Unit 5

Numbers

Albert Sung

Prime Factorization

- A composite number can be represented as a product of smaller integers.

$$1001 = 7 \times 143$$

- This is called (integer) factorization.
- We can continue the process until all factors are primes.

$$1001 = 7 \times 11 \times 13$$

- This is called prime factorization.
- Another way to factorize it:

$$1001 = 11 \times 91$$

- Continuing,

$$1001 = 11 \times 7 \times 13$$

- The same factors are obtained.
- Is prime factorization unique?

Outline of Unit 5

- 5.1 Divisibility
- 5.2 Primes and Co-primes
- 5.3 Euclidean Algorithm
- 5.4 Unique Factorization Theorem

Unit 5.1

Divisibility

Number Theory

- Number theory studies integers and operations on them.
- Its very basics (e.g. addition and multiplication) has natural applications in everyday life.
- Is more “advanced” number theory useless?
- No, it is vital for modern cryptography.
  - e.g. online transaction, e-banking, secure communications…
  - more in Unit 7.

Divisibility = Sharing Equally

- Can the muffins be shared equally by the little animals?
- No, because 8 is *not* divisible by 3.

- Divisibility is the central concept of number theory.

Divisibility

- **Definition:** Given two integers n and d, we say that n is divisible by d iff n equals d times some integer:

$$\boxed{\exists k \in \mathbb{Z}, \qquad n = d \times k.}$$

- **Notation:** $d \mid n$ ("*d* divides *n*")
- We can also say that
  - "*d* is a factor of *n*."
  - "*d* is a divisor of *n*."
  - "*n* is a multiple of *d*."

- Why do we care about the definition, which is so trivial?
- It allows us to prove general properties.

Classwork

a) What are the divisors of 4?

b) Is it true that $2 \mid 0$?

Transitivity of Divisibility

Theorem:

For all integers a, b, and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

By definition of divisibility,

$$b = ar \text{ and } c = bs \quad \text{for some integers } r \text{ and } s.$$

By substitution,

$$c = bs = (ar)s = a(rs).$$

Since rs is an integer, by definition of divisibility,

$$a \mid c. \qquad \textit{Q.E.D.}$$

Division with Remainders

- Division over integers is not always possible, but we can generalize it:

Quotient-Remainder Theorem: (Proof omitted)

Given any integer n and positive integer d, there exist unique integers q and r such that

$$n = d \times q + r, \text{ where } 0 \leq r < d.$$

r can take only d values, $0, 1, 2, \ldots, d-1$.

Terminology:

- n is the dividend,
- d is the divisor,
- q is the quotient, and
- r is the remainder.

Intuition

- $n = dq + r$, where $0 \leq r < d$.

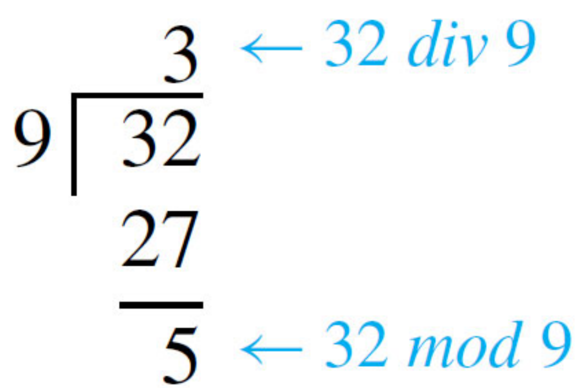
- Intuition:
  - Split n objects into groups of size d.
  - Form the groups one by one.
  - There might be some objects left that are not enough for a new group.
  - The number of objects left is r.
  - The number of groups formed is q.
- Idea: Repeatedly subtract d from n.
  - (If $n < 0$, repeatedly add d to n.)

The existence of q and r is intuitively clear.

Quotient and Remainder

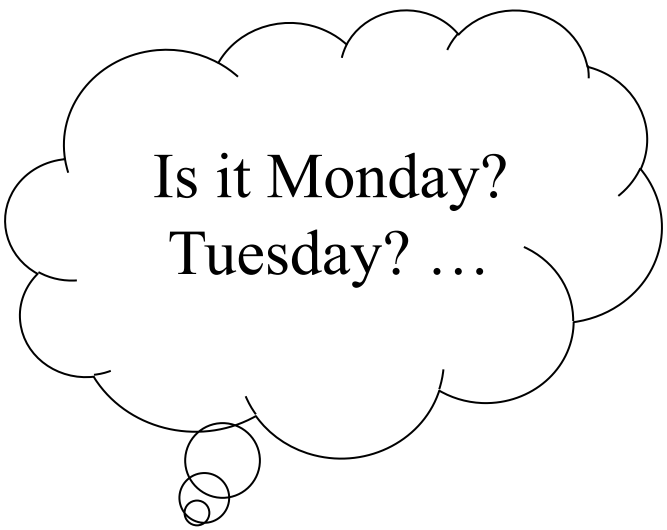
- *n* div *d* denotes the quotient *q* obtained when *n*/*d*.
- *n* mod *d* denotes the remainder *r* obtained when *n*/*d*.

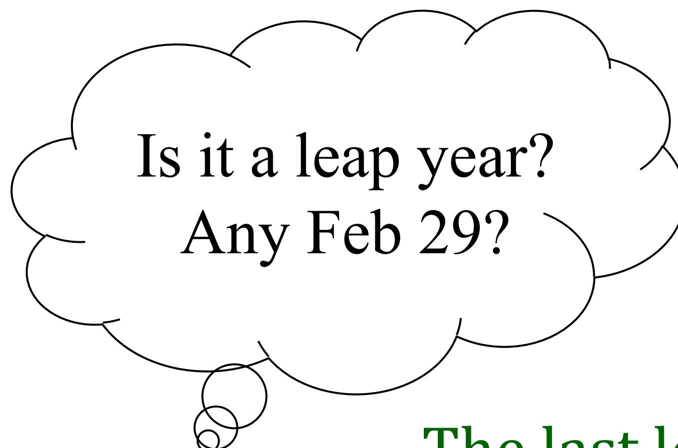
- Example:



Classwork

- What day of the week will it be 1 year from today?





The last leap year is 2020 and the next leap year is 2024.

Unit 5.2

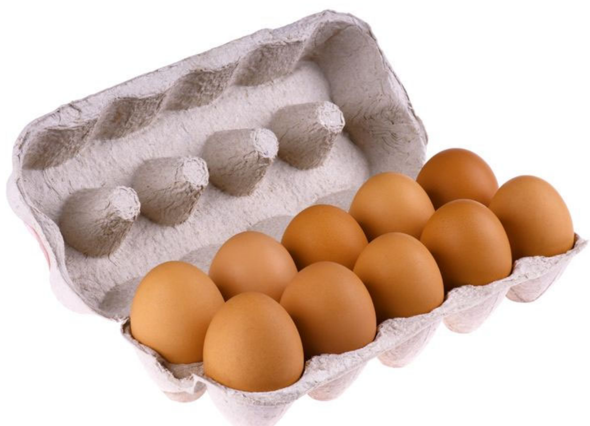
Primes and Co-Primes

Arranging Eggs

- Is it possible to arrange a certain number of eggs in an array of several (i.e., more than 1) rows and columns?

6

10



7?

Primes

- **Definition:**

a) An integer p is a prime if $p > 1$ and the only positive divisors of p are 1 and p itself.

b) An integer $n > 1$ that is not a prime is called a composite.

- **Example:**

a) 1 is not a prime

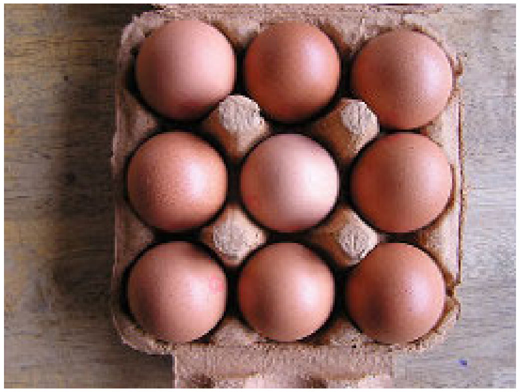
b) 2 is a prime as only $1|2$ and $2|2$

c) 4 is a composite as not only $1|4$, $4|4$ but also $2|4$

Arranging Two Groups of Eggs

- Is it possible to arrange a eggs and b eggs in two arrays both of d rows, where $d > 1$?

$a = 9$



$d = 3$

$b = 15$

It is possible if a and b have a common divisor $d > 1$.

It is impossible if they are co-prime (defined in the next slide).

Greatest Common Divisor

- **Definition:** The greatest common divisor (gcd) of two numbers, a and b, is the largest integer that divides both a and b.
  - e.g., gcd(24, 16) = 8.

- **Definition:** Two numbers, a and b, are said to be co-prime or relatively prime if

$$\boxed{\gcd(a, b) = 1.}$$

  - e.g. 14 and 9 are relatively prime.

Classwork

a) $\gcd(18, 12) = ?$

b) $\gcd(5, 5) = ?$

c) $\gcd(3, 1) = ?$

d) $\gcd(8, 0) = ?$

Euler's Totient Function

- Euler's totient function $\phi(n)$ counts integers from 1 up to n that are co-prime with n.
  - $\phi(1) = 1$
  - $\phi(2) = 1$
  - $\phi(3) = 2$
  - $\phi(4) = 2$
  - $\phi(5) = 4$
  - $\phi(6) = 2$

    $\vdots$
  - $\phi(10) = ?$

- Euler's totient function is also called **Euler's phi function**.
- It plays a key role in the RSA encryption system (see Unit 7).

What is $\phi(p)$ if p is a prime?

Phi Function Formulas

Theorem:

a) If p is a prime and $k \geq 1$, then
$$\phi(p^k) = p^k - p^{k-1}.$$

b) If m and n are co-prime, then
$$\phi(mn) = \phi(m)\phi(n).$$

Why is it useful?

- $\phi(x)$ can be found by factorizing x.
- By Unique Factorization Theorem (discussed later), every number x can be expressed as $p_1^{k_1} p_2^{k_2} \dots p_j^{k_j}$.
- By (b), $\phi(x) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \dots \phi\left(p_j^{k_j}\right)$.
- Each term can then be obtained by (a).

Example

What is $\phi(24)$?

Answer:

- $24 = 2^3 \times 3$
- $\phi(24) = \phi(2^3) \times \phi(3) = (2^3 - 2^2) \times 2 = 8$

Illustration of the proof of (a)

- Consider $\phi(8) = \phi(2^3)$.
- Counting: 1, 2, 3, 4, 5, 6, 7, 8

Multiples of 2 are not co-prime with 8

- There are $\frac{8}{2} = 4$ such numbers. $\left(\frac{p^k}{p} = p^{k-1}\right)$
- $\phi(2^3) = 2^3 - 2^2$

Proof of (a) (optional)

- There are p^k numbers in $\{1, 2, \dots, p^k\}$.
- Except the multiples of p, all numbers in this set are co-prime with p^k.
- There are p^{k-1} multiples of p in this set.
- Therefore,

$$\phi(p^k) = p^k - p^{k-1}.$$

Q.E.D.

Proof of (b) is omitted.

Unit 5.3

Euclidean Algorithm

Euclid (~300 B.C.)

Euclid

Who's Euclid?

(2.5 min) https://www.youtube.com/watch?v=440gbGszjk8

What's an Algorithm?

- An algorithm is a step-by-step method to solve a problem.
- (5 min) https://www.youtube.com/watch?v=6hfOvs8pY1k

How to find gcd(*a*, *b*)?

- **Method 1:** By Short Division
  - (pen-and-paper method in primary schools)

  i. Divide *a* and *b* by any of their common factor and obtain the corresponding quotients.

  ii. Let the two quotients be two new dividends.

  iii. Repeat Steps 1 and 2 until the two quotients obtained are relatively prime.

  iv. gcd(*a*, *b*) equals the product of all the dividers.

- Cons: Time consuming.

2	540	840
2	270	420
3	135	210
5	45	70
	9	14

co-prime

gcd (540, 840)
$= 2 \times 2 \times 3 \times 5$
$= 60$

How to find gcd(a, b)?

- **Method 2:** By a simple **for** loop

  Idea (assume $a > b$):
  - Test $b, b-1, b-2, \ldots$ until a divisor of both a and b is found.
- Example: gcd(12, 8)
  - 8 is not a divisor of 12
  - 7 is not a divisor of 12
  - 6 is a divisor of 12 but not a divisor of 8
  - 5 is not a divisor of 12
  - 4 is a divisor of both 12 and 8.
  - Therefore, gcd(12, 8) = 4.
- Cons: Time consuming.

Pseudo-Code for Method 2 (optional)

Procedure naïve_gcd(a, b)

Input: Two integers a and b with $a \geq b \geq 0$

Output: gcd(a, b)

$x := b$;

while $a \bmod x \neq 0$ or $b \bmod x \neq 0$

$\quad x := x - 1$;

return x;

How to find gcd(a, b)?

- **Method 3:** By Euclidean Algorithm

  Let a be the larger number, i.e., $a \geq b \geq 0$.

  The key idea is based on

$$\boxed{\gcd(a, b) = \gcd(b, a \bmod b).}$$

  i. If $b = 0$, then $\gcd(a, b) = a$. (Done!)
  ii. Otherwise, find $\gcd(b, a \bmod b)$. *Divide-and-conquer!*

- Pros: Very efficient.
  - It has been proved that the number of steps required is at most 5 times the number of digits of b.

Pseudo-Code for Euclidean Algorithm (optional)

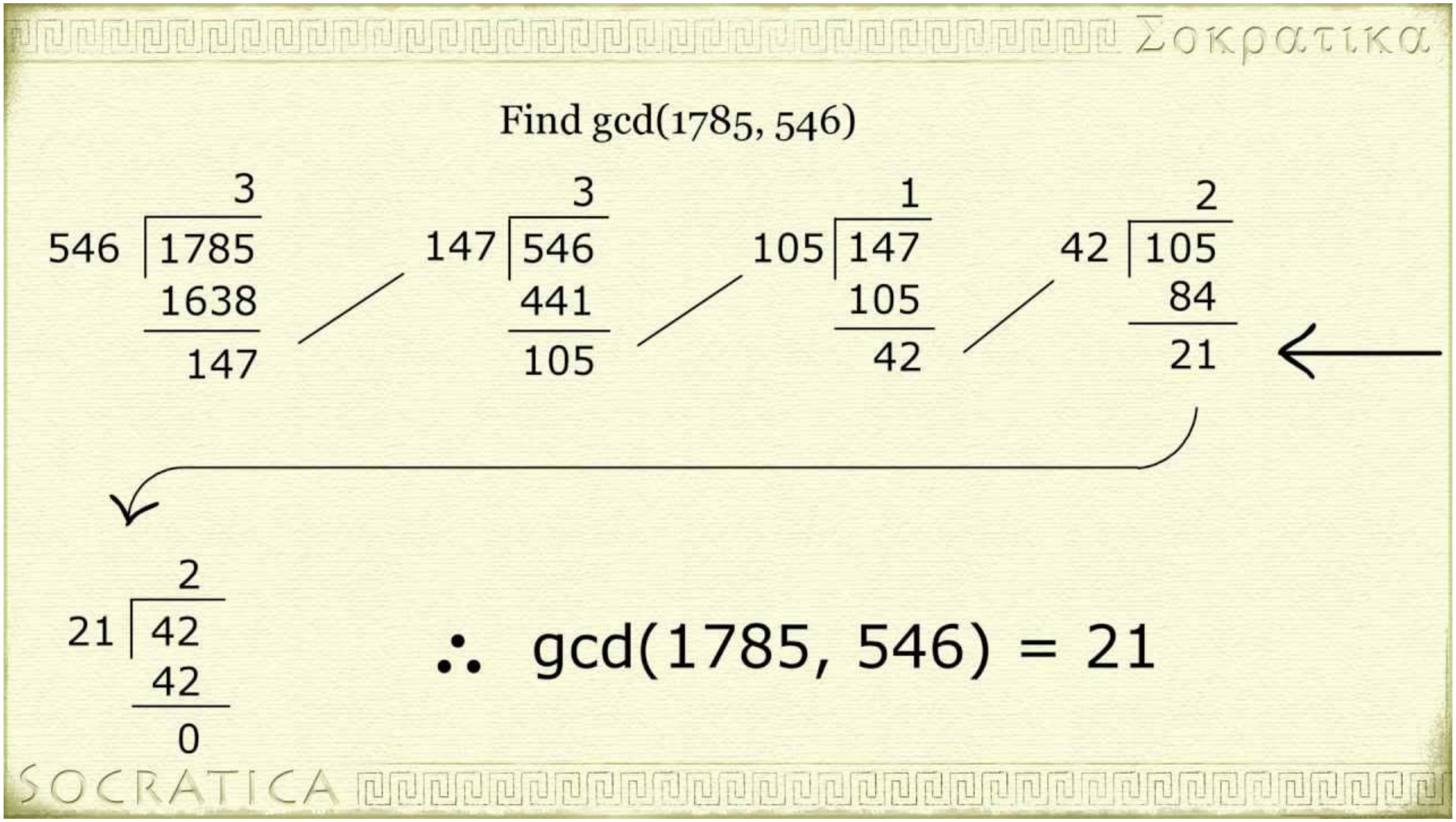
Procedure Euclid(a, b)

Input Two integers a and b with $a \geq b \geq 0$

Output gcd(a, b)

```
if b = 0,
        return a;
else
        return Euclid(b, a mod b);
```

Euclidean Algorithm: An Example



Euclidean Algorithm: An Example

(2 min) https://www.youtube.com/watch?v=fwuj4yzoX1o

Why does it Work?

Theorem: gcd(a, b) = gcd(b, r), where r = a mod b.

Proof:

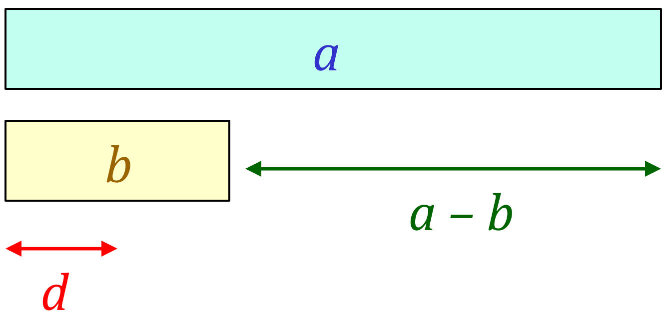
a) gcd(a, b) ≤ gcd(b, r).

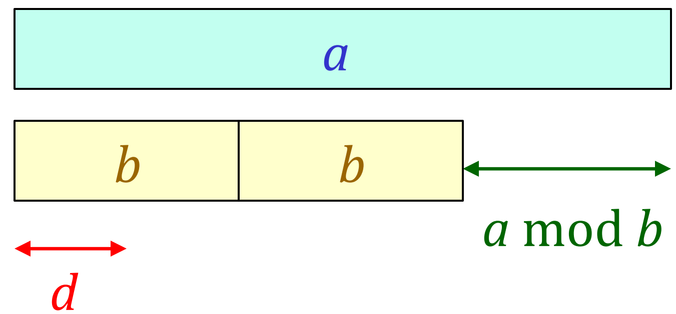
- Suppose d is a common divisor of a and b.
  - i.e., $a = dh$ and $b = dk$ for some integers h and k.
- Let $a = bq + r$. Then $r = (a - bq) = (dh - dkq) = d(h - kq)$.
- Therefore, d is a divisor of r.
  - In other words, d is a common divisor of b and r.
- A common divisor of a and b is also a common divisor of b and r.
- Therefore, gcd(a, b) ≤ gcd(b, r).

b) gcd(b, r) ≤ gcd(a, b). (It can be proved similarly.)

Hence, their gcds are equal. *Q.E.D.*

Theorem – Geometric Interpretation



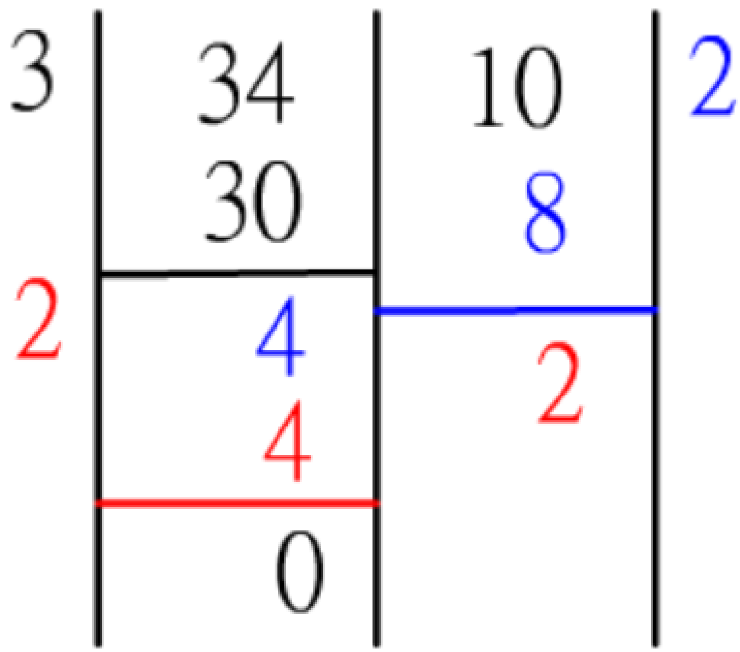


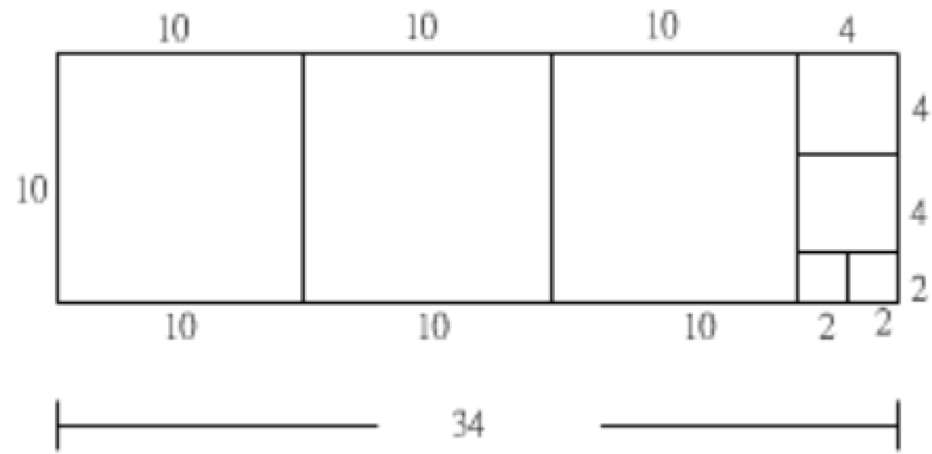
If d divides a and b, it also divides $a - b$.

If d divides a and b, it also divides $a \bmod b$.

$$\boxed{\text{Hence, } \gcd(a, b) = \gcd(b, a \bmod b).}$$

Pen-and-Paper Method





Geometric interpretation of Euclidean algorithm

Unit 5.4

Unique Factorization Theorem

How to Verify it?

$d = \gcd(a, b)$

I can check that *d* is a divisor of *a* and *b*. But is it the greatest one?

Certificate for gcd

Lemma: If d divides both a and b, and $d = ax + by$ for some integers x and y, then $d = \gcd(a, b)$.

Proof:

Since d is a common divisor of a and b,

$$d \leq \gcd(a, b).$$

Since $\gcd(a, b)$ divides both a and b, it divides $d = ax + by$,

$$\gcd(a, b) \leq d.$$

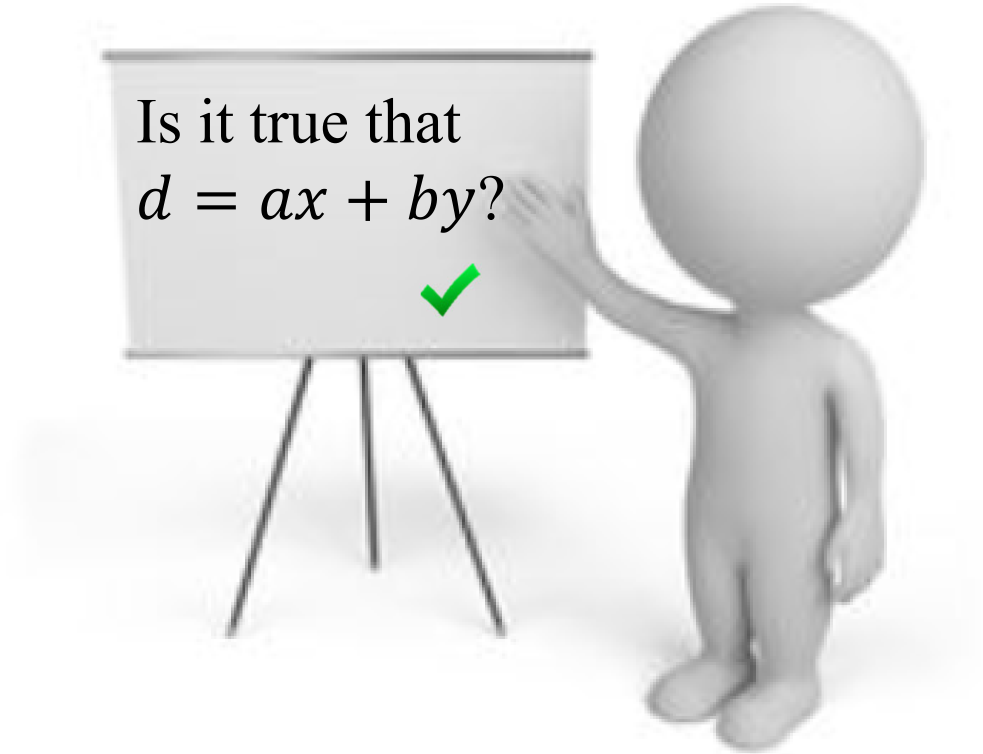
Hence,

$$d = \gcd(a, b).$$

Q.E.D.

How to Verify it?

$d = \gcd(a, b)$
Certificate: x, y



Can the Certificate always be Found? And How?

Can we always find integers x and y such that $\gcd(a,b) = ax + by$?

Yes, it is guaranteed by Bézout's identity.
(pronunciation: bay zoh)

In addition, x, y (as well as the gcd) can be computed by the extended Euclidean algorithm.

Bézout's Identity

There exists integers x and y such that
$\gcd(a, b) = ax + by$.

- x and y are called Bézout's coefficients.
- They are not unique.
- A pair of x, y can be computed by extended Euclidean algorithm, which serves as a constructive proof.

Example: Pen-and-Paper Method

$$1785(1) + 546(0) = 1785$$
$$1785(0) + 546(1) = 546$$
$$1785(1) + 546(-3) = 147$$
$$1785(-3) + 546(10) = 105$$
$$1785(4) + 546(-13) = 42$$
$$1785(-11) + 546(36) = 21$$

1785	546		
1	0	1785	(a)
0	1	546	(b)
1	–3	147	(c) = (a) – 3(b)
–3	10	105	(d) = (b) – 3(c)
4	–13	42	(e) = (c) – (d)
–11	36	21	(f) = (d) – 2(e)

$$\boxed{ax + by = d}$$

Stop because 42 is a multiple of 21.

Extending Euclid's Algorithm (optional)

- Recall that Euclidean algorithm is based on

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

- Assume that $d = \gcd(b, a \bmod b)$ and that

$$d = bx' + (a \bmod b)y'.$$

- Then

$$\begin{aligned} d &= bx' + \left(a - \left\lfloor \frac{a}{b} \right\rfloor b\right) y' \\ &= ay' + b\left(x' - \left\lfloor \frac{a}{b} \right\rfloor b\right) \end{aligned}$$

$\lfloor z \rfloor$: largest integer smaller than z.
e.g. $\left\lfloor \frac{13}{3} \right\rfloor = 4$

Pseudo-Code (optional)

Procedure ext-Euclid(a, b)

Input Two integers a and b with $a \geq b \geq 0$

Output Integers x, y, d such that $d = ax + by$

if $b = 0$,

  return $(1, 0, a)$;

else

  $(x', y', d) =$ ext-Euclid$(b, a \bmod b)$;

  return $(y', x' - \lfloor a/b \rfloor y', d)$;

Euclid's Lemma

Lemma: If p is prime and $p|ab$, then $p|a$ or $p|b$, for all integers a and b.

Proof:

If $p|a$, we are done.

Suppose $p \nmid a$. (we need to prove that $p|b$.)

Then, $\gcd(a, p) = 1$.

$\exists x, y \in \mathbb{N}, ax + py = 1$ (by Bézout's identity)

$abx + pby = b$ (multiply both sides by b)

Since p divides the left side, it also divides b.

Q.E.D.

Generalization of Euclid's lemma

Corollary: If p is prime and it divides a product of several integers, then p divides at least one of those integers.

Proof:

Suppose $p|a_1 a_2 \ldots a_k$.

By Euclid's lemma, $p|a_1$ or $p|a_2 \ldots a_k$.

Apply the lemma again and again, we obtain $p|a_1$ or $p|a_2$ or … or $p|a_k$.

Q.E.D.

Unique Factorization Theorem

Theorem:

Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers, $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}.$$

Moreover, this representation is unique up to (except for) the order of the factors.

- It is also called the fundamental theorem of arithmetic.

Proof (Existence) (optional)

- We prove by mathematical induction.
- (Base case) 2 is a prime.
- (Induction hypothesis) Assume the statement is true that for all integers from 2 up to $n - 1$.
- (Induction step) Consider the integer n.
  - If n is a prime, done.
  - If not, $n = ab$, where $1 < a \leq b < n$. By the induction hypothesis, both a and b are product of primes. Hence, $n = ab$ is also a product of primes.

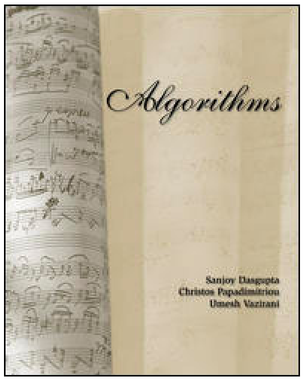
Q.E.D.

Proof (Uniqueness) (optional)

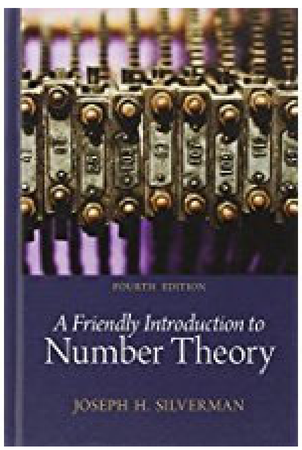
- Suppose a given number N has two representations:
$$N = p_1 p_2 \ldots p_m = q_1 q_2 \ldots q_n$$
- Note that $p_1 | q_1 q_2 \ldots q_n$.
- By Euclid's lemma, $p_1 | q_i$ for some *i.*
- Since q_i is prime, $p_1 = q_i$.
- Dividing N by p_1, we can reduce one factor from both representations.
- Reasoning the same way, we can show that $m \leq n$ and every p_i is a q_j.
- Applying the same argument with the role of p's and q's reversed, we can show that $n \leq m$ (hence $m = n$) and every q_j is a p_i.

Q.E.D.

Recommended Reading



- Section 1.2, S. Dasgupta, C. Papadimitriou, and U. Vazirani, *Algorithms*, McGraw-Hill, 2008.



- Chapters 5 and 7, J. H. Silverman, *A Friendly Introduction to Number Theory*, 4th ed., Pearson, 2013.