암호학기초 HW#3 2019 1629 이주현

Chapter 9

15. Show that every prime is either in the form $4k+1$ or $4k+3$ $k \in \mathbb{Z}^+$.

For an integer n, n can be written in form of $4k+r$ where $r \in \{0, 1, 2, 3\}$. Among these 4 cases, $4k+0$ and $4k+2$ cannot represent prime number as both are at least divisible with 2.

Thus. only $4k+1$ and $4k+3$ can represent a prime number.

17. Find the value of $\phi(29)$, $\phi(32)$, $\phi(80)$, $\phi(100)$, $\phi(101)$.

i) 29 is a prime. $\rightarrow \phi(29) = 29-1 = 28.$

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

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

iv) $100 = 2^2 \times 5^2 \rightarrow \phi(100) = (2^2 - 2) \times (5^2 - 5) = 2 \times 20 = 40.$

v.) 101 is a prime. $\rightarrow \phi(101) = 101 - 1 = 100$.

21. Find the following using Fermat's little theorem.

a. $5^{15} \bmod 13 = ((5^2 \bmod 13) \times (5^{13} \bmod 13)) \bmod 13.$
$= ((-1 \bmod 13) \times (5 \bmod 13)) \bmod 13 = \boxed{8 \bmod 13}$

b. $15^{18} \bmod 17 = ((15 \bmod 17) \times (15^{17} \bmod 17)) \bmod 17.$
$= ((15 \bmod 17) \times (15 \bmod 17)) \bmod 17 = \boxed{4 \bmod 17}$

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

d. $145^{102} \bmod 101 = ((145^{101} \bmod 101) \times (145 \bmod 101)) \bmod 101.$
$= ((44 \bmod 101) \times (44 \bmod 101)) \bmod 101 = \boxed{17 \bmod 101}$

23. Find the following using Euler's theorem.

a. $12^{-1} \bmod 77 = 12^{\phi(77)-1} \bmod 77.$ $(\phi(77) = 6 \times 10 = 60)$
$= 12^{59} \bmod 77 = \boxed{45 \bmod 77}$

b. $16^{-1} \bmod 323 = 16^{\phi(323)-1} \bmod 323$ $(\phi(323) = 16 \times 18 = 288)$
$= 16^{287} \bmod 323 = \boxed{101 \bmod 323}$

c. $20^{-1} \bmod 403 = 20^{\phi(403)-1} \bmod 403$ $(\phi(403) = 30 \times 12 = 360)$
$= 20^{359} \bmod 403 = \boxed{262 \bmod 403}$

d. $44^{-1} \bmod 667 = 44^{\phi(667)-1} \bmod 667$ $(\phi(667) = 22 \times 28 = 616)$
$= 44^{615} \bmod 667 = \boxed{379 \bmod 667}$

25. Can 2^n-1 be used for primality test?

Using the online database of known sequences, a lot of n that makes 2^n-1 ... prime are primes. These examples are 2, 3, 5, 7 where 2^n-1 equals to 3, 7, 31, 127, respectively. The smallest prime n that makes composite 2^n-1 is 11. as $2^{11}-1 = 2047$, which can be divisible with 23, 89.

26. Run the Fermat primality test.

i) $2^{100-1} \bmod 100 = 88$ (X) $\therefore$ Composite
ii) $2^{110-1} \bmod 110 = 72$ (X) $\therefore$ Composite
iii) $2^{130-1} \bmod 130 = 88$ (X) $\therefore$ Composite
iv) $2^{150-1} \bmod 150 = 88$ (X) $\therefore$ Composite
v) $2^{200-1} \bmod 200 = 88$ (X) $\therefore$ Composite
vi) $2^{250-1} \bmod 280 = 62$ (X) $\therefore$ Composite
vii) $2^{291-1} \bmod 271 = 1$ (O) $\therefore$ maybe prime? $\Rightarrow$ prime!
viii) $2^{341-1} \bmod 341 = 1$ (O) $\therefore$ Maybe prime? $\Rightarrow$ Composite.
ix) $2^{561-1} \bmod 561 = 1$ (O) $\therefore$ maybe prime? $\Rightarrow$ Composite.

27. Run the Miller-Rabin primality test.

i) $n = 100$, $m = 100-1 = 99$, $k = 0$. $\Rightarrow$ Composite.

ii) $n = 109$, $m = 27$, $k = 2$
$T = 2^{27} \bmod 109 = 33$, $k = 0$
$T = 33^2 \bmod 109 = 108 \bmod 109 = (-1) \bmod 109$, $k = 1$. $\Rightarrow$ Pseudoprime.

iii) $n = 201$, $m = 25$, $k = 3$.
$T = 2^{25} \bmod 201 = 95$, $k = 0$
$T = 95^2 \bmod 201 = 181 \bmod 201$, $k = 1$.
$T = 181^2 \bmod 201 = 199 \bmod 201$, $k = 2$. $\Rightarrow$ Composite.

iv) $n = 271$, $m = 135$, $k = 1$
$T = 2^{135} \bmod 271 = 1 \bmod 271$ $\Rightarrow$ Pseudoprime.

v) $n = 341$, $m = 85$, $k = 2$.
$T = 2^{85} \bmod 341 = 32$. $k = 0$
$T = 32^2 \bmod 341 = 1 \bmod 341$, $k = 1$ $\Rightarrow$ Composite.

vi) $n = 349$, $m = 87$, $k = 2$
$T = 2^{87} \bmod 399 = 213$, $k = 0$
$T = 213^2 \bmod 349 = 348 \bmod 344, = (-1) \bmod 349$, $k = 1$ $\Rightarrow$ pseudoprime

vii) $n = 2047$, $m = 1023$, $k = 1$

$T = 2^{1023} \bmod 2047 = 1 \bmod 2047$, $k = 0$. ⇒ Pseudoprime.

28. Use the recommended test to determine whether integers are primes.

i) 271 is not easy to divide. → Miller-Rabin test.

$n = 271$, $m = 135$, $k = 1$

for $a = 2$, $T = 2^{135} \bmod 271 = 1$.
for $a = 3$, $T = 3^{135} \bmod 271 = -1$.
for $a = 4$, $T = 4^{135} \bmod 271 = 1$.
⇒ pseudoprime.

ii) 3149 is not easy to divide. → Miller-Rabin test.

$n = 3149$, $m = 787$, $k = 2$.

for $a = 2$, $T = 2^{787} \bmod 3149 = 2523$ ($k = 0$)
$T = 2523^2 \bmod 3149 = 140$ ($k = 1$).
→ Composite.

iii) 9673 is easy to divide: $9673 \div 17 = 569 \cdots 0$.

→ Composite.