C3: Elementary Number Theory & Method of Proof

January 10, 2020

1 Definition

1.1 Even

1. Integer n is even iff $n = 2k$. k is an integer.
2. Divisible by 2
3. n is even $\iff \exists k \ni n = 2k$

1.2 Odd

1. Integer n is odd iff $n = 2k + 1$, k is integer
2. n is odd $\iff \exists k \ni n = 2k + 1$

1.2.1 Example 1

Which of the following is even or odd number?

- If even, write it as 2k;
- if odd, write it as 2k + 1.

1. 0
$$2\left(0\right), even$$
2. 35
$$2\left(17\right) + 1, odd$$
3. $6ab^2$
$$2\left(3ab^2\right), even$$

1.3 Prime

1. Integer n is prime iff $n > 1$, and $\forall \mathbb{Z}^+ r, s$, if $n = rs$, then $r = 1$ OR $s = 1$.
2. An integer n is prime provided that $n > 1$ and the only positive divisors of n are 1 and n
3. Symbolically, $n = prime \iff \exists$ positive integers r, s, if $n = rs$ then $r = 1 \cup s = 1$

1.4 Composite

1. An integer n is composite, iff, $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.
2. Symbolically, n is composite positive integers r and s such that $n = r \cdot s$ and $r \neq 1$ and $s \neq 1$.
3. Every integer greater than 1 is either prime or composite.

1.4.1 Example 2

Write the first 5 prime numbers and composite numbers.

1. Prime: $2, 3, 5, 7, 11$
2. Composite: $4, 6, 8, 9, 10$

1.5 Divisible

If n and d are integers, $d \neq 0$, then n is divisible by d iff, $n = d \cdot k$ for some integer k. Denoted $d|n$, read as "d divides n"

1. $d|n$ also means:
   (a) n is a multiple of d
   (b) d is a factor of n
   (c) d is a divisor of n
   (d) d divides n
2. Symbolically, $d \neq 0$, $d|n \iff \exists$ an integer k such that $n = d \cdot k$.

1.5.1 Example 3

Is 12 divisible by 4?

$$12 = 4 \cdot 3, 3 \in \mathbb{Z}$$

1. Yes, 12 is divisible by 4

1.5.2 Example 4

Which of the following are true and which are false?

1. $3|100$
2. $3|99$
3. $-3|3$
4. $-2|-7$

1.5.3 Note

1. For all integers n and d with $d \neq 0$, $d \nmid n \iff \frac{n}{d}$ is not an integer.

1.6 Rational

- A real number r is rational iff, $r = a|b$ for some integers a and b with $r = a|b$.
- r is rational $\iff \exists$ integers a and b such that $r = a|b$ and $a \neq 0$.

1.7 Irrational

1. Real number, NOT rational.

1.7.1 Example 5

Which of the following are rational numbers?

1. 13/4. Rational
2. $-5/8$. Rational
3. 0.56. Rational
4. 6. Rational
5. 0 . Rational
6. 4/0. Irrational

2 Unique Factorization Theorem

1. For any integer $n > 1$, there exists a positive integer k, distinct prime number $p_1, p_2, ..., p_k$ and positive integers $e^1, e^2, ..., e^k$ such that:
   (a) $n = p_1^{e_1} \cdot p_2^{e_2} \cdot ...p_k^{e_k}$

2. For any other expression of n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

3. To put it simply, for every positive number. You can obtain that figure through the multiplication of prime numbers with different power together.

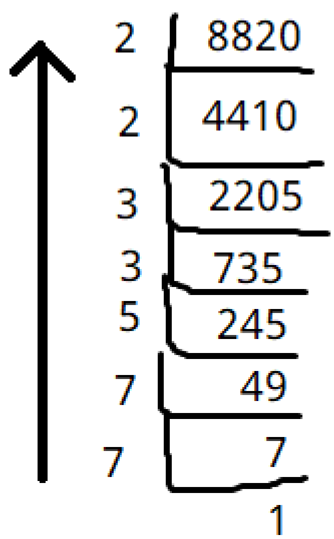
3 Standard Factor Form

1. For any integer $n > 1$, the standard factored form of n is an expression of the form
$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot ... \cdot p_k^{e_k}, k > 0;$$
   (a) $p_1, p_2, ..., p_k$ are prime numbers; $e^1, e^2, ..., e^k$are positive integers; and
$$p_1 > p_2 > \ldots > p_k$$

2. Put it simply, its unique factorization theorem, but the biggest prime numbers comes first.

3.1 Example 6

Write 8,820 in standard factored form

1. 

2. $8820 = 7^2 * 5 * 3^2 * 2^2$

4 Quotient-Remainder Theorem

1. Given any integer n and positive integer d, there evists unique integers q and r such that $n = d \cdot q + r, 0 \leq r < d$
2. Put it simply, any integer can be obtained by $\boldsymbol{n}umber*\boldsymbol{q}uotient+\boldsymbol{r}emainder$ (or $nq + r$).

4.1 Example 7

Find the integers for q and r for the following values of n and d, in the form $n = d \cdot q + r, 0 \leq r < d$

1. $n = 62, d = 4$
$$62 = 4\,(15) + 2$$
2. $n = -62, d = 4$
$$-62 = 4\,(-15) - 2$$
3. $n = 62, d = 80$
$$62 = 80\,(0) + 62$$

5 'div' and 'mod'

1. Given non-negative integer n and positive integer d,
   (a) n div $d =$ the integer quotient obtained when n is divided b y d.
   (b) $n \mod d =$ the integer remainder obtained when n is divided by d.
2. Symbolically, if n and d are positive integers,
   (a) $n \operatorname{div} d = q$
   (b) $n \mod d = r$
3. Put it simply, given any 2 combination of the below, it is possible to find the third value:
   (a) number, n
   (b) divisor, d
   (c) remainder, r

5.1 Example 8

Compute 23 div 6 and 23 mod 6.

1. $23 = 6\,(3) + 5$
   (a) Use the regular division method to find the other terms/
2. $23\text{div}6 = q = 3$
3. $23 \mod 6 = r = 5$

6 Floor

Given any real number x, the floor of x, denoted $\lfloor x \rfloor$, is

$$\lfloor x \rfloor = \text{that unique integer } n \text{ such that } n \leq x < n+1$$

1. Symbolically, if $x =$ real number, n is an integer, then

$$\lfloor x \rfloor = n \iff n \leq x \leq n+1$$

2. To put it simply, the floor of a number is the closest integer below it or equal to it.

7 Ceiling

Given any real number x, the ceiling of x, denoted $\lceil x \rceil$, is

$$\lceil x \rceil = \text{that unique integer } n \text{ such that } n-1 < x \leq n$$

1. Symbolically, if $x =$ real number, n is an integer, then

$$\lfloor x \rfloor = n \iff n-1 < x \leq n$$

2. To put it simply, the ceiling of a number is the closest integer equal to or above it.

7.1 Example 9

Compute the floor and the ceiling for each of the following values of x:

1. $\frac{25}{4}$
   (a) $\lfloor \frac{25}{4} \rfloor = 6$
   (b) $\lceil \frac{25}{4} \rceil = 7$
2. 37.999
   (a) $\lfloor 37.999 \rfloor = 37$
   (b) $\lceil 37.999 \rceil = 38$
3. -3.61
   (a) $\lfloor -3.61 \rfloor = -4$
   (b) $\lceil -3.61 \rceil = -3$

7.2 Example 10

If k is an integer, what are $\lfloor k \rfloor$ and $\lfloor k + \frac{1}{2} \rfloor$

Solution:

1. Suppose k is an integer.
2. Then because k is an integer and $k \leq k < k + 1$,

$$\lfloor k \rfloor = \lfloor k + \frac{1}{2} \rfloor = k$$

8 Methods of Proof

1. **Theorem**: A mathematics declarative statement with a proof
2. **Result:** Generic word for theorem
3. **Fact:** Small theorem
4. **Proposition**: A theorem, bigger than fact, smaller than theorem.

9 Method of direct proof

1. Express that statement to be proved in the form "$\forall x \in D, if\, P\left(x\right), then\, Q\left(x\right)$" (mentally)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (Suppose $x \in D$ and $P(x)$)
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

9.1 Directions for Writing Proofs of Universal Statements

1. Write the theorem to be proved.
2. Clearly mark the beginning of your proof with the word Proof.
3. Make your proof self-contained.
4. Write proofs in complete English sentences.

9.2 Common Mistakes

1. Arguing from examples.
2. Using the same letter to represent two different things.
3. Jumping to conclusion.
4. Begging the question.
5. Misuse of the word if

9.3 Theorem

If the sum of any two integers is even, then so is their difference.

1. Workings
   (a) Let the even integers be m and n. Since they are even integers, added together they should be $2k$.
   (b) Question is $m - n = ?$. We would like to know if $m - n = 2l$, where l is another number.
2. Proof
   (a) Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (Suppose $x \in D$ and $P(x)$)
      i. Suppose m and n are two particular but arbitrarily chosen integers such that $m + n$ is even.
      ii. By definition of even,
      $$m + n = 2k, k \in \mathbb{Z}$$
   (b) Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.
      i. Since the difference of integers is an integer, $l = k - n$ is a integer, and hence, by definition of even, $m - n$ is an even integer $(m - n) = 2l$.
      ii. Therefore, if the sum of any 2 integers is even, then so is their difference.

9.4 Example 11

Prove: For all integers k and l, if k, l are both odd, then $k + l$ is even.

1. Mental calculations

$$\begin{aligned} n &= 2k+1 \\ n^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ &= 2\left(2k^2+2k\right)+1 \\ &= 2m+1\,(odd) \end{aligned}$$

2. Proof
   (a) Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (Suppose $x \in D$ and $P(x)$)
      i. **Suppose** n is a particular but arbitrarily chosen odd integer.
   (b) Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.
      i. **By definition** of odd, $n = 2k+1, k \in \mathbb{Z}$
      ii. Then,

$$\begin{aligned} n^2 &= 4k^2+4k+1 \\ &= 2\left(2k^2+2k\right)+1 \end{aligned}$$

      iii. **Since** the sum of products of integers is an integer, $2k^2+2k$ is an integer, and hence by definition of odd, n^2 is an odd integer.
      iv. **Therefore,** if n is odd, then n^2 is odd.

9.5 Theorem

Every integer is a rational number.

1. Express that statement to be proved in the form "$\forall x \in D, if\, P\left(x\right), then\, Q\left(x\right)$" (mentally)
   (a) Equivalent form: $\forall n \in \mathbb{R}$, if n is an integer, then n is a rational number.
2. Do some mental calculations

$$n = \frac{n}{1}, n \in \mathbb{Z}$$

3. Proof:
   (a) Suppose n is a particular but arbitrarily chosen integer.
   (b) Then $n = \frac{n}{1}, where\, n, 1 \in \mathbb{Z}$
   (c) Since n can be written as a fraction of integers where $1 \neq 0$, hence by definition of rational, n is a rational number.
   (d) Therefore, every integer is a rational number.

9.6 Theorem

The sum of any two rational numbers is rational.

1. Equivalent form:
   (a) If s and r are rational numbers, then $s + r$ is rational.
2. Mental notes:
   (a) $S = \frac{ad}{bd}, R = \frac{bc}{bd}$
   (b) $S + R = \frac{ad+bc}{bd} = \frac{p}{q}$
3. Proof:
   (a) Suppose s and r are particular but arbitrarily chosen rational numbers.
   (b) By definition of rational numbers,

$$\begin{aligned} S &= \frac{a}{b} \ni a, b \in \mathbb{Z}, b \neq 0 \\ r &= \frac{c}{d} \ni c, d \in \mathbb{Z}, d \neq 0 \\ S + r &= \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \\ ad + bc &= \mathbb{Z} \\ bd &\in \mathbb{Z}, \neq 0 \end{aligned}$$

      i. Therefore, $S + r$ is rational

9.7 Theorem: Transitivity of Divisibility

For all integers a, b and c, if a divides b and b divides c, then a divides c.

1. $\frac{b}{a} = k, \frac{c}{d} = l,\ k, l \in \mathbb{Z}$
   (a) $b = ka, c = lb$
   (b) $c = lka$
   (c) $\frac{c}{a} = lk \in \mathbb{Z}$
   (d) $\therefore a$ divides c
2. Proof:
   (a) **Suppose** a**,** b, c are particular, but arbitrary chosen integers such that a divides b and b divides c.
   (b) **By definition** of divisibility,

$$b = ka, c = lb, k, l \in \mathbb{Z}$$

(c) Then $c = (kl)\, a, kl \in \mathbb{Z}$

(d) Since the product of integers is an integer, kl is an integer, and hence by definition of divisibility, a divides c.

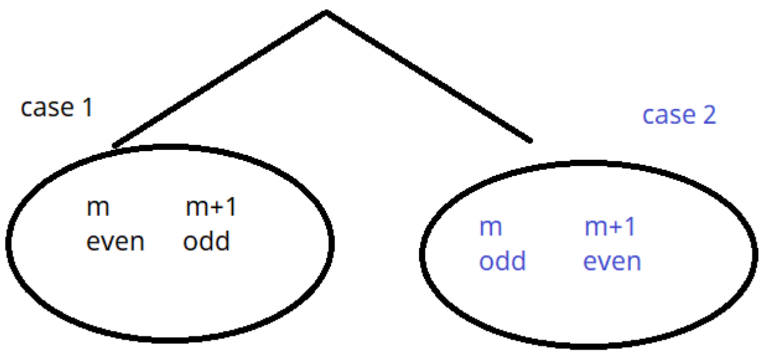
(e) Therefore, for all integers a, b and c, if a divides b and b divides c, then a divides c.

9.8 Theorem

Any two consecutive integers have opposite parity.

$$m, m+1$$

1. Equivalent form: If m is an even (odd) integer, then m + 1 is odd (even).



   (a)

2. Proof:

   (a) Suppose m and $m{+}1$ are particular but arbitrarily chosen consecutive integers.

   (b) By the parity property, m is either odd or even.

   (c) Case 1: If m is even

      i. By definition of even, $m = 2k, k \in \mathbb{Z}$

      ii. Then $m + 1 = 2k + 1$

         A. which is an odd integer.

      iii. Therefore if m is even, then $m + 1$ is odd.

   (d) Case 2: If m is odd

      i. **By definition** of odd, $m = 2k + 1$

      ii. **Then** $m + 1 = 2k + 2 = 2\,(k + 1) = 2l$

      iii. **Since** the sum of integers is an integer, $k + 1$ is an integer and hence by definition of even, $m + 1$ is an even integer.

      iv. **Therefore** if m is odd, then m + 1 is even.

   (e) Regardless of which case actually occurs, either m or m + 1 is even, the other will be an odd integer.

9.9 Theorem

For all real numbers x and all integers m,

$$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$

1. Equivalent form:
   (a) If x is a real number and m is an integer, then
   $$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$
2. Proof:
   (a) **Suppose** x and m are particular but arbitrarily chosen real number and integer, respectively.
   (b) Let $n = \lfloor x \rfloor$. **By definition** of floor
   $$n \leq x < n + 1$$
   (c) **Then** $n + m \leq n + 1 + m = m + n + 1$
   (d) **Since** the sum of integers is an integer, $m + n$ is an integer and hence by definition of floor, $\lfloor x + m \rfloor = n + m$.
   (e) However $n = \lfloor x \rfloor$, **hence** by substitution,
   $$\lfloor x + m \rfloor = \lfloor x \rfloor + m$$

9.10 Theorem

For any integer n,

$$\lfloor \frac{n}{2} \rfloor = \begin{cases} \frac{n}{2} & \text{, if n is even } (= 2k) \\ \frac{n-1}{2} & \text{, if n is odd } (= 2k+1) \end{cases}$$

1. Proof:
   (a) **Suppose** n is a particular but arbitrarily chosen integer.
   (b) Case 1: If n is even.
      i. **By definition** of even, $n = 2k, k \in \mathbb{Z}$
      ii. Then $\lfloor \frac{n}{2} \rfloor = \lfloor \frac{2k}{2} \rfloor = \lfloor k \rfloor = k$
      iii. Since $n = 2k$, so $k = \frac{n}{2}$
      iv. Therefore $\lfloor \frac{n}{2} \rfloor = \frac{n}{2}$
   (c) Case 2: If n is odd.
      i. By definition of odd, $n = 2k + 1, k \in \mathbb{Z}$
      ii. Then $\lfloor \frac{n}{2} \rfloor = \lfloor \frac{2k+1}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = k$
      iii. Since $n = 2k + 1$, so $k = \frac{n-1}{2}$
      iv. Therefore $\lfloor \frac{n}{2} \rfloor = \frac{n-1}{2}$

10 Method of Proof by Indirect Argument I: Contradiction

1. We try to prove the statement is false
2. If the statement CANNOT be proved as false (AKA leads to contradiction), then it's true
3. In maths terms, we use
$$\sim P = False$$
   (a) To indicate
$$P = True$$

10.1 Theorem

- There is no greatest integer.

1. Negation: There is a greatest integer.
   (a) Proof:
      i. **Suppose not.**
      ii. **Suppose** there is a greatest integer, N.
      iii. **Then** $N \geq k, \forall k \in \mathbb{Z}$
      iv. **Let** $M = N + 1$
      v. **Since** the sum of integers is an integer, M is an integer and $M > N$. Thus M is an integer that is greater than the greatest integer.
      vi. **This contradicts with the supposition.** Hence, the supposition is false. The statement is true.

10.2 Theorem

- The sum of any rational number and any irrational number is irrational. Negation: The sum of at least one rational and at least one irrational number is rational

1. Proof:
   (a) Suppose not.
   (b) Suppose there is a rational number r and an irrational number s such that $r + s$ is rational.
2. Proof:
   (a) Suppose not.

(b) Suppose there is a rational number r and an irrational number s such that $r + s$ is rational.

(c) By definition of rational,

$$r = \frac{a}{b}, \{a, b\} \in \mathbb{Z}, b \neq 0$$

(d) Then

$$\begin{aligned} s + \frac{a}{b} &= \frac{c}{d} \\ s &= \frac{c}{d} - \frac{a}{b} \\ &= \frac{cb - ad}{bd} \end{aligned}$$

(e) Since the difference and product of integers are integers, $bc - ad$ and bd are integers and $bd \neq 0$ by zero product property. By definition, s is rational.

(f) This contradicts with the supposition that s is an irrational number and so **the sum of any rational number and any irrational number is irrational.**

11 Method of Proof by Indirect Argument II: Contraposition

1. Express the statement to be proved in the form

$$\forall x \in D, p(x) \to q(x)$$

   (a) Done mentally

2. Rewrite the statement in the contraposition form $\forall x$ in D, if $Q(x)$ is false then $P(x)$ is false

3. Prove the contrapositive by a direct proof.

   (a) Suppose x is a (particular but arbitrarily chosen) element in D such that $Q(x)$ is false.

   (b) Show that $P(x)$ is false.

11.1 Proposition

Given any integer n, if n^2 is even then n is even.

11.2 Proposition

- Given any integer n, if n^2 is even then n is even.
- Contrapositive: If n is odd , then n^2 is odd.

Proof:

1. **Suppose** n is a particular but arbitrarily chosen odd integer.
2. From the previous example (example 12)

$$\begin{aligned} n &= 2k+1 \\ n^2 &= (2k+1)^2 \\ &= 4k^2+4k+1 \\ &= 2\left(2k^2+2k\right)+1\,is\,odd \end{aligned}$$

   , the product of two odd integers is odd, hence $n^2 = n \cdot n$ is odd.
3. **Therefore** the statement is true

11.3 Classical Theorem

- **Statement**: $\sqrt{2}$ irrational.
- **Negation**: $\sqrt{2}$ is rational.

Proof:

1. **Suppose not**.
2. **Suppose** $\sqrt{2}$ is rational.
3. **By definition** of rational, there are integers m, n with no common divisor such that $\sqrt{2} = \frac{m}{n}$.
4. **Then**

$$\begin{aligned} 2 &= \frac{m^2}{n^2} \\ m^2 &= 2n^2 \end{aligned}$$

   (a) This implies m is even, $m = 2k, k \in \mathbb{Z}$
5. For $\left(m^2 = 2n^2\right) \implies \left[(2k)^2 = 2n^2\right]$

$$\begin{aligned} (2k)^2 &= 2n^2 \\ 4k^2 &= 2n^2 \\ n^2 &= 2k^2 \end{aligned}$$

6. Since $2k^2$ is divisible by 2, which is even. Then n^2, and therefore n is even too.
7. Hence both m and n are even with common factor of 2.
8. **This contradicts with the supposition and so the supposition is false, and the theorem is true.**

11.4 Proposition

- $1 + 3\sqrt{2}$ is irrational.
- Negation: $1 + 3\sqrt{2}$ is rational

Proof:

1. **Suppose not**.
2. **Suppose** $1 + 3\sqrt{2}$ is rational.
3. **By definition** of rational,

$$\begin{aligned} 1 + 3\sqrt{2} &= \frac{a}{b}, ab \in \mathbb{Z} \\ 3\sqrt{2} &= \frac{a}{b} - 1 \\ &= \frac{a-b}{b} \end{aligned}$$

4. **Then**. $\sqrt{2} = \frac{a-b}{3b} \in \mathbb{Q}$. However, $\sqrt{2} \notin \mathbb{Q}$. This is a contradiction.
5. **Since** the difference and product of integers are integers, $a - b$ and $3b$ are integers, $3b \neq 0$ by zero product property. Hence, according to our proof, $\sqrt{2}$ is rational.
6. **This contradicts with the theorem $\sqrt{2}$ is irrational, and so the supposition is false. Hence, $1 + 3\sqrt{2}$ is irrational**

12 Disproof by Counterexample

To disprove a statement of the form "$\forall x \in D$, if $P(x)$ then $Q(x)$" find a value of x in D for which $P(x)$ is true and $Q(x)$ is false. Such x is called a counterexample.

12.1 Example 13

Disprove the following statement by finding a counterexample.

- $\forall$ real numbers a and b, if $a^2 = b^2$ then $a = b$.

Finding counterexamples:

1. Let $a = -1, b = 1$
2. $a^2 = 1, b^2 = 1$
   (a) From this, $a^2 = b^2$
3. But $a \neq b$
4. Therefore, it is disproven

12.2 Notes

Many theorems can proved either direct or indirect way.

1. Try first to prove directly.
2. If not succeed, look for counterexample.
3. Finally proof by contradiction or contraposition

13 Algorithms

Step-by-step method for performing some action. E.g. food preparation recipes, directions for assembling equipment, sewing pattern instructions,

13.1 Greatest Common Divisor, gcd

Let a and b be integers that are not both zero. The greatest common divisor of a and b, denoted $gcd(a, b)$, is that integer d with the following properties:

1. d is a common divisor of both a and b, that is $d|a$ and $d|b$.
2. For all integers c, if c is a common divisor of both a and b, then c is less than or equal to d, that is
   (a) For all integers c, if $c|a$ and $c|b$, then $c \leq d$.

13.1.1 Example 14:

Find $gcd(27, 72)$

1. Using the repeated devision method
   (a) 2....72
   (b) 2....36
   (c) 2....18
   (d) 3....9
   (e) 3

2. $27 = 3 \cdot 3 \cdot 3 = 3^3$
3. $72 = 2^3 \cdot 3^2$
4. From both the figure above, they have a common:

$$3^2 = 9$$

5. Therefore, 9 is the common divisor

13.1.2 Example 15:

Find $gcd(10^{20}, 6^{30}) = 2^{20}$

$$10^{20} = 2^{20} \cdot 3^{20}$$
$$6^{10} = 2^{30} \cdot 3^{30}$$

1. Both of them have the same 2^{20} together, therefore, 2^{20} is the greatest common divisor.

13.1.3 Note

$gcd(0, 0)$ is not allowed.

13.2 Least Common Multiple, lcm

For two nonzero integers a and b, the least common multiple, denoted $lcm(a, b)$, is the positive integer c such that

1. $a|c$ and $b|c$,
2. for all integers m, if $a|m$ and $b|m$, then $c|m$.

Example

1. $\frac{c}{2}, \frac{c}{3}$. Min $c = 6$
   (a) In english: If 2 divides c, and 3 divides c, then the minimum c for LCM is 6.
   (b) **Conjencture:** $LCM\,(a, b) \cdot GCM\,(a, b) = a \cdot b$
   Proof:
      i. Let $d = gcd\,(a, b)$ and $l = lcm\,(a, b)$.
      ii. By definition, $\frac{ab}{d}$ is a common multiply of a, b, since $\frac{a}{d}$ and $\frac{b}{d}$ are integers.
      iii. By Euclidean algorithm, $\frac{a}{d}, \frac{b}{d}$ are relatively prime. (no integer greater than one that divides them both)
         A. Assume n is the common multiple of a and b.

B. We can find integers k and k' such that $n = ka$ and $n = k'b$.

C. By dividing both sides by d, we still remain integer, but we now get $k'\frac{b}{d} = k\frac{a}{d}$.

iv. Hence, $\frac{a}{d}$ divides $\frac{b}{d}k'$.

v. Since $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime, then $\frac{a}{d}$ divides k'.

vi. Hence, $n = k'b = q\frac{ab}{d}$ for some integer q.

vii. So $\frac{ad}{d}$ divides n.

viii. Hence, $lcm\,(a,b) = \frac{ab}{d} = \frac{ab}{gcd(a,b)}$

13.2.1 Example 16:

Find $lcm(12, 18)$.

1. Assume that $\frac{c}{12} \in \mathbb{Z}$, AKA if we take an integer, multiply by 12, we get c.
2. Assume that $\frac{c}{18} \in \mathbb{Z}$, AKA if we take an integer, multiply by 18, we get c.
3. Minimum $c = ?$
4. $12 = 2^2 * 3$, $18 = 2 * 3^2$
5. $gcd\,(a,b) = gcd\,(12,18) = 2 * 3 = 6$
6. $a * b = 12 * 18 = 216$
7. Plug into the formula

$$\begin{aligned} lcm\,(a,b) &= \frac{ab}{gcd\,(a,b)} \\ &= \frac{216}{6} \\ &= 36 \end{aligned}$$

8. Minimum $c = 36$

13.2.2 Notes

1. $lcm(1, n) = n$
2. For $a, n \in \mathbb{Z}^+, lcm(a, na) = na$
3. For $a, m, n \in \mathbb{Z}^+$ with $m \leq n$, $lcm(a^m, a^n) = a^n$ and $gcd(a^m, a^n) = a^m$

13.3 The Euclidean Algorithm

The Euclidean algorithm can be described as follows:

1. Let A and B be integers with $A > B \geq 0$.
2. First check whether $B = 0$.
   (a) If yes, $gcd(A, B) = A$.
   (b) If it isn't, then $B > 0$ and the quotient-remainder theorem can be used to obtain $A = B \cdot q + r, 0 \leq r < B$
   (c) Thus, $gcd(A, B) = gcd(B, r)$.
      i. From point 2.
         A. If x divides a and b, then x divides $a - bq = r$
         B. If x is a number, and x divides B and r, then x must divide $bq + r = a$.
   (d) Since $0 \leq r < B < A$, the largest number of the pair (B, r) is smaller than the largest number of the pair (A, B).
3. Repeat the process in (2), but use B instead of A and r instead of B.
4. The repetitions will be terminated when r = 0.

13.4 Example 17

Use Euclidean algorithm to find $gcd(1188, 385)$ and then rewrite them in the form of $sA + tB$

1. Solution:
   (a) $1188 = 385\,(3) + 33$
   (b) $385 = 33\,(11) + 22$
   (c) $33 = 22\,(1) + 11$
   (d) $22 = 11\,(2) + 0$
2. $gcd(1188, 385) = gcd\,(11, 0) = 11$
   (a) $11 = S\,(1188) + t\,(385)$
   (b)

$$\begin{aligned}
11 &= 33 - 22\,(1) \\
&= 33 - (385 - 33\,(11)) \\
11 &= 12\,(33) - 385 \\
11 &= 12\,(1188 - 3\,(385)) - 385 \\
11 &= 12\,(1188) - 37\,(385) \\
11 &= 12\,(1188) + (-37)\,(385)
\end{aligned}$$