Prime Factorization

Every integer \( > 1 \) factors uniquely into a weakly decreasing sequence of primes.

Unique Prime Factorization

Example:
\[
61394323221 = 53 \cdot 37 \cdot 37 \cdot 37 \cdot 11 \cdot 11 \cdot 7 \cdot 3 \cdot 3 \cdot 3
\]

Prime Divisibility

Lemma: \( p \) prime and \( p \mid ab \) implies \( p \mid a \) or \( p \mid b \)

pf: say not \( (p \mid a) \), so \( \gcd(p,a) = 1 \)
so, \( sa + tp = 1 b \)
\[
pl \quad pl \quad so \quad pl
\]
QED
**Prime Divisibility**

**Cor:** If $p$ is prime, and $p | a_1 \cdot a_2 \cdots a_m$ then $p | a_i$ for some $i$.

**pf:** by induction on $m$.

---

**Unique Prime Factorization**

Every integer $n > 1$ has a unique factorization into primes: $p_1 \cdots p_k = n$ with $p_1 \geq p_2 \geq \cdots \geq p_k$

**pf:**

Suppose not. Choose smallest $n > 1$:

$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$

$p_1 \geq p_2 \geq \cdots \geq p_k$

$q_1 \geq q_2 \geq \cdots \geq q_m$

If $q_1 = p_1$, then $p_2 \cdots p_k = q_2 \cdots q_m$ is smaller nonunique.

So can assume $q_1 > p_1 \geq p_i$
Unique Prime Factorization

pf: but $q_1|n = p_1 \cdot p_2 \cdots p_k$

so $q_1|p_i$ for some $i$ by Cor,

contradicting that $q_1 > p_i$

QED