Cryptography 1/29

Reagan Shirk

January 29, 2020

Modular/Residue Class Ring

- $\left(\frac{\mathbb{Z}}{m\mathbb{Z}}, +, \times\right)$
- We will prove constructivitiy ($\gcd(a, m) = 1$ iff a is invertible) on Monday I think
- $\gcd(a, m) = 1 \iff ax + my = 1 \iff x = a^{-1} (\text{mod } m)$
- Example of... something
  - $71x \equiv 2 (\text{mod } 128)$
  - We are looking for $71x = 2$ in $\left(\frac{\mathbb{Z}}{128\mathbb{Z}}\right)$
  - Algorithm 1: Exhaustive search
    - Because you have a finite ring, you know that your search is finite
    - Still a bad idea though because it's exponential
  - Algorithm 2: Find the inverse of 71 mod 128
    - Run extended eucilidean algorithm on 71, 128
    - $\gcd(71, 128) = 1$ which we know because no odd number will share a factor with a power of 2

$$\begin{aligned}
128 &= 71 + 1 \times 57 \\
71 &= 1 \times 57 + 14 \\
57 &= 4 \times 14 + 1 \\
1 &= 57 - 4 \times 14 \\
&= 57 - 4 \times (71 - 57) \\
&= 5 \times 57 - 4 \times 71 \\
&= 5 \times (128 - 71) - 4 \times 71 \\
&= 5 \times 128 - 9 \times 71 \\
(-9) \times 71x &= -18 (\text{mod} 128) \\
x &= -18 (\text{mod} 128) \\
&= 110
\end{aligned}$$

- Unit Group $= \mathbb{R}^* = \mathbb{R} - \{0\}$
  - $\left(\frac{\mathbb{Z}}{12\mathbb{Z}}\right)^* = \{1, 5, 7, 11\}$
  - $\left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right)^* = \left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right) - \{0\}$
- $\mathbb{Z}^* = \{1, -1\}$
- $\mathbb{Q}^* = \mathbb{Q} - \{0\}$

Zero Divisor

- a is a zero divisor if $a \neq 0$ but $\exists b \neq 0$ such that $ab = 0$
- Example
  - In $\frac{\mathbb{Z}}{12\mathbb{Z}}$, $3 \times 4 = 0$ and $8 \times 3 = 0$ so these are zero divisors

Order

- Say we have group $2 \in \left(\frac{\mathbb{Z}}{13\mathbb{Z}}\right)^*$
  - We start with $2^1 = 2$, then $2^2 = 4$, $2^3 = 8$, $2^4 = 3$, $2^5 = 6$, $2^6 = -1 = 12$, $2^7 = -2 = 11$, $2^8 = -4 = 9$, $2^9 = 5$, $2^{10} = 10$, $2^{11} = 7$, $2^{12} = 1$
    - This shows that the order of this group (and of 2) is 12
    - If someone could explain to me how we came up with these powers that'd be gr8
- G is a finite group
  - $|G|$ is called the *order of a group*
  - Let $a \in G$, then the order of a, denoted by $ord(a)$, is defined by the least positive integer x such that $a^x = 1$

Groups

- There are three conditions to be in a group
- The only one I heard was that it has to be invertible, I'm sure I have it in my notes somewhere else
- Abelian group: $ab = ba$
- Cyclic Group: $\exists$ a generator

Three Important Things to Remember...

- Units
- Zero Divisor
- Order (esp the order)