Number Theory

This is a quick summary of some 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

$$a = qn + r$$
$$b = q'n + r$$

and write

$$a \equiv b \bmod n$$

It follows from this definition 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

$$n \mid a - b$$

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

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

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:

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

Rearrange the previous equations to be differences:

$$r = (q)b - a$$

```
30 = 198 - (1)168
18 = 168 - (5)30
12 = 30  - (1)18
 6 = 18  - (1)12
 0 = 12  - (2)6
```

I've struggled with coding this algorithm. I find it relatively easy to work out by myself when going in reverse, so let's try that first.

We must first go through forward to generate the lines above and find the *gcd*. Then, start with the next to last line:

$$6 = 18 - (1)12$$

Substitute for $12 = 30 - (1)18$ from the previous line:

$$6 = 18 - 1\ [30 - (1)18\ ]$$

Consolidate:

$$6 = (2)18 - 1(30)$$

Note the equality holds. Switch terms

$$6 = -(1)30 + (2)18$$

Substitute for $18 = 168 - (5)30$ from the previous line:

$$6 = -(1)30 + 2\ [168 - (5)30\ ]$$

Consolidate

$$6 = -(11)30 + 2(168)$$

Switch terms:

$$6 = 2(168) - (11)30$$

Substitute for $30 = 198 - (1)168$ from the previous line:

$$6 = 2(168) - 11\ [\ 198 - (1)168\ ]$$

$$6 = 13(168) - 11(198)$$

$$6 = -11(198) + 13(168)$$

Every equation above is a true equation, they all work out to 6.

Thus we have expressed the *gcd* as a linear combination of a and b.

And now if we take mod 198 of both sides we have

$$13(168) \bmod 198 \equiv 6$$

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

$$1 = y \cdot b \bmod a$$

We've derived y, and shown that y and b are multiplicative inverses mod a. That's the point.

forward direction

Start with

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

The next line is

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

Then

$$12 = 30 - (1)18 = (a - b) - (-5a + 6b) = 6a - 7b$$

Finally

$$6 = 18 - (1)12 = (-5a + 6b) - (6a - 7b) = -11a + 13b$$

which is just what we had before.

Chinese Remainder Theorem

theorem

Let r and s be positive integers which are relatively prime, and let a and b be any two integers.

Then there exists an integer N such that

$$N \equiv a \bmod r$$
$$N \equiv b \bmod s$$

Furthermore, N is uniquely determined mod rs.

One way to see this is to consider two side by side expansions, one with with s copies of Z_r and the other with r copies of Z_s.

```
o o o o o x x x x x o o o o o x x x x x o o o o o x x x x x
# # # # # # * * * * * * # # # # # # * * * * * * # # # # # #
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
                          N
```

Any particular N in Z_{rs} corresponds to a unique pair of remainders mod r and mod s.

In this example, $N = 11$

$$N \equiv 1 \bmod 5$$

$$N \equiv 5 \bmod 6$$

Of all the numbers in Z_{rs}, only N gives this pair of remainders $(1, 5)$.

There is a family of numbers $N + krs$ $(k = 0, 1, 2 \dots)$. Every number in the family has the same remainder mod r and, similarly, has the same remainder mod s, because krs gives zero remainder with both r and s.

example

Let $r = 5$ and $s = 6$. Suppose $a = 8$ and $b = 11$.

$$a = 8 \equiv 3 \bmod 5$$

$$b = 11 \equiv 5 \bmod 6$$

There must be some $N < rs$ (namely 23), with the same remainders: $N \equiv 3$ mod 5 and $N \equiv 5$ mod 6. The next such number is $N + rs$.

```
 3  8 13 18 23 28 33 38 43 48 53
 5 11 17 23 29 35 41 47 53
```

Euler Phi Function

$\phi(n)$ is defined to be the number of non-negative integers less than n that are relatively prime to n. $\phi(1)$ is defined to be 1.

$$\phi(2) = 1, \quad \{1\}$$
$$\phi(3) = 2, \quad \{1, 2\}$$
$$\phi(4) = 2, \quad \{1, 3\}$$
$$\phi(5) = 4, \quad \{1, 2, 3, 4\}$$

If p is prime, then

$$\phi(p) = p - 1$$

If p is prime and a is a positive integer

$$\phi(p^a) = p^a - p^{a-1}$$

If $n = pq$ where p and q are prime, or $n = ab$ where a and b are *relatively* prime:

$$\phi(n) = \phi(p)\ \phi(q) = (p-1)(q-1)$$
$$\phi(n) = \phi(a)\ \phi(b) = (a-1)(b-1)$$