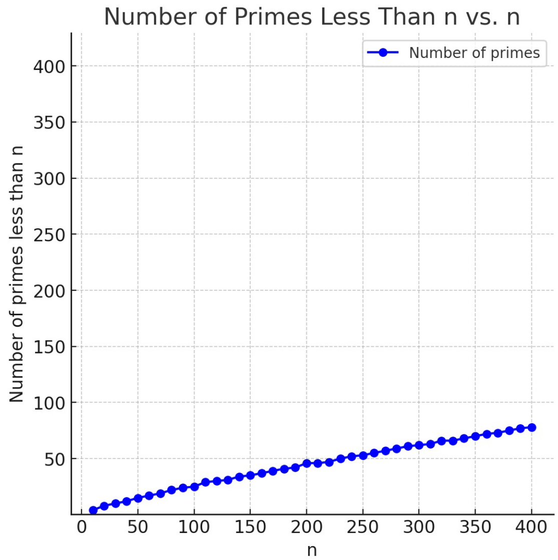
Finish Ch. 3 : Euclid + Prime :
Start Ch 4 :

Main Goal: Great Theorem : There are an ∞ # of prime numbers.



Tool # 1 (theorem) If $a|b$ & $a|c$ then $a|(b-c)$

Ex

$a = 14$ know $a|b$, $a|c$

$b = 28$ $14|28$ & $14|42$

$c = 42$ $28 = n \cdot 14$ & $42 = m \cdot 14$

$d = 140$ verify : $14|(42-28) = 14|14$

$14|28$, $14|140 \Rightarrow 14|(140-28)$

$\Rightarrow 14|112$ true

$112 = 14 \cdot 8$

proof $a|b \Rightarrow b = a \cdot n$

$a|c \Rightarrow c = a \cdot m$

So $b - c = a \cdot n - a \cdot m = a(n-m)$

$\Rightarrow b - c =$ multiple of a

$a|(b-c)$

Tool # 2 : Fundamental Theorem of Arithmetic : Every positive whole number factors uniquely into a product of primes

prime decomposition :

- $10 = 2 \cdot 5$
- $73 = 1 \cdot 73$
- $136 = 2 \cdot 68 = 2 \cdot 2 \cdot 34 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 17 = 2^3 \cdot 17$

(eg ① show we can factor into primes
└ Euclidean Alg.

② unique

$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$
$\Updownarrow$
$n = q_1 \cdot q_2 \cdot \ldots \cdot q_\ell$

thm: $\exists$ an ∞ # of primes

proof:

these are all the prime #'s

Assume that $\exists$ only k many primes, $\underbrace{2, 3, 5, 7, 11, \ldots, P_k}$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad P_1 \; P_2 \; P_3, \ldots \; P_k$

Form a number multiply every prime together, then add 1

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot P_k + 1.$$

$12 = 2 \cdot 6$

$\Rightarrow 2$ divides 12

Apply F.T.A. to the number n.

$$n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot P_k + 1 = P_i \cdot P_j \cdot P_l \cdot \ldots \cdot P_m$$

where the P_*'s are some of the primes above

$$= P_1 \cdot P_2 \cdot P_3 \cdot P_4 \cdot \ldots \cdot P_k + 1 = P_2 P_5 \cdot P_{19} \cdot \ldots \cdot P_{25}$$

Some P_* prime divides n., say, (by renaming) $P_i \mid n$.

e.g., $P_2 \mid n$ but P_2 also divides $P_1 \cdot P_2 \cdot P_3 \cdot \ldots \cdot P_k$.

By tool #1.

since $P_2 \mid n$ & $P_2 \mid n-1 \Rightarrow P_2 \mid (n-(n-1)) = P_2 \mid 1$ $\otimes$

since by def. a prime is > 1.

Next Homework TIPS

Let's color all primes : blue or magenta :

Blue: If p = multiple of 4, plus 1

$p = 4k+1$

1

Blue

5, 9

$5 \cdot 9 = 45$

$$\begin{array}{r} 11 \\ 4\overline{)45} \\ \underline{44} \\ 1 \end{array}$$

$(4k_1+1)(4k_2+1)$

$= 4k_3+1$

Magenta: $P = 4k+3 = 4k-1$

$19 = 4(4)+3 = 4k+3$

$$\begin{array}{r} 4 \\ 4\overline{)19} \\ \underline{16} \\ 3 \end{array}$$

7 is also Magenta

$19 \cdot 7 = 70 + 63 = 133$

$$\begin{array}{r} 33 \\ 4\overline{)133} \\ \underline{12} \\ 13 \\ \underline{12} \\ 1 \end{array}$$

$(4k_1+3)(4k_2+3) \neq 4k_3+3$

$16k_3 + 12k_1 + 12k_2 + 9$

$9 = 4 \cdot 2 + 1$

$4(M)+1$