# Math135 - November 6'th, 2015

## GCRT and Complex Systems of Congruences

**Generalized Chinese Remainder Theorem (GCRT)**

If $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ and $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, then for any choice of integers $a_1, a_2, \ldots, a_k$, there exists a solution to the simultaneous congruences

$$\begin{gathered} n \equiv a_1 \pmod{m_1} \\ n \equiv a_2 \pmod{m_2} \\ \vdots \\ n \equiv a_k \pmod{m_k} \end{gathered}$$

Also, if $n = n_0$ is one integer solution, then the complete solution is

$$n \equiv \not\Leftarrow_0 \pmod{m_1 m_2 \ldots m_k}$$

**Example:**

Find all $x \in \mathbb{Z}$ such that $x \equiv 5 \pmod 6$
$x \equiv 2 \pmod 7$
$x \equiv 3 \pmod{11}$

Solution:

$x = 3 + 11k, k \in \mathbb{Z}$
Sub into 2'nd equation.

$$\begin{aligned} 3 + 11k &\equiv 2 \pmod 7 \\ 4k &\equiv 6 \pmod 7 \\ 8k &\equiv 12 \pmod 7 \text{ (Since } [4]^{-1} = [2]) \\ k &\equiv 5 \pmod 7 \\ k &= 5 + 7j, j \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} x &= 3 + 11(5 + j) \\ x &= 58 + 77j \\ x &\equiv 58 \pmod{77} \end{aligned}$$

Now $k \equiv 58 \pmod{77}$ is the solution to the last 2 congruences, now we solve:

$x \equiv 5 \pmod 6$
$x \equiv 58 \pmod{77}$

$$\begin{aligned} 58 + 77j &\equiv 5 \pmod 6 \\ 5j &\equiv -53 \pmod 6 \\ 5j &\equiv -5 \pmod 6 \\ j &\equiv -1 \pmod 6 \text{ (Allowed since 5 and 6 are coprime)} \\ j &\equiv 5 \pmod 6 \end{aligned}$$

From that, we get $j = 5 + 6l$

We sub that into our solution for x and we get $x = 58 + 77(5 + 6l)$
$= 443 + 462l$

$$x \equiv 443 \pmod{462}$$

**Challenging Twists:**

i) Solve the following system of congruences:

$3x \equiv 2 \pmod 5$
$2x \equiv 6 \pmod 7$

To solve, first solve for x in each of the congruences.

$$\begin{aligned} 3x &\equiv 2 \pmod 5 \\ 6x &\equiv 4 \pmod 5 \\ x &\equiv 4 \pmod 5 \end{aligned} \qquad \begin{aligned} 2x &\equiv 6 \pmod 7 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Now, we solve this new system of congruences as we've done previously.

$x \equiv 4 \pmod 5$
$x \equiv 3 \pmod 7$

$x = 4 + 5j, j \in \mathbb{Z}$
$4 + 5j \equiv 3 \pmod 7$
$5j \equiv -1 \pmod 7$
$5j \equiv 6 \pmod 7$
$15j \equiv 18 \pmod 7$
$j \equiv 4 \pmod 7$

**First, Convert the first congruence into an equality.**
**Next, sub it into the second congruence.**
**Solve for j.**

**Express as an equation. Sub back into the equation for x and solve.**

$j = 4 + 7l, l \in \mathbb{Z}$
$x = 4 + 5(4 + 7l)$
$x = 24 + 35l$
$x \equiv 24 \pmod{35}$

ii) Solve the following system of congruences:

$x \equiv 4 \pmod 6$
$x \equiv 2 \pmod 8$

$$\begin{aligned} x &= 4 + 6k, k \in \mathbb{Z} \\ 4 + 6k &\equiv 2 \pmod 8 \\ 6k &\equiv -2 \pmod 8 \\ 6k &\equiv 6 \pmod 8 \end{aligned}$$

Now we have a problem. We cannot divide by 6 because 6 and 8 are not coprime.
$[6]^{-1}$ does not exist in $\mathbb{Z}_8$!
If we turn this congruence into an equation, we may be able to simplify.

$6k = 6 + 8l, l \in \mathbb{Z}$

$3k = 3 + 4l$

$3k \equiv 3 \pmod 4$ (Since 3 and 4 are coprime, we can divide both sides by 3)

$k \equiv 1 \pmod 4$

$k = 1 + 4m, m \in \mathbb{Z}$

$x = 4 + 6(1 + 4m)$

$x = 10 + 24m$

$x \equiv 10 \pmod{24}$

iii) Solve $x^2 \equiv 34 \pmod{99}$

We could solve this the same way we've solved polynomial congruences in the past (A table from 0 to our modulus), but figuring out what $1^2, 2^2, \ldots, 97^2, 98^2$ are in modulus 99 will be tedious and difficult. Instead, we can split the modulus into factors and solve a system of congruences instead!.

$x^2 \equiv 34 \pmod 9 \implies x^2 \equiv 7 \pmod 9$

$x^2 \equiv 34 \pmod{11} \implies x^2 \equiv 1 \pmod{11}$

First, solve one of the congruences using the table method.

| | | |
|---|---|---|
| $x \pmod 9$ | 0 1 2 3 **4** **5** 6 7 8 | So, $x \equiv 4, 5 \pmod 9$ |
| $x^2 \pmod 9$ | 0 1 4 0 **7** **7** 0 4 1 | |

Now do the same thing for the other congruence.

| | | |
|---|---|---|
| $x \pmod{11}$ | 0 **1** 2 3 4 5 6 7 8 9 **10** | So, $x \equiv 1, 10 \pmod{11}$ |
| $x^2 \pmod{11}$ | 0 **1** 4 9 5 3 3 5 9 4 **1** | |

I'm confused by what the prof did here, but I'll write exactly what he did.

| | |
|---|---|
| $x \equiv 1 \pmod{11} \implies$ | 01, 12, **23**, 34, 45, 56, **67**, 78, 89 |
| $x \equiv 10 \pmod{11} \implies$ | 10, 21, **32**, 43, 54, 65, **76**, 87, 98 |

$\therefore x \equiv 23, 32, 67, 76 \pmod{99}$

**Splitting Modulus (SM)**

Let $p$ and $q$ be coprime positive integers. Then for any two integers $x$ and $a$,

$$\left.\begin{array}{l} x \equiv a \pmod p \\ x \equiv a \pmod q \end{array}\right. \iff x \equiv a \pmod{pq}$$