משפט השאריות הסיני

1. יהיו \( N = \prod_{i=1}^{k} n_i \) גורדי. \( \gcd (n_i, n_j) = 1 \) עבור \( i \neq j \) לכל \( n_1, n_2, \ldots, n_k \) מתמקמים \( \{a_i|1 \leq i \leq k\} \) לאימורכת המשוואה \( \begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \)

והם יחיד פתרון ב \( \mathbb{Z}_N \), בהיות \( \gcd (n_i, m_i) = 1 \) לכל \( n_i \).

ה�始: \( \forall g, h \in G : \varphi (g \cdot h) = \varphi (g) \cdot \varphi (h) \) הפונקציה \( \varphi : G \rightarrow H \) הומומורפיזם אם \( G \simeq H \) אריתמטית הומומורפיזם בין \( G \) לבין \( H \).
Theorem 1. Assume that the functions map to the set of $n$ integers, where $n$ is a prime number. Let $f(x)$ be a polynomial over $\mathbb{F}_n$. Then, for any $a \in \mathbb{F}_n$, the function $f'(x) = f(a)$ is a polynomial of degree at most $n-1$.

Proof. Let $f(x) = \sum_{i=0}^{d} a_i x^i$ be a polynomial of degree $d$ over $\mathbb{F}_n$. Then, $f(a) = \sum_{i=0}^{d} a_i a^i$ is a polynomial of degree at most $d$. Since $a \in \mathbb{F}_n$, we have $a^i \in \mathbb{F}_n$ for all $i$, and the degree of $f(a)$ is at most $d$. However, since $\mathbb{F}_n$ is a field, $a$ is invertible, and thus $f(a)$ is a polynomial of degree at most $d$.

Example 2.5: Consider the polynomial $f(x) = x^2 + 2x + 3$ over $\mathbb{F}_5$. Then, $f(2) = 2^2 + 2*2 + 3 = 4 + 4 + 3 = 11 \equiv 1 \pmod{5}$.

Theorem 2.6: Let $f(x)$ and $g(x)$ be polynomials over $\mathbb{F}_n$. Then, the greatest common divisor (gcd) of $f(x)$ and $g(x)$ is a polynomial of degree at most $\min\{d, e\}$, where $d = \deg f$ and $e = \deg g$.

Proof. By the Euclidean algorithm, we can find polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$, where $\deg r < \deg g$. Then, the gcd of $f(x)$ and $g(x)$ is the gcd of $g(x)$ and $r(x)$, and so on. After at most $d$ steps, we get a remainder of degree at most $d$, which is the gcd of $f(x)$ and $g(x)$.

Example 2.7: Consider the polynomials $f(x) = x^3 + 2x^2 + 3x + 1$ and $g(x) = x^2 + 1$ over $\mathbb{F}_5$. Using the Euclidean algorithm, we find that $\gcd(f(x), g(x)) = x + 1$.

GCD over polynomials

Definition 2.1: Let $\mathbb{F}$ be a field and let $d$ be a positive integer. The polynomial $x^d$ is called the polynomial of degree $d$ over $\mathbb{F}$.

Theorem 2.2: Let $a \in \mathbb{F}$ be an irreducible polynomial of degree $d$ over $\mathbb{F}$. Then, $\mathbb{F}[x]/(a(x))$ is a field.

Proof. Let $\mathbb{F}[x]/(a(x))$ be the quotient ring of polynomials over $\mathbb{F}$ modulo $a(x)$. Then, $\mathbb{F}[x]/(a(x))$ is a field if and only if $a(x)$ is irreducible. Since $a(x)$ is irreducible, it is the only polynomial of degree $d$ over $\mathbb{F}$, and thus $\mathbb{F}[x]/(a(x))$ is a field.

Example 2.3: Consider the polynomial $a(x) = x^3 + 2x^2 + 3x + 1$ over $\mathbb{F}_5$. Then, $\mathbb{F}[x]/(a(x))$ is a field.

Theorem 2.4: Let $a \in \mathbb{F}[x]$ be a polynomial of degree $d$. Then, $\mathbb{F}[x]/(a(x))$ is a field if and only if $a(x)$ is irreducible.

Proof. Let $\mathbb{F}[x]/(a(x))$ be the quotient ring of polynomials over $\mathbb{F}$ modulo $a(x)$. Then, $\mathbb{F}[x]/(a(x))$ is a field if and only if $a(x)$ is irreducible. Since $a(x)$ is irreducible, it is the only polynomial of degree $d$ over $\mathbb{F}$, and thus $\mathbb{F}[x]/(a(x))$ is a field.

Example 2.5: Consider the polynomial $a(x) = x^3 + 2x^2 + 3x + 1$ over $\mathbb{F}_5$. Then, $\mathbb{F}[x]/(a(x))$ is a field.
 Também conhecido como polinômio monômio, é um polinômio que tem um termo linear com coeficiente 1.

DEFINIÇÃO: O polinômio monômio $p(x) = x^2 + 2$.

Exemplo: Se $p(x) = x^2 + 2$, então $p(x)$ é um polinômio monômio.

DEFINIÇÃO: Se $p(x)$ e $q(x)$ são polinômios, então $p(x) | q(x)$ se e somente se $p(x)$ divide $q(x)$.

Lembre-se que $p(x)$ e $q(x)$ não podem ser ambos 0.

DEFINIÇÃO: Se $p(x)$ e $q(x)$ são polinômios, então o polinômio monômio $p(x)$ que divide o maior número de termos é chamado de $\text{gcd}(a,b)$, onde $a,b \in \mathbb{F}[x]$.

DEFINIÇÃO: O algoritmo de Euclides é aplicado também em polinômios, com a diferença de que os polinômios são substituídos por números inteiros.

```python
# Assumes deg a(x) >= deg b(x)
# return value is interpolated as ( s(x) , t(x) )
def PolyGCD( a(x) , b(x) ) :
    if deg b(x) == 0 : return (1,0)
    else :
        (s(x) , t(x)) = PolyGCD( b(x) , a(x) % b(x) )
        return (t(x) , s(x) - t(x) * ( a(x) // b(x) ) )
```