Prime Numbers

Recall

Computing arithmetic operations mod m.

Let m be an integer larger than 1. Let x and y be any integers. Then,

$$[(x \bmod m) + (y \bmod m)] \bmod m = [x + y] \bmod m$$

$$[(x \bmod m)(y \bmod m)] \bmod m = [xy] \bmod m$$

Computing exponents:

$46^{10} \bmod 7$

$= (46 \bmod 7)^{10} \bmod 7$

$= 4^{10} \bmod 7$

$4^1 \bmod 7 = 4$

$4^2 \bmod 7 = 4^1 * 4^1 \bmod 7 = 4 * 4 \bmod 7 = 16 \bmod 7 = 2$

$4^4 \bmod 7 = (4^2 \bmod 7) * (4^2 \bmod 7) = 2 * 2 \bmod 7 = 4 \bmod 7 = 4$

$4^8 \bmod 7 = (4^4 \bmod 7) * (4^4 \bmod 7) = 4 * 4 \bmod 7 = 16 \bmod 7 = 2$

$4^{10} \bmod 7 = (4^8 \bmod 7) * (4^2 \bmod 7) = 2 * 2 \bmod 7 = 4 \bmod 7 = 4$

Since $4^{10} \bmod 7 = 4$, then $46^{10} \bmod 7 = 4$

Primes

What's so great about primes?

Building blocks of integers

Cryptology

Primes

What is a prime number?

Divisible only by 1 and itself

2,3,5,7,11,13,17,19...

Fundamental Theorem of Arithmetic

Prime numbers are the building blocks of integers.

Every integer greater than 1 can be uniquely written as either prime or the product of two or more primes.

Use non-decreasing order and exponential notation.

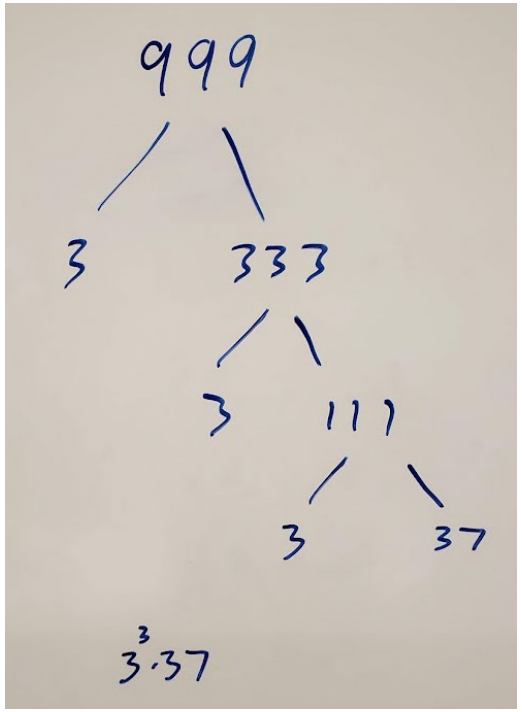
Examples:

$100 = 2 * 2 * 5 * 5 = 2^2 5^2$

$641 = 641$ 641 is prime

$999 = 3 * 3 * 3 * 37 = 3^3 * 37$

$1024 = 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 * 2 = 2^{10}$



Greatest Common Divisor (GCD)

- Greatest Common Divisor – Largest integer that divides both numbers (i.e., the largest factor of both numbers)

  What is the GCD of 24 and 36?

  Factors of 24: 1, 24, 2, 12, 3, 8, 4, 6

  Factors of 36: 1, 36, 2, 18, 3, 12, 4, 9, 6

- Relatively Prime or Coprime means their **GCD is 1**

  What is the GCD of 17 and 22?

  Factors of 17: 1, 17

  Factors of 22: 1, 22, 2, 11

Rosen, Kenneth. *Discrete Mathematics and Its Applications, 7th Edition*. McGraw-Hill, 2012

Least Common Multiple (LCM)

Least Common Multiple – Smallest positive multiple of both numbers. The smallest integer that both numbers divide.

What is the LCM of 3 and 5?

3 * 5 = 15

Multiples of 3: 3, 6, 9, 12, 15, 18, ...

Multiples of 5: 5, 10, 15, 20, ...

What is the LCM of 4 and 8?

4 * 8 = 32. But 32 is not the **lowest** multiple of 4 and 8.

The multiples of 4: 4, 8, 12, 16, ...

The multiples of 8: 8, 16, 24, ...

The smallest common multiple of both numbers is 8

Another way of thinking about it: The LCM is the smallest integer that both numbers divide:

4 | 8 and 8 | 8, so 8 is the LCM of 4 and 8.

Rosen, Kenneth. *Discrete Mathematics and Its Applications, 7th Edition*. McGraw-Hill, 2012

Finding GCD and LCM with Prime Factorization

What is the prime factorization of 26?

$2 \cdot 13$

What is the prime factorization of 36?

$2^2 \cdot 3^2$

What is gcd(26, 36)?

$26 = 2^1 \cdot 3^0 \cdot 13^1$
$36 = 2^2 \cdot 3^2 \cdot 13^0$
$\gcd(26, 36) = 2^1 \cdot 3^0 \cdot 13^0 = 2$

What is lcm(26,36)?

$26 = 2^1 \cdot 3^0 \cdot 13^1$
$36 = 2^2 \cdot 3^2 \cdot 13^0$
$\text{lcm}(26, 36) = 2^2 \cdot 3^2 \cdot 13^1 = 468$

Given:
$x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$
$y = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$

Then:
$\gcd(x, y) = p_1^{\min\{a_1, b_1\}} \cdot p_2^{\min\{a_2, b_2\}} \cdots p_r^{\min\{a_r, b_r\}}$
$\text{lcm}(x, y) = p_1^{max\{a_1, b_1\}} \cdot p_2^{\max\{a_2, b_2\}} \cdots p_r^{\max\{a_r, b_r\}}$

Finding Primes

- Trial Division (Brute Force)
  - Divide by each prime up to $\sqrt{n}$

    Example: Is 421 prime?

2 | 421 no
3 | 421 no
5 | 421 no
7 | 421 no
11 | 421 no
13 | 421 no
17 | 421 no
19 | 421 no

421 is prime

Can we use brute force to figure out if this number is prime?

3520154665960884202608832800756586623196257878464375664777310986924523236473006660983701810856106524203115367 7

- Sieve of Eratosthenes
  - Whiteboard demo
  - Python demo

Prime Number Theorem

There are an infinite number of primes

The Prime Number Theorem:

Helps us estimate how many prime numbers are in the range 2 through x.

We define $\pi(x)$ as the number of primes from 2 to x.

Then,

$$\lim_{x\to\infty}\left(\frac{\pi(x)}{x/\ln(x)}\right)=1 \qquad \left(\frac{\pi(x)}{x}\right)\approx\frac{1}{\ln(x)} \qquad \pi(x)\approx\frac{x}{\ln(x)}$$

The ratio of prime numbers between 2 and x to all numbers between 2 and x approaches 1/ln x as x approaches infinity.

Prime Number Theorem

The ratio of primes to all numbers is approximately $1/\ln(x)$.

$$\left(\frac{\pi(x)}{x}\right) \approx \frac{1}{\ln(x)}$$

As x gets larger, the ratio gets smaller.

In other words, primes become more sparse the larger the range.

If we choose a random number between 2 and x, the likelihood that it is prime is $1/\ln(x)$.

The number of primes in the range 2 through x is approximately $\pi(x) \approx \frac{x}{\ln(x)}$

Example:
How many primes are there between 2 and 1000?

$$\frac{x}{\ln(x)} = \frac{1000}{\ln(1000)} \approx 145$$

In Python, $\ln(x)$ is `math.log(x)`

Python demo