DEF: For an integer n, n is prime means $n > 1$ and $\forall d \in \mathbb{Z}, d>0 \wedge d \mid n \rightarrow d = 1 \vee d = n$

only positive divisors are 1 and n

n is composite means $n > 1$ and $\exists s,t \in \mathbb{Z}$ s.t. $s \neq 1 \wedge t \neq 1 \wedge n = s \cdot t$

1, 3
3 is prime

1, 37
37 is prime T

6 is composite T
1, 2, 3, 6

111 is composite T
1, 3, 37, 111

0 is composite F
(not > 1)

1 is neither prime nor composite
(also not > 1)

THM: For any prime p, and $a \in \mathbb{Z}$, if $p \mid a$, then $p \nmid a+1$.

Proof: Suppose p is prime and $a \in \mathbb{Z}$ and $p \mid a$. [want $p \nmid a+1$]

Suppose $p \mid a+1$ [goal: contradiction]

We have $p \mid -a$ (prev thm with $c = -1$)

$a + b = a + (-b)$

and so $p \mid (a+1)+-a$ i.o.w. $p \mid 1$ (prev thm $a \mid b \wedge a \mid c \rightarrow a \mid b+c$)

and $p \leq 1$ (prev thm $a, b > 0$ $a \mid b \rightarrow a \leq b$)

but $p > 1$ (def prime)

$\Rightarrow\Leftarrow$

So $p \mid a+1 \rightarrow c$

$\therefore p \nmid a+1$ (contradiction rule)

THM: For all integers $n \geq 2$, there is some prime p s.t. $p \mid n$

$3300 = 10 \cdot 330$

3300
10 330
2 5

$n \mid 10$ $10 \mid 3300$

THM: There are an infinite number of primes

Every finite list of primes is incomplete such that there is a prime not on the list.

Proof: Suppose $p_1, p_2, \ldots, p_k$ is a finite list of all primes. (need: a prime not on that list)

Let $a = p_1 \cdot p_2 \cdot \cdots \cdot p_k$

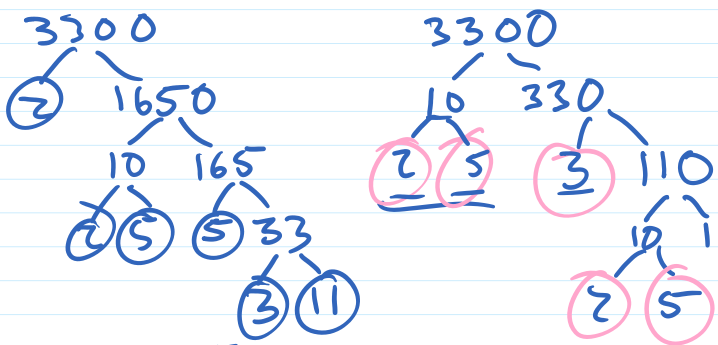
Note $p_i \mid a$ for all $1 \le i \le k$ $\quad a = p_i \cdot \underbrace{(p_1 \cdot \cdots \cdot p_{i-1} \cdot p_{i+1} \cdot \cdots \cdot p_k)}_{\text{integer b/c all } p_i \in \mathbb{Z} \text{ and } \mathbb{Z} \text{ closed under } \cdot}$

So $p_i \nmid a+1$ for all $1 \le i \le k$ (prev. thm)

$a+1 \ge 2$ so there is a prime p s.t. $p \mid a+1$ (prev thm)

$p \ne p_i$ for all $1 \le i \le k$ b/c $p \mid a+1$ and $p_i \nmid a+1$

So p is prime not on list $p_1, \ldots, p_k$



$2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$3300 = 2 \cdot 5 \cdot 330$

$= 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$3300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$= 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$= 1 \cdot 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11$

$\vdots$

Unique prime factorization (Fundamental Thm of Arithmetic)

THM: For all integers $n \ge 2$, there is some list of primes $p_1, \ldots, p_k$ s.t. $n = p_1 \cdot p_2 \cdot \cdots \cdot p_k$ and $p_1 \le p_2 \le \cdots \le p_k$ and that list is unique.

a is congruent to b modulo n $-(a-b)=b-a$

DEF: For any integer $n \geq 2$, and any $a,b \in \mathbb{Z}$, $a \equiv b \pmod{n}$ means $n \mid a-b$
"modulus"

a, b have same remainder when divided by modulus (n)

$10 \mid 1643729415\underset{\mathbb{Z}}{0}$

$10 \mid 1643729417\underset{\mathbb{Z}}{0}$

$16437294167 \equiv 17 \pmod{10}$ 27 1467 7 −3

$467 \equiv 5 \pmod{11}$

$-43 \equiv 2 \pmod{3}$ 5 8 101

$-3 = -1\cdot 10 + 7$ (3)

$467 = 42\cdot 11 + \underset{\mathbb{Z}}{5}$

n is even $n \equiv 0 \pmod{2}$ $2 \mid n-0$

n is odd $n \equiv 1 \pmod{2}$ $2 \mid n-1$

$-43 = -45 + 2 = -15\cdot 3 + 2$

THM: For any integer $n \geq 2$ and any integer m, $m \equiv 0 \pmod{n}$ iff

QRT for $\equiv \pmod{n}$

THM: For any integer $n \geq 2$ and any integer m, there is a unique integer r such that
$m \equiv r \pmod{n}$
and $0 \leq r < n$

Proof: Let $n \geq 2$, $m \in \mathbb{Z}$.
By QRT, there is a unique q, r s.t. $m = q\cdot n + r$ and $0 \leq r < n$

That r is the unique r s.t. $m \equiv r \pmod{n}$

THM: For any integer $n \geq 2$ and any integers a,b,c,d, if $a \equiv b \pmod{n}$
and $c \equiv d \pmod{n}$
then $a+c \equiv b+d \pmod{n}$
and $a\cdot c \equiv b\cdot d \pmod{n}$

Suppose $n \geq 2$ and $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

Then $n \mid a-b$ and $n \mid c-d$ by def of $\equiv$ [want $n \mid a+c-(b+d)$]

and so $n \mid (a-b)+(c-d)$ by thm where $(a-b)+(c-d) = (a+c)-(b+d)$

and $n \mid (a+c)-(b+d)$ by sub and by def $\equiv$ $a+c \equiv b+d \pmod{n}$

Find k s.t. $467 + 96001948 + (-99) \equiv k \pmod{10}$

$467 \equiv 7 \pmod{10}$ $7 + 8 + (-9) \equiv k \pmod{10}$

$96001948 \equiv 8 \pmod{10}$ $6 \equiv k \pmod{10}$

$-99 \equiv -9 \pmod{10}$ $6 = k$

$10 \mid (-99-(-9))$ $10 \mid (-99-1)$

$10 \mid -90$ $10 \mid -100$

$3^{12} = 3^4\cdot 3^4\cdot 3^4$

$18 \equiv 3 \pmod{5}$ $5 \mid 18-3$ $18^{12} \equiv 3^{12} \pmod{5}$

$\vdots$ $\equiv 1 \pmod{5}$

$18 \equiv 3 \pmod{5}$

$3^4 = 81$

$81 \equiv 1 \pmod{5}$

$81 \equiv 1$

$\vdots$

$18 \equiv 3 \pmod 5$

$18^{12} \equiv 3^{12} \pmod 5$

$\equiv 1 \pmod 5$

$3^4 = 81$

$81 \equiv 1 \pmod 5$

$81 \equiv 1$

$81 \equiv 1$

if n^2 is even n is even

THM: For any integer n, if $n^2 \equiv 0 \pmod 2$ then $n \equiv 0 \pmod 2$

THM: For any integer n, if $n^2 \equiv 0 \pmod 3$ then $n \equiv 0 \pmod 3$

DEF: For integers a,b not both 0, the greatest common divisor of a and b is the largest positive d s.t. $d \mid a$ and $d \mid b$

$\gcd(6, 21) = 3$

$\gcd(28, 144) = 4$

$\gcd(24616, 15678) = 2$

$24616 = 2\cdot 2\cdot 2\cdot 17\cdot 181$ $\qquad$ $15678 = 2\cdot 3\cdot 3\cdot 13\cdot 67$

$\gcd(1040279, 1034273) =$ ___

$1040279 = 1007\cdot 1031$

THM: For any integers a,b,q,r, if $b\neq 0$ and $a = b\cdot q + r$, then $\gcd(a,b) = \gcd(b, r)$

gives Euclidean algorithm for computing $\gcd(a,b)$:

compute $q = a \text{ div } b$

$r = a \bmod b$

repeat with new $a = b$, new $b = r$ until new $b = r = 0$

$\gcd(24616, 15678) = \gcd(15678, 8938)$ $\qquad$ $24616 = 1\cdot 15678 + 8938$

$= \gcd(8938, 6740)$ $\qquad$ $15678 = 1\cdot 8938 + 6740$

$= \gcd(6740, 2198)$ $\qquad$ $8938 = 1\cdot 6740 + 2198$

$= \gcd(2198, 146)$ $\qquad$ $6740 = 3\cdot 2198 + 146$

$= \gcd(146, 8)$ $\qquad$ $2198 = 15\cdot 146 + 8$

$= \gcd(8, 2)$ $\qquad$ $146 = 18\cdot 8 + 2$

$= \gcd(2, 0)$ $\qquad$ $8 = 4\cdot 2 + 0$

$= 2$

Proof: Let a,b,q,r be integers such that $b\neq 0$ and $a = b\cdot q + r$.

We show a) $\qquad$ to come Feb 14 ♡

and b)

and therefore $\gcd(a,b) = \gcd(q,r)$