Announcements

- The peer editing assignment is due in class on April 4 (Tuesday).
- No office hour on March 31 (Friday) or April 3 (Monday). I will be away from campus.

The integers are more complicated than they seem

Two famous unsolved problems about prime numbers:

- Goldbach's conjecture: Every even integer greater than 2 can be expressed as the sum of two prime numbers. True or false? Examples: $12 = 5 + 7$, $20 = 3 + 17 = 7 + 13$.
- Twin prime conjecture: There are infinitely many prime numbers p for which $p + 2$ is prime too. True or false? Examples: $17 + 2 = 19$, $29 + 2 = 31$.

Algebraic properties of the integers

$\mathbb{Z}$ has two binary operations (plus and times) that are commutative and associative, and multiplication distributes over addition; there is an additive identity 0, and every element has an additive inverse; there is a multiplicative identity 1 (but not every element has a multiplicative inverse).

These properties are Axioms A1 to A8 on pages 151–152.

Are there other number systems that satisfy these properties? Yes, the rational numbers $\mathbb{Q}$ satisfy these properties and more: every nonzero element has a multiplicative inverse.

Example of a deduction from the algebraic axioms

Interaction of the additive identity with multiplication: $e \cdot b = e$ for every element b, where e is the additive identity element.

Proof.

$a + e = a$ for every element a, by definition of additive identity. In particular, $e + e = e$.
Then $(e + e) \cdot b = e \cdot b$.
By the distributive property, $e \cdot b = (e \cdot b) + (e \cdot b)$.
Add the additive inverse of $e \cdot b$ to both sides:
$-(e \cdot b) + (e \cdot b) = -(e \cdot b) + ((e \cdot b) + (e \cdot b))$.
By the associative property and the definition of additive inverse, $e = e + (e \cdot b)$. Then by the definition of additive identity, $e = e \cdot b$. □