Simultaneous Linear, and Non-linear Congruences

CIS002-2 Computational Alegrba and Number Theory

David Goodwin

david.goodwin@perisic.com

University of Bedfordshire

09:00, Friday 18th November 2011

Outline

Outline

Polynomials

Lemma (5.4)

Let $f(x)$ be a polynomial with integer coefficients, and let $n \geq 1$. If $a \equiv b \bmod (n)$ then $f(a) \equiv f(b) \bmod (n)$.

- Suppose $f(x)$ is prime for all integers x, and is not constant.
- If we choose any integer a, then $f(a)$ is a prime p.
- For each $b \equiv a \bmod (p)$, Lemma 5.4 implies that $f(b) \equiv f(a) \bmod (p)$, so $f(b) \equiv 0 \bmod (p)$ and hence $p \mid f(b)$.
- By our hypothesis, $f(b)$ is prime, so $f(b) = p$.
- There are infinitely many integers $b \equiv a \bmod (p)$, so the polynomial $g(x) = f(x) - p$ has infinitely many roots.
- Having degree $d \geq 1$, $g(x)$ can have at most d roots, so such a polynomial $f(x)$ cannot exist.

Theorem (5.5)

There is no non-constant polynomial $f(x)$, with integer coefficients, such that $f(x)$ is prime for all integers x.

Outline

University of Bedfordshire

Theorem (5.6)

If $d = \gcd(a, n)$, then the linear congruence

$$ax \equiv b \bmod (n)$$

has a solution if and only if $d \mid b$. If d does divide b, and if x_0 is any solution, then the general solution is given by

$$x = x_0 + \frac{nt}{d}$$

where $t \in \mathbb{Z}$; in particular, the solutions form exactly d congruence classes $\bmod(n)$, with representatives

$$x = x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

Questions

Example

Consider the following congruences:

1. $10x \equiv 3 \bmod (12)$
2. $10x \equiv 6 \bmod (12)$

Questions

Example

Consider the following congruences:

1. $10x \equiv 3 \bmod (12)$ - Here $a = 10$, $b = 3$, $n = 12$, so $d = gcd(10, 12) = 2$. $2 \nmid 3$, so there are no solutions.
2. $10x \equiv 6 \bmod (12)$ - Here $a = 10$, $b = 6$, $n = 12$, so $d = gcd(10, 12) = 2$. $2 \mid 6$, so there are two classes of solutions. $x_0 = 3$ and $x = x_0 + 6t$, where $t \in \mathbb{Z}$.

University of Bedfordshire

Lemma (5.7)

A *Let $m \mid a, b, n$, and let $a' = a/m$, $b' = b/m$ and $n' = n/m$; then*

$$ax \equiv b \bmod (n) \qquad \textit{if and only if} \qquad a'x \equiv b' \bmod (n')$$

B *Let a and n be coprime, let $m \mid a, b$, and let $a' = a/m$ and $b' = b/m$; then*

$$ax \equiv b \bmod (n) \qquad \textit{if and only if} \qquad a'x \equiv b' \bmod (n)$$

Exercises

For each of the following congruences, decide whether a solution exists, and if it does exist, find the general solution:

1. $3x \equiv 5 \bmod (7)$
2. $12x \equiv 15 \bmod (22)$
3. $19x \equiv 42 \bmod (50)$
4. $18x \equiv 42 \bmod (50)$

Outline

Chinese Remainder Theorem

Theorem (5.8)

Let $n_1, n_2, \ldots, n_k$ be positive integers, with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$, and let $a_1, a_2, \ldots, a_k$ be any integers. Then the solutions of the simultaneous congruences

$$x \equiv a_1 \bmod (n_1), \qquad x \equiv a_2 \bmod (n_2), \qquad \ldots \qquad x \equiv a_k \bmod (n_k)$$

form a single congruence class $\bmod(n)$, where $n = n_1 n_2 \ldots n_k$.

Let $c_i = n/n_i$, then $c_i x \equiv 1 \bmod (n_i)$ has a single congruence class $[d_i]$ of solutions $\bmod(n_i)$. We now claim that $x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + \cdots + a_k c_k d_k$ simultaneously satisfies the given congruences.

Questions

Example

Solve the following simultaneous congruence:
$x \equiv 2 \bmod (3)$, $x \equiv 3 \bmod (5)$, $x \equiv 2 \bmod (7)$

Questions

Example

Solve the following simultaneous congruence:
$x \equiv 2 \bmod (3)$, $x \equiv 3 \bmod (5)$, $x \equiv 2 \bmod (7)$
We have $n_1 = 3$, $n_2 = 5$, $n_3 = 7$, so $n = 105$. $c_1 = 35$, $c_2 = 21$, $c_3 = 15$. $d_1 = -1$, $d_2 = 1$, $d_3 = 2$ gives $x \equiv 23 \bmod (105)$.

Outline

Theorem (5.9)

Let $n = n_1 \dots n_k$ where the integers n_i are mutually coprime, and let $f(x)$ be a polynomial with integer coefficients. Suppose that for each $i = 1, \dots, k$ there are N_i congruence classes $x \in \mathbb{Z}_{n_i}$ such that $f(x) \equiv 0 \bmod (n_i)$. Then there are $N = N_1 \dots N_k$ classes $x \in \mathbb{Z}_n$ such that $f(x) \equiv 0 \bmod (n)$.

Exercises

How many classes of solutions are there for each of the following congruences?

1. $x^2 - 1 \equiv 0 \bmod (168)$
2. $x^2 + 1 \equiv 0 \bmod (70)$
3. $x^2 + x + 1 \equiv 0 \bmod (91)$
4. $x^3 + 1 \equiv 0 \bmod (140)$

Outline

University of Bedfordshire

Chinese Remainder Theorem - An Extension

Theorem (5.10)

Let $n = n_1, \dots, n_k$ be positive integers, and let $a_1, \dots, a_k$ be any integers. Then the simultaneous congruences

$$x \equiv a_1 \bmod (n_1), \dots, x \equiv a_k \bmod (n_k)$$

have a solution x if and only if $\gcd(n_i, n_j)$ divides $a_i - a_j$ whenever $i \neq j$. When this condition is satisfied, the general solution forms a single congruence class $\bmod(n)$, where n is the least common multiple of $n_1, \dots, n_k$.

Exercises

Determine which of the following sets of simultaneous congruences have solutions, and when they do, find the general solution:

1. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv 4 \bmod (21)$.
2. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv -2 \bmod (21)$.
3. $x \equiv 13 \bmod (40)$, $x \equiv 5 \bmod (44)$, $x \equiv 38 \bmod (275)$.
4. $x^2 \equiv 9 \bmod (10)$, $7x \equiv 19 \bmod (24)$, $2x \equiv -1 \bmod (45)$.