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 24th November 2011
09:00, Tuesday 28th November 2011
09:00, Friday 02nd December 2011

Outline

1. Linear Congruences
2. Simultaneous Linear Congruences
3. Simultaneous Non-linear Congruences
4. Chinese Remainder Theorem - An Extension

University of Bedfordshire

Outline

1. Linear Congruences
2. Simultaneous Linear Congruences
3. Simultaneous Non-linear Congruences
4. Chinese Remainder Theorem - An Extension

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*

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

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*

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

Algorithm for solution

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ so $gcd(a'', b''') > 1$ and return to step 4 with b''' instead of b''. Or use $ca''x \equiv cb'' \bmod (n')$ in step 4, where the least absolute reside a''' of ca''' satisfies $|a'''| < |a''|$

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2,$
$5x \equiv 3 \bmod (7),$
$gcd(5, 3) = 1,$
$5x \equiv 3 \bmod (7),$
$5 \neq \pm 1,$
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7),$
$gcd(5, 10) = 5,$
$x \equiv 2 \bmod (7),$
$x_0 = 2,$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

University of Bedfordshire

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. If $a'' = \pm 1$ then $x_0 = \pm b''$
6. Else use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. If $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. If $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

University of Bedfordshire

Example: $10x \equiv 6 \bmod (14)$

Example

$gcd(10, 14) = 2$,
$5x \equiv 3 \bmod (7)$,
$gcd(5, 3) = 1$,
$5x \equiv 3 \bmod (7)$,
$5 \neq \pm 1$,
$10 = 3 + (1 \times 7)$
gives $5x \equiv 10 \bmod (7)$,
$gcd(5, 10) = 5$,
$x \equiv 2 \bmod (7)$,
$x_0 = 2$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 2 + 7t \qquad (t \in \mathbb{Z})$$

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1$,
$4x \equiv 13 \bmod (47)$,
$4 \neq \pm 1$,
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47)$,
$x \equiv 3 \times 52 \bmod (47)$,
$x \equiv 3 \times 5 \bmod (47)$,
$x \equiv 15 \bmod (47)$,
$x_0 = 15$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1,$

$4x \equiv 13 \bmod (47),$

$4 \neq \pm 1,$

$4 \times 12 = 48 \equiv 1 \bmod (47)$

$x \equiv 12 \times 13 \bmod (47)$

$x \equiv 3 \times 4 \times 13 \bmod (47),$

$x \equiv 3 \times 52 \bmod (47),$

$x \equiv 3 \times 5 \bmod (47),$

$x \equiv 15 \bmod (47),$

$x_0 = 15,$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

EXAMPLE: $4x \equiv 13 \bmod (47)$

EXAMPLE

$gcd(4, 47) = 1$,
$4x \equiv 13 \bmod (47)$,
$4 \neq \pm 1$,
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47)$,
$x \equiv 3 \times 52 \bmod (47)$,
$x \equiv 3 \times 5 \bmod (47)$,
$x \equiv 15 \bmod (47)$,
$x_0 = 15$,

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1$,
$4x \equiv 13 \bmod (47)$,
$4 \neq \pm 1$,
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47)$,
$x \equiv 3 \times 52 \bmod (47)$,
$x \equiv 3 \times 5 \bmod (47)$,
$x \equiv 15 \bmod (47)$,
$x_0 = 15$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

EXAMPLE: $4x \equiv 13 \bmod (47)$

EXAMPLE

$gcd(4, 47) = 1$,
$4x \equiv 13 \bmod (47)$,
$4 \neq \pm 1$,
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47)$,
$x \equiv 3 \times 52 \bmod (47)$,
$x \equiv 3 \times 5 \bmod (47)$,
$x \equiv 15 \bmod (47)$,
$x_0 = 15$,

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

University of Bedfordshire

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1,$
$4x \equiv 13 \bmod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47),$
$x \equiv 3 \times 52 \bmod (47),$
$x \equiv 3 \times 5 \bmod (47),$
$x \equiv 15 \bmod (47),$
$x_0 = 15,$

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. If $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1,$
$4x \equiv 13 \bmod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47),$
$x \equiv 3 \times 52 \bmod (47),$
$x \equiv 3 \times 5 \bmod (47),$
$x \equiv 15 \bmod (47),$
$x_0 = 15,$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1,$
$4x \equiv 13 \bmod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47),$
$x \equiv 3 \times 52 \bmod (47),$
$x \equiv 3 \times 5 \bmod (47),$
$x \equiv 15 \bmod (47),$
$x_0 = 15,$

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $4x \equiv 13 \mod (47)$

Example

$gcd(4, 47) = 1,$
$4x \equiv 13 \mod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \mod (47)$
$x \equiv 12 \times 13 \mod (47)$
$x \equiv 3 \times 4 \times 13 \mod (47),$
$x \equiv 3 \times 52 \mod (47),$
$x \equiv 3 \times 5 \mod (47),$
$x \equiv 15 \mod (47),$
$x_0 = 15,$

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \mod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \mod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \mod (n')$ and return to step 4.

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1,$
$4x \equiv 13 \bmod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47),$
$x \equiv 3 \times 52 \bmod (47),$
$x \equiv 3 \times 5 \bmod (47),$
$x \equiv 15 \bmod (47),$
$x_0 = 15,$

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

EXAMPLE: $4x \equiv 13 \bmod (47)$

EXAMPLE

$gcd(4, 47) = 1,$
$4x \equiv 13 \bmod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47),$
$x \equiv 3 \times 52 \bmod (47),$
$x \equiv 3 \times 5 \bmod (47),$
$x \equiv 15 \bmod (47),$
$x_0 = 15,$

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

Example: $4x \equiv 13 \bmod (47)$

Example

$gcd(4, 47) = 1,$
$4x \equiv 13 \bmod (47),$
$4 \neq \pm 1,$
$4 \times 12 = 48 \equiv 1 \bmod (47)$
$x \equiv 12 \times 13 \bmod (47)$
$x \equiv 3 \times 4 \times 13 \bmod (47),$
$x \equiv 3 \times 52 \bmod (47),$
$x \equiv 3 \times 5 \bmod (47),$
$x \equiv 15 \bmod (47),$
$x_0 = 15,$

1. Calculate $d = gcd(a, n)$ and use $f' = \frac{f}{d}$
2. Use $a'x \equiv b' \bmod (n')$
3. Find $m = gcd(a', b')$ and use $f'' = \frac{f}{d}$
4. Use $a''x \equiv b'' \bmod (n')$
5. **If** $a'' = \pm 1$ then $x_0 = \pm b''$
6. **Else** use $b''' = b'' + kn'$ and return to step 4. Or use $ca''x \equiv cb'' \bmod (n')$ and return to step 4.

So the general solution has the form

$$x = 15 + 47t \qquad (t \in \mathbb{Z})$$

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

1. Linear Congruences
2. Simultaneous Linear Congruences
3. Simultaneous Non-linear Congruences
4. Chinese Remainder Theorem - An Extension

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 $n = 105$.
$c_1 = 35$, $c_2 = 21$, $c_3 = 15$.
$d_1 = -1$, $d_2 = 1$, $d_3 = 1$.
$x_0 = (2\times35\times-1))+(3\times21\times1))+(2\times15\times1)) = -70+63+30 = 23$.
So the solutions form the congruence class $[23] \bmod (105)$, that is, the general solution $x = 23 + 105t$ where $t \in \mathbb{Z}$.

Outline

1. Linear Congruences
2. Simultaneous Linear Congruences
3. Simultaneous Non-linear Congruences
4. Chinese Remainder Theorem - An Extension

Simultaneous Non-linear Congruences

It is sometimes possible to solve simultaneous congruences by Chinese Remainder Theorem when the congruences aren't all linear. We must inspect the non-linear congruences to give multiple simultaneous linear congruences.

An Example

Example

Consider the simultaneous congruences

$$x^2 \equiv 1 \bmod (3) \quad x \equiv 2 \bmod (4)$$

By inspection we find $x^2 \equiv 1 \bmod (3)$ can be written as $x \equiv \pm\sqrt{1} \bmod (3)$.

So this first congruence can be $x \equiv 1$ or $-1 \bmod (3)$.

$$x \equiv 1 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

or

$$x \equiv 2 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

.

Giving solutions $x \equiv \pm\sqrt{4} \bmod (12)$ which is $x^2 \equiv 4 \bmod (12)$.

An Example

Example

Consider the simultaneous congruences

$$x^2 \equiv 1 \bmod (3) \quad x \equiv 2 \bmod (4)$$

By inspection we find $x^2 \equiv 1 \bmod (3)$ can be written as $x \equiv \pm\sqrt{1} \bmod (3)$.

So this first congruence can be $x \equiv 1$ or $-1 \bmod (3)$.

$$x \equiv 1 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

or

$$x \equiv 2 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

.

Giving solutions $x \equiv \pm\sqrt{4} \bmod (12)$ which is $x^2 \equiv 4 \bmod (12)$.

An Example

Example

Consider the simultaneous congruences

$$x^2 \equiv 1 \bmod (3) \quad x \equiv 2 \bmod (4)$$

By inspection we find $x^2 \equiv 1 \bmod (3)$ can be written as $x \equiv \pm\sqrt{1} \bmod (3)$.
So this first congruence can be $x \equiv 1$ or $-1 \bmod (3)$.

$$x \equiv 1 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

or

$$x \equiv 2 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

.

Giving solutions $x \equiv \pm\sqrt{4} \bmod (12)$ which is $x^2 \equiv 4 \bmod (12)$.

An Example

Example

Consider the simultaneous congruences

$$x^2 \equiv 1 \bmod (3) \quad x \equiv 2 \bmod (4)$$

By inspection we find $x^2 \equiv 1 \bmod (3)$ can be written as $x \equiv \pm\sqrt{1} \bmod (3)$.
So this first congruence can be $x \equiv 1$ or $-1 \bmod (3)$.

$$x \equiv 1 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

or

$$x \equiv 2 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

.

Giving solutions $x \equiv \pm\sqrt{4} \bmod (12)$ which is $x^2 \equiv 4 \bmod (12)$.

An Example

Example

Consider the simultaneous congruences

$$x^2 \equiv 1 \bmod (3) \quad x \equiv 2 \bmod (4)$$

By inspection we find $x^2 \equiv 1 \bmod (3)$ can be written as $x \equiv \pm\sqrt{1} \bmod (3)$.
So this first congruence can be $x \equiv 1$ or $-1 \bmod (3)$.

$$x \equiv 1 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

or

$$x \equiv 2 \bmod (3) \text{ and } x \equiv 2 \bmod (4)$$

.
Giving solutions $x \equiv \pm\sqrt{4} \bmod (12)$ which is $x^2 \equiv 4 \bmod (12)$.

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 $f(x) \equiv 0 \bmod (n)$.

Start with $f(x) = x^2 - 1$. We aim to find the number of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \bmod (n)$.

If we set $n = p^e$, where p is prime, if $p > 2$ then p^e divides $(x-1)$ or $(x+1)$, giving $x \equiv \pm 1$.

If $p^e = 2$ or 4, there are one of two classes of solutions.

If $p^e = 2^e \geq 8$, there are four classes of solutions given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$.

Let n be a prime power factorisation $n_1 \ldots n_k$, where $n_i = p_i^{e_i}$ for each $e_1 \geq 1$.

If k is the number of distinct primes dividing n, we find

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8) \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise} \end{cases}$$

University of Bedfordshire

Start with $f(x) = x^2 - 1$. We aim to find the number of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \bmod (n)$.

If we set $n = p^e$, where p is prime, if $p > 2$ then p^e divides $(x-1)$ or $(x+1)$, giving $x \equiv \pm 1$.

If $p^e = 2$ or 4, there are one of two classes of solutions.

If $p^e = 2^e \geq 8$, there are four classes of solutions given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$.

Let n be a prime power factorisation $n_1 \ldots n_k$, where $n_i = p_i^{e_i}$ for each $e_1 \geq 1$.

If k is the number of distinct primes dividing n, we find

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8) \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise} \end{cases}$$

University of Bedfordshire

Start with $f(x) = x^2 - 1$. We aim to find the number of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \bmod (n)$.

If we set $n = p^e$, where p is prime, if $p > 2$ then p^e divides $(x-1)$ or $(x+1)$, giving $x \equiv \pm 1$.

If $p^e = 2$ or 4, there are one of two classes of solutions.

If $p^e = 2^e \geq 8$, there are four classes of solutions given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$.

Let n be a prime power factorisation $n_1 \ldots n_k$, where $n_i = p_i^{e_i}$ for each $e_1 \geq 1$.

If k is the number of distinct primes dividing n, we find

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8) \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise} \end{cases}$$

Start with $f(x) = x^2 - 1$. We aim to find the number of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \bmod (n)$.
If we set $n = p^e$, where p is prime, if $p > 2$ then p^e divides $(x-1)$ or $(x+1)$, giving $x \equiv \pm 1$.
If $p^e = 2$ or 4, there are one of two classes of solutions.
If $p^e = 2^e \geq 8$, there are four classes of solutions given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$.
Let n be a prime power factorisation $n_1 \dots n_k$, where $n_i = p_i^{e_i}$ for each $e_1 \geq 1$.
If k is the number of distinct primes dividing n, we find

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8) \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise} \end{cases}$$

Start with $f(x) = x^2 - 1$. We aim to find the number of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \bmod (n)$.
If we set $n = p^e$, where p is prime, if $p > 2$ then p^e divides $(x-1)$ or $(x+1)$, giving $x \equiv \pm 1$.
If $p^e = 2$ or 4, there are one of two classes of solutions.
If $p^e = 2^e \geq 8$, there are four classes of solutions given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$.
Let n be a prime power factorisation $n_1 \dots n_k$, where $n_i = p_i^{e_i}$ for each $e_1 \geq 1$.
If k is the number of distinct primes dividing n, we find

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8) \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise} \end{cases}$$

Start with $f(x) = x^2 - 1$. We aim to find the number of classes $x \in \mathbb{Z}_n$ satisfying $x^2 \equiv 1 \bmod (n)$.
If we set $n = p^e$, where p is prime, if $p > 2$ then p^e divides $(x-1)$ or $(x+1)$, giving $x \equiv \pm 1$.
If $p^e = 2$ or 4, there are one of two classes of solutions.
If $p^e = 2^e \geq 8$, there are four classes of solutions given by $x \equiv \pm 1$ and $x \equiv 2^{e-1} \pm 1$.
Let n be a prime power factorisation $n_1 \dots n_k$, where $n_i = p_i^{e_i}$ for each $e_1 \geq 1$.
If k is the number of distinct primes dividing n, we find

$$N = \begin{cases} 2^{k+1} & \text{if } n \equiv 0 \bmod (8) \\ 2^{k-1} & \text{if } n \equiv 2 \bmod (4) \\ 2^k & \text{otherwise} \end{cases}$$

Example

Example

consider the congruence

$$x^2 - 1 \equiv 0 \bmod (60)$$

Here $n = 60 = 2^2 \times 3 \times 5$ is the prime-power factorisation, then $k = 3$ and there are $2^k = 8$ classes of solutions, namely $x \equiv \pm 1, \pm 11, \pm 19, \pm 29 \bmod (60)$.

Exercises

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

1. $x^2 - 1 \equiv 0 \bmod (168)$.
   Answer: $N = 2^4 = 16$ since $168 = 2^3 \times 3 \times 7$
2. $x^2 + 1 \equiv 0 \bmod (70)$.
   Answer: $N = 1 \times 2 \times 0 = 0$ since $70 = 2 \times 5 \times 7$
3. $x^2 + x + 1 \equiv 0 \bmod (91)$.
   Answer: $N = 2 \times 2 = 4$ since $91 = 7 \times 13$
4. $x^3 + 1 \equiv 0 \bmod (140)$.
   Answer: $N = 1 \times 1 \times 3 = 3$ since $140 = 2^2 \times 5 \times 7$

Exercises

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

1. $x^2 - 1 \equiv 0 \bmod (168)$.
   Answer: $N = 2^4 = 16$ since $168 = 2^3 \times 3 \times 7$
2. $x^2 + 1 \equiv 0 \bmod (70)$.
   Answer: $N = 1 \times 2 \times 0 = 0$ since $70 = 2 \times 5 \times 7$
3. $x^2 + x + 1 \equiv 0 \bmod (91)$.
   Answer: $N = 2 \times 2 = 4$ since $91 = 7 \times 13$
4. $x^3 + 1 \equiv 0 \bmod (140)$.
   Answer: $N = 1 \times 1 \times 3 = 3$ since $140 = 2^2 \times 5 \times 7$

Exercises

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

1. $x^2 - 1 \equiv 0 \bmod (168)$.
   Answer: $N = 2^4 = 16$ since $168 = 2^3 \times 3 \times 7$
2. $x^2 + 1 \equiv 0 \bmod (70)$.
   Answer: $N = 1 \times 2 \times 0 = 0$ since $70 = 2 \times 5 \times 7$
3. $x^2 + x + 1 \equiv 0 \bmod (91)$.
   Answer: $N = 2 \times 2 = 4$ since $91 = 7 \times 13$
4. $x^3 + 1 \equiv 0 \bmod (140)$.
   Answer: $N = 1 \times 1 \times 3 = 3$ since $140 = 2^2 \times 5 \times 7$

Exercises

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

1. $x^2 - 1 \equiv 0 \bmod (168)$.
   Answer: $N = 2^4 = 16$ since $168 = 2^3 \times 3 \times 7$
2. $x^2 + 1 \equiv 0 \bmod (70)$.
   Answer: $N = 1 \times 2 \times 0 = 0$ since $70 = 2 \times 5 \times 7$
3. $x^2 + x + 1 \equiv 0 \bmod (91)$.
   Answer: $N = 2 \times 2 = 4$ since $91 = 7 \times 13$
4. $x^3 + 1 \equiv 0 \bmod (140)$.
   Answer: $N = 1 \times 1 \times 3 = 3$ since $140 = 2^2 \times 5 \times 7$

University of Bedfordshire

Exercises

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

1. $x^2 - 1 \equiv 0 \bmod (168)$.
   Answer: $N = 2^4 = 16$ since $168 = 2^3 \times 3 \times 7$
2. $x^2 + 1 \equiv 0 \bmod (70)$.
   Answer: $N = 1 \times 2 \times 0 = 0$ since $70 = 2 \times 5 \times 7$
3. $x^2 + x + 1 \equiv 0 \bmod (91)$.
   Answer: $N = 2 \times 2 = 4$ since $91 = 7 \times 13$
4. $x^3 + 1 \equiv 0 \bmod (140)$.
   Answer: $N = 1 \times 1 \times 3 = 3$ since $140 = 2^2 \times 5 \times 7$

Outline

1. Linear Congruences
2. Simultaneous Linear Congruences
3. Simultaneous Non-linear Congruences
4. Chinese Remainder Theorem - An Extension

Chinese Remainder Theorem - An Extension

Theorem (5.10)

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

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

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 $n_1, \ldots, n_k$.

Exercises

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

1. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv 4 \bmod (21)$.
   Answer: No Solutions, since $5 \not\equiv 4 \bmod (7)$
2. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv -2 \bmod (21)$.
   Answer: $x \equiv 19 \bmod (42)$
3. $x \equiv 13 \bmod (40)$, $x \equiv 5 \bmod (44)$, $x \equiv 38 \bmod (275)$.
   Answer: $x \equiv 1413 \bmod (2200)$
4. $x^2 \equiv 9 \bmod (10)$, $7x \equiv 19 \bmod (24)$, $2x \equiv -1 \bmod (45)$.
   Answer: The congruences are equivalent to $x \equiv 3$ or $7 \bmod (10)$, $x \equiv 13 \bmod (24)$ and $x \equiv 22 \bmod (45)$, with solution $x \equiv 157 \bmod (360)$

Exercises

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

1. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv 4 \bmod (21)$.
   Answer: No Solutions, since $5 \not\equiv 4 \bmod (7)$
2. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv -2 \bmod (21)$.
   Answer: $x \equiv 19 \bmod (42)$
3. $x \equiv 13 \bmod (40)$, $x \equiv 5 \bmod (44)$, $x \equiv 38 \bmod (275)$.
   Answer: $x \equiv 1413 \bmod (2200)$
4. $x^2 \equiv 9 \bmod (10)$, $7x \equiv 19 \bmod (24)$, $2x \equiv -1 \bmod (45)$.
   Answer: The congruences are equivalent to $x \equiv 3$ or $7 \bmod (10)$, $x \equiv 13 \bmod (24)$ and $x \equiv 22 \bmod (45)$, with solution $x \equiv 157 \bmod (360)$

University of Bedfordshire

Exercises

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

1. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv 4 \bmod (21)$.
   Answer: No Solutions, since $5 \not\equiv 4 \bmod (7)$
2. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv -2 \bmod (21)$.
   Answer: $x \equiv 19 \bmod (42)$
3. $x \equiv 13 \bmod (40)$, $x \equiv 5 \bmod (44)$, $x \equiv 38 \bmod (275)$.
   Answer: $x \equiv 1413 \bmod (2200)$
4. $x^2 \equiv 9 \bmod (10)$, $7x \equiv 19 \bmod (24)$, $2x \equiv -1 \bmod (45)$.
   Answer: The congruences are equivalent to
   $x \equiv 3$ or $7 \bmod (10)$, $x \equiv 13 \bmod (24)$ and $x \equiv 22 \bmod (45)$,
   with solution $x \equiv 157 \bmod (360)$

EXERCISES

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

1. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv 4 \bmod (21)$.
   Answer: No Solutions, since $5 \not\equiv 4 \bmod (7)$
2. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv -2 \bmod (21)$.
   Answer: $x \equiv 19 \bmod (42)$
3. $x \equiv 13 \bmod (40)$, $x \equiv 5 \bmod (44)$, $x \equiv 38 \bmod (275)$.
   Answer: $x \equiv 1413 \bmod (2200)$
4. $x^2 \equiv 9 \bmod (10)$, $7x \equiv 19 \bmod (24)$, $2x \equiv -1 \bmod (45)$.
   Answer: The congruences are equivalent to $x \equiv 3$ or $7 \bmod (10)$, $x \equiv 13 \bmod (24)$ and $x \equiv 22 \bmod (45)$, with solution $x \equiv 157 \bmod (360)$

Exercises

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

1. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv 4 \bmod (21)$.
   Answer: No Solutions, since $5 \not\equiv 4 \bmod (7)$
2. $x \equiv 1 \bmod (6)$, $x \equiv 5 \bmod (14)$, $x \equiv -2 \bmod (21)$.
   Answer: $x \equiv 19 \bmod (42)$
3. $x \equiv 13 \bmod (40)$, $x \equiv 5 \bmod (44)$, $x \equiv 38 \bmod (275)$.
   Answer: $x \equiv 1413 \bmod (2200)$
4. $x^2 \equiv 9 \bmod (10)$, $7x \equiv 19 \bmod (24)$, $2x \equiv -1 \bmod (45)$.
   Answer: The congruences are equivalent to
   $x \equiv 3$ or $7 \bmod (10)$, $x \equiv 13 \bmod (24)$ and $x \equiv 22 \bmod (45)$,
   with solution $x \equiv 157 \bmod (360)$

University of Bedfordshire