

CS/MATH 111, Discrete Structures - Winter 2019.

Discussion 4 - Number Theory and Cryptography

Andres, Sara, Elena

University of California, Riverside

January 28, 2019

Outline

Euler's Totient

Problem 2

Primes, congruent to 3 (mod 4)

Conditions for parameters for RSA

Miller-Rabin Primality Test

Euler's Totient ¹

The totient $\varphi(n)$ of a positive integer $n > 1$ is defined to be the number of positive integers less than n that are coprime to n .

- ▶ $\varphi(1)$ is defined to be 1.
- ▶ If the prime factorization of n is given by: $n = p_1^{e_1} * \dots * p_n^{e_n}$, then $\varphi(n) = n * (1 - \frac{1}{p_1}) * \dots * (1 - \frac{1}{p_n})$.
- ▶ For example:
 - ▶ $9 = 3^2$, so $\varphi(9) = 9 * (1 - \frac{1}{3}) = 6$
 - ▶ $4 = 2^2$, so $\varphi(4) = 4 * (1 - \frac{1}{2}) = 2$
 - ▶ $15 = 3 * 5$, so $\varphi(15) = 15 * (1 - \frac{1}{3}) * (1 - \frac{1}{5}) = 15 * \frac{2}{3} * \frac{4}{5} = 8$

¹For more info have a look at <https://tinyurl.com/kxtcf95> ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡ ◀ ≡ ◀

Euler's Totient ²

The totient $\varphi(n)$ of a positive integer $n > 1$ is defined to be the number of positive integers less than n that are coprime to n .

- ▶ When n is a prime number, then $\varphi(n) = n - 1$.
- ▶ When m and n are coprime, then $\varphi(m * n) = \varphi(m) * \varphi(n)$.
- ▶ If n is the product of two prime number, p and q , then $\varphi(n) = (p - 1) * (q - 1)$.
- ▶ For example: $\varphi(15) = \varphi(3) * \varphi(5) = 2 * 4 = 8$.

²For more info have a look at <https://tinyurl.com/y75o4ogh>

Outline

Euler's Totient

Problem 2

Primes, congruent to 3 (mod 4)

Conditions for parameters for RSA

Miller-Rabin Primality Test

Problem 2

- ▶ “Break” RSA by guessing the factorization of n
- ▶ Compute Eulers Totient Function

$$\phi(n)$$

- ▶ Compute the decryption exponent d by computing

$$e^{-1} \pmod{\phi(n)}$$

solve this by enumerating.

- ▶ Using private key pair (d, n) , decrypt the messages by

$$M = C^d \pmod{n}$$

C stands for the encrypted messages.

Problem 2

- ▶ Show computation for 3 letters in \LaTeX : step-by-step, explaining everything;
- ▶ For the remaining message:
Need to write a program (any language) – Attach the program or compute by hand. All the computations attach (It is ok if written in pen).
- ▶ Decode the message

Outline

Euler's Totient

Problem 2

Primes, congruent to 3 (mod 4)

Conditions for parameters for RSA

Miller-Rabin Primality Test

Infinitely many primes, congruent to 3 (mod 4)

- ▶ Assume that $p_i = \{p_1, p_2, \dots, p_k\}$, where $p_1 = 3$, are primes of the form:

$$p_i \equiv 3 \pmod{4}$$

- ▶ We will construct a new one³ by looking at

$$N = 4 \cdot (p_1 \cdot p_2 \cdot \dots \cdot p_k) - 1$$

³ $N = 4 \cdot (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 3$ would also work.

Infinitely many primes, congruent to 3 (mod 4)

- ▶ $N = 4 \cdot (p_1 \cdot p_2 \cdot \dots \cdot p_k) - 1 \equiv 3 \pmod{4}$
- ▶ Let q be a prime factor of N , s.t. $q \mid N$, then:
 - ▶ $q \not\equiv 0 \pmod{4}$ [q should not be prime]
 - ▶ $q \not\equiv 2 \pmod{4}$ [N is odd]
 - ▶ $q \not\equiv 3 \pmod{4}$ [q should be part of $\{p_1, p_2, \dots, p_k\}$]
 - ▶ $q \equiv 1 \pmod{4}$
- ▶ Then, $N = q_1 \cdot q_2 \cdot \dots \cdot q_t$ and $\forall i \in \{1, 2, \dots, t\} : q_i \equiv 1 \pmod{4}$.
- ▶ So, $N \equiv 1 \pmod{4}$, which is a contradiction of our initial definition of N .

Outline

Euler's Totient

Problem 2

Primes, congruent to 3 (mod 4)

Conditions for parameters for RSA

Miller-Rabin Primality Test

Conditions for parameters for RSA

What if ???

$$\gcd(e, \phi(n)) > 1$$

$$d \equiv e^{-1} \pmod{\phi(n)}$$

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

- ▶ p and q are small...
- ▶ $p = q$
 - ▶ $\phi(n) = (p-1)(q-1)$?
 - ▶ $\phi(n) = (p-1)(p-1)$???
- ▶ Is double encryption correct?
- ▶ Is double encryption more secure?

Example

p	q	e	d	correct?	Encrypt $M = 7$ if correct. Justify if not correct.
6	11	5	29		
19	7	5	37		
17	17	9	89		
29	11	7	37		
3	7	5	5		

Example

p	q	e	d	$correct?$	<i>Encrypt $M = 7$. Justify.</i>
6	11	5	29	No	6 is not prime
19	7	5	37	No	$n = 133$ and $C = 7^5 \pmod{108}$
17	17	9	89	No	$p = q$
29	11	7	37	No	$e \cdot d \not\equiv 1 \pmod{\phi(n)}$
3	7	5	5	Yes	$n = 21$ and $C = 7^5 \pmod{12}$

Outline

Euler's Totient

Problem 2

Primes, congruent to 3 (mod 4)

Conditions for parameters for RSA

Miller-Rabin Primality Test

Miller-Rabin Primality Test

Primality is easy! ⁴

- ▶ A primality test is a test or algorithm for determining whether an input number is prime.
- ▶ N is prime if it has no divisors less or equal to \sqrt{N} .
- ▶ Most popular algorithms for primality testing are **probabilistic**; may output a composite number as a prime.

⁴A nice intro to primality tests at <https://tinyurl.com/m2aksy7>

Miller-Rabin Primality Test⁶

- ▶ Let n be a prime number⁵. Then $n - 1$ is even and we can write it as $2^s \cdot d$
- ▶ So we have:

$$n - 1 = 2^s \cdot d$$

where s and d are positive integers, and d is odd.

- ▶ For each a (a random positive integer), either...
 1. $a^d \equiv 1 \pmod{n}$ or
 2. $a^{2^r \cdot d} \equiv -1 \pmod{n}$, For all $0 \leq r \leq s - 1$.
- ▶ If we can find a , s.t. (1) and (2) are not true for all r , then n is not prime.

⁵ $n > 2$

⁶A great resource at <https://tinyurl.com/yafmmzax>

Example

Is $n = 221$ prime?

- ▶ We write $n - 1 = 220 = 2^2 \cdot 55$, so $s = 2$ and $d = 55$.
- ▶ We randomly select a number a s.t. $1 < a < n - 1$. Let $a = 174$.
- ▶ We proceed to compute:
 - ▶ $a^{2^0 \cdot d} \pmod{n} = 174^{55} \pmod{221} = 47 \neq 1, -1$
 - ▶ $a^{2^1 \cdot d} \pmod{n} = 174^{110} \pmod{221} = 220 = -1$
- ▶ Since $220 \equiv -1 \pmod{n}$, either 221 is prime, or 174 is a **strong liar** for 221.
- ▶ Keep trying...

Example

Is $n = 221$ prime?

- ▶ We write $n - 1 = 220 = 2^2 \cdot 55$, so $s = 2$ and $d = 55$.
- ▶ We try another random a , this time let $a = 137$:
 - ▶ $a^{2^0 \cdot d} \bmod n = 137^{55} \bmod 221 = 188 \neq 1, -1$
 - ▶ $a^{2^1 \cdot d} \bmod n = 137^{110} \bmod 221 = 205 \neq 1, -1$
- ▶ Hence 137 is a **witness** for the compositeness of 221, and 174 was in fact a strong liar.
- ▶ Factors of 221 are 13 and 17.

Reference

- ▶ Discrete Mathematics and Its Applications. Rosen, K.H. 2012. McGraw-Hill.
Chapter 4: Number Theory and Cryptography.