1. Let \( n = \prod p_i^{a_i} \) denote the prime factorization of \( n \). If \( n \) is prime, then \( n = p^1 \) for some prime \( p \).

2. Suppose \( p \) is prime, \( a, b \in \mathbb{N} \) and \( q = \gcd(a, p) \). Then \( q \mid p \) if and only if \( q = 1 \) or \( q = p \). That is: either \( p \mid a \) or \( a \) is relatively prime to \( p \).

3. Facts (well-known and often covered in 347): Every integer \( n \geq 2 \) can be written in a unique way as

\[ n = \prod p_i^{a_i}, \quad \text{where} \quad a_i \geq 0 \quad \text{and} \quad p_i \text{ are primes} \]

4. We use the notation \( \ell_p(n) \) to denote the power of a prime \( p \) that divides \( n \). For example, if \( n = 345 = 3 \cdot 5 \cdot 23 \), then \( \ell_3(345) = 1, \ell_5(345) = 1, \ell_{23}(345) = 1 \), and \( \ell_2(345) = 0 \).

In this notation, \( n = \prod p_i^{\ell_p(n)} \).

5. By the usual laws of algebra and the unique factorization theorem (often called the Fundamental Theorem of Arithmetic), we observe that

\[ \ell_p(mn) = \ell_p(m) + \ell_p(n) \]

for all primes \( p \).

6. It follows from (5) that \( a \mid b \iff \ell_p(a) \leq \ell_p(b) \) for all primes \( p \).
7. Suppose \( m = \prod_{i=1}^{k} p_i^{a_i}, \quad n = \prod_{i=1}^{k} p_i^{b_i}, \) where \( a_i \geq 0, b_i \geq 0. \)

If \( q = \prod_{i=1}^{r} p_i^{c_i}, \) then \( q \mid m \) and \( q \mid n \) if and only if \( c_i \leq a_i \) and \( c_i \leq b_i \).

That is,

\[ q \mid m \iff c_i \leq \min(a_i, b_i), \quad 1 \leq i \leq m. \]

Put another way,

\[ \text{gcd}(m, n) = \prod_{i=1}^{r} \min(a_i, b_i). \]

8. Theorem: If \( \text{gcd}(a, c) = 1 \) and \( \text{gcd}(b, c) = 1 \), then \( \text{gcd}(ab, c) = 1. \)

Proof 1:

Note that \( \text{gcd}(a, c) = 1 \) means that any prime \( p \) that divides \( c \) cannot divide \( a \), and \( \text{gcd}(b, c) = 1 \) means that any prime \( p \) that divides \( c \) cannot divide \( b \). If \( p \) is a prime dividing \( ab \), then \( p \) divides \( ab \) or \( p \) divides \( c \), so \( p \) cannot be a prime dividing \( c \).

Proof 2 (Non-Conceptual)

There exist integers \( r, s \) so that \( ar + cs = 1 \) and integers \( t, u \) so that \( bt + cu = 1. \) So,

\[ ar + cs = 1 \Rightarrow arb + csb = b \quad \text{and} \quad bt + cu = 1 \Rightarrow (arb + csb) t + cu = 1 \Rightarrow arb + csb + t = 1 \Rightarrow (ab)(rt) + c(sbt + u) = 1. \]

9. The Euler phi function \( \phi(n) \) is defined to be the number of integers \( \alpha \), \( 0 < \alpha < n \) for which \( \text{gcd}(\alpha, n) = 1. \)

Example:

\[ \phi(4) = 2: \quad \text{gcd}(1, 4) = \text{gcd}(3, 4) = 1, \quad \text{gcd}(2, 4) = 2 \geq 1 \]

\[ \phi(8) = 4: \quad \text{gcd}(1, 8) = \text{gcd}(3, 8) = \text{gcd}(5, 8) = \text{gcd}(7, 8) = 1 \]

\[ \phi(14) = 6: \quad \text{gcd}(1, 14) = 1, \text{ gcd}(3, 14) = 1, \text{ gcd}(5, 14) = 1, \text{ gcd}(7, 14) = 1, \text{ gcd}(9, 14) = 1, \text{ gcd}(11, 14) = 1 \]
10. Suppose \( p \) is prime and \( m > 1 \). We can compute \( \phi(p^m) \) directly. How can \( \phi(p^m) \) be greater than 1? Then \( g | p^m \), which means that \( g \) is a power of \( p \). Thus, \( \gcd(a, p^m) > 1 \iff p | a \).

How many multiples of \( p \) are there \( \leq p^m \)?

- \( a = p \cdot b \)
- \( 0 \leq a < p^m \iff 0 \leq p b < p^m \iff 0 \leq b < p^{m-1} \)

So there are \( p^{m-1} \) multiples of \( p \). Hence, \( \phi(p^m) = p^m - p^{m-1} \).

We have \( 4 = 2^2, \phi(4) = 2^2 - 2^1 = 2 \); \( 8 = 2^3, \phi(8) = 2^3 - 2^2 = 4 \).

The last page. Here's another one: \( 9 = 3^2 \).

- \( a = 0, 1, 2, 3, 4, 5, 6, 7, 8 \).
- I've crossed out the multiples \( \geq 3 \times 3 \), so \( \phi(9) = 3^2 - 3 = 6 \).

11. Suppose \( \gcd(m, n) = 1 \). We claim that \( \phi(mn) = \phi(m)\phi(n) \).

This is a sketch of the proof. We use the Chinese Remainder Theorem, and the fact that \( \gcd(a, mn) = 1 \iff \gcd(a, m) = 1 \iff \phi(a, m) = 1 \). (Why is this fact true? In one direction, \( a \) has no primes (common with \( n \).) In the other, if \( \gcd(a, mn) = 1 \) then \( a \) has no primes (common with \( n \).)"

I have crossed out common factors of 5 and common factors of 6 (diagonal). What's left is 1, 7, 13, 19, 11, 17, 23, 29: \( \phi(30) = \phi(5)\phi(6) = 4 \).