CS250: Discrete Math for Computer Science

L7: Chinese Remainder Theorem

Sun-Zi's Puzzle

Solve the following simultaneous congruence equations:

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

Solve: $x \equiv 2 \pmod 3 \quad x \equiv 3 \pmod 5 \quad x \equiv 2 \pmod 7$

3, 5, 7 **pairwise prime**: $\gcd(3,5) = \gcd(5,7) = \gcd(3,7) = 1$

First, solve the following:

$$
\begin{array}{lll}
d_3 \equiv 1 \pmod 3 & d_5 \equiv 0 \pmod 3 & d_7 \equiv 0 \pmod 3 \\
d_3 \equiv 0 \pmod 5 & d_5 \equiv 1 \pmod 5 & d_7 \equiv 0 \pmod 5 \\
d_3 \equiv 0 \pmod 7 & d_5 \equiv 0 \pmod 7 & d_7 \equiv 1 \pmod 7 \\
d_3 \equiv \mathbf{70} \pmod{105} & d_5 \equiv \mathbf{21} \pmod{105} & d_7 \equiv \mathbf{15} \pmod{105} \\
35 \cdot 2 \equiv 1 \pmod 3 & 21 \cdot 1 \equiv 1 \pmod 5 & 15 \cdot 1 \equiv 1 \pmod 7
\end{array}
$$

Solution:

$$
\begin{aligned}
x &\equiv \mathbf{70} \cdot 2 + \mathbf{21} \cdot 3 + \mathbf{15} \cdot 2 \pmod{105} \\
&\equiv 35 + 63 + 30 \pmod{105} \\
&\equiv 128 \pmod{105} \\
&\equiv \mathbf{23} \pmod{105}
\end{aligned}
$$

Chinese Remainder Theorem

Thm: [Sun Zi, Qin Jiushao 1247] Let moduli $m_1, \ldots, m_k$ be pairwise prime, let $P = m_1 \cdot m_2 \cdots m_k$. For all $a_1 \ldots a_k$, there exists a **unique solution (mod P)** to the simultaneous equations

$$x \equiv a_1 \pmod{m_1} \quad x \equiv a_2 \pmod{m_2} \quad \cdots \quad x \equiv a_k \pmod{m_k}\,.$$

proof: Let $q_i = P/m_i \;=\; m_1 \cdot m_2 \cdots m_{i-1} \cdot m_{i+1} \cdots m_k$.

$\gcd(q_i, m_i) = 1$. Using **Euclid's Algorithm**, compute $(q_i)^{-1}_{m_i}$.

Let $d_i = q_i \cdot (q_i)^{-1}_{m_i} \quad d_i \equiv 1 \pmod{m_i} \qquad d_i \equiv 0 \pmod{m_j},\ j \neq i$

$b \;=\; d_1 \cdot a_1 + d_2 \cdot a_2 + \cdots + d_m \cdot a_m \quad b \equiv a_i \pmod{m_i}$.

b is **unique** by **counting:** $P = m_1 \cdot m_2 \cdots m_k$ possible choices for $a_1, \ldots, a_k$, corresponding to exactly all the P elements of Z_P. $\square$

Solve: $x \equiv a_1 \pmod 3 \quad x \equiv a_2 \pmod 5 \quad x \equiv a_3 \pmod 7$

First, solve the following:

$$
\begin{array}{llll}
d_3 \equiv 1 \pmod 3 & d_5 \equiv 0 \pmod 3 & d_7 \equiv 0 \pmod 3 \\
d_3 \equiv 0 \pmod 5 & d_5 \equiv 1 \pmod 5 & d_7 \equiv 0 \pmod 5 \\
d_3 \equiv 0 \pmod 7 & d_5 \equiv 0 \pmod 7 & d_7 \equiv 1 \pmod 7 \\
d_3 \equiv \mathbf{70} \pmod{105} & d_5 \equiv \mathbf{21} \pmod{105} & d_7 \equiv \mathbf{15} \pmod{105} \\
35 \cdot 2 \equiv 1 \pmod 3 & 21 \cdot 1 \equiv 1 \pmod 5 & 15 \cdot 1 \equiv 1 \pmod 7
\end{array}
$$

Example: $a_1 = 1, \quad a_2 = 2, \quad a_3 = 3$

Solution:

$$
\begin{aligned}
\textbf{Solution:} \quad x &\equiv d_3 \cdot a_1 + d_5 \cdot a_2 + d_7 \cdot a_3 \pmod{105} \\
\textbf{Solution:} \quad x &\equiv \mathbf{70} \cdot 1 + \mathbf{21} \cdot 2 + \mathbf{15} \cdot 3 \pmod{105} \\
&\equiv 70 + 42 + 45 \pmod{105} \\
&\equiv 157 \pmod{105} \\
&\equiv \mathbf{52} \pmod{105}
\end{aligned}
$$

$\forall a, m > 1$ (a has mult. inverse mod m iff $\gcd(a, m) = 1$)

$\times$ mod 6	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\forall a, m > 1$ (a has mult. inverse mod m iff $\gcd(a, m) = 1$)

Def: $\mathbf{Z}_m^\star = \{a \mid 0 < a < m \ \wedge \ \gcd(a, m) = 1\}$

This is the **multiplicative group** mod m.

$\mathbf{Z}_m^\star$ is the set of positive integers less than m that are relatively prime to m, with multiplication mod m.

$\mathbf{Z}_6^\star = \{1, 5\}$

$\mathbf{Z}_6^\star$	1	5
1	1	5
5	5	1

$\mathbf{Z}_5^\star = \{1, 2, 3, 4\}$

$\mathbf{Z}_5^\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\mathbf{Z}_m^\star = \{a \mid 0 < a < m \wedge \gcd(a, m) = 1\}$

$\mathbf{Z}_m^\star$ is the **multiplicative group mod m**.

A **group** is a set G, with a binary operation $\star$, s.t.

- G is **associative:** $\forall abc \in G\ (\ a \star (b \star c) \ = \ (a \star b) \star c\ )$
- G has an **identity element,** 1, $\forall a \in G\ (a \star 1 \ = \ 1 \star a \ = \ a)$
- G has **inverses:** $\forall a \in G\ \exists a^{-1} \in G (a \star a^{-1} \ = \ a^{-1} \star a \ = \ 1)$

$\mathbf{Z}_6^\star \ = \ \{1, 5\}$

$\mathbf{Z}_6^\star$	1	5
1	1	5
5	5	1

$\mathbf{Z}_3^\star \ = \ \{1, 2\}$

$\mathbf{Z}_3^\star$	1	2
1	1	2
2	2	1

$\mathbf{Z}_6^\star$ and $\mathbf{Z}_3^\star$ are **isomorphic** ($\mathbf{Z}_6^\star \cong \mathbf{Z}_3^\star$). This means they are **identical:** only the names of their elements are changed.

Cyclic Groups

Def: An n-element group, G, is **cyclic** iff it has an element $g \in G$ called a **generator** s.t. $G = \langle g \rangle = \{g, g^2, g^3, \ldots, g^n = 1\}$.

Fact: For all primes, p, $\mathbf{Z}_p^\star$ is cyclic.

$\mathbf{Z}_3^\star$	1	2
1	1	2
2	2	1

iClicker: What are the generators of $\mathbf{Z}_3^\star$?

A: $\{1\}$, **B:** $\{2\}$, **C:** $\{1, 2\}$

$\mathbf{Z}_5^\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

iClicker: What are the generators of $\mathbf{Z}_5^\star$?

A: $\{1, 4\}$, **B:** $\{1, 2\}$, **C:** $\{2, 3\}$, **D:** $\{3, 4\}$

Discrete Logs

Def: If g is a generator of the group $Z_m^\star$, and $a \in Z_m^\star$, then $\log_g a \pmod{m} = e$ iff $g^e \equiv a \pmod{m}$.

$\mathbf{Z}_3^\star$	1	2
1	1	2
2	2	1

$$\log_2(1) \pmod 3 = 2$$
$$\log_2(2) \pmod 3 = 1$$

$\mathbf{Z}_5^\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

iClicker: What is $\log_3 2 \pmod 5$?

A: 1, **B:** 2, **C:** 3, **D:** 4

Fermat's Little Theorem

Thm: [Fermat, 1640] Let p be prime, and $a \in \mathbf{Z}_p^\star$. Then:

$$a^{p-1} \equiv 1 \pmod{p} .$$

proof: Let $f_a : \mathbf{Z}_p^\star \to \mathbf{Z}_p^\star$ be given by $f_a(x) = (a \cdot x) \,\%\, p$

Claim: f_a is 1:1 and onto.

proof: Suppose that for some $b, c \in \mathbf{Z}_p^\star$,

$$\begin{aligned} f_a(b) &= f_a(c) \\ a \cdot b &\equiv a \cdot c && \pmod{p} \\ a_p^{-1} \cdot a \cdot b &\equiv a_p^{-1} \cdot a \cdot c && \pmod{p} \\ b &\equiv c && \pmod{p} \\ b &= c \end{aligned}$$

Thus, f_a is 1:1.

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod{p}$

Lemma: For a **finite** set S, if $f : S \overset{1:1}{\to} S$, then $f : S \underset{\text{onto}}{\overset{1:1}{\to}} S$.

Let $S = \{a_1, a_2, \ldots, a_n\}$

Since f is 1:1, $f(a_1), f(a_2), \ldots, f(a_n)$ are **distinct** elements of S.

Thus, $S = \{f(a_1), f(a_2), \ldots, f(a_n)\}$. $\square$

Thus, $f_a(x) = (a \cdot x)$ is 1:1 and onto. $\square$

We say that $f_a : \mathbf{Z}_p^\star \underset{\text{onto}}{\overset{1:1}{\to}} \mathbf{Z}_p^\star$ is a **permutation** of $\mathbf{Z}_p^\star$.

Thm: For p prime, $a \in \mathbf{Z}_p^\star$, $a^{p-1} \equiv 1 \pmod{p}$

proof: $f_a : \mathbf{Z}_p^\star \xrightarrow[\text{onto}]{1:1} \mathbf{Z}_p^\star; \quad f_a(x) = (a \cdot x)$

$$
\begin{aligned}
Z_p^\star = \{1, 2, \ldots, p-1\} &= \{f_a(1), f_a(2), \ldots, f_a(p-1)\} \\
\{1, 2, \ldots, p-1\} &= \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} \\
\prod_{i \in \mathbf{Z}_p^\star} i &\equiv \prod_{i \in \mathbf{Z}_p^\star} a \cdot i \pmod{p} \\
\prod_{i \in \mathbf{Z}_p^\star} i &\equiv a^{p-1} \prod_{i \in \mathbf{Z}_p^\star} i \pmod{p} \\
1 &\equiv a^{p-1} \pmod{p} \qquad \square
\end{aligned}
$$