# Math 321

Q's RSA $\quad C = M^e \bmod n$

$M = C^d \bmod n$

$119 = 7 \cdot 17 \rightarrow m = 6 \cdot 16 = 96$

$\gcd(96, 5) \qquad 1 = (1)(96) + (-19)(5)$

$1 \bmod 96 = (-19)(5) \bmod 96$

$\boxed{-19} \cdot 5 \equiv 1 \bmod 96$

$\boxed{-19} = d$

$-19 \equiv (-19 + (n)96) \bmod 96$

$d = -19 + 96 = \boxed{77}$

# 17 p. 344 $\qquad |ASCII| = 128$

5 characters. '@' at least once.

$|\text{exactly } 1| + |\text{exactly } 2| + \cdots + |\text{exactly } 5|$

$5(127^4) + \qquad + \qquad (1)$

$10(127^3) \rightarrow$ @ @ $\square$ _ _

@ _ @ _ _

@ _ _ @ _

@ _ _ _ @

_ @ @ _ _

$$|\text{all}| = |\text{exactly } \emptyset| + \underbrace{|\text{exactly } 1| + \cdots + |\text{exactly } 5|}_{\text{want!}}$$

$$|\text{all}| - |\text{exactly } \emptyset \text{ @'s}| = \text{want!}$$

$$\boxed{128^5 - 127^5}$$

5.2

Pigeonhole principle!

if you have $K$ boxes.

$b_1$ $b_2$ ... $b_K$

if you then have $N$ objects, $N > K$, to put in the boxes then at least one box will have two or more objects.

Generalized version

thm: if $N$ objects are placed into $K$ boxes, then at least one box contains at least $\lceil N/K \rceil$ objects.

ex: 6 boxes and 3 objects.

at least one box has at least $\lceil 3/6 \rceil = 1$ object.

or

one or more boxes have one or more objects.

ex 6 boxes and 49 objects.

one or more boxes have $\lceil \frac{49}{6} \rceil = 9$ objects

ex given 6 numbers when divided by 5 I know 2 or more will have same remainder.

When you divide by 5 $r = \{0, 1, 2, 3, 4\}$

$|r| = 5$

box = same remainder $\rightarrow$ $|\text{box}| = 5$
object = number $\rightarrow$ $|\text{objects}| = 6$

$\rightarrow$ by pigeonhole principle 2 or more numbers have same remainder.

ex

$M_1 = \frac{a+b}{2}$ $\quad$ $a+b$


midpt: $\frac{a+b}{2}$

want $\frac{a+b}{2} \in \mathbb{Z} \to \frac{a+b}{2} = K \to a+b = \overbrace{2K}^{\text{even}}$

ok.. $a, b$ have same parity (even, even) or (odd, odd)

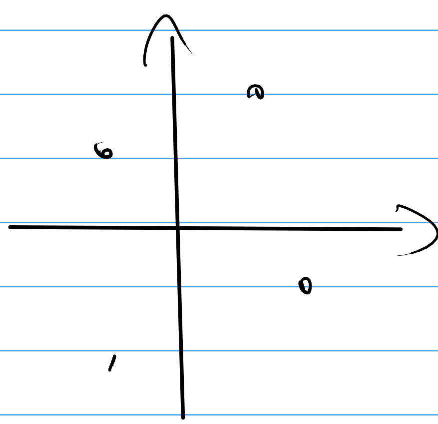
$\to a+b$ is even!

Problem: how many integer points are needed to have an integer midpoint.

$|\text{objects}| = \boxed{3}$ b/c boxes = parity
objects = numbers

$|\text{parity}| = 2$

2D



$M = \left( \frac{x_1+x_2}{2}, \frac{y_1+y_2}{2} \right)$

(o, e) $\quad$ (e, o)

(o, o) $\quad$ (e, e)