
CHAPTER 9

Mathematics of Cryptography: Part 3

(Solution to Practice Set)

Review Questions

1. A positive integer is a *prime* if and only if it is exactly divisible by two integers, 1 and itself. A *composite* is a positive integer with more than two divisors.
2. Two positive integers, a and b , are said to be *relatively prime*, or *coprime*, if $\gcd(a, b) = 1$.
3.
 - a. The function $\pi(n)$ finds the number of primes smaller than or equal to n .
 - b. Euler's phi-function, $\phi(n)$, which is sometimes called the Euler's totient function, finds the number of integers that are both smaller than n and relatively prime to n .
4. The Sieve of Eratosthenes is a method to find all primes less than n . We write down all the integers between 2 and n . We cross out all integers divisible by 2 (except 2 itself). We cross out all integers divisible by 3 (except 3 itself). And so on. When we have crossed out all integers divisible by all primes less than $\sqrt{n}$, the remaining integers are primes.
5. We discussed two versions of Fermat's little theorem. The first version says that if p is a prime and a is an integer such that p does not divide a , then we have $a^{p-1} \equiv 1 \pmod{p}$. The second version removes the condition on a . It says that if p is a prime and a is an integer, then $a^p \equiv a \pmod{p}$. Two immediate applications of this theorem is to find solutions to exponentiation and multiplicative inverses when the modulus is a prime.
6. Euler's Theorem is a generalization of Fermat's little theorem. The modulus in the Fermat theorem is a prime, the modulus in Euler's theorem is an integer. We introduce two versions of this theorem. The first version says that if a and n are coprime, then $a^{\phi(n)} \equiv 1 \pmod{n}$. The second version says if $n = p \times q$, $a < n$, and k is an integer, then $a^{k \times \phi(n) + 1} \equiv a \pmod{n}$. Two immediate applications of this theorem is to find solutions to exponentiation and multiplicative inverses when the modulus is a composite but we can easily find the value of $\phi(n)$.

7.

- a. Mersenne defined the formula $M_p = 2^p - 1$ that was supposed to enumerate all primes. However, not all Mersenne numbers are primes.
 - b. Fermat defined the formula $F_n = 2^{2^n} + 1$ that was supposed to enumerate all primes. However, not all Fermat's numbers are primes.
8. A deterministic algorithm always gives a correct answer; a probabilistic algorithm gives an answer that is correct most of the time, but not all of the time. We mention two deterministic algorithms for primality testing: divisibility and AKS. We discussed three probability algorithms for primality testing: Fermat, square-root, and Miller-Rabin.
9. We mentioned the trial-division, Fermat, Polard $p - 1$, Polard rho, quadratic sieve, and number field sieve.
10. The Chinese remainder theorem (CRT) solves a set of congruent equations with one variable but different moduli, which are relatively prime. The Chinese remainder theorem has several applications in cryptography. One is to solve quadratic congruence. The other is to represent a very large integer in terms of a list of small integers.
11. A quadratic congruence is an equations of the form $a_2x^2 + a_1x + a_0 \equiv 0 \pmod{n}$. In this text, we have limited our discussion to equations of the form $x^2 \equiv a \pmod{n}$. In this equation a is called a quadratic residue (QR) if the equation has two solutions; a is called quadratic nonresidue (QNR) if the equation has no solutions.
12. The group $G = \langle \mathbb{Z}_p^*, \times \rangle$ has primitive roots. The primitive roots can be thought as the base of logarithm. Given $x = \log_g y$ for any element y in the set, there is another element x that is the log of y in base g . This type of logarithm is called discrete logarithm.

Exercises

13.

- a. The number of primes between 100,000 and 200,000 can be found as $\pi(200,000) - \pi(100,000)$. Using the upper and lower limits devised by Gauss and Lagrange, we have

$$\begin{array}{lll} 16385 < \pi(200,000) < 17985 & \rightarrow & \pi(200,000) \approx 17200 \\ 8688 < \pi(100,000) < 9587 & \rightarrow & \pi(100,000) \approx 9138 \\ \pi(200,000) - \pi(100,000) \approx & 17200 - 9138 \approx & 8062 \end{array}$$

- b. The number of composites between 100,000 and 200,000 is

$$100,000 - 8062 \approx 91938$$

- c. The ratio of primes to composites in the above range is $8062/91938$ or approximately 8.77 percent. This ratio for numbers between 1 to 10 (without considering 1 and 10) is 4/4 or 100 percent.

14.

- a. All of these numbers have the same largest prime factor, because

100	=	$(2 \times 5)^2$	=	$2^2 \times 5^2$	→	Largest factor is 5
1000	=	$(2 \times 5)^3$	=	$2^3 \times 5^3$	→	Largest factor is 5
10,000	=	$(2 \times 5)^4$	=	$2^4 \times 5^4$	→	Largest factor is 5
100,000	=	$(2 \times 5)^5$	=	$2^5 \times 5^5$	→	Largest factor is 5
1,000,000	=	$(2 \times 5)^6$	=	$2^6 \times 5^6$	→	Largest factor is 5

- b. However, when we add 1 to each integer, the largest prime factor changes unpredictably.

101	=	1×101	→	Largest factor is 101
1001	=	$7 \times 11 \times 13$	→	Largest factor is 13
10,001	=	73×137	→	Largest factor is 137
100,000	=	11×9091	→	Largest factor is 9091
1,000,000	=	101×9901	→	Largest factor is 9901

15. When an integer is divided by 4, the remainder is either 0, 1, 2, or 3. This means that an integer can be written as $(4k + 0)$, $(4k + 1)$, $(4k + 2)$, or $(4k + 3)$, in which k is the quotient. An integer in the form $(4k + 0)$ or $4k$ is not a prime because it is divisible by 4. An integer in the form $(4k + 2)$ can be a prime only if $k = 0$ (the integer is 2 and it is the first prime). The other two forms, $(4k + 1)$ and $(4k + 3)$, can represent a prime or a composite. This means that any prime can be either in the form of $(4k + 1)$ or $(4k + 3)$. However, this does not mean that any integer in one of these forms is a prime.

16. We show some primes for each form:

- a. $p = 5k + 1$:

$$k = 2 \rightarrow p = 11 \quad k = 6 \rightarrow p = 31 \quad k = 8 \rightarrow p = 41 \quad k = 10 \rightarrow p = 51$$

- b. $p = 5k + 2$:

$$k = 0 \rightarrow p = 2 \quad k = 1 \rightarrow p = 7 \quad k = 3 \rightarrow p = 17 \quad k = 7 \rightarrow p = 37$$

- c. $p = 5k + 3$:

$$k = 0 \rightarrow p = 3 \quad k = 2 \rightarrow p = 13 \quad k = 4 \rightarrow p = 23 \quad k = 8 \rightarrow p = 43$$

- d. $p = 5k + 4$:

$$k = 3 \rightarrow p = 19 \quad k = 5 \rightarrow p = 29 \quad k = 9 \rightarrow p = 49 \quad k = 11 \rightarrow p = 59$$

- 17.**
- a.** $\phi(29) = 29 - 1 = 28$ **(29 is a prime)**
 - b.** $\phi(32) = \phi(2^5) = 2^5 - 2^4 = 16$ **(2 is a prime)**
 - c.** $\phi(80) = \phi(2^4 \times 5^1) = (2^4 - 2^3) \times (5^1 - 5^0) = 8 \times 4 = 32$ **(2 and 5 are primes)**
 - d.** $\phi(100) = \phi(2^2 \times 5^2) = (2^2 - 2^1) \times (5^2 - 5^1) = 2 \times 20 = 40$ **(2 and 5 are primes)**
 - e.** $\phi(101) = 101 - 1 = 100$ **(101 is a prime)**

- 18.**
- a.** $(2^{24} - 1) = (2^{12} - 1) \times (2^{12} + 1)$. Because none of the factors is 1, $(2^{24} - 1)$ is a composite.
 - b.** $(2^{16} - 1) = (2^8 - 1) \times (2^8 + 1)$. Because none of the factors is 1, $(2^{16} - 1)$ is a composite.
 - c.** In general, if a positive integer can be written in the form $(2^n - 1)$ and n is an even integer greater than 2, then $(2^n - 1) = (2^{n/2} - 1) \times (2^{n/2} + 1)$. If $n = 2$, then we have $(2^n - 1) = 3$, a prime.

19. We have $(10 = 3 + 7)$, $(24 = 11 + 13)$, $(28 = 11 + 17)$, and $(100 = 11 + 89)$.

20. Some of these primes are shown below. We can always check the primeness using Appendix H.

$n = 1$	$\rightarrow$	$(n^2 + 1) = 2$	$n = 2$	$\rightarrow$	$(n^2 + 1) = 5$
$n = 4$	$\rightarrow$	$(n^2 + 1) = 17$	$n = 6$	$\rightarrow$	$(n^2 + 1) = 37$
$n = 10$	$\rightarrow$	$(n^2 + 1) = 101$	$n = 14$	$\rightarrow$	$(n^2 + 1) = 197$
$n = 16$	$\rightarrow$	$(n^2 + 1) = 257$	$n = 20$	$\rightarrow$	$(n^2 + 1) = 401$
$n = 24$	$\rightarrow$	$(n^2 + 1) = 577$	$n = 26$	$\rightarrow$	$(n^2 + 1) = 677$

21.

a.

$$\begin{aligned}(5^{15} \bmod 13) &= [(5^2 \bmod 13) \times (5^{13} \bmod 13)] \bmod 13 \\ &= [(-1 \bmod 13) \times (5 \bmod 13)] \bmod 13 = -5 \bmod 13 = \mathbf{8 \bmod 13}\end{aligned}$$

b.

$$\begin{aligned}(15^{18} \bmod 17) &= [(15 \bmod 17) \times (15^{17} \bmod 17)] \bmod 17 \\ &= [(-2 \bmod 17) \times (-2 \bmod 17)] \bmod 17 = \mathbf{4 \bmod 17}\end{aligned}$$

c.

$$(456^{17} \bmod 17) = (456 \bmod 17) = \mathbf{14 \bmod 17}$$

d.

$$\begin{aligned}(145^{102} \bmod 101) &= [(145^{101} \bmod 101) \times (145 \bmod 101)] \bmod 101 \\ &= [145 \times 145] \bmod 101 = [44 \times 44] \bmod 101 = 17 \bmod 101\end{aligned}$$

22. We know that if p is a prime, $x^{-1} \bmod p = x^{p-2} \bmod p$.

a.

$$5^{-1} \bmod 13 = 5^{13-2} \bmod 13 = 5^{11} \bmod 13 = \mathbf{8 \bmod 13}$$

$$15^{-1} \bmod 17 = 15^{17-2} \bmod 17 = 15^{15} \bmod 17 = \mathbf{8 \bmod 17}$$

c.

$$27^{-1} \bmod 41 = 27^{41-2} \bmod 41 = 27^{39} \bmod 41 = \mathbf{38 \bmod 41}$$

d.

$$70^{-1} \bmod 101 = 70^{101-2} \bmod 101 = 70^{99} \bmod 101 = \mathbf{13 \bmod 101}$$

$$15^{-1} \bmod 17 = 15^{17-2} \bmod 17 = 15^{15} \bmod 17 = \mathbf{8 \bmod 17}$$

c.

$$27^{-1} \bmod 41 = 27^{41-2} \bmod 41 = 27^{39} \bmod 41 = \mathbf{38 \bmod 41}$$

d.

$$70^{-1} \bmod 101 = 70^{101-2} \bmod 101 = 70^{99} \bmod 101 = \mathbf{13 \bmod 101}$$

23. We know that if n is an integer, $x^{-1} \bmod n = x^{\phi(n)-1} \bmod n$.

a.

$$12^{-1} \bmod 77 = 12^{\phi(77)-1} \bmod 77 = 12^{59} \bmod 77 = \mathbf{45 \bmod 77}$$

b.

$$16^{-1} \bmod 323 = 16^{\phi(323)-1} \bmod 323 = 16^{287} \bmod 323 = \mathbf{101 \bmod 323}$$

c.

$$20^{-1} \bmod 403 = 20^{\phi(403)-1} \bmod 403 = 20^{359} \bmod 403 = \mathbf{262 \bmod 403}$$

d.

$$44^{-1} \bmod 667 = 44^{\phi(667)-1} \bmod 667 = 44^{615} \bmod 667 = \mathbf{379 \bmod 667}$$

ط

24. For each Mersenne number, $M_p = 2^p - 1$, we try some integers in the form $2kp + 1$ to find a possible divisor.

- a. $M_{23} = 2^{23} - 1 = 8,388,607$ is not a prime. When $k = 2$, $2kp + 1 = 47$ divides the number: $8,388,607 = 47 \times 178,481$. **M_{23} is a composite**
- b. $M_{29} = 2^{29} - 1 = 536,870,911$ is not a prime. When $k = 4$, $2kp + 1 = 233$ divides the number: $536,870,911 = 233 \times 2,304,167$. **M_{29} is a composite**
- c. $M_{31} = 2^{31} - 1 = 2,147,483,647$ is a prime. If this number is a composite, it must have a divisor less than 46,341 (the square root of M_{31}), which means that k in $2kp + 1$ must be less than 748. We tried all $k = 0$ to 747 with no success. **M_{31} is a prime**

25. It can be checked that if $2^n - 1$ is a prime, then n is a prime. However, there are some values of n for which $2^n - 1$ is a composite, but n is a prime ($n = 11$, for example). In other words, if n is a prime, $2^n - 1$ may or may not be a prime; if $2^n - 1$ is a prime, then n is a prime. This is to say that not all Mersenne numbers are primes. Since Mersenne's idea cannot be used for primality test, the fact stated in this problem cannot be used for primality test.

$2^2 - 1 = 3$ is a prime	→	$n = 2$ is a prime
$2^3 - 1 = 7$ is a prime	→	$n = 3$ is a prime
$2^4 - 1 = 15 = 3 \times 5$ is a composite	→	$n = 4$ is a composite
$2^5 - 1 = 31$ is a prime	→	$n = 5$ is a prime

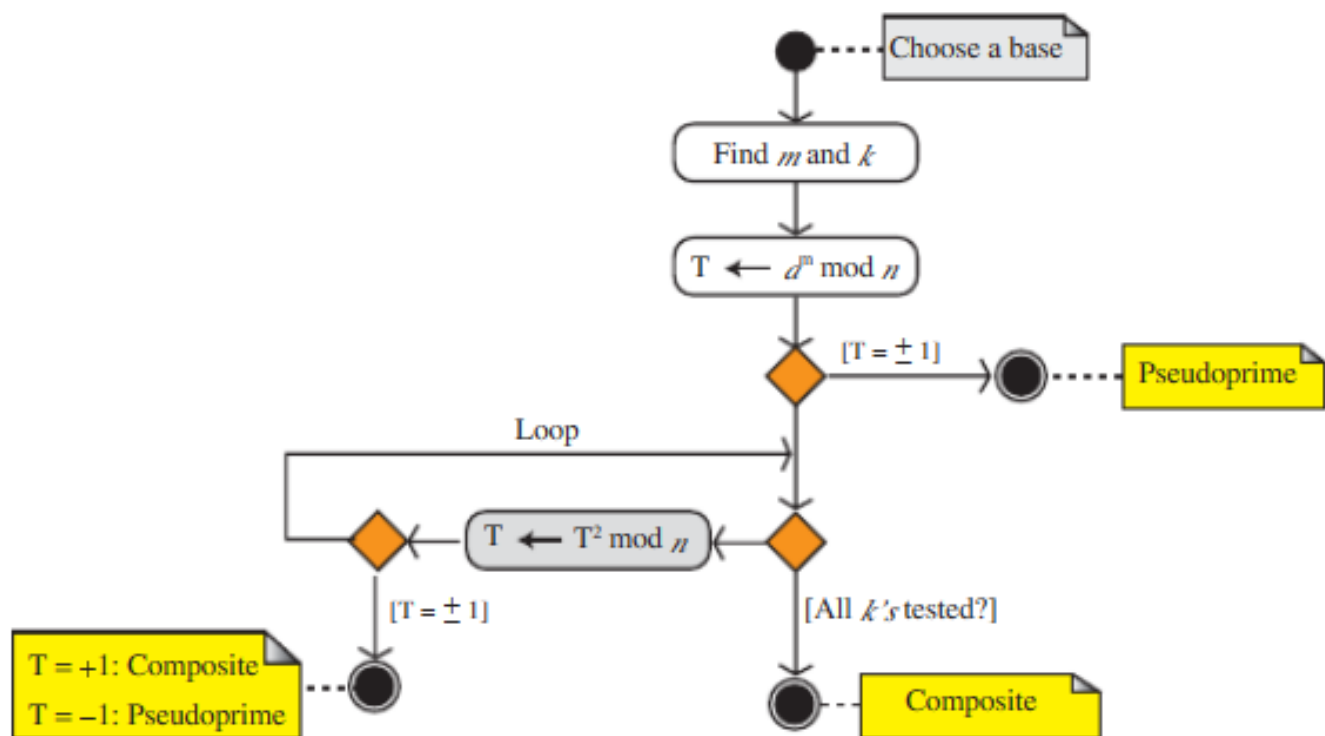
$2^6 - 1 = 63 = 3 \times 5$ is a composite	→	$n = 6$ is a composite
$2^7 - 1 = 127$ is a prime	→	$n = 7$ is a prime
$2^8 - 1 = 255 = 5 \times 51$ is a composite	→	$n = 8$ is a composite
$2^9 - 1 = 511 = 7 \times 73$ is a composite	→	$n = 9$ is a composite
$2^{10} - 1 = 1023 = 3 \times 341$ is a composite	→	$n = 10$ is a composite
$2^{11} - 1 = 2047 = 23 \times 89$ is a composite	→	$n = 11$ is a prime

26. The following shows the results of the Fermat test on this group of integers. Note that if the integer does not pass the test, it is definitely a composite; if it passes the test, it may be a prime. The last two integers pass the test, but we know that they are composite.

$n = 100$	→	$2^{n-1} \bmod n = 88$ (not passed)	→	composite
$n = 110$	→	$2^{n-1} \bmod n = 72$ (not passed)	→	composite
$n = 130$	→	$2^{n-1} \bmod n = 88$ (not passed)	→	composite
$n = 150$	→	$2^{n-1} \bmod n = 88$ (not passed)	→	composite
$n = 200$	→	$2^{n-1} \bmod n = 88$ (not passed)	→	composite
$n = 250$	→	$2^{n-1} \bmod n = 62$ (not passed)	→	composite
$n = 271$	→	$2^{n-1} \bmod n = 1$ (passed)	→	prime
$n = 341$	→	$2^{n-1} \bmod n = 1$ (passed)	→	composite
$n = 561$	→	$2^{n-1} \bmod n = 1$ (passed)	→	composite

27. The flow in the Miller-Rabin algorithm may be better understood using the chart in Figure S9.27. We follow the chart in each case.

Figure S9.27 *Solution to Exercise 27*



a. $n = 100 \rightarrow 100 - 1 = 99 \times 2^0 \rightarrow m = 99$ and $k = 0$.

Pre-loop → $T = 2^{99} \bmod 100 = 88$

Loop is by-passed because $k = 0 \rightarrow$ **Composite** (100 is an even integer)

b. $n = 109 \rightarrow 109 - 1 = 27 \times 2^2 \rightarrow m = 27$ and $k = 2$.

Pre-loop → $T = 2^{27} \bmod 109 = 33$

$k = 1 \rightarrow T = T^2 \bmod 109 = 108 \bmod 109 = (-1) \bmod 109$

Loop is broken because $T = -1 \rightarrow$ **Pseudoprime** (109 is actually a prime)

c. $n = 201 \rightarrow 201 - 1 = 25 \times 2^3 \rightarrow m = 25$ and $k = 3$.

Pre-loop → $T = 2^{25} \bmod 201 = 95$

$k = 1 \rightarrow T = T^2 \bmod 201 = 181 \bmod 201$

$k = 2 \rightarrow T = T^2 \bmod 201 = 199 \bmod 201$

Loop is terminated → **Composite** ($201 = 3 \times 67$)

d. $n = 271 \rightarrow 271 - 1 = 135 \times 2^1 \rightarrow m = 135$ and $k = 1$.

Pre-loop → $T = 2^{135} \bmod 271 = 1 \bmod 271$

$T = +1$ in the initialization step → **Pseudoprime** (271 is actually a prime)

e. $n = 341 \rightarrow 341 - 1 = 85 \times 2^2 \rightarrow m = 85$ and $k = 2$.

Pre-loop → $T = 2^{85} \bmod 341 = 32$

$k = 1 \rightarrow T = T^2 \bmod 341 = 1 \bmod 341$

Loop is broken because $T = +1 \rightarrow$ **Composite** ($341 = 11 \times 31$)

f. $n = 349 \rightarrow 349 - 1 = 87 \times 2^2 \rightarrow m = 87$ and $k = 2$.

Pre-loop → $T = 2^{87} \bmod 349 = 213$

$k = 1 \rightarrow T = T^2 \bmod 349 = 348 \bmod 349 = (-1) \bmod 349$

Loop is broken because $T = -1 \rightarrow$ **Pseudoprime** (349 is actually a prime)

g. $n = 2047 \rightarrow 2047 - 1 = 1023 \times 2^1 \rightarrow m = 1023$ and $k = 1$.

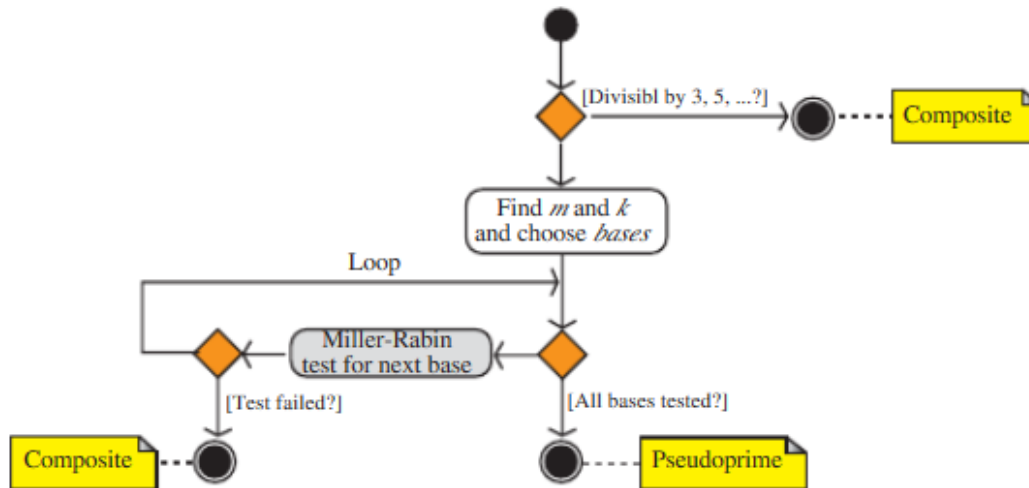
Pre-loop → $T = 2^{1023} \bmod 2047 = 1 \bmod 2047$

$T = +1$ in the initialization step → **Pseudoprime** (but $2047 = 23 \times 89$)

In this case, the test declares the integer 2047 as a pseudoprime, which is actually a composite.

- 28.** We use the chart in Figure S9.28 to follow the recommended primality test that include several instances of Miller-Rabin test, each with a different base. For each number we use the base set (2, 3, 4).

Figure S9.28 *Solution to Exercise 28*



- a. $n = 271$ is not divisible by 3, 5, 7, 11, 13, 17, 19, 23. We start Miller-Rabin tests. The tests tells us that 271 is a pseudoprime; it is in fact a prime.

Initialization: $271 - 1 = 135 \times 2^1 \rightarrow m = 135$ and $k = 1$		
$a = 2$	$\rightarrow$	$T = a^{135} \bmod 271 = 1$
$a = 3$	$\rightarrow$	$T = a^{135} \bmod 271 = -1$
$a = 4$	$\rightarrow$	$T = a^{135} \bmod 271 = 1$
The number passes three Miller-Rabin tests $\rightarrow$ Pseudoprime		

- b.** $n = 3149$ is not divisible by 3, 5, 7, 11, 13, 17, 19, 23. We start Miller-Rabin tests. This integer fails the test; it is definitely a composite ($3149 = 47 \times 67$).

Initialization: $3149 - 1 = 787 \times 2^2 \rightarrow m = 787$ and $k = 2$		
$a = 2$	$\rightarrow$	$T = a^{787} \bmod 3149 = 2523 \quad T = T^2 \bmod 3149 = 140$
The number fails the Miller-Rabin test for $a = 2 \rightarrow$ Composite		

- c.** $n = 9673$ is not divisible by 3, 5, 7, 11, 13, but is divisible by 17. It is **composite** and no Miller-Rabin tests are needed ($9673 = 17 \times 569$).

29.

- a.** We test the claim using $(3 - 2)^p \bmod p = (3^p - 2) \bmod p$ with $x = 3$, $a = 2$, and some small primes.

$p = 2$	$(3 - 2)^2 \bmod 2 = 1$	$(3^2 - 2) \bmod 2 = 1$
$p = 3$	$(3 - 2)^3 \bmod 3 = 1$	$(3^3 - 2) \bmod 3 = 1$
$p = 7$	$(3 - 2)^5 \bmod 7 = 1$	$(3^7 - 2) \bmod 7 = 1$

- b.** We also test the claim using $x = 7$, $a = 3$, and some primes.

- b. $n = 3149$ is not divisible by 3, 5, 7, 11, 13, 17, 19, 23. We start Miller-Rabin tests. This integer fails the test; it is definitely a composite ($3149 = 47 \times 67$).

Initialization: $3149 - 1 = 787 \times 2^2 \rightarrow m = 787$ and $k = 2$		
$a = 2$	$\rightarrow$	$T = a^{787} \bmod 3149 = 2523 \quad T = T^2 \bmod 3149 = 140$
The number fails the Miller-Rabin test for $a = 2 \rightarrow$ Composite		

- c. $n = 9673$ is not divisible by 3, 5, 7, 11, 13, but is divisible by 17. It is **composite** and no Miller-Rabin tests are needed ($9673 = 17 \times 569$).

29.

- a. We test the claim using $(3 - 2)^p \bmod p = (3^p - 2) \bmod p$ with $x = 3$, $a = 2$, and some small primes.

$p = 2$	$(3 - 2)^2 \bmod 2 = 1$	$(3^2 - 2) \bmod 2 = 1$
$p = 3$	$(3 - 2)^3 \bmod 3 = 1$	$(3^3 - 2) \bmod 3 = 1$
$p = 7$	$(3 - 2)^5 \bmod 7 = 1$	$(3^7 - 2) \bmod 7 = 1$

- b. We also test the claim using $x = 7$, $a = 3$, and some primes.

$p = 2$	$(7 - 3)^2 \bmod 2 = 0$	$(7^2 - 3) \bmod 2 = 0$
$p = 5$	$(7 - 3)^5 \bmod 5 = 4$	$(7^5 - 3) \bmod 5 = 4$
$p = 17$	$(7 - 3)^{17} \bmod 17 = 4$	$(7^{17} - 3) \bmod 17 = 4$

30. Generally, $p_n > n \times \ln n$. The following shows some primes and their approximations. As n becomes larger, the ratio of error becomes smaller.

$n = 1$	$p_n = 2$	$n \times \ln n = 0$
$n = 25$	$p_n = 97$	$n \times \ln n = 80.47$
$n = 168$	$p_n = 997$	$n \times \ln n = 860.80$
$n = 668$	$p_n = 4999$	$n \times \ln n = 4344.86$
$n = 10,000$	$p_n = 104,729$	$n \times \ln n = 92103.40$

31.

a.

$$\begin{array}{lcl}
 a_1 = 2 & m_1 = 7 & a_2 = 3 \quad m_2 = 9 \quad \rightarrow \quad M = 63 \\
 M_1 = 9 & M_1^{-1} = 9^{-1} \bmod 7 = 4 & ; \quad M_2 = 7 \quad M_2^{-1} = 7^{-1} \bmod 9 = 4 \\
 & & x = (2 \times 9 \times 4 + 3 \times 7 \times 4) \bmod 63 = 30
 \end{array}$$

b.

$$\begin{array}{lcl}
 a_1 = 4 & m_1 = 5 & a_2 = 10 \quad m_2 = 11 \quad \rightarrow \quad M = 55 \\
 M_1 = 11 & M_1^{-1} = 11^{-1} \bmod 5 = 1 & ; \quad M_2 = 5 \quad M_2^{-1} = 5^{-1} \bmod 11 = 9 \\
 & & x = (4 \times 11 \times 1 + 10 \times 5 \times 9) \bmod 55 = 54
 \end{array}$$

c.

$$\begin{array}{lcl}
 a_1 = 7 & m_1 = 13 & a_2 = 11 \quad m_2 = 12 \quad \rightarrow \quad M = 156 \quad M_1 = 12 \quad M_2 = 13 \\
 M_1 = 12 & M_1^{-1} = 12^{-1} \bmod 13 = 12 & ; \quad M_2 = 13 \quad M_2^{-1} = 13^{-1} \bmod 12 = 1 \\
 & & x = (7 \times 12 \times 12 + 11 \times 13 \times 1) \bmod 156 = 59
 \end{array}$$

32. The following show QRs and QNRs in each case.

a. QRs and QNRs in $\mathbf{Z}_{13}^*$

$$\text{QRs: } 1, 3, 4, 9, 10, 12 \quad \text{QNRs: } 2, 5, 6, 7, 8, 11$$

b. QRs and QNRs in $\mathbf{Z}_{17}^*$

$$\text{QRs: } 1, 2, 4, 8, 9, 13, 15, 16 \quad \text{QNRs: } 3, 5, 6, 7, 10, 11, 12, 14$$

c. QRs and QNRs in $\mathbf{Z}_{23}^*$

$$\text{QRs: } 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18 \quad \text{QNRs: } 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22$$

33.

- a. The integer 4 is a QR in $\mathbf{Z}_7^*$. Since $7 = 4 \times k + 3$ with $k = 1$, we can use the following expressions to find the solutions.

$$x: 4^{(7+1)/4} \bmod 7 = 2$$

$$x: -4^{(7+1)/4} \bmod 7 = -2$$

- b. The integer 5 is a QR in $\mathbf{Z}_{11}^*$. Since $11 = 4 \times k + 3$ with $k = 2$, we can use the following expressions to find the two solutions:

$$x: 5^{(11+1)/4} \bmod 11 = 4$$

$$x: -5^{(11+1)/4} \bmod 11 = -4$$

- c. The integer 7 is not a QR in $\mathbf{Z}_{13}^*$ (see Exercise 32). **This equation has no solutions.**
- d. The integer 12 is not a QR in $\mathbf{Z}_{17}^*$ (see Exercise 32). **This equation has no solutions.**

14.

- a. $n = 14 = 2 \times 7 \rightarrow p_1 = 2$ and $p_2 = 7$. The four new equations are

$$x^2 \equiv 4 \pmod{2} \rightarrow x \equiv \pm 0 \pmod{2}$$

$$x^2 \equiv 4 \pmod{7} \rightarrow x \equiv \pm 2 \pmod{7}$$

We have four sets of equations: The solution gives us $x = 2$ and $x = 12$.

Set 1: $x \equiv + 0 \pmod{2}$

$x \equiv + 2 \pmod{7}$

Set 2: $x \equiv + 0 \pmod{2}$

$x \equiv - 2 \pmod{7}$

Set 3: $x \equiv - 0 \pmod{2}$

$x \equiv + 2 \pmod{7}$

Set 4: $x \equiv - 0 \pmod{2}$

$x \equiv - 2 \pmod{7}$

- b. $n = 10 = 2 \times 5 \rightarrow p_1 = 2$ and $p_2 = 5$. The four new equations are

$$x^2 \equiv 1 \pmod{2} \rightarrow x \equiv \pm 1 \pmod{2}$$

$$x^2 \equiv 0 \pmod{5} \rightarrow x \equiv \pm 0 \pmod{5}$$

$$x^2 \equiv 1 \pmod{2} \rightarrow x \equiv \pm 1 \pmod{2}$$

$$x^2 \equiv 0 \pmod{5} \rightarrow x \equiv \pm 0 \pmod{5}$$

We have four sets of equations: The solution gives us $x = 5$.

Set 1: $x \equiv + 1 \pmod{2}$

$x \equiv + 0 \pmod{5}$

Set 2: $x \equiv + 1 \pmod{2}$

$x \equiv - 0 \pmod{5}$

Set 3: $x \equiv - 1 \pmod{2}$

$x \equiv + 0 \pmod{5}$

Set 4: $x \equiv - 1 \pmod{2}$

$x \equiv - 0 \pmod{5}$

- c. $n = 33 = 3 \times 11 \rightarrow p_1 = 3$ and $p_2 = 11$.

$$x^2 \equiv 1 \pmod{3} \rightarrow x \equiv \pm 1 \pmod{3} \quad x^2 \equiv 7 \pmod{11} \rightarrow \text{no solutions}$$

Since the second equation has no solution, the equation $x^2 \equiv 7 \pmod{33}$ has no solution.

- d. $n = 34 = 2 \times 17 \rightarrow p_1 = 2$ and $p_2 = 17$. The four new equations are

$$x^2 \equiv 12 \pmod{2} \rightarrow x \equiv \pm 0 \pmod{2} \quad x^2 \equiv 12 \pmod{17} \rightarrow \text{No solutions}$$

Since the second equation has no solution, the equation $x^2 \equiv 12 \pmod{34}$ has no solution.

35. We use tables based on Figure 9.7. We first calculate all powers of a 's.

- a. $y = 21^{24} \pmod{8} \rightarrow a = 21, x = 24 = 11000_2$. Shaded areas represent no multiplications. All calculations are in modulo 8. The answer is $y = 1$.

a^i s	x_i	$y = 1 \pmod{8}$
$a^1 = 5 \pmod{8}$	0	$y = 1 \pmod{8}$
$a^2 = 1 \pmod{8}$	0	$y = 1 \pmod{8}$
$a^4 = 1 \pmod{8}$	0	$y = 1 \pmod{8}$
$a^8 = 1 \pmod{8}$	1	$y = 1 \times 1 \pmod{8} = 1 \pmod{8}$
$a^{16} = 1 \pmod{8}$	1	$y = 1 \times 1 \pmod{8} = 1 \pmod{8}$

The table shows that we can stop whenever a^{x_i} becomes 1.

- b. $y = 320^{23} \pmod{461} \rightarrow a = 320, x = 23 = 10111_2$. Shaded areas represent no multiplications. All calculations are in modulo 461. The answer is $y = 373$.

a^i s	x_i	$y = 1 \pmod{461}$
$a^1 = 320 \pmod{461}$	1	$y = 1 \times 320 \pmod{461} = 320 \pmod{461}$
$a^2 = 58 \pmod{461}$	1	$y = 320 \times 58 \pmod{461} = 120 \pmod{461}$
$a^4 = 137 \pmod{461}$	1	$y = 120 \times 137 \pmod{461} = 305 \pmod{461}$
$a^8 = 329 \pmod{461}$	0	$y = 305 \pmod{461}$
$a^{16} = 367 \pmod{461}$	1	$y = 305 \times 367 \pmod{461} = 373 \pmod{461}$

- c. $y = 1776^{41} \pmod{2134} \rightarrow a = 1776, x = 41 = 101001_2$. Shaded areas represent no multiplications. All calculations are in modulo 2134. The answer is $y = 698$.

a^s	x_i	$y = 1 \bmod 2134$
$a^1 = 1776 \bmod 2134$	1	$y = 1 \times 1776 \bmod 2134 = 1776 \bmod 2134$
$a^2 = 124 \bmod 2134$	0	$y = 1776 \bmod 2134$
$a^4 = 438 \bmod 2134$	0	$y = 1776 \bmod 2134$
$a^8 = 1918 \bmod 2134$	1	$y = 1776 \times 1918 \bmod 2134 = 504 \bmod 2134$
$a^{16} = 1842 \bmod 2134$	0	$y = 504 \bmod 2134$
$a^{32} = 2038 \bmod 2134$	1	$y = 504 \times 2038 \bmod 2134 = \mathbf{698} \bmod 2134$

- d. $y = 2001^{35} \bmod 2000 \rightarrow a = 2001, x = 35 = 100011_2$. Shaded areas represent no multiplications. All calculations are in modulo 2001. The answer is **$y = 1$** .

a^s	x_i	$y = 1 \bmod 2000$
$a^1 = 1 \bmod 2000$	1	$y = 1 \times 1 \bmod 2000 = 1 \bmod 2000$
$a^2 = 1 \bmod 2000$	1	$y = 1 \times 1 \bmod 2000 = 1 \bmod 2000$
$a^4 = 1 \bmod 2000$	0	$y = 1 \bmod 2000$
$a^8 = 1 \bmod 2000$	0	$y = 1 \bmod 2000$
$a^{16} = 1 \bmod 2000$	0	$y = 1 \bmod 2000$
$a^{32} = 1 \bmod 2000$	1	$y = 1 \times 1 \bmod 2000 = \mathbf{1} \bmod 2000$

The table shows that we can stop whenever a^{x_i} becomes 1.

36.

- a. The order of the group is $\phi(19) = 18$.
- b. The following shows the order of each element:

ord (1)= 1 ord(2)= 18 ord (3)= 18 ord (4)= 9 ord (5)= 9 ord (6)= 9
ord (7)= 3 ord(8)= 6 ord (9)= 9 ord (10)= 18 ord (11)= 3 ord (12)= 6
ord (13)= 18 ord(14)= 18 ord (15)= 18 ord (16)= 9 ord (17)= 9 ord (18)= 2

- c. The number of primitive roots is $\phi(\phi(19)) = \phi(18) = 6$.

- d. The primitive roots are those element with order 18. They are **2, 3, 10, 13, 14**, and **15**.
- e. We know that the group is cyclic because 19 is a prime. Any of the primitive root can generate all elements of the group. For example, if we choose $g = 2$ as the generator, we can generate all elements as shown below (all calculations are in modulo 19).

$g^1 \rightarrow 2$	$g^2 \rightarrow 4$	$g^3 \rightarrow 8$	$g^4 \rightarrow 16$	$g^5 \rightarrow 13$	$g^6 \rightarrow 7$
$g^7 \rightarrow 14$	$g^8 \rightarrow 9$	$g^9 \rightarrow 18$	$g^{10} \rightarrow 17$	$g^{11} \rightarrow 15$	$g^{12} \rightarrow 11$
$g^{13} \rightarrow 3$	$g^{14} \rightarrow 6$	$g^{15} \rightarrow 12$	$g^{16} \rightarrow 5$	$g^{17} \rightarrow 10$	$g^{18} \rightarrow 1$

- f. We can create a table of discrete logarithms for bases **2, 3, 10, 13, 14**, and **15**.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$L_2(x)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9
$L_3(x)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9
$L_{10}(x)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9
$L_{13}(x)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9
$L_{14}(x)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9
$L_{15}(x)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

37.

- a. To solve the equation $x^5 \equiv 11 \pmod{17}$, we need to find a primitive root in the group $G = \langle \mathbf{Z}_{17}^*, \times \rangle$ and the discrete logarithm table for that root. The first primitive root in this group is 3 (primitive roots are 3, 5, 6, 7, 10, 11, 12, and 14). The discrete logarithm table for this root (base) can be found as

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$L_3(x)$	16	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

We then apply the function L_3 to both sides of the congruence. Note that the working modulus is $\phi(17) = 16$ and $L_3(11) = 7$ (from the table).

$$L_3(x^5) \equiv L_3(11) \pmod{16} \rightarrow 5 \times L_3(x) \equiv 7 \pmod{16} \rightarrow 5 \times L_3(x) \equiv 7 \pmod{16}$$

Now we need to solve the congruence equation $5 \times L_3(x) \equiv 7 \pmod{16}$. Recall from Chapter 2 that this equation has only one solution because $\gcd(5, 16) = 1$.

$$L_3(x) \equiv 5^{-1} \times 7 \pmod{16} \equiv 11 \pmod{16}$$

Now we can use the table to find x if $L_3(x) = 11$; the answer is $x = 7$, which can be checked as $7^5 \equiv 11 \pmod{17}$. We can also write a program to test all of values of x from 1 to 17 to see if any of this values satisfies the equation. We did so; the only value is $x = 7$.

- b. To solve the equation $2x^{11} \equiv 22 \pmod{19}$ or $2x^{11} \equiv 3 \pmod{19}$, we need to find a primitive root in the group $G = \langle \mathbf{Z}_{19}^*, \times \rangle$ and the discrete logarithm table for that root. The first primitive root in this group is 2 (see Exercise 36). The discrete logarithm table for this root (base) can be found as

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$L_2(x)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

We then apply the function L_2 to both sides of the congruence. Note that the working modulus is $\phi(19) = 18$, $L_2(2) = 1$ and $L_2(3) = 13$.

$$\begin{aligned} L_2(2x^{11}) &\equiv L_2(3) \pmod{18} \rightarrow L_2(2) + 11 \times L_2(x) \equiv L_2(3) \pmod{18} \\ &\rightarrow 1 + 11 \times L_2(x) \equiv 13 \pmod{18} \rightarrow 11 \times L_2(x) \equiv 12 \pmod{18} \end{aligned}$$

Now we need to solve the congruence equation $11 \times y \equiv 12 \pmod{18}$. Recall from Chapter 2 that this equation has only one solution because $\gcd(11, 18) = 1$.

$$11 \times y \equiv 12 \pmod{18} \rightarrow y \equiv 11^{-1} \times 12 \pmod{18} \equiv 5 \times 12 \pmod{18} \equiv 6 \pmod{18}$$

Now we can use the table to find x if $L_2(x) = 6$; the answer is $x = 7$, which can be checked as $2 \times 7^{11} \equiv 3 \pmod{19}$. We can also write a program to test all of values of x from 1 to 19 to see if any of this values satisfies the equation. We did so; the only value is $x = 7$.

- c. The equation $5x^{12} + 6x \equiv 8 \pmod{23}$ cannot be solved using the discrete logarithm discussed in this chapter because there is no property of discrete logarithm that allows us to extract $L(x)$ from $L(5x^{12} + 6x)$. However, we can write a program to test all of values of x from 1 to 22 to see if any of these values satisfies the equation. We did so, but find no value of x satisfying the congruence; the congruence has no solution.

38. One million operations per second means 3,600,000,000 operations per hour.

- a. If we assume that the complexity of divisibility test is 2^{n_b} (which is very unrealistic), then

$$2^{n_b} = 3,600,000,000 \rightarrow 2^{n_b} \approx 2^{32} \quad n_b \approx 32$$

This means $n < 2^{32}$

- b. The complexity of ASK is $(\log_2 n_b)^{12}$.

$$(\log_2 n_b)^{12} = 3,600,000,000 \rightarrow \log_2 n_b = 6.25 \rightarrow n_b \approx 2^{6.25} \rightarrow n_b \approx 76$$

This means $n < 2^{76}$

- c. The complexity of Fermat is n_b if we use Fast Exponentiation algorithm.

$$n_b = 3,600,000,000$$

This means $n < 2^{3,600,000,000}$

However, as we know the algorithm is probabilistic. We are not sure if the result is correct.

- d. The complexity of square root test is n or 2^{n_b}

$$2^{n_b} = 3,600,000,000 \rightarrow 2^{n_b} \approx 2^{32} \quad n_b \approx 32$$

This means $n < 2^{32}$

However the test is not deterministic. We are not sure if the result is correct.

- e. The main operation in Miller-Rabin test is Fermat test, so the complexity is somehow more than Fermat. However, the test is not deterministic.

39. One million operations per second means 3,600,000,000 operations per hour.

- a. The complexity of trial division method is exponential (2^{n_b}).

$$2^{n_b} = 3,600,000,000 \rightarrow 2^{n_b} \approx 2^{32} \quad n_b \approx 32$$

This means $n < 2^{32}$

- b. The complexity of Fermat method is subexponential or $2^{(\log_2 n_b)^2}$. For simplicity, we assume the complexity to be $2^{(\log_2 n_b)^2}$.

$$2^{(\log_2 n_b)^2} = 3,600,000,000 \rightarrow 2^{(\log_2 n_b)^2} \approx 2^{32} \rightarrow (\log_2 n_b)^2 \approx 32 \\ \rightarrow (\log_2 n_b) \approx 5.7 \rightarrow n_b \approx 2^{5.7} \rightarrow 52$$

This means $n < 2^{52}$

- c. The complexity of Pollard rho method is exponential or $(2^{n_b/4})$.

$$2^{n_b/4} = 3,600,000,000 \rightarrow 2^{n_b/4} \approx 2^{32} \quad n_b \approx 128$$

This means $n < 2^{128}$

- d. The complexity here is e^C where $C = (\ln n \ln \ln n)^{1/2}$. Since it is very difficult to calculate n in this case, we assume that $C = \ln n)^{1/2}$ or $C = (\ln n)$.

$$e^{\ln n} = 3,600,000,000 \rightarrow \ln n = 3,600,000,000$$

This means $n < e^{3,600,000,000}$

- e. The complexity here is e^C where $C = 2(\ln n)^{1/3}(\ln \ln n)^{2/3}$. Since it is very difficult to calculate n in this case, we assume that $C = 2(\ln n)^{1/3}(\ln n)^{2/3} = 2(\ln n)$

$$e^{2 \ln n} = 3,600,000,000 \rightarrow \ln n = 1,800,000,000$$

This means $n < e^{1,800,000,000}$

40.

Square_and_Multiply(a, x, n)

```
{
    y ← 1
    for (i=0 to  $n_b-1$ )
    {
        if ( $a = 1$ )
            return y                // no need to continue
        if ( $x_i = 1$ )
            y ←  $y \times a \bmod n$ 
        a ←  $a^2 \bmod n$ 
    }
    return y
}
```

41.

Square_and_Multiply(a, x, n)

```
{
    y ← 1
    for (i= $n_b-1$  downto 0)
    {
        a ←  $a^2 \bmod n$ 
        if ( $x_i = 1$ )
            y ←  $y \times a \bmod n$ 
    }
}
```

```

    return  $y$ 
}

```

42.

Square_and_Multiply(a, x, n)

```

{
     $y \leftarrow 1$ 
    while ( $x > 0$ )
    {
        if ( $x \bmod 2 = 1$ )
             $y \leftarrow y \times a \bmod n$            // not needed in the last round
         $a \leftarrow a^2 \bmod n$ 
         $x \leftarrow x/2$                          // integer division
    }
    return  $y$ 
}

```

43.

```

FermatPrimalityTest( $a, n$ )           // We can use different bases
{
     $y \leftarrow \text{Square\_and\_Multiply}(a, n-1, n)$    // See Algorithm 9.7 in the text
    if ( $y = 1$ )
        return ( $n$  is probably a prime)
    return ( $n$  is a composite)
}

```

44.

SquareRootPrimalityTest(n)

```

{
    for ( $a = 2$  to  $n/2 + 1$ )           //  $n$  is normally odd
    {
         $x \leftarrow a^2 \bmod n$ 
         $y \leftarrow (-a)^2 \bmod n$ 
        if ( $x = 1 \bmod n$ ) or ( $y = 1 \bmod n$ )
            return ( $n$  is a composite)
    }
    return ( $n$  is probably a prime)
}

```

45.

ChineseRemainderTheorem($k, a[1 \dots k], m[1 \dots k]$)

```
{
    M ← 1
    for (i = 1 to k)
        M ← M × m[i]
    for (i = 1 to k)
    {
        M[i] ← M / m[i]
        InvM[i] ← M[i]-1 mod m[i]
    }
    x ← 0
    for (i = 1 to k)
        x ← [x + (a[i] × M[i] × InvM[i])] mod M
    return x
}
```

46.

```
FindQuadraticResidues(p)           // p is a prime
{
    for (a = 2 to n/2 + 1)           // n is normally odd
    {
        x ← Square_and_Multiply(a, (p - 1)/2, p)
        if (x = 1 mod p)
            insert a in QRList
        else
            insert a in QNRList
    }
    return QRList and QNRList
}
```

47.

```
FindFirstPrimitiveRoot(p)           // p is a prime
{
    for (a = 2 to p - 1)
    {
        i ← 1
        while (ai mod p ≠ 1)
        {
            i ← i + 1
        }
        if (i = p - 1)                 // order a = φ(p)
            return a
    }
}
```

48.

```

FindAllPrimitiveRoots( $p$ )                                //  $p$  is a prime
{
    for ( $a = 2$  to  $p-1$ )
    {
         $i \leftarrow 1$ 
        while ( $a^i \bmod p \neq 1$ )
        {
             $i \leftarrow i + 1$ 
        }
        if ( $i = p-1$ )                                     // order  $a = \phi(p)$ 
            Insert  $a$  to PrimitiveRootList
    }
    return PrimitiveRootList
}

```

49.

```

FindAllDiscreteLogs( $p$ )                                //  $p$  is a prime
{
    PrimitiveRootList  $\leftarrow$  FindAllPrimitiveRoots( $p$ )    // See Exercise 48
    Create a DiscreteLogTable sorted on  $y$ 
    for (each  $g$  in PrimitiveRootList)
    {
        for ( $x = 1$  to  $p-1$ )
        {
             $y \leftarrow g^x \bmod p$ 
            insert  $x$  to  $L_g$  row of DiscreteLogTable under  $y$  column
        }
    }
    return DiscreteLogTable
}

```