Why double every other digit?

- Don't have to — different check sum.

$$\begin{array}{ccc} & 12 & & 21 & \\ & \downarrow & & \downarrow & \\ 4 : & \underbrace{22} & & \underbrace{41} & : 5 \end{array}$$

However Luhn's alg sees no diff. between 09 and 90

- Luhn's alg. is a coarse check.

Verhoeff's alg. Damm's alg.

Use Luhn to find the missing digit.

5457 6238 9?23 4113

$$2 \equiv 62 + ? \equiv 0 \pmod{10}$$

Because ? is in an odd spot → missing digit is 8. If it in an even spot, it would 4.

PPSNs

This uses digits and letters:

$$A \longleftrightarrow 1$$
$$B \longleftrightarrow 2$$
$$C \longleftrightarrow 3$$
$$\vdots \quad \vdots \quad \vdots$$
$$W \longleftrightarrow 23$$

$$d_1 d_2 \cdots d_9.$$

$$\boxed{d_8 \equiv 8d_1 + 7d_2 + 6d_3 + 5d_4 + 4d_5 + 3d_6 + 2d_7 + 9d_9 \pmod{23}}$$

Verify 1234567FA

↳ 1234567$\underline{6}$1
8

(mod 23)

$$8(1)+7(2)+6(3)+5(4)+4(5)+3(6)+2(7)+9(1)$$
$$\equiv \cancel{8}+(-9)+(-5)+\cancel{4}+(-3)+(-5)+(\cancel{-9})+\cancel{9}$$
(−3)
$$\equiv -9-3-5 \equiv -17 \equiv 6.$$

Find the missing digit: 2 zeros

1213001W?

Call missing letter x. $0 \equiv 9x + 18\ (23)$

$$8(1) + 7(2) + 6(1) + 5(3) + 2(1) + 9x \equiv 0 \quad (23)$$

$$-1 \qquad \cancel{-2} \qquad \cancel{2}$$

$$\boxed{9x - 1 \equiv 0 \pmod{23}}$$

Finding missing letter is to solve for x.

$$\boxed{9x \equiv 1 \quad (23)}$$

No tools :(There is one solution and it is $\boxed{x \equiv 18} \rightarrow$ R.

$$2x \equiv 1 \pmod{6}$$ Not prime.

No x's that work!

Multiplicative inverses

Such a number is something we are very used to. If $a \in \mathbb{R}$, then we can find $b \in \mathbb{R}$ such that

$$a \cdot b = 1. \qquad b = \frac{1}{a} = a^{-1}$$

We know the integers do not contain M.I.s

With $\mathbb{Z}_m$ sometimes they are ~~the~~ there and sometimes not.

Let $a \in \mathbb{Z}_m$. We say it has an (mult.) inverse if there is some $x \in \mathbb{Z}_m$ such that

$$a \cdot x \equiv 1 \pmod{m}.$$

Notation is same: $x = a^{-1}$.

<u>Thm.</u>

$ax \equiv 1 \pmod{m}$ has a solution if and only if $\gcd(a, m) = 1$.