Lecture 11: Primality and Divisibility

http://book.imt-decal.org, Ch. 3.1

Introduction to Mathematical Thinking

March 5, 2019

Suraj Rampure

Announcements

- Quiz grades will be released tomorrow.
- **Homework 5 will follow a different schedule**:
  - It will be due **next Friday**, March 15
  - It is similar to the length of two homeworks, but all of it is relevant for next Thursday's quiz
  - Question 1 is a mid-semester feedback survey – please fill it out and be as detailed as possible!
  - Will also post more practice questions as I see necessary, but they will be optional
- Again, feel free to reach out if you have any concerns regarding your performance in this class

Number Theory

Now, we will begin talking about number theory:

the branch of mathematics that deals with the properties and relationships of numbers, especially positive integers

Today:

- Division Algorithm
- Divisibility
- Primality
- Fundamental Theorem of Arithmetic
- Greatest Common Divisors and Lowest Common Multiples

Next two classes: Modular arithmetic (will heavily rely on this content, though).

Chapter 3 is a work in progress, though 3.1 is almost complete. Most of what we will cover today is already posted there. Would highly recommend taking a look.

Division Algorithm

The division algorithm states that if n is any integer and d is a positive integer, there exist unique integers q, r such that

positive or negative

$$n = dq + r$$

where $0 \leq r < d$.

n : dividend
d : divisor
q : quotient
r : remainder

Examples

1) consider $n=23$, $d=5$

$23 = 5 \cdot 4 + 3$

2) consider $n=-37$, $d=8$

$-37 = 8 \cdot -5 + 3$

remainder when dividing -37 by 8 is 3.

$d \mid n$

Divisibility

In the case where $r = 0$ in $n = dq + r$, we can say that "d **divides** n", represented as $d|n$.

More formally, if we have that

$$\forall a \in \mathbb{N}, b \in \mathbb{Z}, a|b \Rightarrow \exists c \in \mathbb{Z} : b = ac$$

$8 \mid 24 \implies \exists c : 8c = 24, \ c \in \mathbb{Z}$

$\rightarrow c = 3$

$8 \mid (-24) \rightarrow 8(-3) = -24$

$3 \nmid 22$ b.c. $\neg \exists c : 3c = 22, \ c \in \mathbb{Z}$

Prime Numbers

We say an integer $n > 1$ is **prime** if its only factors are 1 and n. If n has factors other than 1 and itself, then we say it is **composite**. The number 1 is neither prime nor composite.

The smallest few prime numbers are $2, 3, 5, 7, 11, 13, \ldots$ However, it turns out that there are infinitely many primes, and therefore there does not exist a largest prime. We will look a proof of this fact shortly.

a % b : remainder when dividing a by b

Determine if n is prime

Given n, how can we determine if n is prime?

Solution 1: Enumerate through $i = 2, 3, \ldots, n-1$, and see if $i | n$.

```
def is_prime(n):
        if n <= 1:
                return False
        for i in range(2, n):
                if n % i == 0:
                        return True   False
        return False
               True
```

How can we optimize this?

Key Observation: If n is not prime, then we can find a, b such that $n = ab$.

- If we have $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > n$
- Therefore, we must have $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$
- Therefore, we can just look at the integers up until $\lfloor \sqrt{n} \rfloor$

Updated implementation:

```
def is_prime(n):
        if n <= 1:
                return False
        for i in range(2, int(n**0.5)):
                if n % i == 0:
                        return True
        return False
```

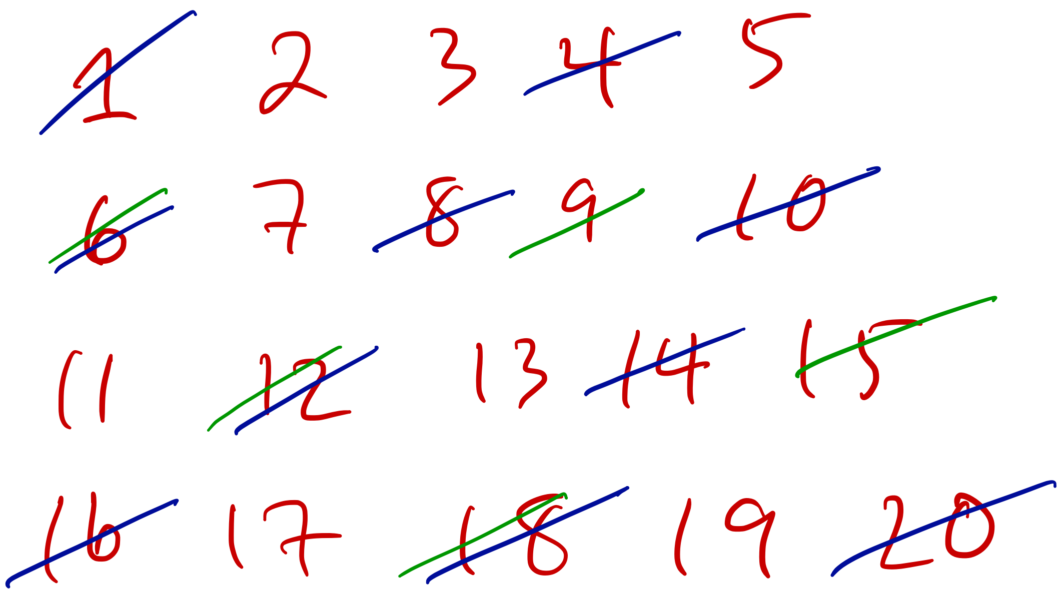
Finding all primes up to n

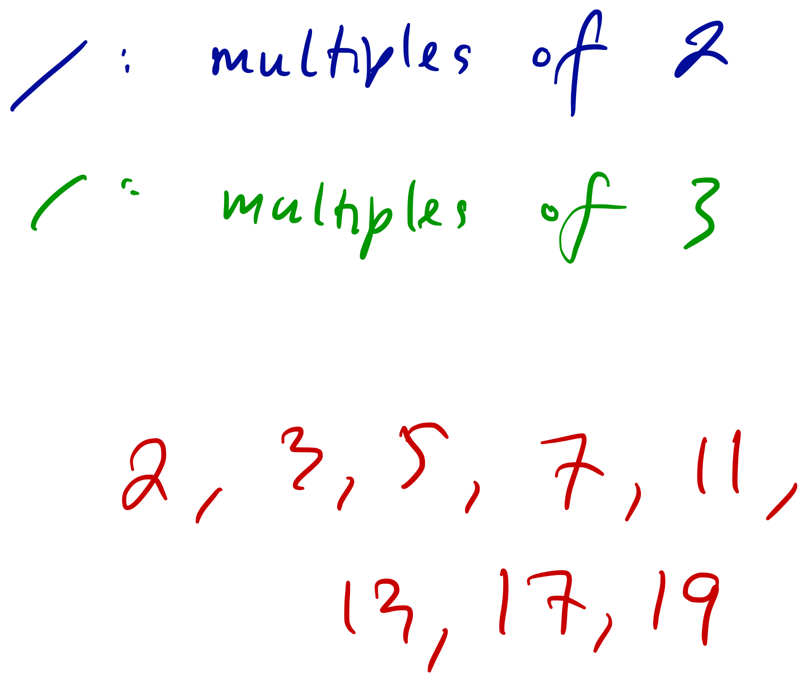
Now, let's consider the problem of finding all primes up to and including n. In other words, we want a function with the following behavior:

$$f(3) \rightarrow [2, 3]$$

$$f(20) \rightarrow [2, 3, 5, 7, 11, 13, 17, 19]$$

This can be done by the Sieve of Eratosthenes.





Fundamental Theorem of Arithmetic

The FTA states that any natural number $n > 1$ is either a prime or can be written as a unique product of prime factors.

For example, we can say that

$$
\begin{aligned}
2520 &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \\
&= 5 \cdot 7 \cdot 3 \cdot 2 \cdot 3 \cdot 2 \cdot 2 \\
&= 2^3 \cdot 3^2 \cdot 5 \cdot 7
\end{aligned}
$$

FTA states

1. We can write 2520 as the product of primes
2. This prime factorization is unique – i.e., any product of primes that equates to 2520 will consist of the three 2s, two 3s, one 5, and one 7

Determining Prime Factorizations

As an example, let's determine the prime factorization of 19600.

$$19600 = 2^4 \cdot 5^2 \cdot 7^2$$

2	19600
5	
2	1960
5	
2	196
2	98
7	49
7	

2	48
2	24
2	12
2	6
3	3
1	3

$$\rightarrow 48 = 2^4 \cdot 3$$

Canonical Representation of Natural Numbers

We can now say

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$$

where $p_1, p_2, \dots, p_k$ are the prime factors of n and $a_1, a_2, \dots, a_k$ represent their respective multiplicities ($a_i \in \mathbb{N}_0$).

e.g. $50 = 2^1 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdots\cdots$

$= 2^1 \cdot 5^2$

1) Why isn't 1 prime?

$$10 = 1 \cdot 2 \cdot 5$$
$$= 1^2 \cdot 2 \cdot 5$$
$$= 1^{100} \cdot 2 \cdot 5$$

these representations aren't unique.

2) What if $a_i \in \mathbb{Z}$? → can cover all positive rationals

~~e.g.~~ $$\frac{12}{35} = \frac{2^2 \cdot 3}{5 \cdot 7} = 2^2 \cdot 3 \cdot 5^{-1} \cdot 7^{-1}$$

255558

Example: What is the smallest number whose digits multiply to 10,000?

$$10000 = 10^4 = (2\cdot 5)^4 = 2^4 \cdot 5^4$$

22225555 < 55552222

2222 → 44

2222 → 28

digits: 2, 8, 5, 5, 5, 5

→ **255558**

Proof: Infinitely Many Primes

Proof by Contradiction

Assume only finitely many primes, $p_1, p_2, p_3, \dots, p_{k-1}, p_k$

Consider $q = p_1 p_2 p_3 \cdots p_{k-1} p_k + 1$

1) q is prime → contradiction! q not in list

2) q is not prime

→ $\exists p^*$ s.t. $p^* | q$, p^* prime

Claim: p^* not in $p_1, p_2, \dots p_k$

why? suppose $p^* = p_i$, $i \in [1, k]$

suppose $p^* = p_i$

$$\frac{q}{p^*} = \frac{p_1 p_2 p_3 \cdots p_{k-1} p_k}{p^*} + \frac{1}{p^*}$$

if $p^* | q \rightarrow \frac{q}{p^*} = n_1$, $n_1 \in \mathbb{N}$

if $p^* = p_i$, $\frac{p_1 p_2 p_3 \cdots p_{k-1} p_k}{p^*} = n_2$, $n_2 \in \mathbb{N}$

$\rightarrow n_1 = n_2 + \frac{1}{p^*} \rightarrow$ only possible when $p^* = 1$

but : 1 is not prime!

$\therefore$ p^* is not in $p_1, p_2, \cdots p_k$

$\therefore$ there exists a prime not in our list

$\therefore$ by contradiction, primes are infinite.

Multiplication Using the Canonical Representation

Suppose we have $n_1 = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ and $n_2 = p_1^{b_1} p_2^{b_2} ... p_k^{b_k}$. Then, by exponent laws,

$$n_1 \cdot n_2 = p_1^{a_1+b_1} p_2^{a_2+b_2} ... p_k^{a_k+b_k}$$

For example, consider 1200 and 2520.

$$1200 = 2^4 \cdot 3^1 \cdot 5^2 \cdot 7^0$$
$$2520 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1$$

$$1200 \cdot 2520 = 2^7 \cdot 3^3 \cdot 5^3 \cdot 7^1$$

2	2520
5	
2	252
2	126
3	63
3	
7	

Greatest Common Divisor

Now, consider the idea of the **greatest common divisor** of two numbers a, b, $\gcd(a, b)$.

This is, we want the largest d such that $(d|a) \wedge (d|b)$.

Consider 1200, 2520

$$1200 = 2^4 \cdot 3^1 \cdot 5^2 \cdot 7^0$$
$$2520 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1$$

$$\gcd(1200, 2520) = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 = \boxed{120}$$

$$2^{\min(3,4)} \mid 2^3 \quad \text{and} \quad 2^{\min(3,4)} \mid 2^4$$

General Formula for GCD

Suppose we have $a = p_1^{c_1} \cdot p_2^{c_2} \cdot \ldots \cdot p_k^{c_k}$ and $b = p_1^{d_1} \cdot p_2^{d_2} \cdot \ldots \cdot p_k^{d_k}$. Then:

$$\gcd(a, b) = p_1^{min(c_1, d_1)} \cdot p_2^{min(c_2, d_2)} \cdot \ldots \cdot p_k^{min(c_k, d_k)}$$

Note: Iff $\gcd(a, b) = 1$, we say a, b are **relatively prime** or **coprime**, i.e. they share no factors (other than 1).

if p is prime,

$\gcd(a, p) = 1$, a not a multiple of p

Linear Combinations

The following theorem will become widely useful when we start talking about modular arithmetic:

$$\forall a, b \in \mathbb{N}, \exists u, v \in \mathbb{Z} : au + bv = \gcd(a, b)$$

potentially negative

Note, we are not saying u, v are unique.

e.g. consider $a = 5$, $b = 13$ $\gcd(5, 13) = 1$

$$5u + 13v = 1$$

$$5(-5) + 13(2) = 1$$

$$5(8) + 13(-3) = 1$$

Euclid's GCD Algorithm

Euclid presents another method way to compute $\gcd(a, b)$:

```
def gcd(a, b):
        assert a >= b
        if b == 0:
                return a
    return gcd(b, a % b)
```

$$\gcd(a, b) = \gcd(b, a \% b)$$

$$\gcd(13, 5) \qquad 13 = 5 \cdot 2 + 3$$

$$\gcd(5, 3) \qquad 5 = 3 \cdot 1 + 2$$

$$\gcd(3, 2) \qquad 3 = 2 \cdot 1 + 1$$

$$\gcd(2, 1)$$

$$\gcd(1, 0)$$

$$\therefore \gcd(13, 5) = 1$$

$1200 = 2^4 \cdot 3^1 \cdot 5^2 \cdot 7^0$
$2520 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1$

2^4 is a multiple of both $2^3, 2^4$
3^2 " " $3^1, 3^2$

Lowest Common Multiples

In a similar fashion, we can define the lowest common multiple between a, b:

$$\operatorname{lcm}(a, b) = p_1^{max(c_1,d_1)} \cdot p_2^{max(c_2,d_2)} \cdot \ldots \cdot p_k^{max(c_k,d_k)}$$

Here, the $\min$ from the $\gcd$ is replaced with the $\max$. This is because a divisor will be less than or equal to a number, whereas a multiple will be greater than or equal to a number.

For example: $a = 1200 = 2^4 \cdot 3 \cdot 5^2$ and $b = 2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

$$\gcd(1200, 2520) = 2^{min(4,3)} \cdot 3^{min(1,2)} \cdot 5^{min(2,1)} \cdot 7^{min(0,1)} = 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 = 120$$

$$\operatorname{lcm}(1200, 2520) = 2^{max(4,3)} \cdot 3^{max(1,2)} \cdot 5^{max(2,1)} \cdot 7^{max(0,1)} = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^1 = 25200$$

Example

Prove that $ab = \operatorname{lcm}(a,b) \cdot \gcd(a,b)$.

$$\max(x,y) + \min(x,y) = x + y$$

$$\operatorname{lcm}(a,b) = p_1^{\max(c_1,d_1)} p_2^{\max(c_2,d_2)} \cdots p_k^{\max(c_k,d_k)}$$

$$\gcd(a,b) = p_1^{\min(c_1,d_1)} p_2^{\min(c_2,d_2)} \cdots p_k^{\min(c_k,d_k)}$$

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) = p_1^{c_1+d_1} p_2^{c_2+d_2} \cdots p_k^{c_k+d_k}$$