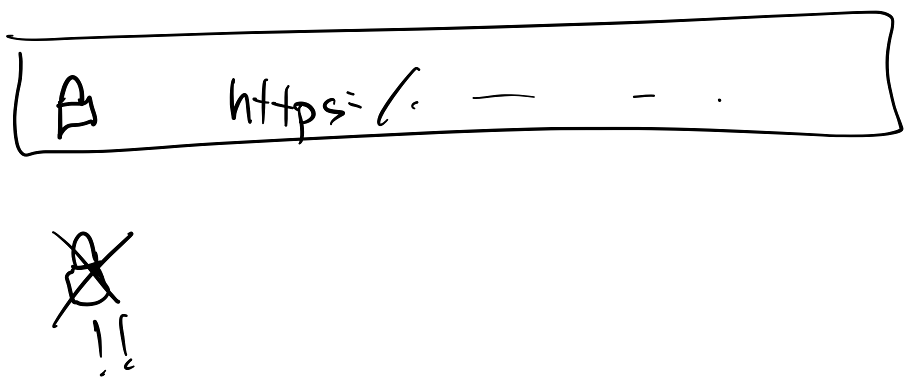
Puzzler (last chance at this one):

Last time, Alice and Bob wanted to exchange messages, but the only time they met was in a class where Carl sat between them. Everything they exchanged had to go through Carl. To prevent him from reading their notes, they devised a scheme of using both of their locks on the outside of the suitcase.

But a problem happened: To all appearances, the locks seem identical. In other words, Alice can't see whether or not a lock on the suitcase is really Bob's. She suspects that Carl has been switching suitcases, and the locks that she assumed were Bob's were actually Carl's! It looks like some of the notes she received weren't actually from Bob, but maybe from Carl instead!

This time we're changing the problem a bit: All the locks are now combination locks. Anyone can buy as many combination locks as they want. There is also a blackboard in front of the room, and if anyone wants, they can share the combination to any of their locks if they want.

This time, two kinds of briefcases are available: the regular ones from before, and new smaller ones that can fit inside the regular briefcases. What can Bob and Alice work out (with Carl possibly hearing the whole plan) so that Bob can send a private message to Alice, and Alice can be sure the message came from Bob?



Language of modular arithmetic

Recall: $[a]_d$ means the type of number which when divided by d has the same remainder as a does when divided by d.

Ex: • 1 is a number of type $[1]_2$ and also of type $[6]_5$

• 21 is also a number of type $[6]_5$

- $[8]_7$ and $[1]_7$ mean the same thing.
  both mean having a remainder of 1 when divided by 7.

These symbols $[a]_d$ represent what are called "congruence classes" modulo d.

$[5]_7$ is a congruence class modulo 7

8 & 22 are in the same congruence class modulo 7

same remainder when divided by 7.

$8 \equiv 22 \pmod{7}$ means 8 & 22 are in same congruence class modulo 7

$[1]_7$

Some numbers congruent to 4 modulo 9 are: 13, 22, 31

PollEv.com/dkrashen

What is a "type" of number?

<u>Def</u> Type of number means subset of $\mathbb{Z}$.

example:

even $\longleftrightarrow \{\ldots,-4,-2,0,2,4,\ldots\}$

$= \{2m \mid m \in \mathbb{Z}\}$

$= \{n \in \mathbb{Z} \mid n \text{ is divisible by } 2\}$

$[3]_7 = \{\ldots, 3, 10, 17, 24 \ldots\}$

10 has type $[3]_7$

$\Updownarrow$

$10 \in [3]_7$

Desriby congruence classes (subsets of $\mathbb{Z}$)

Proposition: Given $a, b \in \mathbb{Z}$, d a pos integer, the followy statements are equivalent:

1. $[a]_d = [b]_d$ (equality of sets)
2. a is in class $[b]_d$ (assertion of set membership $a \in [b]_d$)
3. b is in class $[a]_d$
4. $a-b$ is divisible by d.

Preliminary lemma:

Suppose $a \in \mathbb{Z}$, $d > 0$ integer then $a \in [a]_d$

Pf: $[a]_d$ means the integers whose remainder when divided by d is the same as the remainder of a when divided by d.
But by def the remainder of a when divided by d is the remainder of a when divided by d. so $a \in [a]_d$.

Proof of prop.

Suppose 1 (i.e. $[a]_d = [b]_d$)
want to show 2 (i.e. $a \in [b]_d$)
by lemma, $a \in [a]_d$ by hypothesis $[a]_d = [b]_d$.
So $a \in [b]_d$. ✓

Suppose 2 (i.e. $a \in [b]_d$)
want to show 3 (i.e. $b \in [a]_d$)

$a \in [b]_d$ means a & b have the same remainder when divided by d. that also means $b \in [a]_d$.
✓

Suppose 3 (i.e. $b \in [a]_d$)
want to show 4 (i.e. $a - b$ is a mult. of d)

since $b \in [a]_d$, a, b same remainder when dividing by d.

i.e. $a = qd + \underline{r}$ $\quad b = q'd + \underline{r}$

$$a - b = qd + r - q'd - r = (q - q')d - \underbrace{(\cancel{r - r})}_{0}$$

$$= (q - q')d$$

a mult. of d. ✓

Final challenge assume $a - b$ mult of d (*)

want to show $\underline{[a]_d = [b]_d}$.

By def, this means we want to show $[a]_d$ & $[b]_d$ same elements — i.e. if $m \in [a]_d$ then $m \in [b]_d$

& vise versa.

we'll show only $m \in [a]_d$ implies $m \in [b]_d$ (reverse follow similarly)

<u>Utility:</u> $\quad [a]_d = \{a, a+d, a-d, a+2d, a-2d \ldots\}$

$$[13]_{11} = \{13, 2, -9, -20, \ldots\}$$

$$-20 = (-2) \cdot 11 + \underline{2},$$

Assertion:

$$[a]_d + [b]_d = [a+b]_d$$

given a number congruent to a mod d

" " " " b " " d

add them, get a number cong. to $a+b$ mod d.

$[a]_d = \{a+md \mid m \in \mathbb{Z}\}$ $\qquad$ $\{b+md \mid m \in \mathbb{Z}\} = [b]_d$

a' $\qquad$ b'

$$a'+b' \in \{a+b+md \mid m \in \mathbb{Z}\} = [a+b]_d$$

Can do arithmetic (add, sub, mult, exp.) w/ congruence classes as if they are numbers.

Observation: $[5]_7[3]_7 = [1]_7$

$$[10]_7 = [3]_7$$

$$[5]_7[10]_7 = [1]_7$$

Observe: $[n]_7 = [0]_7$ if and only if $[5n]_7 = [0]_7$

if $[n]_7 = [0]_7$

$[5n]_7 = [5]_7 [n]_7$

$= [5]_7 [0]_7 = [0]_7.$

if $[5n]_7 = [0]_7$

then $[3]_7 [5n]_7 = [3] \cdot [0] = [0]$

$\parallel$

$[3 \cdot 5 \cdot n] = [3 \cdot 5] [n]$

$= [1] \cdot [n] = [n]$

Suppose $n = a + 10b$

$[5n]_7 = [5a]_7 + \overbrace{[5]_7 [10]_7}^{[1]} [b]_7$

$= [5a + b]_7$

$5392 \rightsquigarrow 5 \cdot 2 + 539 = 549$

$9 \cdot 5 + 54 = 99$

$[5] = [-2]$

$= 9 \cdot 5 + 9$

$= 45 + 9 = \cancel{54}$