정수론 HW4

20011759 박수민

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

이다(울프람 알파 사용)  
이므로 Proth prime test를 사용할 수 있다. 사용 언어는 파이썬이다.

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

, Proth prime test에 의해 은 소수이다.

**2. Pollard rho method를 이용하여 137703491을 소인수분해하시오**

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

Pollard rho method는 n = pq꼴인 숫자를 소인수 분해할 때 쓰므로  
이다

**3.공개키: 이다. (253, 17891)를 복호화해라**

우선 (울프람 알파 사용)

에서 임을 이용해서

**4. 일 때, 를 구하시오**

이와 같은 방식으로 전개하면 다음과 같이 얻을 수 있다.

**5. Pell equation 의 자연수 해를 모두 구하시오**

에서 인데 즉, 의 임의의 자연수 해 이다. 하지만 이 해가 가장 작은 근이라는 보장은 없다. 이는 brutal force로 일일이 찾아보면, 이므로 일 때 자연수 근이 존재하는지 확인하면 된다. 이 경우, 존재하지 않으므로 가 최소로 작은 근, 즉 이다.   
Pell equation 정리에 의해 모든 자연수 근은 다음과 같이 정리된다.