Ⅰ. 소인수분해 자기주도학습	저는 1 학년 ( )반 ( )번 사랑스러운 ( )입니다.	17
배움주제 : ㅅㅅ	이해도	
	☆☆☆☆☆	

<<소수를 사용하여 암호를 만든다.>>

소수는 찾기 힘들기 때문에 좋은 암호가 된다. 이 암호는 금융 거래와 공인 인증, 신용 카드, 인터넷 쇼핑, 신분 증명 등에 이용된다.

소수는 무한히 많기 때문에 가장 큰 소수는 찾을 수도 없고, 존재하지도 않는다. 하지만 수학자들은 오랫동안 더 큰 소수를 찾기 위해 노력해 왔다.

프랑스 수학자 메르센은 자신의 이름을 딴 '메르센 소수'를 만들었다. 메르센 소수는 2 의 **거듭제곱**에서 1 을 뺀 것, 즉 '2^n-1'이 소수일 때를 말한다.

가장 작은 첫 번째 메르센 소수는 3, 두 번째는 7, 그다음 메르센 소수는 31 이다. 1 부터 100 까지의 수 가운데 메르센 소수는 3, 7, 31 뿐이다.

$2^2-1=4-1=3$, $2^3-1=8-1=7$, $2^5-1=32-1=31$

$2^7-1=128-1=127$

기술이 발달함에 따라 컴퓨터를 사용해서 아주 큰 메르센 소수도 찾을 수 있게 되었다. 1997 년에 발견된 36 번째 메르센 소수는 89 만 5932 자리의 수로, 컴퓨터 출력하면 그 숫자의 나열이 나열이 450 쪽이나 된다. 2004 년에는 조시핀들리가 723 만 5733 자리의 41 번째 메르센 소수를 발견했다. 이 소수는 지금까지 발견된 가장 큰 소수이며, 숫자의 길이도 25km 에 달한다.

수학자들은 왜 이렇게 큰 소수를 찾으려고 하는 것일까?

그것은 소수가 암호에 사용되기 때문이다. 큰 소수를 곱하여 나온 수를 암호로 정하고, 그

수를 알아야 암호를 풀 수 있게 하는 것이다. 큰 소수는 찾기 힘들기 때문에 암호로 사용하기 좋다. 이런 암호는 해독하는 데 오랜 시간이 걸리므로 아주 좋은 암호가 된다. 따라서 더 큰 소수를 알고 있다면 더 풀기 어려운 암호를 만들 수 있다.

세계 2 차 대전은 일본과 미국의 암호 전쟁이라고 할 만큼 상대방이 풀 수 없는 암호 만들기와 그 암호 해독의 치열한 대결을 벌였다. 1942 년 미국은 일본의 암호를 해독함으로써 미드웨이 해전에서 승리할 수 있었다. 미래의 전쟁은 이처럼 '수학의 전쟁'이 될 것이다.

전쟁이나 국가의 중요한 기밀에 쓰이던 암호는 이제 우리 생활에도 깊숙히 들어와 있다. 암호는 각종 금융 거래와 신용 카드, 인터넷 쇼핑 등의 보안을 담당하고 있다. 최근에는 컴퓨터가 광범위하게 사용되면서 개인 정보가 유출되거나 시스템이 파괴되는 일이 일어나기도 한다. 그래서 이런 일을 막기 위해 풀리지 않는 암호를 만드는 것은 더욱더 중요해지고 있다.

[꼬물 꼬물 수학이야기 발췌]

소수는 특히 첨단 정보화 사회가 된 오늘날에는 정보를 보호하는 암호에 사용되고 있다. 최근에 사용되는 암호는 대부분 소수를 이용한 공개 열쇠 암호 방식으로 만들어져 있다. 공개 열쇠 암호 방식은 암호를 만드는 방식은 공개되지만 그 암호를 원래의 문장으로 돌려놓는(이 과정을 복호라고 한다) 열쇠를 알아내기가 거의 불가능한 방식이다. 이런 방식이 가능한 이유는 큰 정수를 소인수 분해 하는 것이 매우 어렵기 때문이다. 예를 들어 어떤 두 소수를 곱한 수 4067351 을 이용하여 암호를 만들었다는 것을 공개한다. 그런데 암호를 원래의 문장으로 돌려놓기 위해서는 이 수가 어떤 두 소수의 곱으로 되어 있는지 알아야 한다. 사실 이 수는 두 소수 1733 과 2347 의 곱이다. 그런데 두 소수 1733 과 2347 을 주고 이들의 곱 4067351 을 계산하는 문제는 아주 쉽지만, 거꾸로 4067351 이 어떤 두 소수의 곱으로 되어 있는지를 찾는 소인수분해 문제는 매우 어렵다. 실제로

사용되는 공개 열쇠 암호 방식은 예를 든 방법보다 훨씬 복잡하고 정교하지만, 소인수분해가 어렵다는 암호의 근본 원리는 같다.

1977 년에 공개열쇠 암호 방식이 처음 발표될 당시, 예로 들었던 두 소수를 곱한 수(수가 너무 크기 때문에 여기서는 생략한다)를 인수분해 하는데 약 40,000,000,000,000,000 년이 걸릴 것으로 예상했다. 그러다가 1994 년에 인수분해 알고리즘이 개발되며 인수분해를 좀 더 빨리 할 수 있게 되었는데, 다행스럽게도 인수분해 알고리즘을 이용해도 100 년 이상 걸린다. 그래서 공개열쇠 암호방식은 오늘날 은행의 저금통장의 비밀번호에서부터 인터넷에서 사용되는 ID 와 암호 등 다양하게 이용되고 있다. 그러나 인수분해 알고리즘이 계속해서 발전하고 있기 때문에 그에 대응하여 더 큰 소수가 필요하게 되었다. 그래서 소수를 연구하는 수학자들은 더 큰 소수를 찾기 위해 지금도 노력하고 있다.

1. 거듭제곱이란?

2. 현재까지 알려진 가장 큰 소수는 몇 자리의 수인가? (검색을 통해 찾아보세요.)

3 . 실생활에서 수학과 관련된 주제를 찾아 1 가지 이상 작성하여보세요 .

(단순한 사칙연산 즉 , 더하기 , 빼기 , 곱하기 , 나누기 내용은 생략합니다 .)