Cryptography 1/22

Reagan Shirk

January 22, 2020

Greatest Common Divisor (GCD)

- Greatest = magnitude
- Example: What is the GCD of 8 and 12?
  - 8: {1, 2, 4, 8, -1, -2, -4, -8}
  - 12: {1, 2, 3, 4, 6, 12, -1, -2, -3, -4, -6, -12}
  - Common Divisors: {1, 2, 4, -1, -2, -4}
  - Greatest Common Divisor: 4
- How do we find the GCD for large numbers?
  - What we did above is probs not the best option
- Theorem: $\forall a, b \in \mathbb{Z}$, a common divisor of a and b must divide gcd(a, b)
  - Notation:
    * $n\mathbb{Z} = \{0, n, -n, 2n, -2n, 3n, -3n, \cdots\}$
      · The set of integral multiples of n (all integers that are multiples of n)
    * $n\mathbb{Z} + m\mathbb{Z} = \{a + b \mid a \in n\mathbb{Z}, b \in m\mathbb{Z}\}$
  - Example: $2\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$
    * Why is the above true? Because 4 is a multiple of 2, so we can say that

$$2\mathbb{Z} + 4\mathbb{Z} \subseteq 2\mathbb{Z}$$

$$2\mathbb{Z} \subseteq 2\mathbb{Z} + 4\mathbb{Z}$$

  - Example: $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ because $3 - 2 = 1$
- Lemma: $\exists\ g$ such that $n\mathbb{Z} + m\mathbb{Z} = g\mathbb{Z}$
  - Prove by contradiction: let g be the least positive integer in $n\mathbb{Z} + m\mathbb{Z}$
    * $g = na + mb$
    * Cryptography: finding g isn't really that interesting to us, we'd rather find a and b
  - We want to show two things:
    * $g|n,\ g|m$, otherwise if $g \nmid n$, then $n = qg + r$ for $0 < r < g$ which implies that $r = n - qg$ and that means that $r \in n\mathbb{Z} + m\mathbb{Z}$ which is a contradiction because g is supposed to be the smallest value in the set but we just found a number smaller than g
    * $g\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$
- Lemma: If $x|n,\ x|m \Rightarrow x|g$

$$\begin{aligned} &\gcd(n,m)|n \\ &\gcd(n,m)|m \\ \Rightarrow\ &\gcd(n,m)|g \\ &\quad \text{and } g \text{ is a common divisor greater than 0} \\ &\quad\ \Rightarrow g|\gcd(n,m) \end{aligned}$$

- So this is cool and all but we still haven't figured out how to find the GCD
  - Remainder sequence: 97, 30, 7, 2, 1, 0
    * $n = 97,\ m = 30$
    * $97 \bmod 30 = 7$
    * $97 \div 30 = 3$
    * $30 \bmod 7 = 2$

* $30 \div 7 = 4$
* $7 \bmod 2 = 1$
* $7 \div 2 = 3$
* $2 \bmod 1 = 0$
* $2 \div 1 = 2$
* You stop because you can't divide 1 by 0
* The number right before 0 is the GCD: 1
* Don't really know what this is for..? But I guess I'll write it down

$$\begin{aligned}
97 &= 3 \times 30 + 7 \\
30 &= 7 \times 7 + 2 \\
7 &= 3 \times 2 + 1 \\
2 &= 2 \times 1 + 0 \\
1 &= 7 - 3 \times 2 \\
&= 7 - 3 \times (30 - 4 \times 7) \\
&= (-3) \times 30 + 13 \times 7 \\
&= (-3) \times 30 + 13 \times (97 - 3 + 30) \\
&= (-42) \times 30 + 13 \times 97
\end{aligned}$$

* If $n = qm + r$, then $\gcd(n, m) = \gcd(m, r)$
  * Just have to prove that and then you're done