XM452 Lecture Notes 4

Erdaifu Luo

26 March 2023

§18 Reduced Residue System; Euler's ϕ function

§18.1 Reduced Residual System

$ax \equiv 1 \pmod{n}$ has a solution if, and only if $(a, n) = 1$.

Definition 18.1 (Reduced Residual System)**.** Let $S = \{a_1, \dots, a_n\}$, be a complete residue system mod n. Let $S' \subset S$ be the subset of those integers a_j such that

$$(a_j, 1) = 0.$$

S' is called a **reduced residue system mod n**.

Example 18.2 (a) $S = \{0, 1, 2, 3\}$ is a complete residue system mod 4, while $S' = \{1, 3\}$ is the reduced residue system.

(b) $S = \{11, 12, 13, 14\}$ is a complete residue system mod 4, while $S' = \{11, 13\}$ is the reduced residue system.

In these cases, the reduced systems have the same number of elements. Moreover,

$$1 \equiv 13 \pmod{4} \text{ and } 3 \equiv 11 \pmod{4}$$

so the numbers in the reduced residue system match up mod 4.

Theorem 18.3

Let s' be a reduced residue system mod n. If $(a, n) = 1$, then a is congruent mod n to a unique number of S'.

If S'' is another reduced residue system, then S' and S'' have the same number of elements and the mod n congruence classes of the members of S' are the same as those of S''. In other words, the elements match up mod n.

Proof. Let S be a complete residue system mod n and let $S' \subset S$ be the reduced system (S' consists of those members in S that are relatively prime to n).

Suppose $(a, n) = 1$. Since S is a complete residue system, there is a unique integer $b \in S$ with

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

But if $(a, n) = 1$, and

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

then $(b, n) = 1$, and thus $b \in S'$.

Now let S'' be another reduced residue system. Every element of S'' is congruent mod n to a unique element of S'. Conversely, every element of S' is congruent to an unqiue element of S''. □

§18.2 Euler's ϕ function

The number of elements in a reduced residual system for n does not depend on the reduced residual system. We call that number ϕn, coined by Euler.

Theorem 18.4 (Euler's Phi Function)

$\phi(n)$ is the number of positive integers less than or equal to n that are relatively prime to n.

Proof. This number is the number of elements in the reduced residue system S' contained in the complete residue system $\{0, 1, \ldots, n-1\}$. □

Here's an observation. If p is a prime, then

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

because every positive integer $a < p$ is relatively prime to p.

§19 Euler's Theorem; Fermat's Little Theorem; Pseudoprimes

§19.1 Theorems of Euler and Fermat

Let $\phi(n)$ be Euler's function.

Theorem 19.1 (Euler's Theorem)

If $(a, n) = 1$, then

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

Proof. Let S be a complete residue system mod n. Let

$$S'' = \{a_1, \ldots, a_{\phi(n)}\}$$

be the corresponding reduced residue system

$$S'' = \{aa_1, \ldots, aa_{\phi(n)}\}$$

is also a reduced residue system, since each $(a_j, n) = 1$, and $(a, n) = 1$, each $(aa_j, n = 1)$.

Each aa_j is congruent to exactly one element of S. So aa_j is congruent to exactly one element in S'.

Thus the numbers

$$aa_1, \ldots, aa_{\phi(n)}$$

are just a rearrangement (mod n) of the numbers

$$a_1, \ldots, a_{\phi(n)},$$

so

$$(aa_1)(aa_2)\dots(aa_{\phi(n)}) \equiv a_1\dots a_{\phi(n)} \pmod n.$$

Therefore,

$$a^{\phi(n)} \cdot (a_1 \dots a_{\phi(n)}) \equiv (a_1 \dots a_{\phi(n)}) \pmod n.$$

Since each a_j is relatively prime to n, we can divide to get

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

□

Theorem 19.2 (Fermat's Little Theorem)

Suppose p is a prime, then for all a,

$$a^p \equiv a \pmod p.$$

If $p \nmid a$, we can "divide" by a and get

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

Proof. If $p \mid a$, then

$$a^p \equiv a \pmod p$$

since both a^p and a are congruent to 0 mod p.

Suppose $p \nmid a$, since p is prime,

$$\phi p \equiv p - 1,$$

and hence the second congruence follows from the above theorem. The first congruence is simply a times the second, and so it holds. □

§19.2 Pseudoprimes

Fermat's theorem says that for every prime p, since

$$2^p \equiv 2 \pmod p,$$

then

$$p \mid (2^p - 2).$$

The ancient Chinese knew this and also believed if $n > 1$ is an integer and $n \mid (2^n - 2)$, then n is a prime. They were wring, because 341 was a counter point.

Definition 19.3 (Pseudoprimes)**.** One calls a composite integer n that has the property that

$$n \mid (2^n - 2),$$

a **pseudoprime**.

There are infinitely many pseudoprimes.

§20 A Formula for Euler's ϕ function

§20.1 Finding the Formula

Theorem 20.1

$\phi(n)$ is multiplicative.

Proof. Let $(m, n) = 1$. Show $\phi(mn) = \phi(m) \cdot \phi(n)$. First, make an array with m columns and n rows. The numbers in the j-th column are:

$$0m + j, 1m + j, 2m + j, \dots, m(n-1) + j.$$

Every element in the j-th column is relatively prime to m or none are:

The top entry of the j-th column is $0m+j = j$. If $(j, m) \neq 1$, the j-th column contains 0 elements that are relatively prime to m. If $(j, m) = 1$, it contains n elements that are relatively prime to m.

Since there are $\phi(m)$ j's between 1 and m with $(i, m) = 1$, there are $\phi(m)$ columns that contain elements relatively prime tp m.

Since $(m, n) = 1$, the n numbers in the j-th column form a complete residue system mod n.

The number in the j-th column relatively prime to n form a reduced residue system mod n, so there are $\phi(n)$ of them.

There are $\phi(m)$ columns with entries relatively prime to m. Each of those columns has $\phi(n)$ entries relatively prime to n. Thus the entire array has

$$\phi(m) \cdot \phi(n)$$

entries relatively prime to both m and n.

Since the entries are all between 1 and mn, there are exactly

$$\phi(m) \cdot \phi(n)$$

numbers between 1 and mn relatively prime to both m and n.

Since $(m, n) = 1$, a is relatively prime to $m \cdot n$ if and only if a is relatively prime to m and n. So,

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

□

Theorem 20.2

Suppose the prime factorization of n is

$$n = p_1^{a_1} \dots p_k^{a_k}$$

where p_j's are distinct primes.

Then,

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

Proof. Since ϕ is multiplicative, so

$$n = \phi p_1^{a_1} \dots \phi p_k^{a_k}.$$

So we just need to find a formula for $\phi(p^a)$ where p is a prime.

Every number is relatively prime to p^a unless it is divisible by p. The integers between 1 and p^a that are divisible by p are

$$p, 2p, \dots, p^{a-1}p.$$

So, p^{a-1} negative integers $\leq p^a$ are divisible by p and hence are not relatively prime to p^a. So,

$$\phi(p^a) = \phi(p^a) - \phi(p^{a-1}).$$

In other words,

$$\phi(p^a) = \phi(p^a)\left(1 - \frac{1}{p}\right).$$

Thus,

$$\begin{aligned}\phi(n) &= \phi p_1^{a_1} \dots \phi p_k^{a_k}\\ &= p^{a_1} \cdot \left(1 - \frac{1}{p_1}\right) \dots p^{a_k}\left(1 - \frac{1}{p_k}\right)\\ &= p^{a_1}p^{a_2} \dots p^{a_k} \cdot \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)\\ &= n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

□

§21 Polynomial Congruence

Definition 21.1 (Polynomial Congruence)**.** Two polynomials $f(x)$ and $g(x)$ that have integral coefficients are said to be **polynomially congruent mod n** if the coefficients of each power of x (including the constant term, i. e. the coefficient of x^0) in $f(x)$ is congruent mod n to the coefficient of the corresponding powers fo x in $g(x)$.

Example 21.2

$$(x+1)^2 \equiv x^2 + 1 \text{ (poly mod 2)}$$

since

$$(x+1)^2 \equiv x^2 + 2x + 1 \equiv x^2 + 0x + 1 \text{ (poly mod 2)}$$

Fermat's theorem tells us

$$x^3 \equiv x \pmod 3.$$

However,

$$x^3 \not\equiv x \text{ (poly mod 3)}.$$

Note that in every situation does not occur when we're talking about equalities instead of congruences. Two polynomials $f(x)$ and $g(x)$ are the asme of $f(x) = g(x)$ for every integer value of x. That is, equality for every value of x is the same as equality between the polynomials.

Theorem 21.3

If $f(x) \equiv g(x)$ (poly mod 3), then for every integer x,

$$f(x) \equiv g(x) \pmod{n}.$$

The example of $f(x) = x^3$ and $g(x) = x$ shows that the converse of this theorem is not true.

Theorem 21.4

If

$$f_1(x) \equiv f_2(x) \text{ (poly mod n)}$$

and

$$g_1(x) \equiv g_2(x) \text{ (poly mod n)}$$

then

$$f_1(x) + g_1(x) \equiv f_2(x) + g_2(x) \text{ (poly mod n)}$$

and

$$f_1(x) \cdot g_1(x) \equiv f_2(x) \cdot g_2(x) \text{ (poly mod n)}$$

Proof. The coefficients of the sums and products of polynomials are determined as combinations of sums and products of the coefficients of original polynomials.

So changing the coefficients of the original polynomials mod n changes the coefficients of the sum or product mod n. □