Numbers (8A)

Please send corrections (or suggestions) to youngwlim@hotmail.com.

This document was produced by using OpenOffice and Octave.

GCD

A 24-by-60 rectangle is covered with ten 12-by-12 square tiles, where 12 is the GCD of 24 and 60.

$24 = 2 \cdot 12 \Rightarrow 12 \mid 24 \Leftrightarrow 24 \text{ mod } 12 = 0$

$60 = 5 \cdot 12 \Rightarrow 12 \mid 60 \Leftrightarrow 60 \text{ mod } 12 = 0$

More generally, an a-by-b rectangle can be covered with square tiles of side-length d only if d is a common divisor of a and b

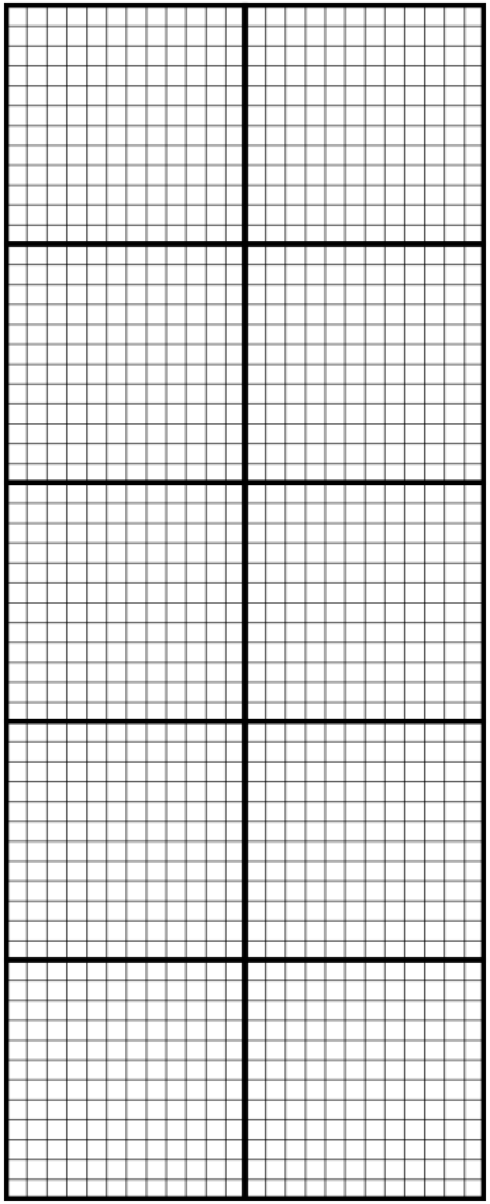
$d \mid a$
$d \mid b$

d : common divisor

the largest d : gcd

(greatest common divisor)

https://en.wikipedia.org/wiki/Greatest_common_divisor



LCM

What is the LCM of 4 and 6?

Multiples of 4 are:

4, 8, **12**, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, ...

and the multiples of 6 are:

6, **12**, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, ...

Common multiples of 4 and 6 are simply the numbers that are in both lists:

12, 24, 36, 48, 60, 72, ...

So, from this list of the first few common multiples of the numbers 4 and 6, their least common multiple is **12**.

https://en.wikipedia.org/wiki/Least_common_multiple

GCD * LCM

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_n^{a_n}$$

$$b = p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_n^{b_n}$$

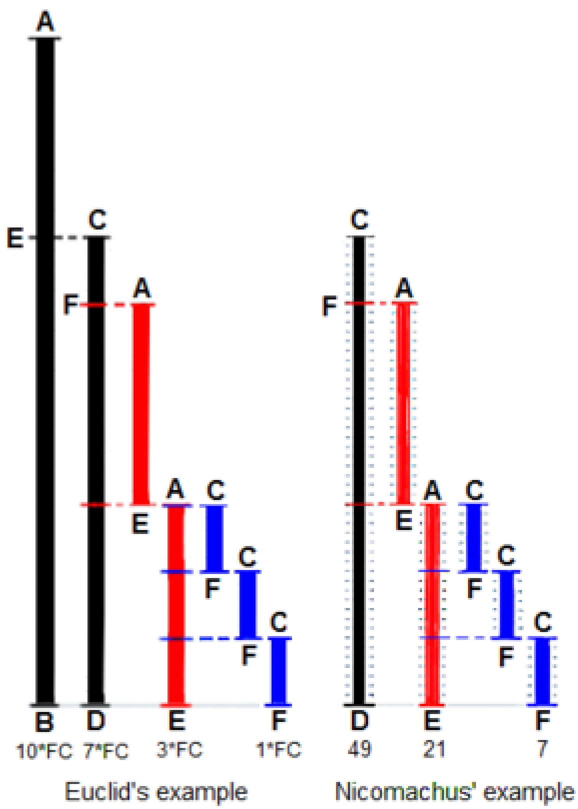
Prime Factorization

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

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

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

Finding common unit length



https://en.wikipedia.org/wiki/Euclidean_algorithm

Euclid's method for finding
the greatest common divisor (GCD)
of two starting lengths BA and DC,
both defined to be multiples of
a common "unit" length.

The length DC being shorter,
it is used to "measure" BA,
but only once because remainder EA is less than DC.

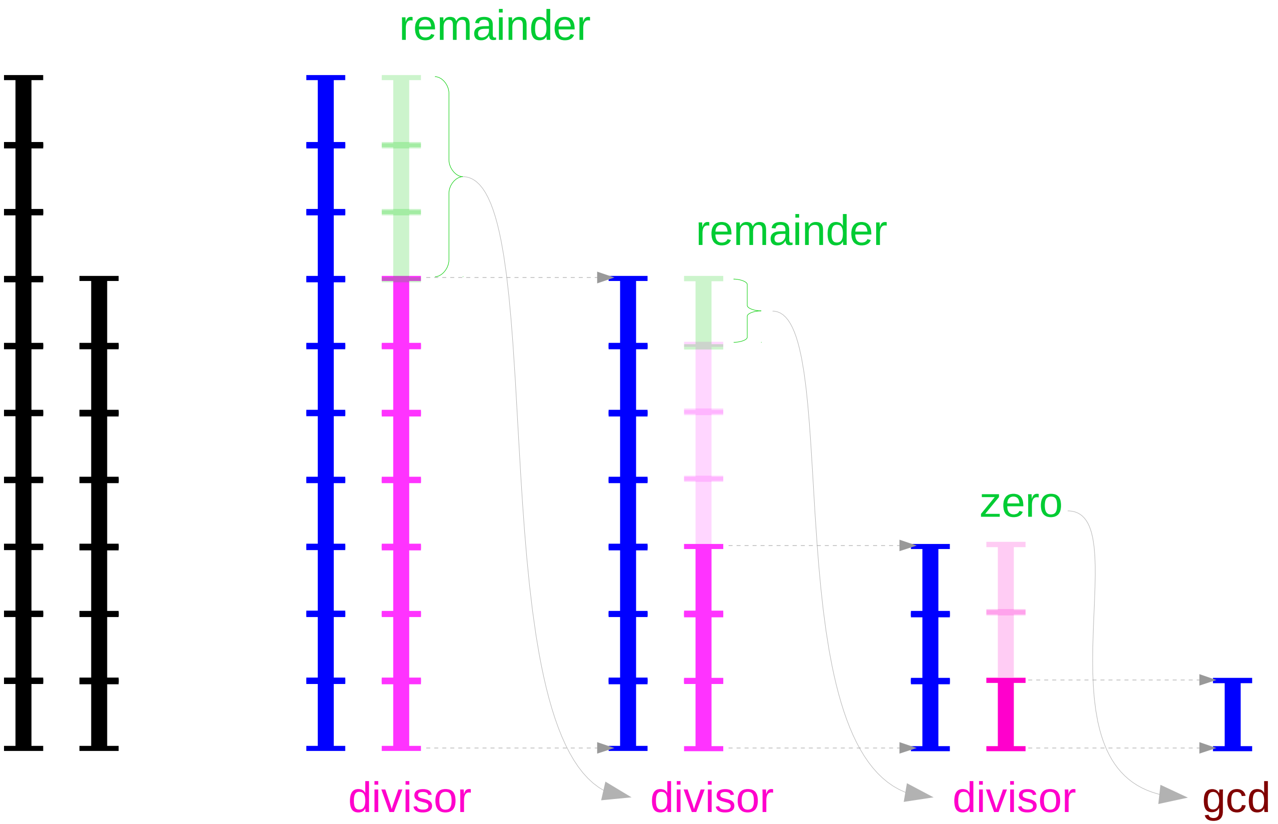
EA now measures (twice) the shorter length DC, with remainder FC shorter than EA.

Then FC measures (three times) length EA.

Because there is no remainder,
the process ends with FC being the GCD.

On the right Nicomachus' example with numbers 49 and 21 resulting in their GCD of 7 (derived from Heath 1908:300).

Euclid Algorithm Steps



https://en.wikipedia.org/wiki/Euclidean_algorithm

Euclid Algorithm

```
(%i3) factor(1071);
(%o3) 3^2 7 17

(%i4) factor(462);
(%o4) 2 3 7 11

(%i5) gcd(1071, 462);
(%o5) 21
```

Step k	Equation	Quotient and remainder
0	$1071 = q_0\, 462 + r_0$	$q_0 = 2$ and $r_0 = 147$
1	$462 = q_1\, 147 + r_1$	$q_1 = 3$ and $r_1 = 21$
2	$147 = q_2\, 21 + r_2$	$q_2 = 7$ and $r_2 = 0$; algorithm ends

$$1071 = 3^2 \cdot 7 \cdot 17$$

$$462 = 2 \cdot 3 \cdot 7 \cdot 11$$

$$gcd(1071, 462) = 3 \cdot 7 = 21$$

$$1071 = 2 \cdot 462 + 147$$

$$462 = 3 \cdot 147 + 21$$

$$147 = 7 \cdot 21 + 0$$

https://en.wikipedia.org/wiki/Euclidean_algorithm

Common Divisor

$1071 = 2 \cdot 462 + 147$

$462 = 3 \cdot 147 + 21$

$147 = 7 \cdot 21 + 0$

common divisor d

$d \mid 1071$ and $d \mid 462$

1071 **mod** $d = 0$	⟺	$d \mid 1071$
462 **mod** $d = 0$	⟺	$d \mid 462$

https://en.wikipedia.org/wiki/Euclidean_algorithm

Common Divisor Properties

common divisor d?

d | 1071 *and* d | 462 ➡ 1071 **mod** d = 0 *and* 462 **mod** d = 0

1071 = 2 · 462 + 147 remainder

(2 · 462 + 147) **mod** d = 0 ⇦ 1071 **mod** d = 0

2 · (462 **mod** d) + 147 **mod** d = 0 ⇦ 462 **mod** d = 0

2 · 0 + 147 **mod** d = 0

147 **mod** d = 0 ⇨ 147 **mod** d = 0

d | 462 *and* d | 147

https://en.wikipedia.org/wiki/Euclidean_algorithm

Reducing GCD Problems

$1071 = 2 \cdot 462 + 147$ | d | 1071 *and* d | 462 | $gcd(1071, 462)$

$462 = 3 \cdot 147 + 21$ | d | 462 *and* d | 147 | $gcd(462, 147)$

$147 = 7 \cdot 21 + 0$ | d | 147 *and* d | 21 | $gcd(147, 21)$

1071
462
147
21

https://en.wikipedia.org/wiki/Euclidean_algorithm

Linear Combination of gcd(1071, 462)=21

$1071 = 2 \cdot 462 + 147$ ⇒ $1071 - 2 \cdot 462 = 147$

$462 = 3 \cdot 147 + 21$ ⇒ $462 - 3 \cdot 147 = 21$ ⇒ $462 - 3 \cdot (1071 - 2 \cdot 462) = 21$

$7 \cdot 462 - 3 \cdot 1071 = 21$

$147 = 7 \cdot 21 + 0$

$gcd(1071, 462) = 21$
$= -3 \cdot 1071 + 7 \cdot 462$

$$gcd(a, b) = s\,a + t\,b$$

https://en.wikipedia.org/wiki/Euclidean_algorithm

Linear Combination of gcd(252, 198)=18

$252 = 1 \cdot 198 + 54$ → $252 - 1 \cdot 198 = 54$

$198 = 3 \cdot 54 + 36$ → $198 - 3 \cdot 54 = 36$

$54 = 1 \cdot 36 + 18$ → $54 - 1 \cdot 36 = 18$

$36 = 2 \cdot 18$

$(252 - 1 \cdot 198) - 1 \cdot (198 - 3 \cdot (252 - 1 \cdot 198)) = 18$

$252 - 1 \cdot 198 - (4 \cdot 198 - 3 \cdot 252) = 18$

$4 \cdot 252 - 5 \cdot 198 = 18$

https://en.wikipedia.org/wiki/Euclidean_algorithm

$$gcd(a, b) = s\,a + t\,b$$

Bezout's Identity – gcds as linear combinations

$a, \quad b \in \mathbf{Z}^+$

$$^\exists x, ^\exists y \in \mathbf{Z}$$

$$x a + y b = \mathbf{gcd}(a, b)$$

Bezout's coefficients (not unique)

Bezout's identities

Generally, a **linear combination** of a & b must be unique and its coefficients x & y need not be *integers*.

https://en.wikipedia.org/wiki/Euclidean_algorithm

Pairs of Bézout Coefficients Examples

$42 = 3 \cdot 12 + 6$ → $42 - 3 \cdot 12 = 6$

$12 = 2 \cdot 6$

$(1 \cdot 42 - 3 \cdot 12) = 6$

$(-3 \cdot 12 + 1 \cdot 42) = 6$

$\vdots$

$$12 \times -10 + 42 \times 3 = 6$$
$$12 \times -3 + 42 \times 1 = 6$$
$$12 \times 4 + 42 \times -1 = 6$$
$$12 \times 11 + 42 \times -3 = 6$$
$$12 \times 18 + 42 \times -5 = 6$$

$\vdots$

$$x\,a + y\,b = \gcd(a, b)$$

$$x \cdot 12 + y \cdot 42 = \gcd(12, 42)$$

Generally, x & y are not unique
unless a & b are relatively prime

https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity

Pairs of Bézout Coefficients – not unique

$$\vdots$$

$$12 \times -10 + 42 \times 3 = 6$$

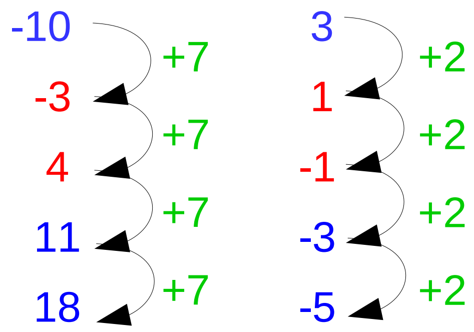
$$12 \times -3 + 42 \times 1 = 6$$

$$12 \times 4 + 42 \times -1 = 6$$

$$12 \times 11 + 42 \times -3 = 6$$

$$12 \times 18 + 42 \times -5 = 6$$

$$\vdots$$



42/6=7

|-3| < |7|
|4| < |7|

12/6=2

|1| < |2|
|-1| < |2|

https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity

Pairs of Bézout Coefficients – 2 minimal pairs

$$x\,a + y\,b = gcd(a, b)$$

$$\vdots$$

$$12 \times -10 + 42 \times 3 = 6$$
$$12 \times -3 + 42 \times 1 = 6$$
$$12 \times 4 + 42 \times -1 = 6$$
$$12 \times 11 + 42 \times -3 = 6$$
$$12 \times 18 + 42 \times -5 = 6$$

$$\vdots$$

42/6=7　　12/6=2

Among these pairs of Bézout coefficients, exactly two of them satisfy

$$|x| \le \left|\frac{b}{\gcd(a,b)}\right| \quad \text{and} \quad |y| \le \left|\frac{a}{\gcd(a,b)}\right|,$$

|-3| < |7|　　|1| < |2|
|4| < |7|　　|-1| < |2|

https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity

The Extended Euclidean Algorithm always produces one of these two minimal pairs.

Pairs of Bézout Coefficients – all pairs

$$x\,a + y\,b = gcd(a, b)$$

all pairs can be represented in the form

$$\left(x + k\frac{b}{\gcd(a,b)},\ y - k\frac{a}{\gcd(a,b)}\right),$$

$\vdots$

12×-10	$+$	42×3	$= 6$
12×-3	$+$	42×1	$= 6$
12×4	$+$	42×-1	$= 6$
12×11	$+$	42×-3	$= 6$
12×18	$+$	42×-5	$= 6$

$\vdots$

42/6=7 12/6=2

-3 + 7k 1 + 2k

The Extended Euclidean Algorithm always produces one of these two minimal pairs.

https://en.wikipedia.org/wiki/B%C3%A9zout%27s_identity

Extended Euclid Algorithm

$$r_0 = a \qquad r_1 = b$$
$$s_0 = 1 \qquad s_1 = 0$$
$$t_0 = 0 \qquad t_1 = 1$$
$$\vdots \qquad \vdots$$
$$r_{i+1} = r_{i-1} - q_i r_i \quad \text{and } 0 \le r_{i+1} < |r_i| \quad (\text{this defines } q_i)$$
$$s_{i+1} = s_{i-1} - q_i s_i$$
$$t_{i+1} = t_{i-1} - q_i t_i$$
$$\vdots$$

index i	quotient q_{i-1}	Remainder r_i	s_i	t_i
0		240	1	0
1		46	0	1
2	240 ÷ 46 = 5	240 − 5 × 46 = 10	1 − 5 × 0 = 1	0 − 5 × 1 = −5
3	46 ÷ 10 = 4	46 − 4 × 10 = 6	0 − 4 × 1 = −4	1 − 4 × −5 = 21
4	10 ÷ 6 = 1	10 − 1 × 6 = 4	1 − 1 × −4 = 5	−5 − 1 × 21 = −26
5	6 ÷ 4 = 1	6 − 1 × 4 = 2	−4 − 1 × 5 = −9	21 − 1 × −26 = 47
6	4 ÷ 2 = 2	4 − 2 × 2 = 0	5 − 2 × −9 = 23	−26 − 2 × 47 = −120

Given a & b, the extended Euclid algorithm produce the same coefficients.
Uniquely, one is chosen among many possible Bézout's coefficients

https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm

Relatively Prime Numbers

$$gcd(a, n) = 1$$

Relatively prime numbers a & n

$$s a + t n = 1$$

$$s a + t n \equiv 1 \pmod{n}$$

$$t n \bmod n = 0$$

$$s a \equiv 1 \pmod{n}$$

$$\bar{a} a \equiv 1 \pmod{n}$$

the **inverse** of a exists : s

linear combination of **gcd**(a, n)=1

Finding an modulo inverse

Finding an inverse of a modulo n

Relatively prime numbers a & n

Euclid Algorithm	$gcd(a, n) = 1$
↓	
Linear Combination	$s a + t n \equiv 1 \pmod{n}$
↓	
The inverse of a → s	$s a \equiv 1 \pmod{n}$

Linear Combination of gcd(101, 4620)=1

From Rosen's book

4620 = 45 · 101 + 75	4620 – 45 · 101 = 75	26·101–35·(4620–45·101) = –35·4620+1601·101
101 = 1 · 75 + 26	101 – 1 · 75 = 26	–9·75+26·(101–1·75) = 26·101–35·75
75 = 2 · 26 + 23	75 – 2 · 26 = 23	8·26–9·(75–2·26) = –9·75+26·26
26 = 1 · 23 + 3	26 – 1 · 23 = 3	–1·23+8·(26–1·23) = 8·26–9·23
23 = 7 · 3 + 2	23 – 7 · 3 = 2	3 – (23 – 7·3) = –1·23+8·3
3 = 1 · 2 + 1	3 – 1 · 2 = 1	3 – 1 · 2 = 1
2 = 2 · 1		

Young Won Lim
6/21/17

Inverse of 101 modulo 4620

1601

$4620 = 45 \cdot 101 + 75$

$-35 \cdot 4620 + 1601 \cdot 101 = 1$

$1601 \cdot 101 = 1 \pmod{4620}$

1601 is an inverse of 101 modulo 4620

Congruence

Etymology

Middle English, from Latin congruentia (“agreement”), from congruēns, present active participle of congruō (“meet together, agree”).

Noun: congruence (plural congruences)

The quality of agreeing or corresponding; being suitable and appropriate.

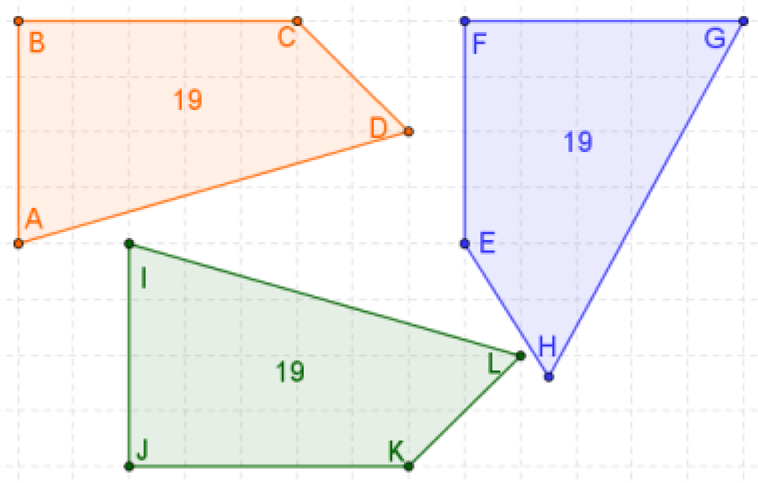
(mathematics, number theory) A relation between two numbers indicating they give the same remainder when divided by some given number.

(mathematics, geometry) The quality of being isometric — roughly, the same measure and shape.

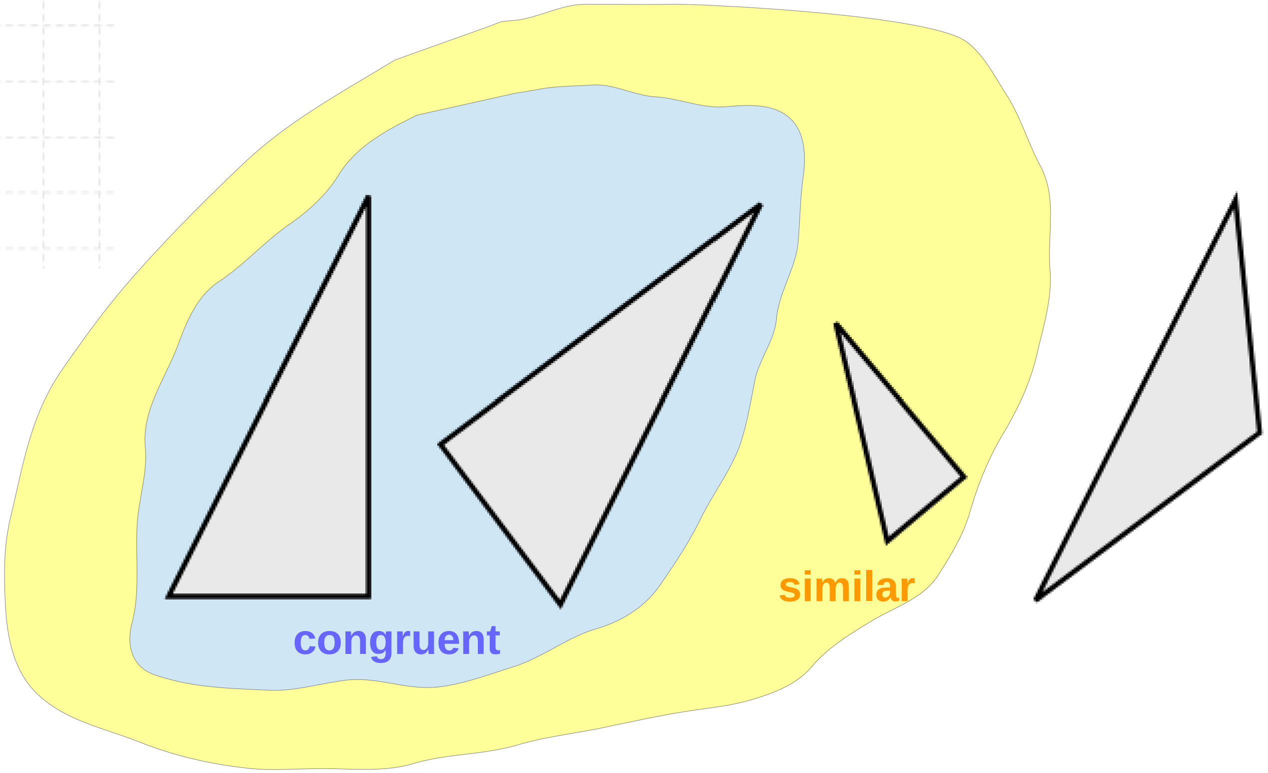
(algebra) More generally: any equivalence relation defined on an algebraic structure which is preserved by operations defined by the structure.

https://en.wiktionary.org/wiki/congruence

Congruence in Geometry



congruent



https://en.wikipedia.org/wiki/Congruence_(geometry)

Congruent modulo n

$$a \equiv b \pmod{n}$$

a is congruent to b modulo n

$$n \mid (a - b)$$

n divides (a-b)

$$(a - b) \bmod n = 0$$

$$(a \bmod n) = (b \bmod n)$$

the same remainder

A remainder is positive (0, .. n-1)

Congruence Relation

Modular arithmetic can be handled mathematically by introducing a congruence relation on the integers that is compatible with the operations on integers: addition, subtraction, and multiplication. For a positive integer n, two integers a and b are said to be **congruent modulo n**, written:

$$a \equiv b \pmod{n},$$

if their difference $a - b$ is an integer multiple of n (or n divides $a - b$). The number n is called the *modulus* of the congruence.

For example,

$$38 \equiv 14 \pmod{12}$$

because 38 − 14 = 24, which is a multiple of 12.

The same rule holds for negative values:

$$\begin{aligned} -8 &\equiv 7 \pmod{5} \\ 2 &\equiv -3 \pmod{5} \\ -3 &\equiv -8 \pmod{5}. \end{aligned}$$

Equivalently, $a \equiv b \bmod n$ can also be thought of as asserting that the remainders of the division of both a and b by n are the same. For instance:

$$38 \equiv 14 \pmod{12}$$

because both 38 and 14 have the same remainder 2 when divided by 12. It is also the case that 38 − 14 = 24 is an integer multiple of 12, which agrees with the prior definition of the congruence relation.

https://en.wikipedia.org/wiki/Modular_arithmetic

Properties of a Congruence Relation

A remark on the notation: Because it is common to consider several congruence relations for different moduli at the same time, the modulus is incorporated in the notation. In spite of the ternary notation, the congruence relation for a given modulus is binary. This would have been clearer if the notation $a \equiv_n b$ had been used, instead of the common traditional notation.

The properties that make this relation a congruence relation (respecting addition, subtraction, and multiplication) are the following.

If

$$a_1 \equiv b_1 \pmod{n}$$

and

$$a_2 \equiv b_2 \pmod{n},$$

then:

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$
- $a_1 - a_2 \equiv b_1 - b_2 \pmod{n}.$

The above two properties would still hold if the theory were expanded to include all real numbers, that is if a_1, a_2, b_1, b_2, n were not necessarily all integers. The next property, however, would fail if these variables were not all integers:

- $a_1 a_2 \equiv b_1 b_2 \pmod{n}.$

https://en.wikipedia.org/wiki/Modular_arithmetic

Remainders

The notion of modular arithmetic is related to that of the remainder in Euclidean division. The operation of finding the remainder is sometimes referred to as the modulo operation, and denoted with "mod" used as an infix operator. For example, the remainder of the division of 14 by 12 is denoted by $14 \bmod 12$; as this remainder is 2, we have $14 \bmod 12 = 2$.

The congruence, indicated by "≡" followed by "mod" between parentheses, means that the operator "mod", applied to both members, gives the same result. That is

$$A \equiv B \pmod{n}$$

is equivalent to

$$A \bmod n = B \bmod n.$$

The fundamental property of multiplication in modular arithmetic may thus be written

$$(a \bmod n)(b \bmod n) \equiv ab \pmod{n},$$

or, equivalently,

$$((a \bmod n)(b \bmod n)) \bmod n = (ab) \bmod n.$$

https://en.wikipedia.org/wiki/Modular_arithmetic

Linear Congruence Problems

$$a\,x \equiv b \pmod{n}$$

A linear congruence

$$find\ \ x = ?$$

$$a\,x = b$$

A linear equation

$$find\ \ x = ?$$

A remainder is positive (0, .. n-1)

Modular Multiplicative Inverse

A linear congruence

$$a\,x \equiv b \pmod{n}$$

$$\bar{a}\,a \equiv 1 \pmod{n}$$

$$\bar{a}\,a\,x \equiv \bar{a}\,b \pmod{n}$$

$$x \equiv \bar{a}\,b \pmod{n}$$

A linear equation

$$a\,x = b$$

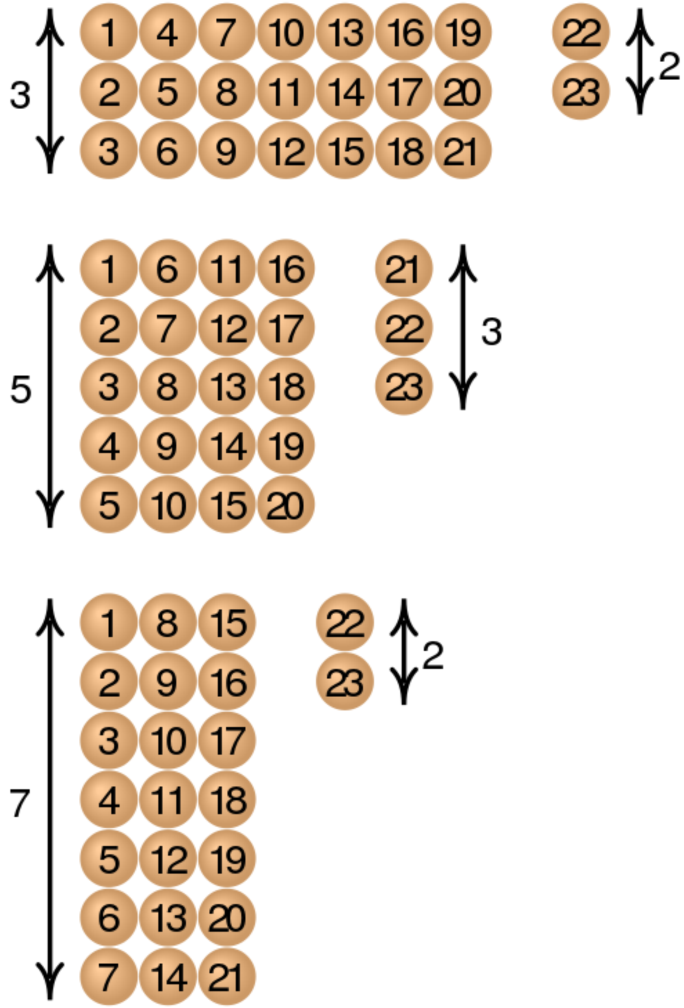
$$a^{-1}a = 1$$

$$a^{-1}a\,x = a^{-1}b$$

$$x = a^{-1}b$$

A remainder is positive (0, .. n-1)

Chinese Remainder Theorem



https://en.wikipedia.org/wiki/Chinese_remainder_theorem

$$x \equiv 2 \pmod{3}$$

and

$$x \equiv 3 \pmod{5}$$

and

$$x \equiv 2 \pmod{7}$$

Sunzi's original formulation:
x
≡ 2 (mod 3)
≡ 3 (mod 5)
≡ 2 (mod 7)
with the solution
$x = 23 + 105k$ where $k \in \mathbb{Z}$

Chinese Remainder Theorem

$x \equiv a_1 \pmod{m_1}$ and

$x \equiv a_2 \pmod{m_2}$ and

• • •

$x \equiv a_n \pmod{m_n}$

$m_1, \; m_2, \; \cdots \; m_n$ *pairwise relatively prime*

$x \equiv b \pmod{m_1 m_2 \cdots m_n}$ *has a unique solution*

https://en.wikipedia.org/wiki/Chinese_remainder_theorem

m_i, m, and M_i

$$x \equiv 2 \pmod{3}$$
$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

$$m_1 = 3$$
$$m_2 = 5$$
$$m_3 = 7$$

$$m = 3 \cdot 5 \cdot 7 = 105$$

$$M_1 = m/m_1 = 3 \cdot 5 \cdot 7/3 = 35$$
$$M_2 = m/m_2 = 3 \cdot 5 \cdot 7/5 = 21$$
$$M_3 = m/m_3 = 3 \cdot 5 \cdot 7/7 = 15$$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

$$m = m_1 m_2 m_3$$

$$M_1 = m/m_1 = m_2 m_3$$
$$M_2 = m/m_2 = m_1 m_3$$
$$M_3 = m/m_3 = m_1 m_2$$

$$M_1 \ \mathbf{mod} \ m_2 = M_1 \ \mathbf{mod} \ m_3 = 0$$
$$M_2 \ \mathbf{mod} \ m_1 = M_2 \ \mathbf{mod} \ m_3 = 0$$
$$M_3 \ \mathbf{mod} \ m_1 = M_3 \ \mathbf{mod} \ m_2 = 0$$

$$M_i \ \mathbf{mod} \ m_j = M_j \ \mathbf{mod} \ m_i = 0$$
$$\text{for } i \neq j$$

Inverse of M_i

$m_1, \; m_2, \; m_3 \; : \; \textit{pairwise relatively coprime}$

$\mathbf{gcd}(M_1, m_1) = 1 \;\Rightarrow\; M_1 \cdot y_1 = 1 \pmod{m_1}$ — y_1 : the inverse of M_1 — $m_2 m_3$

$\mathbf{gcd}(M_2, m_2) = 1 \;\Rightarrow\; M_2 \cdot y_2 = 1 \pmod{m_2}$ — y_2 : the inverse of M_2 — $m_1 m_3$

$\mathbf{gcd}(M_3, m_3) = 1 \;\Rightarrow\; M_3 \cdot y_3 = 1 \pmod{m_3}$ — y_3 : the inverse of M_3 — $m_1 m_2$

$M_1 \cdot y_1 = 1 \pmod{m_1}$	$M_1 \cdot y_1 = 0 \pmod{m_2}$	$M_1 \cdot y_1 = 0 \pmod{m_3}$	$m_2 m_3$
$M_2 \cdot y_2 = 0 \pmod{m_1}$	$M_2 \cdot y_2 = 1 \pmod{m_2}$	$M_2 \cdot y_2 = 0 \pmod{m_3}$	$m_1 m_3$
$M_3 \cdot y_3 = 0 \pmod{m_1}$	$M_3 \cdot y_3 = 0 \pmod{m_2}$	$M_3 \cdot y_3 = 1 \pmod{m_3}$	$m_1 m_2$

Sum of $a_i M_i y_i$

$$
\begin{array}{llll}
a_1 & M_1 \cdot y_1 = 1 \ (\textbf{mod } m_1) & M_1 \cdot y_1 = 0 \ (\textbf{mod } m_2) & M_1 \cdot y_1 = 0 \ (\textbf{mod } m_3) \\
a_2 & M_2 \cdot y_2 = 0 \ (\textbf{mod } m_1) & M_2 \cdot y_2 = 1 \ (\textbf{mod } m_2) & M_2 \cdot y_2 = 0 \ (\textbf{mod } m_3) \\
a_3 & M_3 \cdot y_3 = 0 \ (\textbf{mod } m_1) & M_3 \cdot y_3 = 0 \ (\textbf{mod } m_2) & M_3 \cdot y_3 = 1 \ (\textbf{mod } m_3)
\end{array}
$$

$$
\begin{array}{lll}
a_1 M_1 \cdot y_1 = a_1 \ (\textbf{mod } m_1) & a_1 M_1 \cdot y_1 = 0 \ (\textbf{mod } m_2) & a_1 M_1 \cdot y_1 = 0 \ (\textbf{mod } m_3) \\
a_2 M_2 \cdot y_2 = 0 \ (\textbf{mod } m_1) & a_2 M_2 \cdot y_2 = a_2 \ (\textbf{mod } m_2) & a_2 M_2 \cdot y_2 = 0 \ (\textbf{mod } m_3) \\
a_3 M_3 \cdot y_3 = 0 \ (\textbf{mod } m_1) & a_3 M_3 \cdot y_3 = 0 \ (\textbf{mod } m_2) & a_3 M_3 \cdot y_3 = a_3 \ (\textbf{mod } m_3)
\end{array}
$$

$$a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3 = a_1 M_1 \cdot y_1 = a_1 \ (\textbf{mod } m_1)$$

$$a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3 = a_2 M_2 \cdot y_2 = a_2 \ (\textbf{mod } m_2)$$

$$a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3 = a_3 M_3 \cdot y_3 = a_3 \ (\textbf{mod } m_3)$$

X = Sum of $a_i M_i y_i$

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$x \equiv a_3 \pmod{m_3}$$

$$a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3 = a_1 M_1 \cdot y_1 = a_1 \pmod{m_1}$$
$$a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3 = a_2 M_2 \cdot y_2 = a_2 \pmod{m_2}$$
$$a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3 = a_3 M_3 \cdot y_3 = a_3 \pmod{m_3}$$

$$x = a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3$$

Chinese Remainder Examples (1)

$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$
$x \equiv 2 \pmod{7}$

$m_1 = 3$
$m_2 = 5$
$m_3 = 7$

$3 \cdot 5 \cdot 7 = 105 = m$

$M_1 = m/m_1 = 3\cdot 5\cdot 7/3 = 35$ $\quad m_2 m_3$
$M_2 = m/m_2 = 3\cdot 5\cdot 7/5 = 21$ $\quad m_1 m_3$
$M_3 = m/m_3 = 3\cdot 5\cdot 7/7 = 15$ $\quad m_1 m_2$

$M_1 = 2 \pmod{m_1}$	$M_1 = 0 \pmod{m_2}$	$M_1 = 0 \pmod{m_3}$	$m_2 m_3$
$M_2 = 0 \pmod{m_1}$	$M_2 = 1 \pmod{m_2}$	$M_2 = 0 \pmod{m_3}$	$m_1 m_3$
$M_3 = 0 \pmod{m_1}$	$M_3 = 0 \pmod{m_2}$	$M_3 = 1 \pmod{m_3}$	$m_1 m_2$

$M_1 \cdot y_1 = 35 \cdot 2 = 2 \cdot 2 = 1 \pmod{3}$ $\qquad y_1\ (=2)$: *the inverse of* $M_1\ (=35)$
$M_2 \cdot y_2 = 21 \cdot 1 = 1 \cdot 1 = 1 \pmod{5}$ $\qquad y_2\ (=1)$: *the inverse of* $M_2\ (=21)$
$M_3 \cdot y_3 = 15 \cdot 1 = 1 \cdot 1 = 1 \pmod{7}$ $\qquad y_3\ (=1)$: *the inverse of* $M_3\ (=15)$

$M_1 \cdot y_1 = 1 \pmod{m_1}$	$M_1 \cdot y_1 = 0 \pmod{m_2}$	$M_1 \cdot y_1 = 0 \pmod{m_3}$
$M_2 \cdot y_2 = 0 \pmod{m_1}$	$M_2 \cdot y_2 = 1 \pmod{m_2}$	$M_2 \cdot y_2 = 0 \pmod{m_3}$
$M_3 \cdot y_3 = 0 \pmod{m_1}$	$M_3 \cdot y_3 = 0 \pmod{m_2}$	$M_3 \cdot y_3 = 1 \pmod{m_3}$

Chinese Remainder Examples (2)

$M_1 \cdot y_1 = 35 \cdot 2 = 2 \cdot 2 = 1 \pmod{3}$ $\quad y_1\ (=2)$: *the inverse of* $M_1\ (=35)$

$M_2 \cdot y_2 = 21 \cdot 1 = 1 \cdot 1 = 1 \pmod{5}$ $\quad y_2\ (=1)$: *the inverse of* $M_2\ (=21)$

$M_3 \cdot y_3 = 15 \cdot 1 = 1 \cdot 1 = 1 \pmod{7}$ $\quad y_3\ (=1)$: *the inverse of* $M_3\ (=15)$

$M_1 = 35$ $\qquad y_1 = -1 + 3 * k$

$35 = 11 \cdot 3 + 2$ ↓ $\quad 35 - 11 \cdot 3 = 2$ ↑ $\quad 3 - 1 \cdot (35 - 11 \cdot 3) = -1 \cdot 35 + 12 \cdot 3$

$3 = 1 \cdot 2 + 1$ $\quad 3 - 1 \cdot 2 = 1$ $\quad 3 - 1 \cdot 2 = 1$

$M_2 = 21$ $\qquad y_2 = 1 + 5 * k$

$21 = 4 \cdot 5 + 1$ ↓ $\quad 21 - 4 \cdot 5 = 1$ ↑ $\quad 1 \cdot 21 - 4 \cdot 5 = 1$

$M_3 = 15$ $\qquad y_3 = 1 + 7 * k$

$15 = 2 \cdot 7 + 1$ ↓ $\quad 15 - 2 \cdot 7 = 1$ ↑ $\quad 1 \cdot 15 - 2 \cdot 7 = 1$

Chinese Remainder Examples (3)

a_1	$M_1 \cdot y_1 = 1 \pmod{m_1}$	$M_1 \cdot y_1 = 0 \pmod{m_2}$	$M_1 \cdot y_1 = 0 \pmod{m_3}$
a_2	$M_2 \cdot y_2 = 0 \pmod{m_1}$	$M_2 \cdot y_2 = 1 \pmod{m_2}$	$M_2 \cdot y_2 = 0 \pmod{m_3}$
a_3	$M_3 \cdot y_3 = 0 \pmod{m_1}$	$M_3 \cdot y_3 = 0 \pmod{m_2}$	$M_3 \cdot y_3 = 1 \pmod{m_3}$

$$m_1 = 3$$
$$m_2 = 5$$
$$m_3 = 7$$

$$x = a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3$$

$$x = a_1 M_1 \cdot y_1 = a_1 \pmod{m_1}$$
$$x = a_2 M_2 \cdot y_2 = a_2 \pmod{m_2}$$
$$x = a_3 M_3 \cdot y_3 = a_3 \pmod{m_3}$$

$$M_1 = 3 \cdot 5 \cdot 7 / 3 = 5 \cdot 7 = 35$$
$$M_2 = 3 \cdot 5 \cdot 7 / 5 = 3 \cdot 7 = 21$$
$$M_3 = 3 \cdot 5 \cdot 7 / 7 = 3 \cdot 5 = 15$$

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

$$x = 233 = 23 \pmod{105}$$

$$m = 3 \cdot 5 \cdot 7 = 105$$

Chinese Remainder Summary

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$x \equiv a_3 \pmod{m_3}$

$m = m_1 m_2 m_3$

$M_1 = m/m_1 = m_2 m_3$
$M_2 = m/m_2 = m_1 m_3$
$M_3 = m/m_3 = m_1 m_2$

$m_1, \; m_2, \; m_3$: *pairwise relatively coprime*

$\gcd(M_1, m_1) = 1 \;\Rightarrow\; M_1 \cdot y_1 = 1 \pmod{m_1}$ — y_1 : *the inverse of* M_1

$\gcd(M_2, m_2) = 1 \;\Rightarrow\; M_2 \cdot y_2 = 1 \pmod{m_2}$ — y_2 : *the inverse of* M_2

$\gcd(M_3, m_3) = 1 \;\Rightarrow\; M_3 \cdot y_3 = 1 \pmod{m_3}$ — y_3 : *the inverse of* M_3

$$x = a_1 M_1 \cdot y_1 + a_2 M_2 \cdot y_2 + a_3 M_3 \cdot y_3$$

Chinese Remainder Theorem

Let $n_1, ..., n_k$ be integers greater than 1, which are often called *moduli* or *divisors*. Let us denote by N the product of the n_i.

The Chinese remainder theorem asserts that if the n_i are pairwise coprime, and if $a_1, ..., a_k$ are integers such that $0 \le a_i < n_i$ for every i, then there is one and only one integer x, such that $0 \le x < N$ and the remainder of the Euclidean division of x by n_i is a_i for every i.

This may be restated as follows in term of congruences: If the n_i are pairwise coprime, and if $a_1, ..., a_k$ are any integers, then there exists an integer x such that

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned},$$

and any two such x are congruent modulo N.[11]

https://en.wikipedia.org/wiki/Chinese_remainder_theorem

Upper and Lower Bounds

https://en.wikipedia.org/wiki/Algorithm

References

[1] http://en.wikipedia.org/
[2]