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
- $\gcd(a, m) = 1 \iff ax + my = 1 \iff x = a^{-1} \pmod{m}$
- Example of…something
  - $71x \equiv 2 \pmod{128}$
  - 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

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

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