Math 215 Spring 2023 Number Theory II

Euler Phi Function and Sums of Divisors

Sankar Sitaraman – nature-lover.net/math

Math Dept, Howard University

2-1-2023

Outline

Definition of Euler Phi Function

These are a recap of what was done in Chapter 11. See notes titled "Congruences."
Euler Phi Function $\phi(n)$ for $n = 1, 2, 3, ...$ gives the number of elements in $\{1, 2, 3, ..., n-1\}$ that are relatively prime to n.

Examples:
$\phi(1) = 1$ by convention.
$\phi(2) = 1$.
$\phi(p) = p - 1$ for all primes.
$\phi(4) = 3$.
$\phi(6) = 2$.

Euler Phi Function for Powers of Primes

Given $n = p^k, k \geq 2$ we can divide the numbers smaller than n into p^{k-1} blocks of length p.

In $1, 2, ..., p$ we have $p - 1$ integers prime to p^k.
In $p + 1, p + 2, ..., 2p - 1, 2p$ again we have $p - 1$ integers prime to p^k.

Continuing thus, we see that there are totally $p^{k-1}(p - 1)$ numbers smaller than p^k that are prime to it.
So $\phi(p^k) = p^{k-1}(p - 1)$.

Multiplicativity of Euler Phi Function

Using chinese remainder theorem , in chapter 11 we showed that

$$\phi(mn) = \phi(m)\phi(n) \text{ if } gcd(m,n) = 1.$$

See notes titled "Congruences."

Thus

$$\phi(n) = \prod \phi(p_i^{a_i}) = \prod p_i^{a_i - 1}(p_i - 1) = \prod p_i^{a_i} \prod \left(1 - \frac{1}{p_i}\right)$$

$$= n \prod \left(1 - \frac{1}{p_i}\right).$$

Multiplicativity of Sums of a multiplicative function

FACT: If $F(n)$ is multiplicative (for example, like $\phi(n)$), then so is $F(d_1) + F(d_2) + ... + f(d_r)$ where the d_i are all the divisors of n.

Proof: If m, n are relatively prime, then the set of divisors of mn is the cartesian product of the set of divisors of m with the set of divisors of n. If d denotes divisors of mn and d_i are the divisors of m and e_j are the divisors of n then
$gcd(d_i, e_j) = 1 \ \forall i, j$ and $\{d\} = \{d_i e_j\}$.
Let $F(m) = \sum_{i=1}^{r} F(d_i)$ and $F(n) = \sum_{j=1}^{s} F(e_j)$.
Then $F(mn)$ equals

$$\sum_{i=1,j=1}^{i=r,j=s} F(d_i e_j) = \sum_{i=1,j=1}^{i=r,j=s} F(d_i)F(e_j) = \left(\sum_{i=1}^{r} F(d_i)\right)\left(\sum_{j=1}^{s} F(e_j)\right).$$

A theorem on sum of ϕ of divisors -first proof conclusion

Let $F(m) = \sum_{i=1}^{r} \phi(d_i)$ where all divisors of m are d_i. Using the property we just showed, we get, if its prime factorization is $m = \prod p_j^{a_j}, j = 1, 2, ..., k,$

$$F(m) = \sum_{i=1}^{r} \phi(d_i) = \prod_{j=1}^{k} F(p_j^{a_j}) = \prod_{j=1}^{k} \sum_{t=0}^{a_j} \phi(p_j^t)$$

$$= \prod_{j=1}^{k} \left(\sum_{t=1}^{a_j} (p_j^{t-1}(p_j - 1)) + \phi(1) \right) = \prod_{j=1}^{k} \left(\sum_{t=1}^{a_j} (p_j^t - p_j^{t-1}) + 1 \right)$$

$$= \prod_{j=1}^{k} p_j^{a_j} = m.$$

A theorem on sum of ϕ of divisors - other elementary proofs

Proof 2 sketch:

$$\phi(m) = m \prod_{P|m} \left(1 - \frac{1}{p}\right) = \sum \mu(d) \frac{m}{d} \implies \sum_{d|m} \phi(d) = m.$$

Here the second equality uses the Mobius function *mu* to carry out an inclusion-exclusion argument. The third one uses what is called the Mobius inversion formula. This is part of a general theory of Dirichlet convolution of arithmetic functions.

Proof 3 sketch: Show that the set of numbers k such that $gcd(k, m) = d$ is given by $\phi(m/d)$. Then these sets cover the numbers 1 to m disjointly and so the sum of $\phi(m/d)$ must equal m.

Group theory proof of theorem on sum of *phi* of divisors

The same can be proved using the following group theory fact:

FACT: In a cyclic group G of order n, there is exactly one subgroup of order d_i for each divisor of n and the number of generators of each such subgroup os $\phi(d_i)$.

Basically, if g is a generator of G then $g_i = g^{n/d_i}$ generates the unique subgroup of order d_i and any g_i^k with $gcd(k, d_i) = 1$ will also generate the same subgroup.

On the other hand, each element of G generates a subgroup of G! Counting the elements of the group in two ways, we get $\sum \phi(d_i) = n$.

This theorem is used in reverse to show that the multiplicative group mod any prime is cyclic.

Group theory proof of existence of primitive root mod any prime p

As promised, we use the theorem in reverse to show that the multiplicative group mod any prime is cyclic.
In fact, we will prove that there are $\phi(p-1)$ generators of $\mathbb{F}_p^*$ for any prime p.

Key fact: $x^{p-1}-1$ has exactly $p-1$ roots.

This follows from Fermat's little theorem since $1, 2, 3, ..., p-1$ are all roots. Let the divisors of $p-1$ be $d_1, d_2, ..., d_k$.

Now we showed, in a cyclic group, that there is a unique cyclic subgroup H_{d_i} of order d_i and if g_i is a generator of H_d then any g_i^k with $gcd(k, d_i) = 1$ will also generate H_{d_i}. Thus there are $\phi(d_i)$ generators of the subgroup of order d_i and thus exactly $\phi(d_i)$ elements of order d_i.

contd: existence of primitive root mod any prime p

continued from above:

Here, we need to prove this differently.
First, we know that each element $g \in \mathbb{F}_p^*$ has order dividing d_i for some d_i dividing $p-1$ from Lagrange's theorem.

This means g will be a solution of $x^{d_i} - 1$ *in* $\mathbb{F}_p^*$. We know from the fundamental theorem of algebra, that there will be at most d_i such solutions.
All such solutions will form a subgroup H_{d_i} of order at most d_i.
Within each subgroup if there is an element g_i of order exactly d_i, then it generates that whole subgroup and any g_i^k with $gcd(k, d_i) = 1$ will also have order exactly d_i and also generate the subgroup. All the rest of the powers of g_i will have order smaller than d_i. So there will be at most $\phi(d_i)$ elements of order exactly d_i.

conclusion: existence of primitive root mod any prime p

Now we look at the result we proved in chapter 27, namely $\phi(d_1) + \phi(d_2) + ... + \phi(d_k) = p - 1$, in two different ways.

In one way, this is the total number of possible elements of order exactly d_i summed over all d_i.
On the other hand, each element has order equal to a divisor of $p - 1$, so the left hand side actually includes all elements of $\mathbb{F}_p^*$.
This cannot happen unless there are exactly $\phi(d_i)$ elements of order d_i for each d_i, and that includes $p - 1$ which is also counted as a divisor of itself!
So there will always be an element of order $p - 1$ generating $\mathbb{F}_p^*$, called the primitive root mod p.

Some remarks on primitive roots

Although primes have the nice property that they always have primitive roots generating the multiplicative groups mod p the location of those primitive roots can be quite random.

The best results we have, by Burgess, says that the least primitive root mod a prime p is smaller than $f(p)\sqrt[4]{p}$ where $f(p)$ is very small compared to p.

Assuming generalized Riemann Hypothesis, Wang showed that the least primitive root is much smaller than $\log(p)^2 m^6$ where m is the number of prime factors of $\phi(p-1)$. It is known that $m < 2\log(p-1)/\log\log(p-1)$ for large enough p.

Textbook's proof of existence of primitive roots

In the book the proof is done using the following steps:

1. For any divisor n of $p-1$, $x^n - 1$ has exactly n solutions in $\mathbb{F}_p^*$.
2. If $\psi(d)$ is number of elements of order exactly d then

$$\psi(d_1) + \psi(d_2) + ... + \psi(d_k) = n, \text{ where } d_i | n.$$

   This is done by counting solutions of $x^n - 1$ in two ways.
3. Show that $\psi(d) = \phi(d)$ for each d.

Artin's primitive roots conjecture

1. Artin(1930): Given $a \neq \pm 1$, a not a perfect square, it is primitive root mod infinitely many primes.
2. (Stronger form) It is primitive root mod about 37% of primes.
3. (Gupta-Murty , Heath-Brown) one of 2,3 or 5 is primitive root mod infinitely many primes

An application of primitive roots

Chapter 29, problem 4.

1. Given k divides $p-1$ show that there are exactly k *distinct* solutions for $x^k - 1$ in $\mathbb{F}_p^*$.
2. More generally, how many solutions does $x^k = a \pmod{p}$ have?
3. Given 3 is a primitive root mod the prime1987, how many solutions to $x^{111} \equiv 729 = 3^6 \pmod{1987}$?

Solution: An application of primitive roots

Solution to Chapter 29, problem 4.

1. Given k divides $p-1$ show that there are exactly k *distinct* solutions for $x^k - 1$ in $\mathbb{F}_p^*$: Already proved in chapter 28 that there are exactly k solutions. Also proved that there is a generator (primitive root). Let it be g. Then $(g^i)^k = g^{ik} \equiv 1 \implies i = (p-1)/k, 2(p-1)/k, ..., (k-1)(p-1)/k$ and all these powers are distinct (prove!).

Solution continued: An application of primitive roots

(continued)Solution to Chapter 29, problem 4.

(2) More generally, how many solutions does $x^k = a \pmod{p}$ have?

(3) Given 3 is a primitive root mod the prime1987, how many solutions to $x^{111} \equiv 729 = 3^6 \pmod{1987}$?

Suppose $x \equiv g^t, a \equiv g^r \pmod{p}$. Then, because g has order $p-1$ we get

$$x^k \equiv a \implies g^{tk} \equiv g^r \pmod{p} \implies tk \equiv r \pmod{p-1}$$

So number of solutions is $gcd(k, p-1)$. In (3) this is $gcd(111, 1986) = 3$. If $k|p-1$ then gcd is k and we get k solutions. If $gcd(k, p-1) = 1$ then we get exactly one solution which is 1. In this case g^k itself is a generator as we have seen!

Another application of primitive roots

ElGamal cryptosystem

This is based on difficulty of solving **Discrete Logarithm Problem**:

Given $a \in \mathbb{F}_p^*$ it is hard to calculate r where $a \equiv g^r \pmod{p}$ with g being a generator / primitive root mod p.

1. A sends B $a \equiv g^k \pmod{p}$. k is the *secret key* and a is the *public key.*
2. B picks a random r and sends A $e_1 = g^r$ and $e_2 = ma^r$ where m is the message.
3. A calculates $e_2 e_1^{-k}$ to get the message.