Chapter 4 Properties of the Integers: Mathematical Induction

§ 4.4 The Greatest Common Divisor: The Euclidean Algorithm (2)

Slides for a Course Based on the Text
Discrete & Combinatorial Mathematics (5th Edition)
by Ralph P. Grimaldi

(c) Fall 2018, Justie Su-Tzu Juan
EX 4.36: Def: \( \forall x, y \in \mathbb{Z}^+, x \mod y = \) the remainder after \( x \) is divided by \( y \).

ex: \( 7 \mod 3 = 1; \ 18 \mod 5 = 3 \).

ex: \( a = 168, \ b = 456 \):

\[
\begin{align*}
 r_0 &= 168 \quad \text{and} \\
 d_0 &= 456. \\
 \therefore \ r &> 0 \\
 \therefore \ c_1 &= 456, \ d_1 = 168, \\
 r_1 &= 456 \mod 168 = 120 > 0; \\
 c_2 &= 168, \ d_2 = 120, \\
 r_2 &= 168 \mod 120 = 48 > 0; \\
 c_3 &= 120, \ d_3 = 48, \\
 r_3 &= 120 \mod 48 = 24 > 0; \\
 c_4 &= 48, \ d_4 = 24, \\
 r_4 &= 48 \mod 24 = 0. \\
 \therefore \ \gcd(a, b) &= 24 (= d_4 ).
\end{align*}
\]
EX 4.37 : 2 containers : 17 ounces and 55 ounces. How to use this two containers to measure exactly one ounce?

\[
\begin{align*}
\text{(一盎司} &= 0.283494 \text{ kg} \quad 17 \rightarrow 4.8 \text{ kg} \quad 55 \rightarrow 15.6 \text{ kg})
\end{align*}
\]

Sol.

\[
\begin{align*}
55 &= 3 \times 17 + 4, \quad 0 < 4 < 17 \\
17 &= 4 \times 4 + 1, \quad 0 < 1 < 4 \\
\Rightarrow 1 &= 17 - 4 \times 4 = 17 - 4 \times [55 - 3 \times 17] \\
&= 13 \times 17 - 4 \times 55.
\end{align*}
\]

\[\therefore\text{ 小的装13次，逐次倒至大的；}
\]

\[\text{清掉大的4次，最终会只剩 1 ounce.}\]
EX 4.38: Debug a Pascal program in 6 minutes. Debug a C++ program in 10 minutes. Work 104 minutes and doesn’t waste any time. How many programs can he debug in each language?

Sol.

Let \( x, y \in \mathbb{N} \), \( 6x + 10y = 104 \iff 3x + 5y = 52 \)

\[ \therefore \text{gcd}(3, 5) = 1, \text{ and } 3(2) + 5(-1) = 1 \]

\[ \therefore 3(104) + 5(-52) = 52 \]

\[ \Rightarrow 3(104 - 5k) + 5(-52 + 3k) = 52, \forall k \in \mathbb{Z} \]

\[ x = 104 - 5k \geq 0 \text{ and } y = -52 + 3k \geq 0 \]

\[ \Rightarrow 17 + 1/3 = 52/3 \leq k \leq 104/5 = 20 + 4/5 \]

\[ \therefore \exists 3 \text{ possible solution:} \]

a) \((k = 18) : x = 14, y = 2.\]

b) \((k = 19) : x = 9, y = 5.\]

c) \((k = 20) : x = 4, y = 8 .\]

(c) Fall 2018, Justie Su-Tzu Juan
4.4 The Greatest Common Divisor: The Euclidean Algorithm

Thm 4.8: If \( a, b, c \in \mathbb{Z}^+ \), the Diophantine equation \( ax + by = c \) has an integer solution \( x = x_0, y = y_0 \iff \gcd(a, b) | c \).

Def 4.4: \( \forall a, b, c \in \mathbb{Z}^+ \),

1. \( c \) is called a common multiple of \( a, b \equiv a | c \) and \( b | c \).
2. \( c \) is the least common multiple of \( a, b \) \( \text{lcm}(a, b) \equiv \) the smallest of all common multiple of \( a, b \).

EX 4.39: a) \( 12 = 3 \cdot 4 \), \( \therefore \) \( \text{lcm}(3, 4) = 12 = \text{lcm}(4, 3) \).

\( 90 = 6 \cdot 15 \), but \( \text{lcm}(6, 15) \neq 90 \), \( \text{lcm}(6, 15) = 30 \).

b) \( \forall n \in \mathbb{Z}^+ \), \( \text{lcm}(1, n) = \text{lcm}(n, 1) = n \).

c) \( \forall a, n \in \mathbb{Z}^+ \), \( \text{lcm}(a, na) = na \).

d) \( \forall a, m, n \in \mathbb{Z}^+ \), with \( m \leq n \), \( \text{lcm}(a^m, a^n) = a^n \), \( \gcd(a^m, a^n) = a^m \).
§ 4.4 The Greatest Common Divisor : The Euclidean Algorithm

Thm 4.9 : Let \( a, b, c \in \mathbb{Z}^+ \), with \( c = \text{lcm}(a, b) \).

If \( d \) is a common multiple of \( a \) and \( b \), then \( c \mid d \).

Proof.

If not, then by division algorithm, \( d = qc + r \), where \( 0 < r < c \).

\[ \because c = \text{lcm}(a, b), \quad \therefore \exists m \in \mathbb{Z}^+ \text{ s.t. } c = ma, \]

\[ \therefore d \text{ is a common multiple of } a \text{ and } b, \quad \therefore \exists n \in \mathbb{Z}^+ \text{ s.t. } d = na. \]

\[ \Rightarrow na = d = qc + r = qma + r \]

\[ \Rightarrow (n - qm) a = r > 0 \]

\[ \therefore a \mid r. \]

In a similar way, \( b \mid r. \)

\[ \therefore (a \mid r \text{ and } b \mid r) \Rightarrow r \text{ is a common multiple of } a \text{ and } b. \]

but \( 0 < r < c \) \( \iff \) (\( \therefore c \) is the least common multiple of \( a, b \))

Hence \( c \mid d. \)
Thm 4.10 : \( \forall a, b \in \mathbb{Z}^+, ab = \text{lcm}(a, b) \cdot \text{gcd}(a, b) \)

Proof. (reader)

EX 4.40 : a) \( \forall a, b \in \mathbb{Z}^+, \) of \( a, b \) are relatively prime, then \( \text{lcm}(a, b) = ab. \)

b) \( \because \) \( \text{gcd}(168, 456) = 24 \) (by EX 4.36)
\( \therefore \) \( \text{lcm}(168, 456) = (168)(456) / 24 = 3192. \)
Chap 4 Properties the Integers: Mathematical Induction

§ 4.5 The Fundamental Theorem of Arithmetic

Slides for a Course Based on the Text

*Discrete & Combinatorial Mathematics* (5th Edition)

by Ralph P. Grimaldi
Lemma 4.2: If \( a, b \in \mathbb{Z}^+ \) and \( p \) is a prime, \( p \mid ab \Rightarrow p \mid a \text{ or } p \mid b \).

Proof.

If \( p \mid a \), then we are finished.

If \( p \nmid a \): \( \therefore p \) is prime,

\[ \therefore \gcd(p, a) = 1. \] i.e. \( \exists x, y \in \mathbb{Z} \text{ s.t. } px + ay = 1 \).

Then for \( p(bx) + (ab)y = b \):

\[ \therefore p \mid p \wedge p \mid ab, \]
\[ \therefore p \mid p(bx) \wedge p \mid (ab)y. \quad (\text{by Thm 4.3(d)}) \]
\[ \therefore [p(bx) + (ab)y = b] \wedge p \mid p(bx) \wedge p \mid (ab)y, \]
\[ \therefore p \mid b. \quad (\text{by Thm 4.3(e)}) \]

Lemma 4.3: Let \( a_i \in \mathbb{Z}^+, \forall i \in \{1, 2, \ldots, n\} \).

\[ [(p \text{ is prime}) \wedge (p \mid a_1 a_2 \ldots a_n)] \Rightarrow \exists i \in \{1, 2, \ldots, n\}, p \mid a_i. \]

Proof. (reader)
§ 4.5 The Fundamental Theorem of Arithmetic

EX 4.38 : Show that $\sqrt{2}$ is irrational. (Aristotle (384 – 322 B. C.))

Proof. Suppose $\sqrt{2}$ is not irrational. say $\sqrt{2} = \frac{a}{b}$, where $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = 1$.

$\therefore \sqrt{2} = \frac{a}{b}, \therefore 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid a$ (by Lemma 4.2)

Let $a = 2c$ for some $c \in \mathbb{Z}^+$.

$\therefore 2b^2 = a^2, \therefore 2b^2 = 4c^2 \Rightarrow 2c^2 = b^2 \Rightarrow 2 \mid b^2 \Rightarrow 2 \mid b$ (by Lemma 4.2)

$\therefore 2 \mid a \land 2 \mid b \Rightarrow 2 \mid \gcd(a, b), i.e. \gcd(a, b) \geq 2 \rightarrow \leftarrow$

$\therefore \sqrt{2}$ is irrational.

Note : $\sqrt{p}$ is irrational for every prime $p$ (exercise)

Thm 4.11 : The Fundamental Theorem of Arithmetic

$\forall n > 1, n \in \mathbb{Z}^+, n$ can be written as a product of primes uniquely, up to the order of the primes.

(c) Fall 2018, Justie Su-Tzu Juan
\[ \forall n > 1, n \in \mathbb{Z}^+, \text{n can be written as a product of primes uniquely, up to the order of the primes.} \]

### § 4.5 The Fundamental Theorem of Arithmetic

**Proof. (1/3)**

∃: If not exist such product:

Let \( m > 1 \) be the smallest integer

not expressible as a product of primes.

\[ \therefore m \text{ is not a prime,} \quad (\text{o.w. prime is a product of one factor } \rightarrow \leftarrow) \]

\[ \therefore \text{Let } m = m_1 \, m_2, \text{ where } 1 < m_1 \leq m_2 < m. \]

\[ \therefore m_1 < m, \, m_2 < m, \]

\[ \therefore m_1, \, m_2 \text{ can be written as product of primes.} \]

\[ \therefore m = m_1 \, m_2 \]

\[ \therefore \text{we can obtain a prime factorization of } m. \rightarrow \leftarrow \]
Proof. (2/3)

! : Prove by induction on $n$

Let $S(n)$: $n$ have a unique prime factorization

$n = 2$: $S(2)$ is true.

Suppose $n = 2, 3, 4, \ldots, h - 1$, $S(n)$ is true.

Now, consider $n = h$:

Suppose $h = p_1^{s(1)} p_2^{s(2)} \cdots p_k^{s(k)} = q_1^{t(1)} q_2^{t(2)} \cdots q_r^{t(r)}$.

Where $p_i, q_j$ are primes, $\forall \ 1 \leq i \leq k, 1 \leq j \leq r$.

and $p_1 < p_2 < \cdots < p_k$ and $q_1 < q_2 < \cdots < q_r$.

and $s(i) \in \mathbb{Z}^+, t(j) \in \mathbb{Z}^+, \forall \ 1 \leq i \leq k, 1 \leq j \leq r$. 
Proof. (3/3)

\[ p_1 \mid h, \quad \therefore p_1 \mid q_1^{t(1)} q_2^{t(2)} \ldots q_r^{t(r)}. \]

By Lemma 4.3, \( \exists 1 \leq j \leq r, p_1 \mid q_j \).
\[ \therefore p_1, q_j \text{ are primes.} \quad \therefore p_1 = q_j. \]

In the same way,
\[ q_1 \mid h \Rightarrow \exists 1 \leq e \leq k, q_1 = p_e. \]
\[ \Rightarrow p_1 \leq p_e = q_1 \leq q_j = p_1, \quad \therefore e = j = 1, \text{ i.e. } p_1 = q_1. \]

Let \( n_1 = h / p_1 = p_1^{s(1)-1} p_2^{s(2)} \ldots p_k^{s(k)} = q_1^{t(1)-1} q_2^{t(2)} \ldots q_r^{t(r)}. \)
\[ \therefore n_1 < h, \quad \therefore \text{ by I. H.:} \]
\[ k = r, p_i = q_i \quad \forall \ 1 \leq i \leq k, \]
\[ s(1) - 1 = t(1) - 1, \text{ and } s(i) = t(i) \quad \forall \ 2 \leq i \leq k = r. \]
\[ \therefore s(1) - 1 = t(1) - 1 \Rightarrow s(1) = t(1). \]
\[ \Rightarrow \text{ The prime factorization of } h \text{ is unique.} \]
EX 4.39 : Find the prime factorization of 980220.

Sol.

\[
\begin{align*}
2 & \mid 980220 = 2^1 (490110) \\
2 & \mid 490110 = 2^2 (245055) \\
3 & \mid 245055 = 2^2 \cdot 3^1 (81685) \\
5 & \mid 81685 = 2^2 \cdot 3^1 \cdot 5^1 (16337) \\
17 & \mid 16337 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 17^1 (961) \\
31 & \mid 961 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 17^1 \cdot 31^2 \\
31 & \\
\end{align*}
\]
4.5 The Fundamental Theorem of Arithmetic

EX 4.40: Suppose \( n \in \mathbb{Z}^+ \) and
\[
10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n = 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14,
\]
17 \mid n \text{ or not?}

Sol.

\[
\therefore 17 \mid (21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16 \cdot 15 \cdot 14),
\]
\[
\therefore 17 \mid (10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot n).
\]
But 17 \nmid 10, 17 \nmid 9, 17 \nmid 8, 17 \nmid 7, 17 \nmid 6, 17 \nmid 5,
17 \nmid 4, 17 \nmid 3, 17 \nmid 2,
\therefore \text{By Lemma 4.3, } 17 \mid n.
\]
§ 4.5 The Fundamental Theorem of Arithmetic

EX 4.41: For $n \in \mathbb{Z}^+$, Find the number of positive divisors of $n$.

ex: $2 : 1, 2 \sim 2$
    $3 : 1, 3 \sim 2$
    $4 : 1, 2, 4 \sim 3$

Sol.

$\forall n \in \mathbb{Z}^+$, by Thm4.11, let $n = p_1^{e(1)} p_2^{e(2)} \cdots p_k^{e(k)}$,
where $p_i$ is prime $\forall 1 \leq i \leq k$, $e(i) > 0 \ \forall 1 \leq i \leq k$.

If $m \mid n$, then $m = p_1^{f(1)} p_2^{f(2)} \cdots p_k^{f(k)}$
where $0 \leq f(i) \leq e(i), \ \forall 1 \leq i \leq k$.

∴ the number of positive divisors of $n$ is
$(e(1) + 1) (e(2) + 1) \cdots (e(k) + 1)$.
§ 4.5 The Fundamental Theorem of Arithmetic

ex: ① $29338848000 = 2^8 \cdot 3^5 \cdot 5^3 \cdot 7^3 \cdot 11$:
有 $(8 + 1)(5 + 1)(3 + 1)(3 + 1)(1 + 1) = 9 \cdot 6 \cdot 4 \cdot 4 \cdot 2$
$= 1728$ 個 positive divisors.
② 其中有多少個為 $360 = 2^3 \cdot 3^2 \cdot 5$ 的倍數:
it must satisfy: $2^{t(1)} \cdot 3^{t(2)} \cdot 5^{t(3)} \cdot 7^{t(4)} \cdot 11^{t(5)}$ where
$3 \leq t(1) \leq 8$, $2 \leq t(2) \leq 5$, $1 \leq t(3) \leq 3$, $0 \leq t(4) \leq 3$, $0 \leq t(5) \leq 1$
$\Rightarrow [(8 - 3) + 1][(5 - 2) + 1][(3 - 1) + 1][(3 - 0) + 1][(1 - 0) + 1]$
$= 6 \cdot 4 \cdot 3 \cdot 4 \cdot 2 = 576.$
③ 其中有多少個為 perfect square:
it mast satisfy: $2^{s(1)} \cdot 3^{s(2)} \cdot 5^{s(3)} \cdot 7^{s(4)} \cdot 11^{s(5)}$ where
$s(1) = 0, 2, 4, 6, 8$; $s(2) = 0, 2, 4$; $s(3) = 0, 2$; $s(4) = 0, 2$; $s(5) = 0$.
i.e. $(2^2)^{r(1)} \cdot (3^2)^{r(2)} \cdot (5^2)^{r(3)} \cdot (7^2)^{r(4)}$ where
$0 \leq r(1) \leq 4$, $0 \leq r(2) \leq 2$, $0 \leq r(3) \leq 1$, $0 \leq r(4) \leq 1$,
$\Rightarrow 5 \cdot 3 \cdot 2 \cdot 2 \cdot 1 = 60.$
§ 4.5 The Fundamental Theorem of Arithmetic

\[
\text{Def : } (\prod_{i=m}^{n}) = \prod_{i=m}^{n} x_i = x_m \cdot x_{m+1} \cdot \ldots \cdot x_n \text{ where } m, n \in \mathbb{Z}.
\]

\[
i \text{: index, } m \text{: lower limit, } n \text{: upper limit.}
\]

\[n - m + 1 \text{ terms.}\]

\text{ex : } ① \quad \prod_{i=3}^{7} x_i = x_3 \cdot x_4 \cdot x_5 \cdot x_6 \cdot x_7 = \prod_{j=3}^{7} x_j
\]

② \quad \prod_{i=3}^{6} i = 3 \cdot 4 \cdot 5 \cdot 6 = 6! / 2!

③ \quad \prod_{i=m}^{n} i = m (m + 1) (m + 2) \ldots (n - 1) n = \frac{n!}{(m - 1)!}

\forall m, n \in \mathbb{Z}^+ \text{ with } m \leq n.

④ \quad \prod_{i=7}^{11} x_i = x_7 \cdot x_8 \cdot x_9 \cdot x_{10} \cdot x_{11}

= \prod_{j=0}^{4} x_{7+j} = \prod_{j=0}^{4} x_{11-j}

(c) Fall 2018, Justie Su-Tzu Juan
EX 4.42 : \( m, n \in \mathbb{Z}^+ \), let \( m = p_1^{e(1)} p_2^{e(2)} \ldots p_t^{e(t)} \), \( n = p_1^{f(1)} p_2^{f(2)} \ldots p_t^{f(t)} \), where \( p_i \) is prime, \( e(i) \geq 0, f(i) \geq 0 \), \( \forall \ 1 \leq i \leq t \).

Let \( a_i = a(i) = \min\{e(i), f(i)\} \equiv \) the smaller of \( e(i) \) and \( f(i) \), \( \forall \ 1 \leq i \leq t \)

\[ b_i = b(i) = \max\{e(i), f(i)\} \equiv \) the larger of \( e(i) \) and \( f(i) \), \( \forall \ 1 \leq i \leq t \)

then (1) \( \gcd(m, n) = \prod_{i=1}^{t} p_i^{a(i)} \), (2) \( \text{lcm}(m, n) = \prod_{i=1}^{t} p_i^{b(i)} \)

ex : \( m = 491891400 = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^1 \cdot 13^2 \)
\( n = 1138845708 = 2^2 \cdot 3^2 \cdot 7^1 \cdot 11^2 \cdot 13^3 \cdot 17^1 \)

\[ \rightarrow p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 13, p_7 = 17. \]

\[ \rightarrow a_1 = 2, a_2 = 2, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 2, a_7 = 0 \]

\[ \therefore \ \gcd(m, n) = 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 13^2 \cdot 17^0 = 468468. \]

\[ \rightarrow b_1 = 3, b_2 = 3, b_3 = 2, b_4 = 2, b_5 = 2, b_6 = 3, b_7 = 1 \]

\[ \therefore \ \text{lcm}(m, n) = 2^3 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^3 \cdot 17^1 \]
\[ = 1195787993400. \]
§ 4.5 The Fundamental Theorem of Arithmetic

Note: Any two consecutive integers are relatively prime. (HW 19. § 4.4)

EX 4.39 : Can we find three consecutive positive integers whose product is a perfect square?
(i.e. \( \exists m, n \in \mathbb{Z}^+. \text{ s.t. } m(m + 1)(m + 2) = n^2 ? \))

Sol. (1/2)

Suppose \( \exists m, n \in \mathbb{Z}^+, \text{ s.t. } m(m + 1)(m + 2) = n^2. \)

1. \( \therefore \text{gcd}(m, m + 1) = 1 = \text{gcd}(m + 1, m + 2), \)
   \( \therefore \forall \text{ prime } p_i, p_i \mid (m + 1) \Rightarrow p_i \nmid m \text{ and } p_i \nmid (m + 2). \)
   \( \therefore m(m + 1)(m + 2) = n^2, \therefore p_i \mid (m + 1) \Rightarrow p_i \mid n^2. \)
   \( \therefore n^2 \text{ is a perfect square, } \)
   \( \therefore \) the exponents \( t_i \) of \( p_i \) in the prime factorizations of \( n^2 \)
   must be even.
EX 4.39: Can we find three consecutive positive integers whose product is a perfect square? 
(i.e. \( \exists m, n \in \mathbb{Z}^+. \text{ s.t. } m(m + 1)(m + 2) = n^2 \)?)

Sol. (2/2)

\[ \therefore \text{the exponents } t_i \text{ of } p_i \text{ in the prime factorizations of } n^2 \]
\[ \text{must be even.} \]
\[ \therefore m + 1 \text{ is a perfect square.} \]

2. \[ \therefore n^2 = m(m + 1)(m + 2) \text{ and } n^2, m + 1 \text{ are perfect square,} \]
\[ \Rightarrow m(m + 2) \text{ is a perfect square.} \]
\[ \text{but } m^2 < m^2 + 2m = m(m + 2) < m^2 + 2m + 1 = (m + 1)^2 \]
\[ \therefore m(m + 2) \text{ cannot be a perfect square. } \rightarrow \leftarrow \]
\[ \therefore \text{There are no three consecutive positive integer whose product is a perfect square.} \]