MATH406: Introduction to Number Theory

Michael Li

Contents

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 - Divides: 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 $n = dk \geq d$

2.2 Euclid's Theorem

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

Definition - 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 $p \mid k \implies k \mid n \implies p \mid n$

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

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

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

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

Thus $p_i \mid 2 * 3 * 5 * \cdots * p_n$ and $p_i \mid N$ (by Lemma 2.6) $\implies p_i \mid N - (2 * 3 * 5 * \cdots * p_n) \implies p_i \mid 1$ 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 $a, b \in Z$ with $b > 0$. Then there exists unique $q, r \in Z$ such that $a = bq + r$ with $0 \leq r < b$

Proof: Let $S = \{n \in Z \mid bn \leq a\}$. 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 mutliple 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

Definition - Relatively Prime: a, b are **relatively prime** if $\gcd(a, b) = 1$

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

Proposition 2.10: Let $a, b \in Z$ 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 $a, b \in Z$, not both 0, and $e \in Z^+$. 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 $a, b \in Z$ with $a \geq 0, b > 0$. Then we have

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

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 cleary 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): For $a, b \in Z$ with at least one non-zero, $\exists x, y \in Z$ 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

$$a = dq + r \implies r = a - dq = a - (ax_0 + by_0)q = a(1 - x_0 q) + b(-y_0 q)$$

Thus $r \in S$. But since d is the smallest positive element of S and $0 \le r < d$, 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 $e \le d$

$e \mid a$ and $e \mid b \implies e \mid ax_0 + by_0 = d$. Thus $e \le d$ and d is the largest common factor of a, b

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

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

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

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

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

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

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

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

$$\begin{aligned} 21963 &= 2745 * 8 + 3 \\ 2745 &= 343 * 8 + 1 \\ 343 &= 42 * 8 + 7 \\ 42 &- 5 * 8 + 2 \\ 5 &= 0 * 8 + 5 \end{aligned}$$

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 $a_k \leq n - 1$

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

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

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

- **Example**: for $n = 10$, we have $1 = 0.\bar{9}$
- **Example**: $0.01_7 = 0.0006\bar{6}_7$

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 $x^k - 1 = (x - 1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$

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

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

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

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

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 $x^k + 1 = (x+1)(x^{k-1} - x^{k-2} + x^{k-3} - \cdots - x + 1)$

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

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

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

3 Linear Diophantine Equation

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

- 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 $a, b, c \in Z$ 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

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

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

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

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

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

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 $d \mid b \implies \frac{a}{d}, \frac{b}{d} \in Z$

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 $a, b, c \in Z$ 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

$$x = x_0 + bt \qquad y = y_0 - at \qquad t \in Z$$

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

$$x = -150 + 14t \qquad y = -180 + 17t \qquad t \in Z$$

Proposition 3.3: Let $a, b \in Z^+$ and relatively prime. Then there are no non-negative $x, y \in Z$ 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 $a, b \in Z^+$ and relatively prime. If $n > ab - a - b$ then there exists non-negative $x, y \in Z$ 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

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

Now we show that $x_1 \geq 0$

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

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

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 $a, b \in Z$ 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 $a_1, a_2, \ldots, a_3 \in Z$ 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 integers > 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 $a, b \in Z^+$ where $a = 2^{a_2} 3^{a_3} \cdots$ and $b = 2^{b_2} 3^{b_3} \cdots$. Then $a \mid b$ if and only if $a_p \leq b_p$ 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 $\forall p, a_p + c_p = b_p \implies a_p \leq b_p$

$\impliedby$ 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 $a, b \in Z^+$ 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 $\gcd(a, b) = 2^{d_2} 3^{d_3} \cdots$ 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 $n \in Z^+$. Then there exists $r \in Z, r \geq 1$ and a squarefree integer $s \geq 1$ such that $n = r^2 s$

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

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

Let $r = p_1^{a_1} p_2^{p_2} \cdots$ 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 $m \in Z^+$. Then m is a kth power if and only if all exponents in the prime factorization of m are multiples of k

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

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

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

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

By brute force, we see that $a = 1, b = 2, c = d = \cdots = 0$ 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 $d, e, \ldots$

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 $A = 2^a 3^b 5^c \cdots = 2 * 3^2 (2^j 3^k 5^{c'} \cdots)^3 = 18B^3$ for any $B \geq 1$

5.2 Irrationality Proof

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

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

Proof: Suppose by contradiction that $\sqrt{2}$ is rational and $\sqrt{2} = a/b \in Q$ 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 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 $k \in Z$ and $k \geq 2$. Let $n \in Z^+$ that is not a perfect kth power. Then $\sqrt[k]{n}$ is irrational

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

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

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

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

Let $a = 2^{y_2}3^{y_3} \cdots$. Since a^k is a perfect power, by Proposition 5.1, every exponent is of 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 kth power

5.3 Rational Root Theorem

Theorem 5.4 (Rational Root Theorem): let $P(X) = a_nX^n + \cdots + a_1X + a_0$ 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: $P(u/v) = 0 \implies a_n(u/v)^n + \cdots + a_0 = 0 \implies a_nu^n + \cdots + a_0v^n = 0$

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

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

5.4 Pythagorean Triples

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

Definition - 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 kth powers of integers

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

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 kth 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 $n = 2k \implies n^2 = 4j^2 \implies 4 \mid n$

Let n be odd $\implies n = 2k + 1 \implies n^24k(k + 1) + 1$

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

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

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

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

Then $c = \dfrac{c+a}{2} + \dfrac{c-a}{2}$ and $a = \dfrac{c+a}{2} - \dfrac{c-a}{2}$ 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: $\dfrac{c+a}{2}$ and $\dfrac{c-a}{2}$ whose product is a square

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

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

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

Since $\dfrac{c-a}{2} = m^2$ and $\dfrac{c+a}{2} = n^2$ 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 $m \in Z^+$. Then m is a difference of 2 squares if and only if either m is odd or m is a multiple of 4

Proof: $\impliedby$ 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 $x = \dfrac{(u+v)}{2}$ and $y = \frac{(u-v)}{2}$ then clearly $x, y \in Z$ since u, v have the same parity

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

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

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

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

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 $\lfloor \frac{n}{p^j} \rfloor$ multiples of p^j up to n

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

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 $1 \leq j \leq k$

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

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

Proof:

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

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

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

As an example, consider the product

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

Now consider using m primes

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

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

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

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

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

Thus $\zeta(s) \geq \frac{1}{s-1}$ diverges as $s \to 1^+$. 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 and only if $a - b$ is a multiple of m

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

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 $a \in Z$ and $m \in Z^+$ 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 $a, b, c \in Z$ and $m \in Z^+$. Then

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

Proof:

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

Proposition 6.5: Let $a, b, c, d \in Z$ and $m \in Z^+$. 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: $a \equiv b \pmod{m} \implies a = b + k_1 m$ and $c \equiv d \pmod{m} \implies c = d + k_2 m$

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

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

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

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 $\frac{d}{k} \in Z \implies 0 \leq k \leq d - 1$

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 be 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

- Divide a, b, m be a common factor. Then solved the reduced congruence

  Example: $15x \equiv 25 \pmod{55} \implies 3x \equiv 5 \pmod{11} \implies x \equiv 9 \pmod{11}$

Proposition 6.9: Let $n \in Z^+$ and $a, b \in Z$. 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: $x^2 \equiv 1 \pmod{p} \iff x^2 - 1 \equiv 0 \pmod{0} \iff (x-1)(x+1) \equiv 0 \pmod{p}$

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 $x \equiv \pm 1 \pmod{p}$

6.2 Modular Exponentiation

Consider $3^{385} \pmod{479}$

Using **repeated squaring**, we see that

$$\begin{aligned}
3^2 &\equiv 9 \pmod{479} \\
3^4 &\equiv 81 \pmod{479} \\
3^8 &\equiv 81^2 \equiv 334 \pmod{479} \\
3^{16} &\equiv 334^2 \equiv 428 \pmod{479} \\
3^{32} &\equiv 428^2 \equiv 206 \pmod{479} \\
3^{64} &\equiv 206^2 \equiv 284 \pmod{479} \\
3^{128} &\equiv 284^2 \equiv 184 \pmod{479} \\
3^{256} &\equiv 184^2 \equiv 326 \pmod{479}
\end{aligned}$$

Thus we see that

$$3^{385} \equiv 3^{256} 3^{128} 3^1 \equiv 326 * 184 * 3 \equiv 327 \pmod{479}$$

6.3 Divisibility Tests

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

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

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

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

  $\impliedby$ 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 $a_0 \equiv 0 \pmod{10} \implies a_0 = 0$ or $a_0 = 5$

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

Poroposition 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

$$n = a_m 10^m + \cdots + a_1 0 + a_0 \equiv a_m + \cdots + a_1 + a_0 \pmod 3$$

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

$\impliedby$ 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 $\displaystyle\sum_{n=0}^{k} a_i \equiv 0 \pmod 3$

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

$$n = a_m 10^m + \cdots + a_1 0 + a_0 \equiv a_0 - a_1 + \cdots + (-1)^m a_m \pmod{11}$$

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:

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

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

Example: Consider $n = 42735$

$$\begin{aligned}
4273 - 2(5) &= 4263 \\
426 - 2(3) &= 420 \\
42 - 2(0) &= 42 \\
4 - 2(2) &= 0
\end{aligned}$$

Thus $7 \mid 42735$

6.4 Linear Congruences

Theorem 6.18: Let $m \in Z^+$ 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

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

Where x_0 can be found by satisfying

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

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

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

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

Which implies that $x \equiv x_0 \pmod{\frac{m}{d}}$

To show that these solutions are distinct mod m, let $x_1 = x_0 + (\frac{m}{d})k_1$ and $x_2 = x_0 + (\frac{m}{d})k_2$ be distinct solutions and suppose $x_1 \equiv x_2 \pmod{m}$

Then $x_1 - x_2 = mk_3 \iff (\frac{m}{d})(k_1 - k_2) = mk_3 \iff k_1 - k_2 = dk_3 \implies k_1 \equiv k_2 \pmod{d}$

- **Note** that $0 \leq k \leq d - 1$

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

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

Thus x_0 is a solution we desire

Corollary 6.19: If $\gcd(a, m) = 1$, then $ax = b \pmod{m}$ 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: $5x = 6 \pmod{11} \implies x = 10$ 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 $\gcd(28, 31)$

$$\begin{aligned} 31 &= 1 * 28 + 3 \\ 28 &= 9 * 3 + 1 \\ 3 &= 3 * 1 \end{aligned}$$

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

$$\begin{aligned} 31 &= 1 * 31 + 0 * 28 \\ 28 &= 0 * 31 + 1 * 28 \\ 3 &= 1 * 31 - 1 * 28 \\ 1 &= 1 * 28 - 9 * 3 = -9 * 31 + 10 * 28 \end{aligned}$$

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

Definition - 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 $7^{-1} \equiv 11 \pmod{19}$

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

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 $ax - my = 1$
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 $a \pmod m$

6.5 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: $x \equiv a \pmod m \implies x = a + mt \equiv b \pmod n \implies mt \equiv (b - a) \pmod n$

Since m, n are relatively prime, there is a unique solution (call it t_0). Clearly $x = a + mt_0$ is a solution to both congruences

- $x = a + mt_0 \equiv a \pmod m$
- $x = a + mt_0 \equiv a + (b - a) \equiv b \pmod n$

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

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

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: $x \equiv 2 \pmod 3$ $\qquad$ $x \equiv 4 \pmod 5$

$x \equiv 4 \pmod 5 \implies x = 4 + 5k \equiv 2 \pmod 3$ for some $k \in Z$

$\implies 5k \equiv 1 \pmod 3 \implies -1k \equiv 1 \pmod 3 \implies k \equiv 2 \pmod 3$

Thus $x = 4 + 5(2 + 3l)$ for some $l \in Z$

Thus $x \equiv 14 \pmod{15}$

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

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_1} \\ &\cdots \\ x &\equiv a_3 \pmod{m_r} \end{aligned}$$

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

Proof by Induction:

Base Case $r = 2$ is handled by previous Theorem

IH: Suppose that for an arbitrary $k \leq n$, CRT holds true

IS: Prove CRT is true for $n+1$

Consider the first n congruences. By IH, they have a unique solution mod $m_1 m_2 \cdots m_n$. Call the solution x_0

Now we have the system

$$\begin{aligned} x &\equiv a_{n+1} \pmod{m_{n+1}} \\ x &\equiv x_0 \pmod{m_1, \cdots, m_n} \end{aligned}$$

This is handled by the previous theorem, thus CRT holds for any $n \geq 2$

Example Let $x \equiv 2 \pmod 3 \qquad x \equiv 3 \pmod 5 \qquad x \equiv 2 \pmod 7$

Taking the largest modulus, we have $x = 2 + 7k \equiv 3 \pmod 5 \implies 7k \equiv 1 \pmod 5 \implies k \equiv 3 \pmod 5$

Thus $k = 3 + 5l \equiv 2 \pmod 3$. Now plugging this back into the original equation for x, we get

$$x = 2 + 7(3 + 5l) = 23 + 35l \equiv 2 \pmod 3$$

This implies that $l \equiv 0 \pmod 3 \implies l = 3m$

Thus $x = 23 + 35(3m) \equiv 23 \pmod{105}$

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

$$\begin{aligned} x^2 &\equiv 1 \pmod{25} \implies x \equiv 1, 24 \pmod{25} \\ x^2 &\equiv 1 \pmod{11} \implies x \equiv 1, 10 \pmod{11} \end{aligned}$$

Thus solutions are of the form

$$\begin{aligned} x \equiv 1 \pmod{25} &\qquad x \equiv 1 \pmod{11} \implies x \equiv 1 \pmod{275} \\ x \equiv 1 \pmod{25} &\qquad x \equiv 10 \pmod{11} \implies x \equiv 76 \pmod{275} \\ x \equiv 24 \pmod{25} &\qquad x \equiv 1 \pmod{11} \implies x \equiv 199 \pmod{275} \\ x \equiv 24 \pmod{25} &\qquad x \equiv 10 \pmod{11} \implies x \equiv 274 \pmod{275} \end{aligned}$$

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

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

6.6 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 $1 \pmod m$

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

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

7 Fermat, Euler, and Wilson

7.1 Fermat's Theorem

Lemma 8.3: For a prime p,

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

Proof: Using the binomial theorem, we have that

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Where

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \implies p! = k!(p-k)!\binom{p}{k}$$

Clearly p divides the LHS and thus p must also divide the RHS.

However, for $0 < k < p$, clearly $p \nmid (p-k)!$ and $p \nmid k!$. Thus $p \mid \binom{p}{k}$

Lemma 8.4: Let $b \not\equiv 0 \pmod{p}$, then the set

$$b, 2b, \ldots, (p-1)b \pmod{p}$$

contains each nonzero congruence class mod p exactly once

Proof: Let $a \not\equiv 0 \pmod{p}$ be arbitrary and look at the linear congruence

$$bx \equiv a \pmod{p}$$

This must have a unique solution x where $1 \leq x \leq p-1$

Thus a belongs to one of the congruence classes defined by $\{b, 2b, \ldots, (p-1)b\} \pmod{p}$

Since a was arbitrary, every congruence class occurs

To show that each congruence class only occurs once, BWOC suppose that

$$bi \equiv bj \pmod{p} \implies i \equiv j \pmod{p} \qquad 1 \leq i < j \leq p-1$$

However, the given bounds on i, j make this impossible.

Thus each nonzero congruence class occurs exactly once among the multiples of b

Example: Let $p = 7$ and $b = 2$

Then the numbers $2, 4, 6, 8, 10, 12 \pmod{7}$ are the same as $2, 4, 6, 1, 3, 5 \pmod{7}$

Thus every nonzero congruence class mod 7 is represented exactly once

Fermat's Theorem: For a prime p, the following hold true

- $\forall b \in Z, b^p - b \equiv 0 \pmod{p}$
- $b \not\equiv 0 \pmod{p} \implies b^{p-1} \equiv 1 \pmod{p}$

Proof 1 (Using Lemma 8.3): Show that $b^p \equiv b \pmod p$ by Induction

Base Case: $b = 0 \implies 0^p \equiv 0 \pmod p$ and $b = 1 \implies 1^p \equiv 1 \pmod p$

IH: Assume that for any arbitrary b, we have that $b^p \equiv k \pmod b$

IS: Show for $b+1$. From the binomial coefficients formula and Lemma 8.3, we see that

$$(b+1)^p \equiv b^p + 1 \equiv \underbrace{b+1}_{\text{by IH}} \pmod p$$

The above proves Fermat's Theorem for non-negative integers

Now for negative integers, suppose that $b < 0$. Then for an odd prime p, we have $(-b)^p \equiv -b \pmod p$ by the ideas above.

- If p is odd, then $(-1)^p \equiv -1 \pmod p$
- If p is 2, then clearly $-b^p \equiv -b \pmod p \implies b^p \equiv b \pmod p$

Proof 2 (Using Lemma 8.4): Suppose that $b \not\equiv 0 \pmod p$.

From Lemma 8.4, we know that

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} bi \pmod p \implies (p-1)! \equiv b^{p-1}(p-1)!$$

Since $p \nmid (p-1)!$, we have that

$$b^{p-1} \equiv 1 \pmod p$$

Multiplying both sides by b gives the other form

$$b^p \equiv b \pmod p$$

Note that for the case where $b \equiv 0 \pmod 0$, we have that $b^p \equiv 0^p \equiv 0 \equiv 0 \pmod p$

Thus the congruence holds for all $b \in Z$

Example: $2^6 = 64 \equiv 1 \pmod 7$ and $2^7 \equiv 2 \pmod 7$

Example: $3^{28} = (3^4)^7 \equiv 1^7 \equiv 1 \pmod 5$

- This follow from the second claim in Fermat's Theorem (since $3^{5-1} \equiv 1 \pmod 5$)

Example: Divide 23 into 7^{200}. What is the remainder?

By Fermat's Theorem, we know that $7^{22} \equiv 1 \pmod{23}$

Thus $7^{200} = (7^{22})^9 * 2^2 \equiv 1^9 * 49 \equiv 3 \pmod{23}$

Corollary 8.2: For prime p and $b \not\equiv 0 \pmod p$,

$$x \equiv y \pmod{p-1} \implies b^x \equiv b^y \pmod p$$

Proof: We know that $x = y + (p-1)k$ for some $k \in Z$

Thus we see that $b^x = b^y b^{(p-1)k} \implies b^x \equiv b^y \pmod p$ by Fermat's Theorem

Upshot: We can apply the Divisional Algorithm to the exponent of an integer with $p-1$ to quickly evaluate congruences mod p

Fermat Primality Test: If n is odd, $b \not\equiv 0 \pmod{n}$, and $b^{n-1} \not\equiv 1 \pmod{n}$, then n is not prime

Proof: Using Fermat's Theorem, we see that for an odd prime p, $b^{p-1} \equiv 1 \pmod{p}$

Now by contraposition, suppose that n is odd and that $p^{n-1} \not\equiv 1 \pmod{n}$, we get that n is not prime

Upshot: We can quickly test if a number n is not prime by looking at $2^{n-1} \not\equiv 1 \pmod{n}$

- **Note**: $2^{n-1} \equiv 1 \pmod{n}$ DOES NOT guarantee n is prime

Example: For $n = 77$, we see that

$2^{n-1} = 2^{76} \equiv 9 \pmod{77} \not\equiv 1 \pmod{77}$

Thus 77 is not prime

7.2 Euler's Theorem

Definition - Euler Function: $\phi(n)$ is the number of integers $1 \leq j \leq n$ such that $\gcd(j, n) = 1$

Examples:

- $\phi(12) = 4$ this comes from $\{1, 5, 7, 11\}$
- For any prime p, $\phi(p) = p - 1$

Proposition 8.6: For $m, n \in Z^+$, if $\gcd(m, n) = 1$ then

$$\phi(mn) = \phi(m)\phi(n)$$

Proof: Define $T_n = \{1 \leq j \leq n \mid \gcd(j, n) = 1\}$, so $|T_n| = \phi(n)$

Now define a function $f : T_{mn} \to T_m \times T_n$ where $f(a) = (a \pmod{m}, a \pmod{n})$

Firstly, we show that $a \pmod{m} \in T_m$, i.e. $a \pmod{m}$ is relatively prime to m. Similar for $a \pmod{n}$

Suppose $a \equiv l \pmod{m} \implies a = mk + l$ for some $k, l \in Z$

If d is a common divisor for l, m, then $d \mid a$ and $d \mid mn \implies d = 1$ since $a \in T_{mn}$

Now we show that this function is 1-1 and onto

- 1-1: Suppose $f(a) = f(b)$ for some $a, b \in T_{mn}$, we show that $a = b$

  Then $(a \pmod{m}, a \pmod{n}) = (b \pmod{m}, b \pmod{n}) \implies a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$

  Thus $\underbrace{mn \mid (b - a)}_{\gcd(m,n)=1} \implies b \equiv a \pmod{mn}$

  Since $0 \leq a, b \leq mn$, we must have that $b = a$

- Onto: Take $(r, t) \in T_m \times T_n$, so $\gcd(r, m) = 1$ and $\gcd(t, n) = 1$

  By CRT, $x \equiv r \pmod{m} \qquad x \equiv t \pmod{n}$ has a unique solution mod mn, call it a

  We show that $\gcd(a, mn) = 1 \implies a \in T_{mn}$

  BWOC, suppose we have a prime p such that $p \mid a$ and $p \mid mn$

  This implies either $p \mid a$ and $p \mid m$ OR $p \mid a$ and $p \mid n$ since $\gcd(m, n) = 1$

Thus $a = mk + r = nl + t \implies p \mid r$ and $p \mid m$ OR $p \mid t$ and $p \mid n$

Contradiction since we supposed $\gcd(r, m) = 1$ and $\gcd(t, n) = 1$

Thus $\gcd(a, mn) = 1 \implies a \in T_{mn}$

Proposition 8.7: For a prime p and $k \geq 1$,

$$\phi(p^k) = p^k - p^{k-1}$$

Proof: For $1 \leq j \leq p^k$, there are p^{k-1} multiples of p, namely $\{(1)p, (2)p, \dots, (p^{k-1})p\}$

These multiples are exactly when $\gcd(j, p^k) \neq 1$

Theorem 8.8: Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorization of n where each exponent $a_i \geq 1$. Then

$$\phi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1}) = n \prod_{p \mid n} (1 - \frac{1}{p})$$

Proof: Applying Propositions 8.6 and 8.7, we see that

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{a_i}) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1})$$

For the second part of the equality of the theorem, note that $p^a - p^{a-1} = p^a(1 - \frac{1}{p})$. Thus we see that

$$\begin{aligned} \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_i - 1}) &= \prod_{i=1}^{r} p_i^{a_i} (1 - \frac{1}{p_i}) \\ &= n \prod_{i=1}^{r} (1 - \frac{1}{p_i}) \\ &= n \prod_{p \mid n} (1 - \frac{1}{p}) \qquad \text{since each } a_i \geq 1 \end{aligned}$$

Example: $\phi(100)$

- Applying Propositions 8.6, 8.7, we get that $\phi(100) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 40$
- Applying Theorem 8.8, we get that $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$

Lemma 8.10: Let T_n be the set of $1 \leq j \leq n$ with $\gcd(j, n) = 1$. Choose any $b \in T_n$ and let $bT_n \mod n$ be the set of numbers of the form $bt \mod n$ for $t \in T_n$. Then each $t \in T_n$ is congruent to exactly one element of $bT_n \mod n$

Proof: Let $t \in T_n$. Then $\gcd(t, n) = 1$

This means that $bx \equiv t \pmod{n}$ has a unique solution. Call it x_0

We claim that $\gcd(x_0, n) = 1 \implies x_0 \in T_n$

Suppose $d \mid x_0$ and $d \mid n$

Then $n \mid bx_0 - t \implies d \mid bx_0 - t \implies d \mid t$ and $d \mid n \implies n = 1$ since $\gcd(t, n) = 1$

The uniqueness of follows from the uniqueness of x_0

Example: Let $n = 12, b = 5$

Then we have $T = \{1, 5, 7, 11\}$ and $bT = \{5, 25, 35, 55\} \equiv \{5, 1, 11, 7\} \mod 12 = T$

Euler's Theorem: For any b such that $\gcd(b, n) = 1$, we have that

$$b^{\phi(n)} \equiv 1 \pmod{n}$$

- **Note**: This generalizes Fermat's Theorem since $\phi(p) = p - 1$

Proof: Consider the set T_n from Lemma 8.10. Then

$$\prod_{i \in T_n} i \equiv \prod_{i \in T_n} bi \equiv b^{\phi(n)} \prod_{i \in T_n} i \pmod{n}$$

Lemma 8.10 says that the second product is just a rearrangement of the first product. Thus we get that

$$1 \equiv b^{\phi(n)} \pmod{n}$$

Example: $\phi(10) = 4$ and $\gcd(3, 10) = 1 \implies 3^4 = 81 \equiv 1 \pmod{10}$

Example: $3^{84} \pmod{100}$

We see that $\phi(100) = 40$ so by Euler's Theorem, we have that $3^{40} \equiv 1 \pmod{100}$

Thus $3^{84} = (3^{40})^2 3^4 \equiv 81 \pmod{81}$

Corollary 8.11: Take $b \in Z$ such that $\gcd(b, n) = 1$. Then

$$x \equiv y \pmod{\phi(n)} \implies b^x \equiv b^y \pmod{n}$$

- **Note**: This also generalizes the Corollary of Fermat's Theorem since $\phi(p) = p - 1$

Proof: We know that $x = y + \phi(n)k$ for some $k \in Z$

Thus we see that $b^x \equiv b^y (b^{\phi(n)})^k \equiv b^y \pmod{n}$

Example: Let $n = 15$. Then we have $\phi(n) = 8$ and $9 \equiv 1 \pmod{8}$

Thus $2^9 \equiv 2^1 \pmod{15}$

Example: Let $n = 10$. Then $\phi(n) = 4$ and $5 \equiv 1 \pmod{4}$

Thus for any b such that $\gcd(b, 10) = 1$, we have that $b^5 \equiv b \pmod{10}$

Thus b^5 and b have the same last digit for $b \in \{1, 3, 7, 9\}$

Example: Given $m \in Z$, let $\gcd(m, 77) = 1$ and let $c \equiv m^7 \pmod{77}$. Find $c^{43} \pmod{77}$

$\phi(77) = 60$ and $301 \equiv 1 \pmod{60}$

Thus we see that $c^{43} \equiv (m^7)^{43} \equiv m^{301} \equiv m \pmod{77}$

Example: Find the last digit of 3^{7^5}

First, note that $\phi(4) = 2$ and $5 \equiv 1 \pmod 2$

Thus $7^5 \equiv 7^1 \equiv 3 \pmod 4$

Furthermore, we see that $\phi(10) = 4$.

Thus $3^{7^5} \equiv 3^3 \equiv 27 \equiv 7 \pmod{10}$

7.3 Wilson's Theorem

Wilson's Theorem: For a prime p

$$(p-1)! \equiv -1 \pmod p$$

Proof: For integers $1 \leq b \leq p-1$, $bx \equiv 1 \pmod p$ has a unique solution $1 \leq x \leq p-1$

We pair multiple inverses with each other

- Note that $b^2 \equiv 1 \pmod p$ only if $b \equiv \pm \pmod p$, so $b \equiv 1$ and $b \equiv p-1 \pmod p$ are the only numbers that are paired with themselves

Now rearrange the factors so that each inverse is next to each other. This gives

$$(p-1)! \equiv 1(p-1) \equiv -1 \pmod p$$

Example: For $p = 7$, we have $(p-1)! = 6! = 720 \equiv -1 \pmod 7$

This comes from $6! = (6)(5*3)(4*1)(1) \equiv -1*1*1*1 \equiv -1 \pmod 7$

Corollary 8.13: For $n \geq 2$, n is prime if and only if $(n-1)! \equiv -1 \pmod n$

Proof: $\implies$ If n is prime, then $(n-1)! \equiv -1 \pmod n$ by the Wilson's Theorem

$\impliedby$ BWOC suppose n is composite. Then $n = ab$ for $a, b \in Z$ and $1 < a < n$

Thus a is a factor of $(n-1)! \implies (n-1)! \equiv 0 \pmod a$.

But we also have that $(n-1)! \equiv -1 \pmod n \implies (n-1)! \equiv -1 \pmod a$

Contradiction. Thus n must be prime

Example: Let $n = 6$, then $(n-1)! = 5! = 120 \equiv 0 \not\equiv -1 \pmod 6$

Thus n is not prime

8 Cryptography

Shift Cipher: $x \to x + k \pmod{26}$ has key space size of 26

Affine Cipher: $x \to ax + b \pmod{26}$ where $\gcd(a, 26) = 1$ has key space size of $12 * 26$

8.1 RSA

RSA Setup:

1. Alice chooses 2 primes p, q and calculates $n = pq$ and $\phi(n) = (p-1)(q-1)$
2. Alice chooses an encryption key e such that $\gcd(e, \phi(n)) = 1$
3. Alice calculates a decryption key such that $ed \equiv 1 \pmod{\phi(n)}$
4. Alice makes n, e public and d, p, q private

RSA Encryption:

1. Bob looks up Alice's public values n, e
2. Bob writes the message as $m \pmod n$
3. Bob computes $c \equiv m^e \pmod n$
4. Bob sends c to Alice

RSA Decryption

1. Alice receives c
2. Alice computes $m \equiv c^d \pmod n$

Example

Let $p = 3598279$ and $q = 781629$

Then $n = 28122813702491 \qquad \phi(n) = 28122802288584 \qquad e = 233 \qquad d = 27519308677241$

Let $A = 01, B = 02, \ldots, Z = 26$ be the alphabet

Suppose Bob wants tos send CAR $\implies m = 030118 = 30118$

Then $c \equiv m^e \pmod n \equiv 21666077416496 \pmod n$

Finally, Alice decrypts the text as $m \equiv c^d \equiv 30118 \pmod n$

Proposition 9.1: Let $n = pq$ for distinct primes p, q, and take e, d satisfying $ed \equiv 1 \pmod{\phi(n)}$. Then for all m, we have

$$m^{ed} \equiv m \pmod n \qquad c \equiv m^e \pmod n \implies m \equiv c^d \pmod n$$

Proof: Suppose $\gcd(m, n) = 1$.

Then $ed \equiv 1 \pmod{\phi(n)} \implies ed = 1 + k\phi(n)$ for some $k \in Z$

Thus using Euler's Theorem, we have

$$m^{ed} \equiv m^{1+k\phi(n)} \equiv m(m^{\phi(n)})^k \equiv m \pmod n$$

Otherwise, suppose that $\gcd(m, n) \neq 1$. So possible values are p, q, pq

- $pq \implies m \equiv 0 \pmod n \implies m^{ed} \equiv 0 \equiv m \pmod n$
- $p \implies m \equiv 0 \pmod p \implies m^{ed} \equiv 0 \equiv m \pmod p$

  However since $q \nmid m$, we have by Fermat Theorem that $m^{q-1} \equiv 1 \pmod q$

  Thus $m^{ed} \equiv m(m^{q-1})^{k(p-1)} \equiv m \pmod q$

  Thus $p \mid m^{ed} - m$ and $q \mid m^{ed} - m \implies pq \mid m^{ed} - m \implies m^{ed} \equiv m \pmod{pq}$

9 Order and Primitive Roots

9.1 Orders of Elements

Definition - Order: The **order** of $a \mod n$, denoted $\text{ord}_n(a)$ is the smallest positive integer such that

$$a^m \equiv 1 \pmod n$$

- In particular powers of $a \mod n$ create a cyclic group

- The order of an integer a has to exist because of Euler's Theorem: $a^{\phi(n)} \equiv 1 \pmod{n}$. Thus $\text{ord}_n(a) \leq \phi(n)$

Theorem 11.1: Let n be a positive integer and a be an integer where $\gcd(a, n) = 1$. Take any integer m. Then

$$a^m \equiv 1 \pmod{n} \iff \underset{n}{\text{ord}}(a) \mid m$$

Proof: Let $m_0 = \text{ord}_n(a)$

$\implies$ Suppose $a^m \equiv 1 \pmod{n}$. Now apply the division algorithm to m, m_0, so $m = m_0 q + r$ where $0 \leq r < m_0$

Now we see that

$$a^m = a^{m_0 q + r} \equiv a^r \equiv 1 \pmod{n}$$

Since m_0 is the smallest positive exponent that yields 1 and $r < m_0$, we must have that $r = 0 \implies m_0 \mid m$

$\impliedby$ If $m_0 \mid m$, then $m = m_0 k$. Thus we have

$$a^m \equiv (a^{m_0})^k \equiv 1 \pmod{n}$$

Corollary 11.2:

- For a prime p and integer a such that $a \not\equiv 0 \pmod{p}$, then $\text{ord}_p(a) \mid p - 1$
- For a positive integer n and integer a such that $\gcd(a, n) = 1$, we have $\text{ord}_n(a) \mid \phi(n)$

Proof: The first point follows from the second point

By Euler's Theorem, we have that

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Thus using Theorem 11.1, we have that $\text{ord}_n(a) \mid \phi(n)$

Example: $\text{ord}_{23}(3)$

Divisors of $23 - 1 = 22$ are $\{1, 2, 11, 22\}$. By inspection we see that $3^{11} \equiv 1 \pmod{23}$

Thus $\text{ord}_{23}(3) = 11$

9.1.1 Fermat Numbers

Recall that Fermat Numbers are of the form

$$F_n = 2^{2^n} + 1$$

Proposition 11.3: For $n \geq 2$, let p be a prime dividing F_n. Then $p \equiv 1 \pmod{2^{n+2}}$

Proof: If $p \mid 2^{2^n} + 1$, then $2^{2^n} \equiv -1 \pmod{p}$. Squaring both sides yields

$$2^{2^{n+1}} \equiv 1 \pmod{p}$$

Thus by Theorem 11.1, $\text{ord}_p(2) \mid 2^{n+1}$, so $\text{ord}_p(2) = 2^j$ for some $j \leq n + 1$

BWOC, suppose that $j \leq n$, then we have

$$2^{2^n} \equiv (2^{2^j})^{2n-j} \equiv 2^{2^n} \equiv 1 \pmod p$$

But we had $2^{2^n} \equiv -1 \pmod p$. Contradiction

Thus we must have $\text{ord}_p(2) = 2^{n+1}$

Thus by Corollary 11.2, $2^{n+1} \mid p-1$

Since $n \geq 2$, we must have that $p \equiv 1 \pmod 8$

We claim that $p \equiv 1 \pmod 8 \implies \exists b \in Z$ such that $b^2 \equiv 2 \pmod p$ (Exercise 11.2.31)

Thus we have

$$2^{2n+1} \equiv (2^2)^{2^n} \equiv 2^{2^n} \equiv -1 \pmod p \implies b^{2n+2} \equiv 1 \pmod p$$

Thus $\text{ord}_p(b)$ divides 2^{n+2} and does not divide $2^{n+1} \implies \text{ord}_p(2) = 2^{n+2}$

Thus by Corollary 11.2, $2^{n+2} \mid p-1 \implies p \equiv 1 \pmod{2^{n+2}}$

Example: Factor F_5

By Proposition 11.3, any prime must be congruent $1 \mod 128$. Some of the primes include

$$257, \quad 641, \quad ,769, \quad ,1153, \quad ,1409$$

By inspection, we see that $F_5 = 641 * 6700417$

- **Note**: Any prime factor of 6700417 must also be a prime factor of F_5 and therefore must be $1 \mod 128$. Thus 6700417 has no prime factors less than $\sqrt{6700417} \implies 6700417$ is prime

Non-Example: Factor $F_4 = 65537$

Any prime factors of F_4 must be $p \equiv 1 \pmod{64}$. The first two such primes are $193, 257$ but $193 \nmid 65537$ and $257 > \sqrt{65537} \implies F_4$ is prime

9.1.2 Mersenne Numbers

Recall that Mersenne numbers are of the form

$$M_p = 2^p - 1$$

where p is a prime

Proposition 11.4: Let p, q be primes and suppose that $q \mid 2^p - 1$. Then $q \equiv 1 \pmod p$

Proof: If $2^p \equiv 1 \pmod q$, then by Theorem 11.1, $\text{ord}_q(2) \mid p \implies \text{ord}_q(2) = 1$ or p

- If $\text{ord}_q(2) = 1 \implies 2^1 \equiv 1 \pmod q$ which is impossible
- Therefore $\text{ord}_q(2) = p \implies p \mid q-1 \implies q \equiv 1 \pmod p$ by Corollary 11.2

9.2 Primitive Roots

Definition - Primitive Root: For a prime p, if the order of $g \mod p$ equals $p-1$, then g is a **primitive root**

Example: $\text{ord}_5(2) = 4 \implies 2$ is a primitive root for 5

Non-Example: $\text{ord}_7(2) = 3 \implies 2$ is not a primitive root for 7

Proposition 11.5: Suppose $\gcd(g, p) = 1$ for a prime p, then the following are equivalent

- g is a primitive root, $\text{ord}_p(g) = p - 1$
- Every integer that is non-zero mod p is congruent to a power of $g \mod p$

Proof $1 \to 2$: Let g be a primitive root. We claim that $1, g, g^2, \ldots, g^{p-2} \pmod p$ are distinct

BWOC, suppose $g^i \equiv g^j \pmod p$ for $0 \leq i, j \leq p-2$

Then $g^j - i \equiv 1 \implies p - 1 = \text{ord}_p(g) \mid j - i$. Contradiction since $0 \leq j - i < p - 1$

Thus powers of g mod p give $p-1$ distinct congruence classes

Proof $2 \to 1$: Let $m = \text{ord}_p(g)$. Then

$$1, g, g^2, \ldots, g^{m-1} \pmod p$$

are distinct

Since $g^m \equiv 1$, the cycle starts again. Thus $m = p - 1$ by definition

Proposition 11.6: Let g be a primitive root for an odd prime p. Then

$$g^{(p-1)/2} \equiv -1 \pmod p$$

Proof: Let $x \equiv g^{(p-1)/2} \pmod p$. Then

$$x^2 \equiv g^{p-1} \equiv 1 \pmod p \implies x \equiv \pm 1 \pmod p$$

- If $x \equiv 1 \pmod p \implies g^{(p-1)/2} \equiv 1 \pmod p$. Contradiction since the order of g is $p-1$
- Thus $x \equiv -1 \pmod p$ as desired

Proposition 11.7: For a positive integer and $\gcd(x, n) = 1$. Let $m = \text{ord}_n(x)$ and take an integer i. Then

$$\underset{n}{\text{ord}}(x^i) = \frac{m}{\gcd(i, m)}$$

Proof: Let $k = \text{ord}_n(x^i)$

Then $x^{ik} \equiv 1 \pmod n \implies ik \equiv 0 \pmod m$

Now let $d = \gcd(i, m)$. then

$$\frac{i}{d} k \equiv 0 \pmod{\frac{m}{d}}$$

Since $\gcd(i/d, m/d) = 1$, we can divide the congruence by i/d to get

$$k \equiv 0 \pmod{m/d} \implies k \geq \frac{m}{d}$$

Furthermore, since i/d is an integer,

$$(x^i)^{m/d} \equiv (x^m)^{i/d} \equiv 1 \pmod p$$

Thus by Theorem 11.1, $k \mid \frac{m}{d} \implies k \leq \frac{m}{d}$

Thus we see that $k = \dfrac{m}{d}$

Corollary 11.8: For a prime p and a primitive root g mod p, we have that

$$\operatorname*{ord}_p(g^i) = \frac{p-1}{\gcd(i, p-1)}$$

Proof: Follows from Proposition 11.7 using $x = g$ and $m = p - 1$

Example: Since 2 is a primitive root for 13, we have that $2^8 \equiv 9 \pmod{13}$. Proposition 11.7 says that

$$\operatorname*{ord}_{13}(9) = \frac{12}{\gcd(8, 12)} = 3$$

Corollary 11.8: Let g be a primitive root for a prime p. The primitve roots for p are numbers congruent to $g^i \pmod p$ for $\gcd(i, p-1) = 1$

Proof: Since g is a primite root, every number that is nonzero mod p is congruent so some g^i

By Corollary 11.8, $\text{ord}_p(g^i) = p - 1$ if and only if $\gcd(i, p-1)$

Example: Numbers relatively prime to 12 are $1, 5, 7, 11$. Thus the primitive roots for 13 are

$$2, \quad 2^5 \equiv 6, \quad 2^7 \equiv 11, \quad 2^{11} \equiv 7$$

- **Note**: Fermat's Theorem tells us that everything starts over at $2^{12} \equiv 1$, so

$$2^{17} \equiv 2^{15} 2^5 \equiv 2^5 \equiv 6 \pmod{13}$$

Theorem 11.10: Let p be a prime. There are $\phi(p-1)$ primitive roots g for p where $1 \leq g < p$

Proof: Let g be a primitive root. The other primitive roots are exactly $g^i \pmod p$ where $1 \leq u \leq p - 1$ with $\gcd(i, p-1)$

There are $\phi(p-1)$ such values of i, so we are done

Example: The number of primitive roots for 10003 is

$$\phi(100002) = 28560$$

Example: Suppose we want to show that 6 is a primitive root mod 41

Let $m = \text{ord}_{41}(6)$. Since $m \mid 40$, by Corollary 11.2, we see that $m \in \{1, 2, 4, 5, 8, 10, 20, 40\}$

Calculation shows that $6^{20} \equiv -1 \pmod{41}$. Then m cannot be a divisor of 20

- BWOC, if $6^5 \equiv 1 \pmod{41}$, then $6^{20} \equiv (6^5)^4 \equiv 1^4 \equiv 1$. Contradiction

The only remaining choices are $m = 8$ and $m = 40$

- If $m = 8$, then $6^8 \equiv 10 \pmod{41} \implies m \neq 8$
- Thus we must have $m = 40$. Thus 6 is a primitive root for 41

Proposition 11.11: For a prime p and $h \neq 0 \pmod{p}$, the following are equivalent

- h is a primitive root for p
- For each prime q dividing $p - 1$, we have

$$h^{(p-1)/q} \not\equiv 1 \pmod{p}$$

Proof $1 \to 2$: If h is a primitive root, then

$$\operatorname*{ord}_p(h) = p - 1 > (p-1)/q > 0$$

Thus for each q,

$$h^{(p-1)/q} \not\equiv 1 \pmod{p}$$

Proof $2 \to 1$: Let $m = \text{ord}_p(h)$

Corollary 11.2 says that $m \mid p - 1$.

If $m \neq p - 1$, let p be a prime dividing $(p-1)/m$ such that $qk = (p-1)/m$ for some k

Then we have

$$mk = (p-1)/q \implies h^{(p-1)/q} \equiv (h^m)^k \equiv 1 \pmod{p}$$

Contradiction. Thus $m = p - 1$

9.3 Discrete Log Problem

Definition - Discrete Log Problem (DLP): Given a prime p, a primitive root g, and $h \not\equiv 0 \pmod{p}$, find x such that $g^x \equiv h \pmod{p}$

- Here the answer x is called the **discrete log** of h

Example: Suppose we want to solve $3^x = 1594323$ without mods

- $3^{10} = 59049 \qquad 3^{15} = 14348907 \implies x$ is between 10 and 15. By inspection $x = 13$ works

Now suppose we want to solve $3^x \equiv 8 \pmod{43}$. This is clearly harder since higher powers are reduced mod 43

- Brute force approach gives us $x = 39$
- In particular, $x = 81$ also works

$$3^{81} \equiv 3^{42}3^{39} \equiv 1 * 3^{39} \equiv 8 \pmod{43}$$

In general, using Fermat's Theorem, $x = 39 + 42k$ for any integer k

9.3.1 Baby Step-Giant Step Method

Let g be a primitive root for a prime p and let $h \not\equiv 0 \pmod{p}$. We solve

$$g^x \equiv h \pmod{p}$$

1. Let $N = \lceil \sqrt{p-1} \rceil$
2. Make two lists

- $g^i \pmod{p}$ for $0 \le i \le N-1$
- $hg^{-Nj} \pmod{p}$ for $0 \le j \le N-1$

3. Find a match between the two lists $g^i \equiv hg^{-Nj} \pmod{p}$
4. $x = i + Nj$ solves the DLP

Note: There is always a match since we can express n in terms of base $N \implies n = \underbrace{x_0}_{j} + \underbrace{x_1}_{k} N$

Example: Solve $2^x \equiv 9 \pmod{19}$. Here

$$N = \lceil \sqrt{19-1} \rceil = 5$$

Since $h = 9$, we have the lists

- $2^0 \equiv 1, \quad 2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 16$
- $9 * 2^{-0} \equiv 9, \quad 9 * 2^{-5} \equiv 8, \quad 9 * 2^{-10} \equiv 5, \quad 9 * 2^{-15} \equiv 15, \quad 9 * 2^{-20} \equiv 7$

Both lists have 8 in common, so a match is $2^3 \equiv 8 \equiv 9 * 2^{-5}$

Thus $2^8 \equiv 9$

9.3.2 Index Calculus

Baby Step-Giant Step Method is slow when p is large. In this section, we solve DLPs faster

Notationwise, we usually let $\log(h)$ be the DLP of h when p, g are understood

Example: Solve $2^x \equiv 55 \pmod{101}$

$$\log(h) \implies x \text{ such that } 2^x \equiv h \pmod{101}$$

First ignore 55 and compute some other discrete logs instead

- Choose a set of small primes $\{3, 5, 7\}$. Call this set a **factor base**

The first goal is to compute their discrete logs by computing $2^r \pmod{101}$ for randomly chosen values of r and trying to factor the results using only $3, 5, 7$

$$\begin{aligned}
2^7 &\equiv 27 \equiv 3^3 * 5^0 * 7^0 \pmod{101} \\
2^9 &\equiv 7 \equiv 3^0 * 5^0 * 7^1 \pmod{101} \\
2^{17} &\equiv 75 \equiv 3^1 * 5^2 * 7^0 \pmod{101} \\
2^{24} &\equiv 5 \equiv 3^0 * 5^1 * 7^0 \pmod{101} \\
2^{47} &\equiv 63 \equiv 3^2 * 5^0 * 7^1 \pmod{101}
\end{aligned}$$

Relations such as $2^{22} \equiv 77 \pmod{101}$ are excluded since 77 is not a product of numbers in the factor base

We want to find $\log(n)$ for $n \in \{3, 5, 7\}$

- Since $2^9 \equiv 7 \implies \log(7) = 9$
- Since $2^{24} \equiv 5 \implies \log(5) = 24$
- To get $\log(3)$, we look at the prime factorizations we already have

$$3 \equiv (3^3 * 5^0 * 7^0)(3^0 * 5^0 * 7^1)(3^2 * 5^0 * 7^1)^{-1} \equiv 2^7 * 2^9 \equiv 2^{-47} \equiv 2^{-31} \equiv 2^{69}$$

Finally, we now find $\log(55)$ by computing $55 * 2^r \pmod{101}$ for random values of r until we obtain a number that can be factored using only primes in the factor base

$$55 * 2^{25} \equiv 45 \equiv 3^2 * 5 \pmod{101} \implies 55 \equiv 2^{-25} * 3^2 * 5 \pmod{101} \equiv 2^{-25} * 2^{2*69} * 2^{24} \equiv 2^{37} \pmod{101}$$

Thus we conclude that $x = 37$

The steps above can be generalized into

Let g be a primitive root for prime p and let $h \not\equiv 0 \pmod{p}$. We solve

$$g^x \equiv h \pmod{p}$$

1. Choose a factor base B of small primes
2. Compute $g^r \pmod{p}$ for many random values of r and try to factor the results using only primes from B
3. Use combinations of successes from Step 2 to evaluate $\log(q)$ for all $q \in B$
4. Computer $h * g^r \pmod{p}$ for random values of r and try to factor these using only primes from B. If this happens, evaluate $\log(h)$ using the values of $\log(q)$ for $q \in B$

10 Diifie-Hellman Key Exchange

1. Alice and Bob agree on a large prime p and a primitive root $g \mod p$
2. Alice chooses a secret a and computes $h_1 \equiv g^a \pmod{p}$
3. Bob chooses a secret b and calculates $h_2 \equiv g^b \pmod{p}$
4. Alice sends h_1 to Bob and Bob sends h_2 to Alice
5. Alice computes $k \equiv h_2^a \pmod{p}$
6. Bob computes $k \equiv h_1^b \pmod{p}$

Thus Alice and Bob have computed $k \equiv g^{an}$, which is their shared key

- **Note** an eavesdropper can intercept $g, g^a \pmod{p}$, and $g^b \pmod{p}$. If Discrete Log Problem is easy, they can use g and g^a to find a, then compute $k \equiv g^{ba}$

11 Quadratic Reciprocity

11.1 Squares and Square Roots Mod Primes

Definition - Quadratic Residue: If a is a square mod n, then a is a **quadratic residue** mod n

- If not, then a is a **quadratic nonresidue**

Examples:

- 2 is a square mod 7 since $3^2 \equiv 2 \pmod{7}$

- -1 is a square mod 5 since $2^2 \equiv 1 \pmod 5$
- 2 is not a square mod 3 since for $x^2 \not\equiv 2$ for $x = 0, 1, 2$

Proposition 13.1: Let p be an odd prime and let $q \not\equiv 0 \pmod p$. Then

$$a^{(p-1)/2} \equiv \pm 1 \pmod p \quad \text{and} \quad a \text{ is a square mod } p \iff a^{(p-1)/2} \equiv 1 \pmod p$$

Proof: Let $b \equiv a^{(p-1)/2} \pmod p$. Then $b^2 \equiv a^{p-1} \equiv 1 \pmod p$ by Fermat's Theorem

Thus by Corllary 6.11, $b \equiv a^{(p-1)/2} \equiv \pm 1 \pmod p$

$\implies$ Let a be a square mod p, then $x^2 \equiv a$ for some x. Thus we have

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod p$$

by Fermat's Theorem

$\impliedby$ Suppose $a^{(p-1)/2} \equiv 1 \pmod p$ and let g be a primitive root mod p. Then $g^i \equiv a$ for some i, so

$$1 \equiv a^{(p-1)/2} \equiv g^{i(p-1)/2} \pmod p$$

Thus $p - 1 \mid i(p-1)/2 \implies (p-1)k = i(p-1)/2$ for some k

Thus $i = 2k$ and therefore $a \equiv g^i \equiv (g^k)^2$

Thus a is a square mod p

Definition Legendre Symbol: For an odd prime p and integer $a \not\equiv 0 \pmod p$, we define the **Legendre symbol** as

$$(\frac{a}{p}) = \begin{cases} +1 & x^2 \equiv a \pmod p \text{ has a solution} \\ -1 x^2 \equiv a \pmod p \text{ has no solution} \end{cases}$$

Examples

- $(\frac{2}{7}) = +1$
- $(\frac{-1}{5}) = +1$
- $(\frac{2}{3}) = -1$

Proposition 13.3: For an odd prime p and $a, b \not\equiv 0 \pmod p$, we have

- *(a) Euler's Criterion*:

$$(\frac{a}{p}) \equiv a^{(p-1)/2} \pmod p$$

- *(b)

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$$

- *(c)*

$$a \equiv b \pmod p \implies (\frac{a}{p})(\frac{b}{p})$$

- *(d)*

$$(\frac{-1}{p}) = \begin{cases} +1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

Proof:

(a): Using Proposition 13.1, we know that

- If a is a square mod p, then $a^{(p-1)/2} \equiv +1 \equiv (\frac{a}{p}) \pmod p$
- If a is not a square mod p, then $a^{(p-1)/2} \equiv -1 \equiv (\frac{a}{p}) \pmod p$

(b): The congruence of *(a)* also holds for b, ab. Thus

$$(\frac{a}{p})(\frac{b}{p}) \equiv a^{(p-1)/2}b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv (\frac{ab}{p}) \pmod p$$

Since $-1 \not\equiv +1 \pmod p$ for $p \geq 3$, the congruence above must hold

(c): If $a \equiv b \pmod p$, then $x^2 \equiv a \pmod p$ has a solution if and only if $x^2 \equiv b \pmod p$ has a solution. This is what (c) is saying

(d): Note that $(p-1)/2$ is even if $p \equiv 1 \pmod 4$ and odd if $p \equiv 3 \pmod 4$. Thus

$$(\frac{-1}{p}) \equiv (-1)^{(p-1)/2} = \begin{cases} +1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

Note that $(\frac{x^2}{p}) = 1$ if $p \nmid x$ since x^2 will be a square mod p. Thus from part *(b)*, we have that

$$(\frac{x^2}{p}) = (\frac{x}{p})^2 = (\pm 1)^2 = 1$$

Theorem 13.4: For distinct odd primes p, q, we have

- *(a) Quadratic Reciprocity*:

$$(\frac{q}{p}) = (-1)^{(p-1)(q-1)/4}(\frac{p}{q}) = \begin{cases} (\frac{p}{q}) & p, \equiv 1 \pmod 4 \vee q \equiv 1 \pmod 4 \\ -(\frac{p}{q}) & p \equiv q \equiv 3 \pmod 4 \end{cases}$$

- *(b) Supplementary Law 1*:

$$(\frac{-1}{p}) = (-1)^{(p-1)/2} = \begin{cases} +1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

- *(c) Supplementary Law 2*:

$$(\frac{2}{p}) = (-1)^{(p^2-1)/8} = \begin{cases} +1 & p \equiv 1, 7 \pmod 7 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases}$$

Example: Is 23 a square mod 419?

$$
\begin{aligned}
(\frac{23}{419}) &= -(\frac{419}{23}) \quad \text{since } 23 \equiv 419 \equiv 3 \pmod 4 \\
&= -(\frac{5}{23}) \quad \text{since } 419 \equiv 5 \pmod{23} \\
&= -(\frac{23}{5}) \quad \text{since } 5 \equiv 1 \pmod 4 \\
&= -(\frac{3}{5}) \quad \text{since } 23 \equiv 3 \pmod 5 \\
&= -(\frac{5}{3}) \quad \text{since } 5 \equiv 1 \pmod 4 \\
&= -(\frac{2}{3}) \quad \text{since } 5 \equiv 2 \pmod 3 \\
&= -(-1) = +1 \quad \text{by Supplementary Law 2}
\end{aligned}
$$

Thus 23 is a square root mod 419

Non-Example: Is 295 a square mod 401?

$$(\frac{295}{401}) = (\frac{5}{401})(\frac{59}{401})$$

Where

$$(\frac{5}{401}) = (\frac{401}{5}) = (\frac{1}{5}) = +1 \qquad (\frac{59}{401}) = (\frac{401}{59}) = (\frac{47}{59}) = -(\frac{59}{47}) = -(\frac{12}{47}) = -(\frac{12}{47}) = -(\frac{4}{47})(\frac{3}{47}) = -(\frac{3}{47}) = +(\frac{47}{3}) = (\frac{2}{3}) = -1$$

Thus

$$(\frac{295}{401}) = (+1)(-1) = -1$$

Thus 295 is not a square mode 401

Consider: For which primes p is 5 a square mod p?

To answer this, we look at 5 mod p for each p and get a list of primes. By Quadratic Reciprocity

$$(\frac{5}{p}) = (\frac{p}{5}) = \begin{cases} +1p & \equiv \pm 1 \pmod 5 \\ -1 & p \equiv \pm 2 \pmod 5 \end{cases}$$

Thus the primes for which 5 is a quadratic residue form congruence classes

$$p \equiv 1 mod 5 \qquad p \equiv 4 \mod 5$$

Consider: For which primes p is 3 a square mod p

The answer to this depends on p mod 12

- If $p \equiv 1 \pmod{12}$, then

$$(\frac{3}{p}) = (\frac{p}{3}) = (\frac{1}{3}) = +1$$

- If $p \equiv 5 \pmod{12}$, then

$$(\frac{3}{p}) = (\frac{p}{3}) = (\frac{2}{3}) = -1$$

- If $p \equiv 7 \pmod{12}$, then

$$(\frac{3}{p}) = -(\frac{p}{3}) = -(\frac{1}{3}) = -1$$

Thus we need to consider the congruence class of p both mod 3 and mod 4 $\implies$ we are looking at p mod 12

This wasn't necessary in the previous case since $5 \equiv 1 \pmod 4$ and $3 \equiv 3 \pmod 4$, so a negative sign never occurs in Quadratic Reciprocity

Upshot: For a prime p, when asking if a is a square mod p, the answer depends only on the congruence class of p mod $4a$

11.2 Computing Square Roots Mod p

Proposition 13.5: Let $p \equiv 3 \pmod 4$ be prime and take $x \not\equiv 0 \pmod p$. Then exactly one of x or $-x$ is a square mod p. Let

$$y \equiv x^{(p+1)/4} \pmod p \implies y^2 \equiv \pm x \pmod p$$

Proof: Since $p \equiv 3 \pmod 4$, by Proposition 13.3, we have that $(\frac{-1}{p}) = -1$. Thus

$$(\frac{-x}{p}) = (\frac{-1}{p})(\frac{x}{p}) = -(\frac{x}{p})$$

Therefore exactly one of $(\frac{x}{p})$ and $(\frac{-x}{p})$ is $+1$ and the other is -1

Thus exactly one of x and $-x$ is a square mod p

Now let $y \equiv x^{(p+1)/4}$. Then

$$y^2 \equiv (x^{(p+1)/4})^2 \equiv x^{(p+1)/2} \equiv x^{(p-1)/2}x \equiv (\pm 1)x \pmod p$$

since $x^{(p-1)/2} \equiv \pm 1$ by Proposition 13.1

Proposition 13.6: Let $p \equiv 5 \pmod 8$ be prime and take $x \not\equiv 0 \pmod p$. If $x \equiv y^2 \pmod p$, then

$$y \equiv \begin{cases} \pm x^{(p+3)/8} & x^{(p-1)/4} \equiv 1 \pmod p \\ \pm 2^{(p-1)/4}x^{(p+3)/8} & x^{(p-1)/4} \equiv -1 \pmod p \end{cases}$$

Proof: Since $x^{(p-1)/4} \equiv y^{(p-1)/2} \equiv \pm 1 \pmod p$, so the cases above are the only possibilities

- Assume that $x^{(p-1)/4} \equiv 1$. Then we see that

$$(x^{(p+3)/8})^2 \equiv x^{(p+3)/4} \equiv x^{(p-1)/4}x \equiv x \equiv y^2 \pmod p \implies \pm x^{(p+3)/8} \equiv y \pmod p$$

- Assume that $x^{(p-1)/4} \equiv -1$. Then we see that

$$(2^{(p-1)/4}x^{(p+3)/8})^2 \equiv 2^{(p-1)/2}x^{(p-1)/4}x \equiv (\frac{2}{p})(-1)y^2 \equiv y^2 \pmod p$$

Thus by Supplementary Law 2, we have that $(\frac{2}{p}) = -1$ when $p \equiv 5 \pmod 8$

Thus the formula in the proposition holds