1 Division

We know how to do many things with these numbers: add, subtract, multiply and divide. However, when we divide we may write it differently here:

$$3\overline{)23} \quad \begin{matrix} 7 & \text{R } 2 \end{matrix}$$

will be written as $23 = 3 \cdot 7 + 2$. In general that is a divided by b is written as

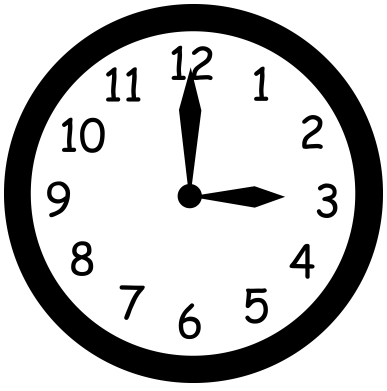
$$a = b \cdot q + r$$

where q is called the **quotient** and r is the **remainder**. And $0 \leq r < b$. Important point here is that the q and r are unique. This fact is important and not true for all sets of numbers. But it is true for $/Z$.

Definition 1.1. *We say a* **divides** *b (written $a|b$) if when we divide a by b we get a remainder of zero. Equivalently we can say $a|b$ if and only if there is some $k \in \mathbb{Z}$ so that $b = ka$. We call b a* **divisor** *of a.*

Definition 1.2. *We say $p \in \mathbb{N}$ is a* **prime** *if the only divisors of p are 1 and itself.*

2 Clock Math



1. What time is it 3 hours after to 5 o'clock?
2. How did you find your answer?
3. What time is it 9 hours after to 5 o'clock?
4. How did you find your answer? What is different and how did you andle it?

When we use a twelve hur clock we will write the above problems as

$$3 + 5 \equiv 8 \mod 12$$
$$\text{and } 9 + 5 \equiv 2 \mod 12$$

Here are a few more clock additions to attempt

1. $3 + 10 \mod 12$
2. $3 + 20 \mod 12$
3. $3 + 50 \mod 12$
4. $3 + 12 \mod 12$

How about these

1. $3 - 10 \mod 12$
2. $3 - 20 \mod 12$
3. $3 - 50 \mod 12$
4. $3 - 12 \mod 12$

How about

1. $0 \mod 12$
2. $1000 \mod 12$
3. $-1000 \mod 12$

What techniques did you use to solve these (reduce modulo 12)?
So your techniques are

1. add or subtract a 12

2. add or subtract a multiple of 12

3. divide by 12 and look for your remainder

4. Also maybe you observed $12 \equiv 0 \mod 12$

For our first clock we used integer hours and a twelve hour clock. Let's continue with integers for today but let's look at clocks of different number of hours, say a seven hour clock.

Reduce the following mod 7.

Here are a few more clock additions to attempt

1. $3 + 10 \mod 7$

2. $3 + 20 \mod 7$

3. $3 + 50 \mod 7$

4. $3 + 7 \mod 7$

How about these

1. $3 - 10 \mod 7$

2. $3 - 20 \mod 7$

3. $3 - 50 \mod 7$

4. $3 - 7 \mod 7$

How about

1. $0 \mod 7$

2. $1000 \mod 7$

3. $-1000 \mod 7$ see note below.[1]

So our techniues modulus 7 are

1. add or subtract a multiple of 7

2. divide by 7 and look for your remainder

3. and $7 \equiv 0 \mod 7$

[1] careful with your division here.

2.1 Multiplication

Now we can add with a 12 hour and seven hour clock with the same techniues. Can we multilpy, divide or use exponentiation? Here are some multiplications for you to try.

$3 * 7 \mod 12$ $\quad 5 * 7 \mod 12$ $\quad 8 * 9 \mod 12$

$21 * 72 \mod 12$ $\quad 35 * 35 \mod 12$ $\quad (-1) * 7 \mod 12$

$11 * 10 \mod 12$ $\quad (-1) * (-2) \mod 12$

Notice $11 * 10 \equiv (-1) * (-2) \mod 12$. Why is this so? Write it down carefully. Can this be a new technique?

So to reduce mudulo 12 we can

1. add or subtract a multiple of 12
2. divide by 12 and look for your remainder
3. notice $12 \equiv 0 \mod 12$ and
4. substitue "equal" values to make calculations easier.

Find the "easy" substitution for the following.

$6 * 5 \mod 7$ $\quad 50 * 3 \mod 7$ $\quad 51 * 52 \mod 7$

$55! \mod 7$ $\quad 6! \mod 7$ $\quad 55 * 54 * 53 * 52 * 51 * 50 \mod 7$

Any other observations? Look at $6! \mod 7$ snd $55 * 54 * 53 * 52 * 51 * 50 \mod 7$ carefully. Can you make a guess as to what is happening here?

2.2 Division

So we can add and multiply now but can we divide? I did promise only integers would be used so let's see what happens here. Solve the following fpr x.

1. $3x \equiv 1 \mod 7$
2. $5x \equiv 1 \mod 7$
3. $2x \equiv 8 \mod 7$
4. $3x \equiv 4 \mod 7$

Let me do the first one for you. We want to find a nuber x where $x \in \{0, 1, 2, 3, 4, 5, 6\}$ so that $3x \equiv 1 \mod 7$. Well maybe I can just guess. Let me try each possible value of x an see if any work.

try	sub into equation	Is it 1?	
$x = 0$	$3x \equiv 3(0) \equiv 0 \mod 7$	No.	So $x \neq 0$, Not our answer
$x = 1$	$3x \equiv 3(1) \equiv 3 \mod 7$	No.	So $x \neq 1$, Not our answer
$x = 2$	$3x \equiv 3(2) \equiv 6 \mod 7$	No.	So $x \neq 2$, Not our answer
$x = 3$	$3x \equiv 3(3) \equiv 9 \equiv 2 \mod 7$	No.	So $x \neq 3$, Not our answer
$x = 4$	$3x \equiv 3(4) \equiv 12 \equiv 5 \mod 7$	No.	So $x \neq 4$, Not our answer
$x = 5$	$3x \equiv 3(5) \equiv 15 \equiv 1 \mod 7$	Yes!	So our answer is $x = 5$
$x = 6$	$3x \equiv 3(6) \equiv 18 \equiv 4 \mod 7$	No.	So $x \neq 6$, Not our answer

So we get $x = 5$. That is $\frac{1}{3} \equiv 5 \mod 7$. Do you see this? You complete the other problems.

Here are a few more to solve.

a. $5x \equiv 1 \mod 12$ d. $7x \equiv 2 \mod 7$

b. $2x \equiv 8 \mod 12$ e. $12x \equiv 9 \mod 12$

c. $3x \equiv 4 \mod 12$

What happened here? Any guesses? Do d. and e. seem to make sense? How? Does c. make sense? Why?

Homework Problem 1. Our undestanding of this modular arithmatic seems flawed or incomplete. Please take some guesses as to what is going on. As a summary all of answers made sense mod 7. But we had problems mod 12. Summary of my problems a. gave us ne answer, b. yielded two answers and c. ad no answers.

Again a summary of our work so far

So to reduce mudulo 12 we can

1. add or subtract a multiple of 12
2. divide by 12 and look for your remainder
3. $12 \equiv 0 \mod 12$ and $7 \equiv 0 \mod 7$
4. substitue "equal" values to make calculations easier.
5. Our algebra $ax = 1 \mod 7$ "seems" fine and
6. Our algebra $ax = 1 \mod 12$ "seems" roublesome

Homework Problem 2. What is going on with $8! \mod 7$? Try $4! \mod 5$ $10! \mod 11$ $12! \mod 13$ and formulate a guess as to what is going on. Notice each problem has a prime number clock.

2.3 Exponentiation

Okay now we have a basic undestanding of addition, subtraction, division and multiplication $\mod n$. Let'slook at a new class of problems, exponentiation.

$2^{10} \mod 7 \quad 2^{2018} \mod 7$

Okay that second one looks hard so let's just try that first one.

$2^1 \equiv 2 \mod 7$
$2^2 \equiv 4 \mod 7$
$2^3 \equiv 8 \equiv 1 \mod 7$
$2^4 \equiv 2^3 2^1 \equiv (1) \cdot (2) \equiv 2 \mod 7$ as the number get larger use the previous calculation
$2^5 \equiv 2^4 2^1 \equiv (2) \cdot (2) \equiv 4 \mod 7$
$2^6 \equiv 2^5 2^1 \equiv (4) \cdot (2) \equiv 1 \mod 7$
$2^7 \equiv 2^6 2^1 \equiv (1) \cdot (2) \equiv 2 \mod 7$
$2^8 \equiv 2^7 2^1 \equiv (2) \cdot (2) \equiv 4 \mod 7$
$2^9 \equiv 2^8 2^1 \equiv (4) \cdot (2) \equiv 1 \mod 7$
$2^{10} \equiv 2^9 2^1 \equiv (1) \cdot (2) \equiv 2 \mod 7$

So $2^10 \equiv 2 \mod 7$.

Was there any patterns ya'll noticed? Can we use that pattern to help with $2^{2018} \mod 7$?. First notice

$$2018 = 3(672) + 2.$$

So

$$2^{2018} \equiv 2^{3(672)+2} \equiv 2^{3(672)} \cdot 2^2 (2^3)^{672} \cdot 4 \equiv (1)^{672} \cdot 4 \equiv 4 \mod 7.$$

Wow. Not too hard.

Here are two for you to try.

$2^{10} \mod 13 \quad 2^{2018} \mod 13$

Note I fund the following division useful $2018 = 6(q) + r$.

3 Theorems

4 Proofs

5 Cryptography

5.1 Caeser's Cipher

5.2 The Hill Cipher

5.3 RSA