CHAPTER 9

Mathematics of Cryptography: Part 3

(Solution to Old-Numbered Problems)

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.

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.

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 $\boldsymbol{a^{p-1} \equiv 1 \pmod{p}}$. The second Version removes the condition on a. It says that if p is a prime and a is an integer, then $\boldsymbol{a^p \equiv a \pmod{p}}$. Two immediate applications of this theorem is to find solutions to exponentiation and multiplicative inverses when the modulus is a prime.

7.

a. Mersenne defined the formula $\boldsymbol{M_p = 2^p - 1}$ that was supposed to enumerate all primes. However, not all Mersenne numbers are primes.

b. Fermat defined the formula $\boldsymbol{F_n = 2^{2^n} + 1}$ that was supposed to enumerate all primes. However, not all Fermat's numbers are primes.

9. We mentioned the trial-division, Fermat, Polard $p - 1$, Polard rho, quadratic sieve, and number field sieve.

11. A quadratic congruence is an equations of the form $\boldsymbol{a_2x^2 + a_1x + a_0 \equiv 0 \pmod{n}}$. In this text, we have limited our discussion to equations of the form $\boldsymbol{x^2 \equiv a \pmod{n}}$. 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.

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

$$16385 < \pi(200{,}000) < 17985 \quad \rightarrow \quad \pi(200{,}000) \approx 17200$$
$$8688 < \pi(100{,}000) < 9587 \quad \rightarrow \quad \pi(100{,}000) \approx 9138$$
$$\pi(200{,}000) - \pi(100{,}000) \approx 17200 - 9138 \approx 8062$$

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.

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.

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 primes)**

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

21.

a.

$$(5^{15} \bmod 13) = [(5^2 \bmod 13) \times (5^{13} \bmod 13)] \bmod 13$$
$$= [(-1 \bmod 13) \times (5 \bmod 13)] \bmod 13 = -5 \bmod 13 = 8 \bmod 13$$

b.

$$(15^{18} \bmod 17) = [(15 \bmod 17) \times (15^{17} \bmod 17)] \bmod 17$$
$$= [(-2 \bmod 17) \times (-2 \bmod 17)] \bmod 17 = 4 \bmod 17$$

c.

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

d.

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

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

a.

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

b.

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

c.

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

d.

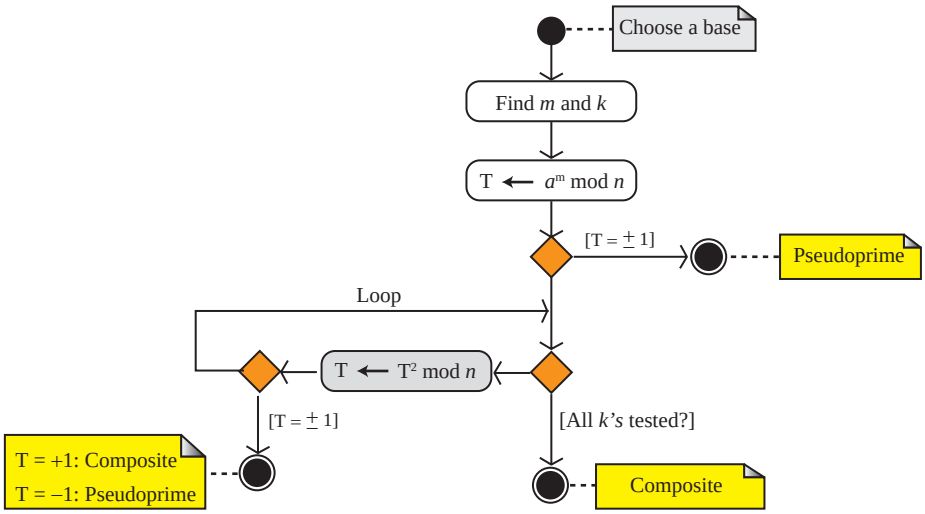
$$44^{-1} \bmod 667 = 44^{\phi(667)-1} \bmod 667 = 44^{615} \bmod 667 = 379 \bmod 667$$

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	$\rightarrow$	$n = 2$ is a prime
$2^3 - 1 = 7$ is a prime	$\rightarrow$	$n = 3$ is a prime
$2^4 - 1 = 15 = 3 \times 5$ is a composite	$\rightarrow$	$n = 4$ is a composite
$2^5 - 1 = 31$ is a prime	$\rightarrow$	$n = 5$ is a prime
$2^6 - 1 = 63 = 3 \times 5$ is a composite	$\rightarrow$	$n = 6$ is a composite
$2^7 - 1 = 127$ is a prime	$\rightarrow$	$n = 7$ is a prime
$2^8 - 1 = 255 = 5 \times 51$ is a composite	$\rightarrow$	$n = 8$ is a composite
$2^9 - 1 = 511 = 7 \times 73$ is a composite	$\rightarrow$	$n = 9$ is a composite
$2^{10} - 1 = 1023 = 3 \times 341$ is a composite	$\rightarrow$	$n = 10$ is a composite
$2^{11} - 1 = 2047 = 23 \times 89$ is a composite	$\rightarrow$	$n = 11$ is a prime

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 $\rightarrow$ $\mathbf{T = 2^{99} \bmod 100 = 88}$

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 $\rightarrow$ $\mathbf{T = 2^{27} \bmod 109 = 33}$

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

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

c. $n = 201 \rightarrow 201 - 1 = 25 \times 2^3 \rightarrow m = 27$ and $k = 3$.

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

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

$k = 2$ $\rightarrow$ $\mathbf{T = T^2 \bmod 201 = 199 \bmod 201}$

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

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

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

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

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

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

$k = 1$ $\rightarrow$ $\mathbf{T = T^2 \bmod 341 = 1 \bmod 341}$

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	→	**$T = 2^{87} \bmod 349 = 213$**
$k = 1$	→	**$T = T^2 \bmod 349 = 348 \bmod 349 = (-1) \bmod 349$**

Loop is broken because T = –1 → 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 × 89)

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

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.

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

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

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

31.

a.

$a_1 = 2$ $m_1 = 7$ $a_2 = 3$ $m_2 = 9$ → $M = 63$

$M_1 = 9$ $M_1^{-1} = 9^{-1} \bmod 7 = 4$; **$M_2 = 7$ $M_2^{-1} = 7^{-1} \bmod 9 = 4$**

$x = (2 \times 9 \times 4 + 3 \times 7 \times 4) \bmod 63 = 30$

b.

$a_1 = 4$ $m_1 = 5$ $a_2 = 10$ $m_2 = 11$ → $M = 55$

$M_1 = 11$ $M_1^{-1} = 11^{-1} \bmod 5 = 1$; **$M_2 = 5$ $M_2^{-1} = 5^{-1} \bmod 11 = 9$**

$x = (4 \times 11 \times 1 + 10 \times 5 \times 9) \bmod 55 = 54$

c.

$a_1 = 7$ $m_1 = 13$ $a_2 = 11$ $m_2 = 12$ → $M = 156$ $M_1 = 12$ $M_2 = 13$

$M_1 = 12$ $M_1^{-1} = 12^{-1} \bmod 13 = 12$; **$M_2 = 13$ $M_2^{-1} = 13^{-1} \bmod 12 = 1$**

$x = (7 \times 12 \times 12 + 11 \times 13 \times 1) \bmod 156 = 59$

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.

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

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:

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

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.**

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

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

***a*'s**	x_i	$y = \mathbf{1} \bmod 8$
$a^1 = 5 \bmod 8$	0	$y = 1$ **mod 8**
$a^2 = 1 \bmod 8$	0	$y = 1$ **mod 8**
$a^4 = 1 \bmod 8$	0	$y = 1$ **mod 8**
$a^8 = 1 \bmod 8$	1	$y = 1 \times 1 \bmod 8 = 1 \bmod 8$
$a^{16} = 1 \bmod 8$	1	$y = 1 \times 1 \bmod 8 =$ **1** $\bmod 8$

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

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

***a*'s**	x_i	$y = \mathbf{1} \bmod 461$
$a^1 = 320 \bmod 461$	1	$y = 1 \times 320 \bmod 461 = 320 \bmod 461$
$a^2 = 58 \bmod 461$	1	$y = 320 \times 58 \bmod 461 = 120 \bmod 461$
$a^4 = 137 \bmod 461$	1	$y = 120 \times 137 \bmod 461 = 305 \bmod 461$
$a^8 = 329 \bmod 461$	0	$y = 305$ **mod 461**
$a^{16} = 367 \bmod 461$	1	$y = 305 \times 367 \bmod 461 =$ **373** $\bmod 461$

c. $y = 1776^{41} \bmod 2134 \rightarrow a = 1776, x = 41 = 101001_2$. 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	$y = \mathbf{1776 \bmod 2134}$
$a^4 = 438 \bmod 2134$	0	$y = \mathbf{1776 \bmod 2134}$
$a^8 = 1918 \bmod 2134$	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.

37.

a. To solve the equation $x^5 \equiv 11 \pmod{17}$, we need to find a primitive root in the group $\mathbf{G} = <\mathbf{Z}_{17}^*, \times>$ 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).

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

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.

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

Now we can use the table to find x if $L_3(x) = 11$; the answer is $\boldsymbol{x = 7}$, 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 $\boldsymbol{x = 7}$.

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 $\mathbf{G} = <\mathbf{Z}_{19}^*, \times>$ 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 $L_2(3) = 13$.

$$\mathbf{L_2(2x^{11}) \equiv L_2(3) \pmod{18} \quad \rightarrow \quad L_2(2) + 11 \times L_2(x) \equiv L_2(3) \pmod{18}}$$
$$\mathbf{\rightarrow 1 + 11 \times L_2(x) \equiv 13 \pmod{18} \rightarrow 11 \times L_2(x) \equiv 12 \pmod{18}}$$

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 $\gcd(11, 18) = 1$.

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

Now we can use the table to find x if $L_2(x) = 6$; the answer is $\boldsymbol{x = 7}$, 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 $\boldsymbol{x = 7}$.

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 to allows us 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 this values satisfies the equation. We did so, but find no value of x satisfying the congruence; the congruence has no solution.

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 $\boldsymbol{n < 2^{32}}$

b. The complexity of Fermat method is subexponential or $2^{p(\log_2 n_b)}$. 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 $\boldsymbol{n < 2^{52}}$

c. The complexity of Polard 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 $\boldsymbol{n < 2^{128}}$

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 $\boldsymbol{n < e^{3{,}600{,}000{,}000}}$

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 $\boldsymbol{n < e^{1{,}800{,}000{,}000}}$

41.

```
Square_and_Multiply (a, x, n)
{
    y ← 1
    for (i = n_b − 1 downto 0)
    {
        a ← a^2 mod n
        if (x_i = 1)
            y ← y × a mod n
    }
    return y
}
```

43.

```
FermatPrimalityTest (a, n)                    // We can use different bases
{
    y ← 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)
}
```

45.

```
ChineseRemainderTheorem(k, a[1 … k], m[1 … 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
}
```

47.

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

49.

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