1

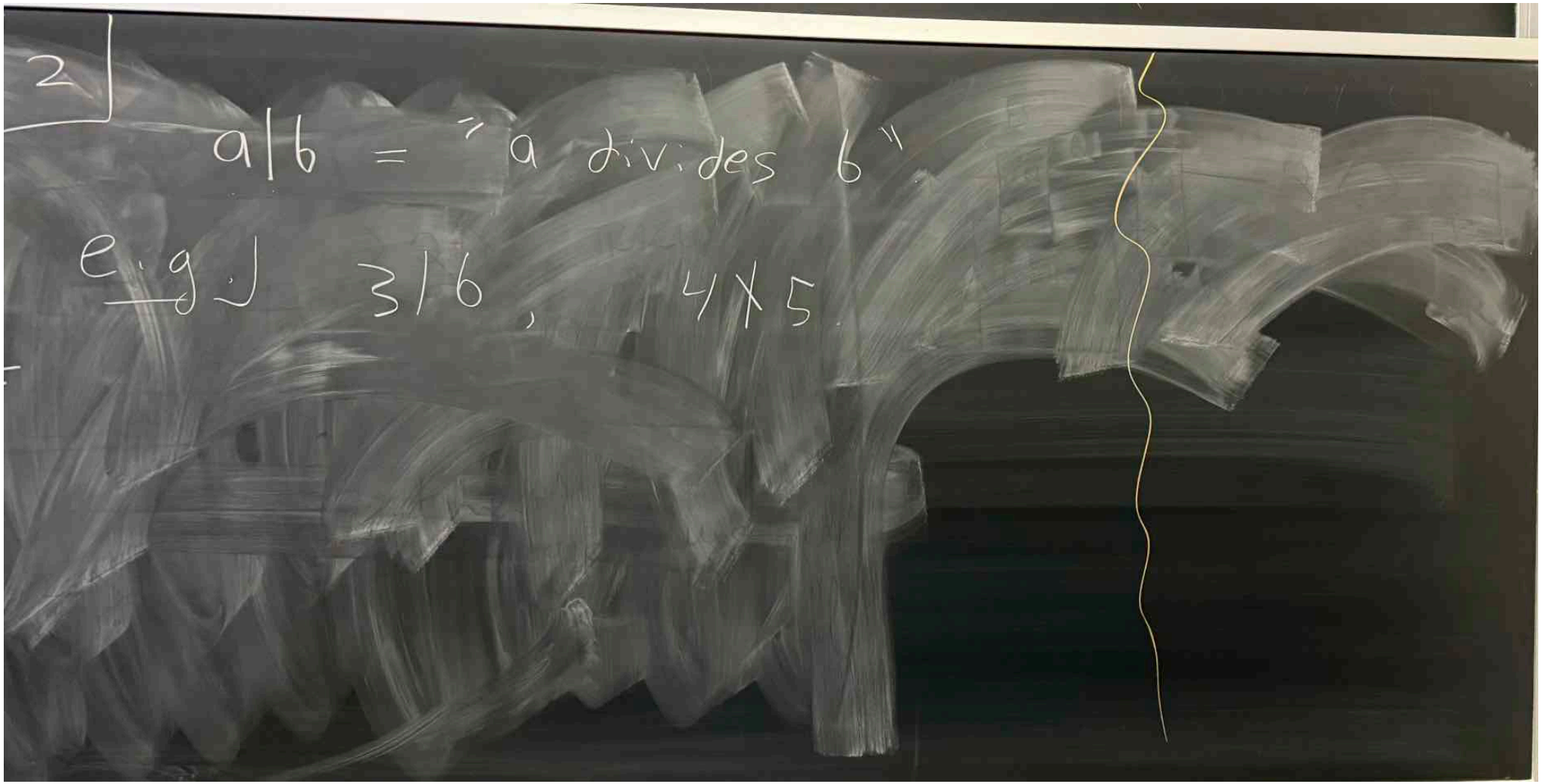
Notation:

$\mathbb{N} = \{0, 1, 2, \dots\}$

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}\}$

$\mathbb{R}$ = real numbers $= \{\dots, e, \pi, -\sqrt{2}, 3, \dots\}$


2
a|b = "a divides b"
e.g. 3|6, 4|5

1 Number theory: what is it?

In short: Number theory is the study of $\mathbb{Z}$.

e.g.
- ("Easy") **Thm** (Legendre): Every $X \in \mathbb{N}$ is a sum of four squares.
- (Very hard) **Thm** (Wiles, Taylor–Wiles, ...): The equation $x^n + y^n = z^n$ has no non-trivial solutions w/ $x, y, z \in \mathbb{Z}$.
- ("Impossible") **Conjecture** (Riemann hypothesis): The function $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ has no non-trivial zeros.

A **Conjecture** is a statement of expected mathematical fact for which no proof is known

4] Conj: The function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ has no non-trivial zeros.

A conjecture is a precise math statement w/o proof

2 Primes

Definition: A prime is a Positive integer whose positive divisors are 1 and itself.

$a|b \iff b = a \cdot c$, $a|0 \quad 0 = 0 \cdot a$

Proposition: If p and q are primes and $p|q$, then $p=q$.

Proof: The only positive divisors of q are 1 and q as q is prime. But, p is a positive divisor of q. So, $p=1$ or $p=q$. But, $p \neq 1$ so $p=q$. ∎

A proposition is a statement of mathematical fact "less important" than a theorem

Remark: Prop 1 could have been a lemma.

7

Proposition: If p and q are primes that are one apart, then they are (up to relabeling) 2 and 3.

Pf: Assume that p and $q = p+1$ are primes. One of p or $p+1$ is even. But this means $2 \mid p$ or $2 \mid p+1$. As p and $p+1$ are primes!

8) this implies $p=2$ or $p+1=2$.
If $p+1=2$, then $p=1$, but 1 is not a prime. So, $p=2$ and $p+1=3$. ∎

A Conjecture is a precise math statement w/o proof

Thm (Euclid): The set $\mathbb{P}$ is infinite.

Pf: We will show that for any finite list of primes $p_1, \dots, p_m$ there is a prime p not in this list.

Set $N = p_1 \cdots p_m + 1$. We consider two cases:

Case 1: N is prime.

In this case $p = N$ is an example, as $N > p_i$ for all i.

Case 2: N is not prime.

Then $S = \{d \in \mathbb{N} : d \mid N \text{ and } 1 < d < N\}$ is non-empty.

Remark: Formatting can greatly impact readability of proofs

By LIP, S has a minimal element d_0.

Claim 1: d_0 is prime.

Pf: Suppose not. Then there is some k $d_0' < d_0$ dividing d_0. But, since $d_0 | N$ we deduce $d_0' | N$. So, $d_0' \in S$. But this then contradicts that d_0 is minimal element of S. ▨

Claim 2: $d_0 \neq p_i$ for any i.

Pf: If $d_0 = p_i$, then $p_i | N = p_1 \cdots p_m + 1$. But as p_i divides $p_1 \cdots p_m$ we see $p_i | (N - p_1 \cdots p_m) = 1$. As $p_i > 0$ this implies $p_i = 1$. This is a contradiction ▨

Claim:

Pf:

formatting helpful way to break up long proofs

Thus, in either case 1 or case 2 we've produced such a p (i.e., $p = N$ or $p = d_0$), as desired. ∎