A Number Theory Environment (partial)

(from William Curtis's *How to Improve Your Math Grades,* on occampress.com)[1]

[1] This line has been added to the first page of the chapter because Google does not reveal this information when it makes the chapter accessible following a user's search.

I chose number theory (or, more correctly, *classical* number theory) to illustrate some features of Environments because, on the one hand, the student who has never studied the subject can nevertheless quickly understand what the subject is about — it is about the integers, ... -3, -2, -1, 0, 1, 2, 3, ... — and can quickly understand the congruence relation between integers (two integers are congruent mod an integer *m* if they both have the same remainder when divided by *m*). On the other hand, the proofs are often difficult (an understatement, as many generations of amateurs have learned!). Furthermore some of the problems for which solution methods are known, admirably illustrate the value of actually writing down the heuristic, e.g., such problems as solving a congruence (see under "congruence, how to solve a").

The sources of the information in these pages are: Apostol, Tom M., *Introduction to Analytic Number Theory*, Springer-Verlag, N.Y., 1972, and Niven, Ivan, and Zuckerman, Herbert B., *An Introduction to the Theory of Numbers*, John Wiley and Sons, N.Y., 1980. A theorem or definition *x.y* from the first is referenced and labelled as "A *x.y*"; from the second as "NZ *x.y*".

Among the Environment features which are illustrated are:

- Alphabetical ordering of topics for quick reference, rather than the logical ordering found in most textbooks and classroom lectures;

- Division of the Environment into three sections, the first containing alphabetical terms, the second containing symbols which are not in the English alphabet, and the third containing proofs;

- An example of the Universal Template for Mathematical Entities (see "congruence").

- Explicit writing out of a heuristic for solving congruences (see "congruence, how to solve a"). Given such a heuristic, and, of course, a proof of its correctness, I hope it is clear why I have so little use for "working the problems" at the end of the chapter.

- Layout of each page aimed at "understanding at a glance";

- Indication, via underlining, of words and phrases that can be looked up in the Environment. (In an online Environment, these would, of course, be hypertext links.) *Note*: the sample pages include only a few explanations of all topics marked by this symbol. The look-up-able symbols that are used in equations are not underlined, as this makes the equations to hard to read.

- Example of structured proof (see under “Proofs”, “Theorem (NZ 2.25b), proof”). This proof is much longer than the one in the referenced text, but I think you will find it is also much more rapidly understood. Short proof, long time spent in decoding, has been exchanged for Long proof, shorter time spent in decoding.

congruence

Definition and purpose of congruence
See congruence, definition of.

Ways of representing congruence
See congruence, definition of.

Common operations on, or involving, congruence
Addition
See congruence, arithmetic rules for.
Subtraction
See congruence, arithmetic rules for.
Multiplication
See congruence, arithmetic rules for.
Division
See congruence, arithmetic rules for.
Finding the number of solutions to a congruence
See congruence, number of solutions.
Solving a congruence
See congruence, how to solve a.

Congruence from an algebraic point of view
Additive groups (mod *m*)
See additive groups mod *m*.

Multiplicative groups (mod *m*)

See multiplicative groups mod *m*.

Elements of order r

See order r elements.

Elements of order $\phi(m)$, i.e., primitive roots

See primitive root.

Theorems concerning congruences

Theorems concerning congruences (mod p^1)

See congruences (mod p^1).

Theorems concerning congruences (mod p^k)

See congruences (mod p^k).

Theorems concerning congruences (mod *m*), $m = p_1^{e1}p_2^{e2}...p_j^{ej}$

See congruences (mod $p_1^{e1}p_2^{e2}...p_j^{ej}$)

Types of congruence

See congruence, types of.

congruence, arithmetic rules for

Basic Idea

Congruence, ≡, is like equality, =, except that you can't always cancel common factors. (See Theorem NZ 2.3, (1), (2) under Division Rules in this section.)

Note! Some of the following rules will be more rapidly understood — in fact, will be self-evident, if you think of congruence in terms of the wheel-and-spokes model given under congruence, definition of.

Congruence, like equality, is an equivalence relation, since it is reflexive, symmetric, and transitive (see Theorem NZ 2.1, modified under **Algebraic Properties of ≡** in this section). For a given modulus *m*, all numbers congruent to a given *u* (i.e., all numbers on a spoke) constitute an equivalence class.

Arithmetic Rules for Congruence

Algebraic Properties of ≡

Theorem NZ 2.1, modified

If a, b, c, d, x, y, denote integers
Then (0) $a \equiv a \pmod{m}$ (Reflexivity)
(1) $a \equiv b \pmod{m}$
$b \equiv a \pmod{m}$
$a - b \equiv 0 \pmod{m}$
are equivalent statements (Symmetricality)
(2) **If** $a \equiv b \pmod{m}$
and $b \equiv c \pmod{m}$
Then $a \equiv c \pmod{m}$ (Transitivity)

Addition and Multiplication Rules

(3) **If** $a \equiv b \pmod{m}$
and $c \equiv d \pmod{m}$
Then $ax + cy \equiv bx + dy \pmod{m}$

(4) **If** $a \equiv b \pmod{m}$
and $c \equiv d \pmod{m}$
Then $ac \equiv bd \pmod{m}$

Division Rules

Theorem NZ 2.3

(1) $ax \equiv ay \pmod{m}$ **iff** $x \equiv y$ (mod $m/((a, m)$)

(2) **If** $ax \equiv ay \pmod{m}$
and $(a, m) \equiv 1 \pmod{m}$
Then $x \equiv y \pmod{m}$

congruence, definition of

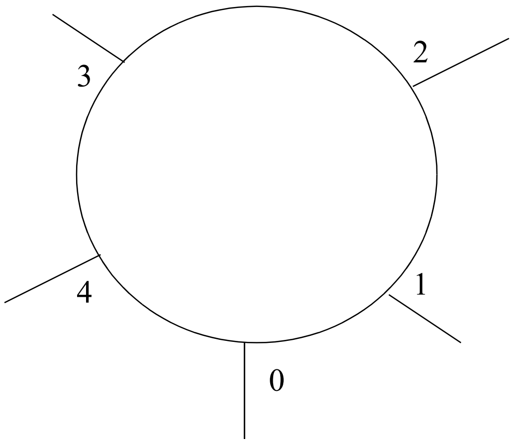
Definition

If *m*, *a*, *b* are integers
and *m* is a divisor of (*a* - *b*),
or *a*, *b*, have the same remainder when divided by *m*, then we can say that:

a is congruent to *b* modulo *m*, and we write:
$a \equiv b \pmod{m}$

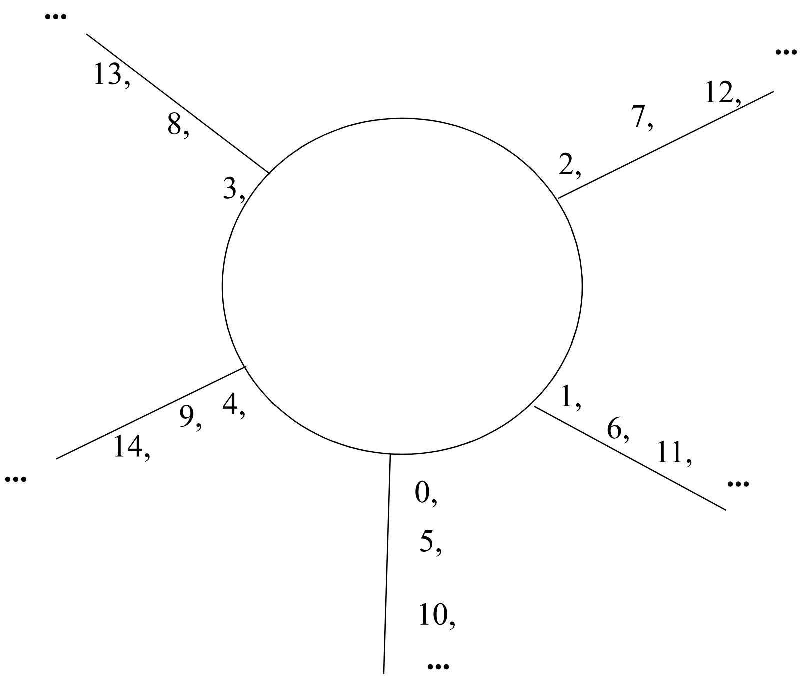
Basic Idea

The “wheel-and-spokes” model below is a way of understanding congruence. We draw a circle, or “wheel”, with *m* “spokes”, as shown. Here, *m* = 5. One spoke, the 0 spoke, is always positioned vertically, as shown.



We then begin writing the non-negative integers in succession, counterclockwise, starting with 0 at the 0 spoke (see drawing below in this section). We can, of course, also write the negative integers in the same way by extending the spokes to the inside of the wheel.

Integers 0, 1, 2, ..., *m* - 1, constitute the possible remainders when any integer is divided by *m*. They are also called “minimum residues”. It is easy to see that:



$a \equiv b \pmod{m}$
can be expressed as:
a and *b* lie on the same spoke of the *m*-wheel.

Related

Complete system of residues
Reduced system of residues
Factorial theorems

congruence, how to solve a

If the congruence(s) are all linear, i.e., are all of the form,
$ax \equiv b \pmod{m}$
Then If there is only one congruence, see
linear congruence, how to solve a;
If there is more than one congruence, see

set of linear congruences, how to solve a.

If the congruence is not linear, i.e., is a polynomial of the form,
$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_\mathrm{n} \equiv 0 \pmod{m}$, $n \geq 2$,
and
$m = p$, a prime, see
non-linear congruence mod *p*, how to solve a;

$m = p^k$, $k > 1$, *p* a prime, see
non-linear congruence mod p^k, how to solve a;

$m = p_1^{k1}p_2^{k2}...p_r^{kr}$, p_i a prime, see
non-linear congruence mod $p_1^{k1}p_2^{k2}...p_r^{kr}$, how to solve a.

congruence, types of

Polynomial congruences

$f(x) \equiv 0 \pmod{m}$, where:
$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_\mathrm{n}$
(See polynomial congruences.)

Polynomial congruences containing nth power residues:

$x^n \equiv a \pmod{m}$,
where: *a* is called an *n*th power residue if the congruence has a solution.
(See nth power residues.)

Exponential congruences

$a^r \equiv 1 \pmod{m}$
If *r* is the smallest such *r*, *r* is called the order of *a* mod *m.*
See: exponential congruences,
order r elments.

Exponential congruences in which order of a = ϕ(m)

See: primitive root.

Congruences (mod *p*), *p* a prime

(See congruences (mod *p*).)

Congruences (mod p^k), p a prime, $k > 1$

(See congruences (mod p^k).)

Congruences (mod m), m a product of different primes.

(See congruences (mod m).)

factorial

Definition:

n factorial = $n!$ = $n(n - 1)(n - 2)$ ... 1, where n is a positive integer.

factorial theorems

Theorem:

For all $m \geq n$, $n!$ divides ($m^{(n)} = m(m - 1)(m - 2) \ldots (m - (n - 1))$ (i.e., n terms)).

Proof:

The wheel-and-spokes model of congruence described under congruence, definition of makes possible an intuitive proof.

1. Construct a wheel-and-spokes model for the modulus n.

2. Then, clearly, *any* successive n spokes must include the 0 spoke, i.e., *any* product of n successive spokes is a multiple of n. In particular, this holds for the spoke containing m. Now repeat the same argument for $(m - 1)$, $(m - 2)$, ..., $(m - (n - 1))$, relative to the moduli $(n - 1)$, $(n - 2)$, ... 1, respectively.

linear congruence, how to solve a

To solve a linear congruence, i.e., a congruence of the form,

(0) $ax \equiv b \pmod{m}$

1. Determine if congruence has any solutions and, if so, how many:

To do this:

1.1 Compute (a, m).

1.2 **If** (a, m) does not divide b, **Then** there are no solutions. You're done.

If (a, m) divides b, **Then** there are (a, m) solutions. These are:

(1) $x_0 + t(m/(a, m)), t = 0, 1, 2, ..., (a, m) - 1$, where:

x_0 is any solution of $(a/(a, m))x \equiv b \pmod{m/(a, m)}$

2. Solve for $x = x_0$ in (1).
To do this:

2.1 Write the congruence in (1) as:
(2) $a'x \equiv b \bmod m'$

2.2 Factor m' into its constituent primes:
$m' = p_1^{k1} p_2^{k2} ... p_r^{kr}$

2.3 Solve the following system of linear congruences:
$a'x \equiv b \pmod{p_1^{k1}}$
$a'x \equiv b \pmod{p_2^{k2}}$
.
.
.
$a'x \equiv b \pmod{p_r^{kr}}$
To do this, see set of linear congruences with relatively prime moduli, how to solve a.

2.4 The x found as the solution of (3) is the x_0 in (1). Find the remaining solutions in (1) as indicated there.

3. Check your answers by substituting each into (0). You're done.

primitive root

Definition

A primitive root, a, is an element of the integers mod m such that $\phi(m)$ is the smallest exponent such that:

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

In group theoretical terms, a primitive root, a, is an element of the integers mod m such that the order of a mod m is $\phi(m)$.

Other elements of the integers mod m may have orders less than $\phi(m)$. For example, the order of 6 mod 7 is 2 because $6^2 \equiv 1 \pmod{7}$ and 2 is the smallest such exponent, but the order of 5 mod 7 is 6 because $5^{6 = \phi(7)} \equiv 1 \pmod{7}$ and 6 is the smallest such exponent. 5 is thus a primitive root mod 7.

Symbols

is-congruent-to

$\equiv$ is the symbol for is-congruent-to. See congruence, definition of.

Euler's function

$\phi(m)$ is the symbol for Euler's function.

Definition

$\phi(m)$ = the number of positive integers $\leq m$, and relatively prime to m, i.e., the number of positive n such that:

$1 \leq n \leq m$;

$(n, m) = 1$.

Examples

$\phi(1) = 1$ because only $(1, 1) = 1$;

$\phi(2) = 1$ because only $(2, 1) = 1$;

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

Related

Reduced system of residues

Complete system of residues

Fermat-Euler Theorem

Proofs

Theorem (NZ 2.25b), proof

Theorem (NZ 2.25b): m has a primitive root **iff** $m = 2, 4, p^{n,} 2p^n$, p an odd prime

Proof:
1. Only if part:
We prove the contrapositive, i.e.,
If $m \neq 2, 4, p^n, 2p^n$
Then m has no primitive root.
(See Theorem (NZ 2.25b), step 1, proof.)
End of proof of only if part.

2. If part:
2.1 **If** $m = 2$ Then m has a primitive root.
(See Theorem (NZ 2.25b), step 2.1, proof.)
2.2 **If** $m = 4$ Then m has a primitive root.
(See Theorem (NZ 2.25b), step 2.2, proof.)
2.3 **If** $m = p^n$ Then m has a primitive root.
(See Theorem (NZ 2.25b), step 2.3, proof.)
2.4 **If** $m = 2p^n$ Then m has a primitive root.
(See Theorem (NZ 2.25b), step 2.4, proof.)
End of proof of if part.

End of proof of Theorem (NZ 2.25b)**.**

Theorem (NZ 2.25b), step 1, proof:
1. If $m \neq 2$, Then (a) $m = 2^f, f \geq 3$, **or**
(b) $m = 2^f p_1^{e1} p_2^{e2} ... p_k^{ek}, p_i$ a prime, $f \geq 0$, $k \geq 2$, **or**
(c) $m = 2^f p^n, f \geq 2$.

2. Case (a):
If $\mathrm{m} = 2^f, f \geq 3$
Then m has no primitive root.
(See Theorem (NZ 2.25b), step 1.2, proof.)

3. Case (b):
If $m = 2^f p_1^{e1} p_2^{e2} ... p_k^{ek}, p_i$ a prime, $f \geq 0$, $k \geq 2$
Then m has no primitive root.
(See Theorem (NZ 2.25b), step 1.3, proof.)

4. Case (c):
If $m = 2fp^n$, $f \geq 2$.
Then m has no primitive root.
(See Theorem (NZ 2.25b), step 1.4, proof.)

Theorem (NZ 2.25b), step 1.3, proof:

Step 1.3 asserts:
If $m = 2^f p_1^{e1} p_2^{e2} \ldots p_k^{ek}$, p_i a prime, $f \geq 0$, $k \geq 2$
Then m has no primitive root.

Proof:

General idea: show that the hypothesis implies that, for any relevant a there is a smaller power of a than $\phi(m)$ that is congruent to 1. Hence a cannot be a primitive root mod m.

1.3.1. By the Fermat-Euler Theorem, we know that, for any a such that $(a, m) = 1$:

$$a^{\phi(p_1^{e1})} \equiv 1 \pmod{p_1^{e1}}, \text{ and}$$

$$a^{\phi(m/(p_1^{e1}))} \equiv 1 \pmod{m/(p_1^{e1})}$$

1.3.2. Now since p_1^{e1} and $m/(p_1^{e1})$ are both > 2, by Theorem (A. 2.5e) we know that:

$\phi(p_1^{e1})$ and $\phi(m/(p_1^{e1})$ are both even, hence

$(\phi(p_1^{e1})/2)$ and $(\phi(m/(p_1^{e1})/2)$ are both integers.

1.3.3. Therefore, raising both sides of (1) to the power($\phi(m/(p_1^{e1})/2)$, and raising both sides of (2) to the power $((\phi(p_1^{e1})/2)$, we get:

(3) $$a^{(\phi p_1^{e1})\phi(m/p_1^{e1}))\ /2} \equiv 1\ (\text{mod}\, p_1^{e1});$$

(4) $$a^{(\phi(m/(p_1^{e1}))\phi(p_1^{e1}))\ /2} \equiv 1\ (\text{mod}\, m/p_1^{e1});$$

Clearly, the left-hand sides of (3) and (4) are the same (by the commutative property of multiplication).

1.3.4. Now Theorem (NZ 2.3(3)) implies, informally, that the congruence in (3) and (4) will remain valid if we multiply the moduli, i.e., the Theorem implies that:

If m_1 and m_2 are relatively prime
and $x \equiv y$ (mod m_1)
and $x \equiv y$ (mod m_2)
Then $x \equiv y$ (mod $m_1 m_2$)

This fact, along with a basis rule for multiplying congruences (Theorem (NZ 2.1(4)) under congruence arithmetic rules, enables us to assert from (3) and (4) that:

(5) $$a^{(\phi(m/(p_1^{e1}))\phi(p_1^{e1}))\ /2} \equiv 1\ (\text{mod}\ (\phi(m/(p_1^{e1}))\phi(p_1^{e1})).$$

1.3.5. But by Theorem (A2.5c),

(6) $\phi(m/(p_1^{e1})\phi(p_1^{e1}) = \phi(m/(p_1^{e1})p_1^{e1})$,

and the right-hand side of (6) is clearly equal to $\phi(m)$, so we can write (5) as

(7) $$a^{\phi(m)\ /2} \equiv 1\ (\text{mod}\ m).$$

Hence there is a smaller power of *a* than $\phi(m)$ that is congruent to 1. Hence *a* cannot be a primitive root.

End of proof.

Number Theory Environment (partial)