Relative primes
Lecture 5b: 2022-02-07

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Recall combinations

- Given two integers m and n, the sum of a multiple of m and a multiple of n (allowing negative multiples) is called a combination of m and n.

$$m \cdot x + n \cdot y, \text{ where } x, y \text{ are integers}$$

- The set of combinations is precisely the multiples of $\gcd(m, n)$.
- You can use the Euclidean algorithm to make $\gcd(m, n)$, and therefore any multiple.

Relative primes

- If $\gcd(m, n) = 1$, then you can make any number as a combination of m and n, so we give this a special name, and call them relatively prime.
- Why?

A: Prime numbers are always relatively prime
B: Only prime numbers are relatively prime
C: These numbers are relatives of the prime numbers
D: All of the above
E: None of the above

Equivalent criteria for relative primes

- $\gcd(m, n) = 1$
- The only positive integer dividing both m and n is 1.
- No prime number divides both m and n.
- The prime factorizations of m and n have no primes in common.
- $\operatorname{lcm}(m, n) = mn$
- Any number divisible by both m and n is a multiple of mn.
- The number 1 is a combination of m and n.
- Every whole number is a combination of m and n

Example

- $\gcd(m, n) = 1$
- The only positive integer dividing both m and n is 1.
- No prime number divides both m and n.
- The prime factorizations of m and n have no primes in common.
- $\operatorname{lcm}(m, n) = mn$
- Any number divisible by both m and n is a multiple of mn.
- The number 1 is a combination of m and n.
- Every whole number is a combination of m and n

Try it out

- Are the following pairs of numbers relative prime?
- 49, 77

A: Yes
B: No
E: None of the above

- 50, 77
- 51, 77
- 10231820, 4381292812834

Surprising result

- If 1 is a combination of m and n, then 1 is a combination of m^a and n^b, for any integers a, b.

The Euler ϕ-function

- Called Euler Phi function, or Euler's totient function.
- One of the central activity of mathematicians is counting (e.g. counting divisors).
- $\phi(n)$ counts the number of integers from 0 to $n - 1$ that are relatively prime to n.

Modified sieve of Eratosthenes

- Modified sieve where we cross out only primes found in the prime factorization.

Try it out

- $\phi(18)$

- $\phi(29)$

A: 6
B: 14
C: 28
D: 40
E: None of the above

Quicker strategy

- Each time we remove the multiples of a prime p, we are removing $\frac{1}{p}$ of the remaining numbers.
- So if a prime factorization is $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where each $a_i > 0$, then

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Try it out

- $\phi(1000)$

- $\phi(3993)$

A: 100
B: 400
C: 1210
D: 2420
E: None of the above