MATH453 Elementary Number Theory

Lecture 1: Intro to Number Theory

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

1.1 Introduction

Three branches of number theory: Elementary, Analytic, Algebraic, (Probabilistic)

Connections to other subjects: Discrete mathematics, physics, etc.

1.1.1 Twin Primes

Primes often appear in paris: 3 and 5, 5 and 7, 11 and 13.

Definition 1.1 (Twin Primes). If p and $p+2$ are primes, then we call them ***twin primes***.

A famous conjecture is that there exits infinitely many primes.

Conjecture. There exists infinitely many twin primes.

A follow-up question to this conjecture is: Does the distance between consecutive primes become arbirarily large.

Let $\pi(x)$ denote the number of primes $\leq x$. For example, $\pi(6) = 3$ because there are 3 primes, namely 2, 3, 5, less than or equal to 6. To answer this question, we would like to bound the number of primes less than or equal to x as x grows.

Theorem 1.1 (Prime Number Theorem). As $x \to \infty$, $\pi(x) \sim \frac{x}{\log x}$.

This was first proved by Hadamard and de la Vallée-Poussin in 1869. A slightly better bound uses the notion of a ***logarithmic integral***

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$$

and

$$\pi(x) = \mathrm{li}(x) + \underbrace{\Delta(x)}_{\text{error term}}$$

Next, we bound the error term.

Definition 1.2 (Big-O). We say that $f(x) = O(g(x))$ as $x \to \infty$ if there exists some constant $c > 0$ such that $|f(x)| \leq c|g(x)|$ for sufficiently large x.

The Big-O notation is useful in number theory because it allows us to bound terms that we don't know the exact value of (for example, some error terms). The best known bound on $\pi(x)$ using big-O notation is

$$\pi(x) = \text{li}(x) + O\left(xe^{\frac{\log^{1/5} x}{(\log(\log(x)))^{1/5}}}\right)$$

It is also conjectured that $pi(x) = \text{li}(x) + O(\sqrt{x}\log^2 x)$.

1.2 Riemann Hypothesis

Recall that the geometric series $\sum_{n=1}^{\infty} 1/n^x$ converges for $x > 1$. Similarly, $\sum_{n=1}^{\infty} 1/n^z$ converges for $\text{Re } z > 1$.

We can generalize this for the Riemann zeta function.

Theorem 1.2.

$$\sum_{n=0} z^n = \frac{1}{1-z}$$

when $|z| > 1$.

The series $\sum_{n=0} z^n = \frac{1}{1-z}$ is also called the ***Riemann zeta function***, denote $\zeta(z)$. So this can be equivalently stated as: $\zeta(z)$ has an **analytic continuation** to the entire complex plane.

Conjecture (Riemann Hypothesis). All non-trivial zeros of the Riemann zeta function are on $\text{Re } z = 1/2$.

Pictorially, the Riemann hypothesis can be visualized using the diagram below.

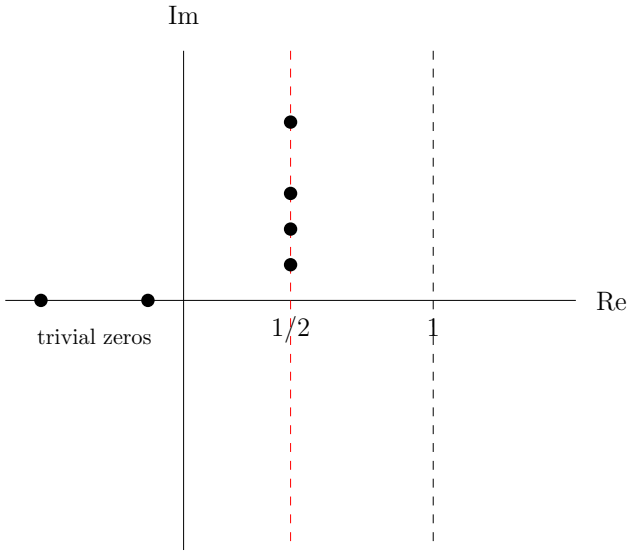

Figure 1.1: The non-trivial zeros of $\zeta(z)$ on a complex plane.

MATH453 Elementary Number Theory

Lecture 2: Congruence and The Division Algorithm

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

2.1 Congruence and Sum of Two Squares

Recall that $a \equiv b \mod c$ if and only if $c \mid (a-b)$.

If $p \equiv 1 \mod 4$, we will show that $p = a^2 + b^2$ for some integers a and b. Such pair of a, b where $a, b \in \mathbb{Z}$ is called a ***lattice point***.

Theorem 2.1 (Fermat's theorem on sum of two squares)**.** An odd prime p can be expressed as $p = x^2 + y^2$ with integers x and y if and only if $p \equiv 1 \mod 4$.

Let $r_2(n)$ denote the number of representations of n as a sum of two squares. We would like to study the behavior of $\sum_{n \le x} r_2(n)$.

We start with **Gauss's attempt** in trying to bound $\sum_{n \le x} r_2(n)$. As we can see, each lattice point can be represented as the coordinate (m, n) of a point on a plane. If we draw a circle with radius r, then all lattice points within the circle have the property

$$m^2 + n^2 \le r^2$$

Then, the problem of bounding $\sum_{n \le x} r_2(n)$ for some x is the same as finding the number of lattice points within the circle centered at $(0, 0)$ with radius $\sqrt{x}$. Because of this, the problem is also known as ***Gauss circle problem***.

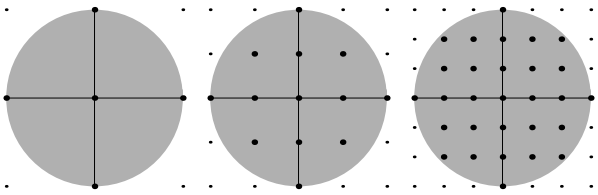

Figure 2.1: Gauss's circle problem

Theorem 2.2 (Gauss's solution)**.**

$$\sum_{n \le x} r_2(n) = \pi x + O(\sqrt{x}) = \pi x + \underbrace{E(x)}_{\text{error term}}$$

So, $E(x) \in O(x^{1/2})$.

Proof. We associate each representation of a number as two squares with a square on the plane, enclosed within the circle of radius $\sqrt{x}$.

Then, the number of such lattice points is bounded above by the area of the larger circle and bounded below by the smaller circle.

$$\pi(\sqrt{x}-1)^2 \leq \sum_{n\leq x} r_2(n) \leq \pi(\sqrt{x}+1)^2$$

We can further rearrange this to get

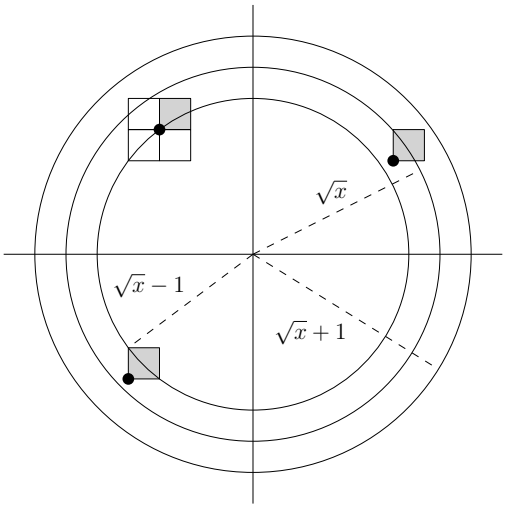

Figure 2.2: Using area to bound the number lattice points.

$$\pi(x-2\sqrt{x+1}) \leq \sum_{n\leq x} r_2(n) \leq \pi(x+2\sqrt{x}+1)$$

Then, $\sum_{n\leq x} r_2(n) = \pi x + O(\sqrt{x})$. ■

Over the years, there have been numerous improvements on bounding the error term.

Theorem 2.3 (Sierpinski 1906)**.**

$$\sum_{n\leq x} r_2(n) = \pi x + O(x^{1/3})$$

2.2 Integer Partition

Next, we will consider the integer partition. A ***partition*** of an integer $n \in \mathbb{Z}^+$ is one way of representing n as a sum of **more than one** (possibly repeating) integers.

We define $P(n)$ to be the number of ways of writing $n \in \mathbb{Z}^+$ as a sum of positive integers (ways to partition n).

For example, $P(4) = 5$ because $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$. Note that 4 itself does not count since we need at least 2 integers for it to be a valid partition.

Conjecture (Ramanujan's Conjecture on Integer Partition). $P(5n+4) \equiv 0 \mod 5$, $P(7n+5) \equiv 0 \mod 7$, $P(11n+6) \equiv 0 \mod 11$.

2.3 Division Algorithm

2.3.1 Propositions About Division

Before we talk about the division algorithm, we first introduce some useful propositions about division.

Proposition 2.1. $a \mid b$ and $b \mid c \implies a \mid c$.

Proof. The proof is straightforward from the definition of the division relation.

Since $a \mid b$, $\exists c_1 \in \mathbb{Z}.\, b = c_1 a$. Similarly, $\exists c_2 \in \mathbb{Z}.\, c = c_2 b$ since $b \mid c$. We can then rewrite c as $c = c_2 b = c_1 c_2 a = (c_1 c_2)a$. Since c_1 and c_2 are all integers, $c_1 c_2$ is also an integer. Then, by definition, $a \mid c$. ■

Proposition 2.2. If $c \mid a$ and $c \mid b$, then $\forall m, n \in \mathbb{Z}.\, c \mid (ma + nb)$.

Proof. Again, this is immediate from the definition and basic arithmetics.

Since $c \mid a$, $\exists c_1 \in \mathbb{Z}.\, a = c_1 c$. Since $c \mid b$, $\exists c_2 \in \mathbb{Z}.\, b = c_2 c$.

Let $m, n \in \mathbb{Z}$ be arbitrary. Then, $ma + mb = mc_1 c + nc_2 c = c(mc_1 + nc_2)$. By definition, $c \mid (ma + mb)$. ■

2.3.2 Floor and Ceiling

Definition 2.1 (Floor). The floor of x, denoted $\lfloor x \rfloor$, is the greatest integer less than or equal to x.

Similarly, we define the ceiling as follows

Definition 2.2 (Ceiling). The ceiling of x, denoted $\lceil x \rceil$, is the smallest integer greater than or equal to x.

Remark. In his lecture notes, Professor Berndt used $[\cdot]$ for floor. I decided to use the more standard notation in my notes to avoid confusion.

Lemma 2.4. For $x \in \mathbb{R}$, $x - 1 < \lfloor x \rfloor \leq x$.

Proof. By contradiction. Suppose not, then there exists some $x \in \mathbb{R}$ such that $x - 1 \geq \lfloor x \rfloor$. Take such x and add 1 to both sides of the inequality, yielding $x \geq \lfloor x \rfloor + 1$. But by definition, $\lfloor x \rfloor$ is the greatest integer less than or equal to x. The fact that $\lfloor x \rfloor + 1$, which is strictly greater than $\lfloor x \rfloor$, is also less than or equal to x contradicts the definition of floor. Therefore, the original lemma holds. ■

2.3.3 The Division Algorithm

The **division algorithm** is also known as the **quotient remainder theorem**. The statement is as follows.

Theorem 2.5 (The Division Algorithm)**.** Let $a, b \in \mathbb{Z}$ such that $b > 0$. Then, there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $0 \leq r < b$.

Proof. We divide the proof into two parts: existence and uniqueness. We first prove **existence** by construction.

Take $q = \lfloor a/b \rfloor$ and $r = a - b\lfloor a/b \rfloor$. Then, we have

$$a = b\left\lfloor \frac{a}{b} \right\rfloor + r$$

This proves that $a = bq + r$. Next, we show that $0 \leq r < b$. By Lemma 2.4,

$$\frac{a}{b} - 1 < \left\lfloor \frac{a}{b} \right\rfloor \leq \frac{a}{b}$$

Since $b > 0$, we can multiply both sides by b, yielding

$$a - b < \left\lfloor \frac{a}{b} \right\rfloor b \leq a$$

Mutiply by -1 and reversing the signs, and then add a to both sides

$$\begin{aligned} b - a &> -\left\lfloor \frac{a}{b} \right\rfloor b && \geq -a \\ b &> -\left\lfloor \frac{a}{b} \right\rfloor b + a && \geq 0 \end{aligned}$$

Since $r = a - b\lfloor a/b \rfloor$, by substitution, $b > r \geq 0$. This proves the existence of such q, r.

Next, we prove the **uniqueness** of such q and r by contradiction. Suppose for contradiction that there exists some $q' \neq q$ and $r' \neq r$ such that $a = bq' + r'$ and $0 \leq r' < b$. Then,

$$a - a = 0 = b(q - q') + (r - r')$$

$|r - r'| < b$ because both $r < b$ and $r' < b$. WLOG, suppose $r' > r$. Then, $r' - r = b(q' - q)$ by rearranging the previous inequality. This implies that $r' - r$ is a multiple of b. But since $r' - r$ is strictly less than b,

$$0 \leq r' - r < b$$

$r' - r$ must be 0. This contradicts the assumption that $r \neq r'$. Similarly, $q = q'$ since $r = r'$, which is also a contradiction. ∎

MATH453 Elementary Number Theory

Lecture 3: Primes

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

3.1 Elementary Properties of Primes

Recall that a natural number **greater than 1** is ***prime*** if it has no factors other than 1 and itself. A natrual number greater than 1 is ***composite*** if it is not prime.

We begin by introducing some elementary facts about prime numbers.

Lemma 3.1. Every integer greater than 1 has a prime divisor.

Proof. By (strong) induction on n.

Base case: $n = 2$. The lemma clearly holds because 2 is a prime.

Inductive step: Let $n \geq 2$ be an arbitrary integer. Suppose that the lemma is true for all integers $2 \leq n' < n$. If n is prime, we are done. So assume n is not prime. Then, by definition, n is composite and can be expressed as $n = ab$ for some $a, b < n$. By induction hypothesis, a and b both have at least one prime divisors. Hence, n also have a prime divisors. ■

Theorem 3.2 (Infinitude of Primes)**.** There exists infinitely many primes.

Proof. By contradiction. Suppose there exist only finitely many primes $p_1, \ldots, p_n$.

Let $N = p_1 p_2 \ldots p_n + 1$. By Lemma 3.1, N has at least one prime divisor and since $\{p_1, \ldots, p_n\}$ are all the primes by assumption, there must exists some i such that $p_i \mid N$. Since $p_i \in \{p_1, \ldots, p_n\}$, we have that $p_i \mid p_1 \ldots p_n$ trivially. Further, $p_i \mid N$, so $p_i \mid N - p_1 \ldots p_n$. This implies that $p_i \mid 1$. But no prime can divide 1. This is a contradiction. ■

Proposition 3.1. If n is composite, then there exists at least one prime $p \leq \sqrt{n}$ dividing n.

Proof. By contradiction. Let n be an arbitrary composite number. By Lemma 3.1, we know that has at least one prime divisor p_j. Suppose for contradiction that all such p_j are $p_j > \sqrt{n}$.

n is composite, so we assume that it has m divisors of n where $m \geq 2$. Then,

$$n > \underbrace{\sqrt{n}\sqrt{n} \cdots \sqrt{n}}_{m} = n^{m/2} \geq n$$

This implies $n > n$, which is a contradiction. ■

3.2 Finding Primes

Algorithm known as the Sieve[1] of Eratosthenes.

To find all primes $\leq x$, we list all integers up to x. Strike out every integer $\leq \sqrt{x}$ that is a multiple of primes $\leq \sqrt{x}$. In the end, whatever remains are primes.

Example (Finding primes ≤ 28)**.** List all numbers:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

2 is prime, so we circle it. Then, we strike out all numbers that is a multiple of 2.

$\boxed{2}$ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~ 27 ~~28~~

The next number, 3, is not struck out, so 3 is prime. We circle 3 and cross out all multiples of 3.

$\boxed{2}$ $\boxed{3}$ ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25 ~~26~~ ~~27~~ ~~28~~

The next number, 5, is not struck out, so 5 is prime. We circle 5 and cross out all multiples of 5 that are not yet struck out.

$\boxed{2}$ $\boxed{3}$ ~~4~~ $\boxed{5}$ ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~

Since $4 < \sqrt{28} < 5$, we can stop here and box all the remaining numbers. They are primes because they are not struck out.

$\boxed{2}$ $\boxed{3}$ ~~4~~ $\boxed{5}$ ~~6~~ $\boxed{7}$ ~~8~~ ~~9~~ ~~10~~ $\boxed{11}$ ~~12~~ $\boxed{13}$ ~~14~~ ~~15~~ ~~16~~ $\boxed{17}$ ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ $\boxed{23}$ ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~

To test if a number n is prime, we test all primes $p \leq \sqrt{n}$. If none divides n, then n is prime. There are more efficient algorithms for primality testing. More recently, the AKS primality testing algorithm was shown to be able to run in polynomial time.

3.3 Consecutive Composites

Proposition 3.2. For every $n \in \mathbb{Z}^+$, there exists n consecutive composite numbers.

Proof. By construction.

$(n+1)!+2$, $(n+1)!+3$, …, $(n+1)!+(n+1)$ are all composite. ∎

Note that this construction may not give the smallest n consecutive composite numbers.

[1] strainer, colanders, used for filtering; this name is likely due to the fact that the algorithm "filters out" the non-primes.

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 Eucliean 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. ■

MATH453 Elementary Number Theory

Lecture 5: Prime Frequency and Factorization

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

5.1 Distribution of Primes

Recall that from calculus, we know that $\sum_{n=1}^{\infty} \frac{1}{n} = \infty$ but $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Now, one might be interested in knowing how the series

$$\sum_{p \text{ prime}} \frac{1}{p}$$

behaves.

Theorem 5.1. For every $y \geq 2$,

$$\sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p} \geq \log\log y - 1$$

Proof. Let $\mathcal{N}$ be the subset of $\mathbb{Z}^+$ whose prime factorizations contain only primes $\leq y$. Consider $\sum_{n=1}^{\lfloor y \rfloor} 1/n$, which is an upper bound on the sum that we are interested in.

$$\sum_{n=1}^{\lfloor y \rfloor} \frac{1}{n} \geq \int_1^{\lfloor y \rfloor + 1} \frac{dx}{x} = \log(\lfloor y \rfloor + 1) \geq \log(y) \tag{5.1}$$

Now, consider the product of the geometric series over all primes $p \leq y$.

$$\prod_{\substack{p \leq y \\ p \text{ prime}}} \left(\sum_{i=0}^{\infty} \frac{1}{p^i} \right) = \prod_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{1 - 1/p} = \sum_{n \in \mathcal{N}} \frac{1}{n} \geq \sum_{n=1}^{\lfloor y \rfloor} \frac{1}{n} \geq \int_1^{\lfloor y \rfloor + 1} \frac{dx}{x} \geq \log y \tag{5.2}$$

Claim. For $0 \leq v \leq \frac{1}{2}$, $e^{v+v^2} \geq \frac{1}{1-v}$. Let $v = 1/p \leq 1/2$.

Then, from the claim,

$$\prod_{\substack{p \leq y \\ p \text{ prime}}} e^{\frac{1}{p} + \frac{1}{p^2}} \geq \prod_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{1 - 1/p} \geq \log y \tag{5.3}$$

Take the logarithm of both sides,

$$\log \prod_{\substack{p \leq y \\ p \text{ prime}}} e^{\frac{1}{p} + \frac{1}{p^2}} \leq \sum_{\substack{p \leq y \\ p \text{ prime}}} \log e^{\frac{1}{p} + \frac{1}{p^2}} = \sum_{\substack{p \leq y \\ p \text{ prime}}} \left(\frac{1}{p} + \frac{1}{p^2} \right) \geq \log\log y \tag{5.4}$$

Further, we observe that

$$\sum_{\substack{p \leq y \\ p \text{ prime}}} \frac{1}{p^2} \leq \sum_{n=2}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6} < 1 \tag{5.5}$$

So it follows that

$$\sum_{\substack{p \le y \\ p \text{ prime}}} \frac{1}{p} > \log\log y - \sum_{\substack{p \le y \\ p \text{ prime}}} \frac{1}{p^2} > \log\log y - 1 \tag{5.6}$$

■

We must also prove the claim we have used in the proof of the theorem.

Lemma 5.2. For $0 \le v \le 1/2$,

$$e^{v+v^2} \ge \frac{1}{1-v}$$

Proof. Let $f(v) = (1-v)e^{v+v^2}$. $f(0) = 1$. We see that the first derivative is non-negative and thus f is non-decreasing on $[0, \frac{1}{2}]$.

$$f'(v) = -e^{v+v^2} + (1-v)(1+2v)e^{v+v^2} = v(1-2v)e^{v+v^2}.$$

Then, since $f(v) = (1-v)e^{v+v^2}$ is non-decreasing on $[0, 1/2]$, we have

$$f(v) = (1-v)e^{v+v^2} \ge f(0) = 1 \qquad \forall v \in [0, 1/2]$$

This implies that $e^{v+v^2} \ge \frac{1}{1-v}$ for $0 \le v \le 1/2$. ■

5.2 Fundamental Theorem of Arithmetic

Now we introduce a few lemmas in preparation for the Fundamental Theorem of Arithmetic.

Lemma 5.3. Let p be prime such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Proof. Assume that $p \mid ab$. If $p \mid a$, then we are done, so assume that $p \nmid a$. Then, a and p are coprime, so $\gcd(p, a) = 1$. There exists some $m, n \in \mathbb{Z}$ such that $ma + np = 1$ by Prop 4.2.

$b = 1 \cdot b$ so $b = mab + npb$. By assumption, $p \mid ab$. Then, there exists $c \in \mathbb{Z}$ such that $ab = pc$. It follows that

$$b = mpc + npb = p(mc + nb)$$

which, by definition of divisiblity, $p \mid b$. ■

Corollary 5.4. Let p be prime, $a_1, \ldots, a_n \in \mathbb{Z}$ for $n \ge 2$. If $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_j$ for at least one $j \in \{1, 2, \ldots, n\}$.

Proof. By Lemma 5.3, $p \mid a_1 \ldots a_{n-1}$ or $p \mid a_n$. Prove by induction on $n \ge 2$. ■

Theorem 5.5 (Fundamental Theorem of Arithmetic)**.** Every integer $a > 1$ can be represented **uniquely** as a product of primes

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

where $p_i \ne p_j$ if $i \ne j$ for positive integers a_i.

Now, we are ready to prove the ***Fundamental Theorem of Arithmetic***. It states the factorizability of any positive integers so the theorem is sometimes called the unique factorization theorem.

Proof. By contradiction.

Assume that there exists some integer without a prime factorization. Take c to be the smallest of such counterexamples. Then, c must be composite (otherwise, c itself would be a unique prime factorization of c). Then, $c = ab$ for some $a, b > 1$ and $a, b < c$. Since c is the smallest counterexample, a and b, which are smaller than c, can be represented as products of primes. Therefore, c indeed has a prime factorization that is the product of the prime factorizations of a and b. This is a contradiction, so c **has a prime factorization**.

It remains to be shown that the factorization of c is unique. Suppose for contradiction that c has two prime factorizations. That is

$$c = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} = q_1^{b_1} q_2^{b_2} \cdots q_n^{b_n}$$

where $p_1 < p_{i+1}$ and $q_j < q_{j+1}$ for all $i \in \{1, \ldots, m-1\}$ and $j \in \{1, \ldots, n-1\}$.

It suffices to show that $p_j = q_j$, $a_j = b_j$ for all j, $m = n$.

Fix arbitrary p_i. By Corollary 5.4, $p_i \mid q_j$ for some j. Since p_i and q_j are prime, it follows that $p_i = q_j$ because otherwise it would be a contradiction. Similarly, fix q_j, and by the same argument, $q_j \mid p_i$ for some i so $p_i = q_j$. Thus, $p_j = q_j$ for all j. This also implies that $m = n$.

Finally, we show that the exponents are also equal. Suppose for contradiction that there exists some j such that $a_j \neq b_j$. Without loss of generality, assume $a_j < b_j$. Since

$$p_j^{b_j} \mid c = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

so $p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} = k p_j^{b_j}$ for some $k \in \mathbb{Z}$. It follows that by dividing both sides by $p_j^{a_j}$,

$$p_1^{a_1} p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n} = k p_j^{b_j - a_j}$$

Since $b_j - a_j > 0$, $p_j \mid p_1^{a_1} p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n}$. By Corollary 5.4, $p_j \mid p_i$ for some $i \neq j$. But this is not possible because for all $i \in \{1 \ldots n\} \setminus \{j\}$, p_i is prime and p_j is **not a factor** of $p_1^{a_1} p_2^{a_2} \cdots p_{j-1}^{a_{j-1}} p_{j+1}^{a_{j+1}} \cdots p_n^{a_n}$. Hence, $p_i \mid p_j$ and $p_i \neq p_j$, which is a contradiction because a prime cannot divide another prime.

Therefore, the prime **factorization is unique**. ■

MATH453 Elementary Number Theory

Lecture 6: LCM and Dirichlet's Theorem

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

6.1 Least Common Multiple

Definition 6.1 (Least Common Multiple)**.** Let $a, b \neq 0$. The ***least common multiple*** of a and b, denoted by $[a, b]$ or $\text{lcm}(a, b)$, is the least $m > 0$ such that $a \mid m$ and $b \mid m$.

Example. What is $\text{lcm}(2^3 3^2 7^5, 2 \cdot 3^5 7 \cdot 11^2)$?
We take the least common multiple of each factor, so we have $2^3 3^5 7^5 11^2$

If $\gcd(a, b) = 1$, $\text{lcm}(a, b) = ab$. In general, we have the following theorem

Theorem 6.1. $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$

Proof. Assume $a, b > 1$. If either a or b is equal to 1, then the proof is trivial. Let

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

so that $p_1, \ldots, p_n$ are the primes in common to a and b. Since $\gcd(a, b)$ is the greatest common **divisor**,

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

Also,

$$\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

Multiply the two together and we get

$$\gcd(a, b) \cdot \text{lcm}(a, b) = p_1^{a_1 + b_1} \cdots p_n^{a_n + b_n} = (p_1^{a_1} \cdots p_n^{a_n}) \cdot (p_1^{b_1} \cdots p_n^{b_n}) = ab$$

■

In practice, we can use theorem to find the least common multiple once we find the greatest common divisor using the Euclidean algorithm.

6.2 Arithmetic Progression and Dirichlet's Theorem

Arithmetic progression is another name for the arithmetic sequence, a sequence of integers in which the difference between two consecutive numbers is constant. In general, the nth term in an arithmetic sequence/progression is given by

$$a_n = a_1 + (n - 1)d$$

How many primes are there in an infinite arithmetic progression? The theorem of Dirichlet tells us that indeed there are infinitely many primes in an infinite arithmetic progression.

Theorem 6.2 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** If $\gcd(a, b) = 1$ (a and b are **relatively prime**), then the set

$$\{an + b \mid n \in \mathbb{Z},\, n \geq 0\}$$

has **infinitely** many primes.

The proof of Dirichlet's theorem is beyond the scope of this course but will be covered in a course on analytic number theory. We can, however, prove some special cases of Dirichlet's theorem.

6.2.1 Special Cases of Dirichlet's Theorem

Lemma 6.3. Let $a, b \in \mathbb{Z}^+$. Suppose $a, b \in \{4n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$. Then, $ab \in \{4n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$.

Proof. Let $a = 4n_1 + 1$ and $b = 4n_2 + 1$. Then,

$$ab = (4n_1 + 1)(4n_2 + 1) = 16n_1n_2 + 4(n_1 + n_2) + 1$$

which can be factored as $4(4n_1n_2 + n_1 + n_2) + 1$. Take $n = (4n_1n_2 + n_1 + n_2)$ which is clearly a non-negative integer. Then, $n = ab \in \{4n + 1 \mid n \in \mathbb{Z},\, n \geq 0\}$. ■

Using this simple fact, we can show that there are infinitely many primes of the form $4n + 1$.

Proposition 6.1. There exist infinitely many primes in $\{4n + 3 \mid n \in \mathbb{Z},\, n \geq 0\}$.

Proof. By contradiction.

Suppose for contradiction that there exist only finitely many primes in $\{4n + 3 \mid n \in \mathbb{Z},\, n \geq 0\}$. Say there exist only $r + 1$ such primes. Clearly, $p_0 = 3$, and we have $p_0, p_1, \ldots, p_r$ from the set that are primes.

Take $N = 4p_1p_2 \cdots p_r + 3$. By the Fundamental Theorem of Arithmetic, N has some prime divisor. We claim that N has some prime divisor $q_j \in \{4n + 3 \mid n \in \mathbb{Z},\, n \geq 0\}$. Further, we claim that if not, all prime divisors of N is of the form $4n + 1$. This is because we assumed that q_j is a prime divisor and the prime numbers ≥ 3 not of the form $4n + 3$ can be written as $4n + 1$ for some n. And if all prime divisors of N are of the form $4n + 1$, then N must also be of the form $4n + 1$ by Lemma 6.3, which is not true. Then, q_j is either 3 or one of $p_1, \ldots, p_r$.

If $q_j = 3$, $q_j \mid 3$ and $q_j \mid N$. It follows that $q_j \mid (N - 3)$ so $q_j \mid 4p_1 \cdots p_r$. This is a contradiction because $p_1, \ldots, p_r$ are primes not including 3. Hence, $q_j \neq 3$.

If $q_j \in \{p_1, \ldots, p_r\}$, then $q_j \mid 4p_1 \ldots p_r$. And by choice of q_j, $q_j \mid N$. It follows that $q_j \mid N - 4p_1 \cdots p_r$. This implies $q_j \mid 3$, which is a contradiction as well becuase $3 \notin \{p_1, \ldots, p_r\}$.

In both cases, we have a contradiction so the assumption that there are finitely many primes of the form $4n + 3$ must be false. ■

Note that this proof will not work for the general case of Dirichlet's theorem because Lemma 6.3 does not hold in the general case.

Let's look another example of a similar special-case proof.

Lemma 6.4. Let $a, b \in \mathbb{Z}^+$. Suppose $a, b \in \{3n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$. Then, $ab \in \{3n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$.

Proof. Similar to the proof for Lemma 6.3. ■

Theorem 6.5. There exist infinitely many primes of the form $3n + 2$ for $n \geq 0$.

Proof. Suppose for contradiction that there exist only finitely many primes of the form $3n + 2$. Say there are $r + 1$ such primes, namely, $2, p_1, \ldots, p_r$.

Similar to the proof for the previous theorem, we let

$$N = 3p_1 \cdots p_r + 2$$

We claim that there exsits a prime divisor of N of the form $3n + 2$. To see why this claim holds, assume that N has no such divisors. Then, there are two possibilities for the prime divisors of N. First, we have $3 \mid N$. This is also not possible because $3 \nmid 2$. This implies that $3n$ is not a prime divisor for N. The only remaining possiblity is that all prime divisors of N are of the form $3n + 1$.

However, by the previous lemma, we know that if all prime divisors of N are of the form $3n + 1$, then N itself must also be of the form $3n + 1$, which is not true. Hence, N must have some prime divisor of the form $3n + 2$. Now, consider the following two cases regarding the prime divisor q of N:

Case 1: $q = 2$. we have $2 \mid N$ and clearly $2 \mid 2$. It follows thata $2 \mid N - 2$, but this is a contradiction because $3p_1 \cdots p_r$ does not contain 2 as a factor. Therefore, $q = 2$ is not possible.

Case 2: $q \in \{p_1, \ldots, p_r\}$. $q \mid N$ and $q \mid 3p_1 \cdots p_r$. It follows that $q \mid 2$. But again, this is not possible becuase q and 2 are both primes.

In both cases, we have a contradiction. This implies that N itself is a prime that is not in $\{2, p_1, \ldots, p_r\}$. Hence, our initial assumption that there are finitely many primes of the form $3n + 2$ must be false, so the theorem holds. ■

MATH453 Elementary Number Theory

Lecture 7: Congruence

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

7.1 Congruence

Definition 7.1. a is congruent to b modulo m for $m \in \mathbb{Z}^+$ iff

$$m \mid (a-b)$$

and we write $a \equiv b \mod m$.

For example, $3 \equiv 7 \mod 2$ because $3 - 7 = -4$ and $2 \mid -4$.

Remark. Note that despite that congruence is denoted by $\equiv$, some properties of equality does not hold. Importantly, $ca \equiv cb \mod m$ DOES NOT imply $a \equiv b \mod m$. For a simple counterexample, consider $4 \equiv 6 \mod 2$ but $2 \not\equiv 3 \mod 2$.

7.1.1 Properties of Congruence Relation

$$\begin{aligned}
&a \equiv a \mod m && && && \text{reflexive}\\
&a \equiv b \mod m &&\iff b \equiv a \mod m && && \text{symmetric}\\
&a \equiv b \mod m \wedge b \equiv c \mod m &&\implies a \equiv c \mod m && && \text{transitive}
\end{aligned}$$

The reflexive and symmetric properties are obvious. We will provide a short proof for the transitive property.

Proof. By definition of congruence, $a \equiv b \mod m$ means $m \mid (a-b)$. And $b \equiv c \mod m$ means $m \mid (b-c)$. It follows by property of divisibility that $m \mid (a - b + b - c)$. Then, $m \mid (a-c)$, which by definition means $a \equiv c \mod m$. ■

Because of these three properties, we say that congruence defines an **equivalence relation**. Hence, equivalence relation of congruence divides integers into **equivalence classes**, known as the **congruence classes** or **residue classes**.

7.1.2 Congruence Classes

Definition 7.2 (Congruence Classes)**.** The congruence class of a modulo m, denoted $[a]_m$, is the set of all integers that are congruent to a modulo m

$$\{z \in \mathbb{Z} \mid m \mid (a-z)\}$$

Example. Let $m = 7$. Then,

$$[0]_7 = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$$
$$[1]_7 = \{\ldots, -13, -6, 1, 8, 15, \ldots\}$$
$$[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$$
$$[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$$

Definition 7.3 (Complete Residue System)**.** A complete residue system modulo m is a set S of integers such that every $n \in \mathbb{Z}$ is congruent to one and only one member of S.

Example. $\{0, 1, 2, 3, 4, 5, 6\}$ is a complete residue system modulo 7.
Although less obvious, $\{14, 57, -12, 1060, -24, -2, 76\}$ is also a complete residue system modulo 7.

Proposition 7.1. $S = \{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.

Proof. Let $a \in \mathbb{Z}$. Apply the division algorithm to a with respect to m, so we have

$$a = mq + r \qquad 0 \leq r \leq m - 1$$

By definition of divisibility, $m \mid (a - r)$, and by definition of congruence, $a \equiv r \mod m$. This shows that every integer is congruent to a member r of $\{0, 1, \ldots, m-1\}$.

We also need to show that a is congruent to only one member of $\{0, 1, \ldots, m-1\}$. We proceed by contradiction. Assume $a \equiv r_1 \mod m$ and $a \equiv r_2 \mod m$ for some $r_1, r_2 \in \{0, 1, \ldots, m-1\}$. By transitivity, $r_1 \equiv r_2 \mod m$, which by definition means $m \mid (r_1 - r_2)$. Since both r_1 and r_2 are between 0 and $m - 1$, $0 \leq r_1 - r_2 \leq m - 1$. Then, $0 \leq r_1 - r_2 \leq m - 1$ and $m \mid (r_1 - r_2)$ imply that $r_1 - r_2 = 0$ because otherwise m cannot divide any non-zero integers less than itself. This shows that $r_1 = r_2$ and thus uniqueness. ■

Proposition 7.2. Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then

$$a + c \equiv b + d \mod m \tag{7.1}$$

$$ac \equiv bd \mod m \tag{7.2}$$

Proof. of Equation (7.1)

By definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. By property of divisibility, $m \mid (a - b + c - d)$. This is equivalence to $m \mid [(a + c) - (b + d)]$, which by definition means $a + c \equiv b + d \mod m$. ■

Proof. of Equation (7.2)

By definition, $m \mid (a - b)$ and $m \mid (c - d)$. Trivially, it follows that $m \mid c(a - b)$. Similarly, $m \mid b(c - d)$. By property of divisibility, $m \mid (ca - cb + bc - bd)$ so $m \mid (ac - bd)$. This by definition means $ac \equiv bd \mod m$. ■

MATH453 Elementary Number Theory

Lecture 8: Congruence Classes and Residue System

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

8.1 Congruence Classes

Recall that from last lecture, we defined

Definition 8.1 (Congruence Classes). The congruence class of a modulo m, denoted $[a]_m$, is the set of all integers that are congruent to a modulo m

$$\{z \in \mathbb{Z} \mid m \mid (a - z)\}$$

And we have the proposition

Proposition 8.1. Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then

$$a + c \equiv b + d \mod m \tag{8.1}$$

$$ac \equiv bd \mod m \tag{8.2}$$

From these two properties, we can define the **addition** and **multiplication** operations on congruence classes $(+, \times)$.

$$[a]_m + [c]_m = [a + c]_m$$

and

$$[a]_m \times [c]_m = [ac]_m$$

Also, recall from last lecture that we cannot just cancel common factors in a congruence relation. We established that in the general case, this will not work. For example, $6 \equiv 3 \mod 3$ but $2 \not\equiv 1 \mod 3$. However, there are cases where we can cancel factors in a congruence.

Proposition 8.2.

$$ca \equiv cb \mod m \iff a \equiv b \mod \frac{m}{\gcd(c, m)}$$

For example, say we have $6 \equiv 3 \mod 3$. By Proposition 8.2, we have $2 \equiv 1 \mod \frac{3}{\gcd(3,3)}$ so $2 \equiv 1 \mod 1$. Now, we prove this proposition.

Proof.

($\implies$): Assume that $ca \equiv cb \mod m$, which by definition, implies that $m \mid (ca - cb)$ and $m \mid c(a - b)$. By definition of divisibility, there exists some d such that $c(a - b) = md$. Then, we can divide both sides by the greatest common divisor of c and m, giving us

$$\frac{c}{\gcd(c, m)}(a - b) = \frac{m}{\gcd(c, m)}d$$

Further, since $\gcd(c, m)$ is the greatest common divisor, $\gcd\left(\frac{c}{\gcd(c,m)}, \frac{m}{\gcd(c,m)}\right) = 1$. This implies

$$\frac{m}{\gcd(c, m)} \mid (a - b)$$

which by definition means $a \equiv b \mod \frac{m}{\gcd(c,m)}$.

($\Longleftarrow$): Assume that $a \equiv b \mod \frac{m}{\gcd(c,m)}$. By definition, $\frac{m}{\gcd(c,m)} \mid (a - b)$. So there exists some d such that

$$a - b = \frac{m}{\gcd(c, m)} d \implies ca - cb = \frac{cm}{\gcd(c, m)} d = \frac{cd}{\gcd(c, m)} m$$

This implies $m \mid (ca - cb)$ since $\frac{cd}{\gcd(c,m)}$ is an integer. Then by definition of congruence, $ca \equiv cb \mod m$. ■

8.2 Reduced Residue System

Also recall that from last lecture, we defined a ***complete residue system***.

Definition 8.2 (Complete Residue System)**.** A **complete residue system** modulo m is a set S of integers such that every $n \in \mathbb{Z}$ is congruent to one and only one member of S.

Definition 8.3 (Reduced Residue System)**.** A **reduced residue system** modulo m is a set of integers $r_1, \ldots, r_n$ such that if $\gcd(a, m) = 1$, then $a \equiv r_j \mod m$ for one and only one value of j.

Stated slightly differently, a reduced residue system modulo m is a set of integers r_i such that $\gcd(r_i, m) = 1$ for all i, and $r_i \not\equiv r_j \mod m$ for all $j \neq i$. That is, each element in a reduced residue system is relatively prime to m and no two elements of the set are congruent modulo m.

Note that the definition of a reduced residue system immediately implies that $n < m$. To see why, suppose $n = m$ and we have a complete residue system. Then, $m \equiv m \mod m$. WLOG, suppose $m = r_j$ for some j (otherwise, we can choose r_j to be some multiple of m). By definition, there's some a such that $a \equiv m \mod m$ but this is impossible since a and m are relatively prime by definition of a reduced residue system. This implies that m or any multiple of m must not be an element in a reduced residue system.

Another way of looking at a reduced residue system is that we can take a complete residue system, remove certain numbers, and get back a reduced residue system. In particular, if we have a complete residue system modulo m, and we remove all r_j such that $\gcd(r_j, m) = 1$, the resulting system is a reduced residue system. This should be clear from the definition of a reduced system.

Additionally, if $\gcd(a, m) = 1$ and $a \equiv r_j \mod m$ for some a, then $\gcd(r_j, m) = 1$. This essentially shows that our alternative definition is the same as the original definition.

Proof. Suppose not. That is, there exists a such that $\gcd(a, m) = 1$ and $m \mid (a - r_j)$ but $\gcd(r_j, m) \neq 1$. This implies there exists some p such that $p \mid r_j$ and $p \mid m$. But we also have $a - r_j = md$ for some d since $m \mid (a - r_j)$. This implies $p \mid a$. But by our assumption, a and m should be relatively prime, so this is a contradiction. ■

8.3 Euler's Phi Function

The number of elements in a reduced residue system modulo m for some fixed m is **constant**. We call this number ***Euler's phi function*** or ***Euler's totient function***. The Euler's phi function for m is denoted by

$$\varphi(m)$$

Theorem 8.1. Let $r_1, \ldots, r_n$ be a complete/reduced residue system modulo m. Let $\gcd(a, m) = 1$. Then,

$$\{ar_1, \ldots, ar_n\}$$

is still a complete/reduced residue system modulo m.

Proof. Suppose for contradiction that $\{ar_1, \ldots, ar_n\}$ is not a complete/reduced residue system modulo m for some m. Then, there must exitsts some i and j such that $ar_i \equiv ar_j \mod m$ (if no such i, j exists, then $\{ar_1, \ldots, ar_n\}$ would indeed be complete/reduced). But since $\gcd(a, m) = 1$, $ar_i \equiv ar_j \mod m \iff r_i \equiv r_j \mod m$. This is a contradiction to the assumption that $\{r_1, \ldots, r_n\}$ is a complete/reduced residue system. ■

MATH453 Elementary Number Theory

Lecture 9: Linear Congruence

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

9.1 Linear Congruence

We are all familiar with linear equations like

$$ax + b = 0$$

We are going to talk about a different kind of linear "equation" known as linear congruence. They are of the form

$$ax \equiv b \mod m$$

Let's consider some linear congruence. First, we look at $3x \equiv 1 \mod 6$. If we try everything from 0 to 5, it is easy to notice that this does not have a solution.

How about $2x \equiv 4 \mod 6$. We have one solution $\{2, 8, 14, \dots, \}$ and another solution $\{5, 11, 17, \dots\}$. In total, we have two solutions. Further, these two solution sets are incongruent because elements from one set is not congruent to those from the other set modulo 6.

$2x \equiv 5 \mod 6$ does not have a solution. But $3x \equiv 1 \mod 5$ have the solution $\{2, 7, 12, \dots, \}$.

The two examples that do not have a solution are $3x \equiv 1 \mod 6$ and $2x \equiv 5 \mod 6$. The ones that do have solutions are $2x \equiv 4 \mod 6$ and $3x \equiv 1 \mod 5$. From these examples, we make the observation that one thing in common among the linear congruences that do not have a solution is that the GCD of a and m does not divide b. In particular, we have that $\gcd(3, 6) \nmid 1$ and $\gcd(2, 6) \nmid 5$. On the other hand, $\gcd(2, 6) \mid 4$ and $\gcd(3, 5) \mid 1$.

We can generalize this into the following theorem:

Theorem 9.1. Let $ax \equiv b \mod m$ be a linear congruence in one variable and let $d = \gcd(a, m)$. If $d \nmid b$, then the linear congruence has no solution in $\mathbb{Z}$. If $d \mid b$, then the linear congruence has exactly d incongruent solutions modulo m in $\mathbb{Z}$.

The proof can be broken into two parts:

(1) Showing that if $d \nmid b$, then the linear congruence has no solution. This can be proved using the contrapositive of the original statement (namely, if the linear congruence has solution, then $d \mid b$);

(2) Showing that if $d \mid b$, then the linear congruence has a solution, x_0. And given a solution x_0, we can construct infinitely many solutions of a given form and that among those infinitely many solutions, we have d incongruent solutions. More specifically, it suffices to show the following:

a. Show that a solution x_0 exists.
b. Given a solution x_0, show that $ax \equiv b \mod m$ has infinitely many solutions in $\mathbb{Z}$ of a given form.
c. Given a solution x_0, show that every solution has the form in (b).
d. Show that there are d incongruent solutions.

Proof. We begin the proof by proving Part (1) by its contrapositive.

Assume that $ax \equiv b \mod m$ has a solution. By definition of congruence, $m \mid ax - b$. By definition of divisibility, $m \mid ax - b$ iff there exists some $y \in \mathbb{Z}$ such that $my = ax - b$. This, in turn, is true iff $ax - my = b$ has a solution. Since d is the gcd of a and m, $d \mid a$ and $d \mid m$. By Proposition 2.2, it follows that $d \mid ax - my$. Since $b = ax - my$ iff $ax \equiv b \mod m$ has a solution, $d \mid b$ if the original linear congruence has a solution.

Now we proceed to prove Part (2)a. Assume $d \mid b$. Since d is the gcd of a and m, by Proposition 4.2, there exists $r, s \in \mathbb{Z}$ such that

$$d = ar + ms$$

■