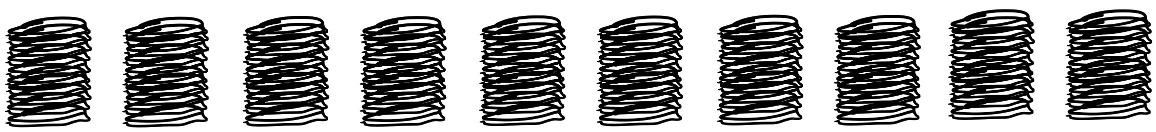
Puzzler: You are given 10 stacks of 10 coins each. One of the stacks contains counterfeit coins, each of which weighs exactly 21 grams. The other nine stacks contain all genuine coins weighing exactly 20 grams.

You are given a very accurate scale to use to weigh the coins. For each weighing, you put some of the coins on the scale and can check the reading of how much it weighs.

But -- the scale is almost out of batteries, so you want to be careful. How many weighings do you need to make in order to accurately determine which pile is counterfeit?



Answer: 1 (why?)

No class on Tues Oct 10

New monthly due date Tues Oct 10 @ midnight

No class Tues Nov 21

Today:

- Arithmetic (Divisibility / Fr 13)
- Cryptography Ideas
- Intro. to graph theory (networks, diagrams...)
- Storytime (hearing the shape of a drum)

Divisibility tricks

4 Rule (How to tell if a number is div. by 4)

i). • a number is div. by 4 exactly when its last 2 digits are divisible by 4.

ii). • for a 2 digit number it's div. by 4 if either
- the 10's digit is even & 1's is 0, 4, 8
- the 10's digit is odd & 1's is 2, 6

ex: 379432 ✓ 59326 ✗

Why does this work?

$$n = \underbrace{a}_{2\text{ digit}} + 100\underbrace{b}_{100\text{'s place }\&\text{ up}}$$

$n = 379432$
$= 32 + 100(3794)$

Q: is $[n]_4 = [0]_4$?

$$[n]_4 = [a+100b]_4 = [a]_4 + [100b]_4$$
$$= [a]_4 + [100]_4 [b]_4$$
$$= [a]_4 + [0]_4 [b]_4$$
$$= [a]_4 + [0 \cdot b]_4 = [a]_4$$

verifies i)

what about 2 digit #s?

$m = c + 10d$

1's   10's

$[m]_4$
$=$
$[c+10d]_4$
$=$
$[c]_4 + [10]_4 [d]_4$
$= [c]_4 + [2]_4 [d]_4$
$= [c+2d]_4$

if d odd $d = 2r+1$

$[c+4r+2]_4$
$=$
$[c+2]_4$

c 1 digit #
and want c+2 mult of 4

$c = 2, 6$

if d even $d = 2l$

if 10's digit (d) is even need 1's to be a mult of 4.

$c = 0, 4, 8$

$[c+4l]_4 = [c]_4$

ii)

Rules:

3 add digits, check if mult of 3
9 " " " " " 9
11 alternately add & subtract, check if mult of 11

$$3157 = 287 \times 11$$

$$\overbrace{3-1+5-7}^{8}$$ with $\underbrace{3 - 1 + 5}_{8}$

7 rule: $n = a + 10b$ is div by 7 iff $5a + b$ is, or if $b - 2a$ is.

$$5693 \rightsquigarrow 569 + 5\cdot 3 = 569 + 15 = 584 \rightsquigarrow 58 + 4\cdot 5 = 78$$

Fri the 13th

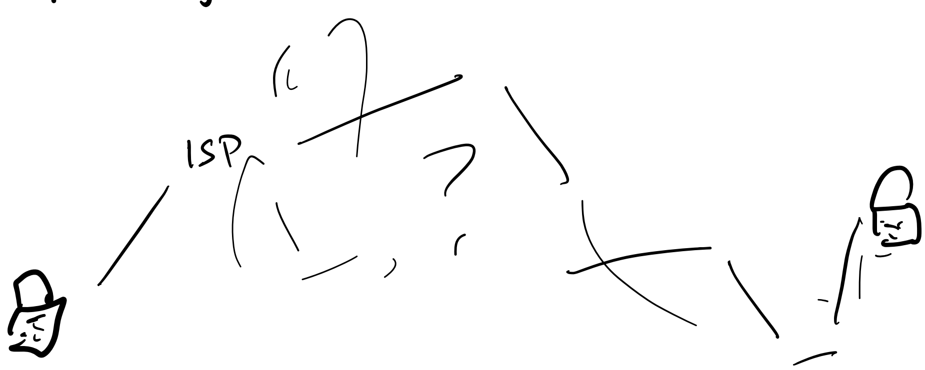
Su	M	....	Sa
0	1		6

$d = [d+52]_7$

			13th
	J	31	$[d]_7$
28	F	28/29	$[d+31]_7 = [d+3]_7$
3~31	M	31	$[d+3+28]_7 = [d+3]_7$
	A	30	$[d+6]$
2~30	M	31	$[d+8] = [d+1]$
3~31	J	30	$[d+4]$
2~30	J	31	$[d+6]$
3	A	31	$[d+2]$
3	S	30	$[d+5]$
2	O	31	$[d]$
3	N	30	$[d+3]$
2	D	31	$[d+5]$

	J	31	$[d]_7$
28	F	28 / 29	$[d+3]_7$
3~31	M	31	$[d+4]_7$
2~30	A	30	$[d]$
3~31	M	31	$[d+2]$
2~30	J	30	$[d+5]$
3	J	31	$[d]$
3	A	31	$[d+3]$
2	S	30	$[d+6]$
3	O	31	$[d+1]$
2	N	30	$[d+4]$
	D	31	$[d+6]$

Cryptography



to send secure messages:

- agree on "secret key" (large #)
- relatively easy to encode & decode

"chunk" message, use key to shuffle
in complicated by reversible way.
AES

All cryptosystems rely on
"1 way functions / processes"

<u>Classic example</u>: discrete logarithm property.

Given prime number p then for "most" numbers
$2 \leq g \leq p-2$ if we consider the sequence

$$[g]_p, [g^2]_p, [g^3]_p \cdots [g^{p-1}]_p$$

same sequence (shuffled) as

$$[1]_p, [2]_p, \cdots, [p-1]_p$$

<u>ex</u>: $[2^{57}]_{101}$ easy.

$$[2^?]_{101} = [35]_{101}$$

$$? = \log_2 [35]_{101}$$

public

Alice: $\qquad g \qquad p \rightsquigarrow$ 100 - 200 digits $\qquad$ **Bob:**

a = secret $\qquad$ " some random $\qquad$ " prime # $\qquad$ b = secret.

$$[g^a]_p \longrightarrow [g^a]_p \rightsquigarrow [g^a]_p^b = [g^{ab}]_p$$

$$[g^b]_p^a \rightsquigarrow [g^b]_p \longleftarrow [g^b]_p$$

$$[g^b]_p^a = [g^{ab}]_p$$

1976 "Diffie-Hellman"

"public key alg."