Math 451

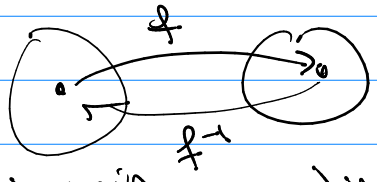
Number Theory / Cryptography

one-to-one and onto

f is an invertable function

Sets: integers

$\ldots, -4, -3, -2, -1, 0, 1, 2, 3, \ldots$



rules: ops $+, -, \times$, sharing (fair)

(tries to)

$\frac{5}{2} = 2.5$ 2 divides 5

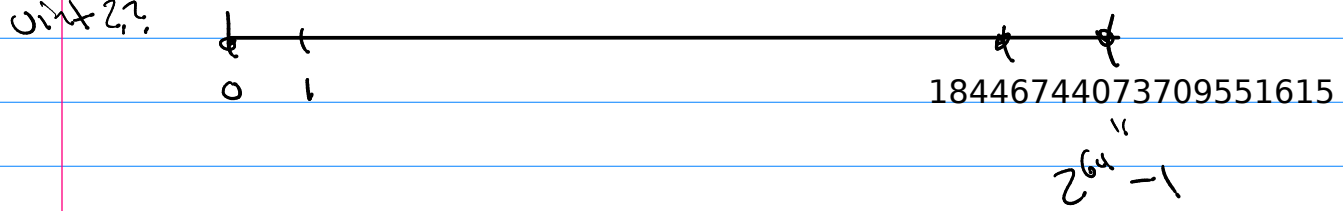
2 divides

sharing

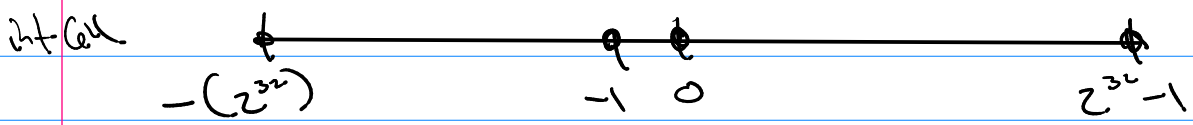
Octave / Matlab int64, uint64

$2^{64} = 18{,}446{,}744{,}073{,}709{,}551{,}616$

uint 2.2:



int 64



---

divides → Division algorithm

Does d divide a fairly?

$$\boxed{a = q \cdot d + r}$$

d is a pos.

$0 \le r < d$

(ex) 5 divides 16 → $16 = 3 \cdot 5 + 1$ No

(ex) 5 divides 20 → $20 = 4 \cdot 5 + 0$ Yes

$$a = q\,d + r$$

q: div, r: mod

div(a,d) = q
mod(a,d) = r
] function [q r] = div_mod(a,d)

Floating point ops. div_mod?

function [q r] = div_mod(a,d) $0 \le r < d$

q = floor(a/d); $\lfloor a/d \rfloor$ $\lfloor q + r/d \rfloor$ $\lfloor a/d \rfloor$

r = a - q*d;

end

(2.5) div_mod with only loops +, −, *