정수론 HW2

20011759 박수민

1. $\boldsymbol{\varphi(8500)}$***을 구하시오.***

$$\begin{aligned}&\varphi(8500) = \varphi(2^2 \times 5^3 \times 17)\\&= \varphi(2^2) \times \varphi(5^3) * \varphi(17)\\&= 2^{2-1} \times (2-1) \times 5^{3-1} \times (5-1) \times (17-1)\\&= 2 \times 25 \times 4 \times 16\\&= 3200\end{aligned}$$

$$\therefore 3200$$

2. $\boldsymbol{\varphi(n) = 14}$***를 만족하는 자연수*** $\mathbf{n}$***은 존재하지 않음을 보이시오***

n은 15 초과의 소인수를 가지지 못한다 왜냐하면 n이 15를 초과하는 소인수를 가진다면 $\varphi(p^a q^b r^c \dots) = p^{a-1}q^{b-1}r^{c-1} \dots (p-1)(q-1)(r-1)\dots$ 에서 $(p-1)$부분에 의해 14를 초과할 수 밖에 없기 때문이다. 그러므로 $\mathrm{n} = 2^{\mathrm{a}}3^b 5^c 7^d 11^e 13^f$라 하자. 그러면 $\varphi(n)$은 다음과 같다

$\varphi(n) = 2^{\mathrm{a}-1}3^{b-1}5^{c-1}7^{d-1}11^{e-1}13^{f-1} \cdot 2 \cdot 4 \cdot 6 \cdot 10 \cdot 12$ 이다. 그런데 4,6,10,12에는 어떠한 정수를 곱해도 14를 만들 수 없다. 그러므로 소인수 5,7,11,13을 가지지 못한다. 그러면 $n = 2^{\mathrm{a}}3^b$ 형태이고 $\varphi(n) = 2^{\mathrm{a}-1}3^{b-1} \cdot 2$이다. 그런데 $14 = 2 \cdot 7$를 보면 알 수 있듯 14를 만들기 위해서는 $\varphi(n)$는 7을 소인수로 포함하고 있어야 하나 $2^{\mathrm{a}-1}3^{b-1} \cdot 2$는 소인수를 2, 3만을 가지므로 7를 가지지 못한다. 그러므로 $\varphi(n) = 14$인 자연수 n은 존재하지 않는다.

3. $\boldsymbol{n}$***이 홀수일 때,*** $\mathbf{5 \nmid n \rightarrow 5 | (n^4 + 4^n)}$ ***임을 보이시오***

$5 \nmid n$이므로 $n = 5a + k, (k = 1\ or\ 2\ or\ 3\ or\ 4)$라 하자.
우선 $1^2 \equiv 1\ (mod\ 5), 2^2 \equiv 4\ (mod\ 5), 3^2 \equiv 4\ (mod\ 5), 4^2 \equiv 1\ (mod\ 5)$이므로 $n^2 = 1\ or\ 4$이다.
$n^4 = (n^2)^2$이므로 $n^4 \equiv 1\ (mod\ 5)$ 임을 알 수 있다. 이제 $4^n \equiv -1\ (mod\ 5)$임을 보이면 된다.
그런데 $4 \equiv -1\ (mod\ 5)$ 이므로 $4^n \equiv (-1)^n\ (mod\ 5)$이다. 이때 n이 홀수이므로 $4^n \equiv -1\ (mod\ 5)$가 된다. $(n^4 + 4^n) \equiv (1 - 1) \equiv 0\ (mod\ 5)$이므로 $5 | (n^4 + 4^n)$ 이다.

4. $\boldsymbol{p \equiv 5 \ mod \ 6}$***을 만족하는 소수*** $\boldsymbol{p}$ ***가 무한히 많다는 것을 보이시오***

$p \equiv 5 \ (mod \ 6)$를 만족하는 소수p 가 유한하다 가정하고 이러한 소수의 집합을 $P = \{p_1, p_2, p_3 \dots p_k\}$ 라 하자. $p_1 < p_2 < p_3 \dots$라 한다면 p_1은 자명하게 5일 것이다.
$n = 6p_2p_3p_4p_5 \dots p_k + 5$라 한다면 $n > p_k$ 이므로 위 가정에 의해 합성수이다.
그렇다면 $n = q_1^{e_1}q_2^{e_2}q_3^{e_3} \dots q_s^{e_s}$형태로 인수분해가 가능하다는 뜻이 된다.($q_1, q_2, q_3 \dots q_s$*은 소수*)

$n = 6p_2p_3p_4p_5 \dots p_k + 5$ 에서 P 의 모든 원소는 홀수이므로 $p_2p_3p_4p_5 \dots p_k$ 은 홀수이고, $6p_2p_3p_4p_5 \dots p_k + 5$은 홀수이다. 그러므로 n의 임의의 소인수 q에 대해, $q \not\equiv 0, 2, 4 \ (mod \ 6)$임을 알 수 있다. ($q \equiv 0 \ or \ 2 \ or \ 4 \ (mod \ 6)$이라면 q는 짝수가 되는데 그러면 n이 짝수가 되기 때문이다.)
그리고 $q \equiv 3 \ (mod \ 6)$이라면 임의의 정수 k에 대해(그리고 임의의 정수 t 에 대해 $q = 6t + 3$으로 두면), $2kq = 2k(6t + 3) = 12kt + 6 \equiv 0 \ (mod \ 6)$, $(2k + 1)q = (2k + 1)(6t + 3) = 12kt + 6t + 6k + 3 \equiv 3 \ (mod \ 6)$이므로 q와 곱해지는 수가 짝수라면 법 6에서 0과 합동, 홀수라면 법6에서 3과 합동이다. 즉, 소수 q와 임의의 정수 곱은 법 6에서 3 또는 0만 합동이고 $n = 6p_2p_3p_4p_5 \dots p_k + 5 \equiv 5 (mod \ 6)$이므로 $q \not\equiv 3 \ (mod \ 6)$이다. 즉, $q \equiv 1 \ or \ 5 \ (mod \ 6)$이다. 그런데 모든 $q_1, q_2, q_3, \dots q_s$에 대해 적어도 하나 이상은 $q \equiv 5 \ (mod \ 6)$이다. 왜냐하면 모든 소인수가 법 6에서 1과 합동이라면 이들의 곱인 n또한 법 6에서 1과 합동이기 때문이다. 즉 $q' \equiv 5 \ (mod \ 6)$인 임의의 n의 소인수를 q'라 두자

$p_1 \nmid 6p_2p_3p_4p_5 \dots p_k$이고 $p_1 \mid 5$이므로 $p_1 \nmid n$이다. 그리고 $p_2, p_3, p_4, p_5 \dots p_k \nmid 5$이고
$p_2, p_3, p_4, p_5 \dots p_k \mid 6p_2p_3p_4p_5 \dots p_k$이므로 $p_2, p_3, p_4, p_5 \dots p_k \nmid n$이다. 즉 P의 원소로는 n을 나눌 수 없으나 $q' | n$이다. 즉, $q' \notin P$인데 $q' \equiv 5 \ (mod \ 6)$이므로 가정과 모순된다. 그러므로 $p \equiv 5 \ (mod \ 6)$를 만족하는 소수p는 무한히 많다.

5. ***밀러 – 라빈 판정법을 사용하여 다음 자연수*** $n = 118901521$ ***이 합성수임을 보이시오***

파이썬을 사용하여 계산하였다.

```
def pow_mod(a,e,m):

    if(e == 1):

        return a % m;

    ebit1 = e % 2;

    e=e>>1

    return (a**ebit1 % m) * ((pow_mod(a,e,m)**2) % m) % m;




n=int(input())


if(n%2==0):

    print("ERROR, n must be odd")

    exit(0)


tmp = n - 1

k=0

while(tmp % 2 == 0):

    k+=1

    tmp = tmp >> 1

q = tmp



isComposite = False
```

```
for a in range(1,n):
    if(pow_mod(a,q,n) == 1):
        continue

    check2 = True
    for i in range(0,k):
        if(pow_mod(a,q*(2**i),n)==n-1):
            check2 = False
            break
    if(not check2):
        continue

    isComposite = True
    break

if isComposite:
    print("n is composite number")
else :
    print("n is not composite number")
```

IDLE Shell 3.9.6

File Edit Shell Debug Options Window Help

```
Python 3.9.6 (tags/v3.9.6:db3ff76, Jun 28 2021, 15:26:21) [MSC v.1929 64 bit (AM
D64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>> 
================ RESTART: D:₩PSM₩나는 한다 작업을₩과제₩정수론₩RabinMiller.py ===
============
118901521
n is composite number
>>> 
```

Ln: 7 Col: 4