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.

  $m \cdot x + n \cdot y$, where x, y 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.

Ex. $m = 6$ $n = 22$

$22 = 6 \cdot 3 + 4$
$6 = 4 \cdot 1 + 2$
$4 = 2 \cdot 2$

$\gcd(6, 22) = 2$

$2 = 6 - 4$
$2 = 6 - (22 - 6 \cdot 3)$
$2 = 6 \cdot 4 - 22$

$10 = 2 \cdot 5 = 5(6 \cdot 4 - 22)$
$= 6 \cdot 10 - 22 \cdot 5$

↑ combo of 6 & 22

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

Ex. (2, 3)

(20, 27)

(7, 27)

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.
- $\text{lcm}(m, n) = mn$
- 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

product of gcd & lcm is product

largest divisor is 1, then only divisor is 1

1 is not prime

else would be a prime number

prop of lcm

using reverse Euclidean alg

scaling up

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.
- $\text{lcm}(m, n) = mn$
- 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

$\gcd(120, 143) = 1$

$120 = 2^3 \cdot 3 \cdot 5$

$143 = 11 \cdot 13$

$\text{lcm}(120, 143) = 17160$

Try it out

- Are the following pairs of numbers relative prime?

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

- 49, 77

$49 = 7^2$

$77 = 7 \cdot 11$

No

- 50, 77

$77 = 50 \cdot 1 + 27$

$50 = 27 \cdot 1 + 23$

$27 = 23 \cdot 1 + 4$

$23 = 4 \cdot 5 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 3 \cdot 1$

gcd = 1

Yes

- 51, 77

$51 = 3 \cdot 17$

$77 = 7 \cdot 11$

Yes, no primes in common

- 10231820, 4381292812834

No, both divisible by 2

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.

Not obvious running Euclidean alg on both gives!

Ex. $\gcd(2, 3) = 1$.

Then $\gcd(256, 729) = 1$
($256 = 2^8$, $729 = 3^6$)

proof. The prime factorization of m & n have no primes in common.

Getting more multiplicative copies of m & n does NOT introduce new primes

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.

Ex. $\phi(6)$ 0, 1, 2, 3, 4, 5

$6 = 2 \cdot 3$ $\phi(6) = 2$

Ex $\phi(8)$ 0, 1, 2, 3, 4, 5, 6, 7

$8 = 2^3$ $\phi(8) = 4$

Ex. $\phi(13)$ 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12

$13 = 13$ $\phi(13) = 12$

Modified sieve of Eratosthenes

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

$\phi(15)$ $\quad 15 = 3 \cdot 5$

~~0~~ 1 2 ~~3~~ 4 ~~5~~ ~~6~~ 7 8 ~~9~~ ~~10~~ 11 ~~12~~ 13 14

Remove $\frac{1}{3}$ of numbers

$15 \cdot \left(1 - \frac{1}{3}\right) = 15 - 5 = 10$

Remove $\frac{1}{5}$ of remaining numbers

$10 \cdot \left(1 - \frac{1}{5}\right) = 10 - 2 = 8$

$\phi(15) = 8$

Try it out

- $\phi(18)$ = 6

$18 = 2 \cdot 3^2$

~~0~~ 1 ~~2~~ ~~3~~ ~~4~~ 5
~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11
~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17

$18 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 6$

- $\phi(29)$ = 28

since 29 is prime

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

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

Ex. $\phi(15) = 15 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$

Ex. $\phi(120) = 120 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$2^3 \cdot 3 \cdot 5$

$= 60\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

$= 40\left(1 - \frac{1}{5}\right) = 32$

Try it out

- $\phi(1000)$

- $\phi(3993)$

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