9장 10/10 2091583 김태곤

15. (4k+1) and (4k+3) are numbers with a remainder of 1 and a remainder of 3 when an integer is divided by 4. In addition to this, there are (4k) and (4k+2). (4k) is divisible by 4, so it is not a prime number. (4k+2) is divisible by 2, so it is not a prime number except for 2 when k=0. All numbers (4k+1) and (4k+3) are not prime number. However it is a prime or composite number. Therefor, it can be a prime number.

17.
$\phi(29) = 29^1 - 29^0 = 28$

$\phi(32) = \phi(2^5) = 2^5 - 2^4 = 16$

$\phi(80) = \phi(2^4 \times 5) = (2^4 - 2^3) \times (5^1 - 5^0) = 8 \times 4 = 32$

$\phi(100) = \phi(2^2 \times 5^2) = (2^2 - 2^1) \times (5^2 - 5^1) = 2 \times 20 = 40$

$\phi(101) = 101^1 - 101^0 = 100$

21.
$a^{p-1} \equiv 1 \bmod p$ (p: prime, a: integer, $p \nmid a$)

$a^p \equiv a \bmod p$ (p: prime, a: integer)

a. $5^{15} \bmod 13 = ((5^2 \bmod 13) \times (5^{13} \bmod 13)) \bmod 13$

$= ((12 \bmod 13) \times (5 \bmod 13)) \bmod 13$

$= 60 \bmod 13 = 8 \bmod 13$

b. $15^{18} \bmod 17 = ((15 \bmod 17) \times (15^{17} \bmod 17)) \bmod 17$

$= ((15 \bmod 17) \times (15 \bmod 17)) \bmod 17$

$= 225 \bmod 17 = 4 \bmod 13$

c. $456^{17} \bmod 17 = 456 \bmod 17 = 14 \bmod 17$

d. $145^{102} \bmod 101 = ((145 \bmod 101) \times (145^{101} \bmod 101)) \bmod 101$

$= ((145 \bmod 101) \times (145 \bmod 101)) \bmod 101$

$= ((44 \bmod 101) \times (44 \bmod 101)) \bmod 101$

$= 1936 \bmod 101 = 17 \bmod 101$

23.
$a^{-1} \bmod n = a^{\phi(n)-1} \bmod n$ (n and a are relatively prime)

$a \times a^{-1} \bmod n = a \times a^{\phi(n)-1} \bmod n = a^{\phi(n)} \bmod n = 1 \bmod n$

$12^1 \bmod 77 = 12$

$12^2 \bmod 77 = 144 \bmod 77 = 67$

$12^4 \bmod 77 = (12^2)^2 \bmod 77 = 67^2 \bmod 77 = 23$

$12^8 \bmod 77 = (12^4)^2 \bmod 77 = 23^2 \bmod 77 = 67$

$12^{16} \bmod 77 = (12^8)^2 \bmod 77 = 67^2 \bmod 77 = 23$

$12^{32} \bmod 77 = (12^{16})^2 \bmod 77 = 23^2 \bmod 77 = 67$

$59 = 32+16+8+2+1$

$(67 \times 23 \times 67 \times 67 \times 12) \bmod 77 = 45$

a. $12^{-1} \bmod 77 = 12^{\phi(77)-1} \bmod 77 = 12^{(7^1-7^0)(11^1-11^0)-1} \bmod 77 = 12^{59} \bmod 77 = 45 \bmod 77$

b. $16^{-1} \bmod 323 = 16^{\phi(323)-1} \bmod 323 = 16^{16 \times 18 - 1} \bmod 323 = 16^{287} \bmod 323 = 101 \bmod 323$

c. $20^{-1} \bmod 403 = 20^{\phi(403)-1} \bmod 403 = 20^{30 \times 12 - 1} \bmod 403 = 20^{359} \bmod 403 = 262 \bmod 403$

d. $44^{-1} \bmod 667 = 44^{\phi(667)-1} \bmod 667 = 44^{22 \times 28 - 1} \bmod 667 = 44^{615} \bmod 667 = 377 \bmod 667$

If we calculate it in the same way as above, we will get the same result

Scanned with CamScanner

25.

$2^2-1=3$
$2^3-1=7$
$2^4-1=15=3\times5$
$2^5-1=31$
$2^6-1=63=7\times9$
$2^7-1=127$
$2^8-1=255=5\times51$
$2^9-1=511=7\times73$
$2^{10}-1=1023=3\times341$
$2^{11}-1=2047=23\times89$

If 2^n-1 is a prime number, then n must be a prime number.
when $n=2,3,5,7$, From these examples we can see that when 2^n-1 is a prime number, n is indeed a prime number.
However, this fact cannot be used as a definitive test for primality. The reason is that while 2^n-1 being prime implies n is prime, the converse is not necessarily true.
2^n-1 may or may not be a prime. when $n=11$, which is not a prime number
In conclusion, the fact that 2^n-1 being prime implies n is prime cannot be used for a reliable primality test because it does not work in the reverse direction.
Not all Mersenne numbers (2^n-1) are primes when n is prime.

26.

if n is prime, $a^{n-1} \equiv 1 \bmod n$ ← Fermat primality test

100 : $2^{99} \bmod 100 = (2^{11})^9 \bmod 100 = (\underbrace{2^{11} \bmod 100 \times 2^{11} \bmod 100 \times \cdots \times 2^{11} \bmod 100}_{\times 9}) \bmod 100$
$= 48^9 \bmod 100 = (48 \bmod 100 \times 48^8 \bmod 100) \bmod 100$
$= (48 \times (48^2)^4 \bmod 100) \bmod 100 = (48 \times 4^4) \bmod 100 = 12288 \bmod 100 = 88$ ← not pass

110 : $2^{109} \bmod 110 = ((2^{12})^9 \times 2) \bmod 110 = (26^9 \times 2) \bmod 110$
$= ((26^3)^3 \times 2) \bmod 110 = (86^3 \times 2) \bmod 110 = (36 \times 2) \bmod 110 = 72$ ← not pass

130 : $2^{129} \bmod 130 = (2 \times (2^{16})^8) \bmod 130 = (2 \times ((65536) \bmod 130)^8) \bmod 130$
$= (2 \times 16^8) \bmod 130 = (2 \times (256 \bmod 130)^4) \bmod 130 = (2 \times (-4)^4) \bmod 130$ ← not pass
$= 512 \bmod 130 = 122$

150 : $2^{149} \bmod 150 = 2^5 \times (2^{12})^{12} \bmod 150 = (2^5 \times 46^{12}) \bmod 150$
$= (2^5 \times 16^6) \bmod 150 = (2^5 \times (2^{12})^2) \bmod 150$
$= (2^5 \times 46^2) \bmod 150 = 62$ ← not pass

200 : $2^{199} \bmod 200 = 88$ ← not pass
250 : $2^{249} \bmod 250 = 62$
If we calculate it in the same way as above, we will got the same result.

271 : $2^{270} \bmod 271 = 1$
341 : $2^{340} \bmod 341 = 1$ pass
561 : $2^{560} \bmod 561 = 1$

$n = 271, 341, 561$ pass Fermat primality test.
but only 271 is a prime number

27. $n-1 = m\times 2^k$ product of an odd integer m and a power of 2

100: $100-1 = 99\times 2^0$

Initialization $T = 2^{99} \bmod 100 = 88$ ← Found in problem 26

no loop ← composite

109: $109-1 = 27\times 2^2$

Initialization $T = 2^{27} \bmod 109 = (2^9)^3 \bmod 109$

$= (-33)^3 \bmod 109 = -76 \bmod 109 = 33 \bmod 109$

k=1 $T = 33^2 \bmod 109 = (-1) \bmod 109$ $T=-1$. So 109 is actually a prime (Pseudoprime)

← If it is -1 in the loop, it is pseudoprime

201 $201-1 = 25\times 2^3$

Initialization $T = 2^{25} \bmod 201 = ((2^{10})^2 \times 2^5) \bmod 201$

$= (19^2\times 2^5) \bmod 201 = 11552 \bmod 201 = 95 \bmod 201$

k=1 $T = 95^2 \bmod 201 = 181 \bmod 201$

k=2 $T = 181^2 \bmod 201 = 199 \bmod 201$ ← 201 is composite, because loop is terminated.

271 $271-1 = 135\times 2^1$

Initialization $T = 2^{135} \bmod 271 = (2^9)^{15} \bmod 271$

$= (-30)^{15} \bmod 271 = ((-30)^3)^5 \bmod 271$

If it is ±1 in the initial stage it is pseudoprime

$= 100^5 \bmod 271 = (10^5)^2 \bmod 271 = 1 \bmod 271$ $T=1$ So 271 is actually a prime (PseudoPrime)

341 $341-1 = 85\times 2^2$

Initialization $T = 2^{85} \bmod 341 = (2^{17})^5 \bmod 341$

$= 128^5 \bmod 341 = 2^{35} \bmod 341$

$= (2^3\times (2^{16})^2) \bmod 341 = (2^3 \times 64^2) \bmod 341 = 32 \bmod 341$

If it is +1 in the loop it is composite

k=1 $T = 32^2 \bmod 341 = 1 \bmod 341$ $T=1$ So 341 is composite

349. $349-1 = 87\times 2^2$

Initialization $T = 2^{87} \bmod 349 = (2^{29})^3 \bmod 349$

$= (2^{30}/2)^3 \bmod 349 = (23^3/2)^3 \bmod 349$

$= (-24)^3 \bmod 349 = -136 \bmod 349 = 213 \bmod 349$

If it is -1 in the loop it is pseudoprime.

k=1 $T = 213^2 \bmod 349 = 348 \bmod 349 = (-1) \bmod 349$ $T=-1$ So 349 is actually a prime (PseudoPrime)

28. 271 : $(2,3,5,7,11,13,17,19,23) \nmid 271$

$271-1 = 135 \times 2^1$

$a=2$ $T = 2^{135} \bmod 271 = 1$ ← found in problem 27

$a=3$ $T = 3^{135} \bmod 271 = -1$ if it is ±1 in the initial stage, it is pseudo prime

$a=4$ $T = 4^{135} \bmod 271 = 1$

271 passes 3 Miller-Rabin tests. So 271 is Pseudo Prime

3149 : $(2,3,5,7,11,13,17,19,23) \nmid 3149$

$3149-1 = 787 \times 2^2$

$a=2$ $T = 2^{787} \bmod 3149 = 2523 \bmod 3149$

$T = (2523)^2 \bmod 3149 = 140 \bmod 3149$ ← 3149 didn't pass Miller-Rabin test
So 3149 is composite

9673 : $(2,3,5,7,11,13) \nmid 9673$

$(17) \mid 9673$ so 9673 is composite