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

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

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

$17 - 2 = 3 \times 5$

Corollary 1

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

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

Proof $a - b = km$

so $a - b \pm m = (k \pm 1)\, m$

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

Corollary 2

For $a = b$

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

for every arbitrary natural number m

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

Corollary 3

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

$ak \equiv bk \pmod{mk}$

for $k \in \mathbf{Q}$

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

Example

let $k = {}^2/_3$

$17 \times {}^2/_3 \equiv 2 \times {}^2/_3 \pmod{5 \times {}^2/_3}$ because

$17 \times {}^2/_3 - 2 \times {}^2/_3 = 3 \times 5 \times {}^2/_3$ TRUE

Corollary 4

$kax \equiv a \pmod{a}$

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

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

Alternative Definition

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.

eg $17 \div 5$ has remainder 2 and

$2 \div 5$ also has remainder of 2.

Proof

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

then $a = mq_1 + r_1$

and $b = mq_2 + r_2$

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 and $r_2 < m$ then $r_1 - r_2 = 0$ 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

$23 \equiv 3 \pmod{10}$

$27 \equiv 7 \pmod{10}$

so $50 = 3 + 7 \pmod{10}$

and $50 = 7 + 3 \pmod{10}$

Theorem 2

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

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

then $ac = bd \pmod{m}$

Proof

let $a = b + sm$

and $c = d + tm$

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

$= bd + smd + tmb + stmn$

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

and following the same argument from Theorem 1 we have

$ac = bd \pmod{m}$

Example 2

$23 \equiv 3 \pmod{10}$

$27 \equiv 7 \pmod{10}$

so $621 = 21 \pmod{10}$ 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

$23 \equiv 3 \pmod{10}$

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

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

Example 3b

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

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

Example 3c

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

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

Theorem 4 (transivity)

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

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

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

Proof

if $a = b + sm$

and $b = c + tm$

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

hence $a = c \pmod{m}$

following the same argument as Theorem 1

Example 4

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

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

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

This technique can be used to solve linear congruencies.

Theorem 5

if hcf $(r,m) = 1$

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

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

Proof

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

then ${}^{r(a-b)}/_{m}$ is an integer

but if hcf $(r,m) = 1$

then ${}^{(a-b)}/_{m}$ is also an integer

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

Example 5a

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

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

now as hcf $(3,7) = 1$

we can divide through by 3 to get

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

Example 5b

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

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

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

even though hcf $(6,4) = 2$

but just because

$30 \equiv 2 \pmod{4}$

it doesn't follow that

$15 \equiv 1 \pmod{4}$

because 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 hcf $(b,m) = 1$

then it does follow that

$a \equiv 0 \pmod{m}$

Example 6a

$32 \equiv 0 \pmod{16}$

	$4\times8 \equiv 0 \pmod{16}$	TRUE
but	$4 \equiv 0 \pmod{16}$	NOT TRUE
and	$8 \equiv 0 \pmod{16}$	NOT TRUE

Example 6b

However

	$105 \equiv 0 \pmod{5}$	TRUE
so	$35\times3 \equiv 0 \pmod{5}$	TRUE
and	$35 \equiv 0 \pmod{5}$	

because 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

hcf $(a,m) = bk$

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

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

   has no solutions if

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

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

   has hcf (a,m) distinct solutions if

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

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

   and hcf $(a,m) = 1$

   then there is one distinct solution

1) and 3) are corollaries of 2)

Examples

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

   has no solutions because

   $2x - 1$ is odd

   and $2k$ is even

   so effectively we have

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

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

so by inspection solutions are

$x = 2$ (14, 26, 38, etc.)

$x = 5$ (17, 29, 41, etc.)

$x = 8$ (20, 32, 44, etc.)

$x = 11$ (23, 35, 47, etc.)

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

The solution set is

$x = 2 + 3k$ $(k = 0,1,2\ldots)$

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

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…)

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 cryptosytem, 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

${}^{1\times2\times3\ldots(p-1)+1}/_p$ 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)

${}^{1\times2\times3\times4\times5\times6+1}/_7 = 103$ an integer.

Euler's Totient Function

φ is pronounced "phi"

If m is a natural number then $\varphi(m)$ 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 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 hcf (a,b) = 1 then

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

Example

$\phi(2\times3) = \phi(2) \times \phi(3)$ TRUE

Property 2 (Euler's Product Formula)

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

then

$\varphi(m) = m(1 - 1/p_1)(1 - 1/p_2)(1 - 1/p_3)\ldots$

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

Example

$\phi(2\times3) = 6(1 - {}^1/_2)(1 - {}^1/_3) = 2$

$\phi(6\times7) = 42(1 - {}^1/_2)(1 - {}^1/_3)(1 - {}^1/_7) = 12$

where p is prime

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

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

$\varphi(p) = p - 1$

which was apparent in the initial list of quotient functions.

Example

$\varphi(3^2) = 3^2 - 3^1 = 6$ TRUE

also $\varphi(3^2) = \varphi(3) + \varphi(3)$

because hcf (3,3) = 1

Divisor Sum

The divisors of 24 are

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

$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(8) + \varphi(12) + \varphi(24) = 24$

This theorem was discovered by Gauss.

Euler's Theorem

if hcf (a,m) = 1

(I omit the hcf from hereon)

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

Example

as hcf (5,4) = 1

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

that is $5^2 \equiv 1 \pmod 4$ TRUE

Fermat's Theorem

if we set m = p where p is prime

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

Now we have already established

$\varphi(p) = p - 1$

a special case of

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

hcf (a,n) $\equiv$ 1 (mod n)

and furthermore there is no integer t for which at $\equiv$ 1 (mod n) then n is prime."

Example 1

hcf (5,4) = 1

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

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

24 $\equiv$ 0 (mod 4) which is TRUE

Example 2

hcf (9,5) = 1

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

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

6560 $\equiv$ 0 (mod 5) which is TRUE

Worked Examples

1) Show 20 $\equiv$ – 7 (mod 9)

   20 – –7 $\equiv$ 0 (mod 9)

2) Show 8 $\equiv$ 23 (mod 5)

   8 – 23 $\equiv$ 0 (mod 5)

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

   27 – 1 $\equiv$ 0 (mod 13)

4) let 12 $\equiv$ 2 (mod 5)

   16 $\equiv$ 1 (mod 5)

so 28 $\equiv$ 2 + 1 (mod 5)

or 28 $\equiv$ 1 + 2 (mod 5)

and 4 $\equiv$ 1–2 (mod 5)

or – 4 $\equiv$ 2 – 1 (mod 5)

Finally 16 × 12 $\equiv$(2 × 1) (mod 5)

   192 $\equiv$ 2 (mod 5)

   190 $\equiv$ 0 (mod 5) TRUE

5) 27$\equiv$ 6 (mod 7)

   (3 × 9) $\equiv$(3 × 2) (mod 7)

   now hcf (3,7) = 1

   so we can divide by 3

   9 $\equiv$ 2 (mod 7)

   7 $\equiv$ 0 (mod 7) TRUE by corollary 2

6) For natural numbers 2,3,4,5,6, …21

   if we define ab $\equiv$ 1 (mod 23) then

   2 × 12 $\equiv$ 1 (mod 23)

   3 × 8 $\equiv$ 1 (mod 23)

   4 × 6 $\equiv$ 1 (mod 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) solve $23x \equiv 17 \pmod{7}$

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

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

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

By converse theorem 1

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

$2x = 10$ by corollary 2

$x = 5$

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

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

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

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

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

so $7x = 7$

and $x + 1$ which is in fact TRUE

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

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 hcf $(3,7) = 1$

we can divide through by 3

$x = -2 \pmod{7}$

so $x = -2 + 7k$

$x = 5$ the principle solution

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

hcf $(18,29) = 1$

so we have one solution

By Theorem 5 as 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 hcf $(9,29) = 1$ we can divide by 9

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

$x \equiv 28 \pmod{29}$

By corollary 2 $x = 28$

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 <u>inductive</u> 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