Euler's Phi Function

Robert Y. Lewis

CS 0220 2023

March 10, 2023

Overview

Exam details

- Friday, March 17, 1:00-1:50pm in Salomon DECI
- Covers material through lecture on Wednesday, March 8 (i.e. this week's recitation)
- Handwritten, no electronic devices
- We will provide a cheat sheet (in advance)

- Time constraints: will not be expecting you to produce long proofs on your own. Know concepts, definitions, vocabulary, proof techniques.

- Review packet, "practice midterm," *recitations*

Definition

Definition: Integers that have no prime factor in common are called *relatively prime*.

In other words, they have no common divisor greater than 1. Or $\gcd(a, b) = 1$. Also, called “co-prime”.

Example: 9 and 14 are relatively prime. Neither are prime. But, they have no prime factors in common. Here, “relative” refers to “relative to each other”, not “kinda”.

What’s *not* relatively prime to 17? 34, sure. But, in general? Precisely the multiples of 17. True of any prime p.

Multiplicative inverse

Lemma: Let n be a positive integer. If k is relatively prime to n, then there exists an integer k^{-1} such that:

$$k \cdot k^{-1} \equiv 1 \pmod{n}.$$

Proof: Since n and k are relatively prime, gcdcombo$(n, k) = (s, t, 1)$. t must be the multiplicative inverse of k (mod n):

$$s \cdot n + t \cdot k = 1 \text{ implies } t \cdot k \equiv 1 \pmod{n}.$$

Solving equations

Corollary: Suppose n is a positive integer and k is relatively prime to n. Then,

$$ak \equiv bk \pmod{n} \quad \text{implies} \quad a \equiv b \pmod{n}$$

Proof: Multiply both sides by k^{-1} and simplify.

Relatively prime permutations

Lemma: Suppose n is a positive integer and k is relatively prime to n. Let $k_1, k_2, \cdots, k_r$ be all the integers in the interval $[1, n)$ that are relatively prime to n. Then, the sequence of remainders on division by n of

$$k_1 \cdot k, k_2 \cdot k, \ldots, k_r \cdot k$$

is a permutation of the sequence $k_1, k_2, \cdots, k_r$.

Example: $n = 18, k = 5$.

j	1	2	3	4	5	6	$= r$
k_j	1	5	7	11	13	17	
$k_j \cdot k$	5	25	35	55	65	85	
$k_j \cdot k \bmod n$	5	7	17	1	11	13	

Relatively Prime Permutation Proof (for reference)

Proof: We will show that the remainders in the first sequence are all distinct and are equal to some member of the sequence of k_js. Since the two sequences have the same length, the first must be a permutation of the second. (Kind of a bijection argument.)

If $k \cdot k_j \equiv k \cdot k_{j'} \pmod{n}$, then $k_j \equiv k_{j'} \pmod{n}$ by the Cancelation rule. Thus, the remainders are all distinct.

Next, we show that each remainder in the first sequence equals one of the k_js. By assumption, k_i and k are relatively prime to n, and therefore so is $k_i k$ by the "you can't split a prime" property. So, $\gcd(k \cdot k_i, n) = 1$. But, by the derivation of Euclid's algorithm, $\gcd(k \cdot k_i, n) = \gcd(n, \text{rem}(k \cdot k_i, n))$. Thus, $\text{rem}(k \cdot k_i, n)$ has a GCD of 1 with n, so it's on the list of relatively prime integers to n. QED.

Fermat's little theorem (reminder)

Theorem: Suppose p is prime and k is not a multiple of p. Then:

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

Since $k^{p-1} \equiv 1 \pmod{p}$ and $k^{p-1} = k \cdot k^{p-2}$, that tells us that k^{p-2} is the multiplicative inverse for k.

Only for prime p!

Remainder reminder: Solving equation mod prime

$3x + 9 \equiv 2$	$\pmod{11}$	
$3x \equiv -7$	$\pmod{11}$	additive shift
$3x \equiv 4$	$\pmod{11}$	pre-mod
$3^{11-2} \cdot 3x \equiv 3^{11-2} \cdot 4$	$\pmod{11}$	multiply both sides
$x \equiv 3^{11-2} \cdot 4$	$\pmod{11}$	Fermat's little theorem
$x \equiv 4 \times 4 = 16$	$\pmod{11}$	Maybe some repeated squaring
$x \equiv 5$	$\pmod{11}$	modding

Double check: $3 \times 5 + 9 = 15 + 9 = 24 = 2 \pmod{11}$.

Key step: $3^{-1} = 4 \pmod{11}$.

Via Fermat's little theorem: $3^{11-2} \bmod 11 = 19683 \bmod 11 = 4$.

But what if we wanted to work mod not-a-prime?

Counting relatively prime numbers

$\phi(n)$: The number of integers in $[0, n)$ that are relatively prime to n.

Examples:

- $\phi(7) = |\{1, 2, 3, 4, 5, 6\}| = 6$.
- $\phi(18) = |\{1, 5, 7, 11, 13, 17\}| = 6$.
- $\phi(20) = |\{1, 3, 7, 9, 11, 13, 17, 19\}| = 8$.
- $\phi(p) = p - 1$ if p is prime. Everybody below p is relatively prime to prime p !

Called Euler's ϕ or totient function.

Euler's Theorem

Theorem: Suppose n is a positive integer and k is relatively prime to n. Then,

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

Proof: Let $k_1, k_2, \ldots, k_r$ denote all integers relatively prime to n where $k_i \in [0, n)$. So, $\phi(n) = r$.

$$\begin{aligned} & = \text{rem}(k_1 \cdot k, n) \cdot \text{rem}(k_2 \cdot k, n) \cdot \cdots \cdot \text{rem}(k_r \cdot k, n) && \text{rel. prime perm.} \\ k_1 \cdot k_2 \cdot \cdots \cdot k_r & = (k_1 \cdot k) \cdot (k_2 \cdot k) \cdot \cdots \cdot (k_r \cdot k) \pmod{n} && \text{pre-mod} \\ & = k_1 \cdot k_2 \cdot \cdots \cdot k_r \cdot k^r \pmod{n} && \text{regroup} \end{aligned}$$

Applying the Cancellation lemma, the claim is proven. QED.

If we could compute $\phi(n)$, we could use it to compute multiplicative inverses. Can we?

Phi of product of two distinct primes

Lemma: For distinct primes p and q, $\phi(pq) = (p-1)(q-1)$.

Proof: Since p and q are prime, any number that is not relatively prime to pq must be a multiple of p or a multiple of q. Among the pq numbers in $[0, pq)$, there are precisely q multiples of p and p multiples of q. Since p and q are relatively prime, the only number in $[0, pq)$ that is a multiple of both p and q is 0. Hence, there are $p + q - 1$ numbers in $[0, pq)$ that are not relatively prime to pq. So, $\phi(pq) = pq - (p + q - 1) = (p-1)(q-1)$ as claimed. QED.

Phi for arbitrary numbers

Theorem: If p is prime, then $\phi(p^k) = p^k - p^{k-1}$ for $k \geq 1$. If a and b are relatively prime, $\phi(ab) = \phi(a)\phi(b)$.

Example:

$$\begin{aligned}
&\phi(750) \\
&= \phi(2 \times 3 \times 5^3) \\
&= \phi(2) \times \phi(3) \times \phi(5^3) \\
&= (2-1) \times (3-1) \times (5^3 - 5^2) \\
&= 2 \times (125 - 25) \\
&= 200.
\end{aligned}$$

Double check that this rule correctly generalizes the rules we already discussed for $\phi(p)$ and $\phi(pq)$.

Note: Practical if factorization is known. Otherwise, not so much.