

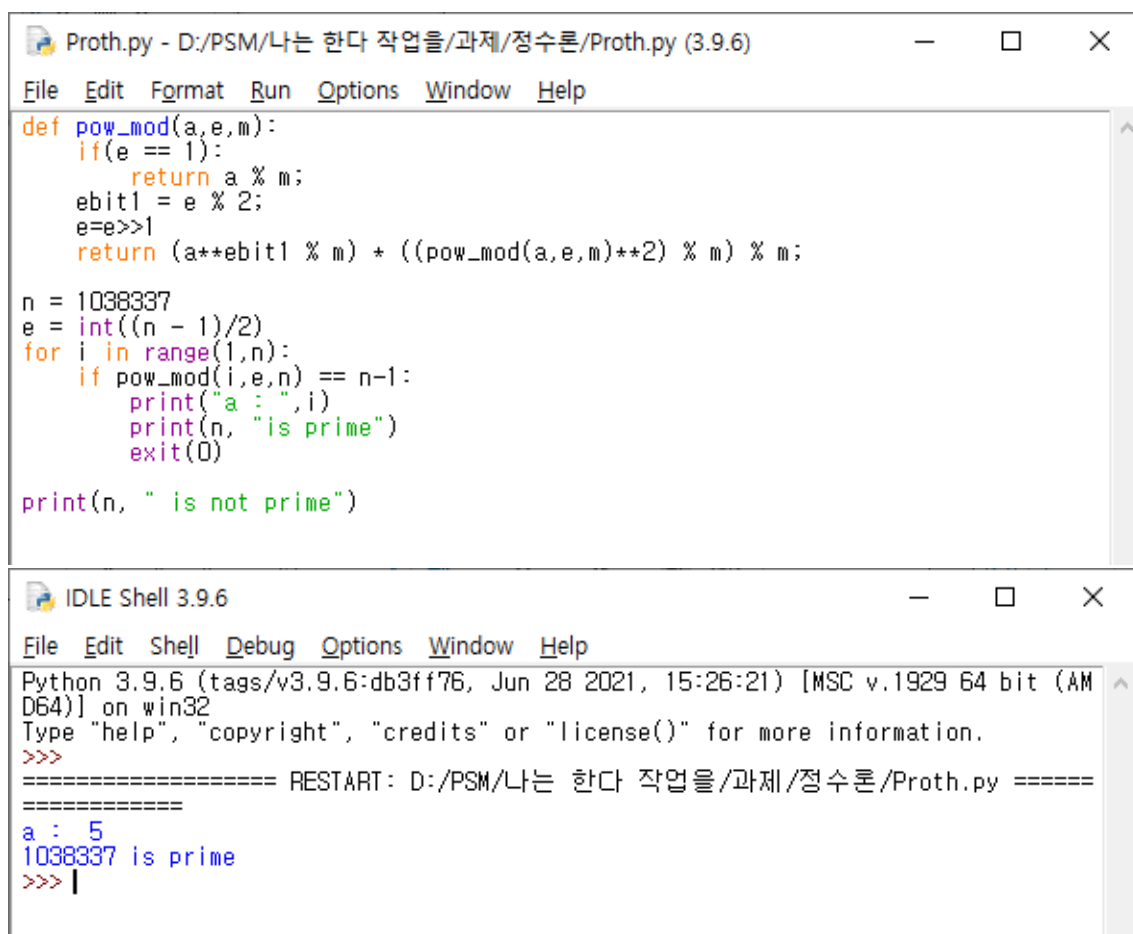
정수론 HW4

20011759 박수민

1. Proth의 prime test를 이용하여 다음 수가 소수임을 보이시오 – 1038337

$1038337 = 2^{11} \cdot 507 + 1$ 이다(울프람 알파 사용)

$507 < 2^{11}$ 이므로 Proth prime test를 사용할 수 있다. 사용 언어는 파이썬이다.



The image shows two windows from the IDLE Python environment. The top window, titled 'Proth.py - D:/PSM/나는 한다 작업을/과제/정수론/Proth.py (3.9.6)', contains a Python script. The script defines a function `pow_mod(a, e, m)` that implements modular exponentiation using the binary method. It then sets `n = 1038337` and `e = int((n - 1) / 2)`. A loop iterates `i` from 1 to `n`. For each `i`, it checks if `pow_mod(i, e, n) == n - 1`. If true, it prints `a :` followed by `i`, then `1038337 is prime`, and exits. If false, it prints `1038337 is not prime`. The bottom window, titled 'IDLE Shell 3.9.6', shows the execution output. It displays the Python version and environment information, followed by a restart message. The output shows `a : 5` and `1038337 is prime`, indicating that 1038337 is a Proth prime.

```
Proth.py - D:/PSM/나는 한다 작업을/과제/정수론/Proth.py (3.9.6)
File Edit Format Run Options Window Help
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 = 1038337
e = int((n - 1) / 2)
for i in range(1, n):
    if pow_mod(i, e, n) == n - 1:
        print("a : ", i)
        print(n, " is prime")
        exit(0)

print(n, " is not prime")

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 (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: D:/PSM/나는 한다 작업을/과제/정수론/Proth.py =====
a : 5
1038337 is prime
>>> |
```

$5^{\frac{1038337-1}{2}} \equiv -1 \pmod{1038337}$, Proth prime test에 의해 1038337은 소수이다.

2. Pollard rho method를 이용하여 137703491을 소인수분해하시오

```
rho.py - D:/PSM/나는 한다 작업을/과제/정수론/rho.py (3.9.6)
File Edit Format Run Options Window Help

    if a > b:
        tmp = a
        a = b
        b = tmp
    #a < b
    if a == 0:
        return b
    if b % a == 0:
        return a
    else:
        return gcd(b % a, a)

def pollard_rho(n):
    def g(x,n):
        return (x*x + 1) % n;

    x = 2
    y = 2
    d = 1
    while d == 1:
        x = g(x,n)
        y = g(g(y,n),n)
        d = gcd(abs(x-y),n)

    if 1 < d < n:
        return d
    else:
        return -1

while True:
    n = int(input())
    if pollard_rho(n) == -1:
        print("has no factor")
        continue
    print("factor: ",pollard_rho(n))
    print("remainder: ",int(n/pollard_rho(n)))
    if n == -1:
        break
```

```
*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 (AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
===== RESTART: D:/PSM/나는 한다 작업을/과제/정수론/rho.py =====
137703491
factor: 17389
remainder: 7919
```

Pollard rho method는 $n = pq$ 꼴인 숫자를 소인수 분해할 때 쓰므로
 $137703491 = 17389 \cdot 7919$ 이다

3.공개키: $(p, r, r^a \pmod p) = (37831, 2, 13103)$ 이다. $(253, 17891)$ 를 복호화해라

우선 $a = 17377$ (울프람 알파 사용)

$(r^k \pmod p, mr^{ak} \pmod p) = (253, 17891)$ 에서 $mr^{ak} \cdot (r^k)^{p-1-a} = mr^{p-1} \equiv 1 \pmod p$ 임을 이용해서

$$17891 \cdot 253^{37831-1-17377} = 17891 \cdot 253^{20453} \equiv 7944$$

$$\therefore 7944$$

4. $\sqrt{86} = [a_0; a_1, a_2, a_3, \dots]$ 일 때, $C_6 = [a_0; a_1, a_2, a_3, a_4, a_5, a_6]$ 를 구하시오

$$\begin{aligned} \sqrt{86} &= 9 + \sqrt{86} - 9 = 9 + \frac{1}{\frac{1}{\sqrt{86} - 9}} = 9 + \frac{1}{3 + (\frac{1}{\sqrt{86} - 9} - 3)} = 9 + \frac{1}{3 + \frac{-3\sqrt{86} + 28}{\sqrt{86} - 9}} \\ &= 9 + \frac{1}{3 + \frac{1}{\frac{\sqrt{86} - 9}{-3\sqrt{86} + 28}}} = 9 + \frac{1}{3 + \frac{1}{1 + (\frac{\sqrt{86} - 9}{-3\sqrt{86} + 28} - 1)}} \dots \end{aligned}$$

이와 같은 방식으로 전개하면 다음과 같이 얻을 수 있다.

$$C_6 = [9; 3, 1, 1, 1, 8, 1] = \frac{983}{106}$$

5. Pell equation $x^2 - 34y^2 = 1$ 의 자연수 해를 모두 구하시오

$$\sqrt{34} = [5; \overline{1, 4, 1, 10}] \text{에서 } C_3 = 5 + \frac{1}{1 + \frac{1}{4+1}} = \frac{35}{6} \text{인데 } 35^2 - 34 \cdot 6^2 = 1 \text{ 즉, } x^2 - 34y^2 = 1$$

의 임의의 자연수 해 $(x_k, y_k) = (35, 6)$ 이다. 하지만 이 해가 가장 작은 근이라는 보장은 없다. 이는 brutal force로 일일이 찾아보면, $y_k = 6$ 이므로 $y = 1, 2, 3, 4, 5$ 일 때 자연수 근이 존재하는지 확인하면 된다. 이 경우, 존재하지 않으므로 $(35, 6)$ 가 최소로 작은 근, 즉 (x_0, y_0) 이다.

Pell equation 정리에 의해 모든 자연수 근은 다음과 같이 정리된다.

$$\{(x_k, y_k) | x_k + y_k \sqrt{34} = (35 + 6\sqrt{34})^k\}$$