Prime factorization

Peter Mayr

CU, Discrete Math, March 20 & 30, 2020

Finally we'll realize our longterm goal of proving:

The Fundamental Theorem of Arithmetic

Every integer > 1 can be written as a product of primes in a unique way.

First we generalize **Euclid's Lemma** from 2 to n factors.

Lemma

Let $n \in \mathbb{N}, a_1, \ldots, a_n \in \mathbb{Z}$, p prime.
If $p | a_1 \cdots a_n$, then $p | a_i$ for some $i \in \{1, \ldots, n\}$.

Proof (by induction on n)

- **Basis step, $n = 1$:** $p | a_1$ and the statement is true.
- **Induction hypothesis:** For a fixed $k \in \mathbb{N}$, if $p | a_1 \cdots a_k$, then $p | a_i$ for some $i \in \{1, \ldots, k\}$.
- **Induction step:** Show the statement follows for $n = k + 1$.
  Assume $p | \underbrace{a_1 \cdots a_k}_{=b} a_{k+1}$.

  By Euclid's Lemma, $p | b$ or $p | a_{k+1}$.
  - If $p | b$, then $p | a_i$ for some $i \in \{1, \ldots, k\}$ by the induction assumption.
  - Else $p | a_{k+1}$.

  In any case $p | a_1$ or $p | a_2$ or $\ldots$ $p | a_k$ or $p | a_{k+1}$. The induction step is proved and so is the Lemma. $\square$

If induction is not strong enough for you any more ...

Theorem
Statement S_n is true for all $n \in \mathbb{N}$.

Proof by strong (complete) induction.

1. **basis step:** Show S_1.
2. **inductive step:** Show $S_1 \wedge \cdots \wedge S_k \Rightarrow S_{k+1}$ for any $k \in \mathbb{N}$.

The only difference to usual induction is that you are allowed to use the

- **induction assumption:** all $S_1, \ldots, S_k$ hold

for proving the induction step.

Example

Which postage values can be obtained with stamps for \$3 and \$7?

Exactly the values of the form

$$n = 3x + 7y \text{ for } x, y \in \mathbb{N}_0$$

- **Base cases.** $n = 3, 6, 7, 9, 10, 12, 13, 14, \ldots$ can be obtained.
- **Conjecture.** All $n \geq 12$ can be obtained.
  We prove this conjecture by strong induction using the base cases above.
- **Assumption for strong induction.** All numbers between 12 and some fixed $k \geq 14$ can be obtained.
- **Induction step.** Show $k + 1$ can be obtained.
  $k - 2$ is ≥ 12 and can be obtained by induction assumption.
  So $k + 1 = (k - 2) + 3$ can.

Note. To get the statement for $k + 1$, it's no use that we have it for k. Hence we need **strong induction.**

Fundamental Theorem of Arithmetic.

1. Every integer $n > 1$ has a factorization into primes

$$n = p_1 p_2 \cdots p_k.$$

Proof of 1. by strong induction on n.

- **Basis step:** $n = 2$ is prime (product of a single prime).
- **Induction assumption:** For fixed $n \in \mathbb{N}$ all numbers $\leq n$ are products of primes.
- **Inductive step:** Show $n + 1$ is a product of primes.
  Case, $n + 1$ prime: $n + 1$ is the product of a single prime.
  Case, $n + 1$ not prime: Then $n + 1 = ab$ for some $1 < a, b < n + 1$. By the (strong) induction assumption

$$a = p_1 \cdots p_k, \qquad b = q_1 \cdots q_\ell$$

  for some primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$.
  Now $n + 1 = p_1 \cdots p_k q_1 \cdots q_\ell$ is also a product of primes. $\square$

Fundamental Theorem of Arithmetic.

1. Every integer $n > 1$ has a factorization into primes
$$n = p_1 p_2 \cdots p_k.$$
2. This prime factorization of n is unique up to ordering. That is, if
$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$
for primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$, then $k = \ell$ and $(p_1, \ldots, p_k)$ is a permutation of $(q_1, \ldots, q_k)$.

Example

$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2 \cdot 3 \cdot 5 \cdot 2$$

Same primes, different order.

Fundamental Theorem of Arithmetic.

2. If
$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$
for primes $p_1, \ldots, p_k, q_1, \ldots, q_\ell$, then $k = \ell$ and $(p_1, \ldots, p_k)$ is a permutation of $(q_1, \ldots, q_k)$.

Proof of 2. by minimal counterexample.

Suppose 2. is false. Then there is some counterexample. Since $\mathbb{N}$ is well-ordered, there must be a minimal (smallest) counterexample n. Note $n > 2$ because 2 can be written as a product of primes in only one way.

Proof of 2. continued

Recall n is minimal such that

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

for primes $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ that are not permutations of each other.

- Since $p_1 | q_1 q_2 \cdots q_\ell$, by Euclid's Lemma $p_1 | q_i$ for some i.
- Since q_i is prime, $p_1 = q_i$.
- Dividing by p_1 yields

$$\frac{n}{p_1} = p_2 \cdots p_k = q_1 q_2 \cdots q_{i-1} q_{i+1} \cdots q_\ell.$$

- $p_2, \ldots, p_k$ and $q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_\ell$ are **not** permutations of each (else $p_1, \ldots, p_k$ and $q_1, \ldots, q_\ell$ would be as well).
- $\frac{n}{p_1}$ is a counterexample for 2. that is smaller than n.

But n was the smallest counterexample. Contradiction!
There is no smallest counterexample (no counterexample at all).

Item 2. of the Fundamental Theorem was proved by a special version of a proof by contradiction combined with induction:

Proof by minimal (smallest) counterexample. To show that a statement S_n is true for every $n \in \mathbb{N}$:

- **basis step:** Show S_1.
- Suppose $k > 1$ is smallest such that S_k is false. Show that there exists some smaller $\ell < k$ such that S_ℓ is false.

An application of prime factorizations

Find common divisors of

$$\begin{aligned} a = \quad & 2^2 \cdot 3^1 \cdot 5^3 \\ b = \quad & 2^3 \cdot 3^0 \cdot 5^1 \\ & 2^2 \cdot 3^0 \cdot 5^1 \quad \text{divides } a, b, \text{ in fact is } \gcd(a, b) \end{aligned}$$

Let $p_1 = 2, p_2 = 3, p_3, \ldots$ be the list of all primes.
Fundamental Theorem of Arithmetic: every $a \in \mathbb{N}$ has a unique form

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \ldots$$

with almost all exponents $e_i \in \mathbb{N}_0$ equal to 0.

Lemma

Let $a = \prod_{i \in \mathbb{N}} p_i^{e_i}, b = \prod_{i \in \mathbb{N}} p_i^{f_i}$ with $e_i, f_i \in \mathbb{N}_0$ for all $i \in \mathbb{N}$. Then

1. $\gcd(a, b) = \prod_{i \in \mathbb{N}} p_i^{\min(e_i, f_i)}$,
2. $\operatorname{lcm}(a, b) = \prod_{i \in \mathbb{N}} p_i^{\max(e_i, f_i)}$,
3. $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof of 1.

Clearly $\prod_{i\in\mathbb{N}} p_i^{\min(e_i,f_i)}$ divides $a = \prod_{i\in\mathbb{N}} p_i^{e_i}$ and $b = \prod_{i\in\mathbb{N}} p_i^{f_i}$.
We show that it is the **greatest** common divisor.

- Assume $d = \prod_{i\in\mathbb{N}} p_i^{g_i}$ is some divisor of a and b.
- Let $i \in \mathbb{N}$ and $g_i \geq 1$. Note that p_i does not divide $\frac{a}{p_i^{e_i}}$ by the Fundamental Theorem of Arithmetic.
- Then $p_i^{g_i}$ cannot divide $\frac{a}{p_i^{e_i}}$.
- Since $p_i^{g_i} | a$, we then get $p_i^{g_i} | p_i^{e_i}$ and $g_i \leq e_i$.
  Note that this holds for $g_i = 0$ as well.
- Similarly $g_i \leq f_i$.
- Hence $g_i \leq \min(e_i, f_i)$.

Hence for any common divisor d of a and b we have

$$d \leq \prod_{i\in\mathbb{N}} p_i^{\min(e_i,f_i)}$$

and the latter is the $\gcd(a, b)$.