Math 321

Modulus

New idea for "same"

a "is the same as" b

have the same remainder when divided by m.

$a \equiv b \pmod{m}$

congruent.

Def:

① $a \bmod m = b \bmod m$

② $m \mid a-b$ — same as $a-b = m \cdot k$

③ $a = b + mk$ for an integer k.

p. 209 (11) $r = a \bmod m = b \bmod m \rightarrow \boxed{a \equiv b \pmod{m}}$

Means $m \mid a-b$

Pf: (direct)

for $a \bmod m$ we use the division algorithm

$a = m \cdot q_1 + (a \bmod m) = \boxed{mq_1 + r}$

& $b \bmod m \rightarrow b = m \cdot q_2 + (b \bmod m) = \boxed{mq_2 + r}$

So $a - b = (mq_1 + r) - (mq_2 + r) = m(q_1 - q_2)$

Showed $(a-b) = m \cdot (q_1 - q_2)$

by def of divides $m \mid (a-b)$

$\rightarrow$ $a \equiv b \pmod{m}$ by def.

Stuff to know

(1) $p \mid T$ same as $T = p \cdot e$

(2) $a \equiv b \pmod{m}$ same as

(1) $m \mid a-b$
(2) $a \bmod m = b \bmod m$
(3) $a = b + km$ for int. k.

(3) $a = b \cdot q + r$

Properties:

Th^{m}: $a \equiv b \pmod{m}$ $\wedge$ $c \equiv d \pmod{m}$

then

(1) $a + c \equiv b + d \pmod{m}$

(2) $ac \equiv bd \pmod{m}$

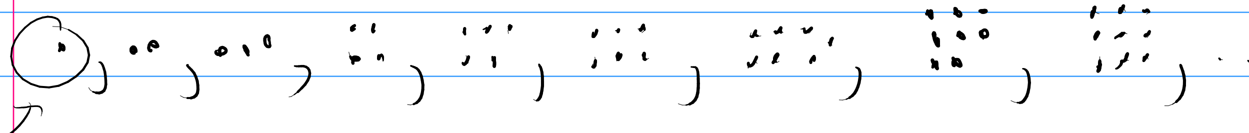
Cor: ① $(a+b) \bmod n = (a \bmod n + b \bmod n) \bmod n$

② $(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$

3.5

$p \mid T$ same as $T = p \cdot c$

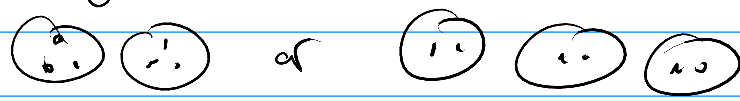
Can you break T into equal shares?



ignore 1 it is obvious that for all n..

$1 \mid n$ and $n \mid n$

what about other group sizes? ..

ex: 6 

Def: $p \geq 2$ is prime if it only has 1 and p as factors.
if a number is not prime we call it composite.

Sieve of Eratosthenes

~~1~~, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~
11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~
~~21~~, ~~22~~, 23, ~~24~~, ~~25~~ ...

So.. how many primes?

thm: (Fund. thm of Arithmetic)

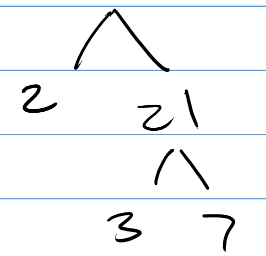
Every positive integer ≥ 2 is a prime or a unique product of primes written in non-dec. order.

ex

$8 = 2 \cdot 2 \cdot 2$

$12 = 2 \cdot 2 \cdot 3$

$42 = 2 \cdot 3 \cdot 7$



Finding Prime Factors.

thm: if n is composite $\rightarrow$ it has a prime divisor $\leq \sqrt{n}$

pf: if $(n = a \cdot b \quad 2 \leq a \leq n-1 \quad b \geq 2)$

$\rightarrow (a \leq \sqrt{n} \text{ or } b \leq \sqrt{n})$

by Contradiction:

$(n = a \cdot b) \wedge \underbrace{(a > \sqrt{n} \wedge b > \sqrt{n})}$

$a \cdot b > \sqrt{n}\sqrt{n} = n$

$a \cdot b > n$

Contradiction!

How many primes?

Thm: there are infinitely many primes.

Pf: (by contradiction)

assume primes are finite.

$P = \{p_1, p_2, p_3, \ldots, p_n\}$ are all primes.

consider $(p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1) = Q$