Cryptography 2/3

Reagan Shirk

February 3, 2020

Class Ring - Multiplication

- $(\frac{\mathbb{Z}}{m\mathbb{Z}}, +, \times)$
- For the multiplication, you want to focus on the units
- $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}^*\right)$: Units
  - $\{a| \ \gcd(a, m) = 1\}$
  - $|\left(\frac{\mathbb{Z}}{m\mathbb{Z}}^*\right)| = \varnothing(m)$
- There are things you can say about the order
  - If $g^x = 1$ then $\text{ord}(g)|x$
  - x can be order x, or a multiple of ...? itself probably?
  - Proving is easy:
    * Assume that $\text{ord}(g) \nmid x$, then $x = q \ \text{ord}(g) + r$ where r is the remainder between 0 and $\text{ord}(g)$
    * This gives a contradiction because $g^r = g^{x - g\text{ord}(g)} = 1$
    * This is a contradiction because $\text{ord}(g)$ is supposed to be the smallest possible number but we found a number smaller than $\text{ord}(g)$
    * Important equation: $\text{ord}(g^n) = \frac{\text{ord}(g)}{\gcd(n, \text{ord}(g))}$
    * Proof:

$$\begin{aligned}
\frac{\text{ord}(g)}{\gcd(n, \text{ord}(g))} &\mid \text{ord}(g^n) \\
&\iff \text{ord}(g) \mid \text{ord}(g^n)\gcd(n, \text{ord}(g)) \\
\text{We know } (g^n)^{\text{ord}(g^n)} &= 1 \\
&\Rightarrow \text{ord}(g) \mid n\text{ord}(g^n) \\
\text{He lost me, sorry} \\
\text{I'll look up the proof later}
\end{aligned}$$

Fermat's Little Theorem

- If p is a prime number and $\gcd(a, p) = 1$, then $a^{p-1} = 1 \pmod p$
- $p - 1 = |\frac{\mathbb{Z}}{p\mathbb{Z}}^*|$
- What is the application?
  - Very very important application is proving that 15 (or just any small number) is a composite number
    * Method 1: $15 = 3 \times 5 \rightarrow$ okay for this example but would be bad for a super big number
    * Method 2: Use Fermat's Little Theorem
      · If $2^{14} \neq 1 \pmod{15}$, then 15 is composite

Repeated Squaring Algorithm

- Take 2^{14}
  - 14 is even, so we can say $2^{14} = 2^{2\times 7}\ 4^7$

– 7 is odd, so we can say $2^{14} = 2^{2 \times 7}$ $4^7 = 4^{2\times3+1} = 4 \times 4^{2\times3}$
– We can continue the process: $2^{14} = 2^{2 \times 7}$ $4^7 = 4^{2\times3+1} = 4 \times 4^{2\times3} = 4 \times 16^3 \equiv 4 \times 1 \pmod{15} = 4$