Elementary Number Theory

Thaqib Mo.

November 18, 2020

1 Integral Domains

Definition 1: Integral Domains

Let R be a commutative ring, then $a \in R$ is called the *zero divisor*, if there is some $b \in R$ with $b \neq 0$ for which $ab = 0$.

An *Integral Domain* is a commutative ring R, with $R \neq \{0\}$ such that 0 is the only *zero divisor*. If we have $ab = 0$ then either $a = 0$ or $b = 0$.

We can define Integral Domains in another equivalent way using the "cancellation law".

Theorem 1

A commutative ring $R \neq \{0\}$ is an integral domain if and only if for all $a, b, c \in R$ if $a \neq 0$ and

$$ab = ac$$

Then

$$b = c$$

Proof. Suppose R is an integral domain, and we have $ab = ac$ and $a \neq 0$ then $ab - ac = 0$ and then $a(b - c) = 0$. Since R is an integral domain we must have $b - c = 0$ that implies $b = c$.

Now suppose R is a ring where the commutative property holds. Assume we have $ab = 0$ If $a = 0$ we are done, suppose $a \neq 0$ then

$$ab = a \cdot 0 \rightsquigarrow b = 0$$

□

Example 1. The ring $\mathbb{Z}$ is an integral domain.

Example 2. The commutative rings $\mathbb{Q}, \mathbb{R}$ are an integral domains.

The rings $\mathbb{Q}$ and $\mathbb{R}$ are more than rings. They are also *fields.*

Definition 2: Fields

A ring F is called a *field* if it is commutative, and if every non zero element in F has a multiplicative inverse. That means if $a \in F$ with $a \neq 0$ then we have $b \in F$ such that

$$ab = 1$$

For the fields $\mathbb{Q}, \mathbb{R}$ if we have $r \in \mathbb{Q}$ then we also have $\frac{1}{r} \in \mathbb{Q}$ and $r \cdot \frac{1}{r} = 1$. The same applies for the field $\mathbb{R}$. The ring $\mathbb{Z}$ is not a field since not every element has a multiplicative inverse.

Theorem 2

Every subring of a field is an integral domain. In particular, every field is an integral domain.

Proof. Let F be a field and R be a sub ring. Since $\times$ in R and $\times$ in F is the same, $(R, \times)$ is commutative and R is a commutative ring. Now suppose we have $a, b \in R$ such that $ab = 0$. If $a = 0$ we are done. Assume $a \neq 0$ since this equation also holds in F then there is some $a^{-1} \in F$ such that $aa^{-1} = 1$ then we get

$$ab = 0$$

$$aba^{-1} = 0a^{-1}$$

$$b = 0$$

$\square$

Example 3. If $n \geq 2$ is composite then $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain. Since there is a factorization of $n = ab$ then $[a], [b]$ are both non zero elements with $[a][b] = [ab] = [n] = [0]$

Example 4. We define the ring of *Gaussian integers* denoted by $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ where addition is given by

$$a + bi + c + di = (a + b) + (c + d)i$$

and multiplication is given by

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

This is a subring is $\mathbb{C}$ the complex numbers.

1.1 Basic Properties of Integral Domains

Theorem 3

If R is an integral domain then $\text{Char}R = 0$ or $\text{Char}R$ is prime.

Proof. Suppose R is an integral domain and $\text{Char}R \neq 0$ and $\text{Char}R$ is not prime. Then if we have $\text{Char}R = 1$, then R is the zero ring since $1 = 0$, which is not possible due to the definition of integral domain. Now suppose $\text{Char}R = n$ where $n > 1$ is not prime. Then we have $n = ab$ then $a \cdot 1_R$ and $b \cdot 1_R$ are non zero elements but $(a \cdot 1)(b \cdot 1) = ab \cdot 1 = 0$ that contradicts the definition of an integral domain. $\square$

Note that this again shows that $\mathbb{Z}/n\mathbb{Z}$ is not an integral domain

Theorem 4

Every finite integral domain is a field.

Proof. Let R be an integral domain, and suppose $|R| = n$. Let $a \in R$ with $a \neq 0$ consider the multiplication map $\phi_a(r) = ar$ then ϕ is injective since if we have $\phi(r) = \phi(s)$ then $ra = sa$ since R is an integral domain we can use the cancellation property to get $r = s$.

So we have an injective function $\phi : R \to R$. Since R is finite then this implies ϕ is surjective. Given that ϕ is injective we have $|\phi(R)| = n$. Since ϕ is surjective there must be some $b \in R$ such that $\phi(b) = 1$ which means $ab = ba = 1$ thus a has an multiplicative inverse in R. By definition R is a field. □

1.2 Divisibility and Associates

Definition 3: Divisibility arbitrary integral domain

Let R be an integral domain, and let $a, b \in R$ we say a divides b and denote it by $a \mid b$ if there is some $c \in R$ such that $b = ac$

For example, consider the Gaussian integers $\mathbb{Z}[i]$ and we say that $2 + i$ divides 5 since $5 = (2 + i)(2 - i)$. If F is a field and $a \in F$ with $a \neq 0$ then $a \mid b$ for any $b \in F$ since $b = a(a^{-1}b)$.

Proposition 1

Let R be an integral domain

(1) For all $a \in R$, we have $a \mid a$.

(2) If $a, b, c \in R$ such that $a \mid b$ and $b \mid c$ then $a \mid c$.

(3) If $a, b, c \in R$ such that $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for all $x, y \in R$.

Proof. (1) Since $a = 1 \cdot a$ that means $a \mid a$.

(2) Given $a \mid b$ we know that $b = ak$ for some $k \in R$ and we also have $c = b\ell$ for some $\ell \in R$. Then

$$c = b\ell = (ak)\ell = a(k\ell)$$

That means we have $a \mid c$.

(3) We know that $b = ak$ and $c = a\ell$ for any $x, y \in R$ we have

$$bx + cy = akx + a\ell y = a(kx + \ell y)$$

Since $kx + \ell y \in R$ we have $a \mid bx + cy$

□

Note since the relation is reflexive and transitive we can define an equivalence relation $a \sim b$ if $a \mid b$ and $b \mid a$. if we have $a \sim b$ then we say a, b are *associate* in R.

We can also make another order relation on the set of equivalence classes under $\sim$ by $[a]_\sim \mid [b]_\sim$ if $a \mid b$. This is well defined and the choice of representative does not matter.

Definition 4

Let R be a ring and then $r \in R$ is called *unit* of R if r has multiplicative inverse in R. The set of all unit of R is denoted by R^*.

This is same as the the group of units of the monoid $(R, \times)$.

Theorem 5

Let R be an integral domain. Given $a, b \in R$ we have $a \sim b$ if and only if $a = ub$ for some $u \in R^*$

Proof. $(\Rightarrow)$ First assume, $a \sim b$ then we have $a \mid b$ and $b \mid a$ so we have $b = ak$ and $a = b\ell$ this leads to

$$b = ak = (b\ell)k = b(\ell k)$$

If we have $b = 0$ then $a = b\ell = 0\ell = 0$ so we have $a = 1 \cdot b$ and we know that $1 \in R^*$. Now consider the case $b \neq 0$, then $b \cdot 1 = b(\ell k)$ applying the cancellation property we get $1 = \ell k$ this means we have $\ell \in R^*$ so $a = \ell b$ where $\ell \in R$.

$(\Leftarrow)$ Suppose $a = ub$ this implies $b \mid a$ for some $u \in R^*$. Multiplying both sides by u^{-1} gives $u^{-1}a = u^{-1}ub \rightsquigarrow b = u^{-1}a$ so we have $a \mid b$.

□

We can apply this to the ring $\mathbb{Z}$ and we get $a \sim b$ if and only if $a = b$ or $a = -b$.

2 Division with Remainder and Greatest Common Divisor

2.1 Division with Remainder in $\mathbb{Z}$

Theorem 6: Quotient and Remainder in $\mathbb{Z}$

Let $a, b \in \mathbb{Z}$, with $b > 0$. Then there exists *unique* integers q, r with $0 \leq r < b$ such that

$$a = \left(b \times \underbrace{q}_{\text{quotient}} \right) + \overbrace{r}^{\text{remainder}}$$

Proof. There are 2 cases. First let $a \geq 0$ and consider the set

$$S = \{n \in \mathbb{N} : n = a - bq \text{ for some } q \in \mathbb{Z}\}$$

S is non empty since $a = a - b(0)$ so we have $a \in S$. So by the Well ordering principle S has a least element. Let r be the least element of S. Then $r = a - bq \rightsquigarrow a = bq + r$. We need to check if $0 \leq r < b$, we have $r \geq 0$ since r is a natural number. Now assume $r \geq b$ then $r - b \geq 0$ that means $r - b = a - bq - b = a - b(q+1)$ that means we have $r - b \in S$ which is a contradiction since r was the least element. Thus we have $0 \leq r < b$.

Otherwise , if $a < 0$ then $-a > 0$ and the first part gives $q_0, r_0 \in \mathbb{Z}$ such that $-a = bq_0 + r_0$. Now if we have $r_0 = 0$ then $-a = bq_0 \rightsquigarrow a = b(-q_0)$. Otherwise if we have $r \neq 0$ then we can write

$$a = b(q_0) - r_0 = b(q_0) - b + b - r_0$$
$$= b(q_0 - 1) + b - r_0$$

We have $q = q_0 - q$ and $r = b - r_0$ both in $\mathbb{Z}$ and $0 < b - r_0 < b$. we have proven the existence of r, q for all $a \in \mathbb{Z}$.

To prove *uniqueness* consider q', r' such that $a = bq' + r'$ we have

$$r + bq = r' + bq'$$

This means we have $r - r' = b(q - q')$ if we have $q = q'$ then $r = r'$ and we are done. Otherwise , if $q \neq q'$ taking the absolute values of both sides

$$|r - r'| = |b||q - q'| \geq b$$

But r, r' are both positive and strictly less than b, so $|r - r'| \geq b$ is a contradiction. So we must have $q' = q \to r = r'$. $\square$

2.2 Division with Remainder in $\mathbb{Z}[i]$

Definition 5: Norm

For $a + bi \in \mathbb{Z}[i]$ we define *norm* of $a + bi$ written as $N(a + bi)$ to be $a^2 + b^2 \in \mathbb{N}$

Example 5. Suppose we want to divide $2 + i$ by $1 + i$ with remainder then we must have

$$2 + i = (1 + i)\gamma + \delta$$

With $0 \geq N(\delta) < N(1 + i)$. First we know that

$$\frac{2 + i}{1 + i} = \frac{3}{2} - \frac{1}{2}i$$

Now we have 4 choices to round this up to the nearest integer. We can so $\frac{3}{2} \to 2$ or 1 and for $\frac{-1}{2}$ we can do 0 or -1. Lets assume we take $\gamma = 2 + 0i$ then the remainder is

$$(2 + i) - (1 + i)2 = -i$$

This leads to $(2 + i) = (1 + i)2 + (-i)$ this remainder is valid since $N(-i) = 1 < N(1 + i)$. We need to show that this works in general.

Theorem 7: Division with remainder in Gaussian integers

Let $\alpha, \beta \in \mathbb{Z}[i]$ then there exists $\gamma, \delta \in \mathbb{Z}[i]$ such that

$$\alpha = \beta\gamma + \delta$$

Proof. Let $\alpha = a + bi$ and $\beta = c + di$ performing division in $\mathbb{C}$ we get

$$\frac{a + bi}{c + di} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2} = r + si$$

Now we choose $m, n \in \mathbb{Z}$ such that $|m - r| \leq \frac{1}{2}$ and $|n - s| \leq \frac{1}{2}$. Then let $\gamma = m + ni \in \mathbb{Z}[i]$ and set $\delta = \alpha - \beta\gamma$, so we have $\alpha = \beta\gamma + \delta$ but we need to show $0 \leq N(\delta) < N(\beta)$. We have $0 \leq N(\delta)$ holds by definition now consider

$$\delta = \alpha - \beta\gamma = \beta(r + si) - \beta(m + ni) = \beta((r - m) + (s - n)i)$$

Taking the complex absolute value and squaring $N(\delta) = |\delta|^2 = |\beta|^2|(r - m) + (s - n)i|^2 = N(\beta)((r - m)^2 + (s - n)^2)$ Since we fixed $|r - m| \leq \frac{1}{2}$ and $|s - n| \leq \frac{1}{2}$ so we get $N(\delta) \leq N(\beta)/2 < N(\beta)$

□

In division with remainder in $\mathbb{Z}[i]$ we loose the uniqueness property. Since we could have choose from 4 possible values of γ which leads to valid values for δ.

Definition 6

Let R be an integral domain, R has a *division algorithm* if there exists a function

$$d : R \setminus \{0\} \to \mathbb{N}$$

called the *divisor function* such that for $a, b \in R$ with $b \neq 0$ we have $q, r \in R$ such that

$$a = bq + r$$

Then either $d(r) < d(b)$ or else $r = 0$

We have proven that both $\mathbb{Z}[i], \mathbb{Z}$ have division algorithm with divisor functions $d(\alpha) = N(\alpha)$ and $d(\alpha) = |\alpha|$ for integers.

2.3 Greatest Common Divisor

Given integers a, b we need to find d dividing both a, b and we need to choose the largest such integer with this property. This can be generalized to any integral domain.

Definition 7: Greatest Common Divisor

Let R be an integral domain let $a, b \in R$ with $a, b \neq 0$ and element $d \in R$ is called the greatest common divisor $(\gcd(a, b))$ if:

#1 $d \mid a$ and $d \mid b$

#2 If $f \in R$ another common divisor of a, b such that $f \mid a$ and $f \mid b$ then $f \mid d$

The gcd of 2 elements may not be unique, rather it picks out a unique equivalence class with respect to the associate relation $\sim$. We can see that in the next theorem.

Theorem 8

Let R be an integral domain. Let $a, b \in R$ with $a, b \neq 0$. If d_1 and d_2 are both greatest common divisor of a, b then $d_1 \sim d_2$. Conversely if d_1 is a greatest common divisor of a, b then $d_1 \sim d_2$ where d_2 is another greatest common divisor.

Proof. Suppose d_1, d_2 are both greatest common divisor of a, b. Since d_1 is a common divisor of a, b and d_2 is the gcd we must have $d_1 \mid d_2$. By symmetry we also have $d_2 \mid d_1$ by definition of the relation we have $d_1 \sim d_2$

Now assume, d_1 is a gcd of a, b and that $d_2 \mid d_1$. Then $d_1 \mid d_2$ and $d_2 \mid d_1$. The transitive property gives $d_2 \mid a$ and $d_2 \mid b$. So d_2 is a common divisor of a, b. Now assume e another common divisor of a, b we must have $e \mid d_1$ again by transitivity we get $e \mid d_2$. Thus d_2 is a gcd of a, b by definition. □

So gcd is not unique in integral domain. It picks out a unique equivalence class $R/\sim$. Then by theorem Theorem 5, if d is a greatest common divisor it takes the form ud for some chosen $u \in R^*$. So we can use the notation $\gcd(a, b)$ do denote the equivalence class of gcds.
For example in the ring $\mathbb{Z}$ if d is one gcd of a, b then do is $-d$ and it is the only other *gdc*.

3 The Euclidean Algorithm

Lemma 1

Let R be an integral domain. Suppose $a, b, q, r \in R$ such that

$$a = bq + r$$

Then some $d \in R$ is gcd of a, b if and only if it is the gcd of b, r. That is

$$\gcd(a, b) \sim \gcd(b, r)$$

Proof. Suppose $\gcd(a, b) = d$ then we have $d \mid a$ and $d \mid b$ it follows from Proposition 1 that

$$d \mid a + b(-q)$$

This is $d \mid r$ so d is a common divisor of both b, r. Now suppose e is a common divisor of b, r then $e \mid b$ and $e \mid b$ again we have

$$e \mid b \cdot q + r$$

So we have $e \mid a$ since e is a common divisor of both a, b then we have $e \mid d$. The same logic follows for the $(\Leftarrow)$ case. □

Now if we have a Integral Domain R with divisor function D we can use the above lemma to compute the gcd of $a, b \neq 0$. First we have

$$a = bq_0 + r_1$$

When $q_0, r_1 \in R$ by definition we have $r_1 = 0$ or $D(r_1) < D(b)$. If we have $r_1 = 0$ then we get $b \mid a$, then let e be another common divisor of a, b we have $e \mid a$ and $e \mid b$ by definition so $b = \gcd(a, b)$. Otherwise we use the lemma to get $\gcd(a, b) \sim \gcd(b, r_1)$ so the task is down to finding the gcd of b, r_1.

We can repeat the procedure to get

$$b = r_1 q_1 + r_2$$

Again either $r_2 = 0$ then r_1 is the gcd or $D(r_2) < D(r_2)$ we again have $\gcd(b, r_1) \sim \gcd(r_1, r_2)$ we continue this process until we get a 0 remainder. So to outline this process we have

$$\begin{aligned} a &= q_0 b + r_1 \\ b &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \\ r_{n-1} &= r_n q_n + 0 \end{aligned}$$

Since the sequence $D(r_1) > D(r_2) > D(r_3) > \cdots > D(r_{n-1})$ is a strictly decreasing sequence of natural numbers, it is bounded below by 0 and it must reach a zero remainder at some point. Using the lemma we get $\gcd(a, b) = r_n$, this leads to the following theorem.

Theorem 9

Let R be an integral domain with a division algorithm. Given any two non zero elements $a, b \in R$ $\gcd(a, b)$ exists.

3.1 Extended Euclidean Algorithm

We can utilize the euclidean algorithm to compute the solutions to linear equations. Suppose we have an integral domain R with division algorithm and non-zero $a, b \in R$. Suppose we have $\gcd(a, b) = d$ we can find $x, y \in R$ such that

$$ax + by = d$$

After running the euclidean algorithm we get

$$\begin{aligned} a &= q_0 b + r_1 \\ b &= r_1 q_1 + r_2 \\ r_1 &= r_2 q_2 + r_3 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n \end{aligned}$$

With the last step with zero remainder left out.

We can reverse the order of these equations and isolate the remainder in each one to get

$$
\begin{aligned}
r_n &= r_{n-2} - r_{n-1}q_{n-1} \\
r_{n-1} &= r_{n-3} - r_{n-2}q_{n-2} \\
&\vdots \\
r_2 &= b - r_1 q_1 \\
r_1 &= a - q_0 b
\end{aligned}
$$

We focus on the first 2 equations

$$
\begin{aligned}
r_n &= r_{n-2} - r_{n-1}q_{n-1} \\
r_{n-1} &= r_{n-3} - r_{n-2}q_{n-2}
\end{aligned}
$$

We can substitute r_{n-1} from the second equation in the first equation to get an equation in the form $r_{n-1} = r_{n-2}x + r_{n-3}y$ then we can use RHS from the third equation for r_{n-2} to get $r_{n-3}x + r_{n-4}y$ then we keep on repeating this until the final equation. This leads to the following theorem

Theorem 10

Let R be in integral domain with a division algorithm and let $a, b \in R$ with $a, b \neq 0$. If $d = \gcd(a, b)$ then there exists $x, y \in R$ such that

$$ax + by = d$$

4 Linear Diophantine Equations and Linear Congruences

4.1 Linear Diophantine Equations in Two Variables

Suppose R is an integral domain with a division algorithm given $a, b, c \in R$ a Linear Diophantine Equations in Two Variables is an equation of the form

$$ax + by = c$$

With $x, y \in R$, there are two main questions

(1) Does a solution to the equation exist?

(2) If yes, can we find **all** the solutions?

Theorem 11

Let $a, b, c \in R$ where R is an integral domain with both a, b not being zero. If there is a solution to the equation

$$ax + by = c$$

Then

$$\gcd(a, b) \mid c$$

Proof. Let $d = \gcd(a, b)$, by definition $d \mid a$ and $d \mid b$ so we must have

$$d \mid ax + by \rightsquigarrow d \mid c$$

□

Theorem 12

Let $a, b, c \in R$ where R is an integral domain with both a, b not being zero. Suppose $\gcd(a, b) \mid c$ then the equation

$$ax + by = c$$

has a solution with $x, y \in R$

Proof. Let $d = \gcd(a, b)$ this exists, by Theorem 9. Moreover by Theorem 10 there exists $x_0, y_0 \in R$ such that

$$ax_0 + by_0 = d$$

Since $d \mid c$ we have $c = kd$ we get

$$c = kd = k(ax_0 + by_0) = a(kx_0) + b(ky_0)$$

$\square$

4.2 Divisibility Results

To solve linear Diophantine equations, it is necessary to establish a few results on divisibility.

Theorem 13

Suppose R is an integral domain with a division algorithm suppose we are given $a, b, c \in R$. If $a \mid bc$ and $1 \sim \gcd(a, b)$ then $a \mid c$

Proof. Given $a \mid bc$ we know that $bc = ak$, then since $\gcd(a, b) = 1$ we have x, y such that

$$ax + by = 1$$

Then we have

$$acx + bcy = c$$

Now since $bc = ak$ we get

$$acx + aky = c$$

$$a(cx + ky) = c$$

Which means $a \mid c$ $\square$

Lemma 2

Let R be an integral domain with division algorithm and suppose we have $a, b \in R$ not both zero. Suppose $d = \gcd(a, b)$ then we have

$$a = a_0 d \ , \ b = b_0 d$$

Then $\gcd(a_0, b_0) \sim 1$

Proof. The equation

$$ax + by = d$$

always has a solution so we have

$$a_0 dx + b_0 dy = d$$

This leads to

$$a_0 x + b_0 y = 1$$

This means $\gcd(a_0, b_0) \mid 1$ and $1 \mid \gcd(a_0, b_0)$ holds. So we have $\gcd(a_0, b_0) \sim 1$. $\square$

4.3 The General Solution of a Linear Diophantine Equation

Theorem 14

Let R be an integral domain with a division algorithm. Let $a, b, c \in R$ such that both a, b are not zero and let $d = \gcd(a, b)$. Assume that $d \mid c$. Also we write $a = a_0 d$ and $b = b_0 d$ then the equation

$$ax + by = c$$

complete set of solutions are

$$(x, y) = (x_0 + kb_0, y_0 - ka_0)$$

Where $k \in R$ is arbitrary and (x_0, y_0) is a particular solution.

Proof. Let (x_0, y_0) be a particular solution to $ax + by = c$ which exists since $\gcd(a, b) \mid c$. Suppose we have another solution (x_1, y_1) then we know that

$$ax_0 + by_0 = c$$

$$ax_1 + by_1 = c$$

Then we get

$$a(x_1 - x_0) + b(y_1 - y_0) = 0$$

We have $a = a_0 d$ and $b = b_0 d$

$$a_0 d(x_1 - x_0) + b_0 d(y_1 - y_0) = 0$$

Applying the cancellation law in the integral domain leads to

$$a_0(x_1 - x_0) = -b_0(y_1 - y_0)$$

Then we have $b_0 \mid a_0(x_1 - x_0)$, but we have $\gcd(a_0, b_0) \sim 1$ by Lemma 2 so we get $b_0 \mid (x_1 - x_0)$ this means we have $x_1 - x_0 = kb_0$ this means we have $x_1 = x_0 + kb_0$. Using this substitution we have

$$a_0 k b_0 = -b_0(y_1 - y_0)$$

This means we have $ka_0 = y_0 - y_1$ this gives $y_1 = y_0 - ka_0$. So we have if (x_0, y_0) is a solution then so is $(x_0 + kb_0, y_0 - ka_0)$.

Conversely we can also check that every ordered pair $(x_1, y_1) = (x_0 + kb_0, y_0 - ka_0)$ is a solution then we have

$$ax_1 + by_1 = a(x_0 + kb_0) + b(y_0 - ka_0) = ax_0 + by_0 + k(ab_0 - ba_0) = c + k(da_0b_0 - db_0a_0) = c$$

$\square$

4.4 Multiplicative Inverses in $\mathbb{Z}/n\mathbb{Z}$

Using Diophantine equation we can construct a procedure for calculating multiplicative inverse of an element when it exists in $\mathbb{Z}/n\mathbb{Z}$. Suppose we have $[a] \in \mathbb{Z}/n\mathbb{Z}$ Then some $[x]$ is the inverse if and only if $[a][x] = [1]$ this means we have

$$ax \equiv 1 \bmod n$$

This is equivalent to $n \mid 1 - ax$ this means we have $1 - ax = ny$ so we have

$$ax + ny = 1$$

Thus finding multiplicative inverse we can find the inverse. Moreover it exists if and only if $\gcd(a, n) = 1$. In the case where $n = p$ is prime then $[a] \in \mathbb{Z}/p\mathbb{Z}$ such that $[a] \neq [0]$, then $\gcd(a, p) = 1$, because we have $a \nmid p$ so there are no common divisors other than 1. This proves that every non-zero element in $\mathbb{Z}/p\mathbb{Z}$ has an inverse therefore it is a field.

Example 6. Suppose we want to find inverse of $[5] \in \mathbb{Z}/13\mathbb{Z}$ this means we have to solve

$$5x + 13y = 1$$

So we run the euclidean algorithm to get

$$\begin{aligned} 13 &= 5(2) + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

So we have $\gcd(5, 13) = 1$ and $[5]^{-1}$ exists. Now we can use the back substitution to get

$$\begin{aligned} 1 &= 3 - 2 \\ 2 &= 5 - 3 \\ 3 &= 13 - 5(2) \end{aligned}$$

Making the substitution we get

$$\begin{aligned}
1 &= 3 - 2 \cdot 1 \\
&= 3 - (5 - 3) \cdot 1 \cdot 1 \\
&= 3 \cdot 2 - 5 \\
&= (13 - 5(2)) \cdot 2 - 5 \cdot 1 \\
&= 13 \cdot 2 - 5 \cdot 5
\end{aligned}$$

So the solution is $x = -5$ so we have $[5]^{-1} = [-5] = [8]$