Number Theory

This is a quick summary of concepts in Chapter 3 of

`https://www.whitman.edu/mathematics/higher_math_online/`

Congruence

For a positive integer n and two integers a and b, we say that a and b are congruent *modulo* n, if they have the same remainder upon division by n, and we write

$$a \equiv b \bmod n$$

By this definition, if $a \equiv b \bmod n$ we can write:

$$a = qn + r$$

$$b = q'n + r$$

and we see that the difference between a and b is evenly divided by n, with no remainder.

$$a - b = (q - q')n$$

The converse is also true. We write $n|a - b$ to mean that n divides $a - b$ evenly. If so, there is some x such that

$$a - b = xn$$

$$a = b + xn$$

Since $b = q'n + r$

$$a = q'n + r + xn$$

$$a = (q' + x)n + r$$

Thus, the remainder when dividing a/n is equal to r, as stated.

"There are a number of elementary properties which follow such as $a \equiv b$ implies $b \equiv a$. The latter ones can can be summarized by saying that in any expression involving +,, and positive integer exponents (that is, any "polynomial"), if individual terms are replaced by other terms that are congruent to them modulo n, the resulting expression is congruent to the original."

casting out nines

In decimal notation, if the representation of x is $d_n \ \ldots d_2 \ d_1 \ d_0$, we mean that

$$x = d_0 + d_1 \ 10^1 + d_2 \ 10^2 + \cdots + d_n \ 10^n$$

All powers of $10 \equiv 1 \bmod 9$ because, for example

$$10^2 \bmod 9 = 10 \bmod 9 * 10 \bmod 9 = 1 * 1 \bmod 9 = 1$$

So

$$x \bmod 9 = (d_0 + d_1 + d_2 + \cdots + d_n) \bmod 9$$

Hence the left-hand side is zero only if $\sum d_i \bmod 9 = 0$.

trick question

Suppose $a = nq + r$. What is the remainder upon dividing a by n? It is not necessarily r!

Example: divide 20 by 6. Well, $20 = 6 \cdot 2 + 8$ but $r > n$ and the correct answer is 2.

important result

$$ma \equiv mb \bmod mn \quad \iff \quad a \equiv b \bmod n$$

Notation

For every integer a we say that $[a] = [a']$ if and only if $a \equiv a'$.

Define $Z_n = \{[0],\ [1],\ [2],\ \ldots [n-1]\}$. For example: $Z_4 = \{[0],\ [1],\ [2],\ [3]\}$. Z_4 is also equal to $\{80], [25], [102], [13]\}$, but this is just confusing.

This formal notation seems a bit too much to me.

Addition and multiplication tables for Z_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

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The usual laws apply for addition, subtraction and multiplication. However, division is different. To divide by a instead, multiply by the multiplicative inverse a^{-1}.

The problem is that some values for a don't have an inverse. Another problem is that $ab = 0$ does not imply that either $a = 0$ or $b = 0$.

However, for Z_p where p is prime, it's all fine. Here is that multiplication table for Z_7:

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0

1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Here, every value has a unique multiplicative inverse, and in fact, for every a and b

$$ax = b$$

has a unique solution.

Note something curious, if we talk about Z_9 and *leave out those elements that do not have an inverse*, including zero, then everything works.

x	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Euclidean algorithm

We've already explored the Euclidean algorithm for finding the greatest common divisor or $gcd(a, b)$. Suppose that $a > b$ (if not, switch them).

Consider $a = 198$, $b = 168$. The algorithm depends on the fact that if m is a divisor of both a and b

$$mx = a$$

$$my = b$$

then m is also a common divisor of their difference.

$$a - b = m(x - y)$$

And if some multiple of b, say cb, can be subtracted from a so that $cb = mcy$ then

$$m(x - cy) = a - cb$$

m is a common divisor of that difference.

One way of formulating the algorithm: given a and b, with $a > b$, find the largest q so that $a = qb + r$. If $r = 0$, the result is b. Otherwise, if $r \neq 0$, set $a = b, b = r$ and repeat.

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

$$198 = 1 \cdot 168 + 30$$

$$168 = 5 \cdot 30 + 18$$

$$30 = 1 \cdot 18 + 12$$

$$18 = 1 \cdot 12 + 6$$

$$12 = 2 \cdot 6 + 0$$

$gcd(198, 168) = 6$. Of course, if we factored these two numbers we would see right away that

$$198 = 2 \times 3^2 \times 11$$

$$168 = 2^3 \times 3 \times 7$$

linear combination

It turns out that m is a *linear combination* of a and b, meaning that there exist integers (one positive and one negative) such that:

$$m = x \cdot a + y \cdot b$$

Start with

$$30 = 198 - 168 = a - b$$

$$18 = 168 - 5 \cdot 30 = b - 5(a - b) = -5a + 6b$$

We can check this calculation:

$$-5 \cdot 198 + 6 \cdot 168 = -990 + 1008 = 18$$

Continue

$$12 = 30 - 18 = (a - b) - (-5a + 6b) = 6a - 7b$$

$$6 = 18 - 12 = -5a + 6b - (6a - 7b) = -11a + 13b$$

Check again and see that this is correct.

Now, for the cases we really care about, the *gcd* will be equal to 1, and we will end up with an equation like:

$$1 = x \cdot a + y \cdot b$$

and we will say that mod a

$$1 = y \cdot b$$