CISC-102
Winter 2020
Week 6

SN: Chapter 11.
Properties of the Integers

Let a,b $\in \mathbb{Z}$ then

1. if c = a + b then c $\in \mathbb{Z}$
2. if c = a - b then c $\in \mathbb{Z}$
3. if c = (a)(b) then c $\in \mathbb{Z}$
4. if c = a/b then c $\in \mathbb{Q}$

If a & b are integers the quotient a/b may not be an integer. For example if c = 1/2, then c is not an integer. On the other hand with c = 6/3 then c is an integer.

We can say that *there exists* integers a,b such that c = a/b is not an integer.

We can also say that *for all* integers a,b we have c = a/b is a rational number.

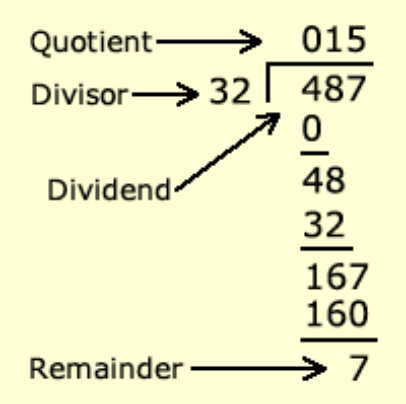
Divisibility

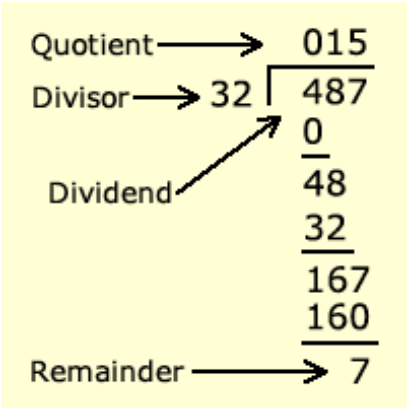
Let a,b $\in \mathbb{Z}$, a $\neq 0$.
If c = $\frac{b}{a}$ is an integer,

or alternately if c $\in \mathbb{Z}$ such that b = ca
then we say that a *divides* b or equivalently,
b is *divisible* by a, and this is written

a | b

NOTE: Recall long division:





Referring to the long division example, b = 32, is the divisor a = 487 is the dividend. The quotient q = 15 and the remainder r = 7.
In this case b *does not divide* a
or equivalently a is *not divisible* by b.

This can be notated as:

$$b \nmid a$$

and we can write a = bq + r or, 487 = (32) (15) + 7

Division Algorithm Theorem

Let $a,b \in \mathbb{Z}$, $b \neq 0$ there exists $q,r \in \mathbb{Z}$, such that:

$$a = bq + r,\ 0 \leq r < |b|$$

NOTE: The remainder in the Division Algorithm Theorem is always positive.

Notation

The *absolute value* of b denoted by

$$|b|$$

is defined as:

$$|b| = b \text{ if } b \geq 0$$

$$\text{and } |b| = -b \text{ if } b < 0.$$

Therefore for values

a = 22, b = 7, and a = -22, b = -7 we get

22 = (7)(3) + 1

but

-22 = (-7)(4) + 6.

Divisibility

Suppose on the other hand that we have a = 217 and b = 7. We have 217 = (31) (7) + 0 so we conclude that b ∣ a.

```
   31
  ----
7 ∣ 217
    21
    ---
     07
      7
      -
      0
```

Division Algorithm Theorem

Let $a,b \in \mathbb{Z}$, $b \neq 0$ there exists $q,r \in \mathbb{Z}$, such that:

$$a = bq + r,\ 0 \leq r < |b|$$

Suppose b = 2. The remainder r can be one of two values, either 0 or 1.

Suppose we have:

$$a = 2q + 0$$

Then a is an even integer.

On the other hand suppose:

$$a = 2q + 1$$

Then a is odd.

Divisibility Theorems.

Let a,b,c $\in \mathbb{Z}$. If a ∣ b and b ∣ c then a ∣ c.

Proof:

Suppose a ∣ b then there exists an integer j such that

(1) b = aj

Similarly if b ∣ c then there exists an integer k such that

(2) c = bk

Replace b in equation (2) with aj to get

(3) c = ajk

Thus we have proved that if a ∣ b and b ∣ c then a ∣ c. □

Divisibility Theorems.

Let a,b,c $\in \mathbb{Z}$. If a ∣ b then a ∣ bc.

Proof:
Since a ∣ b there exists an integer j such that

b = aj, and bc = ajc for all (any) c $\in \mathbb{Z}$.

It should be obvious that a ∣ ajc ($\frac{ajc}{a}$ = jc is an integer)

so a | bc . □

Divisibility Theorems.

Let a,b,c $\in \mathbb{Z}$. If a ∣ b and a ∣ c. Then a ∣ (b + c) and a ∣ (b - c).

Proof:

Since a | b there exist a j $\in \mathbb{Z}$ such that b = aj.

Since a | c there exist a k $\in \mathbb{Z}$ such that c = ak.

Therefore b + c = (aj + ak) = a(j + k).

Obviously a | a(j + k) so a ∣ (b + c).

Similarly a | a(j - k) so a ∣ (b - c). □

Absolute Value

Let a and b be any integers. Then:

(i) $|a| \geq 0$ and $|a| = 0$ if and only if $a = 0$.

(ii) $-|a| \leq a \leq |a|$

(iii) $|ab| = |a|\,|b|$

(iv) $|a + b| \leq |a| + |b|$

(v) $|a - b| \leq |a| + |b|$

(vi) $||a| - |b|| \leq |a + b|$

(vii) $||a| - |b|| \leq |a - b|$

We can verify each of these properties by exhaustive case analysis. For example:

(i) Suppose $a > 0$, then $|a| = a$ so $|a| > 0$.

On the other hand suppose $a < 0$, then $|a| = -a$, so $|a| > 0$.

Finally suppose $a = 0$, so $|a| = 0$. Since we already have shown that $|a| \neq 0$ when $a \neq 0$, we have $|a| = 0$ if and only if $a = 0$.

Another example

(iii) $|ab| = |a|\,|b|$

We consider the following cases:

- $|ab| = 0$, so either a or b or both are 0, therefore $|a| \mid b| = 0$.
- $a > 0$ and $b > 0$ so $|a| = a$ and $|b| = b$, therefore $|ab| = |a|\,|b|$.
- $a < 0$ and $b > 0$ so $|a| = -a$ and $|b| = b$, therefore $|ab| = -ab$ and $|a||b| = -ab$ so $|ab| = |a||b|$.
- $a > 0$ and $b < 0$ so $|a| = a$ and $|b| = -b$, therefore $|ab| = -ab$ and $|a||b| = -ab$, so $|ab| = |a||b|$.
- $a < 0$ and $b < 0$ so $|a| = -a$ and $|b| = -b$, therefore $|ab| = ab$ and $|a||b| = ab$, so $|ab| = |a||b|$.

Also observe that if $a = b$ then $|a| = |b|$ and this can be verified by considering the cases: $a < 0$, and $a \geq 0$.

- **More Divisibility Theorems.**

If $a \mid b$ and $b \neq 0$ then $|a| \leq |b|$.

If $a \mid b$ and $b \mid a$ then $|a| = |b|$.

If $a \mid 1$ then $|a| = 1$.

Prime Numbers

Definition: A positive integer $p > 1$ is called a *prime number* if its only divisors are 1, -1, and p, -p.

The first 10 prime numbers are:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Definition: If an integer $c > 2$ is not prime, then it is *composite*. Every composite number c can be written as a product of two integers a,b such that $a,b \notin \{1,-1, c, -c\}$.

Determining whether a number, n, is prime or composite is difficult computationally. A simple method (which is in essence of the same computational difficulty as more sophisticated methods) checks all integers k, $2 \leq k \leq \sqrt{n}$ to determine divisibility.

Example: Let n = 143

2 does not divide 143
3 does not divide 143
4 does not divide 143
5 does not divide 143
6 does not divide 143
7 does not divide 143
8 does not divide 143
9 does not divide 143
10 does not divide 143
11divides 143, $11 \times 13 = 143$

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

For example:

$12 = 2 \times 2 \times 3$.

17 is prime.

$90 = 2 \times 5 \times 3 \times 3$.

$143 = 11 \times 13$.

$147 = 3 \times 7 \times 7$.

$330 = 2 \times 5 \times 3 \times 11$.

Note: If factors are repeated we can use exponents.

$48 = 2^4 \times 3$.

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof:

(1) We will assume that there are integers that are not prime nor a product of primes. If there are integers that are neither prime nor a product of primes, then let the integer k+1 be the smallest. (This proof concludes by showing that this assumption is false.)

(2) If k+1 is not prime it must be composite and:
$k+1 = ab,\ a,b \in \mathbb{Z},\ a,b \notin \{1,-1, k+1, -(k+1)\}$.

(3) Observe that $|a| < k+1$ and $|b| < k+1$, because $a \mid k+1$ and $b \mid k+1$. We assume that k+1 is the smallest positive integer that is not prime or the product of primes, therefore |a| and |b| are prime or a product of primes.

(4) Since k+1 is a product of a and b it follows that it too is a product of primes.

(5) Thus we have contradicted the assumption that there is a smallest integer that is neither prime nor the product of primes, and we can therefore conclude that every integer $n > 1$ is either prime or written as a product of primes. □

Mathematical Induction (2nd form)

Let P(n) be a proposition defined on a subset of the Natural numbers (b, b+1, b+2, ...) such that:

i) P(b) is true
(Base)
ii) Assume P(j) is true for all j, $b \leq j \leq k$.
(Induction Hypothesis)
iii) Use Induction Hypothesis to show that P(k+1) is true.
(Induction Step)

NOTE: Go back to all of the proofs using mathematical induction that we have seen so far and replace the assumption
(1) Assume P(k) is true for $k \geq b$. (b is the base case value) by
(2) Assume P(j) is true for all j, $b \leq j \leq k$."

and the rest of the proof can remain as is.

Assumption (2) above is stronger than assumption (1). Sometimes this form of induction is called *strong induction.*

NOTE: A stronger assumption makes it easier to prove the result.

Let P(n) be the proposition:

$\sum_{i=1}^{n} 2^i = 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 2$

Theorem: P(n) is true for all $n \in \mathbb{N}$.

Proof:

Base: P(1) is $2 = 2^2 - 2$ which is clearly true.

Induction Hypothesis: P(j) is true for j, $1 \leq j \leq k$.

Induction Step:

$$\sum_{i=1}^{k+1} 2^i = 2^{k+1} - 2 + 2^{k+1}$$

(because P(k) is true)

$$= 2(2^{k+1}) - 2$$

$$= 2^{k+2} - 2 \qquad \square$$

Theorem: Every integer $n > 1$ is either prime or can be written as a product of primes.

Proof: (Mathematical Induction of the 2nd form) Let P(n) be the proposition that all natural numbers $n \geq 2$ are either prime or the product of primes.

Base: n = 2, P(2) is true because 2 is prime.
Induction Hypothesis:
(1) Assume that P(j) is true, for all j, $2 \leq j \leq k$.
Induction Step: Consider the integer k+1.

(2) Observe that if k+1 is prime P(k+1) is true, so consider the case where k+1 is composite. That is: $k+1 = ab$, $a,b \in \mathbb{Z}$, $a,b \notin \{1,-1, k+1, -(k+1)\}$.
(3) Therefore, $|a| < k+1$ and $|b| < k+1$.
So |a| and |b| are prime or a product of primes.
(4) Since k+1 is a product of a and b it follows that it too is a product of primes.
(5) Therefore, by the 2nd form of mathematical induction we can conclude that P(n) is true for all $n \geq 2$. □

Well-Ordering Principle

In our initial proof that shows that integers greater than 2 are either prime or a product of primes we assumed that if that wasn't true for all integers greater than 2, then there was a smallest integer where the proposition is false. (we called that integer k+1.) This statement may appear to be obvious, but there is a mathematical property of the positive integers at play that makes this true.

Theorem: Well Ordering Principle: Let S be a non-empty subset of the positive integers. Then S contains a least element, that is, S contains an element $a \leq s$ for all $s \in S$.

- Observe that S could be an infinite set.
- Well ordering does NOT apply to subsets of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$. It is a special property of the positive integers.

NOTE: The Well Ordering Principle can be used to prove both forms of the Principle of Mathematical Induction.

In essence the statement “use the proposition P(k) to show that P(k+1) is true” uses an underlying assumption:

“Should there be a value of n where the proposition is false then there must be a smallest value of n where the proposition is false”

In all of our induction proofs so far the value k+1 plays the role of that smallest value of n where the proposition may be false. For all other values j, $b \leq j \leq k$, we can assume that P(j) is true. In the induction step we show that P(k+1) is also true, in essence showing that there is no smallest value of n where the proposition is false. And by well ordering this implies that the result is true for all values of n.

Another application of the 2nd form of induction

Consider a two player game, where players take turns removing any number of matches from one of two piles. The last person who plays (removes the last of the matches) wins.

When the two piles start with the same number of matches there is a strategy so that the second player is guaranteed to win no matter what the first player does.

We can prove this using the second form of induction.

Base: 1 match per pile, so player 1 is forced to leave a single pile and player two wins.

Induction Hypothesis: Assume that player two wins whenever we start with two piles of j matches each, for j, $1 \leq j \leq k$.

Induction Step: Suppose we start with two piles of k+1 matches each. Player 1 removes x matches from one of the piles such that $1 \leq x \leq k+1$.

Now you complete the proof.

And another application of the 2nd form of induction

Consider the recursive function defined as:
$F(1) = 1$, $F(2) = 1$ $F(n) = F(n-1) / F(n-2)$ for $n \geq 3$.

Observe that $F(3) = 1/1 = 1$ $F(4) = 1/1 = 1$ etc.

We can prove the obvious using the 2nd form of induction.

The function $F(n) = 1$ for all natural numbers n.

Base: $F(1) = F(2) = 1$. (Note: We need 2 base cases!)
Induction Hypothesis: $F(j) = 1$ for all j, $1 \leq j \leq k$.
Induction Step: $F(k+1) = F(k) / F(k-1)$
$= 1/1$ (Using the Ind. Hyp.)
$= 1$.

Theorem: There exists a prime greater than n for all positive integers n. (We could also say that there are infinitely many primes.)

Proof: Let n be an arbitrary (large) natural number. We will show that there exists a prime number larger than n. Consider $y = n!$ and $x = n! + 1$.

Let p be a prime divisor of x. We show that assuming that $p \leq n$ leads to a contradiction.

Observe that any prime number smaller than n, is a divisor of $n! = y$, because n! is the product of all natural numbers from 1 to n.

So we have $p \mid x$ and $p \mid y$.

According to one of the divisibility theorems we have $p \mid x - y$. But $x - y = 1$ and the only divisor of 1 is -1, or 1, both not prime. So there are no prime divisors of x less than n. And since every integer is either prime or a product if primes, we either have $x > n$ is prime, or there exists a prime p, $p > n$ in the prime factorization of x. □

Theorem: There is no largest prime.

(Proof by contradiction.)

Suppose there is a largest prime. So we can write down all of the finitely many primes as: $\{p_1, p_2, \ldots, p_\omega\}$.

Now let $n = p_1 \times p_2 \times \cdots \times p_\omega + 1$.

Observe that n must be larger the p_ω the largest prime. Therefore n is composite and is a product of primes. Let p_k denote a prime factor of n. Thus we have

$p_k \mid n$

And since $p_k \in \{p_1, p_2, \ldots, p_\omega\}$ we also have

$p_k \mid (n\text{-}1)$

We know that $p_k \mid n$ and $p_k \mid (n\text{-}1)$ implies that $p_k \mid$ n - (n-1) or $p_k \mid 1$. But no integer divides 1 except 1, and 1 is not prime, so $p_k \mid 1$ is impossible, and raises a mathematical contradiction. This implies that our assumption that p_ω is the largest prime is false, and so we conclude that there is no largest prime. □

Greatest Common Divisor

Consider any two integers, a,b, at least one non-zero. If we list the positive divisors in numeric order from smallest to largest, we would get two lists:

a: (1, c1, c2, ... |a|)
b: (1, d1, d2, ... |b|)

Since both lists must contain the number 1, we see that 1 is a common divisor of a and b. Since the greatest divisor of a is |a| and the greatest divisor of b is |b|, we can deduce that amongst the common divisors of a and b, there must be one that is the greatest.

Thus we can say that given two integers a,b, at least one not zero, there is a unique greatest common divisor of a and b.

Computing the greatest common divisor of a non-zero integer a, and 0, is somewhat boring because all non-zero integers divide 0, so the greatest common divisor of a and 0 is always |a|. So let's just assume from now on that neither a nor b is 0.

Example:
Let a = 111, and b = 250. We can construct sorted lists of divisors of a and b yielding:

a: (1, 3, 37, 111)
b: (1, 2, 5, 10, 25, 50, 125, 250)

And by inspection we can deduce that 1 is the greatest common divisor of a and b. When the greatest common divisor of two numbers a,b is 1 we say that a and b are *relatively prime* or *coprime*.

Another example:
Let a = 250, and b = 575. We can construct sorted lists of divisors of a and b yielding:

a: (1, 2, 5, 10, 25, 50, 125, 250)
b:(1, 5, 23, 25, 115, 575)

And by inspection we can deduce that 25 is the greatest common divisor of a and b.

This method of obtaining all divisors of a and b is very computationally intensive, and would make some essential steps of public key encryption schemes non feasible. Remarkably an algorithm invented by Euclid (~ 300 BC) finds greatest common divisors in a much more efficient way.

Euclid's Algorithm

Suppose a,b are non-zero integers. We can define a function on the integers:

$$\gcd(a,b)$$

that returns the greatest common divisor of a and b. It will be convenient to further assume that $|a| \geq |b|$.

Euclid's algorithm to compute gcd(a,b) is way more efficient than computing all the divisors of a and b, and is based on the following observation.

Euclid's Theorem:

Let a,b,q,r be positive integers such that $a = qb + r$ then

$$\textbf{gcd (a,b) = gcd(b,r)}$$

For example: a = 575, b = 250.

575 = (2)(250) + 75 (Use long division to get q and r)

So the claim is that gcd(575, 250) = gcd(250,75).

This can be verified by listing the divisors of 250 and 75.

250: (1, 2, 5, 10, 25, 50, 125, 250)
75: (1, 3, 5, 15, 25, 75)

We can now “iterate” this process by renaming a = 250, b = 75 and repeat the previous calculation. That is:

250 = (3)(75) + 25

We can again verify that gcd(250,75) = gcd(75,25).

Let’s repeat this again, so a = 75 and b = 25

75 = (3)(25) + 0

so we have gcd(75,25) = gcd(25,0), and we have already seen that the greatest common divisor of any non-zero integer a and 0 is |a|.

Therefore by Euclid’s algorithm we have
gcd(575,250) = 25.

NOTE: Euclid’s algorithm is given for positive integers. However,

gcd(a,b) = gcd (-a,b) = gcd(a,-b) = gcd(-a,-b)

so there is no loss of generality if we simply focus on positive integers.

Observe that as a side effect of Euclid's algorithm we can always find integers x,y such that gcd(a,b) = ax + by.

This can be illustrated with the previous example.

(1) 575 = (2) 250 + 75 implies 75 = 575 - (2)250
(2) 250 = (3) 75 + 25 implies 25 = 250 - (3)75
(3) 75 = (3) 25 + 0

Now we can write gcd(575,250) = 25 as:

25 = 250 - (3)75 (Using (2) above)
25 = 250 - (3)[575 - (2)250] (Using (1) above)
25 = (7)250 - (3)575 (Simplify)

To prove Euclid's Theorem we will need a preliminary result. (Math convention uses the word "lemma" for preliminary results that are proved in preparation for the proof of the main theorem.

Lemma: If $g \mid a$ and $g \mid b$
then $g \mid (pa + b)$ for all integers p.

Proof: Since $g \mid a$ and $g \mid b$ we can write

(1) $a = p_a g$ and $b = p_b g$.

Replacing the values of a and b in $g \mid (pa + b)$ using equations (1) we get:

$$g \mid (pp_a g + p_b g)$$

which simplifies to:

$$g \mid g(pp_a + p_b)$$

Now it should be clear that g divides $g(pp_a+p_b)$ and thus we conclude that g divides pa + b. □

Theorem: Let a,b,q,r be positive integers such that:
$a = qb + r$, $0 \leq r < b$, then gcd (a,b) = gcd(b,r)

Strategy of the proof: We show that the gcd(a,b) is a common divisor of b & r and that gcd(b,r) is a common divisor of a & b.

Proof:
(0) Let g1= gcd(a,b) and g2 = gcd(b,r).
(1) Observe that g2 | b and g2 | r, so g2 | pb + r for all integers p, and in particular for q, where a = qb + r.

(a) Therefore, g2 | a, and we have established that g2 is a common divisor of both a and b.

(b) Furthermore, observe that $g2 \leq g1 = gcd(a,b)$

(2) Using the equation a = qb + r we can write
r = - qb + a.
g1 | b and g1 | a so use the lemma (with p = -q) to get g1 | -qb + a or g1 | r.

(a) Therefor g1 | r and we have established that g1 is a common divisor of b and r.

(b) Furthermore, observe that $g1 \leq g2 = gcd(b,r)$

(3) $g2 \leq g1$ and $g1 \leq g2$ implies that g1 = g2, so we can conclude that gcd(a,b) = gcd(b,r). □

Euclid's Algorithm in the Python programming language.

```
def euclid_gcd(a,b):
# Assume a >= b > 0
    r = a % b # this returns r such that a = bq + r
    while r > 0:
        a,b = b,r
        r = a % b # this returns r s.t. a = bq + r
    return b
```

NOTE: The % (mod) operator is found in many programming languages and returns the remainder when doing integer division.

We will argue that euclid_gcd(a,b) finds gcd(a,b) assuming that $a \geq b > 0$.

We first argue that the loop terminates, that is r eventually becomes 0. This is easy to see because the remainder when we divide a by b is less than b. The value of r begins positive and always decreases so it eventually must be zero.

The correctness follows from Euclid's theorem.

It can also be shown that this function is extremely efficient when compared to looking at all the divisors of a and b.

Let a = 250, and b = 575. We can construct a prime factorization of a and b.

Prime factorization:
$250 = (2)(5^3)$
$575 = (5^2)(23)$

We can inspect the prime factorization of a and b to obtain a greatest common divisor.

Observe that 5^2 is the greatest number that divides both a and b, that is the gcd(a,b). Using the prime factorizations of a and b is much less efficient than Euclid's algorithm. Nevertheless, the prime factorization is useful for obtaining other properties of the greatest common divisor.

Least Common Multiple

Given two non-zero[1] integers a,b we can have many values that are positive common multiples of both a & b. By the well ordering principle we know that amongst all of those multiples there is one that is smallest, and this is known as the *least common multiple* of a and b. We can define a function lcm(a,b) that returns this value.

Example: Suppose a = 12, and b = 24,
so we have lcm(a,b) = 24.
In general if a | b then lcm(a,b) = |b|.
At this point it is worth mentioning that if a | b then gcd(a,b) = |a|, and that lcm(a,b) × gcd(a,b) = |ab|.

Example: Suppose a = 13, and b = 24, we have lcm(a,b) = (13)(24).
In general if a and b are relatively prime, that is, if gcd(a,b) = 1 then lcm(a,b) = |ab|

So when gcd(a,b) = 1, we can observe that lcm(a,b) × gcd(a,b) = |ab|.

[1] Multiples of zero are always zero, so this is a boring case.

Let a = 250, and b = 575. We can construct a prime factorization of a and b

Prime factorization
$250 = (2)(5^3)$
$575 = (5^2)(23)$

We can inspect the prime factorization of a and b to obtain the least common multiple.

$250 \times 575 = (2)(5^3) \times (5^2)(23) = (5^2) \times (2)(5^3)(23)$

And since $\gcd(a,b) = 5^2$ we can conclude that
$\text{lcm}(a,b) = (2)\ (5^3)\ (23)$.

So in this case we also have $\text{lcm}(a,b) \times \gcd(a,b) = |ab|$

Given a prime factorization of two integers a,b we can devise a formula to obtain gcd(a,b) as well as lcm(a,b).

Prime factorization
$a = 250 = (2)(5^3)$
$b = 575 = (5^2)(23)$

Let $p_1, p_2, \ldots, p_k$ denote all of the prime factors of both a and b ordered from smallest to largest. In our example the list of prime factors would be 2,5,23.

Let a_i denote the exponent of prime factor p_i, for i, $1 \leq i \leq k$, in a prime factorization of a.

In our example $a_1 = 1$, $a_2 = 3$, $a_3 = 0$.

Similarly we define b_i for i $1 \leq i \leq k$.

In our example $b_1 = 2$, $b_2 = 0$, $b_3 = 1$.

Again referring to our example we have:

$$\gcd(a,b) = 2^{\min(1,0)} \times 5^{\min(3,2)} \times 23^{\min(0,1)}$$

and,

$$\text{lcm}(a,b) = 2^{\max(1,0)} \times 5^{\max(3,2)} \times 23^{\max(0,1)}.$$

In general using p_i, a_i, and b_i as defined above we can express this formula as:

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \cdots \times p_k^{\min(a_k,b_k)}$$

and

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \cdots \times p_k^{\max(a_k,b_k)}$$

Another Example:

$630 = (2) (3^2) (5) (7)$
$84 = (2^2) (3) (7)$

By inspection we can see that:
$\gcd(630,84) = (2) (3) (7) = 42$
And $\text{lcm}(630,84) = (2^2) (3^2) (5) (7) = 1260$

Again we have

$$\begin{aligned} 630 \times 84 &= (2) (3^2) (5) (7) \times (2^2) (3) (7) \\ &= (2) (3) (7) \times (2^2) (3^2) (5) (7) \\ &= \gcd(630,84) \times \text{lcm}(630,84) \end{aligned}$$

These ideas lead to the following theorem that is given without proof.

Theorem: Let a,b be non-zero integers, then

$$\gcd(a,b)\text{lcm}(a,b) = |ab|.$$

Factoring vs. GCD

Factoring an integer N into its prime factors will use roughly $\sqrt{N}$ operations.

Computing gcd(N,m) with Euclid's algorithm for $N > m \geq 0$ will use roughly $\log_2 N$ operations.

N	$\log_2 N$	$\sqrt{N}$
1024	10	32
1099511627776	40	1,048,576
1×10^{301}	1000	3.27×10^{150}

The efficiency of Euclid's gcd algorithm is essential for implementing current public key crypto systems that are commonly used for e-commerce applications.

With a "key" decoding an encrypted message using Euclid's algorithm takes about 1000 operations. Without a "key" breaking an encrypted messaged takes about 3.27×10^{150} operations. This amounts to a small fraction of a second for decoding and many millions of years for breaking the encrypted message.