

MATH406: Introduction to Number Theory

Michael Li

Contents

1	Basics	2
2	Divisibility	2
2.1	Divisibility	2
2.2	Euclid's Theorem	2
2.3	The Sieve of Eratosthenes	3
2.4	The Division Algorithm	3
2.5	The Greatest Common Divisor	3
2.6	The Euclidean Algorithm	4
2.6.1	The Extended Euclidean Algorithm	4
2.7	Other Bases	6
2.8	Fermat and Mersenne Numbers	6
3	Linear Diophantine Equation	7
4	Unique Factorization	8
5	Applications of Unique Factorization	10
5.1	A Puzzle	10
5.2	Irrationality Proof	10
5.3	Rational Root Theorem	11
5.4	Pythagorean Triples	11
5.5	Difference of Squares	12
5.6	Prime Factorization of Factorials	12
5.7	Riemann Zeta Function	13
6	Congruences	14
6.1	Definitions and Examples	14
6.2	Divisibility Tests	15
6.3	Linear Congruences	17
6.4	Chinese Remainder Theorem	18
6.5	Fractions mod m	19

Notes are based off of *An Introduction to Number Theory with Cryptography* (Second edition), by Washington and Kraft

1 Basics

Well-Ordering Principle: All non-empty subsets of N has a smallest member

- **Note:** This is equivalent to the Principle of Induction

2 Divisibility

2.1 Divisibility

Definition 2.1: Given $a, d \in Z$, for $d \neq 0$, d **divides** a if $\exists c \in Z$ such that $a = cd$

Proposition 2.2: Let $a, b, c \in Z$. If $a \mid b$ and $b \mid c \implies a \mid c$

Proof: $b = ea$ and $c = fb \implies c = (fe)a$

Proposition 2.3: Let $a, b, d, x, y \in Z$. If $d \mid a$ and $d \mid b \implies d \mid ax + by$

Proof: $a = md$ and $b = nd \implies ax + by = d(mx + ny)$

Upshot: Every common divisor of both a, b divides any linear combination of a, b

Corollary 2.4: Let $a, b, d \in Z$. If $d \mid a$ and $d \mid b$, then $d \mid a + b$ and $d \mid a - b$

Proof: Apply Proposition 2.3 using $x = 1, y = 1$, and $x = 1, y = -1$, respectively

Lemma 2.5: Let $d, n \in N$ and $d \mid n$. Then $d \leq n$

Proof: Since $d \mid n$, we have $k \in Z$ such that $dk = n$

Since $d \in N$, we also must have $k \in N$ (otherwise $n \notin N$)

Thus $n = dk \geq d * 1$

2.2 Euclid's Theorem

Prime: Integer $p \geq 2$ whose divisors are $1, p$

Composite: Integer $n \geq 2$ not prime such that $n = ab$ for $a, b \in Z$ and $1 < a, b < p$

Lemma 2.6: Every integer greater than 1 is prime or divisible by a prime

Proof 1: If n is NOT prime, then it is divisible by some $a_1 \in Z$ where $1 < a_1 < n$

If a_1 is prime, we are done

Otherwise a_1 is divisible by some $a_2 \in Z$ where $1 < a_2 < a_1 \implies a_2 \mid n$

This creates a decreasing sequence of positive integers, which by the Well Ordering Principle, must have a smallest element a_m

So either some a_i is prime and divides n or we stop at a_m , which is prime. Thus n is divisible by a prime

Proof 2 by Induction: Let $n \in Z, n \geq 2$, and suppose n is composite. Thus $n = kl$ for $k, l \in Z$ where $1 < k, l < n$

Base case: we only care about the first composite n , i.e. $n = 4 = 2 \cdot 2$ thus $2 \mid 4$ and 2 is prime

IH: Suppose the Lemma holds for all $i \in N, i < n$

IS: $n = kl$ where $k < n$. Thus k is either a prime or is divisible by a prime

- If k is prime, we are done since $k \mid n$
- Otherwise $p \mid k$ for some prime $p < k$. Then we have $p \mid k \wedge k \mid n \implies p \mid n$

Euclid's Theorem: there are an infinite number of primes

Proof: Assume by contradiction that there are a finite number of primes $2, 3, 5, \dots, p_n$

Let $N = (2 * 3 * 5 * \dots * p_n) + 1$

Since $N > 2p_n + 1 > p_n$, it is composite and thus is divisible by some p_i in the list of primes

Then we have $p_i \mid 2 * 3 * 5 * \dots * p_n$ and $p_i \mid N \implies p_i \mid N - (2 * 3 * 5 * \dots * p_n) \implies p_i \mid 1$ contradiction since $p_i > 1$

Thus there are an infinite number of primes

2.3 The Sieve of Eratosthenes

Proposition 2.7: If n is composite then n has a prime factor $p \leq \sqrt{n}$

Proof: $n = ab$ where $1 < a \leq b < n \implies a^2 \leq ab = n \implies a \leq \sqrt{n}$

By Lemma 2.6, a has a prime divisor p , where $p \mid a \implies p \leq a \leq \sqrt{n}$

- **Note:** Not all prime factors of n are $\leq \sqrt{n}$. For example, $6 = 2 * 3$ but $3 > \sqrt{6}$

2.4 The Division Algorithm

Division Algorithm: Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exists unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ with $0 \leq r < b$

Proof: Let $S = \{n \in \mathbb{Z} \mid bn \leq a\}$. Clearly S is non-empty since

- If $a \geq 0$, take $n = -1$
- If $a < 0$, take $n = a$

Since S is bounded above by a/b , it has a largest member, call it q

Thus q is the largest integers $\leq a/b$ such that $q \leq a/b < q + 1$

Then we have $bq \leq a < bq + b \implies 0 \leq a - bq < b$

Setting $r = a - bq$ we see that $0 \leq r < b$ and we have $a = bq + r$ so EXISTENCE is done

To show UNIQUENESS let $a = bq + r = bq_1 + r_1$ for $0 \leq r, r_1 < b$

Then we have $b(q - q_1) = r_1 - r$. Since LHS is a multiple of b , RHS is also a multiple of b

But $0 \leq r, r_1 < b \implies -b < r_1 - r < b \implies r_1 - r = 0$ since $b = 0$ is the only multiple of b that satisfies this inequality

Thus $r_1 = r$ and since $b \neq 0 \implies b(q - q_1) = 0 \implies q = q_1$. So q, r are UNIQUE

2.5 The Greatest Common Divisor

Relative Prime: a, b are relatively prime if $\gcd(a, b) = 1$

- By definition, we have $\gcd(a, 0) = a$

Proposition 2.10: Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. Then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$

Proof: Let $c = \gcd(a/d, b/d)$. Then $c \mid (a/d)$ and $c \mid (b/d)$

Thus $a = cdk_1$ and $b = cdk_2$ so cd is a common divisor of a, b

Since d is the greatest common divisor of a, b , we have $d \leq cd \leq d \implies c = 1$

Proposition 2.11: If $a, b \in \mathbb{Z}$, not both 0, and $e \in \mathbb{Z}^+$. Then $\gcd(ea, eb) = e * \gcd(a, b)$

Proof: Let $d = \gcd(ea, eb)$, we show that $d = e * \gcd(a, b)$

$\gcd(a, b) = ax + by \implies e \gcd(a, b) = eax + eby$. If d is a common divisor of ea and eb , then $d \mid e * \gcd(a, b)$

Thus $d \leq e \gcd(a, b)$. But since $e \gcd(a, b)$ is a common divisor of ea, eb , it is the gcd we desire

Various ways to find $\gcd(a, b)$:

1. List all prime factors of a, b and take the largest factor.

Example: $84 = 2 * 2 * 3 * 7$ and $264 = 2 * 2 * 2 * 3 * 11 \implies \gcd(84, 264) = 2 * 2 * 3 = 12$

2. Take Linear Combination of a, b and find a list of possible factors

Example: $d = \gcd(1005, 500) \implies d \mid (1005 - 2 * 500) \implies d = 1$ or $d = 5$. Clearly $d = 5$

Example: $d = \gcd(2n+3, 3n-7) \implies d \mid 3(2n+3) - 2(3n-6) = 21$ so $d \in \{1, 3, 7, 21\}$. Clearly with $n = 9$, $\gcd(21, 21) = 21$

3. Use Euclidean Algorithm

2.6 The Euclidean Algorithm

Euclidean Algorithm: Let $a, b \in \mathbb{Z}$ with $a \geq 0, b > 0$. Then we have

$$\begin{aligned} a &= q_1 b + r_1 & 0 < r_1 < b \\ b &= q_2 r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 & 0 < r_3 < r_2 \\ &\dots \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} &= q_n r_{n-1} + 0 \end{aligned}$$

Where $r_{n-1} = \gcd(a, b)$

Proof: $r_{n-1} \mid r_{n-2}, r_{n-1} \mid r_{n-3}, \dots, r_{n-1} \mid b, r_{n-1} \mid a$ so clearly r_{n-1} is a common factor of a, b

To show that r_{n-1} is the largest common factor, let d be an arbitrary common divisor of a, b

From the first line, we see that $d \mid r_1$. From the second line, $d \mid r_2$. This continues until $d \mid r_{n-1}$

Thus $d \leq r_{n-1}$ which means that r_{n-1} is the largest divisor and $\gcd(a, b) = r_{n-1}$

NOTE: each common divisor of a, b also divides $\gcd(a, b)$

2.6.1 The Extended Euclidean Algorithm

Extended Euclidean Algorithm: $\gcd(a, b)$ can be expressed as a linear combination of a, b .

Example: $\gcd(456, 123)$

$$\begin{aligned} 456 &= 3 * 123 + 87 \\ 123 &= 1 * 87 + 36 \\ 87 &= 2 * 36 + 15 \\ 36 &= 2 * 15 + 6 \\ 15 &= 2 * 6 + 3 \\ 6 &= 2 * 3 \end{aligned}$$

Using the values above, we can create a table

	x	y	
456	1	0	
123	0	1	
87	1	-3	$R_1 - 3R_2$
36	-1	4	$R_2 - R_3$
15	3	-11	$R_3 - 2R_4$
6	-7	26	$R_4 - 2R_5$
3	17	-63	$R_5 - 2R_6$

Thus $3 = 456 * 17 - 123 * 63$

Theorem 2.12 (Bezout's Theorem): Let $a, b \in Z$ with at least one non-zero. Then there exists $x, y \in Z$ such that $\gcd(a, b) = ax + by$

Proof: Let S be a set of integers that can be written in the form $ax + by$ for $x, y \in Z$

Since $a, b, -a, -b \in S$, clearly S contains at least one positive integer.

Using the Well-Ordering Principle, let d be the smallest positive integer in S . Thus $d = ax_0 + by_0$ for $x_0, y_0 \in Z$

We show that d is a common divisor of a, b

$$a = dq + r \implies r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0q) + b(-y_0q)$$

Thus $r \in S$. But since d is the smallest positive element of S and $0 \leq r < d$, we must have $r = 0$

Thus $d \mid a$. Similarly, $d \mid b$. Thus d is a common divisor of a, b

Next we show that for any common divisor of a, b , call it e , we have $e \leq d$

$e \mid a$ and $e \mid b \implies e \mid ax_0 + by_0 = d$. Thus $e \leq d$

Theorem 2.13: Let $n \geq 2$ and $a_1, \dots, a_n \in Z$ with at least one nonzero a_i . Then $\exists x_1, \dots, x_n \in Z$ such that

$$\gcd(a_1, \dots, a_n) = a_1x_1 + \dots + a_nx_n$$

Proof by Induction: By Theorem 2.12, the statement holds for $n = 2$

IH: assume the statement holds for $n = k$. $\gcd(a_1, \dots, a_k) = a_1x_1 + \dots + a_kx_k$

IS: Note that $\gcd(a_1, \dots, a_{k+1}) = \gcd(\gcd(a_1, \dots, a_k), a_{k+1})$

Apply Theorem 2.12 to $a_1x_1 + \dots + a_kx_k$ and a_{k+1} so $\gcd(a_1, \dots, a_{k+1}) = (a_1x_1 + \dots + a_kx_k)y + a_{k+1}x$

But then this satisfies the statement since if we set $y_i = yx_i$ for $1 \leq i \leq k$ and $y_{k+1} = x$

Thus by Induction, $\gcd(a_1, \dots, a_n) = a_1x_1 + \dots + a_nx_n$

Corollary 2.14: If e is a common divisor of a, b then $e \mid \gcd(a, b)$

Proof: $e \mid a$ and $e \mid b \implies e$ divides any linear combination of $a, b \implies e \mid \gcd(a, b) = ax + by$

Proposition 2.15: Let $a, b, c \in Z$ with $\gcd(a, c) = \gcd(b, c) = 1$. Then $\gcd(ab, c) = 1$

Proof: $\gcd(a, c) = 1 \implies ax_1 + cy_1 = 1$

$\gcd(b, c) = 1 \implies bx_2 + cy_2 = 1$

Multiplying these 2 equations we get $1 = (ab)(x_1x_2) + (c)(by_1x_2 + ax_1y_2 + cy_1y_2)$

Thus by Proposition 2.3, any common divisor of ab and c must divide $1 \implies \gcd(ab, c) = 1$

Proposition 2.16: Let $a, b, c \in Z$ with $a \neq 0$ and $\gcd(a, b) = 1$. Then $a \mid bc \implies a \mid c$

Proof: By Theorem 2.12, $1 = ax + by \implies c = acx + bcy$

Thus by Proposition 2.3, $a \mid a$ and $a \mid bc \implies a \mid acx + bcy = c$

Proposition 2.17: Let $a, b, c \in Z$ with a, b nonzero and $\gcd(a, b) = 1$. Then if $a \mid c$ and $b \mid c \implies ab \mid c$

Proof: By Theorem 2.12, $1 = ax + by \implies c = acx + bcy$

$b \mid c \implies ab \mid ac$

$$a \mid c \implies ba \mid bc$$

Since c is a linear combination of ac and bc , by Proposition 2.3, we must have that $ab \mid c$

2.7 Other Bases

We can convert a number from base 10 to any other base using the Division Algorithm

Example: Convert 21963_{10} to base 8

$$21963 = 2745 * 8 + 3$$

$$2745 = 343 * 8 + 1$$

$$343 = 42 * 8 + 7$$

$$42 = 5 * 8 + 2$$

$$5 = 0 * 8 + 5$$

Thus $21963_{10} = 52713_8$ This is because

$$5 * 8^4 + 2 * 8^3 + 7 * 8^2 + 1 * 8 + 3 = 52713_8$$

Note: decimal representations in other bases are NOT unique. For $a_k \leq n - 1$

$$\sum_{k=1}^{\infty} \frac{a_k}{n^k} \leq \sum_{k=1}^{\infty} \frac{n-1}{n^k}, \text{ which is the geometric series and converges}$$

Thus any sequence $\{a_n\}_{n=1}^{\infty}$ for $0 \leq a_k \leq n - 1$ converges

$$\text{In particular, for } j > 1, \sum_{k=j}^{\infty} \frac{n-1}{n^k} = \frac{1}{n^{j-1}}$$

- **Example:** for $n = 10$, we have $1 = 0.\bar{9}$
- **Example:** $0.01_7 = 0.000\bar{6}_7$

2.8 Fermat and Mersenne Numbers

Mersenne Numbers: $M_n = 2^n - 1$ for prime n . Thought to generate prime numbers, but doesn't always work (e.g. $n = 11$ results in a composite number)

Proposition 2.18: If n is composite, then $2^n - 1$ is composite

Proof: Recall that $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \dots + x + 1)$

Since n is composite, $n = ab$. Let $x = 2^a$ and $k = b$

$$\text{Then } 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + \dots + 2^a + 1)$$

$$1 < a < n \implies 1 < 2^a - 1 < 2^n - 1 \text{ so } 2^a - 1 \text{ is a nontrivial factor and } 2^n - 1 \text{ is composite}$$

Corollary 2.18.1: For $k, n \in \mathbb{N}$, $k \mid n \implies M_k \mid M_n$

Proof: Can be seen from the factorization seen in the previous proposition

Corollary 2.18.2: If M_n is prime, then n is prime

Proof: Follows from the contraposition of Proposition 2.18

Fermat Numbers: $F_n = 2^{2^n} + 1$. Thought to generate prime numbers, but doesn't always work (e.g. $n = 5$ results in a composite number)

Proposition 2.19: If $m > 1$ is not a power of 2 then $2^m + 1$ is composite

Proof: Recall that k is odd then $x^k + 1 = (x + 1)(x^{k-1} - x^{k-2} + x^{k-3} - \dots - x + 1)$

Since m is not a power of 2 it has a nontrivial odd factor $a \geq 3$, so $m = ab$. Let $k = a$ and $x = 2^b$

Then $2^{ab} + 1 = (2^b + 1)(2^{b(a-1)} - 2^{b(a-2)} + \dots - 2^b + 1)$

$1 \leq b < m \implies 1 < 2^b + 1 < 2^m + 1$ so $2^b + 1$ is a nontrivial factor and $2^m + 1$ is composite

Proposition 2.20: A regular n -gon is constructable if and only if $n = 2^a F_{n_1} F_{n_2} \dots F_{n_r}$ for distinct Fermat Primes and $a \geq 0$

3 Linear Diophantine Equation

We look for solutions to $ax + by = c$ for $a, b, c \in \mathbb{Z}$

- If $\gcd(a, b) \nmid c$ then there are NO integer solutions (x, y) . This follows from $\gcd(a, b)$ divides any linear combination of a, b

Theorem 3.1: Let $a, b, c \in \mathbb{Z}$ where a, b are not both 0. Then $ax + by = c$ has a solution if and only if $\gcd(a, b) \mid c$

Furthermore, if it has one solution (x_0, y_0) , then there are an infinite number of solutions of the form

$$x = x_0 + \frac{b}{\gcd(a, b)}t \quad y = y_0 - \frac{a}{\gcd(a, b)}t \quad t \in \mathbb{Z}$$

Proof: Let $d = \gcd(a, b)$

\implies Contraposition: If $d \nmid c$ then clearly no solutions

\Leftarrow If $d \mid c$ then by Theorem 2.12, there exists $r, s \in \mathbb{Z}$ such that $ar + bs = d$

$d \mid c \implies df = c$ for $f \in \mathbb{Z} \implies a(rf) + b(sf) = df = c$

Thus $x_0 = rf$ and $y_0 = sf$ is a solution to $ax + by = c$

To show there are an infinite number of solutions, first let $x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$

Then $ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 = c$

Thus there are an infinite number of solutions of this form

To show that every solution has the correct form, fix solutions x_0, y_0 and let u, v be any solution

$au + bv = c = ax_0 + by_0 \implies a(u - x_0) - b(v - y_0) = 0 \implies \frac{a}{d}(u - x_0) = \frac{b}{d}(y_0 - v)$

- The last part follows because $d \mid a$ and $d \mid b \implies \frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$

Thus we have $(a/d) \mid (b/d)(y_0 - v)$

Since, by Proposition 2.10, $\gcd(a/d, b/d) = 1$, we have by Proposition 2.6, $(a/d) \mid (y_0 - v)$

Thus $y_0 - v = \frac{a}{d}t \implies v = y_0 - t\frac{a}{d}$

Furthermore, $\frac{a}{d}(u - x_0) = \frac{b}{d}(\frac{a}{d}t) \implies u = x_0 + \frac{b}{d}t$

Corollary 3.2: Let $a, b, c \in \mathbb{Z}$ with at least one a, b nonzero. If $\gcd(a, b) = 1$ then $ax + by = c$ has infinite number of solutions

Upshot: If (x_0, y_0) is a particular solution, then all solutions are of the form

$$x = x_0 + bt \quad y = y_0 - at \quad t \in \mathbb{Z}$$

General Steps to Solve Linear Diophantine Equation:

1. Verify $\gcd(a, b) \mid c$
 - If no, then there is no solution
 - If yes, divide the equation by d to get $a'x + b'y = c'$ where $\gcd(a', b') = 1$
2. Then use Extended Euclidean Algorithm to solve for $a'x + b'y = 1$, then multiply the solution by the value of c'
3. If one of the solution variable (e.g. x) is negative, we can perform Extended Euclidean Algorithm with a positive x then flip the sign of x at the end
4. General solutions will be $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$
 - **Example:** $-17x + 14y = 30 \implies 17x + 14y = 30$ has the solution $(5 * 30, -6 * 30)$ so the desired solution is $(-150, -180)$ and general solution is of the form

$$x = -150 + 14t \quad y = -180 + 17t \quad t \in \mathbb{Z}$$

Proposition 3.3: Let $a, b \in \mathbb{Z}^+$ and relatively prime. Then there are no non-negative $x, y \in \mathbb{Z}$ such that $ax + by = ab - a - b$

Proof: Observe that $a(-1) + b(a-1) = ab - a - b \implies x = -1$ and $y = a-1$ is a solution

Since $\gcd(a, b) = 1$ every solution has the form $x = -1 + bt$ and $y = a-1 - at = a(1-t) - 1$

Note that $x \geq 0$ if and only if $t > 0$ but then we have $1-t \leq 0 \implies y \leq -1$

Thus it is impossible to find a non-negative solution to $ax + by = ab - a - b$

Proposition 3.4: Let $a, b \in \mathbb{Z}^+$ and relatively prime. If $n > ab - a - b$ then there exists non-negative $x, y \in \mathbb{Z}$ such that $ax + by = n$

Proof: First find a pair (x_0, y_0) such that $ax_0 + by_0 = n \geq ab - a - b + 1$. Note (x_0, y_0) may be negative

Solution has the form $x = x_0 + bt$ and $y = y_0 - at$

We find the smallest possible $y \geq 0$ then show that $x \geq 0$

From Division Algorithm and dividing y_0 by a , we have $y_0 = at + y_1$ for $0 \leq y_1 < a$. Let y_1 be our choice of y

Since $y_1 = y_0 - at$, we take $x_1 = x_0 + bt$ as our choice of x . First note that these are a valid solution

$$ax_1 + by_1 = a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = n$$

Now we show that $x_1 \geq 0$

Suppose by contradiction that $x_1 \leq -1$, then we have

$$n = ax_1 + by_1 \leq a + by_1 \leq -a + b \underbrace{(a-1)}_{0 \leq y_1 < a}$$

Thus $n = ab - a - b$. Contradiction since we said $n > ab - a - b$

Thus (x_1, y_1) is a non-negative solution

4 Unique Factorization

Theorem 4.1: Let p be prime and $a, b \in \mathbb{Z}$ such that $p \mid ab$. Then $p \mid a$ or $p \mid b$

Proof: Let $d = \gcd(a, p)$. If $d = p$ then $d \mid a \implies p \mid a$

Otherwise applying Extended Euclidean Algorithm, $d = 1 = ax + py \implies b = abx + pby$

$p \mid ab$ and $p \mid p \implies p \mid b$, which is a linear combination of p and ab

- **NOTE:** if n is composite, then we CANNOT conclude $n \mid a$ or $n \mid b$ from $n \mid ab$

Corollary 4.2: Let p be prime and $a_1, a_2, \dots, a_r \in \mathbb{Z}$ such that $p \mid a_1 \cdot a_2 \cdots a_r$. Then $p \mid a_i$ for some i

Proof by Induction: clearly statement holds for $r = 1$

IH: assume statement holds for $r = k$

IS: show statement is true for $r = k + 1$. Let $a = a_1 \cdots a_k$ and $b = a_{k+1}$

We can apply Theorem 4.1 where $p \mid ab \implies$ statement holds for any $r \geq 1$

Lemma 4.3: Every integer can be written as a product of primes

Proof: Assume there exist composite integers that cannot be written as product of primes. Let S be the set of these ints > 1

Since all $e \in S$ are positive, by Well Ordering Principle, it has a smallest element s

Since s is composite, we have $s = ab$, but $a, b < s \implies a, b \notin S \implies a, b$ can be written as the product of primes

Thus s is also a product of primes and thus S is empty

Fundamental Theorem of Arithmetic: Any positive integer > 1 is either prime or can be factored exactly one way as a product of primes

Proof: Lemma 4.3 shows that any integer > 1 can be written as a product of primes

For uniqueness, suppose that there are 2 ways of factoring an integer. Let n be the smallest of these integers

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

$$p_1 \mid \text{LHS} \implies p_1 \mid \text{RHS} \implies p_1 \mid q_i$$

Rearranging the RHS, we let $p_1 = q_1$ and now we have $n/p_1 = m = p_2 \cdots p_r = q_2 \cdots q_s$

But $m < n$ so it must have a unique factorization but we see that m can be written using 2 different factorization

Thus we have a contradiction and every positive integer > 1 can be unique factored

Proposition 4.4: Let $a, b \in \mathbb{Z}^+$ where $a = 2^{a_2} 3^{a_3} \cdots$ and $b = 2^{b_2} 3^{b_3} \cdots$. Then $a \mid b \iff a_p \leq b_p$ for all p

Proof: $\implies a \mid b \implies ac = b$ where $c = 2^{c_2} 3^{c_3} \cdots$

Then $2^{a_2+c_2} 3^{a_3+c_3} \cdots = b$

Thus we must have $\forall p, a_p + c_p = b_p \implies a_p \leq b_p$

\Leftarrow suppose $\forall p, a_p \leq b_p$ and let $c_p = b_p - a_p$. Clearly $c_p \geq 0$

Let $c = 2^{c_2} 3^{c_3} \cdots \implies ac = b \implies a \mid b$

Definition - Least Common Multiple: $\text{lcm}(a, b)$ is the smallest positive integer divisible by a, b

Proposition 4.5: Let $a, b \in \mathbb{Z}^+$ where $a = 2^{a_2} 3^{a_3} \cdots$ and $b = 2^{b_2} 3^{b_3} \cdots$. Furthermore, for all p , let $d_p = \min(a_p, b_p)$ and $e_p = \max(a_p, b_p)$. Then $\text{gcd}(a, b) = 2^{d_2} 3^{d_3} \cdots$ and $\text{lcm}(a, b) = 2^{e_2} 3^{e_3} \cdots$

Proof: Let d be any common divisor of a, b such that $d = 2^{d_2} 3^{d_3} \cdots$

$d \mid a \implies d_p \leq a_p$ for all p . Similarly $d \mid b \implies d_p \leq b_p$ for all p

Largest common divisor occurs when $d_p = \min(a_p, b_p)$ for each p

Least common multiple occurs when $e_p = \max(a_p, b_p)$ for each p

Definition - Squarefree: integer whose factors are all distinct (doesn't have a square of a number as a factor)

Proposition 4.7: Let $n \in \mathbb{Z}^+$. Then there exists $r \in \mathbb{Z}, r \geq 1$ and a squarefree integer $s \geq 1$ such that $n = r^2 s$

Proof: Let $n = p_1^{a_1} p_2^{a_2} \dots$.

If a_i is even, write it as $a_i = 2b_i$. Otherwise write $a_i = 2b_i + 1$

Let $r = p_1^{a_1} p_2^{a_2} \dots$ and let $s =$ the product of all primes p_i with odd a_i

Then we have $r^2 s = n$

5 Applications of Unique Factorization

5.1 A Puzzle

Proposition 5.1: Let $k \geq 2$ be an integer and $m \in \mathbb{Z}^+$. Then m is a k th power \iff all exponents in the prime factorization of m are multiples of k

Proof: \Leftarrow Let $m = 2^{y_2} 3^{y_3} \dots$. If each y_p is a multiple of k then $y_p = k z_p \implies m = (2^{z_2} 3^{z_3} \dots)^k$

\implies If $m = n^k$ where $n = 2^{w_2} 3^{w_3} \dots$, then $2^{y_2} 3^{y_3} \dots = m = n^k = 2^{kw_2} 3^{kw_3} \dots$

By Uniqueness of Factorization, $y_p = kw_p$ for each $p \implies$ each exponent for m is a multiple of k

Example: Find a number A such that $2/3 * A^2$ is a cube

Let $A = 2^a 3^b 5^c \dots$ be the prime factorization of A

We have $2/3 * A^2 = 2^{2a+1} 3^{2b-1} 5^{2c} \dots$ is a cube, so $2a+1, 2b-1, 2c, \dots$ are all multiples of 3

By brute force, we see that $a=1, b=2, c=d=\dots=0$ works and gives us $A=18$

To find the general solution, we note that $3 \mid 2c$ and $\gcd(3, 2) = 1$ so c must be a multiple of 3 $\implies c = 3c'$. Similar for d, e, \dots

Since $2a+1$ is odd and a multiple of 3, we have $2a+1 = 3(2j+1) \implies a = 3j+1$

Since $2b-1$ is odd and a multiple of 3, we have $2b-1 = 3(2k+1) \implies b = 3k+2$

Finally, we see that $A = 2^a 3^b 5^c \dots = 2 * 3^2 (2^j 3^k 5^{c'} \dots)^3 = 18B^3$ for any $B \geq 1$

5.2 Irrationality Proof

Rational: Number that can be expressed as a ratio of 2 integers

Theorem 5.2: $\sqrt{2}$ is irrational

Proof: Suppose by contradiction that $\sqrt{2}$ is rational and $\sqrt{2} = a/b \in \mathbb{Q}$ in reduced form

Then we have $2 = a^2/b^2 \implies 2b^2 = a^2$

Clearly a^2 is even $\implies a$ is even so $a = 2a_1$

But then we have $b^2 = 2a_1$ so b^2 is even $\implies b$ is even. This is a contradiction since we said a/b is in reduced form

Thus we have a contradiction and $\sqrt{2}$ is irrational

Theorem 5.3: Let $k \in \mathbb{Z}$ and $k \geq 2$. Let $n \in \mathbb{Z}^+$ that is not a perfect k th power. Then $\sqrt[k]{n}$ is irrational

Proof: We show the contrapositive that if $\sqrt[k]{n}$ is rational then n is a perfect k th power

Suppose $\sqrt[k]{n} = a/b \implies nb^k = a^k$

We can prime factorize n, b to get $n = 2^{x_2} 3^{x_3} \dots$ and $b = 2^{z_2} 3^{z_3} \dots$

Thus we have $nb^k = 2^{x_2+kz_2} 3^{x_3+kz_3} \dots$

Let $a = 2^{y_2} 3^{y_3} \dots$. Since a^k is a perfect power, by Proposition 5.1, every exponent in the prime factorization is a multiple of k

Thus $x_p + kz_p = ky_p \implies x_p = k(y_p - z_p) \implies n$ is a perfect k th power

5.3 Rational Root Theorem

Theorem 5.4 (Rational Root Theorem): let $P(X) = a_nX^n + \dots + a_1X + a_0$ where $a_i \in Z$ such that $a_n \neq 0$ and $a_0 \neq 0$

If $r = u/v \in Q$ with $\gcd(u, v) = 1$ and $P(u/v) = 0$ then $u \mid a_0$ and $v \mid a_n$

Proof: $P(u/v) = 0 \implies a_n(u/v)^n + \dots + a_0 = 0 \implies a_nu^n + \dots + a_0v^n = 0$

$a_{n-1}vu^{n-1} + \dots + a_0v^n = -a_nu^n \implies v \mid a_nu^n$. But $\gcd(u, v) = 1 \implies v \mid a_n$

$a_nu^n + \dots + a_1v^{n-1}u = -a_0v^n \implies u \mid a_0v^n$. But $\gcd(u, v) = 1 \implies u \mid a_0$

5.4 Pythagorean Triples

Pythagorean Triples: positive integers (a, b, c) where $a^2 + b^2 = c^2$

Primitive Pythagorean Triples: Pythagorean triples where $\gcd(a, b, c) = 1$

Example: A primitive way of generating Pythagorean Triples is using odd numbers

$$(2n+1)^2 = 4n^2 + 4n + 1 = (2n^2 + 2n) + (2n^2 + 2n + 1) \implies (2n+1)^2 + (2n^2 + 2n)^2 = (2n^2 + 2n + 1)^2$$

Lemma 5.6: Let $k \in Z, k \geq 2$ and let a, b relatively prime integers such that $ab = n^k$. Then a, b are each k th powers of integers

Proof: Let $n = 2^{x_2}3^{x_3} \dots$. Then $ab = n^k = 2^{kx_2}3^{kx_3} \dots$

Let p be a prime in the prime factorization of a and p^c be the exact power of p in the factorization of a

Since $\gcd(a, b) = 1$, p doesn't occur in the factorization of b , so p^c occurs in ab and n^k has p^{kx_p} as the power of p

Since prime factorization is unique, we have $c = kx_p \implies$ every prime in factorization of a occurs with a power of a multiple of k

Thus a is a k th power integer. Similar for b

Lemma 5.7: The square of an odd integer is 1 more than a multiple of 8. The square of an even integer is a multiple of 4

Proof: Let n be even then $n = 2k \implies n^2 = 4k^2 \implies 4 \mid n^2$

Let n be odd $\implies n = 2k+1 \implies n^2 = 4k(k+1) + 1$

Since k or $k+1$ is even, we have $4k(k+1)$ is a multiple of 8. Thus n^2 is 1 more than a multiple of 8

Theorem 5.5: Let (a, b, c) be a Primitive Pythagorean triple. Then c is odd and exactly one of a, b is even and the other is odd. Assume b is even, then there are relatively prime integers m, n such that $m < n$ and one odd and the other even such that

$$a = n^2 - m^2 \quad b = 2mn \quad c = m^2 + n^2$$

Proof: Let $a^2 + b^2 = c^2$ and $\gcd(a, b, c) = 1$

Suppose by contradiction that both a, b are odd, then by Lemma 5.7, $a^2 + b^2$ is 2 more than a multiple of 8

Thus $a^2 + b^2$ is not a multiple of 4 so by Lemma 5.7, $a^2 + b^2$ cannot be a square. Thus at least one of a, b is even

Suppose by contradiction that both a, b are even. Then $c^2 = a^2 + b^2$ is even so c is even.

But then 2 is common divisor of a, b, c but we have $\gcd(a, b, c) = 1$. Contradiction

Thus one of a, b is even and the other is odd. WLOG let a be odd and b be even

Then we have $a^2 + b^2 = c^2$ is odd.

Let $b = 2b_1$ so we have $c^2 - a^2 = (c+a)(c-a) = b^2 = 4b_1^2$

Thus we have $(\frac{c+a}{2})(\frac{c-a}{2}) = b_1^2$. Since c, a are odd we must have $\frac{c+a}{2}$ and $\frac{c-a}{2} \in Z$

Let $d = \gcd((c+a)/2, (c-a)/2)$ and suppose by contradiction $d > 1$. Then let p be a prime dividing d

Then $c = \frac{c+a}{2} + \frac{c-a}{2}$ and $a = \frac{c+a}{2} - \frac{c-a}{2}$ are multiples of p

Thus $c^2 - a^2 = b^2$ is a multiple of $p \implies p \mid b$ so p is a common divisor of a, b, c , contradicting that $\gcd(a, b, c) = 1$. Thus $d = 1$

Thus we have two relatively prime integers: $(c+a)/2$ and $(c-a)/2$ whose product is a square

By Lemma 5.6, each factor is a square so $\frac{c-a}{2} = m^2$ and $\frac{c+a}{2} = n^2$

Thus $c = \frac{c+a}{2} + \frac{c-a}{2} = n^2 + m^2$ and $a = \frac{c+a}{2} - \frac{c-a}{2} = n^2 - m^2$

Thus $b^2 = c^2 - a^2 = (n^2 + m^2)^2 - (n^2 - m^2)^2 = 4m^2n^2 \implies b = 2mn$

Since $(c-a)/2 = m^2$ and $(c+a)/2 = n^2$ are relatively prime, then $\gcd(n, m) = 1$

Finally since $m^2 + n^2 = c$ is odd, one of m, n is odd and the other is even

5.5 Difference of Squares

Theorem 5.8: Let $m \in \mathbb{Z}^+$. Then m is a difference of 2 squares \iff either m is odd or m is a multiple of 4

Proof: \Leftarrow Let m be odd then $m = 2n + 1 = (n+1)^2 - n^2$.

Otherwise let m be a multiple of 4 then $m = 4n = (n+1)^2 - (n-1)^2$

\implies Suppose $m = x^2 - y^2 = (x+y)(x-y)$. Since $x+y, x-y$ differ by $2y$ (even) they are either both even or both odd

- If they are both even, then $m = (x+y)(x-y)$ is the product of 2 even numbers and is thus a multiple of 4
- If both are odd, then m is clearly odd

As an aside, suppose $m = uv$ where u, v have the same parity and $u \geq v$

If we let $x = \frac{(u+v)}{2}$ and $y = \frac{(u-v)}{2}$ then clearly $x, y \in \mathbb{Z}$ since u, v have the same parity

And we have $x^2 - y^2 = \frac{(u+v)^2}{4} - \frac{(u-v)^2}{4} = uv = m$

Upshot: Writing m as a difference of 2 squares corresponds to factorizing m into 2 factors of the same parity

Example: $m = 15 \implies 15 * 1 = 8^2 - 7^2$ where $8 + 7 = 15$ and $8 - 7 = 1$

$m = 15 \implies 5 * 3 = 4^2 - 1^2$ where $4 + 1 = 5$ and $4 - 1 = 3$

Example: $m = 60 \implies 30 * 2 = 16^2 - 14^2$

$m = 60 \implies 10 * 6 = 8^2 - 2^2$

5.6 Prime Factorization of Factorials

Theorem 5.9: Let $n \geq 1$ and p be a prime. If we write $n! = p^b c$ with $p \nmid c$, then

$$b = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots$$

Proof: write $n = qp + r$ for $0 \leq r < p$. Clearly multiples of p up to n are $p, 2p, \dots, qp$

but we see that $\lfloor \frac{n}{p} \rfloor = \lfloor q + (r/p) \rfloor = q$ so there are $\lfloor \frac{n}{p} \rfloor$ multiples of p up to n

Similarly, there are $\lfloor \frac{n}{p^2} \rfloor$ multiples of p^2 up to n

Thus we can write $b = (\# \text{ of multiples of } p \text{ up to } n) + (\# \text{ of multiples of } p^2 \text{ up to } n) + \dots$

Take m such that $1 \leq m \leq n$ and $m = p^k m_1$ with $p \nmid m_1$.

Then m contributes p^k to $n!$ and contributes k to the exponent b since m is a multiple of p^j for $j \leq k$

Example: $n = 30, p = 5 \implies \lfloor \frac{30}{5} \rfloor + \lfloor \frac{30}{25} \rfloor = 6 + 1 \implies 5^7$ is the power of 5 in 30!

Example: $n = 30, p = 2 \implies \lfloor \frac{30}{2} \rfloor + \lfloor \frac{30}{4} \rfloor + \lfloor \frac{30}{8} \rfloor + \lfloor \frac{30}{16} \rfloor = 15 + 7 + 3 + 1 = 26 \implies 2^{26}$ is the power of 2 in 30!
Thus $2^{26}5^7 = 2^{19}10^7 \implies 30!$ has 7 zeros at the end

5.7 Riemann Zeta Function

Definition - Riemann Zeta Function: For a real number $s > 1$, we define the **Riemann zeta function** as

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

Theorem 5.10: If $s > 1$, then

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} \quad \text{for all primes } p$$

Proof:

Note that the geometric series $1 + r + r^2 + \dots = \frac{1}{1-r} = (1-r)^{-1}$ for $|r| < 1$

Letting $r = p^{-1}$, we get

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots = (1 - p^{-s})^{-1}$$

As an example, consider the product

$$\begin{aligned} (1 - 2^{-s})^{-1}(1 - 3^{-s})^{-1} &= (1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots)(1 + \frac{1}{3^s} + \frac{1}{9^s} + \dots) \\ &= (1 + \frac{1}{2^s} + \frac{1}{4^s} + \dots) + (\frac{1}{3^s} + \frac{1}{2^s 3^s} + \frac{1}{4^s 3^s} + \dots) + (\frac{1}{9^s} + \frac{1}{2^s 9^s} + \frac{1}{4^s 9^s} + \dots) \\ &= \sum_{n \in S(2,3)} \frac{1}{n^s} \quad S(p, q) \text{ are all integers whose prime factorizations only use } p, q \end{aligned}$$

Now consider using m primes

$$(1 - 2^{-s})^{-1}(1 - 3^{-s})^{-1} \dots (1 - p_m^{-s})^{-1} = \sum_{n \in S(2,3,\dots,p_m)} \frac{1}{n^s}$$

The LHS converges to the product over all primes. Since every positive integer has a prime factorization, each n lies in $S(2,3,\dots,p_m)$. Thus RHS converges to the sum over all positive integers n

Infinite Primes Proof: BWOC suppose there are only a finite number of primes. Then

$$\lim_{s \rightarrow 1^+} \prod_p (1 - p^{-s})^{-1} = \prod_p (1 - p^{-1})^{-1}$$

is a finite product and thus must itself be finite

Furthermore, since each of the functions used in the product is continuous at $s = 1$, we have that for $n > 1, x \geq n, s > 1$

$$x^s \geq n^s \implies \frac{1}{n^s} \geq \frac{1}{x^s} \implies \int_n^{n+1} \frac{1}{n^s} dx \geq \int_n^{n+1} \frac{1}{x^s} dx$$

Thus we have

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \geq \sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{x^s} dx = \int_1^{\infty} \frac{1}{x^s} dx = \frac{1}{s-1}$$

Thus $\zeta(s) \geq \frac{1}{s-1}$ diverges as $s \rightarrow 1^+$. Contradiction since we showed that $\prod_p (1 - p^{-s})^{-1}$ converges

Thus there are an infinite number of primes

6 Congruences

6.1 Definitions and Examples

Definition - Congruence: $a \equiv b \pmod{m}$ if $a - b$ is a multiple of m

Proposition 6.2: $a \equiv b \pmod{m} \iff a = b + km$ for some $k \in \mathbb{Z}$

Proof: $a \equiv b \pmod{m}$ if and only if $a - b$ is a multiple of m . Thus $a - b = km \implies a = b + km$

Looking at integers mod m , we get m **congruent classes**. Each integer is only in one congruent class mod m

Proposition 6.3: Let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$ then $\exists! r$, with $0 \leq r \leq m - 1$ such that $a \equiv r \pmod{m}$

Proof: By division algorithm, we have \exists unique q, r such that $a = mq + r$ with $0 \leq r \leq m - 1$

Thus from the previous proposition, $a \equiv r \pmod{m}$

Proposition 6.4: Let $a, b, c \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then

- $a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$
- $a \equiv c \pmod{m}$ and $b \equiv c \pmod{m} \implies a \equiv b \pmod{m}$

Proof:

- $a = a + 0 \cdot m \implies a \equiv a \pmod{m}$
- $a \equiv b \pmod{m} \implies a = b + km \implies b = a + (-k)m \implies b \equiv a \pmod{m}$
- $a - c = (a - b) + (b - c) = (k_1 + k_2)m \implies a \equiv c \pmod{m}$

Proposition 6.5: Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $ac \equiv bd \pmod{m}$

Proof: $a \equiv b \pmod{m} \implies a = b + k_1m$ and $c \equiv d \pmod{m} \implies c = d + k_2m$

- $a + c = (b + d) + (k_1 + k_2)m \implies a + c \equiv b + d \pmod{m}$
- $a - c = (b - d) + (k_1 - k_2)m \implies a - c \equiv b - d \pmod{m}$
- $ac = (b + k_1m)(d + k_2m) = bd + (bk_2 + dk_1 + k_1k_2m)m \implies ac \equiv bd \pmod{m}$

Corollary 6.6: $a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$ for $n \in \mathbb{Z}^+$

Proof: By the previous proposition, $a \equiv b \pmod{m} \implies a^2 \equiv b^2 \pmod{m}$. Repeated multiplication yields $a^n \equiv b^n \pmod{m}$

Proposition 6.7: $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1 \implies a \equiv b \pmod{m}$

$ac \equiv bc \pmod{m} \implies m \mid (ac - bc) \implies m \mid c(a - b)$

If c, m are relatively prime, then we must have $m \mid a - b \implies a \equiv b \pmod{m}$

Proposition 6.8: $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = d \implies a \equiv b \pmod{\frac{m}{d}}$ and $a = b + (\frac{m}{d})k$ with $0 \leq k \leq d - 1$

Proof: $ac \equiv bc \pmod{m} \implies m \mid c(a - b) \implies \frac{m}{d} \mid \frac{c}{d}(a - b)$

Since $\gcd(c, m) = d$, we must have $\gcd(\frac{m}{d}, \frac{c}{d}) = 1 \implies \frac{m}{d} \mid a - b \implies a \equiv b \pmod{\frac{m}{d}}$

Furthermore, $a - b = m(\frac{d}{k})$ where $\frac{d}{k} \in \mathbb{Z} \implies 0 \leq k \leq d - 1$

Various ways to solve equations of the form $ax \equiv b \pmod{m}$:

- Add m to b until we find an easy factor of a

Example: $2c \equiv 7 \pmod{9} \equiv 16 \pmod{9} \implies c = 8$

- Use Proposition 6.8 and divide a, b by a common factor c and m by $\gcd(c, m)$

Example: $6c \equiv 18 \pmod{21} \implies c \equiv 3 \pmod{7}$.

Note: Answer is in terms of mod 7

Proposition 6.9: Let $n \in \mathbb{Z}^+$ and $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n} \implies \gcd(a, n) = \gcd(b, n)$

Proof: $a \equiv b \pmod{n} \implies a = b + nk$. Let d be a divisor of b, n . Then $d \mid a$ since a is a linear combination of b, n

We also must have $b = a - nk \implies$ any common divisor of a, n is also a divisor of b

Thus the set of common divisors for a, n is the same as the set of common divisors of b, n . Thus $\gcd(a, n) = \gcd(b, n)$

Example: $\gcd(1234, 10) = \gcd(4, 10)$ since $1234 \equiv 4 \pmod{10}$

Proposition 6.10: If p is a prime and $ab \equiv 0 \pmod{p}$. Then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$

Proof: $ab \equiv 0 \pmod{p} \implies p \mid ab$. Thus by theorem, $p \mid a$ or $p \mid b \implies a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$, respectively

Corollary 6.11: Let p be a prime. Then $x^2 \equiv 1 \pmod{p}$ has only solutions $x \equiv \pm 1 \pmod{p}$

Proof: $x^2 \equiv 1 \pmod{p} \iff x^2 - 1 \equiv 0 \pmod{p} \iff (x - 1)(x + 1) \equiv 0 \pmod{p}$

By the previous Proposition, this only happens when $x - 1 \equiv 0 \pmod{p}$ or $x + 1 \equiv 0 \pmod{p}$

Thus the only possible solutions are $x \equiv \pm 1 \pmod{p}$

Exercise 6.34

6.2 Divisibility Tests

For $a \in \mathbb{N}$, we can express a in base 10 as

$$a = a_0 + 10^1 a_1 + \cdots + 10^k a_k \quad 0 \leq a_i \leq 9$$

Axiom: $2 \mid a$ if and only if $2 \mid a_0 \implies a \equiv a_0 \pmod{2}$

Proposition 6.12: $10 \mid a$ if and only if $a_0 = 0$ AND $5 \mid a$ if and only if $a_0 = 0$ or $a_0 = 5$

Proof:

Let $a = a_0 + 10a_1 + \cdots + 10^k a_k \quad 0 \leq a_i \leq 9$

- \implies Suppose $10 \mid a \implies 10 \mid a_0 \implies a_0 = 0$ since $0 \leq a_0 \leq 9$

\iff Suppose $a_0 = 0 \implies a = 10a_1 + \cdots + 10^k a_k \implies 10 \mid a$

- We prove that $a \equiv a_0 \pmod{5}$

$$a = a_0 + 10(a_1 + 10a_2 + \cdots + 10^{k-1} a_k) \implies a \equiv a_0 \pmod{5}$$

Thus it follows that $5 \mid a$ if and only if $a_0 \equiv 0 \pmod{5} \implies a_0 = 0$ or $a_0 = 5$

Corollary 6.12.1: $a \equiv a_0 \pmod{10}$

Proposition 6.13: $4 \mid a$ if and only if $4 \mid 10a_1 + a_0$ AND $8 \mid a$ if and only if $8 \mid 100a_2 + 10a_1 + a_0$

Proof:

- Note that $4 \mid 10^j$ for $j \geq 2$. Thus $a \equiv 10a_1 + a_0 \pmod{4} \implies 4 \mid a$ if and only if $4 \mid 10a_1 + a_0$
- Note that $8 \mid 10^j$ for $j \geq 3$. Thus $a \equiv 100a_2 + 10a_1 + a_0 \pmod{8} \implies 8 \mid a$ if and only if $8 \mid 100a_2 + 10a_1 + a_0$

Proposition 6.14: An integer mod 3 (respectively, mod 9) is congruent to the sum of its digits mod 3 (respectively, mod 9)

Proof: Clearly $10 \equiv 1 \pmod{3}$. Since $1^k = 1$ for all integers k , we have

$$10^k \equiv 1^k \equiv 1 \pmod{3}$$

Thus when we look at n expanded in its base 10 form mod 3, we get

$$n = a_m 10^m + \cdots + a_1 10 + a_0 \equiv a_m + \cdots + a_1 + a_0 \pmod{3}$$

Identical for mod 9

Corollary 6.15: An integer n is divisible by 3 if and only if the sum of its digits are divisible by 3. It is divisible by 9 if and only if the sum of its digits is divisible by 9

Example: $8675309 \equiv 38 \pmod{9} \equiv 11 \pmod{9} \equiv 2 \pmod{9}$

Proposition 6.15.1: $6 \mid a$ if and only if $2 \mid a$ and $3 \mid a$

Proof: \implies Suppose $6 \mid a$. Then any factor of 6 also divides a

\Leftarrow Suppose $2 \mid a$ and $3 \mid a$. Then by the unique prime factorization of a , we know that $6 \mid a$

Corollary 6.15.2: $a \equiv 0 \pmod{6}$ if and only if $a_0 \equiv 0 \pmod{2}$ AND $\sum_{n=0}^k a_i \equiv 0 \pmod{3}$

Proposition 6.16: $a \equiv a_0 + a_1 + a_2 + \cdots + (-1)^k a_k \pmod{11}$

Proof: Note that $10 \equiv -1 \pmod{11} \implies 10^k \equiv (-1)^k \pmod{11}$

Thus when we look at n expanded in its base 10 form mod 11, we get

$$n = a_m 10^m + \cdots + a_1 10 + a_0 \equiv a_0 - a_1 + \cdots + (-1)^m a_m \pmod{11}$$

Corollary 6.17: An integer n is divisible 11 if and only if the alternating sum of its digits is divisible by 11

Proposition 6.17.1: To test if $7 \mid a$, take a , truncate the last digit and subtract the rest of the digit by $2 * a_0$. Repeat until we reach one digit and it is 0 or 7. Then $7 \mid a$. Otherwise $7 \nmid a$

Proof:

$$\begin{aligned} a &= a_0 + 10(a_1 + 10a_2 + \cdots + 10^{k-1}a_k) \\ &\equiv (-20)a_0 + 10(a_1 + \cdots + 10^{k-1}a_k) \equiv \pmod{7} \\ &\equiv 10(-2a_0 + a_1 + 10a_2 + \cdots + 10^{k-1}a_k) \pmod{7} \end{aligned}$$

Thus $7 \mid a \implies 7 \mid (-2a_0 + a_1 + 10a_2 + \dots + 10^{k-1}a_k)$, which is the recursion we created above

Example:

6.3 Linear Congruences

Theorem 6.18: Let $m \in \mathbb{Z}^+$ and $a \neq 0$. Then $ax \equiv b \pmod{m}$ has a solution if and only if $d = \gcd(a, m)$ divides b . If $d \mid b$, then there are exactly d solutions distinct mod m . Let x_0 be a solution, then the other solutions are of the form

$$x = x_0 + \left(\frac{m}{d}\right)k \quad 0 \leq k \leq d$$

Where x_0 can be found by satisfying

$$\left(\frac{a}{d}\right)x_0 \equiv \left(\frac{b}{d}\right) \pmod{(m/d)}$$

Proof: $ax \equiv b \pmod{m} \implies ax = b + my \implies ax - my = b$. This is a Diophantine problem with $(a, -m, b)$

Let $d = \gcd(a, m)$. If $d \nmid b$, then there are no solutions

Otherwise let $d \mid b \implies$ solutions are of the form

$$x = x_0 + \left(\frac{m}{d}\right)k \quad y = y_0 + \left(\frac{a}{d}\right)k$$

Which implies that $x \equiv x_0 \pmod{(m/d)}$. To show that these solutions are distinct mod m ,

Let $x_1 = x_0 + \left(\frac{m}{d}\right)k_1$ and $x_2 = x_0 + \left(\frac{m}{d}\right)k_2$ be distinct solutions and suppose $x_1 \equiv x_2 \pmod{m}$

Then $x_1 - x_2 = mk_3 \iff \left(\frac{m}{d}\right)(k_1 - k_2) = mk_3 \iff k_1 - k_2 = dk_3 \implies k_1 \equiv k_2 \pmod{d}$. Thus x_1, x_2 are distinct

Finally, to show that x_0 arises from solving $\left(\frac{a}{d}\right)x_0 \equiv \left(\frac{b}{d}\right) \pmod{(m/d)}$,

Note that $\left(\frac{a}{d}\right)x_0 = \frac{b}{d} + \left(\frac{m}{d}\right)z \implies ax_0 = b + mz \implies ax_0 \equiv b \pmod{m}$

Thus x_0 is a solution we desire

Corollary 6.19: If $\gcd(a, m) = 1$, then $ax \equiv b \pmod{m}$ has exactly 1 solution mod m

Proof: Let $d = 1$ and apply Theorem 6.18. Then $d \mid b \implies$ there is only 1 solution

Example: $6x \equiv 7 \pmod{15}$ has no solutions because $\gcd(6, 15) = 3$ but $3 \nmid 7$

Example: $5x \equiv 6 \pmod{11} \implies x = 10$ is a unique solution since $\gcd(5, 11) = 1$

Example: $9x \equiv 6 \pmod{15}$ has $\gcd(9, 15) = 3$ solutions mod 15

Reducing the equation, we get $3x \equiv 2 \pmod{5} \implies x_0 = 4 \implies$ solutions are $\{4, 4 + \frac{15}{3}, 4 + 2 * \frac{15}{3}\} = \{4, 9, 14\}$

We can also solve linear congruence problems using Extended Euclidean Algorithm

Example: $183x \equiv 15 \pmod{31} \implies 28x \equiv 15 \pmod{31}$

Converting it into a Linear Diophantine problem, we get $28x - 31y = 15$. Now we find $\gcd(28, 31)$

$$31 = 1 * 28 + 3$$

$$28 = 9 * 3 + 1$$

$$3 = 3 * 1$$

Thus $\gcd(28, 31) = 1$. Now we write it as a linear combination of 28, 31

$$31 = 1 * 31 + 0 * 28$$

$$28 = 0 * 31 + 1 * 28$$

$$3 = 1 * 31 - 1 * 28$$

$$1 = 1 * 28 - 9 * 3 = -9 * 31 + 10 * 28$$

Thus $28(10) + 31(-9) = 1 \implies 28(150) + 31(-135) = 15 \implies 28(150) \equiv 15 \pmod{31} \implies x = 26$

Multiplicative Inverse: a has a **multiplicative inverse** b if $ab \equiv 1 \pmod{m}$

Corollary 6.21: a has an inverse mod m if and only if $\gcd(a, m) = 1$

Proof: From Theorem 6.18, $ax = 1 \pmod{m}$ has a solution if and only if $\gcd(a, m) \mid 1 \iff \gcd(a, m) = 1$

Example: $7x \equiv 4 \pmod{19}$ where $7^{-1} = 11$

$$77x \equiv 44 \pmod{19} \implies x \equiv 6 \pmod{19}$$

Steps to solve $ax \equiv b \pmod{m}$ where $\gcd(a, m) = 1$

1. Convert the problem into Linear Diophantine problem $ax - my = b$
2. Use Extended Euclidean Algorithm to find x_0, y_0 such that $ax_0 - my_0 = 1$
3. Compute $x = bx_0$

Steps to find an inverse of $a \pmod{m}$ with $\gcd(a, m) = 1$

1. Convert the problem into Linear Diophantine problem $ax - my = b$
2. Use Extended Euclidean Algorithm to find x_0, y_0 such that $ax_0 - my_0 = 1$
3. $x_0 \pmod{m}$ is the inverse of $a \pmod{m}$

6.4 Chinese Remainder Theorem

Theorem 6.22: Let m, n be relatively prime. Then the system of congruences

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Has a unique solution mod mn

Existence Proof 1: $x \equiv a \pmod{m} \implies a = mt \equiv b \pmod{n} \implies mt \equiv (b - a) \pmod{n}$

By Theorem, since m, n are relatively prime, there is a unique solution. Clearly $x = a + mt_0$ is a solution to both congruences

Existence Proof 2: $\gcd(m, n) = 1 \implies mu + nv = 1 \implies x = bmu + anv$

Note that $\mu \equiv 0 \pmod{m}$ and $nv \equiv 1 - mu \equiv 1 \pmod{m} \implies x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ as desired

Thus x is the desired solution

Uniqueness Proof: Let x_1, x_2 be 2 different solutions. Then we must have

$$\begin{aligned} x_1 &\equiv a \pmod{m} & x_1 &\equiv b \pmod{n} \\ x_2 &\equiv a \pmod{m} & x_2 &\equiv b \pmod{n} \end{aligned}$$

Thus $x_1 \equiv x_2 \pmod{m}$ and $x_1 \equiv x_2 \pmod{n} \implies m \mid (x_1 - x_2)$ and $n \mid (x_1 - x_2) \implies x_1 - x_2$ is multiple of m, n

Since $\gcd(m, n) = 1$, we must have $mn \mid x_1 - x_2 \implies x_1 \equiv x_2 \pmod{mn}$

Example: $x \equiv 2 \pmod{3}$ $x \equiv 4 \pmod{5}$

$\gcd(3, 5) = 1$ and we solve that $3(2) + 5(-1) = 1 \implies x = bmu + anv = (4)(3)(2) + (2)(5)(-1) \equiv 14 \pmod{15}$

Theorem 6.23 Chinese Remainder Theorem: Let $m_1, m_2, \dots, m_r \in \mathbb{Z}^+$ and are pairwise relatively prime. Then

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

Has a unique solution $x \pmod{m_1 m_2 \cdots m_r}$

Existence Proof 1: Pair up the first 2 equations and use Theorem 6.22

$$x \equiv b_1 \pmod{m_1 m_2}$$

Repeat process for m_3 and $m_1 m_2$. Works because pairwise relatively prime implies that m_3 and $m_1 m_2$ have no common divisors

Existence Proof 2: Let $m = m_1 m_2 \cdots m_r$ and $n_i = m/m_i$. We claim that $\gcd(n_i, m_i) = 1$

Suppose by contradiction that $p \mid \gcd(n_i, m_i)$. Then $p \mid n_i \implies p \mid m_j$ for some $j \neq i$

Thus we must have $p \mid \gcd(m_j, m_i)$, contradicting that $\gcd(m_i, m_j) = 1$ and thus we must have $\gcd(n_i, m_i) = 1$

For each i , by Corollary 6.21, there exists u_i such that

$$n_i u_i \equiv 1 \pmod{m_i}$$

Let $x = a_1 n_1 u_1 + \dots + a_r n_r u_r$, then clearly for each m_i

$$x \equiv a_i n_i u_i \equiv a_i \pmod{m_i}$$

Unique Proof: Assume there are 2 solutions x_1, x_2 . Then for each m_i we must have

$$m_i \mid (x_1 - x_2) \quad 1 \leq i \leq r$$

Thus means that $m_1 m_2 \dots m_r \mid (x_1 - x_2)$ since m_i are relatively prime

Thus $x_1 \equiv x_2 \pmod{m_1 m_2 \dots m_r}$ and x_1, x_2 are the same solution

Example Let $x \equiv 2 \pmod{3} \quad x \equiv 3 \pmod{5} \quad x \equiv 2 \pmod{7}$

Then we have $n_1 = 35, n_2 = 21, n_3 = 15$ and

$$35u_1 \equiv 1 \pmod{3} \implies u_1 = 2$$

$$21u_2 \equiv 1 \pmod{5} \implies u_2 = 1$$

$$15u_3 \equiv 1 \pmod{7} \implies u_3 = 1$$

Thus we have $x = a_1 n_1 u_1 + a_2 n_2 u_2 + a_3 n_3 u_3 = (2)(35)(2) + (3)(21)(1) + (2)(15)(1) \equiv 23 \pmod{105}$

UPSHOT: We can factor composite modulus m into distinct prime powers and the solve the system of congruence mod

Example: $x^2 \equiv 1 \pmod{275 = 5^2 * 11}$ can be broken down into

$$x^2 \equiv 1 \pmod{25} \implies x \equiv 1, 24 \pmod{25}$$

$$x^2 \equiv 1 \pmod{11} \implies x \equiv 1, 10 \pmod{11}$$

Thus solutions are of the form

$$x \equiv 1 \pmod{25} \quad x \equiv 1 \pmod{11} \implies x \equiv 1 \pmod{275}$$

$$x \equiv 1 \pmod{25} \quad x \equiv 10 \pmod{11} \implies x \equiv 76 \pmod{275}$$

$$x \equiv 24 \pmod{25} \quad x \equiv 1 \pmod{11} \implies x \equiv 199 \pmod{275}$$

$$x \equiv 24 \pmod{25} \quad x \equiv 10 \pmod{11} \implies x \equiv 274 \pmod{275}$$

Thus the solutions are $x \equiv \{1, 76, 199, 274\} \pmod{275}$

6.5 Fractions mod m

We can interpret $\frac{a}{b} \pmod{m}$ as $a(b^{-1}) \pmod{m}$ where b^{-1} comes from $bb^{-1} \equiv 1 \pmod{m}$

- Only works when $\gcd(b, m) = 1$. Since these are the only b 's with a multiplicative inverse mod m
- Here we interpret $\frac{1}{b}$ as the number we need to multiply b by to get 1 mod m

Example: Calculate $\frac{2}{7} \pmod{19}$

We see that $7^{-1} \equiv 11 \pmod{19}$. Thus $\frac{2}{7} = 2 * 11 \equiv 3 \pmod{19}$