Instructions: We'll use the same whiteboard process until, as a whole class, we decide to use some other process.

Rachel Lander
@hip_fun_mathgrl

Therapist: and what do we say when we don't know the answer

Mathematicians: the proof is trivial and left as an exercise for the reader?

Therapist: no

This is not prime number related, but I think it fits because this is proofs course. Rachel's other tweets are pretty funny too.

1) There's midway anonymous evaluation posted on the "deadlines" document. If you'd like to give feedback about the course, I'd appreciate it.

2) Homework 3 solution posted under Week 3 folder.

3) Break-out room links are posted on the "deadlines" document and will be valid forever (I mean until the end of time, or the end of Google, or the end of this course).

Theorem 1 fill in the blanks

Theorem 1: Every integer $n \geq 2$ is either a prime or can be written as a product of primes.

proof: We will use a proof by strong induction to prove this result.

(Show the first statement in induction is true.)
Note that $n = 2$ is a prime, so the statement is true for $n = 2$.

Now we assume the statement is true for all integers $\ell \geq 2$ up to k, i.e. that every ℓ is either a prime or a product of primes. We will show that $k + 1$ is also a prime or a product of primes. If $k + 1$ is prime, we are done. Suppose not, then there exists a factor e of $k + 1$ such that $1 < e < k + 1$. Let $f = \frac{k+1}{e}$. Then $1 < f < k + 1$ as well. Therefore, by the inductive assumption, each of e, f is either a prime, or a product of primes. Therefore $k + 1 = e \cdot f$ is either a product of two primes, or product of three or more primes. Hence, $k+1$ is a prime or a product of primes, and the statement is true for $k+1$.

This proves that every $n \geq 2$ is either a prime or a product of primes. □

1

Since $\gcd(a,b)$ divides both a, b, $\gcd(a,b) = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ with $0 \leq r_i \leq \alpha_i, 0 \leq r_i \leq \beta_i$ by Theorem 3. Therefore $0 \leq r_i \leq \min\{\alpha_i, \beta_i\}$. This means that $\gcd(a,b)$ divides $\prod_i p_i^{\min(\alpha_i,\beta_i)}$. Note that $\prod p_i^{\min(\alpha_i,\beta_i)}$ also divides both a, b by Theorem 3, therefore, it must equal $\gcd(a,b)$.

A similar proof works for lcm by noting that a, b both divide $\prod p_i^{\max(\alpha_i,\beta_i)}$ and that $\prod p_i^{\max(\alpha_i,\beta_i)}$ divides any number that is divisible by both a, b.

2 a and b

n is congruent to 3 mod 4.

For every p_i, n is congruent to p_i-1 (mod p_i). Since n is not congruent to 0 (mod p_i) for any p_i, no p_i divides n.

Nick

2 c

UPDATED

$$n = 4 p_1 p_2 \cdots p_r - 1$$

First 2 does not divide n because its an odd number

Second 3 does not divide n because 3 is 3 mod 4, so it is one of the p's so n+1 is a multiple of 3 and not n

Cian

2 d

Consider a prime p that divides n. Then $p \neq 2$ and $p \neq 4k+3$ by parts a-c. Since every odd prime is congruent to 1 or 3 mod 4, that leaves us with the fact that all primes that divide n are congruent to 1 mod 4. Then their product will also be congruent to 1 mod 4, since $1 \cdot 1 \equiv 1 \pmod 4$. But $n \equiv 3 \pmod 4$, which is a contradiction.

Extra question to think about: Can we modify the proof of "infinitely many primes of the form 4k+3" to prove "infinitely many primes of the form 4k+1"?

If yes, write the proof here. If no, explain why not.

If we try to repeat the same process as in the previous problem, we would have to claim "All primes that divide n are of the form 4k+3, but their product is 1 mod 4, contradiction."

But two numbers congruent to 3 mod 4 can have a product congruent to 1 mod 4 (3*3=1 (mod4)), so no contradiction.

We will see a different proof for this later (if time permits).

Last page