2.1

$\gcd(m,n) = 1 \Rightarrow \exists\ s, t \in \mathbb{Z}$ s.t.

$$s \cdot m + t \cdot n = \gcd(m,n) = 1$$

s, t can be computed efficiently using Extd. Euclid's Algorithm.

Let $y = a \cdot n \cdot t + b \cdot m \cdot s$

$$y \bmod m = a \cdot n \cdot t \bmod m$$

$$= \left[a \cdot (n \cdot t \bmod m)\right] \bmod m$$

$$= a \cdot 1 \bmod m = a$$

Similarly $y \bmod n = b$.

Let $x = y \bmod (m \cdot n)$

$= y - k \cdot m \cdot n$ for some $k \in \mathbb{Z}$.

Note that $x \in \mathbb{Z}_{m \cdot n}$, and

$$x \bmod m = a$$
$$x \bmod n = b.$$

$\gcd(m,n) = 1$ is necessary. Otherwise take $m = 4$, $n = 6$.

$\nexists\ x \in \mathbb{Z}_{24}$ s.t. $x \bmod 4 = 1$, $x \bmod 6 = 2$.

Proving Uniqueness:

Suppose $\exists$ distinct $x, x' \in \mathbb{Z}_{mn}$ s.t.

$x \bmod m = x' \bmod m = a$ (i)

$x \bmod n = x' \bmod n = b.$ (ii)

Suppose $x > x'$.

Consider $z = x - x'$. $0 < z < m \cdot n$.

From (i), it follows that m divides z.

From (ii), it follows that n divides z.

Claim: If $\gcd(m,n) = 1$, and m divides z and n divides z, then $m \cdot n$ divides z.

Proof: We know that m, n and z have unique prime factorization. Suppose there are t primes less than $m \cdot n$.

$$2 = p_1 < p_2 < \cdots < p_t < m \cdot n$$

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t} \qquad \alpha_i \in \mathbb{N} \cup \{0\}$$

$$n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_t^{\beta_t} \qquad \beta_i \in \mathbb{N} \cup \{0\}.$$

$$z = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_t^{\gamma_t} \qquad \gamma_i \in \mathbb{N} \cup \{0\}.$$

Since m divides z, $\alpha_i \leq \gamma_i$ for all $i \in [t]$

Since n divides z, $\beta_i \leq \gamma_i$ for all $i \in [t]$.

$$m \cdot n = p_1^{\alpha_1 + \beta_1} \cdot p_2^{\alpha_2 + \beta_2} \cdot \dots \cdot p_t^{\alpha_t + \beta_t}$$

Therefore, to show that $m \cdot n$ divides z,

it suffices to show that

$\alpha_i + \beta_i \leq \gamma_i$ for all $i \in [t]$.

Since $\gcd(m, n) = 1$, for all $i \in [t]$, both α_i and β_i cant be non zero.

Therefore, for all $i \in [t]$,

$\alpha_i = \beta_i = 0 \Rightarrow \alpha_i + \beta_i \leq \gamma_i$

$\alpha_i > 0,\ \beta_i = 0 \Rightarrow \alpha_i + \beta_i = \alpha_i \leq \gamma_i$

$\alpha_i = 0,\ \beta_i > 0 \Rightarrow \alpha_i + \beta_i = \beta_i \leq \gamma_i$.

$\blacksquare$

Hence $m \cdot n$ divides z. But $z \in [1, mn-1]$.

This is not possible, hence contradiction.

Hints for remaining questions :

2.2 easy calculations

2.3 If inverse is not unique, then

$\exists\ z \in \mathbb{Z}_p \setminus \{0\}$ s.t. $a \times_p z = 0$.

2.4 We can use WOP. n: smallest nat. number s.t. $d = \gcd(F_n, F_{n+1}) > 1$.

Then d also divides F_n and F_{n-1}.

2.5 (a) $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$

$a = b \cdot q + r \qquad r \in [0, b-1]$.

Can prove using induction on q.

Base case: $q = 0$

$2^r - 1 \bmod (2^b - 1) = 2^r - 1$

Induction Step:

$$2^{b \cdot (q+1) + r} - 1 = \left(2^{b \cdot q + r}\right)\left(2^b - 1\right) + 2^{b \cdot q + r} - 1$$

$$\therefore \left(2^{b(q+1)+r} - 1\right) \bmod (2^b - 1) = 2^{bq+r} - 1 \bmod (2^b - 1)$$

$= 2^r - 1$ [using induction hypothesis]

(b) $\gcd(2^a - 1, 2^b - 1)$: $2^{\gcd(a,b)} - 1$

$\gcd(x, y) = \gcd(y, x \bmod y)$

Therefore, for all a, b,

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^b - 1, 2^{a \bmod b} - 1) \quad (*)$$

$(*)$ suggests a natural proof using strong PMI.

$P(b)$: $\forall a \in \mathbb{N}$, $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$

Base case : $b = 1$

$$\gcd(2^a - 1, 1) = 1 = 2^{\gcd(a,1)} - 1$$

Induction step: Suppose $P(k)$ holds for all $k < b$. To prove : $P(b)$.

Take any $a \in \mathbb{N}$. If $a = k \cdot b$, then

$$2^a - 1 = (2^b - 1)(1 + 2^b + \dots + 2^{(k-1)b})$$

$$\therefore \gcd(2^a - 1, 2^b - 1) = 2^b - 1 = 2^{\gcd(a,b)} - 1.$$

If $a = bq + r$, $0 < r < b$, then

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^b - 1, 2^r - 1)$$

From $P(r)$, it follows that

$$\gcd(2^b - 1, 2^r - 1) = 2^{\gcd(b,r)} - 1$$

Finally, note that $\gcd(b,r) = \gcd(a,b)$.

$$\therefore \gcd(2^a - 1, 2^b - 1) = \gcd(2^b - 1, 2^r - 1)$$
$$= 2^{\gcd(b,r)} - 1$$
$$= 2^{\gcd(a,b)} - 1$$

Hence, using induction, we conclude that $P(b)$ holds for all b.

$\blacksquare$

3.1 Any deg. d polynomial $f(x) \in \mathbb{Z}_p[x]$ has at most d distinct roots.

Proof by induction on d.

$Q(d) :=$ $\forall$ $f(x) \in \mathbb{Z}_p[x]$ s.t. deg. of $f \le d$, $\exists$ at most d numbers $\alpha_1 \dots \alpha_d$ in $\mathbb{Z}_p$ s.t. $f(\alpha_i) = 0$ $\forall$ $i \in [d]$.

Base case $d = 1$: easy

Induction step: Suppose $Q(d)$ holds but $Q(d+1)$ does not hold.

Then there exists a polynomial $f(x)$ of deg. $d+1$ that has at least $d+2$ distinct roots.

Let $\alpha_1, \alpha_2, \dots, \alpha_{d+2}$ be $d+2$ distinct roots.

You showed in Quiz 1 that $(x - \alpha_1)$ divides $f(x)$. Let $f(x) = (x - \alpha_1) *_p g(x)$ where $g(x)$ is a deg. d polynomial.

To arrive at a contradiction, we need to show that $\alpha_2, \alpha_3, \dots, \alpha_{d+2}$ are all roots of $g(x)$.

Take any $i > 1$,

$$0 = f(\alpha_i) = (\alpha_i - \alpha_1) \times_p g(\alpha_i)$$

Since $\alpha_i \neq \alpha_1$, we can conclude that

$g(\alpha_i) = 0$.

$\therefore$ $g(x)$ has atleast $d+1$ roots : $\alpha_2, \alpha_3 \ldots \alpha_{d+1}$.

Contradicts $Q(d)$. $\blacksquare$

Q 3.2 Error Detection

Encode$(m_0 \ldots m_{n-1})$: Let $f(x) = m_0 +_p m_1 \times_p x +_p \cdots +_p m_{n-1} \times_p x^{n-1}$

encoding is $\left(f(1), f(2), \ldots, f(n+t) \right) \in \mathbb{Z}_p^{n+t}$.

Detect$(z'_1, z'_2, \ldots, z'_{n+t})$: Using $z'_1, \ldots, z'_n$, find a poly. $g(x)$ of deg. at most $n-1$ s.t. $g(i) = z'_i$ for all $i \in [n]$

Output "no error" if $g(i) = z'_i$ for all $i \in [n+t]$

If the channel introduced no errors, then clearly Detect outputs "no error".

Suppose channel introduced j errors, $j \in [1, t]$.

Can Detect output "no error"?

Suppose $(m_0, m_1, \dots, m_{n-1})$ is the message encoded, $f(x) = \sum_{i=0}^{n-1} m_i x^i$.

$$\begin{array}{ccc}
(m_0 \dots m_{n-1}) & \xrightarrow{\text{Encode}} & (z_1 \dots z_{n+t}) \\
 & & \Big\downarrow \text{channel} \\
 & & (z'_1 \dots z'_{n+t})
\end{array}$$

Let $g(x)$ be the poly. constructed by Detect using $z'_1 \dots z'_n$.

$g(x) \not\equiv f(x)$, since there is at least one index i s.t. $z_i \neq z'_i$.

Since there are at most t errors, $g(x)$ and $f(x)$ agree on at least n points. Both $g(x)$ and $f(x)$ have deg. $n-1$. This is only possible if

$$f(x) \equiv g(x).$$

$\blacksquare$

Efficient Error Correction: This part is not in course syllabus.

We are given $(z'_1, z'_2, \ldots, z'_{n+2t})$.

Key equation: There exist polynomials $\text{error}(x)$ of deg. $\leq t$,

why? $f(x)$ of deg. $\leq n-1$ s.t.

$$z'_i \times_p \text{error}(i) = f(i) \times_p \text{error}(i) \quad \forall i \in [n+2t]$$

1. Find polynomials $\text{error}(x)$ of deg. $\leq t$, $h(x)$ of deg. $\leq n+t-1$ s.t.

$$z'_i \times_p \text{error}(i) = h(i) \quad \forall i \in [n+2t]$$

$n+2t$ unknowns, $n+2t$ equations.

2. Compute $f(x) = h(x)/error(x)$.

$$f(x) = m_0 +_p m_1 \times_p x +_p \cdots +_p m_{n-1} \times_p x^{n-1}$$

Output $(m_0, m_1, \ldots, m_{n-1})$ as the decoded message.