Number Theory

Alex Shaffer

What is Number Theory

- Number theory is a branch of math that deals primarily in integers and arithmetic functions.
  - An arithmetic function is one that has a domain in either the natural numbers and integers.

Divisibility

- Pretend for a moment you don’t know about fractions or decimals
  - An integer a divides b (written $a|b$) if there is no remainder in the division.
  - 2 divides 4 but 2 does not divide 5
- It turns out the idea of divisibility is super important to number theory and by extension cryptography.

Prime Numbers

- A prime number is one for which no numbers divide it besides 1 and itself.
- $\mathbb{P}$ sometimes is used to denote the set of primes
  - All primes below 100:
  - $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$
- If a number is not prime, then it is a composite number

Sieve of Eratosthenes

- If you have a number n and want to find all prime numbers less than it.
  - Look at the set of all numbers up to n
  - Start at 2, remove all multiples of 2 up to n
  - Then 3 and all of its multiples.
  - Then 5 (not 4 since we removed that) and remove all of its multiples.
  - Continue until you get up to n.

Fundamental Theorem of Arithmetic

- Every integer greater than 1 may be represented by a product of prime numbers that is unique, up to powers of the factors.
  - Trivially true for any prime numbers.
  - Let's try a composite: $60 = 12 \times 5 = 4 \times 3 \times 5 = 2^2 \times 4 \times 5$
  - Proof: https://en.wikipedia.org/wiki/Fundamental_theorem_of_arithmetic

Coprime Numbers

- Numbers m, and n are coprime if they share no prime factors.
- This also means that their greatest common divisor (gdc) is 1.
- Sometimes as a shorthand we will just require gdc(m, n) = 1 instead of saying they must be coprime.

How to Tell if a Number is Prime

- It is famously not easy to tell if a number is prime.
- One method is to just try dividing it by every number less than it.
- Some methods we will discuss soon:
  - Wilsons theorem.
  - Fermat’s primality test (probabilistic not guaranteed)
- https://en.wikipedia.org/wiki/Primality_test

Wilson’s Theorem

- A natural number $n > 1$ is a prime number if and only if the product of all the positive integers less than n is one less than a multiple of n.
- More compactly if $(n\ -1)! \equiv -1\ (mod\ n)$, then n is prime.
- ! Is the factorial operator, for a natural number n, n! is the product of n and all numbers less than n.
  - $n! = (n)(n\ -1)(n\ -2)(n\ -3)\ldots(2)(1)$
- https://en.wikipedia.org/wiki/Wilson%27s_theorem

Fermat’s Little Theorem

- Not to be confused with Fermat’s Last Theorem
- If p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p.
- Alternatively, this may be expressed as:
  - $a^p \equiv a \ (mod\ p)$
  - $a^{p-1} \equiv 1 \ (mod\ p)$ is equivalent.
- https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_little_theorem

The Euler Totient Function

- The Euler totient function, sometimes called the Euler φ function is defined as follows.
  - For a natural number n, $\varphi(n)$ is how many total numbers between 1 and n are coprime to n.
  - $\varphi(n) = \#\{m |\, 1 < m < n, gdc(m, n) = 1\}$

Euler’s Theorem (one of them)

- Euler’s theorem generalizes Fermat’s little theorem.
- If n and a are coprime natural numbers, then:
  - $a^{\varphi(n)} \equiv 1 (mod\ n)$
- This will be super useful for understanding RSA encryption
- https://en.wikipedia.org/wiki/Euler%27s_theorem