Math 4460
1/25/23

Proposition: Let $z, a, b, x, y \in \mathbb{Z}$ with $z \neq 0$.

If $z \mid a$ and $z \mid b$, then $z \mid (xa + yb)$.

proof: Suppose $z \mid a$ and $z \mid b$.

Then, $a = zk$ and $b = zh$ where $k, h \in \mathbb{Z}$

So,

$$\begin{aligned} xa + yb &= x(zk) + y(zh) \\ &= z[xk + yh]. \end{aligned} \qquad (*)$$

Since $x, k, y, h \in \mathbb{Z}$ we know $xk + yh \in \mathbb{Z}$

Thus, hence, ergo we know by $(*)$ that $z \mid (xa + yb)$.

Theorem: Let $n \in \mathbb{Z}$, with $n \geq 2$.

Then, n can be written as the product of one or more primes.

$\boxed{\text{Ex:}}$

$12 = 2 \cdot 2 \cdot 3$ ← product of 3 primes

$11 = 11$ ← product of 1 prime

Proof of theorem: We will use strong/complete induction.

Let $S(n)$ be the statement

"n can written as the product of one or more primes"

When $n=2$, the statement $S(2)$ is true since 2 is the product of one prime.

Let $k \in \mathbb{Z}$ with $k > 2$.
And assume $S(n)$ is true for all $2 \leq n < k$. induction hypothesis

Ex: If $k=6$, you'd be assuming $\underbrace{2, 3, 4, 5}_{2 \leq n < k}$ all factor into one or more primes.

Goal: Show $S(k)$ is true.

Case 1: Suppose k is prime.
Then k is the product of one prime.
So, $S(k)$ is true.

Case 2: Suppose k is not prime.

Then there must exist a positive divisor a of k where $2 \le a < k$ [ie where $a \ne 1, a \ne k$]

So, $k = ab$ where b is also a positive integer.

Note: $b \ne 1$ since if $b = 1$, that would imply $a = k$. And, $b \ne k$, since $b = k$ would imply $a = 1$.

So, $2 \le b < k$.

Since $2 \le a < k$ and $2 \le b < k$ by the inductive hypothesis $S(a)$ and $S(b)$ are both true.

Thus, $a = p_1 p_2 \cdots p_r$ and $b = q_1 q_2 \cdots q_s$

where p_i, q_j are primes and $r \geqslant 1, s \geqslant 1$.

Therefore,

$$k = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$$

can be written as the product of one or more primes.

So, $S(k)$ is true.

By the magical powers of induction $S(n)$ is true for all $n \geq 2$

Magical Induction Proof

Lemma: Let $x, y, z \in \mathbb{Z}$ with $x \neq 0$.
If $x \mid y$ and $x \mid (y+z)$, then $x \mid z$.

proof:
Since $x \mid y$ we know $y = xk$ where $k \in \mathbb{Z}$.
Since $x \mid (y+z)$ we know $y + z = xm$ where $m \in \mathbb{Z}$.
Thus,

$$z = xm - y = xm - xk = x(m-k)$$

Since $m, k \in \mathbb{Z}$ we know $m - k \in \mathbb{Z}$.
Thus, since $z = x(m-k)$ we know $x \mid z$.

$\blacksquare$

Theorem (Euclid)

There are infinitely many primes.

Proof by contradiction:

Suppose there were only a finite number of primes.

Call them $p_1, p_2, \ldots, p_r$

Let $N = p_1 p_2 \cdots p_r + 1$

Ex: If there were only $r=3$ primes then $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and

$N = p_1 p_2 p_3 + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$

Note: $2 \nmid 31$, $3 \nmid 31$, $5 \nmid 31$

By the earlier theorem from today N can be written as the product of one or more primes.

So there must exist a prime that divides N.

Suppose $p_i \mid N$ where $1 \leq i \leq r$

One of the primes from the list of primes

So, $p_i \mid (\underbrace{p_1 p_2 \cdots p_r + 1}_{N})$

But also $p_i \mid \underbrace{p_1 p_2 \cdots p_r}_{p_i \text{ is in here}}$.

By our lemma we must have $p_i \mid 1$.

So, $p_i = \pm 1$.

This is impossible since p_i is prime.

Contradiction.

Thus, there exist an infinite # of primes.

$\boxed{\text{EUCLID}}$

Answer to class question

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30{,}031$$
$$= 59 \cdot 509$$

Another method [for fun, not on any test]

One can show

$$\sum_{\substack{2 \leq p \leq N \\ p \text{ prime}}} \frac{1}{p} > \log(\log(N)) - 1$$

$$\boxed{\text{Ex: } N=6, \quad \frac{1}{2}+\frac{1}{3}+\frac{1}{5} > \log(\log(6))-1}$$

So if you let $N \to \infty$ then

$$\lim_{N\to\infty} \sum_{\substack{2 \leq p \leq N \\ p \text{ prime}}} \frac{1}{p} > \lim_{N\to\infty} \left[\log(\log(N)) - 1\right] = \infty$$

So, $\displaystyle\sum_{\substack{p \text{ is} \\ \text{prime}}} \frac{1}{p}$ diverges.

So, there must be an infinite # of primes otherwise the sum would converge.

Reference: "An introduction to the theory of numbers" by Niven, Zuckerman, Montgomery

How are the primes spaced out?

2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13,
14, 15, 16, 17, 18, 19, 20, 21, 22,
23, 24, 25, 26, 27, 28, 29, 30, 31,
32, 33, 34, 35, 36, 37, 38, 39,
40, 41, 42, 43, 44, 45, 46, 47,
48, 49, 50, 51, 52, 53, 54, 55, 56,
57, 58, 59, 60, 61, 62, 63, 64, 65,
66, 67, 68, 69, 70, 71, 72, 73, 74,
75, 76, 77, 78, 79, 80, 81, 82,
83, 84, 85, 86, 87, 88, 89, 90,
91, 92, 93, 94, 95, 96, 97,
98, 99, 100, 101, ...