20240905 MATH3301 NOTE 2[1]

Author: Be $\sqrt{-1}$maginative, and nothing will be $\frac{\mathrm{d}}{\mathrm{d}x}$ifficult!
Email: u3612704@connect.hku.hk;
Phone: +852 5693 2134; +86 19921823546;

Contents

1 Introduction

Ideal is a powerful tool to unveil the structure of ring, especially, the integer ring and the polynomial ring. To be specific, ideal can be used to study the greatest common divisor, multiplicative group of integers modulo b, Chinese remainder theorem, quadratic residue and so on. Let's review them in today's note.

2 Greatest Common Divisor

Definition 2.1. (**Divisible Relation and Common Divisor**)
Let a, b be integers.
If there exists integer q, such that $a = qb$, then b divides a;
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer.
If b divides all integer in A, then b is a common divisor of A.

Definition 2.2. (**Greatest Common Divisor and Coprime Set**)
Let A be a nonempty subset of $\mathbb{Z}$, and b be an integer. If:
1. b is a common divisor of A;
2. All common divisor b' of A divides b,
then b is a greatest common divisor of A.
If 1 is a greatest common divisor of A, then A is a coprime set.

Proposition 2.3. Let A be a nonempty subset of $\mathbb{Z}$. For all integer b, b is a generator of gen A if and only if it is a greatest common divisor of A.

Proof. We may divide our proof into two directions.
"only if" direction: Assume that b is a generator of gen A.
We may further divide this direction into two steps.
Step 1: In this step, we prove that b is a common divisor of A.
For all $a \in A$, $a = \Sigma_{k=1}^{1} 1a \in \text{gen } A = \text{gen } \{b\}$, so there exists $q \in \mathbb{Z}$, such that $a = qb$, which implies b divides a and the whole set A. Hence, b is a common divisor of A.
Step 2: In this step, we prove that any common divisor b' of A divides b.
Since $b \in \text{gen } \{b\} = \text{gen } A$, there exists $(\lambda_k)_{k=1}^{m}$ in R, there exists $(a_k)_{k=1}^{m}$ in A, such that $b = \Sigma_{k=1}^{m} \lambda_k a_k$. Each a_k is divisible by b', so $a_k = q_k b'$ for some integer q_k. This implies $b = (\Sigma_{k=1}^{m} \lambda_k q_k) b'$, so b' divides b.
The two steps above show that b is a greatest common divisor of A.
Combine the two directions together, we've proven the statement.
"if" direction: Assume that b is a greatest common divisor of A.
According to **Proposition 5.2.**, gen A always has a generator, namely, b'.
According to **"only if" direction**, b' is also a greatest common divisor of A.
Since both b and b' are greatest common divisors of A, they differ by a factor ± 1. Since b' is a generator of A, $b = \pm b'$ is also a generator of A.

Combine the two directions above, we've proven the biconditional.
Quod. Erat. Demonstrandum. □

Theorem 2.4. (**Extended Euclid Algorithm**)
Let a, b be two integers.
The following algorithm always gives a solution $(x, y) \in \mathbb{Z}^2$ to the Bezout equation $xa + yb = \gcd(a, b)$ after finite steps:
Step 1: Ensure that $a \geq b$.
If $a < b$, then construct a new equation $x'b + y'a = \gcd(b, a)$.
As gcd is symmetric, a solution (x', y') to the new equation gives a solution $(x, y) = (y', x')$ to the original equation;
Step 2: Ensure that $b > 0$.
If $b = 0$, then $(1, 0)$ is an desired solution, and the algorithm ends;
If $b < 0$, then construct a new equation $x'a + y'(-b) = \gcd(a, -b)$.
As gcd is fixed under additive inverse, a solution (x', y') to the new equation gives a solution $(x, y) = (x', -y')$ to the original equation;
Step 3: Now both a and b are positive and $a > b$. Apply **Division Algorithm**:

$$\exists (q, r) \in \mathbb{Z}^2, a = qb + r \text{ and } 0 \leq r < b$$

Construct a new equation $x'r + y'b = \gcd(r, b)$.
As replacing a with r won't change gcd, a solution (x', y') to the new equation gives a solution $(x, y) = (x', y' - qx')$ to the original equation.

Proof. Define function $f : \mathbb{Z}^2 \to \mathbb{Z}, f(a, b) = \min\{|a|, |b|\}$. The algorithm stops if and only if $f(a, b) = 0$. We collect the possible values of f in a sequence as the algorithm works. The value of f will decrease at least one after at most 5 steps, and the value of f has a lower bound 0, so the algorithm stops after at most $5|a| + 5|b|$ steps, which is finite. Quod. Erat. Demonstrandum. □

3 Multiplicative Group of Integers Modulo b

Lemma 3.1. Let a_1, a_2, b be three integers.
If a_1, b are coprime and a_2, b are coprime, then $a_1 a_2, b$ are coprime.

Proof.

$$\begin{aligned}
a_1, b \text{ are coprime} &\implies \exists x_1, y_1 \in \mathbb{Z}, x_1 a_1 + y_1 b = 1 \\
a_2, b \text{ are coprime} &\implies \exists x_2, y_2 \in \mathbb{Z}, x_2 a_2 + y_2 b = 1 \\
&\implies \exists X = x_1 x_2, Y = y_1 + y_2 - y_1 y_2 b \in \mathbb{Z}, X(a_1 a_2) + Y b = 1 \\
&\implies a_1 a_2, b \text{ are coprime}
\end{aligned}$$

Quod. Erat. Demonstrandum. □

Lemma 3.2. Let a_1, a_2, b be three integers.
If a_1, b are coprime and $a_1 \equiv a_2 (\text{mod } b)$, then a_2, b are coprime.

Proof.

$$\begin{aligned} a_1, b \text{ are coprime} &\implies \exists x_1, y_1 \in \mathbb{Z}, x_1 a_1 + y_1 b = 1 \\ a_1 \equiv a_2 (\text{mod } b) &\implies \exists q \in \mathbb{Z}, a_1 = a_2 + qb \\ &\implies \exists x_2 = x_1, y_2 = q x_1 + y_1 \in \mathbb{Z}, x_2 a_2 + y_2 b = 1 \\ &\implies a_1, b \text{ are coprime} \end{aligned}$$

Quod. Erat. Demonstrandum. □

Definition 3.3. (**Multiplicative Group of Integers Modulo** b)
Let b be an integer, and $\mathbf{\Phi}(b)$ be the set of equivalence classes that are coprime with b, i.e., the classes with elements coprime with b.
We define multiplicative group of integers modulo b as the set $\mathbf{\Phi}(b)$ equipped with operation $([a_1]_b, [a_2]_b) \mapsto [a_1 a_2]_b$.

Lemma 3.4. Let b be an integer.
For all $[a_1]_b, [a_2]_b \in \mathbf{\Phi}(b)$, $[a_1]_b [a_2]_b = [a_2]_b [a_1]_b$.

Proof.

$$[a_1]_b [a_2]_b = [a_1 a_2]_b = [a_2 a_1]_b = [a_2]_b [a_1]_b$$

Quod. Erat. Demonstrandum. □

Lemma 3.5. Let b be an integer.
For all $[a_1]_b, [a_2]_b, [a_3]_b \in \mathbf{\Phi}(b)$, $([a_1]_b [a_2]_b)[a_2]_b = [a_1]_b ([a_2]_b [a_2]_b)$.

Proof.

$$\begin{aligned} ([a_1]_b [a_2]_b)[a_3]_b &= [a_1 a_2]_b [a_3]_b = [(a_1 a_2) a_3]_b \\ &= [a_1 (a_2 a_3)]_b = [a_1]_b [a_2 a_3]_b = [a_1]_b ([a_2]_b [a_3]_b) \end{aligned}$$

Quod. Erat. Demonstrandum. □

Lemma 3.6. Let b be an integer.
There exists $[1]_b \in \mathbf{\Phi}(b)$, such that for all $[a]_b \in \mathbf{\Phi}(b)$, $[1]_b [a]_b = [a]_b [1]_b = [a]_b$.

Proof. There exist $1, 0 \in \mathbb{Z}$, such that $(1)(1) + 0b = 1$, so $1, b$ are coprime, and:

$$[1]_b[a]_b = [1a]_b = [a]_b$$
$$[a]_b[1]_b = [a1]_b = [a]_b$$

Quod. Erat. Demonstrandum. □

Lemma 3.7. Let b be an integer. For all $[a]_b \in \mathbf{\Phi}(b)$, there exists $[x]_b \in \mathbf{\Phi}(b)$, such that $[x]_b[a]_b = [a]_b[x]_b = [1]_b$.

Proof. As a, b are coprime, there exist $x, y \in \mathbb{Z}$, such that $xa + yb = 1$, so there exist $a, y \in \mathbb{Z}$, such that $ax + yb = 1$, which implies x, b are coprime, and:

$$[x]_b[a]_b = [xa]_b = [1 - yb]_b = [1]_b$$
$$[a]_b[x]_b = [ax]_b = [1 - yb]_b = [1]_b$$

Quod. Erat. Demonstrandum. □

Proposition 3.8. Let b be an integer.
Multiplicative group of integers modulo b is an Abelian group.

Theorem 3.9. (**Euler's Theorem**)[2]
Let a, b be two integers, and $\phi(b) < +\infty$ be the order of $\mathbf{\Phi}(b)$.
If a, b are coprime, then $a^{\phi(b)} \equiv 1 (\text{mod } b)$, i.e., the order of a divides $\phi(b)$.

Proof. We may divide our proof into two parts.
Part 1: In this part, we prove that $f : \mathbf{\Phi}(b) \to \mathbf{\Phi}(b), f([c]_b) = [a]_b[c]_b$ is bijective.
For convenience, assume that $[a]_b^{-1} = [x]_b$.

$$\forall [c_1]_b, [c_2]_b \in \mathbf{\Phi}(b), f([c_1]_b) = f([c_2]_b) \implies [c_1]_b = [x]_b f([c_1]_b) = [x]_b f([c_2]_b) = [c_2]_b$$

$$\forall [d]_b \in \mathbf{\Phi}(b), \exists [c]_b = [x]_b[d]_b \in \mathbf{\Phi}(b), f([c]_b) = [d]_b$$

Hence, f is bijective.
Part 2: In this part, we prove that $[a]_b^{\phi(b)} = [1]_b$, so it follows that $a^{\phi(b)} \equiv 1 (\text{mod } b)$.

$$\prod_{[c]_b \in \mathbf{\Phi}(b)} [c]_b = \prod_{[c]_b \in \mathbf{\Phi}(b)} f([c]_b) = \prod_{[c]_b \in \mathbf{\Phi}(b)} ([a]_b[c]_b) = [a]_b^{\phi(b)} \prod_{[c]_b \in \mathbf{\Phi}(b)} [c]_b$$

We are done if we cancel out the term $\prod_{[c]_b \in \mathbf{\Phi}(b)} [c]_b$. Quod. Erat. Demonstrandum. □

Definition 3.10. (**Prime Number**)
Let p be an integer.
If $p \geq 2$, and p is only divisible by ± 1 and $\pm p$, then p is prime.

Theorem 3.11. (**Fermat's Little Theorem**)[2]
Let a, p be two integers.
If p is prime, then $a^p \equiv a (\text{mod } p)$.

Proof. We may divide our proof into two cases.
Case 1: If $a \equiv 0 (\text{mod } p)$, then $a^p \equiv 0 (\text{mod } p)$;
Case 2: If $a \not\equiv 0 (\text{mod } p)$, then a, p are coprime, so:

$$a^p \equiv a^{\phi(p)+1} \equiv a^{\phi(p)} a \equiv 1a \equiv a (\text{mod } p)$$

Combine the two parts above, we've proven the theorem.
Quod. Erat. Demonstrandum. □

Theorem 3.12. (**Wilson's Theorem**)[2]
Let p be an integer.
If p is prime, then $(p-1)! \equiv -1 (\text{mod } p)$.

Proof. We may divide our proof into two cases:
Case 1: If $p \leq 3$, then $1! \equiv 1 \equiv -1 (\text{mod } 2)$ and $2! \equiv 2 \equiv -1 (\text{mod } 3)$;
Case 2: If $p > 3$, then let's solve the following equation in prime field $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{aligned} x^2 \equiv 1 (\text{mod } p) &\iff x^2 - 1 \equiv 0 (\text{mod } p) \iff (x+1)(x-1) \equiv 0 (\text{mod } p) \\ &\iff x + 1 \equiv 0 \text{ or } x - 1 \equiv 0 (\text{mod } p) \iff x \equiv -1 \text{ or } x \equiv 1 (\text{mod } p) \end{aligned}$$

Hence, we can group every pair of distinct classes $[a_1]_p, [a_2]_p \in \mathbf{\Phi}(b) \backslash \{[-1]_p [1]_p\}$, such that $[a_1]_p [a_2]_p = [a_2]_p [a_1]_p = [1]_p$, so:

$$[(p-1)!]_p = \prod_{a=1}^{p-1} [a]_p = [1]_p [p-1]_p \prod_{a=2}^{p-2} [a]_p = [-1]_p$$

Quod. Erat. Demonstrandum. □

4 Chinese Remainder Theorem

Lemma 4.1. Let $m \geq 2$ be an integer, and $(b_k)_{k=1}^m$ be a finite pairwisely coprime list of integers. The simultaneous congruence system $(x \equiv 0 (\text{mod } b_k))_{k=1}^m$ has general solution $x \equiv 0 (\text{mod } B)$, where B is the product of each b_k.

Proof. We may prove by induction.
Basis Step: When $m = 2$, for all $\xi \in \mathbb{Z}$:

Assume that ξ is a solution to the simultaneous system:

$$\begin{aligned}
\xi \equiv 0(\text{mod } b_1) &\implies \exists q_1 \in \mathbb{Z}, \xi = q_1 b_1 \\
\xi \equiv 0(\text{mod } b_2) &\implies \exists q_2 \in \mathbb{Z}, \xi = q_2 b_2 \\
b_1, b_2 \text{ are coprime} &\implies \exists x_1, x_2 \in \mathbb{Z}, x_1 b_1 + x_2 b_2 = 1 \\
&\implies \exists Q = x_2 q_1 + x_1 q_2 \in \mathbb{Z}, q_1 = Q b_2 \text{ and } q_2 = Q b_1 \\
&\implies \exists Q \in \mathbb{Z}, \xi = Q(b_1 b_2) \\
&\implies \xi \equiv 0(\text{mod } b_1 b_2)
\end{aligned}$$

So ξ is a solution to the product system.
Assume that ξ is a solution to the product system:

$$\begin{aligned}
\xi \equiv 0(\text{mod } b_1 b_2) &\implies \exists Q \in \mathbb{Z}, \xi = Q(b_1 b_2) \\
&\implies \exists q_1 = Q b_2, q_2 = Q b_1 \in \mathbb{Z}, \xi = q_1 b_1 = q_2 b_2 \\
&\implies \xi \equiv 0(\text{mod } b_1) \text{ and } \xi \equiv 0(\text{mod } b_2)
\end{aligned}$$

So ξ is a solution to the simultaneous system.
Hence, the statement is true when $m = 2$.
Inductive Hypothesis: For all integer $t \geq 2$, when $m = t$, assume that the simultaneous congruence system $(x \equiv 0(\text{mod } b_k))_{k=1}^{t}$ has general solution $x \equiv 0(\text{mod } B)$.
Inductive Step: When $m = t + 1$, for all $\xi \in \mathbb{Z}$:

$$\begin{aligned}
\xi \text{ is a solution to} (x \equiv 0(\text{mod } b_k))_{k=1}^{t+1} &\iff (\xi \equiv 0(\text{mod } b_k))_{k=1}^{t} \text{ and } \xi \equiv 0(\text{mod } b_{t+1}) \\
&\iff \xi \equiv 0(\text{mod } B) \text{ and } \xi \equiv 0(\text{mod } b_{t+1}) \\
&\iff \xi \equiv 0(\text{mod } B b_{t+1})
\end{aligned}$$

Hence, the statement is true when $m = t + 1$.
Combine the three parts above, we've proven that the statement holds for all integer $m \geq 2$. Quod. Erat. Demonstrandum. □

Lemma 4.2. Let $m \geq 2$ be an integer, and $(b_k)_{k=1}^{m}$ be a finite pairwisely coprime list of integers, and $l \leq m$ be a natural number. The simultaneous congruence system $(x \equiv \delta_{l,k}(\text{mod } b_k))_{k=1}^{m}$ has general solution $x \equiv B_l X_l(\text{mod } B)$, where B is the product of each b_k, B_l is the product of each b_k except b_l, and $[X_l]_{b_l}$ is the inverse of $[B_l]_{b_l}$ in $\mathbf{\Phi}(b_l)$.

Proof. The solution set of the homogeneous linear system described in **Lemma 4.1.** is an ideal of $\mathbb{Z}$. So the solution set of the nonhomogeneous linear system here is a coset. It suffices to prove that $x = B_l X_l$ is a specific solution. Let's prove by cases.
Case 1: If $k = l$, then $[B_l]_{b_l}[X_l]_{b_l} = [1]_{b_l}$, so $B_l X_l \equiv 1 \equiv \delta_{l,l}(\text{mod } b_l)$.
Case 2: If $k \neq l$, then b_k divides B_l, so $B_l X_l \equiv 0 = \delta_{l,k}(\text{mod } b_k)$.
Combine the two cases above, we've proven that $x = B_l X_l$ is a specific solution.

Quod. Erat. Demonstrandum. □

Theorem 4.3. (**Chinese Remainder Theorem**)
Let $m \geq 2$ be an integer, and $(b_k)_{k=1}^m$ be a finite pairwisely coprime list of integers, and $(a_k)_{k=1}^m$ be a finite list of integers. The simultaneous congruence system $(x \equiv a_k \bmod b_k)_{k=1}^m$ has general solution $x \equiv \Sigma_{k=1}^m a_k B_k X_k (\bmod B)$, where B is the product of each b_k, each B_l is the product of each b_k except b_l, and each $[X_l]$ is the inverse of $[B_l]$ in $\mathbf{\Phi}(b_l)$.

Proof. Again, it suffices to prove that $x = \sum_{k=1}^m a_k B_k X_k$ is a specific solution, which can be done by Fourier expansion:

$$\sum_{k=1}^{m} a_k B_k X_k \equiv \sum_{k=1}^{m} a_k \delta_{k,l} \equiv a_l (\bmod\ b_l)$$

Quod. Erat. Demonstrandum. □

5 Quadratic Residue

Lemma 5.1. Let p be an odd prime number, and a be an integer such that $p \nmid a$. If some integer x satisfies $x^2 \equiv a (\bmod\ p)$, then $a^{\phi(p)/2} \equiv 1 (\bmod\ p)$.

Proof. Since x, p are coprime:

$$a^{\phi(p)/2} \equiv (x^2)^{\phi(p)/2} \equiv x^{2[\phi(p)/2]} \equiv x^{\phi(p)} \equiv 1 (\bmod\ p)$$

Quod. Erat. Demonstrandum. □

Lemma 5.2. Let p be an odd prime number, and a be an integer such that $p \nmid a$. If no integer x satisfies $x^2 \equiv a (\bmod\ p)$, then $a^{\phi(p)/2} \equiv -1 (\bmod\ p)$.

Proof. Since $x^2 \equiv a (\bmod\ p)$ has no solution in prime field $\mathbb{Z}/p\mathbb{Z}$, we can group every pair of distinct classes $[c_1]_p, [c_2]_p \in \mathbf{\Phi}(b)$, such that $[c_1]_p [c_2]_p = [c_2]_p [c_1]_p = [a]_p$, so:

$$[a]_p^{\phi(p)/2} = \prod_{c=1}^{p-1} [c]_p = [(p-1)!]_p = [-1]_p$$

Quod. Erat. Demonstrandum. □

Definition 5.3. (**Legendre Symbol**)[3]
Let p be an odd prime number, and a be an integer.
We define Legendre symbol of a over p as:

$$\left(\frac{a}{p}\right) \equiv a^{\phi(p)/2} \equiv \begin{cases} 1 & \text{if} \quad x \neq 0 \text{ and } \exists x \in \mathbb{Z}, x^2 \equiv a (\text{mod } p); \\ -1 & \text{if} \quad x \neq 0 \text{ and } \forall x \in \mathbb{Z}, x^2 \not\equiv a (\text{mod } p); \\ 0 & \text{if} \quad x = 0; \end{cases}$$

Lemma 5.4. Let p be an odd prime number, and a_1, a_2 be two integers.

$$\left(\frac{a_1 a_2}{p}\right) \equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) (\text{mod } p)$$

Proof.

$$\left(\frac{a_1 a_2}{p}\right) \equiv (a_1 a_2)^{\phi(b)/2} \equiv a_1^{\phi(b)/2} a_2^{\phi(b)/2} \equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) (\text{mod } p)$$

Quod. Erat. Demonstrandum. □

Lemma 5.5. Let p be an odd prime number.
(1) There are $\phi(p)/2$ classes in $\mathbf{\Phi}(p)$ whose element a satisfies $(\frac{a}{p}) \equiv 1 (\text{mod } p)$;
(2) There are $\phi(p)/2$ classes in $\mathbf{\Phi}(p)$ whose element a satisfies $(\frac{a}{p}) \equiv -1 (\text{mod } p)$.

Proof. As $\mathbb{Z}/p\mathbb{Z}$ is a field, the perfect squares $[a_1]_p^2, [a_2]_p^2$ are equal if and only if $[a_1]_p - [a_2]_p = [0]_p$ or $[a_1]_p + [a_2]_p = [0]_p$, so classes in $\mathbf{\Phi}(p)$ give $\phi(p)/2$ distinct perfect squares:

$$[1]_p^2, [2]_p^2, [3]_p^2, \cdots, [\phi(p)/2]_p^2$$

The rest classes in $\mathbf{\Phi}(p)$ are not perfect squares. Quod. Erat. Demonstrandum. □

Lemma 5.6. Let p be an odd prime number, and a be an integer with $(\frac{a}{p}) \equiv 1 (\text{mod } p)$. There exists an integer b, such that $(\frac{b^2-a}{p}) \equiv -1 (\text{mod } p)$.

Proof. Assume to the contrary that for all integer b, $(\frac{b^2-a}{p}) \equiv 0$ or $1 (\text{mod } p)$.
(1) **Lemma 5.5.** ensures the existence of integer s with $(\frac{s}{p}) \equiv -1 (\text{mod } p)$.
(2) For all such integer s with $(\frac{s}{p}) \equiv -1 (\text{mod } p)$, integer $a + s$ also satisfies $(\frac{a+s}{p}) \equiv -1 (\text{mod } p)$, otherwise $s = b^2 - a$ will satisfy $(\frac{s}{p}) \equiv 1 (\text{mod } p)$, a contradiction.
(3) The above argument gives a finite list of p distinct classes $([s + ka]_p)_{k=0}^{p-1}$, whose element a satisfies $(\frac{a}{p}) \equiv -1 (\text{mod } p)$, which contradicts with **Lemma 5.5.**.
Quod. Erat. Demonstrandum. □

Lemma 5.7. Let p be an odd prime number, a be an integer with $(\frac{a}{p}) \equiv 1 (\text{mod } p)$, and b be an integer with $(\frac{b^2-a}{p}) \equiv -1 (\text{mod } p)$.
If we define w as a number with $w^2 \equiv b^2 - a (\text{mod } p)$,
then $\mathbb{Z}/p\mathbb{Z}[w] = \{[x]_p + w[y]_p : [x]_p, [y]_p \in \mathbb{Z}/p\mathbb{Z}\}$ is a field.

Proof. We may divide our proof into eleven parts.
Part 1: We define addition as the following mapping:

$$\mathbb{Z}/p\mathbb{Z}[w] \times \mathbb{Z}/p\mathbb{Z}[w] \to \mathbb{Z}/p\mathbb{Z}[w], ([x_1]_p + w[y_1]_p, [x_1]_p + w[y_2]_p) \mapsto$$

$$([x_1]_p + [x_2]_p) + w([y_1]_p + [y_2]_p)$$

Part 2: Addition is commutative in $\mathbb{Z}/p\mathbb{Z}$,
so addition is commutative in $\mathbb{Z}/p\mathbb{Z}[w]$.
Part 3: Addition is associative in $\mathbb{Z}/p\mathbb{Z}$,
so addition is associative in $\mathbb{Z}/p\mathbb{Z}[w]$.
Part 4: $[0]_p$ is an additive identity in $\mathbb{Z}/p\mathbb{Z}$,
so $[0]_p + w[0]_p$ is an additive identity in $\mathbb{Z}/p\mathbb{Z}[w]$.
Part 5: For all $[x]_p + w[y]_p \in \mathbb{Z}/p\mathbb{Z}[w]$, $[-x]_p, [-y]_p$ are additive inverses of $[x]_p, [y]_p$ in $\mathbb{Z}/p\mathbb{Z}$, so $[-x]_p + w[-y]_p$ is an additive inverse of $[x]_p + w[y]_p$ in $\mathbb{Z}/p\mathbb{Z}[w]$.
Part 6: We define multiplication as the following mapping:

$$\mathbb{Z}/p\mathbb{Z}[w] \times \mathbb{Z}/p\mathbb{Z}[w] \to \mathbb{Z}/p\mathbb{Z}[w], ([x_1]_p + w[y_1]_p, [x_1]_p + w[y_2]_p) \mapsto$$

$$([x_1]_p[x_2]_p + (b^2 - a)[y_1]_p[y_2]_p) + w([x_1]_p[y_2]_p + [y_1]_p[x_2]_p)$$

Part 7: Multiplication is commutative in $\mathbb{Z}/p\mathbb{Z}$,
so multiplication is commutative in $\mathbb{Z}/p\mathbb{Z}[w]$.
Part 8: Multiplication is associative in $\mathbb{Z}/p\mathbb{Z}$,
so multiplication is associative in $\mathbb{Z}/p\mathbb{Z}[w]$.
Part 9: $[1]_p$ is a multiplicative identity in $\mathbb{Z}/p\mathbb{Z}$,
so $[1]_p + w[0]_p$ is a multiplicative identity in $\mathbb{Z}/p\mathbb{Z}$.
Part 10: For all $[x]_p + w[y]_p \in \mathbb{Z}/p\mathbb{Z} \backslash \{[0]_p + w[0]_p\}$, $[x]_p \neq [0]_p$ or $[y]_p \neq [0]_p$, so:

$$\left(\frac{x^2}{p}\right) \neq \left(\frac{b^2 - a}{p}\right)\left(\frac{y^2}{p}\right)$$

Lemma 5.4. suggests that $[x^2 - (b^2 - a)y^2]_p \neq [0]_p$,
so the following multiplicative inverse is always valid:

$$\frac{[x]_p + w[-y]_p}{[x^2 - (b^2 - a)y^2]_p}$$

Part 11: Multiplication distributes over addition in $\mathbb{Z}/p\mathbb{Z}$,
so multiplication distributes over addition in $\mathbb{Z}/p\mathbb{Z}[w]$.
Quod. Erat. Demonstrandum. □

Theorem 5.8. (**Cipolla's Algorithm**)
Let p be an odd prime number, and a be an integer with $(\frac{a}{p}) \equiv 1(\text{mod } p)$, and b be an integer with $(\frac{b^2-a}{p}) \equiv -1(\text{mod } p)$.
If we define w as a number with $w^2 \equiv b^2 - a(\text{mod } p)$, then:
(1) $(b+w)^{\phi(p)/2}(b+w)$ is a solution to $z^2 \equiv a(\text{mod } p)$ in $\mathbb{Z}[w]$;
(2) $(b+w)^{\phi(p)/2}(b+w)$ is real, and it is a solution to $x^2 \equiv a(\text{mod } p)$ in $\mathbb{Z}$.

Proof.

$$\begin{aligned}
[(b+w)^{\phi(p)/2}(b+w)]^p &\equiv (b+w)^{\phi(p)}(b+w)^2 \equiv (b+w)(b+w)^p \\
&\equiv (b+w)\sum_{k=0}^{p}\binom{p}{k}b^{n-k}w^k \equiv (b+w)(b^p+w^p) \\
&\equiv (b+w)\left[\left(\frac{b^2}{p}\right)b + \left(\frac{b^2-a}{p}\right)w\right] \\
&\equiv (b+w)(b-w) \equiv b^2-(b^2-a) \equiv a(\text{mod } p)
\end{aligned}$$

This shows that $(b+w)^{\phi(p)/2}(b+w)$ is a solution to $z^2 \equiv a(\text{mod } p)$ in $\mathbb{Z}[w]$.
As $(\frac{a}{p}) \equiv 1(\text{mod } p)$, $z^2 \equiv a(\text{mod } p)$ actually has two distinct solutions $x_1, x_2 \in \mathbb{Z}/p\mathbb{Z}$, where $\mathbb{Z}/p\mathbb{Z}$ is a subfield of $\mathbb{Z}/p\mathbb{Z}[w]$, so:

$$\begin{aligned}
z^2 \equiv a(\text{mod } p) &\iff z^2 - a \equiv 0(\text{mod } p) \iff (z-x_1)(z-x_2) \equiv 0(\text{mod } p) \\
&\iff z - x_1 \equiv 0 \text{ or } z - x_2 \equiv 0(\text{mod } p) \iff z \equiv x_1 \text{ or } z \equiv x_2(\text{mod } p)
\end{aligned}$$

The above argument proves that $(b+w)^{\phi(p)/2}(b+w)$ has to be real.
Quod. Erat. Demonstrandum. □

References

[1] H. Ren, "Template for math notes," 2021.

[2] "Theorems of Fermat, Euler, and Wilson," jul 8 2021, [Online; accessed 2024-09-05].

[3] "Legendre Symbol," jul 8 2021, [Online; accessed 2024-09-05].