Announcements

- The final draft of the paper is due today in eCampus.
- The last class meeting is Thursday, April 27.
- The final exam is Thursday, May 4, from 3:00 to 5:00 in the afternoon, in this room. The exam covers
  - Chapters 1–4, and
  - Sections 5.1–5.4.

  As usual, please bring your own paper to the exam.
- Next week, I will hold my usual office hour on Monday and Wednesday afternoons from 2:00 to 3:00.

Unique factorization of integers

Theorem

Every positive integer can be written as a product of prime numbers. The product is unique up to reordering the factors.

Proof of existence, by contradiction, using induction.

Seeking a contradiction, suppose there is some positive integer that cannot be written as a product of primes.
Then there is a least such integer, say m.
Now $m \neq 1$, for 1 equals the empty product!
And m cannot be a prime number, for then m would be the product of a single prime.
So there are positive integers a and b less than m such that the composite integer m equals the product ab.
By the minimality of m, both a and b can be written as products of prime numbers.
So their product m can be written as a product of primes. □

The uniqueness part of the theorem

Proof by contradiction.

If some positive integer can be written in two distinct ways as a product of primes, then there is a least such integer, say m. So

$$m = \prod_{j=1}^{k} p_j = \prod_{\ell=1}^{n} q_\ell$$

for prime numbers $p_1, \ldots, p_k$ and $q_1, \ldots, q_n$.

Since p_1 divides the product $\prod_{\ell=1}^{n} q_\ell$, and p_1 is prime, p_1 must divide one of the factors q_ℓ. But q_ℓ is prime too, so q_ℓ must equal p_1.

Dividing both products by this common factor p_1 contradicts the minimality of m. □

Greatest common divisor revisited

Example

Find the gcd of 256 and 220.

Solution (our old method)

$$
\begin{aligned}
256 &= 220 + 36 \\
220 &= 6 \times 36 + 4 \\
36 &= 9 \times 4
\end{aligned}
$$

so $\gcd(256, 220) = 4$.

Solution (a new method, using unique factorization)

$256 = 2^8$ and $220 = 2^2 \times 5 \times 11$, so $\gcd(256, 220) = 2^2$.