Cryptography 2/12

Reagan Shirk

February 12, 2020

Modular Class Ring and Chinese Remainder Theorem

- Say you have $\frac{\mathbb{Z}}{15\mathbb{Z}}$, you can do:

mod15	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
mod3	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
mod5	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4

- And we can see that:

$$x \equiv a_1 \bmod 3$$
$$x \equiv a_2 \bmod 5$$

ϕ Function

- Today we want to prove that if $\gcd(m_1, m_2) = 1$, then $\phi(m_1, m_2) = \phi(m_1)\phi(m_2)$
  - We know that $\phi(p) = p - 1$ and that $\phi(p^m) = p^m - p^{m-1}$
  - As long as you know the factorization of p, you can calculate the ϕ function
- How do you prove this?
  - If a is invertible mod$m_1 m_2$:

$$\begin{aligned} &\Rightarrow \exists\ b \text{ such that } ab \equiv 1(m_1 m_2) \\ &\Rightarrow ab \equiv 1(m_1)\ \&\ ab \equiv 1(\text{mod} m_2) \\ &\Rightarrow a \text{ is invertible mod } m_1\ \&\ a \text{ is invertible mod } m_2 \\ &\text{If } a \text{ is invertible mod } m_1\ \&\text{ it is invertible mod } m_2, \text{ then} \\ &\Rightarrow \exists\ b_2 \text{ such that } ab_1 \equiv 1(m_1) \\ &\exists b_2 \text{ such that } ab_2 \equiv 1(m_2) \\ &\Rightarrow \text{ By CRT }, b \equiv b_1 \bmod m_1\ \&\ b \equiv b_2 \bmod m_2 \\ &\Rightarrow ab \equiv 1 \bmod m_1 m_2 \end{aligned}$$

- I have no idea what any of that means
- If $p \neq q$ and p, q are both primes, then $\phi(p, q) = (p-1)(q-1)$
- What is 51^{38} mod 77?
  - Split it into 11 and 7
  - First calculate 51^{38} mod 7
    - 51 lives in mod7, so it gives you 2. But 38 lives in mod6, so you put the result of 38 mod 6 in the exponent and the final result of 51^{38} mod 7 is 2^2 mod $7 = 4$
- Remember that by FLT, $x^6 = 1 \bmod 7$ if $7 \nmid x$