CS5285
Tutorial 4

Question 1

Modular Exponentiation

(a) Calculate $17^{27} \mod 23$.

(b) Consider the following two cases of raising a number to a certain exponent:

- $a^{255} \mod b$
- $a^{257} \mod b$

Using the square and multiply method, which one of these two exponentiations will be significantly more expensive? Why? Calculate the total number of modular multiplications required for each case (counting a squaring operation as a modular multiplication).

Modular Exponentiation

Method 2 : *Square-and-Multiply Algorithm*

e.g. $11^{15} \bmod 13 = 11^{8+4+2+1} \bmod 13 = 11^8 \times 11^4 \times 11^2 \times 11 \bmod 13$ — (1)

- $11^2 = 121 \equiv 4 \pmod{13}$ — (2)
- $11^4 = (11^2)^2 \equiv (4)^2 \equiv 3 \pmod{13}$ — (3)
- $11^8 = (11^4)^2 \equiv (3)^2 \equiv 9 \pmod{13}$ — (4)

Put (2), (3) and (4) to (1) and get

$11^{15} \equiv 9 \times 3 \times 4 \times 11 \equiv 5 \pmod{13}$

- performed at most $2\lfloor \log_2 15 \rfloor$ modular multiplications
- Complexity = $O(\lg(e))$

Solution 1(a)

We first square 17 several times mod 23 (use the Square-and-Multiply method):

$$
\begin{aligned}
17^2 &\mod 23 = 13 \\
17^4 &\mod 23 = (17^2)^2 \mod 23 = (13)^2 \mod 23 = 8 \\
17^8 &\mod 23 = (17^4)^2 \mod 23 = (8)^2 \mod 23 = 18 \\
17^{16} &\mod 23 = (17^8)^2 \mod 23 = (18)^2 \mod 23 = 2
\end{aligned}
$$

Putting appropriate terms together we get:

$$
\begin{aligned}
17^{27} \mod 23 &= 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17 \mod 23 \\
&= 2 \cdot 18 \cdot 13 \cdot 17 \mod 23 = \mathbf{21}
\end{aligned}
$$

Question 1

Modular Exponentiation

(a) Calculate $17^{27} \mod 23$.

(b) Consider the following two cases of raising a number to a certain exponent:

- $a^{255} \mod b$
- $a^{257} \mod b$

Using the square and multiply method, which one of these two exponentiations will be significantly more expensive? Why? Calculate the total number of modular multiplications required for each case (counting a squaring operation as a modular multiplication).

Solution 1(b)

- $257 = \{100000001\}_b$
- For 257 we need to do 8 square ($a^{256}, a^{128}, a^{64}, a^{32}, a^{16}, a^{8}, a^{4}, a^{2}$) and then 1 multiply ($a^{256} * a^{1}$)

  = 9 total multiplications
- $255 = \{11111111\}_b$
- For 255 we need to do 7 square ($a^{128}, a^{64}, a^{32}, a^{16}, a^{8}, a^{4}, a^{2}$) , 7 multiply ($a^{128} * a^{64} * a^{32} * a^{16} * a^{8} * a^{4} * a^{2} * a^{1}$)

  = 14 total multiplication

Modular Inverse

A is the modular inverse of B mod n if

AB mod n = 1.

A is denoted as B^{-1} mod n.

e.g.

- 3 is the modular inverse of 5 mod 7. In other words, 5^{-1} mod 7 = 3.
- 7 is the modular inverse of 7 mod 16. In other words, 7^{-1} mod 16 = 7.

However, there is no modular inverse for 8 mod 14.

There exists a modular inverse for B mod n if B is relatively prime to n.

Question:
What's the modular inverse of 911 mod 999?

Extended Euclidean Algorithm

The extended Euclidean algorithm can be used to solve the integer equation

$$ax + by = \gcd(a, b)$$

For any given integers a and b.

Example

Let a = 911 and b = 999. Get gcd from the Euclidean algorithm,

$$\begin{aligned}
999 &= 1 \times 911 + 88 \\
911 &= 10 \times 88 + 31 \\
88 &= 2 \times 31 + 26 \\
31 &= 1 \times 26 + 5 \\
26 &= 5 \times 5 + 1 \qquad \Rightarrow \gcd(a, b) = 1 \text{ (so they are relatively prime)}
\end{aligned}$$

Tracing backward, we get

$$\begin{aligned}
1 &= 26 - 5 \times 5 \\
&= 26 - 5 \times (31 - 1 \times 26) = -5 \times 31 + 6 \times 26 \\
&= -5 \times 31 + 6 \times (88 - 2 \times 31) = 6 \times 88 - 17 \times 31 \\
&= 6 \times 88 - 17 \times (911 - 10 \times 88) = -17 \times 911 + 176 \times 88 \\
&= -17 \times 911 + 176 \times (999 - 1 \times 911) = \mathbf{176 \times 999 - 193 \times 911}
\end{aligned}$$

Question 2a

So how do we go about finding inverse of 2019 mod 5285?

We use the Extended Euclidean Algorithm:

$$\begin{aligned}
5285 &= 2 \cdot 2019 + 1247 \\
2019 &= 1247 + 772 \\
1247 &= 772 + 475 \\
772 &= 475 + 297 \\
475 &= 297 + 178 \\
297 &= 178 + 119 \\
178 &= 119 + 59 \\
119 &= 2 \cdot 59 + 1
\end{aligned}$$

So $\gcd(2019, 5285) = 1$, and we know 2019 does have a multiplicative inverse.

Question 2a

We can find it by reversing the process:

$$
\begin{aligned}
1 &= 119 - 2 \cdot 59 = 119 - 2(178 - 119) = 3 \cdot 119 - 2 \cdot 178 \\
1 &= 3(297 - 178) - 2 \cdot 178 = 3 \cdot 297 - 5 \cdot 178 \\
1 &= 3 \cdot 297 - 5(475 - 297) = 8 \cdot 297 - 5 \cdot 475 \\
1 &= 8 \cdot (772 - 475) - 5 \cdot 475 = 8 \cdot 772 - 13 \cdot 475 \\
1 &= 8 \cdot 772 - 13 \cdot (1247 - 772) = 21 \cdot 772 - 13 \cdot 1247 \\
1 &= 21 \cdot (2019 - 1247) - 13 \cdot 1247 = 21 \cdot 2019 - 34 \cdot 1247 \\
1 &= 21 \cdot 2019 - 34 \cdot (5285 - 2 \cdot 2019) = 89 \cdot 2019 - 34 \cdot 5285
\end{aligned}
$$

The modular inverse of $2019 \mod 5285$ is 89.

Question 2b

(b) Without calculating anything, can you tell whether 360 mod 555 has a modular inverse? Explain why.

It is obvious that both numbers are divisible by 5, so they are not relatively prime. Therefore, no multiplicative inverse exists.

Question 3

Calculate $\phi(n)$ for the following values of n.

(a) $n = 83$

(b) $n = 1210$

2) Calculate 39^{191} mod 47

The Euler phi Function

For $n \geq 1$, $\phi(n)$ denotes the number of integers in the interval $[1, n]$ which are relatively prime to n. The function ϕ is called the **Euler phi function** (or the **Euler totient function**).

Fact 1. The Euler phi function is multiplicative. I.e. if $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m) \times \phi(n)$.

Fact 2. For a prime p and an integer $e \geq 1$, $\phi(p^e) = p^{e-1}(p-1)$.

- From these two facts, we can find ϕ for any composite n if the prime factorization of n is known.
- Let $n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$ where $p_1,\ldots, p_k$ are prime and each e_i is a nonzero positive integer.
- Then

$$\phi(n) = p_1^{e_1-1} (p_1-1) . p_2^{e_2-1} (p_2-1) \ldots p_k^{e_k-1} (p_k-1)$$

Fermat's Little Theorem

Let p be a prime. Any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \pmod{p}$.

- We can generalize the Fermat's Little Theorem as follows. This is due to Euler.

  Euler's Generalization Let n be a composite. Then $a^{\phi(n)} \equiv 1 \pmod{n}$ for any integer a which is relatively prime to n.

- E.g. $a=3; n=10$; $\varphi(10)=4 \Rightarrow 3^4 \equiv 81 \equiv 1 \pmod{10}$
- E.g. $a=2; n=11$; $\varphi(11)=10 \Rightarrow 2^{10} \equiv 1024 \equiv 1 \pmod{11}$

Exercise: Compute $11^{1,073,741,823}$ mod 13.
Compute $11^{12}.11^{12}.11^{12}.11^{12}.....11^{4}$ mod 13 $\equiv 3 \pmod{13}$

Solution (3)

1.a) 83
83 is a prime number, so $83^0*(83-1) = 82$

1.b) 1210
1210/2=605 – cannot divide by 2 or 3,
1210/5=121 – cannot divide by 5,7
121/11 = 11, 11/11=1
Prime factorisation of 1210 = 11^2*5*2

So $11^{1*}(11-1)*5^0*(4)*2^0*(1) = 440$

2) Calculate 39^{191} mod 47
$39^{191} = 39^{184}*39^7 =(39^{46})^4*39^7$
$\phi(47)=46$, and $a^{\phi(n)} \equiv 1 \pmod{n}$
$(39^{46})^4*39^7 \bmod 47 \equiv (1)^4*39^7 \bmod 47 \equiv 35$

Question 4a

(a) Can you show why RSA encryption works? Hint: Fermat's Little Theorem...

User Euler's generalisation of Fermat Little Theorem. $a^{\phi(n)}\ mod\ n = 1 \bmod n$.
Lets first show that the following equation is valid $M = M^{ed} \bmod n$
You know that $ed = 1 \bmod \phi(n)$
So $ed = k \cdot \phi(n) + 1 \bmod \phi(n)$
So $M^{ed} \bmod n = M^{k \cdot \phi(n)+1} \bmod n = M \cdot M^{k \cdot \phi(n)} \bmod n$
Apply Fermat: $M \cdot 1 \bmod n = M \bmod n$

Question 4b

(b) Can you encrypt M when it is larger than n?

No. The maximum message size is determined by modulus n, $M < n$. Why?
Lets choose $M = n + x$. Then the process and maths is the same as above...
$C = (n+x)^e \bmod n$, $M = C^d \bmod n = ((n+x)^e)^d \bmod n = (n+x)^{ed} \bmod n$
You know that $ed = 1 \bmod \phi(n)$
So $ed = k \cdot \phi(n) + 1 \bmod \phi(n)$
So $M = (n+x)^{ed} \bmod n = (n+x)^{k \cdot \phi(n)+1} \bmod n = (n+x) \cdot (n+x)^{k \cdot \phi(n)} \bmod n$
Apply Fermat: $M = (n+x) \cdot 1 \bmod n = (n+x) \bmod n = x$
This is not message you encrypted: $n + x \neq x$

The end!

?

Any questions…