SIC Week 3

Question 1a

Which of the following numbers is not a prime number

313,317,379,887,983, 992, 997

The simplest primality test: **trial division**

Given a number n

check whether any prime integer m from 2 to $\sqrt{n}$ evenly divides n (no remainder)

if there is one such integer => n is not prime

if there is no such integer => n is prime

Answer: 992 is not a prime number, the other numbers are prime

Question 1a (Java Code)

```
public class Test1 {

    public static void main(String[] args) {
        int[] numbers = new int[] {313 , 317, 379, 887, 983, 992, 997};
        for(int number : numbers) {
            System.out.printf("Is %d prime? Answer: %s\n",
                        number, isPrime(number) ? "yes" : "no");
        }
    }

    public static boolean isPrime(int n) {

        double squareRootOfN = Math.sqrt(n);

        for(int i = 2; i < squareRootOfN; i++) {
            if(n % i == 0) return false;
        }

        return true;
    }
}
```

Output:
Is 313 prime? Answer: yes
Is 317 prime? Answer: yes
Is 379 prime? Answer: yes
Is 887 prime? Answer: yes
Is 983 prime? Answer: yes
Is 992 prime? Answer: no
Is 997 prime? Answer: yes

Question 1 b, c, d

How to find greatest common divisor:

Find the greatest common divisor (GCD).

252, 180, 96, 60

$252 = 2 \bullet 2 \bullet 3 \bullet 3 \bullet 7$

$180 = 2 \bullet 2 \bullet 3 \bullet 3 \bullet 5$

$96 = 2 \bullet 2 \bullet 2 \bullet 2 \bullet 2 \bullet 3$

$60 = 2 \bullet 2 \bullet 3 \bullet 5$

Write the prime factorization of each number and circle the common prime factors.

$2 \bullet 2 \bullet 3 = 12$

Multiply the common prime factors.

The GCD is 12.

GCD(8, 12) = 4

GCD(9, 21) = 3

GCD(9, 11) = 1

Question 1 e,

What is the value of 51 mod 5

i.e. what is the remainder of 51 / 5?

answer: 51 = 10 * 5 + 1 => 51 mod 5 = 1

What is the value of 389 mod 77

answer: 4

Question 1 f, g

Find two coprime numbers

The probability that any two integers taken randomly are coprime is nearly 60% (http://mathworld.wolfram.com/RelativelyPrime.html)

Pick 2 random number and check gcd(a, b)

    if gcd(a, b) = 1

        a and b are coprime

    else

        a, b are not coprime

Example: integers coprime to 12: 5,7,11,13,17,19,23,25

because gcd(12, 5) = 1, gcd(12, 7) = 1, gcd(12, 19) = 1 ......

Are 6 and 30 coprime?

No, because gcd(6, 30) is 6, not 1

Question 1 h

Find out LCM(30,60) and LCM(14, 21)

$$\operatorname{lcm}(n,m) = \frac{m \cdot n}{\gcd(m,n)}.$$

LCM(30, 60) = 30 * 60 / gcd(30, 60) = 1800 / 30 = 60

LCM(14, 21) = 14 * 21 / gcd(14, 21) = 14 * 21 / 7 = 42

Question 2 (Modular arithmetic)

Online calculator:

- http://www.wolframalpha.com
- https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html
- https://planetcalc.com/3311/

10^{19} mod 33 = 10

5^{11} mod 77 = 38

7^{-1} mod 33 = multiplicative inverse of 7 mod 33 = 19

because 19 * 7 = 1 mod 33

23^{-1} mod 551 = multiplicative inverse of 23 mod 551 = 24

because 24 * 23 = 1 mod 551

Question 2: RSA

Key generation (receiver Bob)

- Pick two prime numbers

  $p = 19$ and $q = 29$

- Calculate n

  $n = p * q = 19 * 29 = 551$

- Calculate $\boldsymbol{\phi}(n)$

  $$\begin{aligned}\boldsymbol{\phi}(n) &= (p - 1) * (q - 1) \\ &= (19 - 1) * (29 - 1) = 504\end{aligned}$$

- Choose a prime number e

  e is coprime to $\boldsymbol{\phi}(n)$,
  i.e. $\boldsymbol{\phi}(n)$ is not divisible by e
  $\gcd(e, 504) = 1$

  Let select e in $1 < e < \boldsymbol{\phi}(n)$
  => Let's pick $e = 59$

- Public key $(n, e) = (551, 59)$

- Private key generation

  Let d be the private key
  => $de = 1 \bmod \boldsymbol{\phi}(n)$
  => $d * 59 = 1 \bmod 504$
  => $d = 299$

Question 2: RSA

Encryption (sender Alice)

- Receive Bob's public key

  $(n, e) = (551, 59)$

- Use the public key to encrypt a message $M = 100$

  $C = M^e \bmod n$
  $= 100^{59} \bmod 551 = 370$

- Send the ciphertext $C = 370$ to Bob

Decryption (receiver Bob)

- Bob receives ciphertext $C = 370$ from Alice
- Bob use the private key $d = 299$ to decrypt

  $M = C^d \bmod n$
  $= 370^{299} \bmod 551$
  $= 100$

Question 3: RSA

Key generation (receiver Bob)

- Pick two prime numbers

  $p = 3$ and $q = 11$

- Calculate n

  $n = p * q = 3 * 11 = 33$

- Calculate $\phi(n)$

  $$\begin{aligned}\phi(n) &= (p - 1) * (q - 1) \\ &= (3 - 1) * (11 - 1) = 20\end{aligned}$$

- Choose a prime number e

  e is coprime to $\phi(n)$,
  i.e. $\phi(n)$ is not divisible by e
  $\gcd(e, 20) = 1$

  Let select e in $1 < e < \phi(n)$
  => Let's pick $e = 7$

- Public key $(n, e) = (33, 7)$

- Private key generation

  Let d be the private key
  => $de = 1 \bmod \phi(n)$
  => $d * 7 = 1 \bmod 20$
  => $d = 3$

Question 3: RSA (continue)

Encryption (sender Alice)

- Receive Bob's public key

  $(n, e) = (33, 7)$

- Use the public key to encrypt a message $M = 2$

  $C = M^e \bmod n$
  $= 2^7 \bmod 33 = 29$

- Send the ciphertext $C = 29$ to Bob

Decryption (receiver Bob)

- Bob receives ciphertext $C = 29$ from Alice
- Bob use the private key $d = 3$ to decrypt

  $M = C^d \bmod n$
  $= 29^3 \bmod 33$
  $= 2$

Question 4

Trudy factorizes 481

481 = 13 * 37

Calculate $\phi(n) = (p-1)*(q-1)$

$= (13-1)*(37-1) = 432$

Given e = 47

If d is the private key, then

$$de = 1\, mod\, \phi(n)$$

d * 47 = 1 mod 432
=> d is the multiplicative inverse of 47 mod 432
=> d = 239 by using Wolfram Alpha website

Given C = 463

Decryption using Private key
$M = C^d\, mod\, n = 463^{239}\, mod\, 481 = 200$

Verify that encryption using the public key generates the intended value:

$$C = M^e\, mod\, n = 200^{47}\, mod\, 481 = 463$$

Link to slides

https://tinyurl.com/y8p67m87

Notes in Week 4:

https://docs.google.com/document/d/1roabI1BR4UKHEUYxNb7BrvOC0ytxNcv4MG8AbwdZt2g/edit?usp=sharing

Asymmetric Key Operations with RSA and OpenSSL

https://docs.google.com/document/d/13XrFhfhohokiP_68Nxa7-7jU480IguQCe_OeQH52ViY/edit?usp=sharing