Lecture 9 Chinese Remainder thm §2.8

Last time Babystep - Giant step to solve DLP.

$g^x = h$ where $\text{ord}(g) = N$.

Complexity $O(\sqrt{N}\log(N\sqrt{N}))$ sorting to find collision. Better approach to finding collision has linear time $\rightsquigarrow O(2^{k/2})$.

Pohig-Hellman: Improve complexity of N if N has small prime divisors.

Factor $N = p_1^{e_1} \cdots p_r^{e_r}$.

Complexity $O\left(\sum_i e_i \sqrt{p_i}\right)$.

The Chinese Remainder Thm

Thm (Chinese Remainder Thm) If $\gcd(m_1, m_2) = 1$ then the map $\mathbb{Z}/m_1m_2\mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ given by $x \longmapsto (x, x)$ is an isomorphism.

What does this mean?

$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ is the ring of pairs (x_1, x_2) where addition is $(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$ & multiplication is $(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2)$

An isomorphism is a bijection preserving $+$ & $\times$.

Another way to formulate the theorem:

Thm Suppose $\gcd(m_1, m_2) = 1$.

① For any $a_1, a_2 \in \mathbb{Z}$ there is a unique $x \in \mathbb{Z}/m_1 m_2 \mathbb{Z}$ such that
$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

② If x is the solution for (a_1, a_2) & y is the solution for (b_1, b_2)

then $x+y$ is the soln for (a_1+b_1, a_2+b_2)

& xy is the soln for $(a_1 b_1, a_2 b_2)$.

Rmk There is a general version of CRT for any ring, not just $\mathbb{Z}$.

By induction, similar statements hold when $m_1, \dots, m_n$ are pairwise relatively prime.

$$\mathbb{Z}/m_1 \cdots m_n \mathbb{Z} \cong \mathbb{Z}/m_1 \times \cdots \times \mathbb{Z}/m_n.$$

Ex Find $x \in \mathbb{Z}/105\mathbb{Z}$ s.t.

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ & $x \equiv 2 \pmod 7$.

Soln $x \equiv 2 \pmod 3$.

$\Rightarrow x \equiv 2 + 3y \pmod{15}$

$\Rightarrow 3 \equiv 2 + 3y \pmod 5$

$\Rightarrow y \equiv 2 \pmod 5$.

$\Rightarrow x \equiv 8 \pmod{15}$.

$\Rightarrow x \equiv 8 + 15z \pmod{105}$

$2 \equiv x \equiv 1 + z \pmod 7$

$\Rightarrow z = 1$

$\Rightarrow x = 23$.