MATH453 Elementary Number Theory

Lecture 4: Famous Conjectures About Primes and the GCD

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

4.1 Famous Conjectures

4.1.1 Goldbach's Conjecture

> **Conjecture** (Goldbach)**.** Every even integer is a sum of two primes.

4.1.2 Mersenne Prime

> **Definition 4.1.** Suppose p is prime. If $2^p - 1$ is also a prime, we say that p is a Mersenne prime.

> **Conjecture** (Infinitude of Mersenne Primes)**.** There exist infinitely many Mersenne primes.

As of October 2021, there are 51 known Mersenne primes. The largest known Mersenne prime is $2^{82,589,933} - 1$.

Both the Mersenne prime problem and the Goldbach's conjecture are unsolved problems in number theory.

4.2 GCD

GCD stands for greatest common divisor, as defined here.

> **Definition 4.2** (Greatest Common Divisor)**.** Let $a, b \in \mathbb{Z}$. The ***greatest common divisor*** of a and b is the largest of all common divisors of a and b. The notation for the GCD of a and b is (a, b) or $\gcd(a, b)$.

> **Proposition 4.1.** $\gcd(\frac{a}{d}, \frac{b}{d}) = 1 \iff (a, b) = d$

Proof.

($\Longleftarrow$): Suppose $\gcd(a, b) = d$ and $\gcd(\frac{a}{d}, \frac{b}{d}) = d'$. We want to show that $d' = 1$. By definition,

$$d' \mid \frac{a}{d} \implies \frac{a}{d} = c_1 d' \implies a = c_1 d' d$$

and

$$d' \mid \frac{b}{d} \implies \frac{b}{d} = c_2 d' \implies b = c_2 d' d$$

Thus, $d'd$ is also a common divisor of a and b. Since d is the **greatest** common divisor, $d' = 1$. Otherwise, it would contradict the maximality of d.

($\implies$): Suppose $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$ and $\gcd(a, b) = d'$. Then,

$$d' \mid a \implies a = d'c_1 \implies \frac{a}{d} = \frac{d}{d'}c_1$$

and

$$d' \mid b \implies b = d'c_2 \implies \frac{b}{d} = \frac{d}{d'}c_2$$

Thus, d'/d is a common divisor of $\frac{a}{d}$ and $\frac{b}{d}$. Since $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$, $d' = d$. So, $\gcd(a, b) = d$. ■

Proposition 4.2. Let $a, b \in \mathbb{Z}$ such that at least one of the two is not 0. Then,

$$\gcd(a, b) = \min\{ma + nb > 0 \mid m, n \in \mathbb{Z}\} > 0$$

Proof. We first show that $\{ma + nb > 0 \mid m, n \in \mathbb{Z}\}$ is not empty. This is trivial because we can arbitrary choose some m, n such that $ma + nb > 0$.

By the Well Ordering Principle, $\{ma + nb > 0 \mid m, n \in \mathbb{Z}\}$ has a minimum. Let $d = m'a + n'b$ be such minimal element.

To prove the proposition, it suffices to show that d is a common divisor of a and b and that d is the greatest common divisor.

Claim: $d \mid a$ and $d \mid b$. WLOG, $b \geq a > 0$. By the division algorithm, $a = dq + r$ where $0 \leq r < d$. Rearrange this and we get

$$r = a - dq = a - (m'a + n'b)q = (1 - m'q)a + n'qb$$

Note that unless $r = 0$, r would be a smaller linear combination of a and b, contradicting the minimality of $d = m'a + n'q$. Therefore, $r = 0$. This implies $a = dq$ so $d \mid a$. The same argument also shows that $d \mid b$.

Claim: d is the greatest common divisor of a and b. Let c be an arbitrary common divisor of a and b. We want to show that $d \geq c$ for all possible choice of c. Since c is a common divisor of a and b, it is also a common divisor of $(m'a + n'b)$. Hence, $c \mid (m'a + n'b)$ so $c \mid d$. This implies that $c \leq d$.

Combining the two claims proves that d is the greatest common divisor. ■

4.3 Euclidean Algorithm

Proposition 4.2 gives us a way to find the greatest common divisor between two numbers. But it is not easy to compute. The Euclidean algorithm is an easier and more commonly used algorithm for finding the GCD.

Lemma 4.1. Let $a, b \in \mathbb{Z}^+$ such that $a \geq b$. Let $a = bq + r$ for $q, r \in \mathbb{Z}$. Then, $\gcd(a, b) = \gcd(b, r)$.

Proof. To prove the lemma, it suffices to prove that for $a = bq + r$, $\gcd(a, b) = c$ if and only if $\gcd(b, r) = c$.

Let c be such that $c \mid a$ and $c \mid b$. Then, $c \mid r$ because r is a linear combination of a and b.

Let $c \mid b$ and $c \mid r$. Then, $c \mid a$ because a is a linear combnation of b and r. Putting the two parts together, we have $c = \gcd(b, r) = \gcd(a, b)$. ■

Now we are ready to state the Euclean algorithm.

Theorem 4.2 (Euclidean Algorithm)**.** Let $a, b \in \mathbb{Z}^+$ with $a \geq b > 0$. By the division algorithm,

$$a = bq_1 + r_1$$

for some $q_1, r_1 \in \mathbb{Z}$ such that $0 \leq r_1 < b$.

If $r_1 > 0$, we apply the division algorithm by letting

$$b = r_1 q_2 + r_2$$

for some $q_2, r_2 \in \mathbb{Z}$ such that $0 \leq r_2 < r_1$.

If $r_2 > 0$, we apply the division algorithm again by letting

$$r_1 = r_2 q_3 + r_3$$

for some $q_3, r_3 \in \mathbb{Z}$ such that $0 \leq r_3 < r_2$.

Repeat until $r_n = 0$ for some n. If $n > 1$, then $\gcd(a, b) = r_{n-1}$. If $n = 1$, $\gcd(a, b) = b$.

Proof. We first observe that the algorithm terminates after a finite amount of iterations since $r_1 > r_2 > \cdots > r_n = 0$ is a strictly decreasing sequence of positive integers.

If $n = 1$, $r_1 = 0$. In this case, $a = bq_1$ for some q_1 and $b \mid a$. It follows that $\gcd(a, b) = b = \gcd(b, 0)$.

Otherwise,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$$

by repeated application of Lemma 4.1. ■