

Mr's G's Little Book on

Congruencies

Definitions

We define $a \equiv b \pmod{m}$

This is an equivalence, where

$$a, b, m \in \mathbf{Z}$$

and $m \neq 0$

b is the remainder when a is divided by m , noting that b is not necessarily the least remainder. So

$$a - b = km \text{ where } k \in \mathbf{Z}$$

$$\text{eg } 17 \equiv 2 \pmod{5}$$

$$17 - 2 = 3 \times 5$$

Corollary 1

$$\text{if } a \equiv b \pmod{m}$$

$$\text{then } a \equiv (b \pm m) \pmod{m}$$

$$\textbf{Proof } a - b = km$$

$$\text{so } a - b \pm m = (k \pm 1)m$$

$$\text{eg } 17 - 2 \pm 5 = (3 \pm 1)5$$

Corollary 2

For $a = b$

$$\text{then } b \equiv b \pmod{m}$$

for every arbitrary natural number m

$$\text{eg } b - b = 0 \times m \text{ (ie } k = 0)$$

Corollary 3

$$\text{if } a \equiv b \pmod{m} \text{ then}$$

$$ak \equiv bk \pmod{mk}$$

$$\text{for } k \in \mathbf{Q}$$

$$\text{providing } ak, bk, mk \in \mathbf{Q}$$

Example

$$\text{let } k = 2/3$$

$$17 \times 2/3 \equiv 2 \times 2/3 \pmod{5 \times 2/3} \text{ because}$$

$$17 \times 2/3 - 2 \times 2/3 = 3 \times 5 \times 2/3 \quad \text{TRUE}$$

Corollary 4

$$kax \equiv a \pmod{a}$$

$$\text{eg } 3 \times 17 \times x = 17 \pmod{17} \text{ because}$$

$$3 \times 17 \times x \equiv k \times 17 \text{ as we fix } k = 3x$$

Alternative Definition

$$\text{For } a \equiv b \pmod{m}$$

when a is divided by m the positive remainder is the same as when b is divided by m conditional that the remainder b is less than m .

$$\text{eg } 17 \div 5 \text{ has remainder } 2 \text{ and}$$

$$2 \div 5 \text{ also has remainder of } 2.$$

Proof

$$\text{If } a \equiv b \pmod{m}$$

$$\text{then } a = mq_1 + r_1$$

$$\text{and } b = mq_2 + r_2$$

$$\text{and } (a-b)/m = (q_1 - q_2) + (r_1 - r_2)/m$$

As $(a-b)/m$ is an integer by definition then $(r_1 - r_2)/m$ must also be an integer.

But as we have stipulated that

$$r_1 \text{ and } r_2 < m \text{ then } r_1 - r_2 = 0 \text{ ie } r_1 = r_2$$

Examples of Congruencies

$$75 \equiv 3 \pmod{12} \quad 10 \equiv -18 \pmod{4}$$

$$-1 \equiv 3 \pmod{4} \quad 5 = 5 \pmod{m}$$

Theorem 1

If $a \equiv b \pmod{m}$

and $c \equiv d \pmod{m}$

then

$$(a \pm c) \equiv b \pm d \pmod{m}$$

Proof

let $a = b + sm$

and $c = d + tm$

then $a + c = b + d + m(s + t)$

now as $s + t$ must be an integer

then $d + m(s + t)$ implies $d \pmod{m}$

so we have $(a \pm c) \equiv b \pm d \pmod{m}$

Converse

If we can break down a congruence

into $(a + c) \equiv b + d \pmod{m}$

and if we can show that $a \equiv b \pmod{m}$

then it must follow that $b \equiv d \pmod{m}$

Example 1

$$23 \equiv 3 \pmod{10}$$

$$27 \equiv 7 \pmod{10}$$

$$\text{so } 50 \equiv 3 + 7 \pmod{10}$$

$$\text{and } 50 \equiv 7 + 3 \pmod{10}$$

Theorem 2

If $a \equiv b \pmod{m}$

and $c \equiv d \pmod{m}$

then $ac \equiv bd \pmod{m}$

Proof

let $a = b + sm$

and $c = d + tm$

$$ac = (b + sm)(d + tm)$$

$$= bd + smd + tmb + stmn$$

$$ac = bd + m(bt + sd + stn)$$

and following the same argument from

Theorem 1 we have

$$ac \equiv bd \pmod{m}$$

Example 2

$$23 \equiv 3 \pmod{10}$$

$$27 \equiv 7 \pmod{10}$$

$$\text{so } 621 \equiv 21 \pmod{10} \quad \text{TRUE}$$

Remembering our initial proviso that “b” need not necessarily be the least remainder.

Theorem 3

If $a \equiv b \pmod{m}$ then by Theorem 2

If $a^2 \equiv b^2 \pmod{m}$ and in general

If $a^n \equiv b^n \pmod{m}$ for n positive

However note that if $a^n \equiv b^n \pmod{m}$ it does not necessarily follow that

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

Example 3a

$$23 \equiv 3 \pmod{10}$$

$$23^2 \equiv 3^2 \pmod{10}$$

$$529 \equiv 9 \pmod{10} \quad \text{TRUE}$$

Example 3b

$$23^3 \equiv 3^3 \pmod{10}$$

$$12167 \equiv 27 \pmod{10} \quad \text{TRUE}$$

Example 3c

$$\text{while } 11^2 \equiv 2^2 \pmod{13} \quad \text{TRUE}$$

$$11 \equiv 2 \pmod{13} \quad \text{NOT TRUE}$$

Theorem 4 (transitivity)

$$\text{if } a \equiv b \pmod{m}$$

$$\text{and } b \equiv c \pmod{m}$$

$$\text{then } a \equiv c \pmod{m}$$

Proof

$$\text{if } a = b + sm$$

$$\text{and } b = c + tm$$

$$\text{then } a = c + (s + t)m$$

$$\text{hence } a \equiv c \pmod{m}$$

following the same argument as

Theorem 1

Example 4

$$\text{If } 15 \equiv 1 \pmod{7}$$

$$\text{and } 1 \equiv -6 \pmod{7}$$

$$\text{then } 15 \equiv -6 \pmod{7}$$

This technique can be used to solve linear congruencies.

Theorem 5

$$\text{if } \text{hcf}(r, m) = 1$$

$$\text{then } ar \equiv br \pmod{m}$$

$$\text{implies } a \equiv b \pmod{m}$$

Proof

$$\text{if } ra \equiv rb \pmod{m}$$

$$\text{then } r(a-b)/m \text{ is an integer}$$

$$\text{but if } \text{hcf}(r, m) = 1$$

$$\text{then } (a-b)/m \text{ is also an integer}$$

The remaining part of the proof is assumed but follows from standard number theory.

Example 5a

$$\text{if } 69 \equiv 6 \pmod{7}$$

$$\text{then } 3 \times 23 \equiv 3 \times 2 \pmod{7}$$

$$\text{now as } \text{hcf}(3, 7) = 1$$

we can divide through by 3 to get

$$23 \equiv 2 \pmod{7} \quad \text{TRUE}$$

Example 5b

$$\text{but note } 42 \equiv 18 \pmod{4} \quad \text{TRUE}$$

$$6 \times 7 \equiv 6 \times 3 \pmod{4}$$

$$\text{we still have } 7 \equiv 3 \pmod{4}$$

$$\text{even though } \text{hcf}(6, 4) = 2$$

but just because

$$30 \equiv 2 \pmod{4}$$

it doesn't follow that

$$15 \equiv 1 \pmod{4}$$

because $\text{hcf}(2, 4) \neq 1$

although by corollary 3

$$15 \equiv 1 \pmod{2}$$

Theorem 6

if $ab \equiv 0 \pmod{m}$

this does not necessarily imply that

$a \equiv 0 \pmod{m}$ NOR $b \equiv 0 \pmod{m}$

However

if $ab \equiv 0 \pmod{m}$

and $\text{hcf}(b, m) = 1$

then it does follow that

$$a \equiv 0 \pmod{m}$$

Example 6a

$$32 \equiv 0 \pmod{16}$$

$$4 \times 8 \equiv 0 \pmod{16} \quad \text{TRUE}$$

$$\text{but } 4 \equiv 0 \pmod{16} \quad \text{NOT TRUE}$$

$$\text{and } 8 \equiv 0 \pmod{16} \quad \text{NOT TRUE}$$

Example 6b

However

$$105 \equiv 0 \pmod{5} \quad \text{TRUE}$$

$$\text{so } 35 \times 3 \equiv 0 \pmod{5} \quad \text{TRUE}$$

$$\text{and } 35 \equiv 0 \pmod{5}$$

because $\text{hcf}(3, 5) = 1$

Solution of Linear Congruencies

Let $ax \equiv b \pmod{m}$

which is equivalent to the Diophantine equation

$$ax - my = b$$

To obtain solutions we are investigating

$$\text{hcf}(a, m) = bk$$

There are three inter-related results of linear congruencies in one unknown

1) $ax \equiv b \pmod{m}$

has no solutions if

$$b /_{\text{hcf}(a, m)} \neq k$$

2) $ax \equiv b \pmod{m}$

has $\text{hcf}(a, m)$ distinct solutions if

$$b /_{\text{hcf}(a, m)} = k$$

3) $ax \equiv b \pmod{m}$

and $\text{hcf}(a, m) = 1$

then there is one distinct solution

1) and 3) are corollaries of 2)

Examples

a) $2x \equiv 1 \pmod{2}$

has no solutions because

$2x - 1$ is odd

and $2k$ is even

so effectively we have

$$1 /_{\text{hcf}(2, 2)} \neq k$$

b) $8x \equiv 16 \pmod{12}$

so by inspection solutions are

$$x = 2 \text{ (14, 26, 38, etc.)}$$

$$x = 5 \text{ (17, 29, 41, etc.)}$$

$$x = 8 \text{ (20, 32, 44, etc.)}$$

$$x = 11 \text{ (23, 35, 47, etc.)}$$

This is because $\text{hcf}(8, 12) = 4$ so there are 4 distinct solutions.

The solution set is

$$x = 2 + 3k \text{ (} k = 0, 1, 2, \dots \text{)}$$

c) $2x \equiv 3 \pmod{5}$

$\text{hcf}(2,5) = 1$

so we are seeking just one solution

$2 \times 4 \equiv 3 \pmod{5}$ TRUE

and our solution set is

$x = 4 + 5k \ (k = 0, 1, 2, \dots)$

Fermat's Little Theorem

For p prime and $a^{p-1} \equiv 1 \pmod{p}$

If we remove the restriction on a , the theorem can be restated

$a^p \equiv a \pmod{p}$ and only if p is prime

eg $3^5 \equiv 3 \pmod{5}$

The RSA cryptosystem, which encodes most secure internet traffic is based on Fermat's Little Theorem

Example

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

So as $5^3 - 5 = 120$ then

$120 \equiv 0 \pmod{3}$ TRUE

because 3 is prime

but $3^4 \equiv 3 \pmod{4}$ NOT TRUE

because 4 is not prime

Wilson's Theorem

For any prime p

$1 \times 2 \times 3 \dots (p-1) + 1 /_p$ is an integer

Hence we state

$(p-1) + 1 \equiv 0 \pmod{p}$

The converse also holds

If $(p-1)! + 1 \equiv 0 \pmod{p}$

then p is prime though an extremely inefficient way of checking primality.

A consequence of Wilson's Theorem is that if $p = 4k + 1$

then $x^2 + 1 \equiv 0 \pmod{p}$ has a solution

Example

let $p = 7$ (a prime)

$1 \times 2 \times 3 \times 4 \times 5 \times 6 + 1 /_7 = 103$ an integer.

Euler's Totient Function

ϕ is pronounced "phi"

If m is a natural number then $\phi(m)$ is the number of natural numbers less than or equal to m and relatively prime to m .

remembering a and b are relatively prime if $\text{hcf}(a,b) = 1$

Examples

$\phi(1) = 1 \{1\}$

$\phi(2) = 1 \{1\}$

$\phi(3) = 2 \{1, 2\}$

$\phi(4) = 2 \{1, 3\}$

$\phi(5) = 4 \{1, 2, 3, 4\}$

$\phi(6) = 2 \{1, 5\}$

$\phi(7) = 6 \{1, 2, 3, 4, 5, 6\}$

$\phi(8) = 4 \{1, 3, 5, 7\}$

$\phi(9) = 6 \{1, 2, 4, 5, 7, 8\}$

$\phi(10) = 4 \{1, 3, 7, 9\}$

Note here the ϕ function is one less when the number is prime. This property will be developed later.

Property 1

if $\text{hcf}(a,b) = 1$ then

$$\phi(a \times b) = \phi(a) + \phi(b)$$

Example

$$\phi(2 \times 3) = \phi(2) + \phi(3) \quad \text{TRUE}$$

Property 2 (Euler's Product Formula)

let $m = p_1^a p_2^b p_3^c \dots$ (ie prime factors)

then

$$\phi(m) = m(1 - 1/p_1)(1 - 1/p_2)(1 - 1/p_3) \dots$$

The proof of this depends upon the fundamental theorem of arithmetic but is not given in full here.

Example

$$\phi(2 \times 3) = 6(1 - 1/2)(1 - 1/3) = 2$$

$$\begin{aligned} \phi(6 \times 7) &= 42(1 - 1/2)(1 - 1/3)(1 - 1/7) \\ &= 12 \end{aligned}$$

where p is prime

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

This follows directly from Property 2 setting $k = 1$ we have

$$\phi(p) = p - 1$$

which was apparent in the initial list of quotient functions.

Example

$$\phi(3^2) = 3^2 - 3^1 = 6 \quad \text{TRUE}$$

$$\text{also } \phi(3^2) = \phi(3) + \phi(3)$$

because $\text{hcf}(3,3) = 1$

Divisor Sum

The divisors of 24 are

1, 2, 3, 4, 6, 8, 12, 24 and

$$\begin{aligned} &\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(8) \\ &+ \phi(12) + \phi(24) = 24 \end{aligned}$$

This theorem was discovered by Gauss.

Euler's Theorem

if $\text{hcf}(a,m) = 1$

(I omit the hcf from hereon)

$$\text{then } a^{\phi(m)} \equiv 1 \pmod{m}$$

Example

as $\text{hcf}(5,4) = 1$

$$\text{then } 5^{\phi(4)} \equiv 1 \pmod{4}$$

$$\text{that is } 5^2 \equiv 1 \pmod{4} \quad \text{TRUE}$$

Fermat's Theorem

if we set $m = p$ where p is prime

$$\text{then } a^{\phi(p)} \equiv 1 \pmod{p}$$

Now we have already established

$$\phi(p) = p - 1$$

a special case of

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

so $a^{p-1} \equiv 1 \pmod{p}$ where p is prime

Euler's Theorem can be used to find the converse of Fermat's Theorem, which introduces the additional

condition for $t < n - 1$

"If there is an integer a with

$$\text{hcf}(a,n) \equiv 1 \pmod{n}$$

and furthermore there is no integer t for which $at \equiv 1 \pmod{n}$ then n is prime.”

Example 1

$$\text{hcf}(5,4) = 1$$

$$5^{\phi(4)} \equiv 1 \pmod{4}$$

$$5^2 - 1 \equiv 0 \pmod{4}$$

$$24 \equiv 0 \pmod{4} \text{ which is TRUE}$$

Example 2

$$\text{hcf}(9,5) = 1$$

$$5^{\phi(5)} \equiv 1 \pmod{5}$$

$$9^4 - 1 \equiv 0 \pmod{5}$$

$$6560 \equiv 0 \pmod{5} \text{ which is TRUE}$$

Worked Examples

1) Show $20 \equiv -7 \pmod{9}$

$$20 - -7 \equiv 0 \pmod{9}$$

2) Show $8 \equiv 23 \pmod{5}$

$$8 - 23 \equiv 0 \pmod{5}$$

3) Show $3^3 \equiv 1 \pmod{13}$

$$27 - 1 \equiv 0 \pmod{13}$$

4) let $12 \equiv 2 \pmod{5}$

$$16 \equiv 1 \pmod{5}$$

so $28 \equiv 2 + 1 \pmod{5}$

or $28 \equiv 1 + 2 \pmod{5}$

and $4 \equiv 1 - 2 \pmod{5}$

or $-4 \equiv 2 - 1 \pmod{5}$

Finally $16 \times 12 \equiv (2 \times 1) \pmod{5}$

$$192 \equiv 2 \pmod{5}$$

$$190 \equiv 0 \pmod{5} \text{ TRUE}$$

5) $27 \equiv 6 \pmod{7}$

$$(3 \times 9) \equiv (3 \times 2) \pmod{7}$$

now $\text{hcf}(3,7) = 1$

so we can divide by 3

$$9 \equiv 2 \pmod{7}$$

$$7 \equiv 0 \pmod{7} \text{ TRUE by corollary 2}$$

6) For natural numbers $2,3,4,5,6, \dots, 21$

if we define $ab \equiv 1 \pmod{23}$ then

$$2 \times 12 \equiv 1 \pmod{23}$$

$$3 \times 8 \equiv 1 \pmod{23}$$

$$4 \times 6 \equiv 1 \pmod{23}$$

$$5 \times 14 \equiv 1 \pmod{23}$$

$$7 \times 10 \equiv 1 \pmod{23}$$

$$9 \times 18 \equiv 1 \pmod{23}$$

$$11 \times 21 \equiv 1 \pmod{23}$$

$$13 \times 16 \equiv 1 \pmod{23}$$

$$15 \times 20 \equiv 1 \pmod{23}$$

$$17 \times 19 \equiv 1 \pmod{23}$$

but I am not clear why this holds !

$$7) \text{ solve } 23x \equiv 17 \pmod{7}$$

we know $21x \equiv 0 \pmod{7}$ for any x

therefore we reduce $23x \equiv 17 \pmod{7}$

$$\text{to } 2x + 21x \equiv (10 + 7) \pmod{7}$$

By converse theorem 1

$$2x \equiv 10 \pmod{7}$$

$$2x = 10 \text{ by corollary 2}$$

$$x = 5$$

$$8) 917x \equiv 33 \pmod{13}$$

$$(910x + 7x) \equiv (20 + 13) \pmod{13}$$

now $910x \equiv 0 \pmod{13}$ for any x

$$7x \equiv 20 \pmod{13}$$

$$\text{Hence } 7x \equiv 7 \pmod{13}$$

$$\text{so } 7x = 7$$

and $x + 1$ which is in fact TRUE

$$9) \text{ Solve } 3x \equiv 1 \pmod{7}$$

$$\text{now hcf}(3,7) = 1$$

so we have one solution

now $1 \equiv -6 \pmod{7}$ so by Theorem 4

$$3x \equiv -6 \pmod{7}$$

and again because $\text{hcf}(3,7) = 1$

we can divide through by 3

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

$$\text{so } x = -2 + 7k$$

$$x = 5 \text{ the principle solution}$$

$$10) \text{ solve } 18x \equiv -76 \pmod{29}$$

$$\text{hcf}(18,29) = 1$$

so we have one solution

By Theorem 5 as $\text{hcf}(2,29) = 1$

we can divide by 2 hence

$$9x \equiv -38 \pmod{29}$$

$$9x \equiv -38 \pmod{29}$$

$$9x \equiv -9 \pmod{29}$$

As $\text{hcf}(9,29) = 1$ we can divide by 9

$$x \equiv -1 \pmod{29}$$

$$x \equiv 28 \pmod{29}$$

By corollary 2 $x = 28$

$$\text{check } 18 \times 28 + 76 \equiv 0 \pmod{29}$$

Available in this series are

- On My TI Calculator what's the difference between Sx and σx ?
It's not what I thought for the first 40 years of the scientific calculator
- Beyond Pascal – Multinomials and Dice Throwing
How a class exercise in dice throwing led to the discovery of multinomials
- Conditional Probability and Bayes Theorem
An investigation into the pitfalls of medical screening
- Hypercomplex Numbers
Instead of making $i^2 = -1$ as in complex numbers what if we just make $i^2 = 1$
- Propositional Calculus
Sherlock Holmes was the great inductive detective but not infallible
- The Harmonic Triangle
How investigating harmonic triangles led to the discovery of a universal series summation formula
- Congruencies
A concise frills-free summary of the major theorems with comprehensible proofs.
- Pentatope Numbers
A short paper demonstrating a serendipitous discovery.

Back page