Ma/CS 6a
Class 4: Primality Testing

By Adam Sheffer

- Send anonymous suggestions and complaints from here.
- Email: adamcandobetter@gmail.com
- Password: anonymous2

There aren’t enough crocodiles in the presentations

Only today! 75% off for Morphine and Xanax.

Why won’t you tell me how to solve the homework?!

Could you open every class by playing Flight of the Valkyries?
Remainder: Euler’s Totient Function

- **Euler’s totient $\varphi(n)$** is defined as follows:
  
  Given $n \in \mathbb{N}$, then
  
  $\varphi(n) = |\{x \mid 1 \leq x < n \text{ and } \gcd(x, n) = 1\}|$.

- In more words: $\varphi(n)$ is the number of natural numbers $1 \leq x \leq n$ such that $x$ and $n$ are relatively prime.

  $\varphi(12) = |\{1, 5, 7, 11\}| = 4$.

Reminder #2: The RSA Algorithm

- **Bob** wants to generate keys:
  
  ◦ Arbitrarily chooses primes $p$ and $q$. ?
  
  $n = pq \checkmark$ find $\varphi(n)$. ?
  
  ◦ Chooses $e$ such that $\gcd(\varphi(n), e) = 1$. ?
  
  ◦ Find $d$ such that $de \equiv 1 \mod \varphi(n)$. ?

- **Alice** wants to pass bob $m$.

  ◦ Receives $n, e$ from Bob.
  
  ◦ Returns $X \equiv m^e \mod n. \checkmark$

- **Bob** receives $X$.

  Calculates $X^d \mod n. \checkmark$
Finding $\varphi(n)$

- **Problem.** Given $n = pq$, where $p, q$ are large primes, find $\varphi(n)$.
  - We need the number of elements in $\{1, 2, ..., n\}$ that are not multiples of $p$ or $q$.
  - There are $\frac{n}{p} = q$ numbers are divisible by $p$.
  - There are $\frac{n}{q} = p$ numbers are divisible by $q$.
  - Only $n = pq$ is divided by both.
  - Thus: $\varphi(n) = n - p - q + 1$.

The RSA Algorithm

- **Bob** wants to generate keys:
  - Arbitrarily chooses primes $p$ and $q$. ?
  - $n = pq \checkmark$ find $\varphi(n)$. \checkmark
  - Chooses $e$ such that $\text{GCD}(\varphi(n), e) = 1$. ?
  - Find $d$ such that $de \equiv 1 \mod \varphi(n)$. ?

- **Alice** wants to pass bob $m$.
  - Receives $n, e$ from Bob.
  - Returns $X \equiv m^e \mod n$. \checkmark

- **Bob** receives $X$.
  - Calculates $X^d \mod n$. \checkmark
Choose $e$ s.t. $\text{GCD}(\varphi(n), e) = 1$

- **Problem.** Given $n = pq$, where $p, q$ are large primes, find $e \in \mathbb{N}$ such that $\text{GCD}(\varphi(n), e) = 1$.
  - We can choose arbitrary numbers until we find one that is relatively prime to $\varphi(n)$.
  - For the “worst” values of $\varphi(n)$, a random number is good with probability $1/\log \log n$.

The RSA Algorithm

- **Bob** wants to generate keys:
  - Arbitrarily chooses primes $p$ and $q$. ?
  - $n = pq \checkmark$ find $\varphi(n)$. \checkmark
  - Chooses $e$ such that $\text{GCD}(\varphi(n), e) = 1$. \checkmark
  - Find $d$ such that $de \equiv 1 \mod \varphi(n)$. ?

- **Alice** wants to pass bob $m$.
  - Receives $n, e$ from Bob.
  - Returns $X \equiv m^e \mod n$. \checkmark

- **Bob** receives $X$.
  - Calculates $X^d \mod n$. \checkmark
Find $d$ such that $de \equiv 1 \mod \varphi(n)$

- **Recall.** Since $\gcd(e, \varphi(n)) = 1$ then there exist $s, t \in \mathbb{Z}$ such that $se + t\varphi(n) = 1$.
- That is, $se \equiv 1 \mod \varphi(n)$.
- We can find $s, t$ by the extended *Euclidean algorithm* from lecture 2.

Quantum Computing

- A *bit* of a computer contains a value of either 0 or 1.
- A quantum computer contains *qubits*, which can be in superpositions of states.
- *Theoretically*, a quantum computer can easily factor numbers and decipher almost any known encryption.
Should We Stop Ordering Things Online?

The RSA Algorithm

- **Bob** wants to generate keys:
  - Arbitrarily chooses primes $p$ and $q$. $\checkmark$
  - $n = pq \checkmark$ find $\varphi(n)$. $\checkmark$
  - Chooses $e$ such that $\text{GCD} (\varphi(n), e) = 1$. $\checkmark$
  - Find $d$ such that $de \equiv 1 \mod \varphi(n)$. $\checkmark$

- **Alice** wants to pass bob $m$.
  - Receives $n, e$ from Bob.
  - Returns $X \equiv m^e \mod n$. $\checkmark$

- **Bob** receives $X$.
  - Calculates $X^d \mod n$. $\checkmark$
Finding Large Primes

- Let $n$ be a LARGE integer (e.g., $2^{4000}$).
- **The prime number theorem.** The probability of a random $p \in \{1, \ldots, n\}$ being prime is about $\frac{1}{\log n}$.

- If we randomly choose numbers from $\{1, \ldots, n\}$, we expect to have about $\log n$ iterations before finding a prime.
  - But how can we check whether our choice is a prime or not?!

Primality Testing

- Given a LARGE $q \in \mathbb{Z}$, how can we check whether $q$ is prime?
- **The naïve approach.** Go over every number in $\{2, \ldots, \sqrt{q}\}$ and check whether it divides $q$.
  - Our numbers are so large that a computer cannot do such a check in a reasonable time!
Recall: Fermat’s Little Theorem

• For any prime $p$ and integer $a$ relatively prime to $p$, we have

$$a^p \equiv a \mod p.$$  

• Pick an integer $a$ that is not a multiple of $q$ and check whether $a^q \equiv a \mod q$.
  ◦ If not, $q$ is not a prime!
  ◦ If yes, ???

Example: Fermat Primality Testing

• Is $n = 355207$ prime?

$$2^{355207} \equiv 84927 \mod 355207.$$  

• $n$ is not prime since $2^n \not\equiv 2 \mod n$.

• We can try 1000 different values of $a$ and see if $a^n \equiv a \mod n$ for each of them.
Carmichael Numbers

- A number \( q \in \mathbb{N} \) is said to be a **Carmichael number** if it is not prime, but still satisfies \( a^q \equiv a \mod q \) for every \( a \) that is relatively prime to \( q \).
  - The smallest such number is 561.
  - Very rare – about one in 50 trillion in the range \( 1 – 10^{21} \).

![R. D. Carmichael](image)

**Example:** Carmichael Numbers

- **Claim.** Let \( k \in \mathbb{N} \setminus \{0\} \) such that \( 6k + 1, 12k + 1, \) and \( 18k + 1 \) are primes. Then
  \[
  n = (6k + 1)(12k + 1)(18k + 1)
  \]
  is a **Carmichael number**.

- **Example.**
  - For \( k = 1 \), we have that 7, 13, 19 are primes.
  - \( 7 \cdot 13 \cdot 19 = 1729 \) is a Carmichael number.
Proof

• We need to prove that for any \(a\) that is relatively prime to \(n\), we have
  \[a^n \equiv a \mod n.\]
• Since \(GCD(a, n) = 1\), this is equivalent to proving \(a^{n-1} \equiv 1 \mod n\).
• We rewrite \(n = 1296k^3 + 396k^2 + 36k + 1\).
• For any such \(a\), we have
  \[a^{n-1} = a^{1296k^3 + 396k^2 + 36k} = (a^6k)^{216k^2 + 66k + 6}.\]

Proof (cont.)

• For any \(a\) relatively prime to \(n\), we have
  \[a^{n-1} = (a^6k)^{216k^2 + 66k + 6}.\]
• Recall. If \(a \in \mathbb{N}\) is not divisible by a prime \(p\) then \(a^{p-1} \equiv 1 \mod p\).
• Since \(a\) and \(6k + 1\) are relatively prime
  \[a^{n-1} \equiv 1^{216k^2 + 66k + 6} \equiv 1 \mod 6k + 1.\]
• Similarly, we have \(a^{n-1} \equiv 1 \mod 12k + 1\) and \(a^{n-1} \equiv 1 \mod 18k + 1\).
• Since \(a^{n-1} - 1\) is divisible by the three primes \(6k + 1, 12k + 1,\) and \(18k + 1\), it is also divisible by their product \(n\). That is, \(a^{n-1} \equiv 1 \mod n.\)
Miller–Rabin Primality Test

- The Miller–Rabin primality test works on every number.

Root of Unity

- **Claim.** For any prime \( p \), the only numbers \( a \in \{0, 1, \ldots, p - 1\} \) such that \( a^2 \equiv 1 \mod p \) are 1 and \( p - 1 \).

- **Example.** The solutions to
  \[ a^2 \equiv 1 \mod 1009 \]
  are exactly the numbers satisfying
  \[ a \equiv 1 \text{ or } 1008 \mod 1009. \]
Root of Unity

- **Claim.** For any prime $p$, the only numbers $a \in \{1, \ldots, p\}$ such that $a^2 \equiv 1 \mod p$ are 1 and $p - 1$.

- **Proof.**
  
  \[
  a^2 \equiv 1 \mod p \\
  a^2 - 1 \equiv 0 \mod p \\
  (a + 1)(a - 1) \equiv 0 \mod p
  \]

- That is, either $p|(a + 1)$ or $p|(a - 1)$.

Roots of Unity Properties

- Given a prime $p > 2$, we write
  
  \[
p - 1 = 2^s d
  \]

  where $d$ is odd and $s \geq 1$.

- **Claim.** For any odd prime $p$ and any $1 < a < p$, one of the following holds.
  
  - $a^d \equiv 1 \mod p$.
  - There exists $0 \leq r < s$ such that $a^{2^r d} \equiv -1 \mod p$.  

Roots of Unity Properties (2)

- **Claim.** For any odd prime $p$ and any $1 < a < p$, one of the following holds.
  - $a^d \equiv 1 \mod p$.
  - There exists $0 \leq r < s$ such that $a^{2^r d} \equiv -1 \mod p$.

- **Proof.**
  - By **Fermat’s little theorem**, $a^{p-1} \equiv 1 \mod p$.
  - Consider $a^{(p-1)/2}, a^{(p-1)/4}, ..., a^{(p-1)/2^s}$. By the previous claim, each such root is $\pm 1 \mod n$.
  - If all of these roots equal 1, we are in the first case. Otherwise, we are in the second.

Composite Witnesses

- Given a composite (non-prime) odd number $n$, we again write $n - 1 = 2^s d$ where $d$ is odd and $s \geq 1$.
- We say that $a \in \{2, 3, 4, ..., n - 2\}$ is a **witness** for $n$ if
  - $a^d \not\equiv 1 \mod n$.
  - For every $0 \leq r < s$, we have $a^{2^r d} \not\equiv -1 \mod n$. 
Example: Composite Witness

- **Problem.** Prove that 91 is not a prime.

  \[ 90 = 2 \cdot 45. \]

  \[ 2^{45} \equiv 57 \mod 91. \]

- **2 is a witness that 91 is not a prime.**

There are Many Witnesses

- Given an odd composite \( n \), the probability of a number \( \{2, \ldots, n - 2\} \) being a witness is at least \( \frac{1}{2} \) (this can be shown with basic group theory).

- Given an odd \( n \in \mathbb{N} \), take \( i \) numbers and check if they are witnesses.

  - If we found a witness, \( n \) is composite.
  - If we did not find a witness, \( n \) is prime with probability at least \( 1 - \frac{1}{2^i} \).
The End

Never forget: With great powers comes great difficulty in prime factorization.