HW 5

Math110 - Summer Session 1

ZhiBin Huang

07/15/2022

Time flies, and guess what. The five weeks have passed in the blink of an eye. Although five weeks are a lot busier than the normal 10 weeks, strictly speaking: Math 110 in Session 1. I reviewed what I learned in math100(reflexivity, transitive, symmetry.) and I also learned a lot of new math such as gcd, lcm and a lot of formulas. Today, I'm going to summarize what I learned during my five weeks of summer vacation. I will go over chapter 1 - 4 in each paragraph and would like to describe deep information such as theorems, propositions, or corollaries.

Chapter 1

Chapter 1 had been called foundation in the class Math 110. It is super useful for basic knowledge and will need to cover a lot in the next few chapters. I think the first chapter is related to the next four chapters. In Chapter 1, we learned divisions, general common divisors(or called gcd), least common divisors(lcm) and one of the important theorems: DioPhantine equations.

Important theorems, propositions, or corollaries.

1. **The Euclidean Algorithm(let a and b belong to integer, when a > 0, b > 0 and a>= b, then we have**

step1 : $a = q_1 \cdot (b) + r_1, \quad 0 < r_1 < b.$

step2 : $b = q_2 \cdot (r_1) + r_2, \quad 0 < r_2 < r_1.$

step3 : $r_1 = q_3 \cdot (r_2) + r_3, \quad 0 < r_3 < r_2$

$\vdots$

stepn : $r_{n-2} = q_n \cdot (r_{n-1}) + r_n, \quad 0 < r_n < r_{n-1}$

I learned the Euclidean algorithm Theorem and I learned that the algorithm is the algorithm for finding the greatest common divisor. The requirement of the Euclidean algorithm is that the numbers a and b must be integers, and the greatest common divisor of the two integers is the largest positive integer that can divide them simultaneously.

Example: gcd(200, 178)

Then let a = 200, b = 178

200 = 1(178) + 22

178 = 8(22) + 2

22 = 11(2) + 0

So the gcd(200,178) = 2

Example : gcd(6666, 1234)

Then let a = 6666, b = 1234

6666 = 5(1234) + 496

1234 = 2(496) + 242

496 = 2(242) + 12

242 = 20(12) + 2

12 = 6(2) + 0

So the gcd(6666,1234) = 2

2. **GCD - LCM Product Formula((let a and b be a positive integer, then:)**

Thm 3 (GCD-LCM product formula). let a and b be positive integers. then $\boxed{\operatorname{lcm}[a,b] = \frac{a \cdot b}{\gcd(a,b)}}$.

For arbitrary $a, b \in \mathbb{Z}$, $\operatorname{lcm}[a,b] = \frac{|a| \cdot |b|}{\gcd(a,b)}$.

The GCD - LCM Product Formula is used to find the lcm(a,b), but it requires that the a and b belong to positive integers. It also important to find the gcd first because the formula need us to use the a*b divides gcd(a,b).

Example: lcm(200, 178) hint: we know that gcd(200,178) = 2

lcm(200,178) = (200 *178) / 2 = 17800

Example : lcm(6666, 1234) hint: we know that gcd(6666,1234) = 2

lcm(6666,1234) = (6666 *1234) / 2 = 4112922

3. **Divisibility Properties**

There are Reflexivity, Linearly, transitivity, cancellation and two out of three principles. Those Properties had been proof in the class and can be used on most of the Division. I will give following example:

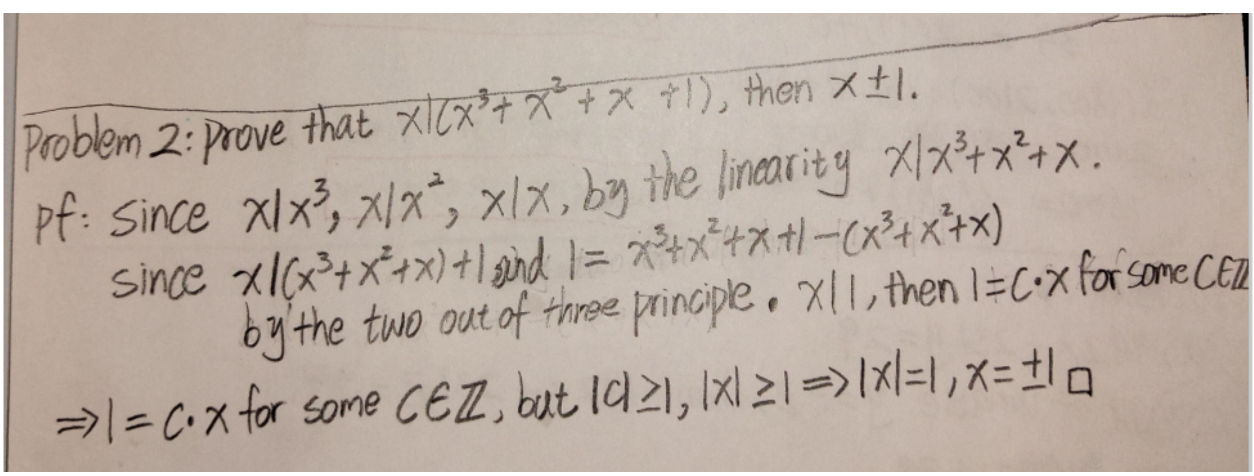
Reflexivity: 1000 | 1000, 6666 | 6666

Linearly: 10 | 20, 10 | 100, then ⇒ 10 | 120

Transitivity: 200 | 400, 400 | 1600, then ⇒ 200 | 1600

Cancellation: 200 | 600 ⇒ 2 * (100) | 6 * (100) ⇒ 2 | 6

Two out of three principles: I use the homework1 problem 2 as example:



Problem 2: prove that $x|(x^3+x^2+x+1)$, then $x \pm 1$.

pf: Since $x|x^3$, $x|x^2$, $x|x$, by the linearity $x|x^3+x^2+x$.

since $x|(x^3+x^2+x)+1$ and $1 = x^3+x^2+x+1-(x^3+x^2+x)$

by the two out of three principle. $x|1$, then $1=c\cdot x$ for some $c \in \mathbb{Z}$

$\Rightarrow 1 = c \cdot x$ for some $c \in \mathbb{Z}$, but $|c| \geq 1$, $|x| \geq 1 \Rightarrow |x| = 1$, $x = \pm 1$ $\square$

4. **Linear Diophantine equations**

Def 3 let a, b, and c be integers, and let x, y be variables

then $a \cdot x + b \cdot y = c$ is called Linear Diophantine eq.

• Solving this eq means solve for integer solution

Coro 2: The Diophantine eq $a \cdot x + b \cdot y = c$ has integer solution $\Longleftrightarrow$ $\gcd(a,b) \mid c$.

Linear Diophantine equations is an equation and the general form looks like: **a x + b y = c**. The number a, b, c must be integer and given integers. It is also important that x, y are two of the unknown integers and we need to check if the equation has the integer solution or not. Here is the example:

Example: 6x+ 297y = 99

Step 1: check if the equation is soluble or not.

gcd(6 , 297) = 3 and 3 | 99, therefore, it is soluble.

297 = 49(6) + 3

6 = 2(3) + 0

Linear combination

3 = 297 - (49)6

33 * 3 = (33) 297 - (33)(49)6

99 = (33) 297 + (-1617) 6

So we have x = -1617 and y = 33 is a solution 6x+ 297y = 99

Example: 192x+ 231y = 36

Step 1: check if the equation is soluble or not.

gcd(192 , 231) = 3 and 3 | 36, therefore, it is soluble.

231 = 1(192) + 39 ⇒ 192 = 4(39) + 36 ⇒ **39 = 1(36) + 3** ⇒ **36 = 12(3) + 0**

Linear combination

3 = 39 - 36

3 = 39 - (192 - 4(39))

3 = 5(231-192) + (-1)192

36 = (60)231 + (-72)192

So we have x = -72 and y = 60 is a solution 192x+ 231y = 36

Chapter 2

Chapter 2 had been called Prime Factorization in the class Math 110. This chapter summarizes a lot of formulas and definitions, which sometimes confuse me a lot and need more time to review. Some knowledge relates to chapter 1 and the professor covers a lot of new knowledge that will be used in the next chapter. In Chapter 2, I review the knowledge of prime and coprime and learn the idea of fundamental theorem of arithmetic (FTA) and Euler's totient function. As my in person experience, I feel like Euler's totient function is super fun and useful.

Important theorems, propositions, or corollaries:

1. **Theorems for prime numbers: There are infinitely many prime numbers.**

thm 1 (Euclid) There are infinitely many prime numbers.

This is true because this is part of the Euclid's theorem. Euclid's theorem is a math statement for number theory. In the Professor lecture , proof of Euclid's theorem. We see that there are infinitely many prime numbers.

Example: The Prime number: 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29…..

2. **The Corollaries 1 in Chapter 2**

Cor 1 If $n \in \mathbb{N}$, then $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$, where $n \geq 0$, $p_1, p_2, \ldots p_r$ are distinct primes, $e_i \geq 1$, $\forall i$.

These corollaries show that if any N number belongs to a natural number, where number N is greater >= 0, we can get the N number by prime number. In other words, We can multiply prime numbers or prime numbers to the power and come up with any number. I will give the following example for reference

Example: The Prime number: 2, 3, 5, 7, 11, 13, 17, 19, 23 and 29.

If I want to decompose 1200, 1400 and 1500:

1200 = (2^4) * 3 * (5^2)   1400 = (2^3) * (5^2) * 7   1500 = (2^2) * 3 * (5^3)

3. **The Propositions 2, 3 in Chapter 2**

Prop 2: let $n \in \mathbb{Z}$, and let p be a prime, then either $p \mid n$ or $\gcd(p, n) = 1$.

Prop 3 let a and b be integer, and let p be a prime. If $p \mid a \cdot b$, then either $p \mid a$ or $p \mid b$. or both

The reason why I chose two propositions at the end is because I think both of them are super useful and important for chapter 2. Especially the proposition 2 especially needs to use this proof many times because of the professor's proof and the homework proof question.

Propositions 2

If we have a number N belong to integer, and have a P number be a prime, then we can see the solution is either P | N or gcd(P, N) = 1.

Example:

Let N be 77 and P as 2

We see that gcd(2,77) = 1, but 2 does not divide 77.

Let N be 88 and P as 2

We see that 2 | 88, but gcd(2, 88) = 2

Propositions 3

If we have two numbers A and B and both of them are an integer, and we have a P number be a prime. We have P|ab and then P|A or P|B or both.

Example:

5 | 150 ⇒ 5 | 50 * 3
but we know 5 does not divides to 3, so we have 5 | 50,
which is one side divides
Then we can see
5 | 50 ⇒ 5 | 10 * 5 ⇒ 5 | 10 or 5 | 5. Which is both divides.

2 | 2800 ⇒ 2 | 70 * 40
Then we can see that
2 | 70 and 2 | 40 ⇒ which is both divides.

4. Arithmetical functions.

<u>Def (Arithmetical function)</u> A function $f: \mathbb{N} \to \mathbb{R}$ (or $\mathbb{C}$) is called an arithmetical function.

<u>Def</u> (multiplicative arithmetical function) An arithmetical function $f: \mathbb{N} \to \mathbb{R}$ is called <u>multiplicative</u>: if $f(m \cdot n) = f(m) \cdot f(n)$ when $\gcd(m,n) = 1$.

This is not the theorems, propositions, or corollaries.
(刘教授，剧本不对啊！被迫营业，千山万水总是情，给个高分谢谢您!
translate: I have fun with this definition and it should be theorem in the future)

Example:
f(x) = cos(x), x belong to R is not an arithmetical function
Because no matter what you plug in the number. X should always belong to N(natural number). By the definition, it is not an arithmetical function.

<u>Def (Arithmetical function)</u> A function $f: \mathbb{N} \to \mathbb{R}$ (or $\mathbb{C}$) is called an arithmetical function.

f(x) = (-17)^x is not a multiplicative arithmetic function
Let m = 2 and n = 3. gcd(2,3) = 1, but
f(m * n) ⇒ f(6) = (-17)^6 = 24137569
f(m) * f(n) = (-17)^2 * (-17)^3 = 289 * -4913 = -1419857
We can see f(m * n) is not equal to f(m) * f(n),
So f(x) = (-17)^x is not a multiplicative arithmetic function

<u>Prop 6</u> The Euler's totient φ is multiplicative. i.e.
If $m, n \in \mathbb{N}$ and $\gcd(m,n) = 1$, then $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Important! This is always true no matter what. One of the great examples of Midterm, but true fact forever.

Chapter 3

Chapter 3 had been called Module Arithmetic in the class Math 110. This chapter 3 summarizes a lot of formulas and definitions, but even right now, it also confuses me a lot and the proof for some theorems is super long sometimes. To be honest, Chapter 3 is one of the most hardest, painful and I will need more time on this chapter. In Chapter 3, I use the knowledge from chapter 1 and 2, which we use to prove some theorems and I learn the idea of congruence of mod, Eulor's theorem and Femat little theorem and the Chinese remainder theorem. It is interesting that I always mess up and misremembered Eulor's theorem and Femat little theorem. I learned better on the Chinese remainder theorem.

Important theorems, propositions, or corollaries.

1. **Congruence Modulo M Theorem**

Thm/ Congruence modulo m is an equivalent relation.
i.e. $\cdot \equiv \cdot \pmod{m}$ satisfies the following axioms:
(1) (Reflexivity) $a \equiv a \pmod{m}$, $\forall a \in \mathbb{Z}$.
(2) (Symmetry) If $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$
(3) (transitivity) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$
then $a \equiv c \pmod{m}$

This is the first theorem I had learned in chapter 3 and it is also a knowledge that surprised me because this is the knowledge I had gained in Math 100. Reflexivity, Symmetry and Transitivity. Those three ideas are significant in Math 100, but they have the same meaning and use in the congruence Module. Here is some example:

Reflexivity: Let M = 6666 and let a = 5555, we see that

5555 三 5555 mod(6666)

Symmetry: Let M = 45 and let A = 47 and B = 2, we see that

47三2 mod(45) ⇐ Both is works ⇒ 2三47 mod(45)

Transitivity:

666三333 mod(37) 333三 296 mod(37) ⇒ 666三296 mod(37)

555三505 mod(50) 505三455 mod(50) ⇒ 555三455 mod(50)

2.

Thm 2 Fix a modulus $m \in \mathbb{N}$. If $a \equiv b \pmod{m}$, $a' \equiv b' \pmod{m}$

then (1) $a \pm a' \equiv b \pm b' \pmod{m}$

(2) $a \cdot a' \equiv b \cdot b' \pmod{m}$

(3) $a \cdot n \equiv b \cdot n \pmod{m}$, $\forall n \in \mathbb{Z}$.

(4) $a^n \equiv b^n \pmod{m}$, $\forall n \in \mathbb{N}$.

This theorem is also super important because it can help us simplify or settle certain problems. I personally like this theorem because it is easy to understand and I use a lot of this theorem to prove some homework questions. These laws have been proved by the professor in the classroom. I will give some own example to

Example: Simplify 15^3 mod(5)

We know that 15^3 = 3375, so we have 15^3 ≡ 3375 mod(5)

We also know that 3375 ≡ 3370 mod(5)

By the

(3) $a \cdot n \equiv b \cdot n \pmod{m}$, $\forall n \in \mathbb{Z}$.

So we can simplify the follow 3375 ≡ 3370 mod(5) ⇒ 675≡ 674 mod(5)

3. **Corollaries check if N is divisible by another number.**

Coro 1 let $n \in \mathbb{N}$, express n in digit form:

$$n = a_r a_{r-1} a_{r-2} \cdots a_0 = a_r \cdot 10^{r-1} + a_{r-1} \cdot 10^{r-2} + \cdots + a_1 \cdot 10 + a_0$$

This theorem is also super important and has already been proved by the professor during the class. We have some of the homework questions that relate to this, and it can help us find if the number N is divisible by another number. I would like to give some example:

Example:

Let n be 12345, can n be divisible by 3? Can n divisible by 9?

So we have 1 + 2 + 3 + 4 + 5 = 15 we can see that 3 | 15 , but 9 is not divisible 15.

So 12345 is divisible by 3, but not 9.

Let N be 12345 * 23333 * 66666, can n be divisible by 3? can n be divisible by 9?

Since 3 | 12345, 3 | 66666, so n can be divisible by 3.
Since none of the numbers can divide 9, so n can not be divisible by 9.

4. **Multiplicative Inverse**

Def (multiplicative inverse mod m). Fix $m \in \mathbb{N}$, and let $a \in \mathbb{Z}$. Then a multiplicative inverse of a modulo m is another integer b s.t. $\boxed{a \cdot b \equiv 1 \pmod{m}}$
i.e. $x = b$ is solution for $ax \equiv 1 \pmod{m}$.

This is not the theorems, propositions, or corollaries.
(刘教授，剧本不对啊！被迫营业，千山万水总是情，给个高分谢谢您！
translate: I have fun with this definition and it should be theorem in the future)
However, It is an important definition. I think I must go over and it is super interesting. Before we find the multiplicative inverse for a number N, we need to determine if N is solvable or not. By checking if their gcd = 1, we can determine if number N is solvable or not. then we can find the multiplicative inverse. Here is an example.
Example: Find the multiplicative inverse of 8 modulo (20, 21, 22, 23, 24)

First Step: Check if the 20, 21, 22, 23, 24 are solvable or not

When M = 20, gcd(8 , 20) = 4, but 4 is not | 1, so no solution, done.
When M = 21, gcd(8 , 21) = 1, 1 | 1, so we have solution
When M = 22, gcd(8 , 22) = 2, but 2 is not | 1, so no solution, done
When M = 23, gcd(8 , 23) = 1, 1 | 1, so we have solution
When M = 24, gcd(8 , 24) = 8, but 8 is not | 1, so no solution, done.

For 21, solve for x in 8x ≡ 1mod(21), find the solution 8x + 21y = 1

21 = 2(8) + 5	1 = 8(8) - 3(21)
8 = 1(5) + 3	1 = 2(8) -3(21-2(8))
5 = 1(3) + 2	1 = 2(8) -3(5)
3 = 1(2) + 1	1 = (8-5)-(5-(8-5))
2 = 2(1) + 0	1 = 3 - 2

So we have x = 6 is a solution for 8x ≡ 1mod(21), so 6 is the multiplicative inverse of 8 mod(21)

For 23, solve for x in 8x ≡ 1mod(23), find the solution 8x + 23y = 1

23 = 2(8) + 7	1 = 3(8) + (-1)(23)
8 = 1(7) + 1	1 = 8 - (23- (2(8)))
7 = 7(1) + 0	1 = 8 - 7

So we have x = 3 is a solution for 8x ≡ 1mod(23), so 3 is the multiplicative inverse of 8 mod(23)

5. Chinese remainder theorem

thm (Chinese Remainder thm) Assume $m_1, m_2, \dots, m_r \in \mathbb{N}$ that are $\boxed{\text{pairwise coprime}}$ then

$$(*)\quad \begin{cases} X \equiv b_1 \pmod{m_1} \\ X \equiv b_2 \pmod{m_2} \\ \vdots \\ X \equiv b_r \pmod{m_r} \end{cases}$$

has a unique solution x_0, $0 \le x_0 < m_1 \cdot m_2 \cdots m_r$

The Chinese remainder theorem is interesting and I am proud because I am Chinese and finally see the theorem from my motherland. The Chinese remainder theorem is a theorem which gives a unique solution to simultaneous linear congruences with coprime moduli. In other words, if we have three congruence equations, then we can set two equations as 0 mod n, then we can use that to calculate the part of the answers. when we sum up the answer, then we can have the equation. This algorithm simply and violently splits and calculates each step, and it has become my favorite algorithm.

Example:

X ≡ 4 mod(8)

X ≡ 15 mod(17)

X ≡ 4 mod(25)

Part 1

X ≡ 4 mod(8)

X ≡ 0 mod(17) ⇒ **425k ≡ 4 mod(8) ⇒ 1K ≡ 4 mod(8)**

X ≡ 0 mod(25) **k = 4** **X = 1700**

Part 2

X ≡ 0 mod(8)

X ≡ 15 mod(17) ⇒ **200k ≡ 15 mod(17) ⇒ 13k ≡ 15 mod(17)**

X ≡ 0 mod(25) **k = 9** **X = 1800**

Part 3

X ≡ 0 mod(8)

X ≡ 0 mod(17) ⇒ **136k ≡ 4 mod(25) ⇒ 11k ≡ 4 mod(25)**

X ≡ 4 mod(25) **k = 139** **X = 18904**

So the answer for this remainder theorem is 1700 + 1800 + 18904 = 22404

22404 mod(8 * 17 * 25) ⇒ 22404 mod(3400) ⇒ 2004 mod(3400), The answer can be 2004.

Chapter 4

Chapter 4 had been called Quadratic residues in the class Math 110. Chapter 4 is one of the most relaxed and interesting chapters I have seen. It is most likely focused on square mod and includes a lot of theorems and ways to determine if that's a square mod or not. Although sometimes I get confused and puzzled when I do the questions, this chapter only has calculation questions and no proof questions, which is my favorite chapter. This chapter also adds the Chinese remainder theorem and it is one of the most easy theorems and useful theorems I had read.

Important theorems, propositions, or corollaries.

Euler's Cutenion, theorem, Corollaries in chapter 4

Thm 3 (Quadratic Reciprocity) Let p, q be odd primes.

then $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$.

Def: For $a \in \mathbb{Z}$, $p \nmid a$, $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{when } a \text{ is a square mod } p \\ -1, & \text{- - - nonsquare mod } p \end{cases}$

Thm 2 (Reciprocity for 2) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$

Coro 2 (Reciprocity for -1) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \leq 3 \pmod 4. \end{cases}$

Coro 4 $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$. $\forall a, b \in \mathbb{Z}$.

All of the theorems above are related to a math knowledge called legendre symbol. In my opinion, the legendre symbol is to judge whether a number is a square residue modulo n. I understand some of the ideas, but not all of them. Here is some example:

Example for theorem 2:

Thm2 (Reciprocity for 2) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$

Is 2 square mod 49?

So we have (2/49), P = 49, then we can see 49 ≡ 1 mod(8), which show (2/49) = 1

2 is square mod 49

Example for theorem 3:

Thm3 (Quadratic Reciprocity) Let p, q be odd primes.

then $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$.

Is 17 square mod 19?

So we have (17/19), q = 17 and P = 19.

(17/19) = (-1)^([17-1]/2)([19-1]/2) * (19 / 17) = (19 / 17)

(19/17) ⇒ (2 / 17), then by theorem 2

(2 / 17) shows p = 17, and 17 ≡ 1 mod(8)

(2 / 17) = 1, which (17/19) ⇒ (19 / 17) = 1, so 17 is the square mod 19.

Example for all of them:

Is 35 square mod 17?

Because 35 is not a prime number, so we use the coro 4

$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$. $\forall a, b \in \mathbb{Z}$

then we have (35/17) ⇒ ((5 * 7) / 17) ⇒ (5 / 17) * (7 / 17)

We first see if (5 / 17) is a square mod or not.

Thm 3 (Quadratic Reciprocity) Let p, q be odd primes.
then $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$.

(5 / 17) = (-1)^([5-1]/2)([17-1]/2) * (17 / 5) = (17 / 5)

(17 / 5) ⇒ (2 / 5), then by the them 2

Thm2 (Reciprocity for 2) $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$

We can see p = 5, we have 5 ≡ 5 mod(8), so we get (5 / 17) = -1.

Then let's take a look at (7 / 17)

(7 / 17) = (-1)^([7-1]/2)([17-1]/2) * (17 / 7) = (17 / 7)

(17 / 7) ⇒ (3 / 7) ⇒ (-4 / 7)

Then we can use coro 4

$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$. $\forall a, b \in \mathbb{Z}$

(-4 / 7) ⇒ (-1 * 4) / 7 ⇒ (-1 / 7) * (4 / 7)

We now can use coro 2 for (-1 / 7)

Coro 2 (Reciprocity for -1) $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4 \\ -1, & \text{if } p \equiv 3 \pmod 4 \end{cases}$

We can see (-1 / 7), p = 7 and 7 ≡ 3 mod(4). So we have (-1 / 7) = -1

For the (4 / 7), we can use coro 4 and fact 1

(4 / 7) ⇒ ((2 * 2) / 7) ⇒ (2 / 7) * (2 / 7) ⇒ So we have (4 / 7) = 1

<u>Fact 1</u>: Any square number is a square mod p.

$$\left(\frac{a^2}{p}\right) = 1.$$

(-4 / 7) = -1 * 1 = -1. And we also have (17 / 7) ⇒ (-4 / 7), which (17/7) = -1

Finally, (35/17) ⇒ ((5 * 7) / 17) ⇒ (5 / 17) * (7 / 17) = -1 * -1 = 1

In this case, we see 35 is a square mod 17

<u>Def</u>: For $a \in \mathbb{Z}$, $p \nmid a$, $\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{when } a \text{ is a square mod } p \\ -1, & \text{- - - nonsquare mod } p \end{cases}$