed upright in a circle. Jay turns over every a-th cup and does so until he first encounters a cup already upside down. What must be true about a and N for every cup to be touched? Prove any claims you make.

HINT: Question 8.

Question 12:
Question five of chapter 10 showed that there is a number *x* between 0 and 59 that satisfies:

$$x \equiv 4 \pmod 5$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 2 \pmod 3$$

Prove that following general result:

Suppose that a, b, and c are three positive integers sharing no common prime factors (meaning that $\gcd(a,b)=1$, $\gcd(a,c)=1$ *and* $\gcd(b,c)=1$*) and suppose* r_1, r_2 *and* r_3 *are three given positive integers. Then there is a value x between 0 and* $abc-1$ *satisfying:*

$$x \equiv r_1 \pmod a$$
$$x \equiv r_2 \pmod b$$
$$x \equiv r_3 \pmod c$$

COMMENT: This result generalizes to more than three given "relatively prime" integers *a*, *b* and *c*. The general result is known as the Chinese Remainder Theorem.