Number Theory

Tyler Chang
April 24, 2018

Elementary Number Theory

One of the main focuses of number theory is understanding the properties of prime numbers. But first, the primes must be rigorously defined:

- b *divides* a (or a is a *divisor* of b) if there exists $q \in \mathbb{Z}$ such that $a = bq$. Denoted $a|b$. Note that for all b, $1|b$ and $b|b$ trivially.
- An integer a has an *inverse* a^{-1} if and only if there exists $a^{-1} \in \mathbb{Z}$ such that $aa^{-1} = a^{-1}a = 1$ (where 1 is the *multiplicative identity* of $\mathbb{Z}$).
- In the ring $\mathbb{Z}$, it is true that the only numbers with inverses are 1 and -1. We capture this by stating that 1 and -1 are *units* of the integers.
- A *prime* p is a positive integer strictly greater than 1 that has no positive divisors besides 1 and itself, any other number is called a *composite*.
- The *greatest common divisor* (GCD) of two positive integers a and b (denoted: $gcd(a, b)$) is the largest integer that divides both a and b.
- Two positive integers a and b are *relatively prime* or *coprime* if $gcd(a, b) = 1$.

The *Euclidean algorithm* states that for $a, b \in \mathbb{Z}$, there exist unique integers q and r with $0 \leq r < b$ such that

$$a = qb + r \text{ where } q \text{ is the } \textit{quotient} \text{ and } r \text{ is the } \textit{remainder.}$$

Though this appears to be a theorem, by rearranging terms we see that always $gcd(a, b)|r$. Then we can iterate as follows until $r_n = 0$ to find $gcd(a, b) = r_{n-1}$:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \end{aligned}$$

The *extended Euclidean algorithm* states that for all $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$. As a corollary:

- If a and b are coprime if and only if there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.
- If p is prime and $p|(q_1 q_2 \ldots q_n)$, then p must divide *at least one* q_i.

The *Fundamental Theorem of Arithmetic* states that every integer has a unique prime factorization.

Generalization to Arbitrary Rings

For cryptography, we will work in the ring of positive integers modulo m. Note that all the above definitions generalize when $\mathbb{Z}$ is instead an arbitrary ring R, though several important theorems (with the exception of the Euclidean algorithm) fail. Notably,

- 1 and -1 are no longer the only units. In fact, if R is the integers modulo m, every element that is coprime to m is a unit.
- There may exist *zero divisors* or *characteristics*: elements p such that $qp = 0$ for all q.

RSA

We are now ready to derive RSA encryption. Let x be some data to be encrypted, represented as a binary integer. Let $m = pq$ where p and q are primes, and m is large. The RSA encryption and decryption functions are respectively given by:

$$E(x) = x^e \bmod m \quad \text{and} \quad D(x) = x^d \bmod m$$

where $ed \equiv 1 \bmod (p-1)(q-1)$.

Since the primes are not well understood, it is prohibitively difficult to factorize m into p and q (for m sufficiently large). This means that one can share e and m, so that anyone can encrypt messages. But only those with the private keys p, q, and d can decrypt messages. This is called *public key encryption.*

To understand how the decryption function undoes the encryption function is a deep exercise in number theory, starting with the *Binomial Theorem.*

The Binomial Theorem Let R be a commutative ring, and let $n \in \mathbb{N}$. Then for all $x, y \in R$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

But if n happens to be a characteristic, all the terms other than x^n and y^n drop out and we get:

The Freshman's Dream Let R be a ring with characteristic p, where p is a prime. Then $(x+y)^p = x^p + y^p$.

Then by using the Freshman's dream in an inductive argument, we can show:

Fermat's Little Theorem Let p be a prime. Then for all $a \in \mathbb{N}$, $a^p \equiv a \bmod p$.

Corollary Let p be a prime. Then if p does not divide a, $a^{p-1} \equiv 1 \bmod p$.

From the corollary, it follows that $D(E(x)) = x$ if e is chosen to be a large prime. Put formally:

RSA Let $x \in \mathbb{Z}$ and let e be a large prime. Let d be an integer such that $ed \equiv 1 \bmod (p-1)(q-1)$. Then x^{ed} (mod m) $= x$.

Prime Gaps

Given that RSA (the standard public key encryption scheme) depends on inability to perform prime factorization, it makes sense to study the distribution of primes. If all the primes were clustered in some meaninful way, or conversely, if they were *too* evenly spaced, then one could leverage this to reduce the search space for performing prime factorization.

Define the *Riemann Zeta function* for s real or complex:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Note that the sum converges uniformly for all $s > 1$, and $\zeta(s)$ is continuous for $s > 1$.

Interestingly, it can be proven that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - 1/p^s}$$

where the right hand side is called the *Euler product*. Because $\zeta(1)$ diverges, it follows by taking a log of the Euler product that $\sum_{p \text{ prime}} \frac{1}{p}$ diverges. The *infinitude of primes* follows as an immediate corollary, since if the primes were finite, the previous sum would be finite trivially (though there exists a much simpler proof by contradiction).

Dirichlet generalized the above by showing that

$$\sum_{n=1}^{\infty} \frac{\chi_q(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \chi_q(n)/p^s}$$

for all functions χ_q which assign $\chi_q(n) = 1$ if q and n are coprime, and $\chi_q(n) = 0$ otherwise.

Consequently, the following generalization is obtained:

$$\sum_{p \equiv \ell \text{ mod } q} \frac{1}{p} \to \infty$$

for all coprime ℓ and q, where the sum is taken over prime numbers p. This implies that there are infinitely many primes in every arithmetic progression $a_n = \ell + nq$ where q and ℓ are coprime.