Review session: combos and primes Lecture 5d: 2022-02-09

MAT A02 – Winter 2022 – UTSC

Prof. Yun William Yu

Prime factorization

- For any positive integer n, can factor by attempting to divide by primes. Only have to check up to $\sqrt{n}$.

Ex. 11240

$= 10 \cdot 1124$

$= 2 \cdot 5 \cdot 2 \cdot 562$

$= 2^2 \cdot 5 \cdot 2 \cdot 281$

$= 2^3 \cdot 5 \cdot 281$

$281 \div 7 = 40 \text{ r } 1$

$\times\ 2^2 = 4$

$\times\ 3^2 = 9$

$\times\ 5^2 = 25$

$\times\ 7^2 = 49$

$\times\ 11^2 = 121$

$\times\ 13^2 = 169$

$\cancel{17^2 = 289}$

$$\begin{array}{r} 25 \text{ r } 6 \\ 11 \overline{)281} \\ \underline{22} \\ 61 \\ \underline{55} \\ 6 \end{array}$$

$$\begin{array}{r} 21 \text{ r } 8 \\ 13 \overline{)281} \\ \underline{26} \\ 21 \\ \underline{13} \\ 8 \end{array}$$

$\Rightarrow$ 281 is prime

$2^3 \cdot 5 \cdot 281$

Try it out

- What is the prime factorization of 12240?

12240

$= 10 \cdot 1224$

$= 2 \cdot 5 \quad 2 \cdot 612 = 2^2 \cdot 5 \cdot 612$

$= 2^2 \cdot 5 \cdot 2 \cdot 306$

$= 2^3 \cdot 5 \cdot 3 \cdot 102$

$= 2^3 \cdot 3 \cdot 5 \cdot 3 \cdot 34$

$= 2^3 \cdot 3^2 \cdot 5 \cdot 2 \cdot 17$

$= 2^4 \cdot 3^2 \cdot 5 \cdot 17$

A: $2^4 \cdot 3^2 \cdot 5 \cdot 17$
B: $2^3 \cdot 3^2 \cdot 5^2 \cdot 7^2$
C: $2^3 \cdot 3^3 \cdot 5 \cdot 13$
D: $2^4 \cdot 7 \cdot 17^2$
E: None of the above

Greatest common divisor

- Use either Euclidean algorithm or prime factorization.

$\gcd(100, 12240)$

$12240 = 2^4 \cdot 3^2 \cdot 5 \cdot 17$

$100 = 10^2 = (2 \cdot 5)^2 = 2^2 \cdot 5^2$

$\gcd(100, 12240) = 2^2 \cdot 5 = 20$

$12240 = 100 \cdot 122 + 40$

$100 = 40 \cdot 2 + 20$

$40 = 20 \cdot 2$

$\gcd = 20$

A: 10
B: 20
C: 25
D: 50
E: None of the above

Advanced Combinations

- Given two integers, m and n, can solve for the combination $\gcd(m,n) = mx + ny$ by reversing the Euclidean algorithm.
- Can solve for any multiple $c \cdot \gcd(m,n) = mx + ny$ by multiplying the above solution by c.
- Can solve for all combinations $0 = mx + ny$ by dividing by all common factors of m and n and considering all multiples of $(x = n, y = -m)$
- Can add 0 to any other solution to get different combinations.

Try it out

$\gcd(100, 12240) = 20$

- Is there an integer combination of 100 and 12240 that is equal to 50? No
- What about 60? Yes, multiple of gcd.
- Can you find three different solutions?

A: Yes
B: No

$12240 = 100 \cdot 122 + 40$

$100 = 40 \cdot 2 + 20$

$40 = 20 \cdot 2$

$20 = 100 - 40 \cdot 2$

$20 = 100 - (12240 - 100 \cdot 122) \cdot 2$

$20 = 100 \cdot (1 + 122 \cdot 2) - 12240 \cdot 2$

$20 = 100 \cdot 245 - 12240 \cdot 2$

$60 = 100 \cdot 735 - 12240 \cdot 6$

1

More solutions

Consider $0 = 100x + 12240y$

Divide by gcd : $0 = 5x + 612y$

$\Rightarrow x = 612, \quad y = -5$

$\Rightarrow 0 = 100 \cdot 612 - 12240 \cdot 5$

$$
\begin{array}{rl}
 & 60 = 100 \cdot 735 - 12240 \cdot 6 \\
+) & \\
\hline
 & 60 = 100 \cdot 1347 - 12240 \cdot 11
\end{array}
$$

2

$60 = 100 \cdot 735 - 12240 \cdot 6 + 0$

$$
\begin{array}{rl}
 & 60 = 100 \cdot 735 - 12240 \cdot 6 \\
- & 0 = 100 \cdot 612 - 12240 \cdot 5 \\
\hline
 & 60 = 100 \cdot 123 - 12240 \cdot 1
\end{array}
$$

3

Counting divisors

- Take all the exponents in the prime factorization of n, add 1 to each of them, and then take the product.

Ex. $12240 = 2^4 \cdot 3^2 \cdot 5 \cdot 17$

Ans. $(4+1)(2+1)(1+1)(1+1)$

$= 5 \cdot 3 \cdot 2 \cdot 2 = 60$

Divisors are everything with smaller exps

Ex. $2^3 \cdot 3 \cdot 5$ or $2 \cdot 17$

or $2^4 \cdot 3 \cdot 5 \cdot 17$, etc.

Try it out

- How many divisors does 100 have?

$$100 = 10^2 = (2 \cdot 5)^2 = 2^2 \cdot 5^2$$

$$(2+1)(2+1) = 9$$

A: 6
B: 8
C: 9
D: 10
E: None of the above

Counting common divisors

- Just need to find the divisors of the greatest common divisor.
- How many numbers are divisors of both 100 and 12240?

$\gcd(100, 12240) = 20$

$20 = 2^2 \cdot 5$

$Ans = (2+1)(1+1) = 3 \cdot 2 = 6$

A: 6
B: 8
C: 9
D: 10
E: None of the above

Euler's ϕ function

counts relative primes

- Can use modified sieve of Eratosthenes to remove all numbers that are not relative primes.
- Alternately, each time we remove multiples of a prime p, we remove $\frac{1}{p}$ 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. $\phi(120) = 120\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$

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

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

$= 40\left(1-\frac{1}{5}\right) = 40 - 8 = 32$

$\cancel{0}\ 1\ \cancel{2}\ \cancel{3}\ \cancel{4}\ 5\ \cdots\cdots\ 119$

Try it out

- $\phi(1000)$ $= 1000 \cdot \left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)$

$1000 = 10^3 = 2^3 \cdot 5^3$

$= 500\left(1-\frac{1}{5}\right) = 400$

- $\phi(3993)$ $= 3993\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)$

$3993 = 3 \cdot 1331$

$= 3 \cdot 11 \cdot 121$

$= 3 \cdot 11^3$

$= 2662 \cdot \left(1-\frac{1}{11}\right)$

$= 2662 - 242$

$= 2420$

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