A Concrete Introduction to Number Theory and Algebra – Chapter 3-4

Libin Wang

School of Computer Science, South China Normal University

September 22, 2020

Table of contents

Definition of congruence（同余）.

Definition

We say that *a is congruent to b modulo m*, and we write

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

if m divides $a - b$. The number m is called the *modulus*（模数）of the congrence.

Definition of congruence（同余）.

Definition

We say that *a is congruent to b modulo m*, and we write

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

if m divides $a - b$. The number m is called the *modulus*（模数）of the congrence.

Some notations.

- $a \equiv b \pmod{m}$ iff $\exists k \in \mathbb{Z}$, $a = km + b$.
- $(a \bmod m) = (b \bmod m)$

Congruence–例.

Example

$$26 \equiv 8 \pmod 9 \qquad \textit{and} \qquad 6 \equiv 55 \pmod 7,$$

since

$$9|(26-8) \qquad \textit{and} \qquad 7|(6-55),$$

or, equivalenty:

$$8 = 26 - 2 * 9 \qquad \textit{and} \qquad 55 = 6 + 7 * 7.$$

Properties of Congruence.

Lemma

If $a_1 \equiv b_1 \pmod{m}$ *and* $a_2 \equiv b_2 \pmod{m}$, *then*

$$a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod{m}$$

and

$$a_1 a_2 \equiv b_1 b_2 \pmod{m}$$

Modular Arithmetic(模算术).

Examples

Since $10000 \equiv 1 \pmod 3$ and $998 \equiv 2 \pmod 3$, then

$$10000 * 998 \equiv 2 \pmod 3$$

.

Properties of Congruence.

Negative number.

Let x and n be two positive integers and $x < n$, what does $-x \bmod n$ mean?

Properties of Congruence.

Negative number.

Let x and n be two positive integers and $x < n$, what does $-x \bmod n$ mean?

Intuition.

Consider that the negative of x is the number x' such that $x + x' = 0$, that is:

$$x + x' \equiv 0 \bmod n.$$

Since $x < n$, hence $x' = n - x$.

Two's Complement（二进制补码）

Two's Complement

A signed number represented in n bits. The range of the numbers is $[-2^{n-1}, 2^{n-1}-1]$, and the rule is described as follows:

- Positive integers, in the range 0 to $2^{n-1}-1$, are stored in regular binary form. The sign bit is set to 0.
- Negative integers $-x$, with $1 \leq x \leq 2^{n-1}$, are calculated by first constructing x in binary, then inverting all the bits of x and finally adding 1. The sign bit is set to 1.

Two's Complement

Another way to remember two's complement.

The negative of x equals $2^n - x$. Since $2^n - x = \underbrace{111\cdots11}_{n} + 1 - x$, and $\underbrace{111\cdots11}_{n} - x$ is the same as inverting all the bits of x.

Cancellation Law.

Theorem

Cancellation Law. If gcd$(c, m) = 1$ *and*

$$ac \equiv bc \pmod{m},$$

then

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

Where gcd shorts for the greatest common divisor.

Cancellation Law.

Proof.

By definition of congruence, we have $m|(ac - bc)$, equivalently, $m|(a-b)c$. Since $gcd(c, m) = 1$, it follows that $m \mid (a - b)$, so as claimed.

$\square$

Cancellation Law.

Another perspective.

If $gcd(c, m) = 1$ then $\exists r, s \in \mathbb{Z}$ s.t.

$$rc + sm = 1$$

$\bmod m$ to both sides of the equation:

$$rc \equiv 1 \bmod m$$

means r is the multiplicative inverse(乘法逆元) of $c \bmod m$, let it be c^{-1}.

Partially solve the congruence $ax \equiv b \pmod{m}$.

Example

To solve $3x \equiv 2 \pmod{11}$.
Firstly, by using egcd algorithm, to compute that $3^{-1} = 4$, *because* $3 * 4 \equiv 1 \pmod{11}$. *Multiply* 4 *to the equation and obtain*

$$x \equiv 8 \pmod{11}.$$

Properties of Congruence.

Lemma

For $n \in \mathbb{N}$, congruence modulo n forms an equivalence relation(等价关系) of $\mathbb{Z}$.

Proof.

It is easy to check that:
1. Reflexive(自反性). $a \equiv a \pmod{n}$
2. Symmetric(对称性). If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
3. Transitive(传递性). If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$ □

Equivalence relation and equivalence classes.

Definition

When a set $\mathbb{S}$ has an equivalence relation on it, then the equivalence relation partitions the set $\mathbb{S}$ into disjoint subsets, called equivalence classes（等价类）, defined by the property that two elements are in the same equivalence class if they are equivalent.

Congruence classes modulo *m*.

The set of congruence classes modulo m is denoted by $\mathbb{Z}/m\mathbb{Z}$. There are exactly m congruence classes in $\mathbb{Z}/m\mathbb{Z}$. That is :

$$\mathbb{Z}/m\mathbb{Z} = \{[0]_m, [1]_m, \cdots, [m-1]_m\}.$$

Example

When $m = 2$, $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$. The congruence class $[1]_2$ is the set of all integers congruent to 1 modulo 2. Thus $[1]_2$ is the set of all odd integers. Similarly, the congruence class $[0]_2$ is the set of all even integers.

Proposition of Congruence.

Proposition

If $[a_1]_m = [a_2]_m$ *and* $[b_1]_m = [b_2]_m$, *then*

$$[a_1 \pm b_1]_m = [a_2 \pm b_2]_m, \qquad \textit{and} \qquad [a_1 b_1]_m = [a_2 b_2]_m.$$

Proof.

It is easy. Transform the form $[a]_m = [b]_m$ to $a \equiv b \pmod{m}$ and use Proposition 2.2. □

Notations of Congruence classes modulo m.

- Any element b of a congruence class $[a]_m$ is called a *representative* of that class.
- The set of all the least nonnegative representative of $\mathbb{Z}/m\mathbb{Z}$ is the set of integers $\{0, 1, 2, \cdots, m-1\}$, that is called the *least residue system* modulo m.
- Any set of m integers, no two of which are congruent modulo m, is called a *complete residue system* modulo m.

Example

Let $m = 7$*, the least residue system modulo* m *is the set* $\{0, 1, 2, 3, 4, 5, 6\}$*, and a complete residue system modulo* m *may be the set* $\{14, 8, 23, 46, 61, 13\}$*.*

Mod Exponentiation.

In this section, we focus on modular exponentiation which is an important arithmetic primitive. Its task is that given integers x, y and m to compute

$$x^y \bmod m.$$

Mod Exponentiation.

Example

To compute $2^{16} \bmod 11$. *We compute:*

$$2^2 \bmod 11 = 4$$

$$2^4 \bmod 11 = 4 * 4 \bmod 11 = 5$$

$$2^8 \bmod 11 = 5 * 5 \bmod 11 = 3$$

$$2^{16} \bmod 11 = 3 * 3 \bmod 11 = 9$$

Mod Exponentiation.

The process can be expressed as a recursive form, by that, we sharply improve the efficiency from performing $O(y)$ multiplications to $O(log(y))$.

$$x^y = \begin{cases} (x^{\lfloor y/2 \rfloor})^2 & \text{if } y \text{ is even;} \\ x \cdot (x^{\lfloor y/2 \rfloor})^2 & \text{if } y \text{ is odd.} \end{cases} \tag{1}$$

Mod Exponentiation(Recusive Version).

Listing 1: Recursive Modular Exponentiation

```
# Recursive Function to calculate
# (x^y)%p in O(log y)
def rec_mod_exp(x, y, p):
    if (y == 0): return 1
    z = rec_mod_exp(x, y/2, p)
    if ((y & 1) == 0): #y is an even number
        return z*z % p
    else: #y is an odd number
        return x*z*z %p
```

Mod Exponentiation: from recursive to iterative.

We describe how to transform the recursive algorithm to an iterative algorithm as follows. Firstly, we treat integer y as a polynomial (or a bianry string):

$$y = y_{n-1}2^{n-1} + y_{n-1}2^{n-1} \cdots + y_1 2 + y_0,$$

where $y_i \in \{0, 1\}$.

Mod Exponentiation: from recursive to iterative.

We describe how to transform the recursive algorithm to an iterative algorithm as follows. Firstly, we treat integer y as a polynomial (or a bianry string):

$$y = y_{n-1}2^{n-1} + y_{n-1}2^{n-1} \cdots + y_1 2 + y_0,$$

where $y_i \in \{0, 1\}$.
Secondly, transform x^y as:

$$x^y = \prod_{i=0}^{n-1} x^{y_i 2^i}$$

Mod Exponentiation: from recursive to iterative.

We describe how to transform the recursive algorithm to an iterative algorithm as follows. Firstly, we treat integer y as a polynomial (or a bianry string):

$$y = y_{n-1}2^{n-1} + y_{n-1}2^{n-1} \cdots + y_1 2 + y_0,$$

where $y_i \in \{0, 1\}$.
Secondly, transform x^y as:

$$x^y = \prod_{i=0}^{n-1} x^{y_i 2^i}$$

Finally, start with x and repeatedly square modulo m, multiply the terms with $y_i = 1$ and get the result.

Mod Exponentiation: Example.

Example

Let $x = 7$, $y = 10$, $m = 11$, *to compute* $x^y \bmod m$. *The bianry string of y is* 1010, *thus we compute:*

$$\begin{aligned} y_0 &= 0, & x^{2^0} &\equiv 7 \bmod m \\ y_1 &= 1, & x^{2^1} &\equiv 5 \bmod m \\ y_2 &= 0, & x^{2^2} &\equiv 3 \bmod m \\ y_3 &= 1, & x^{2^3} &\equiv 9 \bmod m \end{aligned}$$

Then , multiply the terms with $y_i = 1$, *we have*
$x^y = (5 * 9) \bmod 11 = 1$

Mod Exponentiation (Iterative version).

Because the white board is too narrow to show the code, so it is your home work.

Some topics using modular arithmetic.

Our following job is to play with number using modular arithmetic, and find some patterns or rules.

Find the patterns.

Let $p = 7$, and for very $1 \leq a < p$, compute a^i mod p, where $1 \leq i < p$. We have:

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

Find the patterns.

Let $p = 7$, and for very $1 \leq a < p$, compute $a^i \bmod p$, where $1 \leq i < p$. We have:

a	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1
2	4	1	2	4	1
3	2	6	4	5	1
4	2	1	4	2	1
5	4	6	2	3	1
6	1	6	1	6	1

May you find some patterns?

More data to find the patterns.

Let $p = 11$, and for very $1 \leq a < p$, compute a^i mod p, where $1 \leq i < p$. We have:

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

Conjecture.

$$a^{p-1} \equiv 1 \pmod{p}$$

Another computation.

$\forall 1 < a < p$, compute $a * i \bmod p$, for $1 \leq i < p$. For example, let $a = 2$, $p = 7$, we have:

$a * i$	1	2	3	4	5	6
$a = 1$	1	2	3	4	5	6
$a = 2$	2	4	6	1	3	5

Another computation.

Continue the computation...

$a * i$	1	2	3	4	5	6
$a = 1$	1	2	3	4	5	6
$a = 2$	2	4	6	1	3	5
$a = 3$	3	6	2	5	1	4

Another computation.

Continue the computation...

$a * i$	1	2	3	4	5	6
$a = 1$	1	2	3	4	5	6
$a = 2$	2	4	6	1	3	5
$a = 3$	3	6	2	5	1	4

Have a decision?

Another computation.

Finally!

$a * i$	1	2	3	4	5	6
$a = 1$	1	2	3	4	5	6
$a = 2$	2	4	6	1	3	5
$a = 3$	3	6	2	5	1	4
$a = 4$	4	1	5	2	6	3
$a = 5$	5	3	1	6	4	2
$a = 6$	6	5	4	3	2	1

Conjecture.

The trick is, p is a prime number! We conjecture: if p is a prime, $\forall a$ which is not divided by p, $a * i \mod p$, for $1 \leq i < p$, is a permutation of numbers from 1 to $p - 1$.

Conjecture.

The trick is, p is a prime number! We conjecture: if p is a prime, $\forall a$ which is not divided by p, $a * i \bmod p$, for $1 \leq i < p$, is a permutation of numbers from 1 to $p-1$.That is, the numbers

$$a, 2a, 3a, \cdots, (p-1)a \pmod{p}$$

are the same as the numbers:

$$1, 2, 3, \cdots, p-1$$

although they may be in a different order.

Conjecture.

The trick is, p is a prime number! We conjecture: if p is a prime, $\forall a$ which is not divided by p, $a * i \bmod p$, for $1 \leq i < p$, is a permutation of numbers from 1 to $p-1$.That is, the numbers

$$a, 2a, 3a, \cdots, (p-1)a \pmod p$$

are the same as the numbers:

$$1, 2, 3, \cdots, p-1$$

although they may be in a different order.

$$\mathbb{S} = \{a * i \bmod p, 1 \leq i < p\}$$

is also called a complete system of residues modulo p.

Proof by contradition.

Of course, we need a proof!

Proof by contradition.

Of course, we need a proof!

Proof.

Proof by contradiction (informal and incomplete). If we are wrong, then there exist i and j such that,

$$a * i \equiv a * j \pmod{p}$$

where $i \neq j$. However, then we can cancel the a from the equation! (Cancellation Low.) $\square$

Do a simple job!

Multiply all $1 \leq i < p$, and all $a * i \bmod p$, we have:

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (a * i \pmod{p})$$

Do a simple job!

Multiply all $1 \leq i < p$, and all $a * i \bmod p$, we have:

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (a * i \pmod{p})$$

Convince yourself:

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} a * i \equiv a^{p-1} \prod_{i=1}^{p-1} i \pmod{p}$$

Do a simple job!

Multiply all $1 \leq i < p$, and all $a * i \bmod p$, we have:

$$\prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (a * i \pmod{p})$$

Convince yourself:

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} a * i \equiv a^{p-1} \prod_{i=1}^{p-1} i \pmod{p}$$

Cancel the big number, we have:

$$a^{p-1} \equiv 1 \pmod{p}$$

Fermat's little theorem.

Theorem

(Fermat's little theorem.) Let p be a prime number, and let a be any number with $a \not\equiv 0$ mod p. Then

$$a^{p-1} \equiv 1 \pmod{p}.$$

An Exercise using Fermat's little theorem.

Exercise.

Let $p = 17$ be a prime number, and let $a = 3$, what is $a^{2018} \pmod{p}$?

An Exercise using Fermat's little theorem.

Exercise.

Let $p = 17$ be a prime number, and let $a = 3$, what is $a^{2018} \pmod{p}$?

$$3^{2018} \equiv 3^{65*16+2} \equiv 3^2 \equiv 9 \pmod{17}.$$

More computation.

If the modulus is a composite number, then our trick will fail! For example, let $n = 6$,

$a * i$	1	2	3	4	5
$a = 1$	1	2	3	4	5
$a = 2$	2	4	0	2	4
$a = 3$	3	0	3	0	3
$a = 4$	4	2	0	4	2
$a = 5$	5	4	3	2	1

One more computation.

Let $n = 9$,

$a * i$	1	2	3	4	5	6	7	8
$a = 1$	1	2	3	4	5	6	7	8
$a = 2$	2	4	6	8	1	3	5	7
$a = 3$	3	6	0	3	6	0	3	6
$a = 4$	4	8	3	7	2	6	1	5
$a = 5$	5	1	6	2	7	3	8	4
$a = 6$	6	3	0	6	3	0	6	3
$a = 7$	7	5	3	1	8	6	4	2
$a = 8$	8	7	6	5	4	3	2	1

Conjecture.

Conjecture.

If n is a composite number, the numbers

$$a, 2a, 3a, \cdots, (n-1)a \pmod{n}$$

may **NOT** the same as the numbers:

$$1, 2, 3, \cdots, n-1$$

except that...

Conjecture.

Conjecture.

If n is a composite number, the numbers

$$a, 2a, 3a, \cdots, (n-1)a \pmod{n}$$

may **NOT** the same as the numbers:

$$1, 2, 3, \cdots, n-1$$

except that...a is relatively prime to n, namely, $gcd(a, n) = 1$.

Check the observation.

Let $n = 9$,

$a * i$	1	2	4	5	7	8
$a = 1$	1	2	4	5	7	8
$a = 2$	2	4	8	1	5	7
$a = 4$	4	8	7	2	1	5
$a = 5$	5	1	2	7	8	4
$a = 7$	7	5	1	8	4	2
$a = 8$	8	7	5	4	2	1

Conjecture.

We conjecture: Let n be a composite number, denotes

$$S = \{b : 1 \leq b < n \text{ and } gcd(b, n) = 1\}$$

Then $\forall a$ with $gcd(a, n) = 1$, denotes

$$S' = a * S \pmod{n}$$

we have:

$$S = S'$$

Notation.

Euler's phi function.

Define:

$$\phi(n) = |\{b : 1 \leq b < n \text{ and } gcd(b, n) = 1\}|$$

The function ϕ is called *Euler's phi function*.

Notation.

Then:

$$S = \{b_1, b_2, \cdots, b_{\phi(n)} : \ 1 \leq b_i < n \text{ and } gcd(b_i, n) = 1\}$$

$$S' = \{a{*}b_1, a{*}b_2, \cdots, a{*}b_{\phi(n)} \pmod{n} : \ b_i \in S \text{ and } gcd(a, n) = 1\}$$

Proof.

To prove

$$S = S'$$

Check that if there exist:

$$a * b_i \equiv a * b_j \pmod{n}$$

where $b_i \neq b_j$. Then by Cancellation Law,

$$b_i \equiv b_j \pmod{n}.$$

Contradiction!

Do a similar simple job!

Multiply all the numbers in S and S' , we have:

$$\prod_{i=1}^{\phi(n)} b_i = \prod_{i=1}^{\phi(n)} (a * b_i \pmod{n})$$

$$\prod_{i=1}^{\phi(n)} b_i \equiv \prod_{i=1}^{\phi(n)} a * b_i \pmod{n}$$

$$\prod_{i=1}^{\phi(n)} b_i \equiv a^{\phi(n)} \prod_{i=1}^{\phi(n)} b_i \pmod{n}$$

Cancel the big number, we have:

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

Euler's Theorem.

(Euler's Theorem.)

Let n be a positive composite number, a be a positive integer with $gcd(a, n) = 1$, then:

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

More about Euler's Phi Function..

Definition

Euler's Phi Function. Define:

$$\phi(n) = |\{b : 1 \leq b < n \text{ and } gcd(b, n) = 1\}|$$

The function ϕ is called Euler's phi function.

Observations

$\phi(p) = p - 1$, where p is a prime.
$\phi(p^k) = p^k - p^{k-1}$, where p is a prime.

More about Euler's Phi Function..

Question.

How to compute $\phi(m)$ where $m = p^i q^j$ with p and q are prime.

More about Euler's Phi Function..

Question.

How to compute $\phi(m)$ where $m = p^i q^j$ with p and q are prime.

A related question.

How to compute $\phi(mn)$ where $gcd(m, n) = 1$.

More about Euler's Phi Function.

Compute $\phi(mn)$

Display the positive integers not exceeding mn in the following way.

$$
\begin{array}{ccccc}
1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\
3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
r & m+r & 2m+r & \cdots & (n-1)m+r \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
m & 2m & 3m & \cdots & mn
\end{array}
$$

More about Euler's Phi Function.

Basic idea.

Find all the elements which are relatively prime to both n and m, then it is relatively prime to mn. Formally:

$$\forall a, gcd(a, n) == 1 \text{ and } gcd(a, m) == 1 \implies gcd(a, mn) == 1.$$

More about Euler's Phi Function.

Counting

- How many rows satisfy $gcd(r, m) = 1$? Ans : $\phi(m)$. Note that, if $gcd(r, m) = 1$ then $gcd(km + r, m) = 1$, for $k \in [0..n-1]$.
- At rth row, how many integers have $gcd(km + r, n) = 1$, for $k \in [0..n-1]$? Ans: $\phi(n)$. Note that, we have $gcd(n, m) = 1$.
- Hence, there are $\phi(m)$ rows, each containing $\phi(n)$ integers relatively prime to mn.

More about Euler's Phi Function.

Remark

(Why the conclusion holds?) If $gcd(a, m) == 1$ *and* $gcd(a, n) == 1$ *then* $gcd(a, mn) == 1$.

More about Euler's Phi Function.

Remark

(Why the second item holds?) The elements in rth row are: $r, m+r, \cdots, (n-1)m+r$ *with* $gcd(m,n)=1$. $\forall k_i \neq k_j$, $k_i m + r \not\equiv k_j m + r \pmod{n}$. *Otherswise,* $k_i = k_j$ *by our Golden Law(Cancellation Law), contradiction! It means the* n *elements in rth row form "a complete system of residues modulo* n*", that is* $\{r, m+r, \cdots, (n-1)m+r\} \pmod{n} = \{0, 1, 2, \cdots, n-1\}$. *Hence, exactly* $\phi(n)$ *of these integers are relatively prime to* n.

More about Euler's Phi Function.

Theorem

Let m and n be relatively prime positive integers. Then $\phi(mn) = \phi(m)\phi(n)$.

More about Euler's Phi Function.

Some easy generizations.

How to relate $\phi(mn) = \phi(m)\phi(n)$ where $gcd(m, n) = 1$ with $\phi(m)$ where $m = p^i q^j$?

More about Euler's Phi Function.

Some easy generizations.

How to relate $\phi(mn) = \phi(m)\phi(n)$ where $gcd(m, n) = 1$ with $\phi(m)$ where $m = p^i q^j$?
Ans: $gcd(p^i, q^j) = 1$ when p and q are relatively prime. Hence $\phi(p^i q^j) = \phi(p^i)\phi(q^j)$.

More about Euler's Phi Function.

Some easy generizations.

How to relate $\phi(mn) = \phi(m)\phi(n)$ where $gcd(m, n) = 1$ with $\phi(m)$ where $m = p^i q^j$?
Ans: $gcd(p^i, q^j) = 1$ when p and q are relatively prime. Hence $\phi(p^i q^j) = \phi(p^i)\phi(q^j)$.
How to generize the result to $\phi(m)$ where $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$?

More about Euler's Phi Function.

Some easy generizations.

How to relate $\phi(mn) = \phi(m)\phi(n)$ where $gcd(m, n) = 1$ with $\phi(m)$ where $m = p^i q^j$?
Ans: $gcd(p^i, q^j) = 1$ when p and q are relatively prime. Hence $\phi(p^i q^j) = \phi(p^i)\phi(q^j)$.
How to generize the result to $\phi(m)$ where $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$?
Ans: Induction! Left as an exercise.

Exercise.

Prove the following theorem.

Theorem

(Euler's Phi Function.)
Let $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$*, then*
$\phi(m) = m(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k).$

What is a Concrete Introdution?

- Play with numbers.
- Find the patterns, find the fun.
- Programming is a good way to play.

What have been covered?

- Congruence.
- Fermat's little theorem.
- Euler's theorem.

What have been omitted?

- Fast multiplication.
- Powers: how to do fast power.

What is the next step?

- From a new perspective to view Fermat's and Euler's theorems.
- From arithmetic go to algebra.

Homework.

- Prove if $gcd(c, m) = 1$, then exists a unique c^{-1} such that $cc^{-1} \equiv 1 \pmod{m}$.
- Write a Python program that solves the congruence

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

  Given a, b, m as input, return all solutions or an alert tells why the congruence has no solution.
- Prove Wilson's Theorem which says that p is prime iff $(p-1)! \equiv -1 \pmod{p}$.
- Prove Theorem of Euler's Phi Function.
- Write a Python program to compute Eurler's phi function. That is, given an integer n, return $\phi(n)$.