MAT315 Elementary Number Theory Notes (2021 Summer)

Jiaqi Bi, University of Toronto

June 17, 2021

Preface

This typesetting note is intended for academic communication and not-for-profit knowledge sharing. Any institutions or individuals **SHOULD NOT** reproduce or use this note in any form for operational or commercial purposes. This note contains some of the lecture notes instructed by Dr. Gaurav Patil and personal research notes. The author holds the right of the prosecution for any above behaviors. Moreover, this note should not be used as a substitution for the current user's attending lecture or textbook. I strongly recommend the user combine the note with your textbook and lecture to understand the content thoroughly. I hope anyone using this note can have a better understanding of the Elementary Number Theory topic. Students using this copy should not conduct any academic infractions, including but not limited to reproducing, failure of citations, and using this copy in any forms of academic dishonesty mentioned by the University of Toronto. For specific details of academic integrity, please visit https://www.academicintegrity.utoronto.ca/.

Contents

1 Number Theory Course Introduction **4**

2 Logistics **6**

3 Division Algorithm, Bezout's Identity, and Euclid's Algorithm **7**

4 Discussion on Euclid's and Aryabhata's Algorithm **9**

5 Prime Numbers and Unique Factorization **10**

6 Primes, Their Distributions, etc. **13**

7 Congruences **15**

8 Congruences 2: Chinese Remainder Theorem and Others **16**

9 Congruences 3 **20**

10 Periodic Sequences Modulo a composite n **23**

11 Computing Large Powers in Modular Arithmetic **29**

12 Computing $\varphi(n)$, Show Existence of Primitive Roots **31**

1 Number Theory Course Introduction

What is a proof?

- Deductive argument, usually ends with Q.E.D

Method for deciding legitimacy:

- Lack of negative evidence on active search (Scientific)

What does this mean in mathematics? (Proof symbols)

$\boxed{p \implies q}$

- If p is true, and q is true, then $p \implies q$ is true.
- If p is false, and q is true, then $p \implies q$ is true.
- If p is true, and q is false, then $p \implies q$ is false.
- If p is false, and q is false, then $p \implies q$ is true.

$\boxed{p \iff q}$

- If p is true, and q is false, then $p \iff q$ is false.
- If p is false, and q is true, then $p \iff q$ is false.
- If p is true, and q is true, then $p \iff q$ is true.
- If p is false, and q is false, then $p \iff q$ is true.

Proof Deductive Arguments

Example 1.1. *Prove* $n^2 + n + 41$ *is prime for all* $n \in \mathbb{N}$ *is false*

Proof.

Put $n = 1 : 43$, it is prime!

Put $n = 2 : 4 + 2 + 41 = 47$, it is prime!

...

Put $n = 41 : 41^2 + 41 + 41 = 41(41 + 1 + 1) = 41 \cdot 43$, not prime!

So, we found a counter example to disprove the above claim.

□

Interesting Question: When $n = 40 : 40^2 + 40 + 41 = 1681$, is it prime?

Another interesting question: Prove or disprove the following argument: Number of primes $\leq n < \frac{n}{\ln n}$

Peano's Axioms

1. 0 is a natural number

2. Every natural number n has an accessor $S(n)$:

$$0,\ S(0),\ S(S(0)),\ ...$$

3. Natural numbers m and n satisfy $m = n$ if and only if $S(m) = S(n)$, i.e., S is an injection.
4. For every natural number $S(n) = 0$ is false.
5. (Induction/Wellordering Axiom)

$$(0,\ S(0),\ S(S(0)),\ ...$$
$$r,\ S(r),\ SS(r),\ ...)$$

$$\mathbb{N} \sqcup \mathbb{N}$$

$$\left.\begin{array}{l} 0 \in K \\ n \in K \implies S(n) \in K \end{array}\right\} \text{Induction}$$

$\implies \mathbb{N} \subseteq K$

$\iff$ Every subset of natural numbers must have a smallest element. (Well Ordering Principle)

Example 1.2. Define Additive:

- $a + 0 = a$
- $a + S(b) = S(a + b)$

Define Multiplication:

- $a \cdot 0 = 0$
- $a \cdot S(b) = a + a \cdot b$

Let's say 1 is defined as $S(0)$, prove that $a \cdot 1 = a$.

Proof. $a \cdot 1 = a \cdot S(0) = a + a \cdot 0 = a + 0 = a$

□

2 Logistics

Divisibility

Work in $\mathbb{Z}$-any variable defined varies over integers.

1. $a|b$ and $b \neq 0$ implies that $|a| \leq |b|$
2. $a|b$ and $a|c$ then $a|bx + cy$ for any $x,\ y$
3. $a|a$
4. $a|b$ and $b|c \implies a|c$
5. $a|b$ and $b|c \implies a = \pm b$

Definition 2.1. We say $a|b$ if $b = ac$ for some integer c.

Lemma 2.2. Division Algorithm For any integers $a,\ b$, we can find a unique pair $(q,\ r)$ of non-negative integer satisfying:

1. $b = aq + r$
2. $0 \leq r < a$

Proof. $S = \{n \in \mathbb{N} : na > b\}$ by well-ordering principle, this set must have a minimal element say t.
$\implies t \cdot a > b > (t-1) \cdot a$
Note that since b is positive, $t \neq 0, \implies t \geq 1 \implies q = t - 1 \geq 0$
This is equivalent to $a > b - qa \geq 0 \implies a > r \geq 0$
Uniqueness: Assume $b = q_1 a + r_1,\ b = q_2 a + r_2$ such that $0 \leq r_1,\ r_2 < a$, $q_1 a + r_1 = q_2 a + r_2$
$\implies a(q_1 - q_2) = r_2 - r_1 \implies a > r_2 \geq r_2 - r_1 \geq 0$, $r_2 - r_1$ is a multiple of a between $a \cdot 0$ and $a \cdot 1 \implies r_2 - r_1 = a \cdot 0 \implies r_2 = r_1 \implies a \cdot (q_1 - q_2) = 0 \implies \begin{cases} a \neq 0 \\ q_1 = q_2 \end{cases}$

□

3 Division Algorithm, Bezout's Identity, and Euclid's Algorithm

Division Algorithm

Definition 3.1. If $a, b \in \mathbb{Z}$ with $b \neq 0$, then there exists q, r (uniquely) satisfying $a = bq + r$ and $0 \leq r < b$

Exercise 3.2. Try to prove or disprove: If $7 \nmid n$ then $7|n^3 + 1$ or $7|n^3 - 1$

Exercise 3.3. If $d \neq 0$, show that the remainder when a product of numbers is divided by d is the same as the remainder of the product of remainders when each of the initial numbers is divided by d.

Definition 3.4. The Greatest Common Divisor of 2 integers, say $a,\ b$, is written as $\gcd(a,\ b)$ or simply $(a,\ b)$. We say d is the GCD of a and b if

1. $d|a$ and $d|b$
2. $c|a$ and $c|b$, that $c \leq d$

Bezout's Identity
$(a, b) = ax + by$ for some integers x, y

Proof.

$$S = \{ax + by : x, y \in \mathbb{Z}\}$$

$$S \cap \mathbb{N}/\{0\} = \{ax + by : ax + by > 0, x, y \in \mathbb{Z}\} \subseteq \mathbb{N}$$

If this set is non-empty then it must have a smallest element $|a| \subseteq S \cap \mathbb{N}/\{0\}$
(If $a < 0$ then $-a \in S \cap \mathbb{N}/\{0\}$, if $a > 0$ then $a \in S \cap \mathbb{N}/\{0\}$)
Let the smallest element be d, (clearly, $d > 0$) in $S \cap \mathbb{N}/\{0\}$

1. $d = ax_0 + by_0$
2. Notice that if some elements of S are not divisible by d, say $ax_1 + by_1 = dq + r$, where $0 < r < d$

These imply to $r = ax_1 + by_1 - q(ax_0 + by_0) = a(x_1 - qx_0) + b(y_1 - qy_0)$.
$\implies r \in S$, and $r > 0$ and $r < d$. $\implies r \in S \cap \mathbb{N}/\{0\}$.
Contradiction to the smallest of d.

d divides every element of S, this implies to $d|a$ and $d|b$. Assume $c|a$ and $c|b$, this goes to $a = cr, b = cs$. Since $d = ax_0 + by_0$, then $c|d, \implies c \leq d$ $\implies c(rx_0 + sy_0) \implies c|d \implies 0 \leq d$.
This d is a linear combination of a and b, which is (a, b)

□

Lemma 3.5. $a|bc$ and $(a, b) = 1$, then $a|c$

Proof. Since $(a, b) = 1$, by Bezout's identity, one can find $x_0, y_0 \in \mathbb{Z}$ such that $ax_0 + by_0 = 1$. Multiply by c:

$$acx_0 + bcy_0 = c$$

Note that $a|ac$ and $a|bc$, or say $bc = ar$. Then simply this implies to $c = acx_0 + ary_0 = a(cx_0 + ry_0)$

□

Definition 3.6. We say a and b are coprime (relative prime) if $(a, b) = 1$.

Definition 3.7. $\text{lcm}(a, b)$ is the least common multiple of a and b

Redefining primes lemma

Lemma 3.8. p is a prime number $\iff (p|ab \implies p|a$ or $p|b)$, $(p \geq 2)$

Proof. $(\Rightarrow)$

p is a prime and $p|ab$

Case 1: $p \mid a$, we are done!

Case 2: $p \nmid a$, since p is a prime, then the only positive divisors of p are 1 and p. This implies to $(p, a)/p$ and $(p, a)/a$, the GCD must be 1 or p. But $p \nmid a$ so $(p, a) \neq p$, so $(p, a) = 1$.

Bezout's Identity tells us that $px_0 + ay_0 = 1$, $pbx_0 + aby_0 = b$ since $p \mid pb$ and $p \mid ab$, this implies to $p \mid b$.

$(\Leftarrow)$ $(p \mid ab \implies p \mid a$ or $p \mid b)$.

We want to show p is a prime. Assume p is not a prime, $p = xy$ such that $1 < x, y < p$. $p \mid xy \implies p \mid x$ or $p \mid y \implies x \geq p$ or $y \geq p$. This directly contradicts to $1 < x, y < p$.

□

Lemma 3.9. (Recall) If a, b are positive integers, and $a \mid b \implies a \leq b$.

Lemma 3.10. $(a, b) = (a, b + a_n)$ for any integer n

Think of a way to use this to find GCD of 3054 and 12378. Hint: if $m \mid n$ and $n \mid m$ then $m = \pm n$. Modified if $m, n \geq 1$ and $m \mid n$, and $n \mid m$ then $m = n$.

Proof. $(a, b) \mid a$ and $(a, b) \mid b \implies (a, b) \mid b \cdot 1 + a \cdot n \implies (a, b) \mid (a, b+an) = ax_0 + (b+an)y_0$. Then, $(a, b+an) \mid a$ and $(a, b+an) \mid b+an \implies (a, b+an) \mid (b+an) \cdot 1 = a \cdot n \implies (a, b+an) \mid (a, b) = ax_0 + by_0$. Thus, $(a+bn) = (a, b)$ as both are greater or equal to 1. □

Exercise 3.11. Using lemma 3.10, try to find $(3054, 12378)$.

4 Discussion on Euclid's and Aryabhata's Algorithm

Euclid's Algorithm

Definition 4.1. A very efficient way to calculate greatest common divisors, published in Book VII of Euclid's Elements around 300 BC). The formula can be expressed as follows (You may not see this in any lectures or in the textbook, but I generated for you):

$$
\begin{array}{lll}
q_1 = \lfloor \frac{a}{b} \rfloor & a = bq_1 + r_1 & r_1 = a - bq_1 \\
q_2 = \lfloor \frac{b}{r_1} \rfloor & b = q_2 r_1 + r_2 & r_2 = b - q_2 r_1 \\
q_3 = \lfloor \frac{r_1}{r_2} \rfloor & r_1 = q_3 r_2 + r_3 & r_2 = r_1 - q_3 r_2 \\
q_4 = \lfloor \frac{r_2}{r_3} \rfloor & r_2 = q_4 r + r_4 & r_4 = r_2 - q_5 r_3 \\
\ldots & \ldots & \ldots \\
q_n = \lfloor \frac{r_{n-1}}{r_{n-1}} \rfloor & r_{n-2} = q_n r_{n-1} + r_n & r_n = r_{n-2} - q_n r_{n-1} \\
q_{n+1} = \lfloor \frac{r_{n-1}}{r_n} \rfloor & r_{n-1} = q_{n+1} r_n + 0 & r_n = r_{n-1}/q_{n+1}
\end{array}
$$

There is a very close relationship between Euclid's Algorithm and Chinese Remainder Theorem, that we will discuss this theorem in next a few sections with Congruence.

Diophantine Equation

Definition 4.2. The simplest linear Diophantine equation is $ax + by = c$

Think about this: Does $6x + 9y = 2$ have an integer solution? Try to solve it. Hint: $ax + by = c$ has an integer solution if and only if $(a, b) \mid c$.

Equivalence Relations (Modulus)
Let's review some modulus knowledge from the prerequisite.

Definition 4.3. $a \equiv b \pmod{n}$ if $n \mid a - b$.

Exercise 4.4. Test these are equivalence relations:

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n} \implies b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$

Some properties:

1. $a \equiv b \pmod{n}$ if and only if the remainder of a when divided by n equals to the remainder of b when divided by n.
2. If $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$ then $ab \equiv cd \pmod{b}$.

5 Prime Numbers and Unique Factorization

Every number could be written as a product of smaller and smaller numbers. We will discuss about breaking the number to smaller primes.

Definition 5.1. We say p is a prime number if $p > 1$ and only positive divisors of p are 1 and p.

Corollary 5.2. If n is composite (not prime) then n has a prime divisor less than or equal to $\sqrt{n}$

Proof. Since n is composite, then n has a divisor, say r, which is neither 1 nor n, $n = rk$ with $1 < r < n$, then $1 < k < n$. Can both r and $k > \sqrt{n}$? If $r > \sqrt{n}$, $k > \sqrt{n}$, then $n = r \cdot k > \sqrt{n} \cdot \sqrt{n} = n$. n should not be greater than n, so it's contradiction. One of r and k must be less or equal to $\sqrt{n}$, without loss of generality, let $r \leq \sqrt{n}$, $1 < r < \sqrt{n} \implies r$ has prime divisor, say p (This has been shown in the section 1). Then $1 < p \leq r \leq \sqrt{n}$, $p \mid r \mid n \implies p \mid n$ and $1 < p \leq \sqrt{n}$. □

Example 5.3. Is 307 a prime? What about 401?
Solution: Note that $289 < 307 < 324$, that is, $17^2 < 307 < 18^2 \implies 17 < \sqrt{307} < 18$. If 307 were composite then some prime less than 17 would divide: $2, 3, 5, 7, 11, 13, 17$. Therefore 307 is a prime. Try to do 401 by yourself.

Fundamental Theorem of Arithmetic

Definition 5.4. If $n > 1$, then n can be written as a product of prime uniquely (up to order)

Example 5.5. $6 = 2 \times 3 = 3 \times 2$

Corollary 5.6. If $n > 1$, then $n \geq p_1 p_2 ... p_n$ such that $p_1 \leq p_2 \leq p_3 \leq ... \leq p_n$ (p_i- primes). Furthermore, if $n = p_1 p_2 ... p_k = q_1 q_2 ... q_r$ where $p_i's$ and $q_i's$ are primes, and $p_1 \leq p_2 \leq p_3 \leq ... \leq p_n$ and $q_1 \leq q_2 \leq ... \leq q_r$, then $r = k$, and $p_1 = q_1$, $p_2 = q_2$, $p_3 = q_3 ...$

Proof. If n is a prime, $n = p$, you are done. If n is not a prime, then n has prime divisor, say p. Then $n = p \cdot r$ where $1 < r < n$. If one has prime factorization for all integers in 1 to $n - 1$, then $r = q_1, q_2, ..., q_k$, $n = p \cdot r = p_1 q_1 ... q_k$, each of $q_i \mid n$. This implies to $p \leq q_i \implies n = p q_1 q_2 ... q_k$ when $p \leq q_1 \leq q_2 ... \leq q_k$.

$n = q_1 r_1$, if $r_1 = 1$, we are done! If $r_1 \neq 1$, r_1 has a prime divisor.

$n = q_1 q_2 r_2$, if $r_2 = 1$, we are done. If $r_2 \neq 1$, r_2 has a prime divisor.

...
$r_1 > r_2 > r3 ...$

Uniqueness: $n = q_1 q_2 ... q_k = p_1 p_2 ... p_r$ where p_i and q_i are all primes, with $p_1 \leq p_2 \leq ... \leq p_r$ and $q_1 \leq q_2 \leq ... \leq q_k$. Let p denote the smallest prime dividing n, will show $p = q_1 = p_1$.

(Lemma: $p \mid q_1, q_2, ..., q_k$ then p must divide one of $a_1, ..., a_r$)
$p \mid (q_1)(a_2...a_k) \implies p \mid a_1$ or $p \mid a_2(...a_k) \implies p \mid a_2$ or $p \mid a_3...a_r$. $p \mid n = q_1q_2...q_r = p_1p_2...p_k$. This implies to $p \mid q_1q_2...q_r$ and $p \mid p_1p_2...p_k$. So, p divides one of $q_1, q_2, ..., q_r$ and p divides one of $p_1, p_2, ..., p_k$. This implies to $p \leq q_1 \leq q_2... \leq q_r$, and $p \leq p_1 \leq p_2... \leq p_k$. ($p_i's$ and $q_i's$ are prime divisors of n and p is the smallest prime divisor) If $p < q_1$, then $p < q_i$ for each i, so $p \nmid q_i$ for any i. Contradiction. Therefore, $p = q_1$, and $p = p_1$. Then $p_1 = q_1 = p$, this implies to $\frac{n}{p} = p_2...p_k = q_1...q_r \implies p_2 = q_2, p_3 = q_3, ...$ (Inductive hypothesis) □

Proof of infinitude of prime numbers

As we know, there are infinitely many prime numbers in the math world, and mathematicians have tried to prove this thing. One of the most famous technique is called Euclid's Proof. The details of these proofs can be easily found online.

Fundamental Theorem of Arithmetic

$$a = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r} \qquad b = q_1^{\beta_1}q_2^{\beta_2}...q_r^{\beta_r}$$

In terms of prime factorization,

- What does ab look like?
- What does $b \mid a$ look like?
- What does (a, b) look like?
- What does a^m look like?

Example 5.7. Examples of $a = 2^3 \cdot 3^2 \cdot 5$, $b = 3^1 \cdot 5^2 \cdot 7$.

$$\begin{aligned} a^5 &= (2^3 \cdot 3^2 \cdot 5)^5 \\ &= 2^{3\cdot5} \cdot 3^{2\cdot5} \cdot 5^5 \end{aligned} \qquad \begin{aligned} ab &= (2^3 \cdot 3^2 \cdot 5) \cdot 3 \cdot 5^2 \cdot 7^2 \\ &= 2^{3+0} \cdot 3^{2+1} \cdot 5^{1+2} \cdot 7^2 \\ &= 2^{3+0} \cdot 3^{2+1} \cdot 5^{1+2} \cdot 7^{0+2} \end{aligned}$$

Continued on FTA

Rewrite factorization of a and b in terms of all primes dividing both a and b, using 0 as exponent when necessary.

$$a = p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r} \qquad b = p_1^{\beta_1}p_2^{\beta_2}...p_r^{\beta_r}$$

$$ab = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} ... p_r^{\alpha_r+\beta_r}$$

$b \mid a$ if $\beta_i \leq \alpha_i$ for all i,

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} ... \qquad \text{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} ...$$

Theorem 5.8. $\text{lcm}(a,b)(a,b) = |ab|$

Proof. Using FTA, we can find $\text{lcm}(a,b)(a,b) = p_i^{\min(\alpha,\beta)+\max(\alpha,\beta)} = p_i^{\alpha+\beta} = |ab|$ for all $i \in \mathbb{Z}$.

□

Corollary 5.9. Using the FTA, $\frac{ab}{(a,b)}$ is the least common multiple.

Proof.

$$\frac{ab}{(a,b)} = a(\frac{b}{(a,b)}) = b(\frac{a}{(a,b)}) \implies \text{least common multiple of } (a,b) \leq \frac{ab}{(a,b)}$$

On the other hands,

$$a = (a,b)r \qquad b = (a,b) = s, \text{where } (r,s) = 1$$

$$a = (a,b)r \mid \text{lcm}(a,b) = (a,b)rm \implies \text{lcm}(a,b) = (a,b)rm$$

$$\begin{aligned}
&\implies (a,b)s \mid (a,b)rm \text{ since } (r,s) = 1 \\
&\implies s \mid m \\
&\implies m = sk \\
&\implies \text{lcm}(a,b) \\
&= (a,b)rsk \text{ for some integer } k \\
&= \frac{(a,b)r(a,b)sk}{(a,b)} \\
&= \frac{ab}{(a,b)} \cdot k \implies \frac{ab}{(a,b)} \mid \text{lcm}(a,b)
\end{aligned}$$

□

6 Primes, Their Distributions, etc.

Infinitude of primes

Let's talk about Euclid's proof: $p_{k+1} \leq p_1 p_2 ... p_k + 1$

$\pi(x) :=$ number of $\{p \in \mathbb{N} \mid p \text{ is a prime and } p \leq x\}$, so we have:

$$\pi(2) = 1$$

$$\pi(3.5) = 2$$

$$\pi(100) = 25$$

$$\pi(10^3) = 168...$$

Example 6.1. If $p_1 = 2, p_2 = 3, ...$ then show that $p_k \leq 2^{2^{k-1}}$.

Proof. Base Case: $k = 1$, $p_1 = 2 \leq 2^{2^0} = 2$
Induction Hypothesis: $p_r \leq 2^{2^{r-1}}$ when $1 \leq r \leq k$.
Then we have

$$p_{k+1} \leq p_1 p_2 ... p_k + 1 \leq 2^{2^{1-1}} \cdot 2^{2^{2-1}} \cdot 2^{2^{3-1}} ... 2^{2^{k-1}} + 1$$

That is,

$$p_{k+1} \leq 1 + 2^{2^0} \cdot 2^{2^1} \cdot 2^{2^2} ... = 2^{2^0 + 2^1 + ... + 2^{k-1}} + 1$$

Recall that $2^0 + 2^1 + 2^2 + ... = 2^{2^0 + 2^1 + ... + 2^{k-1}} + 1$, and $1 \leq 2^{2^k} \cdot \frac{1}{2}$ so

$$\begin{aligned} p_{k+1} &\leq 2^{2^k - 1} + 1 \\ p_{k+1} &\leq 2^{2^k} \cdot \frac{1}{2} + 1 \\ p_{k+1} &\leq 2^{2^k} \cdot \frac{1}{2} + 2^{2^k} \cdot \frac{1}{2} = 2^{2^k} \end{aligned}$$

if $\pi(x) = k$ then $p_{k+1} \geq x$, (if $p_{k+1} \leq x$ then $\pi(x) \geq k + 1$). This implies to $2^{2^k} \geq p_{k+1} \geq x \implies k \geq \ln \ln(x)$. Thus, $\pi(x) \geq \ln \ln(x)$.

□

Exercise 6.2. Show that if $2^m + 1$ is a prime, then $m = 2^k$ for some k.

Hint: $a^d + b^d = (a + b)(a^{d-1} - a^{d-2} \cdot b + ... + b^{d-1})$ when d is odd. That is, $a + b \mid a^d + b^d$ when d is odd. However, you may find a negation to disprove this. I strongly suggest you to try this before continuing reading.

Example 6.3. Fermat's saying $2^{2^k} + 1$ is prime. People found it is not true, consider $2^{2^5} + 1$.

Exercise 6.4. Using unique factorization, show that every positive integer can be written as a product sn^2 (where s is a product of distinct primes or 1) uniquely.

7 Congruences

Definition 7.1. $a \equiv b \pmod{n}$ or $a \equiv_n b \pmod{n}$ if $n \mid a - b$

Definition 7.2. $a \equiv b \pmod{n}$ if and only if the remainder when a is divided by n is same as when b is divided by n.

Corollary 7.3. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

1. $a + c \equiv b + d \pmod{n}$
2. $ac \equiv bd \pmod{n}$

Proof. 1. $n \mid a - b$ and $n \mid c - d \implies n \mid a - b + c - d \implies n \mid a + c - (b + d) \implies a + c \equiv b + d \pmod{n}$

2. $n \mid a-b$ and $n \mid c-d \implies n \mid (a-b)c \implies n \mid ac-bc, n \mid (c-d)b \implies n \mid bc - bd$ then this gives $n \mid ac - bc + bc - bd \implies n \mid ac - bd \implies ac \equiv bd \pmod{n}$

□

Lemma 7.4. Langrange's Lemma if $q \mid 2^p - 1$ then $p \mid q-1$, $q \mid 2^{p_k} - 1 \implies p_k \mid q - 1 \implies q - 1 \geq p_k \implies q > p_k$ and q is a prime.

Think about how to prove this?

Partition $\mathbb{Z}$

- Set $\{..., -2n, -n, 0, n, 2n, ...\}$ is called $n\mathbb{Z}$.
- Set $\{..., -2n + 1, -n + 1, 1, n + 1, ...\}$ is called $n\mathbb{Z} + 1$. Note that a, b are in $n\mathbb{Z}$ or $n\mathbb{Z} + 1$, which implies to $a \equiv b \pmod{n}$.
- Set $\{..., -2n + i, -n + i, i, n + i, 2n + i, ...\}$ is called $n\mathbb{Z} + i$.
- $n\mathbb{Z} + a = n\mathbb{Z} + b$ if and only if $n \mid a - b$.
- $n\mathbb{Z} + a \cap n\mathbb{Z} + b = \{\emptyset\}$ or $n\mathbb{Z} + a = n\mathbb{Z} + b$.

Then think about the Lagrange's Lemma. Hint: Fix $\equiv_n$, a and $b \in \mathbb{Z}$, you can get $a + b \in \mathbb{Z}$.

8 Congruences 2: Chinese Remainder Theorem and Others

Note that the use of $\equiv_n$ and $\equiv \pmod{n}$ is the same. Equivalence relation divided $\mathbb{Z}$ in to n partitions.

Arithmetic on these n-parts

Example 8.1. $2x + 3 = 0$, we know the solution is in rational number ($\mathbb{Q}$).
$2(x + \frac{3}{2}) = 0$, recall that if $ab = 0$, then $a = 0$ or $b = 0$.
$x + \frac{3}{2} = 0 \implies x = \frac{-3}{2}$, used the cancellation of 2 on both sides.

Example 8.2. $x^2 - 4 = 0 \implies (x + 2)(x - 2) = 0 \implies x = \pm 2$, used difference of squares and the same algorithm as example 8.1.

Arithmetic on partitions (by $\equiv_n$, $\mathbb{Z}/n\mathbb{Z}$)

Example 8.3. $ax \equiv b \pmod{n}$, when does this have solution? How many solutions in $\mathbb{Z}/n\mathbb{Z}$ does this have?
$ax \equiv b \pmod{n}$ if and only if $\exists y_0$ s.t. $ax - b = ny_0$. This implies to $ax \equiv b \pmod{n}$ has a solution. $\iff ax - ny = b$ has a solution $\iff (a, n) \mid b$. If x_0 is a solution, all other possible solutions given by $x_0 + k \cdot (\frac{n}{(n,a)})$, set $\frac{n}{(n,a)}\mathbb{Z} + x_0$, (n, a) solution when $(n, a) \mid b$ in $\mathbb{Z}/n\mathbb{Z}$.

Example 8.4. $ab = 0 \iff a = 0, b = 0$, find a contradiction example in congruences for this property?

$$\begin{aligned} 2 \cdot 3 &\equiv 0 \pmod{6} \\ 2 &\not\equiv 0 \pmod{6} \\ 3 &\not\equiv 0 \pmod{6} \end{aligned}$$

$$ab \equiv 0 \pmod{n} \implies \frac{b}{(a,n)} \equiv 0 \pmod{\frac{n}{(a,n)}}$$

Example 8.5. Solve $x^2 \equiv 1 \pmod{4}$.
Solution is all odd numbers, or $x \equiv 1 \pmod{2}$, or $2\mathbb{Z}+1$, or $\{2\mathbb{Z}+1, 2\mathbb{Z}-1\}$.

Chinese Remainder Theorem

By Sun Tsu.

Find numbers which when divided by $3, 5, 7$, leave remainders $1, 2, 3$ respectively. In math writing, Solve for x:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 2 \pmod 5 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Example 8.6. Find integer N, such that

$$\begin{aligned} N &\equiv 5 \pmod{23} \\ N &\equiv 3 \pmod 7 \end{aligned}$$

Solution:

$$23 \mid N - 5 \iff \exists r, s.t., N = 23r + 5$$

$$7 \mid N - 3 \iff \exists s, s.t., N = 7s + 3$$

In order to find N, we need to find r and s. That is, we rewrite the equation to

$$23r + 5 = 7s + 3 \implies 23r - 7s = -2$$

Using the Euclidean Algorithm, we can easily solve this equation for integer solutions:

$$-2 = -7 \cdot 20 + 23 \cdot 6$$

So, $r = 6$, $s = 20$ is a solution. Thus, $N = 7 \cdot 20 + 3 = 143$ is a solution. In order to find other solutions say N', we need $23 \mid N' - 143$ and $7 \mid N' - 143$. So,

$$\text{lcm}(23, 7) \mid N' - 143 \implies 23 \cdot 7 \mid N' - 143$$

In other words, all solutions are in $23 \cdot 7\mathbb{Z} + 143$:

$$x \equiv 143 \pmod{23 \cdot 7}$$

Example 8.7. Lagrange Interpolation Example: Find a polynomial with rational coefficient such that $f(1) = 2$, $f(2) = 3$, $f(3) = 1$.

Theorem 8.8. Lagrange Polynomial Given a set of $k+1$ data points

$$(x_0, y_0), ..., (x_j, y_j), ..., (x_k, y_k)$$

where no two x_j are the same, the Lagrange interpolation polynomial is a linear combination:

$$L(x) := \sum_{j=0}^{k} y_j \ell_j(x)$$

of Lagrange basis polynomials

$$\ell_j(x) = \prod_{\substack{0 \le m \le k \\ m \ne j}} \frac{x - x_m}{x_j - x_m} = \frac{(x - x_0)}{(x_j - x_0)} ... \frac{(x - x_{j-1})}{(x_j - x_{j-1})} \frac{(x - x_{j+1})}{(x_j - x_{j+1})} ... \frac{(x - x_k)}{(x_j - x_k)}$$

where $0 \le j \le k$.

The proof of this theorem is out of scope of this course, and of course, my knowledge. But it is interesting, and you can find the proof of this theorem online.

Solution of Example 8.7, with the use of Theorem 8.8:

$$A(x-1)(x-2) + B(x-1)(x-3) + C(x-2)(x-3) = f(x)$$

$$f(1) = 2 \iff C(1-2)(1-3) = 2 \implies C = 1$$

$$f(2) = 3 \iff B(2-1)(2-3) = 3 \implies B = -3$$

$$f(3) = 1 \iff A(3-1)(3-2) = 2 \implies A = \frac{1}{2}$$

$$f(x) = \frac{1}{2}(x-1)(x-2) + (-3)(x-1)(x-3) + 1(x-2)(x-3)$$

Definition 8.9. If you have integers $n_1, n_2, ..., n_r$ such that $(n_i, n_j) = 1$, then

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &... \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a unique solution modulo $N = n_1 n_2 ... n_r$. Note that, x can be solved by

$$x = a_1 N_1 y_1 + a_2 N_2 y_2 + ... + a_r N_r y_r$$

With the solution of y_i can be found by

$$\begin{aligned} N_1 y_1 &\equiv 1 \pmod{n_1} \\ N_2 y_2 &\equiv 1 \pmod{n_2} \\ &... \\ N_r y_r &\equiv 1 \pmod{n_r} \end{aligned}$$

that just solve for y_i respectively.

Example 8.10. Solve for the question raised by Sun Tsu:

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

Solution: We have $N = 3 \cdot 5 \cdot 7 = 105$, $N_1 = 105/3 = 35$, $N_2 = 105/5 = 21$, $N_3 = 105/7 = 15$. To get y_1, solve for $35y_1 \equiv 1 \pmod 3$, or equivalently, solve for $2y_1 \equiv 1 \pmod 3$, then we get $y_1 \equiv 2 \pmod 3$. Solve for $21y_2 \equiv 1 \pmod 5$, we get $y_2 \equiv 1 \pmod 5$. Finally, $15y_3 \equiv 1 \pmod 7$, we get $y_3 \equiv 1 \pmod 7$. Hence,

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv 52 \pmod{105}$$

We can easily check that x satisfies $x \equiv 52 \pmod{105}$ is the solution, check:

$$52 \equiv 1 \pmod 3$$

$$52 \equiv 2 \pmod 5$$

$$52 \equiv 3 \pmod 7$$

Exercise 8.11. Solve for x:

$$2x \equiv 1 \pmod 5$$
$$3x \equiv 1 \pmod 7$$
$$7x \equiv 1 \pmod 2$$

Theorem 8.12. Different Statement of Chinese Remainder Theorem
If $n_1, ..., n_r$ are pairwise coprime integers, then $\mathbb{Z}/N\mathbb{Z}$ is in bijective correspondence with

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z}... \times \mathbb{Z}/n_r\mathbb{Z}$$

where $N = n_1, n_2, ..., n_r$.

Exercise 8.13. Find all solutions of $x^2 \equiv 1 \pmod 6$.

Exercise 8.14. Find all solutions of $x^2 \equiv 1 \pmod{23 \cdot 29}$. Hint: Use $x^2 \equiv 1 \pmod{23}$ and $x^2 \equiv 1 \pmod{29}$.

9 Congruences 3

What is the last digit of 3^{233}? It's equivalent to asking what is the remainder of 3^{233} when divided by 10.

$$3^1 \equiv 3 \pmod{10}$$
$$3^2 \equiv 9 \pmod{10}$$
$$3^3 \equiv 7 \pmod{10}$$
$$3^4 \equiv 1 \pmod{10}$$
$$3^5 \equiv 3 \pmod{10}$$
$$3^6 \equiv 9 \pmod{10}$$
$$3^7 \equiv 7 \pmod{10}$$
$$3^8 \equiv 1 \pmod{10}$$
$$...$$

It is not hard to discover:

$$\left.\begin{array}{llll} 3^k \equiv 3 & (\text{mod } 10) & (\text{if } k \equiv 1 & (\text{mod } 4)) \\ 3^k \equiv 9 & (\text{mod } 10) & (\text{if } k \equiv 2 & (\text{mod } 4)) \\ 3^k \equiv 7 & (\text{mod } 10) & (\text{if } k \equiv 3 & (\text{mod } 4)) \\ 3^k \equiv 1 & (\text{mod } 10) & (\text{if } k \equiv 0 & (\text{mod } 4)) \end{array}\right\} \text{Prove by induction}$$

We find that $233 = 4 \cdot 58 + 1$, so $3^{233} \equiv 3 \pmod{10}$

Claim 9.1. $a, a^2, a^3, ..., a^{n+1}$, $a^r \equiv a^s \pmod{n}$ for some $1 \leq r < s \leq n+1$.

Proof. Note if this is not true, then all of $a, a^2, ..., a^{n+1}$ must be different modulo. This implies to some two of these must have same remainder:

$$a^r \equiv a^s \pmod{n}$$

$$a^{r+1} \equiv a^{s+1} \pmod{n}$$

$$...$$

□

Example 9.2. Find (a, n) where sequence $a, a^2, ...$ is not periodic from the beginning.

Solution: $(2, 12)$, $2, 4, 8, 4, 8, 4, 8, ...$

Exercise 9.3. Classify all (a, n) such that sequence $a, a^2, ...$ mod n is not immediately periodic.

Definition 9.4. Fermat's Little Theorem

$$a^{p-1} \equiv 1 \pmod{p} \text{ for any } p \nmid a \text{ and } p - \text{prime}$$

OR

$$p \mid a^p - a \text{ for any } (a, p) \text{ where } p \text{ is a prime.}$$

Example 9.5. If $p = 3$, $a^2 \equiv 1 \pmod{3}$ if $3 \nmid a$

a	a^2	a^3
0	0	0
1	1	1
2	1	2

For $p = 5$:

a	a^2	a^3	a^4
0	0	0	0
1	1	1	1
2	4	3	1
4	1	4	1

If $p = 17$, $17 \mid 10^{16} - 1$, or $10^{16} \equiv 1 \pmod{17}$, $n = a_k 10^k + a_{k-1}10^{k-1} + \ldots \underbrace{\ldots + a_0 10^0}_{\text{17 digits}}$

Definition 9.6. Complete Residue System Mudulo We say a set of n numbers $a_1, a_2, ..., a_n$ is a complete residue system modulo n, if given any integer m,

$$m \equiv a_i \pmod{n} \text{ for some } i$$

Claim 9.7. If $(a, n) = 1$ and $\{a_1, ..., a_n\}$ is a residue system, then so is $\{aa_1, aa_2, ..., aa_n\}$.

Proof. We want to show $aa_i \not\equiv aa_j \pmod{n}$. If $aa_i \equiv aa_j \pmod{n}$ for some i and j, then $n \mid aa_i - aa_j = a(a_i - a_j)$. Then $n \mid a_i - a_j \implies a_i \equiv a_j \pmod{n}$. Contradiction to $\{a_1, ..., a_n\}$ is residue system. □

Example 9.8. Let p be a prime, show that if d is the smallest integer such that $a^d \equiv 1 \pmod{p}$ then $d \mid p - 1$.

Proof. Clearly, $d \leq p - 1$, let's say $p - 1 = d \cdot k + r$, where $1 \leq r \leq d - 1$, then $a^{p-1} \equiv a^{dk+r} \pmod{p} \equiv (a^d)^k \cdot a^r \pmod{p} \equiv a^r \pmod{p}$. This is contradiction to the "smallest" nature of the integer d. □

Example 9.9. Solve $x^{86} \equiv 6 \pmod{29}$

Solution: solution must satisfy $x^{28} \equiv 1 \pmod{29}$, why?

$$86 = 28 \cdot 3 + 2$$

$$x^{28 \cdot 3 + 2} \equiv (x^{28})^3 \cdot x^2 \pmod{29} \equiv x^2 \pmod{29}$$

So,

$$x^2 \equiv 6 \pmod{29}$$

Also, we have $64 \equiv 6 \pmod{29}$, so we will need to solve

$$x^2 \equiv 64 \pmod{29} \implies 29 \mid (x-8)(x+8)$$

Now since 29 is prime, $29 \mid x-8$ or $29 \mid x+8$. Thus, $x \equiv 8 \pmod{29}$ and $x \equiv -8 \pmod{29}$ are all solutions.

Exercise 9.10. $7^{1734250} \equiv 1660565 \pmod{1734251}$, what can you tell about 1734251?

10 Periodic Sequences Modulo a composite n

Recall: Fermat's Little Theorem
If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$ (for p-prime).

Definition 10.1. The period divides $p-1$.

Example 10.2. Consider $2, 2^2, 2^3, ... \pmod{5}$, it would be $2, 4, 3, 1, 2, 4, 3, 1, ...$ where the period is 4. $4 \mid 5-1$.

Example 10.3. Consider $4, 4^2, 4^3, ... \pmod{5}$, it would be $4, 1, 4, 1, ...$ where the period is 2. $2 \mid 5-1$.

So, $a^m \equiv 1 \pmod{n}$ only makes sense when $(a, n) = 1$. That is, when $\{1 \leq a < n : (a, n) = 1\}$ that $Ax \equiv 1 \pmod{n}$ has a solution.

Lemma 10.4. Given $a \not\equiv 0 \pmod{p}$, p is prime, you can find b such that $ab \equiv 1 \pmod{p}$.

Proof.

Method 1: $Ax \equiv B \pmod{N}$ has a solution if and only if $(A, N) \mid B$, $ax \equiv 1 \pmod{p}$ has a solution if and only if $(a, p) = 1 \mid 1$
Method 2: $0, a, 2a, ..., (p-1)a \pmod{p}$ and $0, 1, 2, ..., p-1 \pmod{p}$ are same up-to order changes.
Method 3: $a^{p-1} \equiv 1 \pmod{p}$ as Fermat's Little Theorem. $a(a^{(p-2)}) \equiv 1 \pmod{p}$

□

Note, congruence classes mod p behave more like rational.

$$ax \equiv b \pmod{n} \text{ and } (a, n) = 1$$

Find $at \equiv 1 \pmod{n}, t = a^{-1} \neq \frac{1}{a}, x \equiv bt \pmod{n}$.

Below is the set of relative prime number:

Set of Relative Prime Number		
Up-To	Set	Size
2	$\{1\}$	1
3	$\{1,2\}$	2
4	$\{1,3\}$	2
5	$\{1,2,3,4\}$	4
6	$\{1,5\}$	2
7	$\{1,2,3,4,5,6\}$	6
8	$\{1,3,5,7\}$	4
9	$\{1,2,4,5,7,8\}$	6
10	$\{1,3,7,9\}$	4

Note for primes, $|\{1 \leq a < p : (a,p) = 1\}| = p - 1$.

Example 10.5. Find r such that if $(a, pq) = 1$, that p, q are primes, then $a^r \equiv 1 \pmod{pq}$.

Solution:

$(a, pq) = 1 \iff (a,p) = 1$ and $(a,q) = 1$, so $p \nmid a$ and $q \nmid a$. This implies to $a^{p-1} \equiv 1 \pmod{p}$ and $a^{q-1} \equiv 1 \pmod{q} \implies (a^{(p-1)(q-1)}) = (a^{p-1})^{q-1} \equiv 1^{q-1} \equiv 1 \pmod{p}$. Then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$ for any $(a, pq) = 1$.

Definition 10.6. Euler's totient function: φ. The function is defined as $\varphi(n) :=$ the number of $\{1 \leq a < n : (a,n) = 1\}$.

Also, combining above notes, we can write $a^{\varphi(n)} \equiv 1 \pmod{n}$ if $(a,n) = 1$. If n is a prime, then $\varphi(n) = n - 1$. This implies to Fermat's Little Theorem.

Definition 10.7. Reduced Residue System: $\{a_1, a_2, ..., a_{p(n)}\}$ is a reduced residue system if given any A, such that $(A,n) = 1$, there exists unique a_i such that $A \equiv a_i \pmod{n}$.

Definition 10.8. Recall: We say a and b are coprime if $(a,b) = 1$

Exercise 10.9. Show that any set of $\varphi(n)$ integers coprime n, satisfying no two are equivalent modulo n is a reduced residue system. That is, the set $S = \{b_1, b_2, ..., b_{\varphi(n)}\}$ such that $b_i \not\equiv b_j \pmod{n}$ and $(b_i, n) = 1$ for all i, j

with $i \neq j$, you want to show given A, there exists unique i such that $A \equiv b_i \pmod{n}$.

Solution:

Proof. Suppose this is not true, i.e., you have A with $(A, n) = 1$, $A \not\equiv b_i$ for any i, this means

$$\left.\begin{array}{r} \text{remainder } A \text{ divided by } n \\ \text{remainder } b_1 \text{ divided by } n \\ \text{remainder } b_2 \text{ divided by } n \\ \ldots \end{array}\right\} \text{All different}$$

So, $1 \leq \varphi(n) + 1$ integers $< n$ such that $(r, n) = 1$. Contradiction to the definition of $\varphi(n)$.

□

Corollary 10.10. If $b_1, b_2, ..., b_{\varphi(n)}$ is a reduced residue system and $(a, n) = 1$, then $ab_1, ab_2, ..., ab_{\varphi(n)}$ is a reduced residue system.

Proof. If $ab_i \equiv ab_j \pmod{n}$, $(a, n) = 1 \implies \exists t$ such that $at \equiv 1 \pmod{n}$, $atb_i \equiv atb_j \pmod{n}$, then $b_i \equiv atb_i \equiv atb_j \equiv b_j \pmod{n}$. Contradiction to $b_i's$ is a reduced system.

□

Exercise 10.11. Prove $a^{\varphi(n)} \equiv 1 \pmod{n}$ if $(a, n) = 1$

Solution:

Proof. $\varphi(n) =$ the number of $\{1 \leq a < n : (a, n) = 1\}$, this is equivalent to $b_1 = 1 < b_2 < ... < b_{\varphi(n)} < n$. The set of number is the same as

$ab_1, ab_2, ..., ab_{\varphi(n)} \pmod{n}$ (same up-to order). This will imply to

$$\prod_{i=1}^{\varphi(n)} b_i \equiv \prod_{i=1}^{\varphi(n)} ab_i \pmod{n}$$
$$\implies \prod_{i=1}^{\varphi(n)} b_i \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} b_i \pmod{n}$$
$$(b_i, n) = 1 \implies (\prod_{i=1}^{\varphi(n)} b_i, n) = 1$$
$$\implies 1 \equiv a^{\varphi(n)} \pmod{n}$$

□

Theorem 10.12. Wilson's Theorem
If p is a prime, $(p-1)! \equiv -1 \pmod{p}$ if and only if given $a \in \{1, ..., p-1\}$, you can find a unique b such that $ab \equiv 1 \pmod{p}$

Example 10.13. Consider the set $\{1, 2, 3, 4, 5, 6\} \pmod{7}$:

$$1 \times 1 \equiv 1 \pmod{7}$$
$$2 \times 4 \equiv 1 \pmod{7}$$
$$3 \times 5 \equiv 1 \pmod{7}$$
$$6 \times 6 \equiv 1 \pmod{7}$$

Notice that $(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \cdot 6 \equiv 1 \pmod{7}$, and $-1(6!) \equiv 1 \pmod{7} \implies (6!) \equiv -1 \pmod{7}$

You can also check other examples.

Proof. **Proof of Wilson's Theorem**
$S = \{2, ..., p-2\}$ can be divided into disjoint sets of 2 elements $\{a, b\}$ such that $ab \equiv 1 \pmod{p}$ when $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv \pm 1 \pmod{p}$. Note that S can be expressed to the following:

$$2 \cdot 3 ... (p-2) = \prod_{\frac{p-3}{2} \text{ times}} 1 \equiv 1 \pmod{p}$$

Then

$$(p-2)! \equiv 1 \pmod{p} \implies (p-1)! \equiv -1 \pmod{p}$$

□

Exercise 10.14. Withou using formula for $1^2 + 2^2 + ... + (p-q)^2$, if $p > 3$, can you show $p \mid 1^2 + 2^2 + ... + (p-1)^2$?

Exercise 10.15. Show that

$$\prod_{\substack{1 \le a < n \\ (a,n)=1}} a \equiv -1 \pmod{n}$$

Theorem 10.16. Lagrange's Theorem n modular p arithmetic, a polynomial of degree d has at most d-solution.

Example 10.17. If $f(x)$ has degree d then it has at most d, d distinct solution modulo p. Suppose $d = 2$, prove $x^2 \equiv a \pmod{p}$ has less than 2 solutions modulo p. (Because $d = 1$, $ax \equiv b \pmod{p}$ has at most 1 solution. $a \not\equiv 0 \pmod{p}$)

Proof. If $x^2 \equiv a \pmod{p}$ has no solutions, we are done.
If $x^2 \equiv a \pmod{p}$ has a solution, say r, implies to $r^2 \equiv a \pmod{p} \implies x^2 = a \pmod{p} \iff x^2 \equiv r^2 \pmod{p} \iff x^2 - r^2 \equiv 0 \pmod{p} \iff (x-r)(x+r) \equiv 0 \pmod{p}$ ($ab \equiv 0 \pmod{p} \implies a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$) $\iff (x-r) \equiv 0 \pmod{p}$ or $x + r \equiv 0 \pmod{p} \iff x \equiv -r \pmod{p}$ or $x \equiv r \pmod{p}$. So, there are at most two solutions. $a = 0 - 1501^n$. Otherwise, ...

□

In general, let $f(x)$ be a deg. d polynomial.

$$f(x) = a_d x^d + a_{d-1} x^{d-1} + ... + a_0$$

such that $a_d \not\equiv 0 \pmod{p}$.

Claim 10.18. If $f(r) \equiv 0 \pmod{p}$ then $f(x) \equiv (x-r)g(x) \pmod{p}$ for some deg. $(d-1)$ polynomial $g(x)$.

Proof. Take $f(x) = a_d x^d + a_{d-1}(x^d - r^d) + a_{d-1}(x^{d-1} - r^{d-1}) + ... + a(x-r)$ with $a_d \equiv 0 \pmod{p}$

$$f(r) = a_d r^d + a_{d-1} r^{d-1} + ... + a_0$$
$$\implies f(x) - f(r) = a_d(x^d - r^d) + a_{d-1}(x^{d-1} - r^{d-1} + ... + a(x-r))$$

Recall $x^k - r^k = (x-r)(x^{k-1} + rx^{k-2} + r^2x^{k-3} + ... + r^{k-1})$, $f(x) - f(r)$ has deg. d with $a_d \not\equiv 0 \pmod{p}$, $f(x) - f(r) = (x-r)(a_d x^{d-1} + ...)$ has equal deg. with $(d-1)$ with leading coefficients $\not\equiv 0 \pmod{p}$.

□

Proof. **Proof of Lagrange's Theorem** If $f(x)$ has no solutions, we are done. If $f(r) \equiv 0 \pmod{p}$, $f(x) \equiv f(x) - f(r) \equiv (x-r)(g(x)) \pmod{p}$, looking for solutions to $f(x) \equiv 0 \pmod{p} \iff (x-r)g(x) \equiv 0 \pmod{p}$. In other words, $x \equiv r \pmod{p}$ or $g(x) \equiv 0 \pmod{p}$.

Induction Hypothesis: $g(x) \equiv 0 \pmod{p}$ has at most $d-1$ solutions.

Solutions of f are $\{r,$ solutions of $g\}$. The number of solutions to $f(x) \equiv 0 \pmod{p}$ is at most 1+ of number of solutions to $g(x) \equiv 0 \pmod{p}$.

□

Example 10.19. Use Wilson's Theorem to show $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

11 Computing Large Powers in Modular Arithmetic

This topic you may have learned elsewhere.

Example 11.1. 7^{4587} modulo 853

Think about how to solve this.

1. If 853 is a prime? Yes.

2. By Fermat's Little Theorem,

$$\begin{aligned} 7^{852} &\equiv 1 \pmod{853} \quad 4587 = 852 \times 5 + 327 \\ 7^{4587} &\equiv 7^{852 \cdot 5 + 327} \\ &\equiv 7^{852 \cdot 5} \cdot 7^{327} \\ &\equiv (7^{852})^5 \cdot 7^{327} \\ &\equiv 1^5 \cdot 7^{327} \pmod{853} \end{aligned}$$

Think about $7^{327} \equiv ?\pmod{853}$. What is 327 in binary: $327 = 2^8 + 2^6 + 2^2 + 2^1 + 2^0$.

$$\begin{aligned} 7^{327} &\equiv 7^{2^8 + 2^6 + 2^2 + 2^1 + 2^0} \\ &\equiv 7^{2^8} \cdot 7^{2^6} \cdot 7^{2^2} \cdot 7^{2^1} \cdot 7^{2^0} \pmod{853} \end{aligned}$$

Look at

$$\left.\begin{aligned} 7^{2^0} &\equiv 7 \\ 7^{2^1} &\equiv 7^2 \equiv 79 \\ 7^{2^2} &\equiv 49^2 \equiv -158 \\ 7^{2^3} &\equiv (-158)^2 \equiv 24964 \equiv 227 \\ 7^{2^4} &\equiv (227)^2 \equiv 51529 \equiv 349 \\ 7^{2^5} &\equiv (349)^2 \equiv 675 \\ 7^{2^6} &\equiv (675)^2 \equiv 455625 \equiv 123 \\ 7^{2^7} &\equiv (123)^2 \equiv 15129 \equiv 628 \\ 7^{2^8} &\equiv (628)^2 \equiv 394384 \equiv 298 \end{aligned}\right\} \pmod{853}$$

$$7^{327} \equiv (298)(123)(-158)(49)(7) \equiv 286 \pmod{853}$$

Exercise 11.2. Compute $2^{730} \pmod{731}$ to check if 731 is prime.

Example 11.3. Find solutions to $x^{53} \equiv 1 \pmod{1007}$ or $x^{73} \equiv 1 \pmod{1007}$

Note that $\varphi(1007)$ and 53 are coprime, $(A, 1007) = 1$ for any solutions $x = A$.
$A^{53} \equiv 1 \pmod{1007} \implies A^{53} = 1 + 1007k$ for some k. Thus, if $d \mid A$ and $d \mid 1007 \implies d \mid 1$.

By Bezout's lemma, u and v:

$$u \cdot 53 + v \cdot \varphi(1007) = 1$$

WLOG, assume $u > 0$, $v_* = -v$,

$$u \cdot 53 = 1 + v_* \times \varphi(1007) \implies 1 \equiv A \pmod{1007}$$

12 Computing $\varphi(n)$, Show Existence of Primitive Roots

Definition 12.1. $\varphi(n) = |\{1 \leq a < n : (a, n) = 1\}| \iff$. That is, number of residue classes that have multiplicative inverse. $(a, n) = 1$ if and only if $ax \equiv 1 \pmod{n}$ has a solution.

Recall: **Chinese Remainder Theorem**
If $S =$ Complete residue system $\pmod{m}$
$T =$ Complete residue system $\pmod{n}$ and $(m, n) = 1$,
$S \times T \longleftrightarrow M$ where M is the complete set of residue modulo mn.
$a \pmod{m}, b \pmod{n} \longleftrightarrow c \pmod{mn}$ such that $c \pmod{m} = a \pmod{m}$, $c \pmod{n} = b \pmod{n}$. Note that such things of $c \pmod{n}$ are **classes**.

Definition 12.2. Multiplicative Inverse for a class $[a] \in \mathbb{Z}_n$ is a class $[b] \in \mathbb{Z}_n$ such that $[a][b] = [1]$. A class $[a] \in \mathbb{Z}_n$ is a *unit* if it has a multiplicative inverse in $\mathbb{Z}_n$.

Example 12.3. We sometimes say that integer a is a *unit* $\pmod{n}$, meaning that $ab \equiv 1 \pmod{n}$ for some integer b.

Example 12.4.

$$\begin{aligned} 0 &\mod 3, 0 \mod 5 \longleftrightarrow 0 \mod 15 \\ 1 &\mod 3, 0 \mod 5 \longleftrightarrow 10 \mod 15 \\ 2 &\mod 3, 0 \mod 5 \longleftrightarrow 5 \mod 15 \end{aligned}$$

Theorem 12.5. If m and n are coprime, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. See the textbook. □

For any $d \mid p-1$, number of elements $\pmod p$ with order exactly $d = \varphi(d)$ or 0. In other words, if r has order $d \pmod p$ then you can find $\varphi(d)$ elements with order d.

If $\text{ord}_p(r) = d$, then $\text{ord}_p(r^k) = \frac{d}{(k,d)}$. $r^d \equiv 1 \pmod p$, $(r^k)^{\frac{d}{(k,d)}} \equiv (r^d)^{\frac{k}{(k,d)}} \equiv 1 \pmod p$ implies to $\text{ord}_p(r^k) \mid \frac{d}{(k,d)}$. Let $d' = \text{ord}_p(r^k)$ then $r^{kd'} \equiv 1 \pmod p \implies d \mid kd' \implies \frac{d}{(k,d)} \mid \frac{k}{(k,d)} \cdot d' \implies d' = \frac{d}{(k,d)}$. If $\text{ord}_p(r) = d$, then $1, r, r^2, ..., r^{d-1}$ are distinct modulo p.

r^k when $(k,d) = 1$ also has order d. Then if you have one element of order d, then you have $\varphi(d)$ elements of order d.

Let $\text{ord}_d(s) = d$, then claim $s \equiv r^k \pmod p$ for some k such that $(k,d) = 1$, $1, r, r^2, ..., r^{d-1}$ are distinct modulo p and satisfy $x^d \equiv 1 \pmod p$ has almost d solutions, but $\{1, r, r^2, ..., r^{d-1}\}$ are distinct solutions and thus must be all solutions. Number of elements of order $d = \varphi(d)$ or 0. Every element has order divides $p-1 \pmod p$. Say number of elements with order $d = \psi(d)$.

$$\sum_{d|p-1} \psi(d) = p-1$$

$$\psi(d) = \varphi(d) \text{ or } d$$

$$p-1 = \sum_{d|p-1} \psi(d) \leq \sum_{d|p-1} \varphi(d) = p-1$$

$$\iff \psi(d) = \varphi(d) \text{ for all } d \mid p-1 \implies \psi(p-q) = \varphi(p-1)$$

Example 12.6. Show that $\exists \varphi(p-1)$ primitive roots modulo p.

Proof. $x^2 \equiv a \pmod p$ has a solution if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ (p-odd prime).
$x^2 \equiv a \pmod p$ has solutions say $r^2 \equiv a \pmod p$ raising both sides to $\frac{p-1}{2}$.

$$1 \equiv r^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p$$

if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ then if w is a primitive root, $a \equiv w^r \pmod p$ for some

r.

$$1 \equiv a^{\frac{p-1}{2}} \equiv w^{r \cdot \frac{p-1}{2}} \pmod{p} \implies p-1 \mid r \cdot (\frac{p-1}{2})$$

$$\implies 2 \mid r \implies r = 2s \implies a \equiv (w^s)^2 \pmod{p}$$

$$\implies w^s \text{ is a solution to } x^2 \equiv a \pmod{p}$$

□