2 Mod math

Modular arithmetic is the math you do when you talk about time on a clock. For example, if it's 9 o'clock right now, then it'll be 1 o'clock in 4 hours. Clearly, $9 + 4 \neq 1$ in general. But on a clock something special happens whenever a 12 shows up: we replace it with 0. This is called doing math "modulo 12" or "mod 12".

$[9 + 4]_{12} = [12 + 1]_{12} = [0 + 1]_{12} = [1]_{12}$

Of course, there's nothing special about the number 12. Why not have a clock with 11 numbers, or 30, or 5? On a clock with only 5 numbers, $[3]_5 + [4]_5 = [3 + 4]_5 = [7]_5 = [2]_5$.

The numbers you deal with "mod M" are between 0 and $M - 1$. But it's perfectly fair to say $\cdots = [-8]_5 = [-3]_5 = [2]_5 = [7]_5 = [12]_5 = [17]_5 = [22]_5 = \cdots$. These numbers are said to be "congruent mod 5".

There are a couple ways to think about congruent numbers. Each of the following are equivalent:

i) $[A]_M = [B]_M$
ii) the remainder of $\frac{A}{M}$ = the remainder of $\frac{B}{M}$
iii) $M \mid (A - B)$
iv) $A = jM + x$, $B = kM + x$, for some j and k

When looking at a number between 0 and $M - 1$ it'll be alright to drop the brackets. This means that the "mod" and the "remainder" operations are the same. So for example, $[7]_5 = 2$.

Q 2.0.1: $[1498766367828]_{10} =$?

Q 2.0.2: If it's 5:30pm now, what time will it be in 4753 hours?

Q 2.0.3: Today is Wednesday. What day of the week will it be in one year from today?

Q 2.0.4: By definition, $i^2 = -1$. $i^{58763} =$?

2.1 Properties

For any modulus M:

1) $[M]_M = 0$ (By definition)
2) $[A]_M + [B]_M = [A + B]_M$
3) $[A]_M \cdot [B]_M = [A \cdot B]_M$

Another way to think about "arithmetic mod M" is to think of every number as $jM+x$, and "taking the mod" just means ignoring the "jM". In what follows (and in general) "$\sim$" means "equivalent to".

Proof of 2)

$[A]_M + [B]_M$
$\sim (jM + A) + (kM + B)$
$= (j + k)M + (A + B)$
$\sim [A + B]_M$

Proof of 3)

$[A]_M \cdot [B]_M$
$\sim (jM + A)(kM + B)$
$= jkM^2 + jMB + kMA + AB$
$= (jkM + jB + kA)M + AB$
$\sim [AB]_M$

Q 2.1.1: Do these properties still hold when M is merely a rational number? What about irrational? Prove it.

A quick way to find a sum is to do all the addition inside the mod, instead of add everything and *then* taking the mod. The advantage is that you never have to deal with really difficult math, like 2-digit numbers. For example, for $[5 + 8 + 4 + 7 + 3 + 9 + 2]_7$:

$[5 + 8 + 4 + 7 + 3 + 9 + 2]_7$
$= [5 + 1 + 4 + 0 + 3 + 2 + 2]_7$ Take the mod of each term
$= [5 + 1 + 4 + 3 + 2 + 2]_7$
$= [5 + 1 + 4 + 3 + 4]_7$
$= [5 + 1 + 4]_7$ $[4 + 3]_7 = [7]_7 = [0]_7$
$= [5 + 5]_7$
$= [3]_7$ $[5 + 5]_7 = [10]_7 = [3]_7$
$= 3$

Q 2.1.2: You may already know that you can find the remainder of a number divided by 3 or 9 by adding up the digits. Now we'll prove it.

-What is $[10^k]_9$ for each value of k? Find a pattern, then prove it.

-When a number is written as "1432" what is really meant is $1 \cdot 10^3 + 4 \cdot 10^2 + 3 \cdot 10 + 2 \cdot 10^0$. In general, a base 10 number can be written as $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$. Using the properties of mod math, show that $[a_n \cdot 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10^1 + a_0]_9 = [a_n + a_{n-1} + \cdots + a_1 + a_0]_9$.

Q 2.1.3: Find the remainder of 4701135 when divided by 9.

Q 2.1.4: Make up any 5 digit number. Create a second number by rearranging the digits. Now find the difference between them mod 9.

Why did you get that answer?

Q 2.1.5: Try to construct the same kind of trick for mod 11, as was found in 2.1.2. Con-

struct a similar technique (looking at powers of 10), and use it to find $[1498766367828]_{11}$.

Q 2.1.6: -Say you have a number written in binary notation. Find a quick way of finding out whether or not it's divisible by 3.

-When is $2^n - 1$ divisible by 3?

Q 2.1.7: If you are writing base 8, what numbers can you find an easy divisibility test for, based on the digits?

Mod math can apply to variables and numbers the same. For example, $[x^3]_3 = [x^3 + 3x^2]_3 = [x^3 + 3x^2 - 27x^5]_3$, because $[3]_3 = [0]_3$. As with everything else from now on, x is an integer.

Example: You can show that $[x^5 - x]_5 = 0$.

The only things that x can be are $x = 0, 1, 2, 3, 4$. So, what we're looking for is a polynomial that's zero for every value of x. Starting with the most obvious choice:

$[x(x-1)(x-2)(x-3)(x-4)]_5$

$= [x(x-1)(x-2)(x+2)(x+1)]_5$ $\quad [-4]_5 = [1]_5$, $[-3]_5 = [2]_5$, and modding can pass through both addition and multiplication

$= [x(x^2-1)(x^2-4)]_5$

$= [x(x^2-1)(x^2+1)]_5$ $\quad [-4]_5 = [1]_5$

$= [x(x^4-1)]_5$

$= [x^5 - x]_5$

Q 2.1.8: Show that $[(x+3)^4]_4 = [(x^2+1)^2]_4$.

Q 2.1.9: Using the binomial expansion theorem, show that $[(X+a)^p]_p = [X^p + a^p]_p$, where p is prime.

Q 2.1.10: -Show that if $gcd(x, N) = 1$, then $[ax]_N = [bx]_N$ if and only if $[a]_N = [b]_N$.

-Why is this not the case if $gcd(x, N) \neq 1$?

2.2 Fast Exponentiation

Properties 2 and 3 basically say that "taking the mod" and either multiplication or addition can be done in either order. That is, you can take the mod and then multiply, or you can multiply and then take the mod. For example, $[13 \cdot 44]_6 = [1 \cdot 44]_6 = [1 \cdot 2]_6 = [2]_6 = 2$ This is useful because you can replace large numbers with smaller numbers before you add or multiply.

However, the same does not hold true for exponents. For example:

Exponentiating, then modding: $[2^7]_5 \rightarrow [128]_5 = [3]_5 = 3$.

Modding, then exponentiating: $[2^7]_5 \to [2^2]_5 = [4]_5 = 4$.
So, $[2^7]_5 \neq [2^2]_5$.
If you have an exponent, you have to leave it as it is. There are a few tricks to dealing with exponents, but they're a little more complicated than properties 2 and 3.

First, there's a quick way to find large powers of numbers in mod math. If you're trying to find $[x^N]_M$, and N is very large, then doing all N multiplications may take a tremendously long time. Instead, you can square over and over to find $[x^2]_M$, $[(x^2)^2]_M$, $[((x^2)^2)^2]_M$, ... (which is $[x^2]_M$, $[x^4]_M$, $[x^8]_M$, $[x^{16}]_M$, ...)

Q 2.2.1: Find $[7^1]_{15}$, $[7^2]_{15}$, $[7^4]_{15}$, $[7^8]_{15}$, $[7^{16}]_{15}$, $[7^{32}]_{15}$, and $[7^{64}]_{15}$.

Q 2.2.2: Use what you found in the last question to find $[7^{20}]_{15}$, $[7^{35}]_{15}$, and $[7^{85}]_{15}$.

So, once you know the binary expansion you can fast-exponentiate for any N. The binary expansion is pretty easy to find. All you have to do is find the largest power of 2 that's smaller than or equal to N, subtract it, and repeat.
Example: Express 570 as a sum of powers of 2.

$2^0 = 1$		
$2^1 = 2$		
$2^2 = 4$		
$2^3 = 8$	$512 < 570 < 1024$	$570 = 512 + 58$
$2^4 = 16$	$32 < 58 < 64$	$570 = 512 + 32 + 26$
$2^5 = 32$	$16 < 26 < 32$	$570 = 512 + 32 + 16 + 10$
$2^6 = 64$	$8 < 10 < 16$	$570 = 512 + 32 + 16 + 8 + 2$
$2^7 = 128$	$2 = 2^1$	*done*
$2^8 = 256$		
$2^9 = 512$		
$2^{10} = 1024$		

So, 570=512+32+16+8+2.

Example: $[3^{704}]_{19} =$?
First you find that $704 = 512 + 128 + 64 + 8 + 2$.

$[3^2]_{19} = [9]_{19}$
$[3^4]_{19} = [9^2]_{19} = [5]_{19}$
$[3^8]_{19} = [5^2]_{19} = [6]_{19}$
$[3^{16}]_{19} = [6^2]_{19} = [17]_{19}$
$[3^{32}]_{19} = [17^2]_{19} = [4]_{19}$
$[3^{64}]_{19} = [4^2]_{19} = [16]_{19}$
$[3^{128}]_{19} = [16^2]_{19} = [9]_{19}$
$[3^{256}]_{19} = [9^2]_{19} = [5]_{19}$
$[3^{512}]_{19} = [5^2]_{19} = [6]_{19}$

So, $[3^{704}]_{19} = [(3^{512})(3^{128})(3^{64})(3^8)(3^2)(3)]_{19} = [(6)(9)(16)(6)(9)(3)]_{19} = [139968]_{19} = [14]_{19} = 14$.

Q 2.2.3: For a given N, about how many multiplications do you need for this technique?

Q 2.2.4: $[2^{1030}]_{35} =$?

Q 2.2.5: $[5^{317}]_{12} =$?

2.3 Inverses and Identities

Def: Identity

An "identity" is an element that changes nothing.

The "additive identity" is zero, because $x + 0 = x$ for any x, and the multiplicative identity is 1, because $1 \cdot x = x$ for any x.

Def: Inverse

For any given element, x, the "inverse" is that element that when combined with x gives you the identity.

The "additive inverse" of x is $-x$, since $x + (-x) = 0$.

The "multiplicative inverse" of x is $\frac{1}{x}$, since $x \cdot \frac{1}{x} = 1$ (except for x=0).

Q 2.3.1: What is the additive inverse of $[x]_M$? Remember that the only numbers you have to work with are $0, 1, \cdots, M-1$

The multiplicative inverse is easy to find in regular math: it's just the reciprocal. But in modular arithmetic there are no fractions, so something like "1/3" makes no sense. Instead, the multiplicative inverse of 3 is denoted "3^{-1}". Even though we don't have access to fractions, the multiplicative inverse of a number often still exists!

For example, $[3^{-1}]_{10} = [7]_{10}$ because $[3 \cdot 7]_{10} = [21]_{10} = [1]_{10} = 1$. Keep in mind that the inverse of something is what you need to combine it with to get the identity, which is "1".

So, $[3^{-1}]_{10} = [7]_{10}$ and $[7^{-1}]_{10} = [3]_{10}$.

For relatively small moduli you can find the inverse x^{-1} by adding x to itself over and over until you get 1 (or equivalently by multiplying x by 1, then 2, then ...). For example, to find $[5^{-1}]_{11}$:

$j =$	0	1	2	3	4	5	6	7	8	9	10	11
$[5 \cdot j]_{11} =$	0	5	10	4	9	3	8	2	7	1	6	0

So, $[9 \cdot 5]_{11} = 1$, and $[5^{-1}]_{11} = 9$.

The more common name for this approach is the "brute force approach".

Q 2.3.2: Using the same technique as the example above, find $[1^{-1}]_7$, $[2^{-1}]_7$, $[3^{-1}]_7$, $[4^{-1}]_7$, $[5^{-1}]_7$, and $[6^{-1}]_7$.

Q 2.3.3: Find $[1^{-1}]_{10}$, $[2^{-1}]_{10}$, $[3^{-1}]_{10}$, $[4^{-1}]_{10}$, $[5^{-1}]_{10}$, $[6^{-1}]_{10}$, $[7^{-1}]_{10}$, $[8^{-1}]_{10}$, and $[9^{-1}]_{10}$.

Q 2.3.4: -In the last question several of the numbers didn't have inverses. Is there a pattern behind when a number does or doesn't have an inverse?

-How many times can you add x to itself mod M before the pattern of numbers repeats?

-Does $[14^{-1}]_{36}$ exist?

Q 2.3.5: Find $[1^{-1}]_{115}$.

Q 2.3.6: Find $[114^{-1}]_{115}$.

-Find another way to write "$[114]_{115}$" that would help explain the answer you got.

Q 2.3.7: What is $[(M-1)^{-1}]_M$, for any M?

Q 2.3.8: If $3 \mid M$, then $[(M+1)^{-1}]_{3M} =$?

When you're trying to find an inverse for x mod M what you're trying to do is solve $[j \cdot x]_M = [1]_M$ for j. In other words, you're trying to find j such that $jx = kM + 1$.

So, one way to find $[x^{-1}]_M$, is to solve the "linear Diophantine equation", $jx + kM = 1$, for j (k doesn't matter).

Example: $[13^{-1}]_{17} =$?

This is the same as solving $13j + 17k = 1$, and j is the inverse we're looking for. Like any Diophantine equation, we'll use Euclid's equation.

$A = 17$, $B = 13$

$r_1 = 17$ $r_1 = 1A + 0B$
$r_2 = 13$ $r_2 = 0A + 1B$
$r_3 = 4$ $r_3 = r_1 - 1 \cdot r_2$ $r_3 = 1A - 1B$
$r_4 = 1$ $r_4 = r_2 - 3 \cdot r_3$ $r_4 = -3A + 4B$
So, $4 \cdot 13 + (-3) \cdot 17 = 1$. Therefore, $[13^{-1}]_{17} = [4]_{17}$

Example: $[5^{-1}]_{11} =?$
This is the same as solving $j5 + k11 = 1$.
$A = 11$, $B = 5$
$r_1 = 11$ $r_1 = 1A + 0B$
$r_2 = 5$ $r_2 = 0A + 1B$
$r_3 = 1$ $r_3 = r_1 - 2 \cdot r_2$ $r_3 = 1A - 2B$
Therefore, $(-2) \cdot 5 + 11 = 1$. But, in general, only numbers between 0 and $M - 1$ are used, so $[5^{-1}]_{11} = [-2]_{11} = [9]_{11}$

Q 2.3.9: Find $]3^{-1}]_{32}$.

Q 2.3.10: Find $[53^{-1}]_{97}$.

Q 2.3.11: Find $[13^{-1}]_{52}$.

Q 2.3.12: Find $[5^{-1}]_{653}$.

2.4 The Euler totient function, φ

Def: $\varphi(N)$ is equal to the number of integers less than N that are coprime to N. Two numbers are "coprime" if their gcd is 1. $\varphi(1) = 1$ by definition.

Example: $\varphi(20) =?$
The prime divisors of 20 are 2 and 5. If a number isn't a multiple of 2 or 5, then it's coprime to 20. Those numbers are: 1, 3, 7, 9, 11, 13, 17, 19. That's eight numbers.
$\varphi(20) = 8$

Q 2.4.1: Find $\varphi(N)$ for $N = 1, \cdots, 15$

Q 2.4.2: It's often easier to find the number of numbers less than or equal to N that share a common divisor with N. Once you've done that, then $\varphi(N)$ is what's left.
-What is $\varphi(p)$, where p is prime?
-What is $\varphi(p^k)$, where p is prime?
-What is $\varphi(pq)$, where p and q are prime?

It's worth knowing that when $gcd(A, B) = 1$, $\varphi(AB) = \varphi(A)\varphi(B)$. This allows us to calculate $\varphi(N)$ quickly if we can factor N. For example, $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$.

Q 2.4.3: Find a general formula for $\varphi(N)$, assuming that you already know all of the factors of N.

Q 2.4.4: Prove that the sum of φ of every divisor of N is N.

For example, if $N = 10$, then the divisors are $d = 1, 2, 5, 10$ and $\varphi(1) + \varphi(2) + \varphi(5) + \varphi(10) = 1 + 1 + 4 + 4 = 10$.

Hint: If $gcd(a, b) = x$, then what's $gcd\left(\frac{a}{x}, \frac{b}{x}\right)$?