CSc 466/566

Computer Security

17 : Number Theory — Exponentiation and Totient

Version: 2019/10/29 14:22:05

Department of Computer Science
University of Arizona

collberg@gmail.com

Christian Collberg

Outline

Modular Exponentiation

- Modular exponentiation is an important operation in cryptography:

$$x^y \bmod n = \overbrace{x \cdot x \cdot \cdots \cdot x}^{y} \bmod n$$

Exercise

- Compute: $2^2 \bmod 3 =$

Exercise

- Compute: $2^2 \bmod 3 = 1$
- Compute: $2^4 \bmod 5 =$

Exercise

- Compute: $2^2 \bmod 3 = 1$
- Compute: $2^4 \bmod 5 = 1$
- Compute: $3^4 \bmod 5 =$

Exercise

- Compute: $2^2 \bmod 3 = 1$
- Compute: $2^4 \bmod 5 = 1$
- Compute: $3^4 \bmod 5 = 1$

Modular Exponentiation Tables

- The next two slides have modular exponentiation tables for
  - Z_{10}, x^y mod 10.
  - Z_{13}, x^y mod 13.
- Elements in Z_n that have some power equal to 1 have been highlighted.

Z_{10}, $x^y \bmod 10$

	y								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1^y	1	1	1	1	1	1	1	1	1
2^y	2	4	8	6	2	4	8	6	2
3^y	3	9	7	1	3	9	7	1	3
4^y	4	6	4	6	4	6	4	6	4
5^y	5	5	5	5	5	5	5	5	5
6^y	6	6	6	6	6	6	6	6	6
7^y	7	9	3	1	7	9	3	1	7
8^y	8	4	2	6	8	4	2	6	8
9^y	9	1	9	1	9	1	9	1	9

Z_{13}, x^y mod 13

	y											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
$\mathbf{1}^y$	1	1	1	1	1	1	1	1	1	1	1	1
$\mathbf{2}^y$	2	4	8	3	6	12	11	9	5	10	7	1
$\mathbf{3}^y$	3	9	1	3	9	1	3	9	1	3	9	1
$\mathbf{4}^y$	4	3	12	9	10	1	4	3	12	9	10	1
$\mathbf{5}^y$	5	12	8	1	5	12	8	1	5	12	8	1
$\mathbf{6}^y$	6	10	8	9	2	12	7	3	5	4	11	1
$\mathbf{7}^y$	7	10	5	9	11	12	6	3	8	4	2	1
$\mathbf{8}^y$	8	12	5	1	8	12	5	1	8	12	5	1
$\mathbf{9}^y$	9	3	1	9	3	1	9	3	1	9	3	1
$\mathbf{10}^y$	10	9	12	3	4	1	10	9	12	3	4	1
$\mathbf{11}^y$	11	4	5	3	7	12	2	9	8	10	6	1
$\mathbf{12}^y$	12	1	12	1	12	1	12	1	12	1	12	1

Exercise

- Create the modular exponentiation table for Z_5, $x^y \bmod 5$. Highlight the ones.

	y			
	1	**2**	**3**	**4**
$\mathbf{1^y}$				
$\mathbf{2^y}$				
$\mathbf{3^y}$				
$\mathbf{4^y}$				

Outline

Computing Modular Exponentiation

- Modular exponentiation is an important operation in cryptography.

$$g^n \bmod p = \overbrace{g \cdot g \cdot \cdots \cdot g}^{n} \bmod p$$

Computing Modular Exponentiation

- Modular exponentiation is an important operation in cryptography.

$$g^n \bmod p = \overbrace{g \cdot g \cdot \cdots \cdot g}^{n} \bmod p$$

- Simply iteratively multiplying the g:s together is too slow.

Computing Modular Exponentiation

- Modular exponentiation is an important operation in cryptography.

$$g^n \bmod p = \overbrace{g \cdot g \cdot \cdots \cdot g}^{n} \bmod p$$

- Simply iteratively multiplying the g:s together is too slow.
- In practice, the numbers are very large!!!

Computing Modular Exponentiation

- Modular exponentiation is an important operation in cryptography.

$$g^n \bmod p = \overbrace{g \cdot g \cdot \cdots \cdot g}^{n} \bmod p$$

- Simply iteratively multiplying the g:s together is too slow.
- In practice, the numbers are very large!!!
- Instead, we use Repeated Squaring.

Repeated Squaring

- Instead, we compute

$$g$$

Repeated Squaring

- Instead, we compute

$$g$$

Repeated Squaring

- Instead, we compute

$$\begin{aligned} & g \\ g^2 &= g \cdot g \end{aligned}$$

Repeated Squaring

- Instead, we compute

$$
\begin{aligned}
& g \\
g^2 &= g \cdot g \\
g^4 &= g^2 \cdot g^2
\end{aligned}
$$

Repeated Squaring

- Instead, we compute

$$\begin{aligned} &g \\ g^2 &= g \cdot g \\ g^4 &= g^2 \cdot g^2 \\ g^8 &= g^4 \cdot g^4 \end{aligned}$$

- We can then use these powers to compute g^n:

$$g^{25} = g^{16+8+1} = g^{16} \cdot g^8 \cdot g^1$$

Repeated Squaring

- Instead, we compute

$$\begin{aligned} &g \\ g^2 &= g \cdot g \\ g^4 &= g^2 \cdot g^2 \\ g^8 &= g^4 \cdot g^4 \end{aligned}$$

- We can then use these powers to compute g^n:

$$g^{25} = g^{16+8+1} = g^{16} \cdot g^8 \cdot g^1$$

Repeated Squaring

- Instead, we compute

$$\begin{aligned} g & \\ g^2 &= g \cdot g \\ g^4 &= g^2 \cdot g^2 \\ g^8 &= g^4 \cdot g^4 \end{aligned}$$

- We can then use these powers to compute g^n:

$$\begin{aligned} g^{25} &= g^{16+8+1} = g^{16} \cdot g^8 \cdot g^1 \\ g^{46} &= g^{32+8+4+2} = g^{32} \cdot g^8 \cdot g^4 \cdot g^2 \end{aligned}$$

Repeated Squaring...

- Compute $g^n \bmod p$:

```
function modexp(int g, int n, int p)
    int q ← 1
    int m ← n
    int square ← g
    while m ≥ 1 do
        if odd(m) then
            g ← q · square mod p
        square ← square · square mod p
        m ← ⌊m/2⌋
```

Exercise: Repeated Squaring

Assume that you have already computed

$$\begin{array}{rcl} 3^1 & = & 3 \\ 3^2 & = & 3 \cdot 3 \\ 3^4 & = & 3^2 \cdot 3^2 \\ 3^8 & = & 3^4 \cdot 3^4 \\ \ldots & \ldots & \ldots \end{array}$$

compute these exponentiations:

- Compute 3^5:

Exercise: Repeated Squaring

Assume that you have already computed

$$\begin{array}{rcl} 3^1 & = & 3 \\ 3^2 & = & 3 \cdot 3 \\ 3^4 & = & 3^2 \cdot 3^2 \\ 3^8 & = & 3^4 \cdot 3^4 \\ \dots & \dots & \dots \end{array}$$

compute these exponentiations:

- Compute 3^5: $3^5 = 3^{4+0+1} = 3^4 \cdot 3^1$
- Compute 3^7:

Exercise: Repeated Squaring

Assume that you have already computed

$$\begin{array}{rcl} 3^1 & = & 3 \\ 3^2 & = & 3 \cdot 3 \\ 3^4 & = & 3^2 \cdot 3^2 \\ 3^8 & = & 3^4 \cdot 3^4 \\ \ldots & \ldots & \ldots \end{array}$$

compute these exponentiations:

- Compute 3^5: $3^5 = 3^{4+0+1} = 3^4 \cdot 3^1$
- Compute 3^7: $3^7 = 3^{4+2+1} = 3^4 \cdot 3^2 \cdot 3^1$
- Compute 3^{12}:

Exercise: Repeated Squaring

Assume that you have already computed

$$\begin{array}{rcl} 3^1 & = & 3 \\ 3^2 & = & 3 \cdot 3 \\ 3^4 & = & 3^2 \cdot 3^2 \\ 3^8 & = & 3^4 \cdot 3^4 \\ \cdots & \cdots & \cdots \end{array}$$

compute these exponentiations:

- Compute 3^5: $3^5 = 3^{4+0+1} = 3^4 \cdot 3^1$
- Compute 3^7: $3^7 = 3^{4+2+1} = 3^4 \cdot 3^2 \cdot 3^1$
- Compute 3^{12}: $3^{12} = 3^{8+4+0+0} = 3^8 \cdot 3^4$
- Compute 3^{46}:

Exercise: Repeated Squaring

Assume that you have already computed

$$\begin{array}{rcl} 3^1 & = & 3 \\ 3^2 & = & 3 \cdot 3 \\ 3^4 & = & 3^2 \cdot 3^2 \\ 3^8 & = & 3^4 \cdot 3^4 \\ \dots & \dots & \dots \end{array}$$

compute these exponentiations:

- Compute 3^5: $3^5 = 3^{4+0+1} = 3^4 \cdot 3^1$
- Compute 3^7: $3^7 = 3^{4+2+1} = 3^4 \cdot 3^2 \cdot 3^1$
- Compute 3^{12}: $3^{12} = 3^{8+4+0+0} = 3^8 \cdot 3^4$
- Compute 3^{46}:
  $3^{46} = 3^{32+0+8+4+2+0} = 3^{32} \cdot 3^8 \cdot 3^4 \cdot 3^2$

Outline

Z_n^*

- Z_n^* is the subset of Z_n of elements relatively prime with n:

$$Z_n^* = \{x \in Z_n \text{ such that } \mathrm{GCD}(x, n) = 1\}$$

- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\}$

Z_n^*

- Z_n^* is the subset of Z_n of elements relatively prime with n:

$$Z_n^* = \{x \in Z_n \text{ such that } \mathrm{GCD}(x, n) = 1\}$$

- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\}$
  2. $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Z_n^*

- Z_n^* is the subset of Z_n of elements relatively prime with n:

$$Z_n^* = \{x \in Z_n \text{ such that } \mathrm{GCD}(x, n) = 1\}$$

- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\}$
  2. $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Z_n^*

- Z_n^* is the subset of Z_n of elements relatively prime with n:

$$Z_n^* = \{x \in Z_n \text{ such that } \mathrm{GCD}(x, n) = 1\}$$

- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\}$
  2. $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
- In general, $Z_n^* = \{1, 2, \dots, n-1\}$ if n is prime

Exercise

Compute Z_n^*:

- $Z_3^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* = \{1,3\}$
- $Z_5^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* = \{1,3\}$
- $Z_5^* = \{1,2,3,4\}$
- $Z_6^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* = \{1,3\}$
- $Z_5^* = \{1,2,3,4\}$
- $Z_6^* = \{1,5\}$
- $Z_7^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* = \{1,3\}$
- $Z_5^* = \{1,2,3,4\}$
- $Z_6^* = \{1,5\}$
- $Z_7^* = \{1,2,3,4,5,6\}$
- $Z_8^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* = \{1,3\}$
- $Z_5^* = \{1,2,3,4\}$
- $Z_6^* = \{1,5\}$
- $Z_7^* = \{1,2,3,4,5,6\}$
- $Z_8^* = \{1,3,5,7\}$
- $Z_9^* =$

Exercise

Compute Z_n^*:

- $Z_3^* = \{1,2\}$
- $Z_4^* = \{1,3\}$
- $Z_5^* = \{1,2,3,4\}$
- $Z_6^* = \{1,5\}$
- $Z_7^* = \{1,2,3,4,5,6\}$
- $Z_8^* = \{1,3,5,7\}$
- $Z_9^* = \{1,2,4,5,7,8\}$

Euler's Totient Function

- $\phi(n)$ is the totient of n, the number of elements of Z_n^*:
$$\phi(n) = |Z_n^*|$$
- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\} \Rightarrow \phi(10) = 4$

Euler's Totient Function

- $\phi(n)$ is the totient of n, the number of elements of Z_n^*:
$$\phi(n) = |Z_n^*|$$
- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\} \Rightarrow \phi(10) = 4$
  2. $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \Rightarrow \phi(13) = 12$

Euler's Totient Function

- $\phi(n)$ is the totient of n, the number of elements of Z_n^*:
$$\phi(n) = |Z_n^*|$$
- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\} \Rightarrow \phi(10) = 4$
  2. $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \Rightarrow \phi(13) = 12$

Euler's Totient Function

- $\phi(n)$ is the totient of n, the number of elements of Z_n^*:
$$\phi(n) = |Z_n^*|$$
- Examples:
  1. $Z_{10}^* = \{1, 3, 7, 9\} \Rightarrow \phi(10) = 4$
  2. $Z_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\} \Rightarrow \phi(13) = 12$
- In general, if n is prime, $Z_n^* = \{1, 2, \ldots, n-1\} \Rightarrow \phi(n) = n - 1$.

Exercise

Compute Z_n^*:

- $|Z_3^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| = 2$
- $|Z_5^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| = 2$
- $|Z_5^*| = 4$
- $|Z_6^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| = 2$
- $|Z_5^*| = 4$
- $|Z_6^*| = 2$
- $|Z_7^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| = 2$
- $|Z_5^*| = 4$
- $|Z_6^*| = 2$
- $|Z_7^*| = 5$
- $|Z_8^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| = 2$
- $|Z_5^*| = 4$
- $|Z_6^*| = 2$
- $|Z_7^*| = 5$
- $|Z_8^*| = 4$
- $|Z_9^*| =$

Exercise

Compute Z_n^*:

- $|Z_3^*| = 2$
- $|Z_4^*| = 2$
- $|Z_5^*| = 4$
- $|Z_6^*| = 2$
- $|Z_7^*| = 5$
- $|Z_8^*| = 4$
- $|Z_9^*| = 6$

Euler's Totient Function Values

n	$\phi(n)$	List of Divisors
1	1	1
2	1	1, 2
3	2	1, 3
4	2	1, 2, 4
5	4	1, 5
6	2	1, 2, 3, 6
7	6	1, 7
8	4	1, 2, 4, 8
9	6	1, 3, 9
10	4	1, 2, 5, 10
11	10	1, 11
12	4	1, 2, 3, 4, 6, 12
13	12	1, 13
14	6	1, 2, 7, 14
15	8	1, 3, 5, 15
16	8	1, 2, 4, 8, 16
17	16	1, 17
18	6	1, 2, 3, 6, 9, 18

n	$\phi(n)$	List of Divisors
19	18	1, 19
20	8	1, 2, 4, 5, 10, 20
21	12	1, 3, 7, 21
22	10	1, 2, 11, 22
23	22	1, 23
24	8	1, 2, 3, 4, 6, 8, 12, 24
25	20	1, 5, 25
26	12	1, 2, 13, 26
27	18	1, 3, 9, 27
28	12	1, 2, 4, 7, 14, 28
29	28	1, 29
30	8	1, 2, 3, 5, 6, 10, 15, 30
31	30	1, 31
32	16	1, 2, 4, 8, 16, 32
33	20	1, 3, 11, 33
34	16	1, 2, 17, 34
35	24	1, 5, 7, 35
36	12	1, 2, 3, 4, 6, 9, 12, 18, 36

Euler's Totient Function...

- You can calculate $\phi(n)$ as

$$\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_m})$$

  where $p_1, \ldots, p_m$ are the the prime factors of n.
- Example:
  1. $\phi(35) = 35(1 - \frac{1}{5})(1 - \frac{1}{7}) = 35 \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$

Exercises

1. $\phi(37)=$

Exercises

1. $\phi(37) = \phi(37) = 36$ since 37 is prime.
2. $\phi(38) =$

Exercises

1. $\phi(37)$=$\phi(37) = 36$ since 37 is prime.
2. $\phi(38) = 38 = 19 \times 2 \Rightarrow \phi(38) = 38(1 - \frac{1}{19})(1 - \frac{1}{2}) = 38 \cdot \frac{18}{19} \cdot \frac{1}{2} = 18$

Outline

Readings and References

- Chapter 8.1.7, 8.2.1, 8.5.2 in *Introduction to Computer Security*, by Goodrich and Tamassia.

Acknowledgments

Additional material and exercises have also been collected from these sources:

1. Igor Crk and Scott Baker, *620—Fall 2003—Basic Cryptography*.
2. William Stallings, *Cryptography and Network Security*.
3. Bruce Schneier, *Applied Cryptography*.
4. Neal R. Wagner, *The Laws of Cryptography with Java Code*, http://amadousarr.free.fr/java/javacryptobook.pdf.
5. *Euler's Totient Function Values For n = 1 to 500, with Divisor Lists*, http://primefan.tripod.com/Phi500.html
6. Diffie-Hellman calculator: http://dkerr.home.mindspring.com/diffie_hellman_calc.html.