3) $(R, +, \cdot)$ unitary commutative ring

Assume there is $a \in R$ $(a \neq 0)$ that is invertible and zero divisor

$$\Downarrow \qquad\qquad\qquad \Downarrow$$

$$(*)\ \exists b \in R \quad ab = 1 \qquad\qquad \exists c \neq 0 \quad ac = 0$$

$$c = 1c \overset{(*)}{=} abc = b(ac) = b \cdot 0 = 0$$

$f: X \to Y$

$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

we assumed $x_1, x_2 \in X$ $f(x_1) = f(x_2) \rightsquigarrow \dots \rightsquigarrow x_1 = x_2$

4)

	invertible	not invertible
zero divisor	X	O
not zero divisor	O	

Assume $\exists a \neq 0$: a is $\underbrace{\text{not invertible}}_{\forall b \neq 0 \ \boxed{ab \neq 1}}$ and $\underbrace{\text{not a zero divisor}}_{\forall b \neq 0 \ \boxed{ab \neq 0}}$

$|R| = n$

$R \setminus \{0\} \ni b \longmapsto ab \in R \setminus \{0, 1\}$

$|R \setminus \{0\}| = n - 1 \qquad |R \setminus \{0,1\}| = n - 2$

$\Rightarrow \exists b_1, b_2 \neq 0$, $b_1 \neq b_2$ $\quad ab_1 = ab_2 \Rightarrow a\underbrace{(b_1 - b_2)}_{\neq 0} = 0 \Rightarrow a$ is a zero divisor

A: a is not invertible

$f(x) = ax$

B

$\Rightarrow \dots \Rightarrow a$ zero divisor

$A \Rightarrow B \qquad A \wedge \bar{B} = 0$

zero divisor $a \neq 0 : \exists b \neq 0 \quad ab = 0$

invertible $a \neq 0 : \exists b \neq 0 \quad ab = 1$

Q: $\exists x\, \forall y\, \forall z\, \exists \alpha \quad P(x_1, y_1, z_1, \alpha)$

$\boxed{\exists b \neq 0 \quad ab = 0}$

$\forall b \neq 0$ $\quad$ not$(ab=0)$

$\underbrace{\text{not}(ab=0)}$

$ab \neq 0$

5) $\mathbb{Z}_n$ field $\Leftrightarrow$ n is prime

"$\Rightarrow$" let n be not prime (using contraposition)

$\boxed{\exists\, a, b > 1} : ab = n$

(*) $\quad 1 \cdot n = n \quad n = ab > a$

$\boxed{1 < a < n}$ $\quad [a]_n \cdot [b]_n = [a \cdot b]_n = [n]_n = [0]_n$

left to show : $[a]_n \neq [0]_n$ is true b> (*)

$[1]_n \, [n]_n = [0]_n$

$\Downarrow$

$[0]_n$

$\Leftarrow$ Proposition 2: it is sufficient to show that there are no zero divisors.

Assume $[a]_n, [b]_n \neq [0]_n$, $[a]_n [b]_n = [0]_n$

$a, b < \mathbb{Z} \setminus \{0\}$

$n \mid (ab)$

$\Rightarrow n \mid a \vee n \mid b$

w.l.o.g assume $n \mid a \Rightarrow hn = a \Rightarrow [a]_n = [hn]_n = [0]_n$

($p \in P \Leftrightarrow 1, p$ divide p
no other no. divides p.
$n = 1 \cdot n$)

$6 \mid (10 \cdot 9)$
$\overset{\shortparallel}{2 \cdot 3}$ $\quad 2 \mid 10 \quad 3 \mid 9$

6) Little Fermat's theorem

Let $p \in \mathbb{N}$ be prime,

Then for $a \in \mathbb{Z}_p \setminus \{0\}$:

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

Learn everything that has a name, proposition it's fine.

Proof: $f(x) = ax$ By S..., we know that f is bijective

$$\prod_{x \in \mathbb{Z}_p \setminus \{0\}} x \equiv \prod_{x \in \mathbb{Z}_p \setminus \{0\}} f(x) \equiv \prod_{x \in \mathbb{Z}_p \setminus \{0\}} ax \equiv a^{p-1} \underbrace{\prod_{x \in \mathbb{Z}_p \setminus \{0\}} x}_{} \mod p$$

$1 \cdot 2 \cdot 3 \cdot 4 = 3 \cdot 1 \cdot 4 \cdot 2$

Reshuffling as f,s bijective $\quad$ definition of f $\quad$ commutativity

$\mathbb{Z}_5$ $\quad a = 3$

x	[1]	[2]	[3]	[4]
ax	[3]	[1]	[4]	[2]

Taking the inverse, we get,

$$1 \equiv a^{p-1} \mod p$$

SAMPLE EXAM 2

$\mathbb{Z}_n \quad n = 1111, \quad p = 11$

$\qquad\qquad\qquad\quad q = 101$

$x = 3535$

$y = 901$

1) Give a formula that defines a unitary isomorphism $\phi : \mathbb{Z}_{1111} \to \mathbb{Z}_{11} \times \mathbb{Z}_{101}$

$\phi : \mathbb{Z}_{1111} \to \mathbb{Z}_{11} \times \mathbb{Z}_{101}$

$\phi([z]_{1111}) = ([z]_{11}, [z]_{101})$

2) Use the EEA to deduce an explicit formula for the inverse isomorphism $\phi^{-1} : \mathbb{Z}_{11} \times \mathbb{Z}_{101} \to \mathbb{Z}_{1111}$

$101 = 9.11 + 2$	$1 = 11 - 5.2$
$11 = 5.2 + 1$	$1 = 11 - 5(101 - 9.11)$
	$1 = 11 - 5.101 + 45.11$
	$1 = \underbrace{46.11}_{506} - \underbrace{5.101}_{505}$

$\phi^{-1}([z_1]_{11}, [z]_{101}) = [-505 z_1 + 506 z_2]_{1111}$

$\phi([-505 z_1 + 506 z_2]_{1111}) = ([\underbrace{-5.101}_{\equiv 1 \bmod 11} z_1 + \cancel{46.11 z_2}]_{11}, [\cancel{-5.101 z_1} + 46.11 z_2]_{101})$

$= ([z_1]_{11}, [z_2]_{101})$

3) Using ϕ and ϕ^{-1} and CRT and FLT, calculate x^{2024} efficiently

$[3535]_{1111}^{2024} = ?$

$3535 \equiv 4 \bmod 11$

$3535 \equiv 0 \bmod 101 \qquad a^{p-1} \equiv 1 \bmod p$

$3535 \equiv 0 \mod 101$ $\qquad a \equiv 1 \mod p$

$$[4]_{11}^{2024} = \underbrace{\left([4]_{11}^{10}\right)^{202}}_{[1]_{11}} \left([4]_{11}^{4}\right) \overset{FLT}{=} [1]_{11}^{202} [4]_{11}^{4} = [256]_{11} = [3]_{11}$$

$$[0]_{101}^{2024} = [0]_{101}$$

$$[3535]_{1111}^{2024} = [-505.3 + 506 \cdot 0]_{1111} = [707]_{1111}$$

4) Are x and y invertible?

x is a zero divisor $\Rightarrow$ x is not invertible

y $\gcd(y,n) = \gcd(901, 1111) = \gcd(901, 210) = \gcd(210, 61)$
$= \gcd(61, 27) = \gcd(27, 7) = \gcd(7, 4) = 1$

since $\gcd(y,n) = 1$ $\exists a, b.$ $ay + bn = 1$

$ay \equiv 1 \mod n \Rightarrow y$ is invertible

the inverse is a

$$\phi(y) = (-[1]_{11}, -[8]_{101})$$

Are $\phi(x)$ and $\phi(y)$ invertible?

$\phi(x)$ is not invertible as x is not invertible

$\phi(y)$ is invertible as y is invertible

5) Determine the number of elements of $u := \{u \in \mathbb{Z}_n \mid ux = [0]_n\}$

Hint: use ϕ, ϕ^{-1}

$u = \{11.0, 11.1, \dots, 11.100\}$

Let u s.t $ux \equiv 0$

$$([0]_{11}, [0]_{101}) = \phi([0]_{1111}) = \phi([ux]_{1111}) = ([ux]_{11} \underbrace{[ux]_{101}}_{=0 \text{ as } [x]_{101} = [0]_{101}})$$

$\Rightarrow 0 \equiv ux \mod 11$

$\equiv u \cdot 4 \xLeftrightarrow{4 \text{ is invertible}} u \equiv 0 \mod 11 \Rightarrow u = \{u \in \mathbb{Z}_{1111} \mid u \equiv 0 \mod 11\}$

$= \{[k \cdot 11]_{1111} \mid k \in \mathbb{Z}\}$

$$= \{ [k \cdot 11]_{1111} \mid k = 0, 1, \dots 100 \}$$

$$\Rightarrow |U| = 101 \text{ elements}$$