Other Results from Strayer

These results are covered in the readings from Elementary Number Theory *by James K. Strayer in Spring 2024, and referenced in these notes. All of the results in this section are standard elementary number theory and presented without proof.*

Axiom 1 (Well Ordering Principle)**.** *Every nonempty set of positive integers contains a least element.*

Divisibility facts

Lemma (Proposition 1.2)**.** *Let* $a, b, c, d \in \mathbb{Z}$*. If* $c \mid a$ *and* $c \mid d$*, then* $c \mid ma + nb$*.*

Proposition (Proposition 1.10)**.** *Let* $a, b \in \mathbb{Z}$ *with* $(a, b) = d$*. Then* $(\frac{a}{d}, \frac{b}{d}) = 1$*.*

Lemma (Lemma 1.12)**.** *If* $a, b \in \mathbb{Z}$*,* $a \geq b > 0$*, and* $a = bq + r$ *with* $q, r \in |Z$*, then* $(a, b) = (b, r)$*.*

Prime facts

Lemma (Lemma 1.14)**.** *Let* $a, b, p \in \mathbb{Z}$ *with* p *prime. If* $p \mid ab$*, then* $p \mid a$ *or* $p \mid b$*.*

Corollary (Corollary 1.15)**.** *Let* $a_1, a_2, \ldots, a_n, p \in \mathbb{Z}$ *with* p *prime. If* $p \mid a_1 a_2 \cdots a_n$*, then* $p \mid a_i$ *for some* i*.*

Proposition (Proposition 1.17)**.** *Let* $a, b \in \mathbb{Z}$ *with* $a, b > 1$*. Write* $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ *and* $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ *where* $p_1, p_2, \ldots, p_n$ *are distinct primes and* $a_1, a_2 \cdots, a_n, b_1, b_2, \cdots, b_n$ *are nonnegative integers (possibly zero). Then*

$$(a, b) = p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2\}} \cdots p_n^{\min\{a_n, b_n\}}$$

and

$$[a, b] = p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_n^{\max\{a_n, b_n\}}.$$

Theorem (Theorem 1.19)**.** *Let* $a, b \in \mathbb{Z}$ *with* $a, b > 0$*. Then* $(a, b)[a, b] = ab$*.*

Congruences

Proposition (Proposition 2.5)**.** *Let* $a, b, c, m \in \mathbb{Z}$ *with* $m > 0$*. Then* $ca \equiv cb \pmod{m}$ *if and only if* $a \equiv b \pmod{\frac{m}{(a,m)}}$*.*

Lemma (Chapter 2, Exercise 9)**.** *Let* $a, b, c, m \in \mathbb{Z}$ *with* $m > 0$*. If* $a \equiv b \pmod{m}$ *then* $ac \equiv bc \pmod{mc}$ *for* $c > 0$*.*

Corollary (Corollary 2.15)**.** *Let* p *be a prime number and let* $a \in \mathbb{Z}$*. Then* $a^p \equiv a \pmod{p}$*.*

Learning outcomes:

Author(s): Claire Merriman

The Euler Phi-Function

Theorem (Theorem 3.3)**.** *Let p be prime and let $a \in \mathbb{Z}$ with $a > 0$. Then $\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)$.*