CHAPTER 3 (LECTURE 3): from Stillwell's Elements of Number Theory

§3.1: Congruence mod n:

Casting out the nines: a natural # is divisible by 9 only if the sum of the digits is divisible by 9.

Example: 774 is divisible by 9 as $7+7+4=18$.

Notice if there are 9's then they don't change the result,

Example: $979794 = \underline{9}+7+\underline{9}+7+\underline{9}+4 = \underline{27}+18$

Def^{n}/ $a, b \in \mathbb{Z}$ are congruent mod n, written $a \equiv b \pmod{n}$ if they leave same remainder on division by n. Equivalently $a \equiv b \pmod{n}$ if $n \mid (b-a)$.

Example: Even # congruent mod 2;

$a = 2j$ & $b = 2h \Rightarrow b-a = 2(h-j)$

$\Rightarrow 2 \mid b-a$.

Likewise, odd # congruent mod 2,

$a = 2j+1$, $b = 2h+1 \Rightarrow b-a = (2h+1)-(2j+1)$

$\Rightarrow b-a = 2(h-j)$

$\Rightarrow 2 \mid b-a$

$\Rightarrow b \equiv a \pmod{2}$.

To understand casting out nines we need the arithmetic modulo n.

§3.2 CONGRUENCE CLASSES & THEIR ARITHMETIC

Def^{n}/ congruence class of a mod n : $\{nk+a \mid k \in \mathbb{Z}\}$

can denote $n\mathbb{Z}+a$.

For example even #'s are $2\mathbb{Z}$
odd #'s are $2\mathbb{Z}+1$. We also
can partition $\mathbb{Z}$ into $3\mathbb{Z}$, $3\mathbb{Z}+1$, $3\mathbb{Z}+2$

this partition corresponds to the equivalence relation $\equiv$ mod n on $\mathbb{Z}$. (explained in detail in my typed notes)

Def^{n}/ $(n\mathbb{Z}+a)+(n\mathbb{Z}+b) = n\mathbb{Z}+(a+b)$
$(n\mathbb{Z}+a)(n\mathbb{Z}+b) = n\mathbb{Z}+ab$
} congruence arithmetic

In my typed notes I also use notation $[a] = n\mathbb{Z}+a$. In that notation the above reads

$$[a]+[b] = [a+b]$$
$$[a][b] = [ab]$$

I prove these def^{n}'s are not ambiguous despite the fact the choice of a, b as representative is far from unique. For example, mod 2, $2\mathbb{Z} = [0] = [2] = [42]$ etc. Or mod 3, $3\mathbb{Z}+1 = [1] = [7] = [-5]$ etc. (any blue dot in the dot-diagram)

((((pages 46-47 are covered by my typed notes) with some added care)))

Casting out nines in view of modular arithmetic

Observe $10 \equiv 1 \pmod 9$

$10^2 \equiv 1^2 \pmod 9$

$10^3 \equiv 1^3 \pmod 9$

Generally $10^k \equiv 1 \pmod 9$ for $k \in \mathbb{N}$

Hence $a_k 10^k \equiv a_k \bmod 9$. Consider the base-ten # $a_k a_{k-1} \cdots a_2 a_1 a_0 = n$ which means,

$$n = a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0$$

$$\boxed{n \equiv a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0 \pmod 9}$$

A number $n \in \mathbb{N}$ is congruent to the sum of its decimal digits mod 9. In particular, if $9 \mid n$ then $9 \mid (a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0)$.

Application: to find remainder on division by 9 can find sum of digits and find remainder

$\frac{12345}{9}$ has same remainder as $1+2+3+4+5 = 15 \equiv 6 \bmod 9$.

Of course, it's fun to check,

$$\begin{array}{r} 1361 \\ 9\overline{)12345} \\ 9 \\ \hline 33 \\ 27 \\ \hline 64 \\ 63 \\ \hline 15 \\ 9 \\ \hline (6) \end{array}$$

$$\frac{12345}{9} = 1361 + \frac{6}{9}$$

Ex] How can we see remainders on division by 3?

$$10 = 9+1 \equiv 1 \mod 3$$

$$\Rightarrow 10^k \equiv 1 \mod 3.$$

Hence,

$$a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv$$

$$\hookrightarrow \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \pmod 3$$

For example,

$\frac{1275}{3}$ has remainder same as $\frac{1+2+7+5}{3}$

Namely remainder of 0 since $3 \mid 1275$.

Ex] divisibility by 11?

Key observation $10 \equiv -1 \pmod{11} \hookrightarrow 10^k \equiv (-1)^k \pmod{11}$

$$a_k \cdot 10^k + \cdots + a_2 10^2 + a_1 10 + a_0 \equiv (-1)^k a_n + \cdots + a_2 - a_1 + a_0 \mod 11$$

$\frac{3083}{11}$ has remainder same as $\frac{-3-8+3}{11}$

namely $-8+11 = \boxed{3}$. Let's check,

↖ added 11 to make positive remainder.

$$11 \overline{)3083} \quad 280$$

22

88

88

3

$\therefore \frac{3083}{11} = 280 + \frac{3}{11}$

Divisibility tricks for other #'s and decimals: let's play a bit with other #'s

Ex] $n = a_n \cdots a_2 a_1 a_0$ is divisible by 2 iff $2 \mid a_0$. In other words, n is even only if its decimal ones digit $a_0 = 0, 2, 4, 6$ or 8. Like wise $n \in 2\mathbb{Z}+1 \Rightarrow a_0 = 1, 3, 5, 7$ or 9.

Ex] $n = a_n \cdots a_2 a_1 a_0$ is divisible by 4 when?

Consider,

$$n = a_n \times 10^n + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0$$
$$= (a_n \times 10^{n-2} + \cdots + a_2) \cdot 4 \cdot 25 + 10a_1 + a_0$$
$$\equiv 10a_1 + a_0 \mod 4$$

Thus, the condition needed is $10a_1 + a_0 \equiv 0 \mod 4$. That is, the last two digits are all that matter and,

$$00, 04, 08, 12, 16, 20, \ldots, 96$$

as last digits imply n divisible by 4.

Remark: any # which we may build from factors in 10 ($2 \& 5$) will allow us to see remainders just from the first few digits. For other #'s like 9, 11 or 3 there are other tricks, all from adding or multiplying congruences.

Ex Divisibility by 7 ?

Notice $10 \equiv 3 \mod 7$

$10^2 \equiv 9 \equiv 2 \mod 7$

$10^3 \equiv 2 \cdot 3 = 6 \mod 7$

$10^4 \equiv 2 \cdot 2 = 4 \mod 7$

$10^5 \equiv 2 \cdot 4 = 1 \mod 7$

$10^6 \equiv 10 \equiv 3 \mod 7$

$10^7 \equiv 2$

$10^8 \equiv 6$

$10^9 \equiv 4$

$10^{10} \equiv 1$

So, ∃ some pattern but, it's not so nice.

For example, then

$[987654321] = [$~~$9+8\cdot 2+6\cdot 3+4\cdot 4+1\cdot 5$~~
~~$+3\cdot 6+2\cdot 7+$~~

$= [1 + 2\cdot 3 + 3\cdot 2 + 4\cdot 6 + 5\cdot 4 + 6\cdot 1 + 7\cdot 2 + 8\cdot 6 + 9\cdot 4]$

$= [$~~$1 + 6^{0} + 6 + 24^{3} + 20^{6} + 6 + 14^{0} + 48^{6} + 36^{1}$~~$]$

$= [6 + 3 + 6 + 6 + 6 + 1]$

$= [28]$

$= [0] \quad \therefore \ 7 \mid 987654321.$

aww... somewhere ∃ a mistake the real remainder is (4)

$$
\begin{array}{r}
101093474 \\
7\overline{)\,987654321} \\
7 \\
\hline
28 \\
7 \\
\hline
7 \\
7 \\
\hline
65 \\
63 \\
\hline
24 \\
21 \\
\hline
33 \\
28 \\
\hline
52 \\
49 \\
\hline
31
\end{array}
\quad \rightarrow (4)
$$