MATH 314 Fall 2024 - Class Notes

10/22/2024

Scribe: Kyle Merkins

Summary: Euler's Theorem and introduction to RSA encryption.

Euler's Theorem:
Similar to Fermat's Theorem, but improved for composites.

If $GCD(a, n) = 1$, meaning a and n are coprime, then $a^{\varphi(n)} \equiv 1 \pmod{n}$

- a and n must be coprime
- n cannot be divisible by the square of a prime (square free).

Factor the resulting $a^{\varphi(n)} \equiv 1 \pmod{n}$ from the original a^e to simplify large exponents.

Euler's Theorem Example:

Compute $11^{85} \pmod{21}$

1. Check if a and n are coprime.
   GCD(11,21) = 1, 11 is prime and 11 does not factor into 21.
2. Compute $\varphi(21)$
   $\varphi(21) = \varphi(3) \cdot \varphi(7) = (7^1 - 7^0) \cdot (3^1 - 3^0) = 6 \cdot 2 = 12$
   Using Euler's Theorem, we know that $11^{12} \equiv 1 \pmod{21}$
3. Factor 11^{12} out of the exponent of $11^{85} \pmod{21}$.
   $11^{85} = 11^{84} \cdot 11^1$
   $= 11^{(12)7} \cdot 11^1$
   Since we know that $11^{12} = 1$, through Euler's Theorem, we can write this as:
   $1^7 \cdot 11^1 \pmod{21}$, which is the final answer of $11 \pmod{21}$

RSA Encryption:
A **public key** Cryptography

Involves two keys

- A **public** key that everyone knows and has access to.
- A **private** decryption key that only Alice knows.

Anyone can send Alice a message, but not everyone has the information required to decrypt.

<u>RSA Setup:</u>

- Alice chooses two large prime numbers p and q, each with 120 or more digits and hard to guess.
- Alice computes $n = p \cdot q$, and n is made publicly known.
- Alice then picks an encryption exponent e where $gcd(e, \varphi(n)) = 1$.
- Alic's public key is (e,n). Anyone can send Alice a message with the encryption function $E(x) \equiv x^e \pmod{n}$
- To decrypt messages, Alice needs decryption exponent d.

  Using Euler's Theorem, $d = e^{-1} \pmod{\varphi(n)}$.

  Since Alice knows p and q, she can compute $\varphi(n) = (p-1)(q-1)$ and easily compute d.
- Alice's decryption function is $D(y) = y^d \pmod{(n)}$.

From Eve's perspective, e and n are known, but without p and q Eve can not easily compute d for the decryption method. Factoring a huge number like n to find p and q is difficult with no known fast method.

<u>RSA Example:</u>

RSA using variables $p = 11$, $q = 7$, $n = 11 \cdot 7 = 77$, and $e = 17$.

1. The encryption method $E(x) \equiv x^e \pmod{n}$ is $E(x) \equiv x^{17} \pmod{77}$
2. compute $d = 17^{-1} \pmod{\varphi(77)}$.

   $\varphi(77) = (11-1)(7-1) = 60$

   Use Euclid's extended algorithm to compute: $d = 17^{-1} \pmod{60}$.

   $60 = 3(17) + 9$ $\quad$ $1 = 9 - 1(18)$

   $17 = 1(9) + 8$ $\quad$ $8 = 17 - 1(9)$

   $9 = 1(8) + 1$ $\quad$ $9 = 60 - 3(17)$

   Substitute, distribute, simplify

$1 = 9 - 1(17 - 9)$

$1 = 2(9) - 17$

$1 = 2(60 - 3(17)) - 17$

$1 = -7(17) \pmod{60}$

$1 = 53 \pmod{60}$

Therefore, $d = 53$ and the decryption method is $D(y) = y^{53} \pmod{77}$

3. Suppose Bob wants to send Alice $m = 3$, he will need to compute $E(3) = 3^{17} \pmod{77}$

   $3^{17} \pmod{77} = 3^{16} \cdot 3^1 \pmod{77}$

   Use repeated squaring.

   $3^2 = 9 \pmod{77}$ $\quad$ $3^4 = 9^2 = 81 \pmod{77} = 4 \pmod{77}$

   $3^8 = 4^2 = 16 \pmod{77}$ $\quad$ $3^16 = 16^2 = 256 \pmod{77} = 25 \pmod{77}$

   Therefore, $3^{16} \cdot 3^1 \pmod{77} = 25 \cdot 3 = 75 \pmod{77}$

4. Alice can decrypt Bob's message using the decryption function $d(y) \equiv 75^{53} \pmod{77}$

   Using repeated squaring, just like in Bob's encryption step, we find that $d(y) \equiv 75^{53} \pmod{77} = 3$, which is Bob's message.