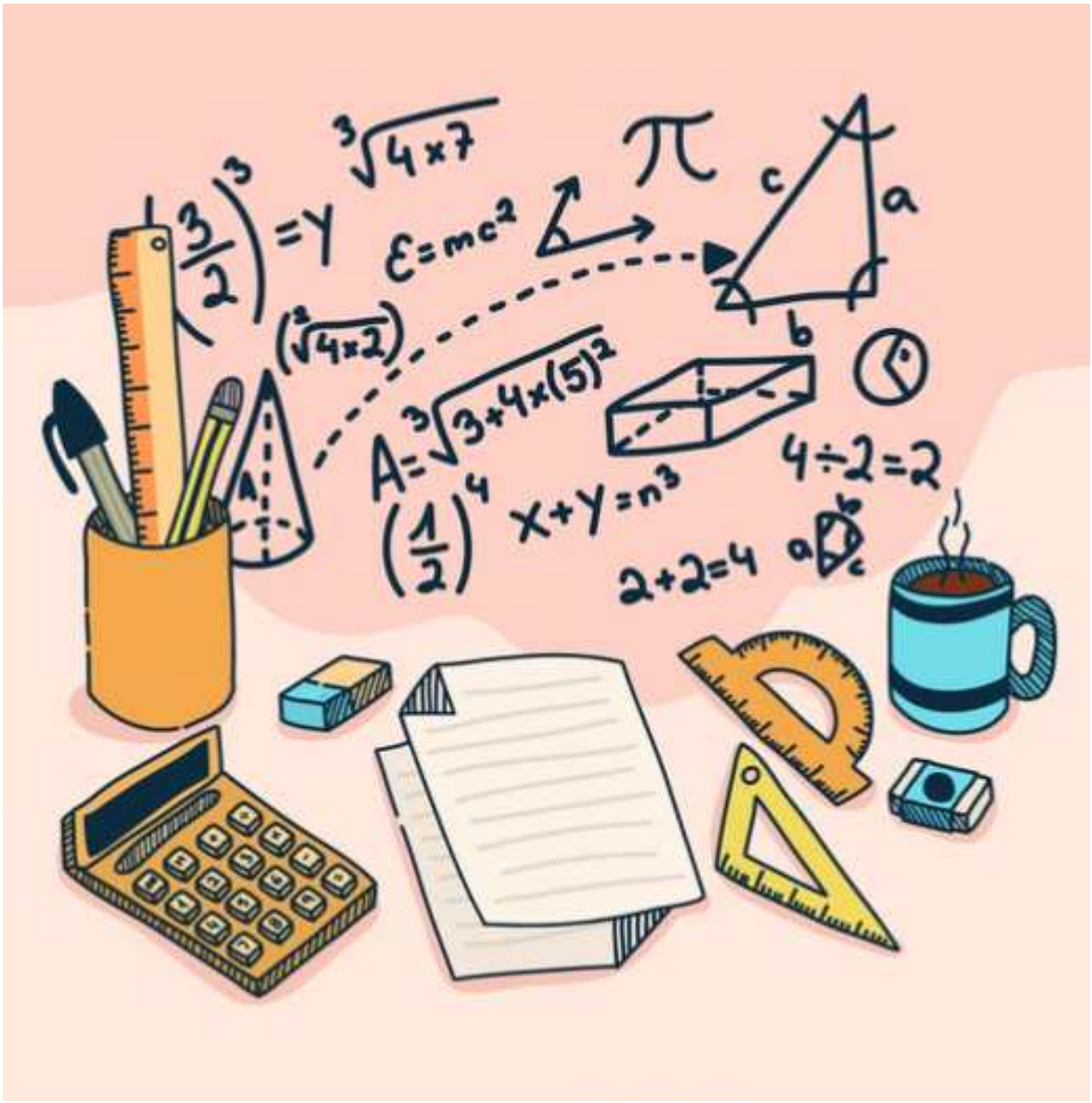
2019년

제 3 회 수학탐구대회



호 남 제 일 고 등 학 교

Contents

Contents

영리한 경제 주체가 되기 위하여

분야 : 주제탐구
10305 김예담, 10312 박현선, 10318 이가현, 10326 정혜민

Ⅰ 탐구 배경 및 목적

□ 예금과 적금에 대하여

가. 탐구 배경

통합 사회 시간에 경제 분야에 대해 학습하게 되었는데, 그 중에서도 예금과 적금에 대해 알게 되었다.
예금과 적금에 대해 관심이 더욱 간 이유는 경제라는게 사람이 살아가면서 상시 접해야 하는 필수적인 분야이며, 나중에 대한민국의 경제 주체가 될 우리가 미리 예금과 적금에 대하여 탐구해본다면 미래의 경제 계획을 수립하는데도 큰 도움이 될거라는 생각이 들었기 때문이다. 또한 예금과 적금 뿐 아니라 단리와 복리에 관해서도 깊이 탐구해보며 더욱 구체적이고 실현가능한 계획을 세울 수 있을 것이라 기대된다.

나. 예금이란?

예금이란 일정한 계약에 의해 금융기관에 금융자산을 맡기는 일 또는 그 자산을 말한다. 대체로 예금에는 일정한 이자가 붙으며, 기한이나 예금방법에 따라 보통예금·당좌예금 별단예금·정기예금·정기적금·통지예금과 각종 부금 등이 있는데, 경제발전에 따라 종류가 늘어난다.
예금은 예금자가 자금의 보관이나 여수(與受)에 수반되는 위험 또는 번잡을 피하거나 이자를 획득하기 위하여 금융기관에 예탁하고, 금융기관은 그 자금을 받아들이고 대개 후일에 약정된 이자와 함께 반환할 것을 계약함으로써 성립되는 것이다.
역사적으로 볼 때 예금이 처음에는 단순하게 수동적인 보관예금으로 나타났지만, 뒤에 대출이 기초가 되는 예금을 적극적으로 받아들이고자 하는 투자예금으로 발전하였고, 근래에는 신용화폐의 발달에 따라 대체예금이 많아지게 되었다. 금융기관에 예입된 자금은 경제발전을 위한 산업자본으로 많이 이용되기 때문에 투자의 기본재원이 되기도 한다.

예금은 성립과정에 따라 본원적 예금(직접예금)과 파생적 예금(간접예금·대체예금)으로 나누어진다. 본원적 예금이란 금융기관 밖에 있던 현금·수표·어음 등이 금융기관에 직접 예입됨으로써 성립되는 예금이고, 파생적 예금은 금융기관이 대출을 하고 그 금액을 일단

거래자의 예금으로 돌림으로써 성립되는 예금이다. 한편, 예금은 예금자가 필요에 따라 언제든지 환불할 수 있는 요구불예금과 계약에 따라 일정한 기간 동안은 원칙적으로 환불할 수 없도록 된 저축성예금으로 분류되기도 한다.

다. 적금이란?

적금(積金)은 은행 예금 상품의 하나로, 일정 기간을 계약하고 정기적 또는 비정기적으로 금액을 불입하여 계약 기간이 만료된 후 이를 이자와 함께 일괄적으로 돌려받는 것이다.
적금은 적은 돈으로 목돈을 만들 수 있는 은행 예금 상품의 하나이며 보통 예금과 비교하면 적금은 계약 기간이 몇 개월 단위로 정해져 있고 계약 기간 내에서는 입금만 가능하며 출금이 불가능하다. 이율은 보통 예금보다 비교적 높다.
적금의 종류에는 불입 방식에 따라 정기적금과 자유적금이 있지만 다르게 분류해 보면 여러가지 종류가 있다.
세율에 따라서는 일반 과세형 적금이 있고 이자에 세금이 적게 붙는 세금우대 적금과 또 세금이 전혀 붙지 않는 비과세 적금 등이 있다. 참고로, 세금우대 적금은 1년 이상만 가능하며 2006년부터는 만 19세 미만의 미성년자는 세금우대 적금을 가입할 수 없다. 2009년부터 세금우대한도가 1000만원으로 하향되었다.
목적에 따라서는 주택적금 등이 있다. 그 외에도, 초·중·고등학교에서는 저축 습관 함양 등을 목적으로 학생들에게 적금을 가입시켜 매월 돈을 불입하게 하고 졸업을 할 때 불입금에 이자를 붙여서 돌려 준다. 또, 군대 내에서도 병사들에게 적금을 가입시켜 봉급을 모을 수 있게 도와주는 사례가 있다.
적금은 이자로써 적지 않은 수익을 얻을 수 있다는 특성 때문에 재테크의 수단으로 이용된다. 적금은 그 특성상 다른 투자 수단에 비해 얻을 수 있는 이익이 적다는 흠이 있으나 그 대신 손실이 발생할 위험이 전혀 없다는 것이 장점으로 작용한다. 적금은 단리로 운용되므로 장기적금은 권장하지 않는다. 3년 이상 장기적금을 계획한다면 1년 단위 적금으로 하여 만기후에 예금으로 바꾸는 등 복리효과가 발생하도록 해야 한다. 저축성보험이 복리로 적용되더라도 불입금 중 일부가 비용으로 차감된 후에 운영되므로 가입시 주의해야 한다.
적금을 불입하다가 어떤 사정에 의해 계약을 취소하고 불입한 금액을 다시 찾아가는 경우가 있다. 이를 해지 또는 해약이라 하며 속된 말로는 '적금을 깬다'라고도 표현한다. 대개 이러한 경우는 이자가 보통예금과 같아진다. (단, 은행에서 지정한 불가피한 사유가 있는 경우는 제외) 정기적금은 정해진 불입횟수와 불입금 모두 지켜야 약정금리를 제공한다.

라. 예금과 적금의 차이

구분		적금	보통예(탁)금/저축예(탁)금
계약 기간		개월 단위 (6, 12, 24 등)	무기한
입·출금	입금	정기적립 자유적립	자유적립
	출금	불가	자유
이자	지급 방식	단리 (단, 정기예금의 경우 만기이자지급식은 복리, 매월이자지급식은 단리이다.)	복리 (대개 보통예금은 6개월, 저축예금은 3개월마다 이자가 '원금에 가산'된다.)
	이율	높음	낮음

II 탐구 내용

□ 단리와 복리

가. 단리란?

단리는 일정한 시기에 오로지 원금에 대해서만 약정한 이율을 적용하여 이자를 계산하는 방법이다. 이때 발생하는 이자는 원금에 합산되지 않기 때문에 이자에 대한 이자가 발생하지 않는다. 따라서 원금에만 이자가 발생한다는 가정하에 단리 계산은 다음과 같이 하면 된다.

$$FV = PV \times [1 + (r \times n)]$$

여기서, FV = 미래가치

PV = 현재가치

r = 수익률 (연이율)

n = 투자기간 (연 단위)

나. 복리란?

복리란 중복된다는 뜻의 한자어 복(復)과 이자를 의미하는 리(利)가 합쳐진 단어로서 말 그대로 이자에 이자가 붙는다는 뜻이다. 따라서 원금과 이자가 재투자된다는 가정하에 복리계산(compounding)은 다음과 같이 계산된다.

$$FV = PV \times (1 + r)n$$

여기서, FV = 미래가치

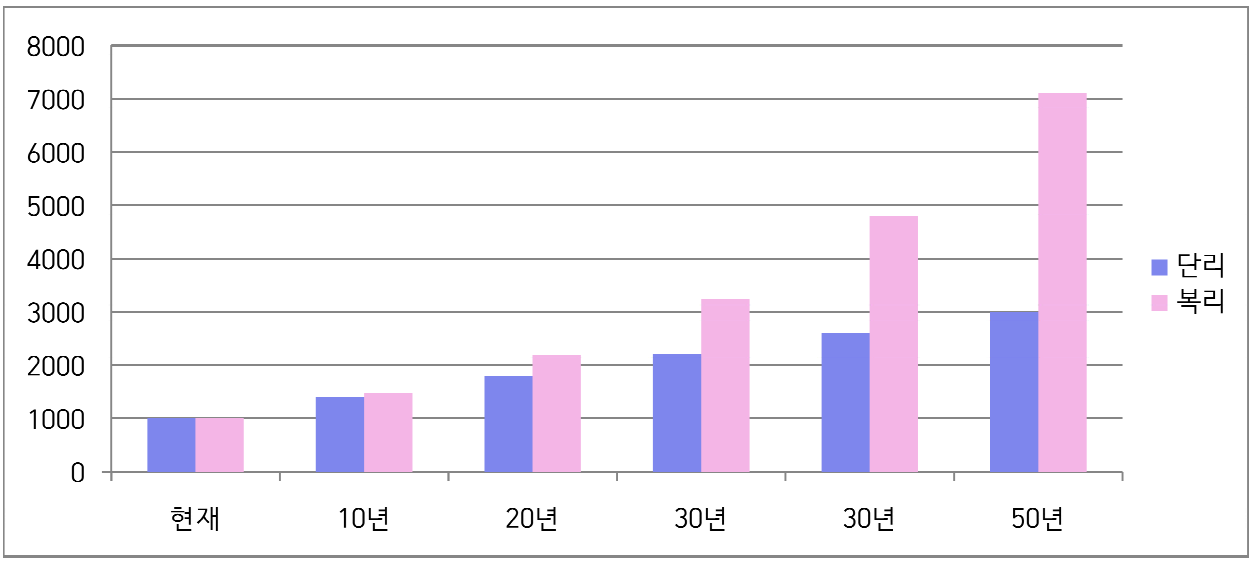
PV = 현재가치

r = 수익률 (연이율)

n = 투자기간 (연 단위)

다. 단리와 복리

일정 금액을 같은 금리의 단리와 복리로 적용했을 때 시간이 흘러 발생하는 원리금에는 차이가 발생한다. 복리는 투자기간이 길어질수록 원리금이 기하급수적으로 증가하며 위력을 발휘하게 된다. 다음 [그림 3-1]은 100만원을 연 4%의 수익률로 투자한 경우 10년 단위로 기간이 길어질수록 투자자산이 증가하는 모습을 보여주고 있다.



단리의 경우는 일정한 비율로 증가하지만 복리의 경우는 초기에는 증가폭이 크지 않지만 기간이 길어질수록 기하급수적으로 증가하여 연 4% 수익률일 때 100만원이 50년 후에는 710만원에 달하게 되어 300만원인 단리의 2배가 넘게 된다.

또한, 투자기간이 긴 경우에는 이러한 복리의 위력이 작은 수익률 차이에도 크게 발생한다. 다음 [그림 3-2]는 100만원을 30년 동안 투자했는데 연 평균 수익률이 각각 4%, 8%, 12%인 경우의 결과를 보여주고 있다. 가장 먼저 눈에 띄는 것은 복리의 경우 투자 결과가 수익률에 비례하지 않는다는 점이다.

예를 들면, 수익률이 연 4%에서 두 배인 연 8%가 되면 3백만원이 1천만원이 되고, 다시 세 배인 연 12%가 되면 투자자산은 거의 30배인 2천 9백만원이 된다. 따라서 장기투자 시에는 단 1%의 수익률 차이가 적지 않은 투자 결과의 차이를 가져오게 된다. 종종 1~2%의 수익률 차이는 대수롭지 않게 보이지만, 이것이 오랜 기간 누적되면 적지 않은 투자성과의 차이를 낳게 된다.

[가설 설정]
1억원을 연 7%의 수익률로 복리 투자했을 때와 연 8%의 수익률로 복리 투자했을 때 5년 뒤와 30년 뒤의 결과는 각각 얼마나 다른가?

1억원을 연 7%의 수익률로 5년 동안 투자한 미래가치는 다음과 같이 계산된다.

1억원×(1+0.07)5 = 1억 4,026만원

1억원을 연 8%의 수익률로 5년 동안 투자한 미래가치는 다음과 같이 계산된다.

1억원×(1+0.08)5 = 1억 4,693만원

따라서 1%의 수익률의 차이가 5년 후 667만원의 차이를 만든다.

1억원을 연 7%의 수익률로 30년 동안 투자한 미래가치는 다음과 같이 계산된다.

1억원×(1+0.07)30 = 7억 6,123만원

1억원을 연 8%의 수익률로 30년 동안 투자한 미래가치는 다음과 같이 계산된다.

1억원×(1+0.08)30 = 10억 627만원

따라서 1%의 수익률의 차이가 30년 후 2억 4,504만원의 차이를 만든다.

결과적으로 복리 효과로 인해 단 1%의 수익률 차이가 투자기간이 길어질수록 얼마나 위력을 발휘하는지를 확인할 수 있다.

[72의 법칙]

72의 법칙은 복리를 계산해 원금이 두 배가 되는 시기를 손쉽게 알아볼 수 있는 법칙이다. 공식은 다음과 같이 간단하다.

72/수익률 = 원금이 두 배가 되는 시기(년)
목표수익률을 정할 때도 72의 법칙을 활용할 수 있다. 만일 10년 안에 원금이 두 배가 되기 위해서는 얼마나 수익을 내야 할까?
'72 나누기 10(년)'을 하면 답은 7.2%(년)가 나온다. 이러한 72법칙을 이용하면 원하는 목표수익률 및 투자기간을 정하는데 도움이 된다. 위에서 언급한 복리는 정기예금에서

운용이 되며, 적금은 단리로 계산이 되므로 적금으로 어느 정도 목돈이 생기면 정기예금으로 전환하여 복리의 효과를 높이는 것이 효율적이다. 장기상품을 선택할 때는 복리가 큰 위력을 발휘한다는 점을 꼭 기억하여야 한다.

[72 법칙 예시]

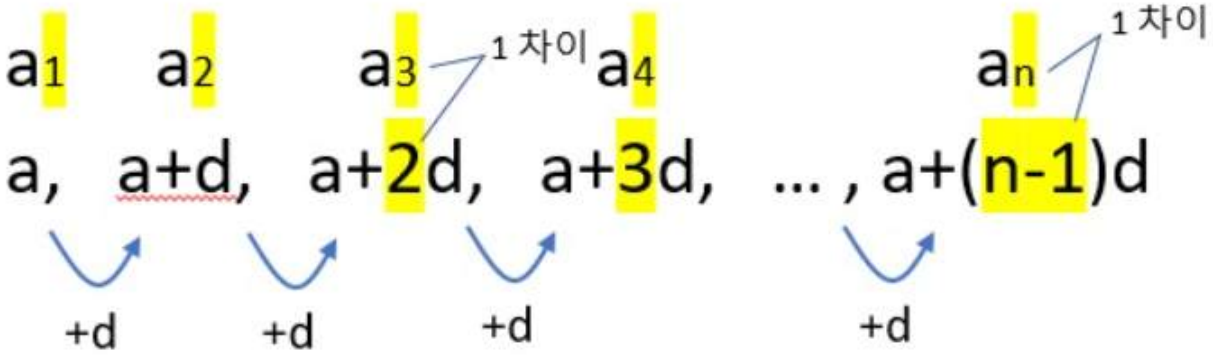
100만원의 돈을 연 5%의 복리상품에 넣는다고 치자. 원금의 2배인 200만원으로 불어나는 시간은 얼마가 걸릴까?

답은 14.4년이다. (72/5=14)

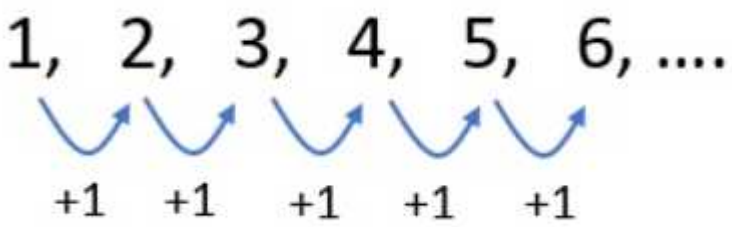
라. 등차수열

앞서 단리와 복리에는 등차수열이 사용되었다고 한다. 등차수열 부분은 아직 배우지 않은 분야이기에 간단히만 짚고 넘어가보았다.

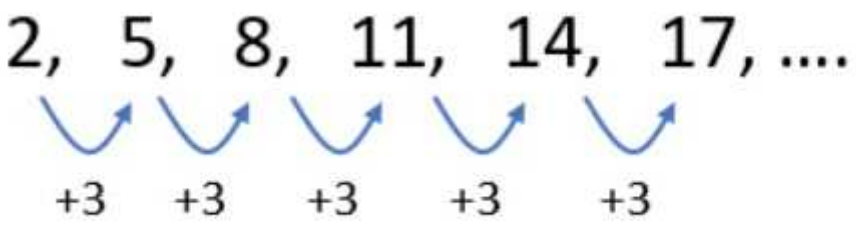
앞의 항에 항상 일정한 수를 더하여 만들어가는 수열이다. 각 항에 더해지는 일정한 수를 '공차'라 한다. 첫째항이 a, 공차가 d인 등차수열은 다음과 같이 전개된다. 더해진 공차의 개수는 수열의 항수보다 하나씩 작으므로, 등차수열의 일반항은 an=a+(n-1)d가 된다.



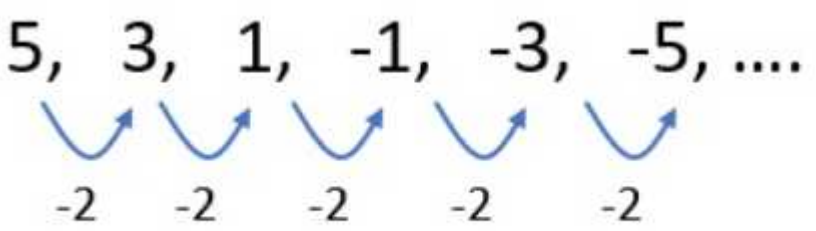
다음 수열은 첫째항이 1, 공차가 1인 등차수열이다. 일반항은 an=1+(n-1)=n이다.



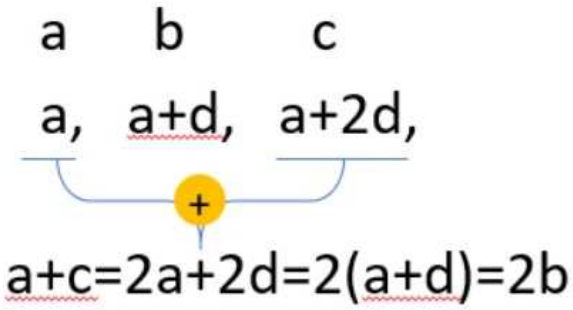
다음 수열은 첫째항이 2, 공차가 3인 등차수열이다. 일반항은 an=2+3(n-1)=3n-1 이다.



다음 수열은 첫째항이 5, 공차가 -2인 등차수열이다. 일반항은 an=5+(-2)(n-1)=-2n+7 이다.



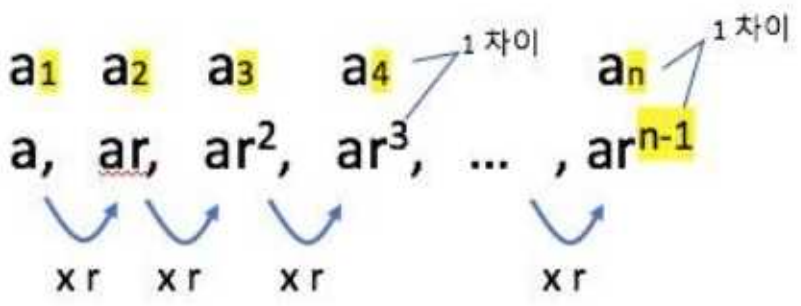
또한 어떤 등차수열의 연속되는 세 항을 a, b, c라고 하면, 이때 b=a+d, c=a+2d가 될 것이다. 여기서 좌우의 항 a와 c를 더하면 가운데 항 b의 값의 2배가 되며, 이를 등차중항이라 한다.



등차중항은 등차수열의 연속되는 세 항뿐 아니라 a1, a5, a9와 같이 동일한 간격으로 떨어져 있는 세 항에도 적용된다.

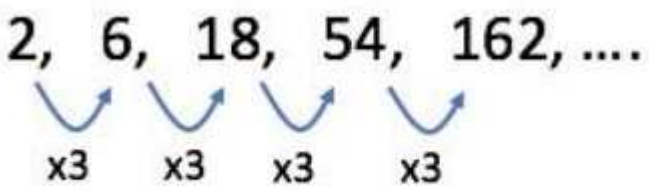
마. 등비수열

등비 수열도 마찬가지로 간단하게만 다루어 보았다.
등비수열은 앞의 항에 항상 일정한 수를 곱하여 만들어가는 수열이다. 여기서 각 항에 곱해지는 일정한 수를 '공비'라 하는데, 첫째 항이 a, 공비가 r인 등비수열은 다음과 같이 전개된다.

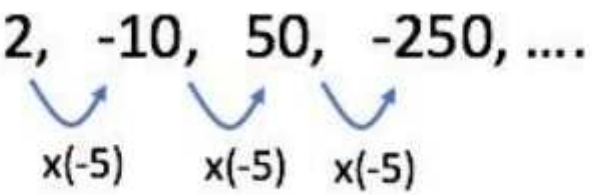


이처럼 곱해진 공비의 개수는 수열의 항수보다 하나씩 작다. 그러므로 등비수열의 일반항은 an=arn−1이 된다.

[예시]



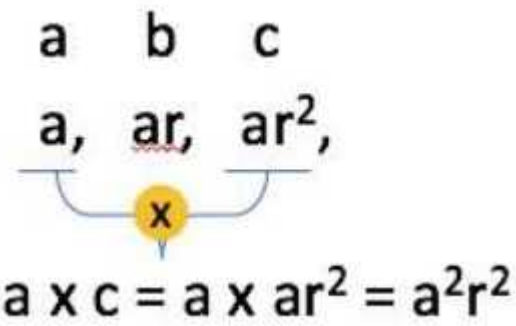
다음 수열은 첫째 항이 2, 공비가 3인 등비수열이다. 일반항은 an=2·3n−1이다.



다음 수열은 첫째 항이 2, 공비가 −5인 등비수열이다. 일반항은 an=2·(−5)n−1이다.

[등비중항]

어떤 등비수열의 연속되는 세 항을 a,b,c라고 하면, b=ar, c=ar2가 될 것이다. 여기서 좌우의 항 a와 c를 곱하면, 가운데 항 b의 제곱이 된다. 이를 등비중항이라 한다.



등비중항은 등비수열의 연속되는 세 항뿐 아니라, a2, a5, a8과 같이 동일한 간격으로 떨어져 있는 세 항에도 적용된다.

3 탐구 결론

□ 활동 후 느낀 점

[10305 김예담]

사회시간에 배운 내용을 수학으로 연계해서 궁금했던 점을 더 자세히 알아볼 기회가 되어 좋았고, 실생활에서 유용한 정보를 얻은 것 같아 앞으로 저축을 할 때 많은 도움이 될 것 같다. 단리 복리에서 나오는 등차수열 등비수열은 2학년 때 배우게 될 내용인데 미리 알아본 것 같아서 뿌듯하기도 했고, 마치 은행원이 된 것 같은 느낌까지 들었다. 무엇보다 조사한 내용을 가시적인 그래프로 만들어보면서 다른 사람에게 설명까지 해보니 더욱 이해가 잘 되고 오래 기억에 남게 되었다. 나중에 다른 친구들에게도 단리와 복리에 대해 쉽게 설명해 줄 수 있을 것 같아 더욱 뿌듯하고 인상깊었던 시간이었다.

[10312 박현선]

아직 등차수열 등비수열을 배우지 않았음에도 복리와 단리에 대해 조사를 하면서 그 개념을 알게 되었다. 단리와 복리에 대해 간단한 개념정도는 알고 있었는데 이를 수식으로

표현해보니 그 원리가 새롭게 느껴졌고 이해하기에도 쉬웠다. 특히 직접 우리가 예금 상황을 가정해서 단리와 복리를 적용하여 직접 계산해보는 것은 단리 복리의 원리를 확실히 이해하도록 도와주었다. 만약 2학년 때 등비수열 등차수열에 대해 배울 때 수학 탐구 대회를 준비하며 공부한 단리와 복리의 원리가 도움이 될 것 같다. 우리의 일상 곳곳에 수학이 녹아 있다는 것을 새삼 다시 느끼게 되었고, 앞으로 예금이나 적금 때문에 은행에 가게 된다면 단리 복리의 원리를 이용해 보아야겠다는 생각을 했다.

[10318 이가현]

저는 이 보고서를 작성하면서 평소에 잘 모르고 있었던 은행 예금을 공부할 수 있었다. 평소 사회시간이나 수학 시간에 예금 문제가 응용되어 나오거나 이런 경제 이야기를 다루는 내용이 나오면 항상 어려워했었는데, 이번 기회에 다양한 자료들을 조사하며 접해보면서 이 내용에 관하여 확실히 알 수 있었던 것 같다. 또 단리와 복리의 장단점을 확실히 알 수 있었다. 예를 들어 단리는 기간이 짧은 대신 이자율이 적고 복리는 기간이 긴 대신 이자율이 높다는 것이다. 저는 이것을 조사하며 나중에 어른이 되었을 때 어떤 경우에는 단리를 들지 복리를 들지 계산할 수 있겠다는 생각이 들었고 그리고 저희의 주제인 예금으로 부자 되는 방법은 엄청 많은 돈을 예금해야 부자가 될 수 있겠다고 생각했다. 왜냐하면 단리를 하던 복리를 하던 원금의 이자를 주는 것이기 때문에 처음에 예치시키는 돈이 많아야 그 이자가 많을 것이기 때문이다.

[10326 정혜민]

수학의 다양한 분야들 중에서도 경제 분야의 수학을 탐구하게 되었는데, 확실히 본래 알고 있던 지식과 연계하여 탐구를 진행해보니 기억에도 오래 남고 이해도 빨리 된 것 같다. 미래의 경제 주체가 될 우리들에게 뜻깊은 시간이 된 것 같고, 나중에 은행에 가서도 영리하게 저축을 할 수 있을 것 같다. 만약 다른 친구들에게 이 개념들을 설명해 줄 수 있는 시간이 있다면 먼저 앞장서서 이 개념을 알기 쉽게 설명해 줄 수 있을 것 같은 자신감까지 생기게 되었다. 경제라는 것이 인간이 살아가면서 떼어놀 수 없는 분야인데 경제에 대한 친밀감도 기를 수 있었고, 2학년때 배울 등차수열, 등비수열에 관해서도 접할 수 있어서 나중에 겪을 수열에 대한 거부감을 줄일 수 있었던 것 같다.

개밥 바라기(금성) 관측기

분야 : 주제탐구
10110 김은서, 10203 김다은, 10206 김예나

1. 탐구 및 작품 제작 동기

누구나 한 번쯤은, 지구에서 가장 빛나는 별, 개밥 바라기 별, 즉 금성에 대해 들어보았을 것이다. 많은 이들이 이 별을 더 오래, 더 많이 보기 위해 특별한 장소를 찾아가고 장비를 구매한다. 궁금증과 호기심이 많은 우리도 별을 보고 싶지만, 돈과 시간, 학생이라는 신분 등 모든 측면에서 제한을 받기에 '과학적 원리를 이용하여 별을 볼 수는 없을까?' 하는 의문이 들었다. 그러다 우연히 국어의 비문학 지문에서 동방, 서방, 최대이각에 대해 알게 되었고, 이 원리에 대해 탐구를 해보고, 삼차원 공간에서 각도를 이용해 오랫동안 별을 관측해보고자 한다.

2. 배경지식 탐색

1) 공전 주기 : 금성-225일, 지구-365일/공전 방향 : 반시계
2) 태양과의 거리비 - 금성:지구=0.7:1
3) 두 행성의 궤도면은 같은 평면 상에 존재하지 않는다
   ->지구와 금성의 궤도면 각도차: 약 3.4도
4) 궤도 이심률 : 물체가 완벽한 원 궤도에서 벗어나 있는 정도를 수치화한 것
   (0<=물체의 이심률<=1)
   ->금성 이심률 : 0.00677323
   지구 이심률 : 0.0167
   두 행성 모두 궤도가 거의 원형에 가깝다(금성 궤도가 상대적으로 더 원에 가까움)
5) 금성과 지구, 태양의 위치 관계
   -이각 : 태양-지구-내행성이 이루는 각도
   -동방/서방 최대 이각 : 각각 지구의 동쪽과 서쪽에서 이루어지는 최대 이각이다. 최대 이각이 이루어질 때 금성을 가장 오랫동안 관측할 수 있다
   -내합 : 태양-금성-지구가 일직선 상에 있는 상태
   -외합 : 금성-태양-지구가 일직선 상에 있는 상태
6) 근일점/원일점 : 타원 궤도에서 중심과 가장 가까운 거리/먼 거리
   ->금성의 근일점 : 약 0.718AU / 원일점 : 약 0.728AU
   지구의 근일점 : 약 0.983AU / 원일점 : 약 1.0167AU

3. 가구에 적용된 수학 원리

-태양 주위를 공전하는 금성과 지구의 궤도 모방
->지구 궤도 내 태양 위치, 금성 궤도 내 태양 위치 계산
-각속도 방정식을 통해 세 천체가 내합, 외합, 최대 이각을 이루는 시간 계산

4. 작품 제작 과정

1. 필요한 준비물을 모두 구비 한다.
   - 우두락
   - 철사
   - 칼, 가위, 자 등
   - 스타이로폼 공(사이즈 별로, 대1, 중1, 소1)
   - 압정(고정)
   - 채색도구 및 점토 등 꾸밀 것
2. 철사 2개로 각각 다른 크기의 천체 공전 궤도 모형을 만든다.
3. 각각의 스타이로폼 공으로 태양, 지구, 금성 모형을 만든다.
4. 우두락 판 위에 압정과 다른 철사를 이용해 앞서 만든 공전 궤도 모형을 고정시킨다.
   ※ 고정 시킬 때에는 크기가 큰 궤도 안에 크기가 작은 궤도가 들어가도록함.
5. 크기가 작은 궤도 안, 정 중앙에 태양을 철사로 고정시킨 후, 금성과 지구 모형을 궤도 모형에 끼워넣는다.
6. 우두락으로 각도기를 만든 뒤, 천체를 이동시키며 동방, 서방 최대 이각 등을 관찰한다.

5. 사용법

천체 모형들을 이동시키며, 우드락으로 만든 각도기를 이용해 변하는 모습들을 관측한다. 제작할 때, 천체들의 공전 궤도를 고려하여 만들었으므로 내합,외합을 이루는 위치, 최대 이각을 이루는 모습을 관측할 수 있다. 이때, 관측한 모습을 탐구 전에 예측했던 모습과 비교하며 관찰을 한다.

6.느낀 점

국어 모의고사를 풀던 중 지문에 나온 동방·서방 최대 이각 등의 내용이 이전의 별에 관한 우리의 호기심과 결합하여 이러한 작품을 만들게 되었다. 지문을 통해 원리를 익히는 것은 금방 할 수 있었다. 하지만, 모형을 만들기 위해 어떻게 해야 할지 몰라 어려움이 있었다. 그렇지만, 서로 머리를 맞대고, 실제 행성 궤도 모형들을 찾아보고, 책과 인터넷 등을 참고하여 천체의 운동에 대하여 탐구하고, 수학적 규칙을 분석함으로써 우리만의 개 밥바라기 관측기를 만들 수 있었다. 만들기까지 어려움도 많았지만, 그렇기 때문에 천체의 운동 내용이 더 오래 기억에 남을 것 같다.

들어 봤냐!? 이런 이차함수

- 포물선의 방정식을 활용해보자 -

분야 : 수학교구

10720 이상혁, 10801 구현모, 10821 전종호, 10823 최건호

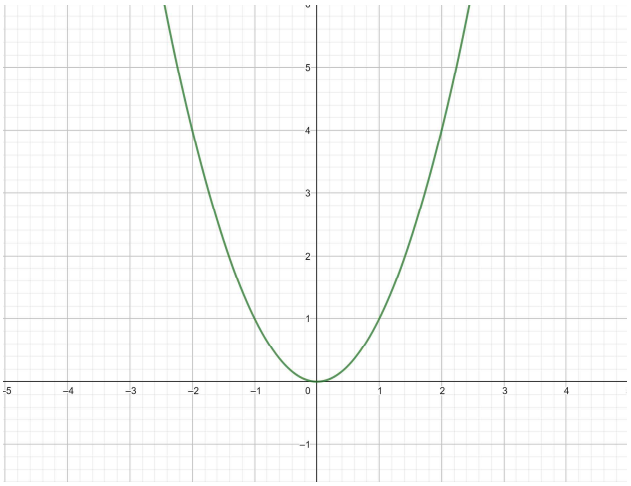
탐구동기

우리는 1학기 때, 이차방정식을 활용한 이차함수에 대해서 배웠었다. 수업시간에 선생님들께서 칠판에 이차함수를 일일이 그리시는 것을 보며 만약에 이차함수를 그리는 도구가 있으면 어떨까? 하는 막연한 생각을 했었다. 방학 동안, '수학, 인문으로 수를 읽다'라는 책을 읽었는데, 우연히 기하학의 포물선에 대해서 알게 되었다. 이에 흥미가 생겨서 이 분야에 대해 더 탐구해봤고, 이 포물선을 회전시키면 우리가 아는 이차함수가 되지 않을까 하는 발상을 했다.
따라서 우리 조는 포물선을 활용한 이차함수 그리는 도구를 기획하게 되었다.

탐구내용

§1. 이차함수에 대한 내용 복습

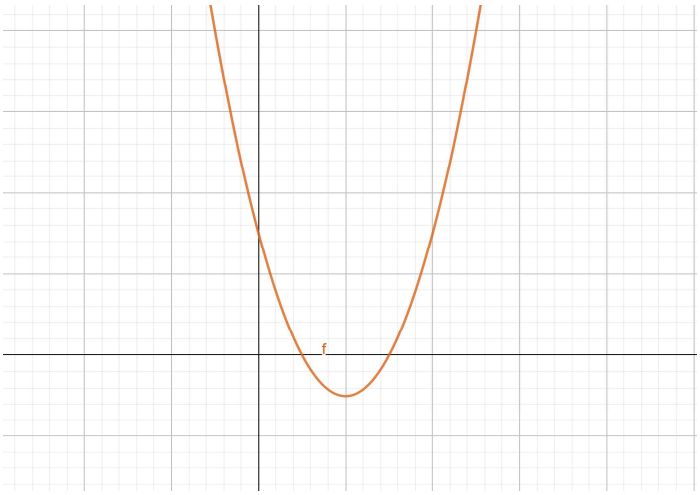
다음은 $y=x^2$ 의 그래프인데, 우리는 이미 배운 내용을 통해서 이 내용을 알아낼 수 있다.



$y=x^2$ 의 그래프 개형은 아래로 볼록 형태이다.
$y=x^2$ 의 축의 방정식은 $x=0$, 즉 y축이다.

(축의 방정식이란, 이차함수 그래프가 대칭이 되는 기준 직선을 의미한다.)
$y=x^2$ 의 꼭짓점은 (0,0) 이다.
$y=x^2$ 과 x축 (y=0) 의 교점은 (0,0) 하나로, 두 그래프는 한점에서 접한다.
(판별식 D를 통해서 교점의 개수를 파악할 수 있다.)

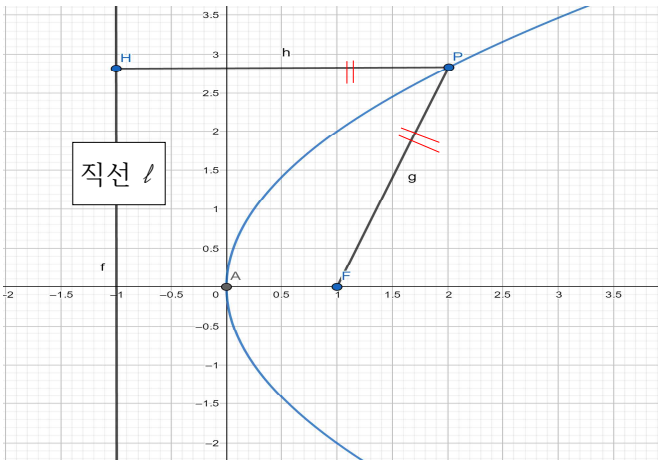
다음은, $y = a(x-p)^2 + q$ 의 그래프이다. (단, a>0)
우리는 $y=x^2$의 그래프를 활용하여 이 그래프에서 다음과 같은 정보를 알아낼 수 있다.



이 그래프의 개형은 아래로 볼록 형태이다. (∵a>0)
이 그래프의 축의 방정식은 x=p 이다.
이 그래프의 꼭짓점은 (p,q)이다.
이 그래프는 x축과 두 점에서 만난다. -> 판별식 D >0 이다.

§2. 포물선에 대해 탐구

다음은, $y^2=4px$의 그래프이다 (p=1)

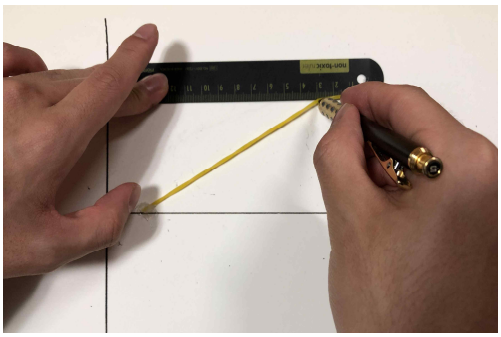


먼저, 포물선이란 위 그림처럼, 선분PF와 선분PH를 만족하는 점 P의 집합이다.
포물선에서 정점 F를 포물선의 초점, 정직선 l을 포물선의 준선이라고 하며, 포물선의 초점 F

를 지나고 준선 l 에 수직인 직선을 포물선의 축, 포물선과 축의 교점을 포물선의 꼭짓점이라고 한다.

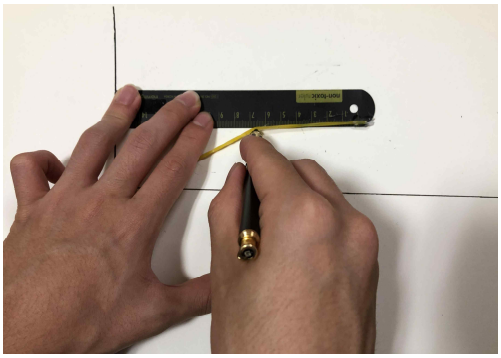
§3. 포물선을 그리는 도구 제작

우리는 먼저 이 포물선을 그리는 도구를 고안했다.



1. x축과 준선을 그린다.
   (y축은 편의상 제외)

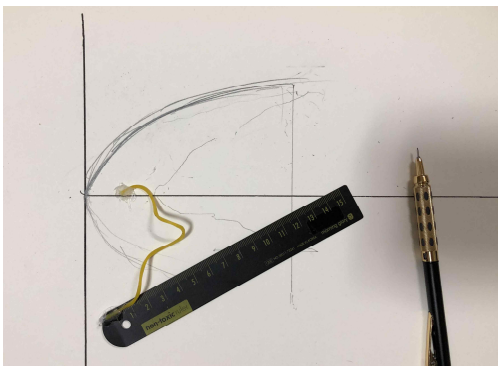
2. 자의 한 끝을 준선에 맞추고
   자의 반대쪽 한 끝에 고무줄을 고정시킨다.



3. 반대쪽 고무줄의 한 끝은
   포물선의 초점이 될 점 F에 고정시킨다.

4. 샤프로 고무줄이 팽팽하도록 당기고,
   자를 천천히 아래쪽으로 내린다.

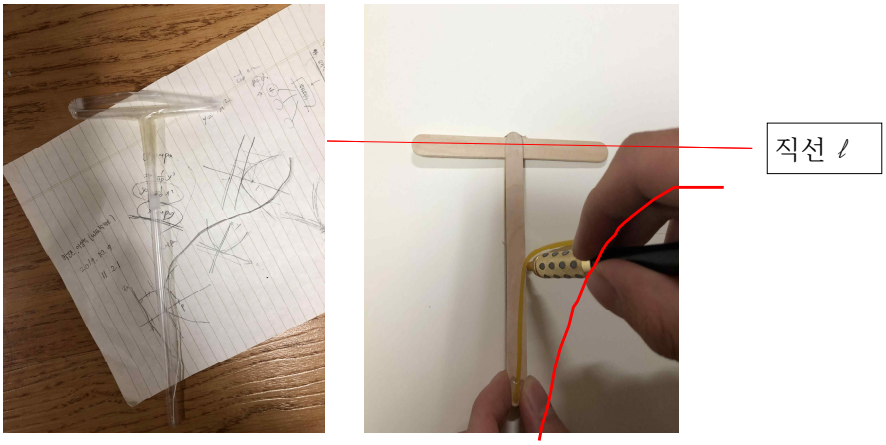
5. 그림이 더 이상 안그려질 경우에는,
   자를 뒤집어서 반대로 그린다.



6. 포물선 완성

포물선을 작도한 이후, 우리는 이 포물선을 90도 회전시켜서 그리면 이차함수가 될 것이라는 발상을 하게 되었다. 따라서 우리는 포물선을 90도 회전시켜서 그릴 수 있는 새로운 도구를 고안했다. 나무젓가락과 빨대를 이용하여 총 두 가지의 버전으로 도구를 만들어봤다. 모양은 알파벳 T에 고무줄을 고정시킨 것으로 동일하다.

§4. 이차함수를 그리는 도구 제작



이렇게 도구를 제작했을 때, T자에 고정하지 않은 고무줄의 한 쪽 끝을 F초점으로 설정하고, 고정시킨다. 고무줄을 팽팽하게 유지하면서 T자의 윗부분을 수평방향으로 이동시키면서 그림을 그리면 직선 l이 준선인 포물선이 그려진다. 위로 볼록 형태의 이차함수 모양이다.

§5. 포물선을 이차함수로 전환

$y^2=4px$ 그래프를 $y=x$ 직선 대칭 시킨 그래프, 즉 역함수 그래프를 구해보자.
x에 대해서 정리하면, $x=y^2/4p$
$\therefore$ $y=x^2/4p$ 이다.
즉, 초점이 $(p,0)$인 포물선을 이차함수로 바꾸면, 이차계수가 $1/4p$인 이차함수가 된다.

§6. 탐구의 기대효과

보통 이차함수 그래프를 그릴 때, x값에 간단한 정수를 넣어 대응되는 y값을 구한 후 점들을 연결하는 방법으로 곡선을 그린다. 또한 이차함수에서 이차항의 계수의 부호를 판별하고, x절편과 y절편을 파악하고 그 점을 찍어서 이차함수의 그래프를 그리기도 한다. 제시한 이 두 가지 방법은 우리가 흔히 알고 있는 통념일 것이다. 하지만 컴퓨터가 아닌 이상, 이차함수의 모든 점들을 좌표평면에 정확히 나타내어 그리는 것은 거의 불가능에 가깝다. 게다가 학교에서 친구들 간에 수학 문제를 서로 풀어줄 때, 그래프를 다 그리고 난 후, 살펴보는 과정에서

잘못 그려진 그래프가 조건과 맞지 않아 다시 그리는 경우도 종종 있다. 이러한 문제점들을 해결하기 위해서 우리 조는 더욱 더 정확하고 빠르게 이차함수 그래프를 그려낼 수 있도록 포물선의 방정식을 이용한 t자 모양의 도구를 만들어냈다. 이 t자 모양의 도구를 사용한다면, 앞으로 이차함수의 그래프를 그려서 설명해야 하는 문제를 마주쳤을 때, 보다 더 정확한 이차함수 그래프 개형을 표현해낼 수 있을 것이다. 이 도구를 사용하면 문제의 조건과 맞지 않는 상황이 생겨서 그래프를 다시 그려서 판단해야 하는 부득이한 상황을 피할 수 있을 것이다. 수학을 가르치는 분야와 관련된 분들에게 유용한 도구가 될 것이라고 생각한다.

내 옆에 수학이 있다고?

분야 : 수학신문
10106 김서연, 10126 이재영, 10229 최영주, 10315 안세희

[대회에 참가한 이유]

대부분의 사람들에게 수학이라는 분야를 떠올리게 한다면 '수학문제를 푼다.' 라고 생각할 것입니다. 이를 통해 지루하다 느낄 수도 있고 어렵다고 느낄 수 도 있을 것입니다. 그러나 일상생활 속에서 쓰이는 수학적인 요소나 신기하고 독특한 방식으로 수학 문제를 풀어나가는 법을 안다면 그 전보다는 더 재미있게 수학을 바라 볼 수 있을 것입니다. 이번 수학 탐구 활동을 통해 수학에는 문제풀이 뿐만 아니라 다양하고 창의적인 요소가 있다는 것을 알고 수학에 더욱 흥미를 가지기 위해 참여하였습니다.

[많은 주제 중 신문을 선택한 이유]

신문은 여러 가지 시사에 관한 뉴스를 비롯한 정보 ·지식 ·오락 ·광고 등 많은 내용을 한 번에 전달할 수 있는 통신수단입니다. 이런 장점을 이용해서 우리는 한 분야가 아닌 여러 분야를 소개해 줄 수 있는 신문을 선택하게 되었습니다. 또한 학생들이 수학을 어려워하는데 이러한 창의적인 요소를 알리고 신문을 통해 많은 학생들이 관심을 가지면 좋겠다고 생각합니다.

[내용 선정 이유]

저희가 살면서 흔히 지나치는 일들이 자세히 보면 수학적 요소가 함유되어 있음을 인식하고 흥미로운 요소들을 알리면서 많은 학생들이 관심을 가질 수 있고, 주변에 있는 일이자 궁금했다며 공감할 수 있는 내용으로 주로 선정하였습니다. 또한 수학이 대학에 진학하는 데에만 필요한 과목이 아닌 우리가 평소에도 자연스럽게 쓰고 볼 수 있는 과목임을 알리고 싶었습니다.

[내용]

인도수학	주변 사람들이 잘 모르는 독특한 수학 풀이 법을 소개하고자 하여 인도수학에 대해서 소개하려 합니다. 인도수학을 통해서는 덧셈, 뺄셈, 곱셈 등의 연산을 독특한 방법으로 할 수 있습니다. 저희 조는 인도수학의 여러 가지 연산중에서 두 가지를 소개할 것입니다. 그 두 가지는 겔로시아 곱셈법과 선긋기를 이용한 곱셈법이고, 이를 통해 곱셈 (두 자릿수 x 두 자릿수) 을 독특한 방식으로 하는 방법을 신문에 소개하려 합니다. 신문에서 직접 인도수학을 사용하여 곱셈을 하는 예시 작성하여 인도수학에 대해 더 쉽게 이해할 수 있도록 소개할 것입니다.
안경과 렌즈의 도수 차이점이 발생하는 이유	시력을 교정하기 위해서 안경과 렌즈를 사용하는데 도대체 왜 안경도수와 렌즈도수가 다를까하는 의문점이 듭니다. 안경 도수와 렌즈 도수가 다른 이유는 정점간거리 (안경렌즈와 눈 사이에 해당하는 거리) 가 있는데 바로 이 12mm 때문에 발생합니다. 안경렌즈는 콘택트렌즈도수 = 안경도수/(1-0.012X안경도수) 인데, 따로 환산표가 있다고 합니다. 환산표는 근시용과 난시용이 따로 있는데, 이 표를 보는 방법은 안경 굴절 검사 값을 기준으로 봅니다. 예를 들어 렌즈도수가 근시용 -7.00일 경우 그에 해당하는 근시용 표를 보면 -6.50으로 계산이 되는 것 입니다.
수학 경시 대회	글로벌 영재학회에서 주관하는 수학 경시대회는 초등학교 1학년 ~ 고등학교 2학년을 대상으로 하고 있으며 반드시 자신의 학년에 맞게 응시하는 것이 원칙입니다. 접수방법으로는 전국 각 지정접수처인 전국 종로학원하늘교육 학원에 방문하여 접수처에 비치된 지원서를 작성 후 접수하는 방법과

	응시료를 우편환으로 교환 후 동봉하여 응시원서와 함께 발송하는 고사 진행본부 우편 접수방법 그리고 홈페이지에서 회원가입 후 접수하는 인터넷 접수방법이 있습니다. 구비서류로는 지원서와 응시료 (과목당 45,000원) 가 있습니다. 응시자 준비물로는 수험표, 컴퓨터용 수성사인펜(흑색)이 있습니다. 성적은 지원서에 기재한 주소지로 발송됩니다. 출제 범위는 해당 학년 1학기 전 범위 ~ 2학기 9월 말 범위까지입니다. 초등 1학년을 제외한 나머지 학년은 이전 학년까지의 모든 범위를 포함하고 있습니다. 문항은 총 초, 중, 고 구분 없이 각 30문항입니다. 문제는 개념적 지식, 절차 식 지식, 추론능력, 문제 해결력 등 4개 영역으로 구분되어 있으며 단순한 계산보다는 영역 간의 상호 관련성 있는 문제를 출제합니다. 시험시간은 전 학년 모두 90분입니다. 고사장은 전라북도에는 유일하게 전주 한일 고등학교에서 이루어집니다.

[느낀 점]

중학교, 고등학교 때 계속 수학이라는 과목을 배워오면서 항상 수학을 배울 때마다 “이걸 커서 어디에 쓰지” 라는 생각과 함께 늘 어렵고 머리 아픈 것만 생각해왔는데 이번 수학 탐구 대회에서 일상생활에서 쓰이는 수학이라는 주제를 통해서 더 알고 싶어지는 계기가 되었습니다. 또 신문에 쓸 내용 중에서 인도수학에 대해 조사를 해보았는데 조사하기 전에 알고 있었던 내용뿐 아니라 다른 방법에 대해서도 알 수 있어서 좋았습니다. 이런 신기한 방법이 있다는 것이 흥미로웠고, 경시대회라는 주제는 나의 수준을 알아볼 수 있는 좋은 시험인 것 같다고 느꼈으며, 기회가 되면 저희도 참여해보고 싶다고 생각했습니다. 이번 수학 탐구 대회를 통해 수학은 일상생활 속 곳곳에 사용되고 있으며 저희가 생각한 것보다 더 일상생활에 스며들어 있다는 것을 알게 되었습니다. 수학에 더 흥미를 가질 수 있는 좋은 기회인 것 같다고 느꼈습니다.

CODE 호제!

분야 : 주제탐구
10201 곽유란, 10212 신수연, 10215 오정효, 10218 윤아라

Ⅰ 서론

많은 사람들이 21세기를 정보화시대라고 한다. 지난 세기에 탄생한 컴퓨터가 짧은 시간에 눈부신 발전을 거듭하면서 인간의 생활양식을 급격히 변화시키고 있다. 그러한 변화 중 가장 중요한 것이 바로 인터넷의 출현이라고 할 수 있다. 모든 것이 정보화되고 그 정보들이 인터넷을 떠다니고 있다.

정보화시대가 도래하면서 정보의 관리, 특히 정보의 보호가 매우 중요한 과제가 되었다. 국가, 회사, 단체 또는 개인이 반드시 보호해야 하는 비밀정보가 보호되지 못한다면 큰 문제가 될 것이다. 거꾸로 그러한 비밀정보를 반드시 알아내야 하는 쪽에서는 그 정보를 알아내기 위하여 필사적인 노력을 경주할 것이다. 이러한 정보전쟁에서 우리가 어느 편에 속하게 될지는 모르는 일이다. 우리가 개발한 신기술 정보를 지켜야하는 입장이 될 수도 있고, 테러집단의 비밀정보를 알아내야 하는 입장이 될 수도 있는 것이다.

암호는 이처럼 비밀정보를 교환하기 위하여 생겨났다. 처음에는 주로 군사용으로 사용되었으나 최근에는 전자상거래를 비롯하여 전자우편이나 휴대전화에 이르기까지 그 응용범위가 확대되고 있다. 수학은 이러한 암호의 이론적 토양을 제공할 뿐만 아니라 다양한 암호체계를 만들고 이렇게 만들어진 암호체계의 효용성과 안전성을 분석하는 암호기술의 핵심적인 도구 역할을 담당하고 있다. 이러한 연유로 암호이론과 기술은 이제 수학의 한 분야로 간주되고 있다.

Ⅱ 본론

가. 암호의 정의

1) 암호 기술이란

암호기술은 중요한 정보를 읽기 어려운 값으로 변환하여 제 3자가 볼 수 없도록 하는 기술입니다. 암호기술의 안전성은 수학적인 원리에 기반하며, 보안에 있어서 중요한 정보를 직접적으로 보호하는 원천기술 입니다.

암호기술을 통해 보호하고자 하는 원본 데이터를 평문(plaintext)라고 하며, 평문에 암호기술을 적용한 것을 암호문(ciphertext)라고 합니다. 이렇게, 평문에 암호기술을 적용하여 암호문으로 변환하는 과정을 암호화라고 하며, 다시 평문으로 복원하는 과정을 복호화라고 합니다. 암호화하기 위해서는 암호 키(key)가 필요하며, 키가 있어야만 암호문을 복호화할 수 있습니다. 그렇

게 때문에 암호 키는 비밀(secret)로 유지되어야 하며 제3자가 알 수 없어야 합니다.
암호기술을 이용하여 데이터 기밀성, 데이터 무결성, 인증 및 부인 방지 등의 기능을 제공할 수 있습니다

2) 암호의 특성
- 기밀성

허락되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 성질
- 무결성

허락되지 않은 사용자 또는 객체가 함부로 수정할 수 없도록 하는 성질
- 인증

사용자 또는 객체의 디지털 정체성을 식별
- 부인방지

정보를 보낸 사람이 나중에 정보를 보냈다는 것을 부인하지 못하도록 함

나. 암호의 종류

1) 대칭키

대칭키 암호(Symmetric-key Cryptography)는 암·복호화에 같은 암호 키를 사용하는 알고리즘이며, 송신자와 수신자는 암호 키가 노출되지 않도록 비밀로 관리해야 합니다. 대칭키 암호는 내부 구조가 간단한 치환과 전치의 조합으로 되어 있어 연산 속도가 빠르다는 장점이 있습니다. 하지만, 송·수신자 간에 동일한 키를 공유해야 하므로 많은 사람들과의 정보 교환 시 많은 키를 관리해야 하는 어려움이 있습니다.

블록 암호　　블록 암호(Block Cipher)는 평문을 고정된 크기의 블록단위로 암·복호화를 수행하며, 각 블록마다 동일한 키가 사용됩니다. 블록 암호는 고정된 크기로 평문을 나누기 때문에, 원하는 길이를 맞추기 위하여 패딩(padding)이라는 기법을 이용합니다. 또한, 하나의 키로 여러 블록을 안전하게 처리하기 위하여 운용 방식(mode of operation)이라는 절차를 이용합니다.

Shannon의 암호 이론에 의하면 전치와 환자를 반복시켜 평문의 통계적 성질이나 암호 키와의 관계가 나타나지 않아 안전한 암호를 구성할 수 있습니다. 대표적인 블록 암호 알고리즘으로는 국산 알고리즘인 SEED, HIGHT, ARIA, LEA와 외산 알고리즘인 DES, AES 등이 있습니다

스트림 암호　스트림 암호(Stream Cipher)는 평문과 동일한 길이의 키스트림(key stream) 수열을 생성하여, 평문과의 XOR연산을 통하여 암·복호화를 수행합니다. 키스트림 수열을 생성할 때, 평문과 독립적으로 생성하는 경우를 동기식 스트림 암호라고 하며, 반대로 평문이 키스트림 수열에 영향을 미치는 경우를 비동기식(혹은 자기동기) 스트림 암호라고 합니다. 구현 여건이 제약되는 환경에서 구현이 용이하며, 무선 통신 등의 환경에 주로 사용된다. 대표적인 스트림 암호 알고리즘으로 RC4, A5/1, A5/2 등이 있습니다.

2) 비대칭키

공개키 암호　비대칭키 암호는 공개키 암호라고도 하며, 대칭키 암호와 달리 암?복호화에 서로 다른 키를 사용하는 알고리즘입니다. 송신자는 수신자의 공개키를 이용하여 암호화하며, 수신자는 자신의 공개키로 암호화된 암호문을 자신의 개인키로 복호화할 수 있습니다. 공개키 암호는 수학적인 난제를 기반으로 설계되어 있고 암복호화에 복잡한 수학 연산을 사용하기 때

문에, 대칭키 암호에 비해 효율성이 떨어질 수 있습니다. 하지만, 여러 송신자가 하나의 공개키로 암호화를 수행하기 때문에 사용자가 많더라도 키를 관리하는 데에 유리합니다. 대표적인 알고리즘으로 RSA, ElGamal, ECC 등이 있습니다.
전자 서명 전자 서명은 인터넷 상에서 본인임을 증명하기 위해 서명을 하는 수단으로, 공개키 암호를 거꾸로 활용하는 방식입니다. 전자 서명 알고리즘으로 DSA, RSA SIgnature, ECDSA 등이 있습니다

3) 해시 함수
해시 함수(Hash Function)는 임의의 길이의 메시지를 입력으로 받아 고정된 길이의 해시 값을 출력하는 함수입니다. 해시 함수에는 암호 키가 사용되지 않기 때문에, 같은 입력에 대해서 항상 같은 해시 값을 얻을 수 있습니다. 이러한 성질로 인해 입력 메시지에 대한 변경할 수 없는 증거 값을 만들어냄으로서, 주로 무결성을 제공하는 목적으로 사용됩니다.
안전한 해시 함수는 역상 저항성, 제 2 역상 저항성, 충돌 저항성을 가져야 합니다.

- 역상 저항성 어떤 해시 값에 대하여, 원래 입력 값을 찾는 것이 어려워야 하며, 이를 일방향성(One-wayness)이라고도 합니다.
- 제 2 역상 저항성 어떤 입력 값에 대하여, 그 입력값의 해시 값과 같은 해시 값을 같은 또다른 입력값을 찾는 것이 어려워야 합니다.
- 충돌 저항성 같은 해시 값을 갖는 두 입력 값을 찾는 것이 어려워야 합니다.

다. 암호의 역사
1) 고대 암호
고대 봉건 사회에서는 황제나 군주가 지방 관리에게 보내는 비밀문서, 전쟁 중의 작전 지시와 보고, 첩자들과의 통신 등 전쟁이나 첩보 시에 정보를 전달해야 하는 경우에 다양한 비밀 통신 기법들이 사용되었다. 예를 들어, 멀리 기밀 정보를 전달해야 하는 경우에는 사자의 머리를 깎고 메시지를 쓴 후 머리를 길러서 보내면 받는 측에서는 사자의 머리를 깎고 메시지를 읽도록 하였다.
또 종이에 쓴 메시지가 그냥 보이지 않지만 불빛에 약품 처리를 하면 메시지가 나타나도록 하는 방법, 비밀 노출을 방지하기 위해 말로 전달하도록 하는 방법 등이 다양하게 사용되었다. 이러한 비밀 통신 방법을 스테가노그래피(Steganography)라고 하는데 적들도 이 통신 방식을 알고 있으면 비밀을 유지하기 어렵다는 한계를 갖고 있다.

- 스키테일 암호

기원전 400년경 고대 그리스의 군사들은 스키테일 암호라고 불리는 전치 암호(Transposition cipher, 문자의 위치를 서로 바꾸는 암호)를 사용한 기록이 있다. 특정 지름을 갖는 막대에 종이를 감고 평문을 횡으로 쓴 다음 종이를 풀면 평문의 각 문자는 재배치되어 정보를 인식할 수 없게 되는데, 암호문 수신자가 송신자가 사용한 막대와 지름이 같은 막대에 종이를 감고 횡으로 읽으면 평문을 읽을 수 있다. 여기서 막대의 지름은 송신자와 수신자 사이에 공유된 비밀키가 된다.

• 시저(Caesar) 암호

로마의 황제였던 줄리어스 시저(Julius Caesar)는 시저 암호라고 불리는 환자 암호(substitution cipher, 문자를 다른 문자로 치환하는 암호)를 사용하였다. 시저는 가족과 비밀 통신을 할 때 각 알파벳순으로 세자씩 뒤로 물려 읽는 방법으로 글을 작성했다. 즉 A는 D로, B는 E로 바꿔 읽는 방식이었다. 수신자가 암호문을 복호화하려면 암호문 문자를 좌측으로 3문자씩 당겨서 읽으면 원래의 평문을 얻을 수 있다. 송신자와 수신자는 몇 문자씩 이동할지를 비밀키로 하여 바꿔가면서 사용할 수 있다.

시저는 브루투스에게 암살당하기 전 가족들로부터 다음과 같은 긴급 통신문을 받았다. 시저가 받은 편지에는 'EH FDUHIXO IRU DVVDVVLQDWRU'라 되어 있었다. 3글자씩 당겨서 읽어보면 뜻은 'BE CAREFUL FOR ASSASSINATOR', 즉 '암살자를 주의하라'는 것이었다. 당시 시저의 권세를 시기했던 일당은 시저를 살해할 암살 음호를 꾸미고 있었으며 시저 자신도 이를 어느 정도 눈치 채고 있었다. 하지만 시저는 구체적으로 암살자가 누구인지 알 수 없었다. 결국 암호문을 전달받은 당일 시저는 원로원에서 전혀 생각지도 못했던 브루투스에게 암살당하면서 "브루투스, 너마저……."라는 말을 남겼다.

• 악보 암호

악보 암호는 전설적인 스파이 마타하리(본명은 마그레타 G. 젤러, Margaretha Geertruida Zelle)가 사용했던 방식이다. 마타하리는 일명 '첩보원 H21'이란 이름으로 프랑스 장교에 접근해 군사 기밀 정보를 독일에 빼돌렸는데, 이때 비밀 통신에 사용된 암호가 악보였다. 일정한 형태의 음표에 알파벳 하나씩을 대응시킨 형태로 얼핏 보기에 평범한 악보처럼 보이지만, 실제로 연주하면 전혀 '음악'이 되지 않는다. 마타하리의 첩보 활동은 20여만 명에 달하는 프랑스군을 죽음으로 몰고 갔다. 그녀는 제 1차 세계 대전이 끝나기 1년 전 프랑스 정보부에 체포돼 사형 당했다.

2) 근대 암호

17세기 근대 수학의 발전과 함께 암호 기술도 발전하기 시작했는데, 프랑스 외교관이었던 Vigenere가 고안한 키워드를 이용한 복수 시저 암호형 방식, Playfair가 만든 2문자 조합 암호 등 다양한 암호 방식으로 발전하였다.

20세기 들어서는 통신 기술의 발전과 기계식 계산기에 대한 연구를 바탕으로 두 차례의 세계 대전을 통해 암호 설계와 해독에 대한 필요성이 높아지면서 암호에 대한 연구가 더욱 활발하게 진행되었다. 근대 암호의 이론적 기초가 된 논문은 1920년 Freidman이 발표한 '일치 반복률과 암호 응용'과 1949년 Shannon이 발표한 '비밀 시스템의 통신 이론'을 들 수 있다. Shannon은 논문에서 일회성 암호 체계가 안전함을 증명했고, 암호 체계 설계의 두 가지 기본 원칙인 '혼돈과 확신 이론'을 제시하였다. 암호 체계를 설계함에 있어 '혼돈(Confusion)'은 평문과 암호문 사이의 상관관계를 숨기는 반면, '확산(Diffusion)'은 평문의 통계적 성격을 암호문 전반에 확산시켜 숨기는 역할을 한다. 혼돈과 확산이라는 두 가지 개념은 오늘날의 암호 체계 설계에도 여전히 적용되고 있다.

Freidman은 2차 세계 대전 중 독일군이 사용하던 에니그마(Enigma) 암호와 일본군이 사용하던 무라사끼 암호를 해독한 사람으로 유명하다. 에니그마 암호는 각기 다른 몇 개의 암호판을 전기적으로 연결하여 원문을 입력하면 전기적 연결에 의해 새로운 암호문을 출력하는 방식으로 이 기계가 존재하지 않으면 암호를 풀 수 없다.

미드웨이 해전에서의 암호 전쟁

태평양 전쟁 당시 일본의 진주만 공습으로 큰 피해를 입고 전력이 약화됐던 미국은 일본의 그 다음 공격 목표가 어디인지를 알아내야 했다. 1942년 4월, 하와이 주둔 미국 해군 정보부의 암호 해독반 블랙 챔버는 일본군의 무전이 증가하고 있음을 발견했다. 이미 일본 해군의 암호 체계인 JN-25를 해독하고 있던 해독반은 AF라는 문자가 자주 나타난다는 사실에 주목했다. AH는 진주만을 뜻하는 것이었다. 암호 해독반의 지휘관이었던 조셉 로슈포르 중령은 AF를 미드웨이 섬이라고 생각했다. 일본의 정찰기가 'AF 근처를 지나고 있다'는 내용의 무선 보고를 해독한 적이 있었던 그는 정찰기의 비행경로를 추정해본 결과 AF가 미드웨이 섬일 것이라는 심증을 갖게 된 것이다.
로슈포르 중령은 체스터 니미츠 제독에게 일본군의 침공이 임박했다는 것과 AF가 자주 언급된다는 점, 그리고 AF가 미드웨이 섬일 것이라는 보고를 한 후, 미드웨이 섬의 담수 시설이 고장 났다는 내용의 가짜 전문을 하와이로 평문 송신하게 하자고 건의했다. 3월에 미드웨이 섬 근처에 일본 해군의 비행정이 정찰 왔던 것을 알고 있던 니미츠 제독은 이 건의를 받아들였다. 사실 미드웨이 섬의 정수 시설은 아무런 문제가 없었다. 이틀 후, 도청된 일본군 암호 중 'AF에 물 부족'이라는 내용이 해독되었다. 이로써 일본군의 다음 공격 목표가 미드웨이 섬이라는 것이 분명해진 것이다.
미군은 암호 해독을 통해 일본의 공격 목표가 미드웨이라는 사실을 알아낸 후 전투에 대비하고 반격을 준비하여 일본의 태평양 함대를 격파하고 전쟁을 승리로 이끌 수 있었다.

3) 현대 암호
현대 암호는 1970년대 후반 스탠퍼드 대학과 MIT 대학에서 시작되었다. 1976년 스탠퍼드 대학의 Diffie와 Hellman은 '암호의 새로운 방향(New Directions in Cryptography)'이라는 논문에서 처음으로 공개키 암호의 개념을 발표하였다. 종래의 관용 암호 방식 또는 대칭키 암호 방식에서는 암호화키와 복호화키가 동일한 비밀키를 사용하기 때문에 송신자와 수신자는 비밀통신을 하기 전에 비밀키를 공유하고 있어야 한다. 반면 공개키 암호 방식에서는 하나의 쌍이 되는 공개키와 비밀키를 생성하여 암호화에 사용되는 공개키는 공개하고, 복호화에 사용되는 비밀키는 사용자가 안전하게 보관하도록 한다. 공개키 암호 방식에서는 송신자와 수신자가 사전에 키를 공유할 필요가 없기 때문에 불특정 다수 사용자 간에 사전 준비가 없이도 암호 통신망을 구축하는데 유용하게 사용할 수 있다.
이어 1978년 MIT 대학의 Rivest, Shamir, Adleman은 소인수 분해 문제에 기반을 둔 RSA 공개키 암호를 개발했는데, 이것은 오늘까지도 가장 널리 사용되는 공개키 암호 방식이다. 공개키 암호의 도입은 현대 암호의 발전에 중요한 계기가 되었다.
한편, 1977년 미국 상무성 표준국(NBS, 현 NIST)은 전자계산기 데이터 보호를 위한 암호 알고리즘을 공개 모집하여, IBM 사가 제안한 DES (Data Encryption Standard)를 표준 암호 알고리즘으로 채택했다. DES의 표준화를 계기로 하여 금융 시스템을 중심으로 상업용 암호화의 이용이 증가하게 되었고 컴퓨터 통신망을 이용한 문서 전송, 전자 자금 이체 등이 활성화되었으며 암호 방식이 일반인들에게 알려지고 널리 사용되는 계기가 되었다.
이전의 암호 방식에서는 사용하는 키뿐만 아니라 암호 알고리즘도 비밀로 하여 암호문의 비밀을 지키려고 하는 경우도 있었으나, 현대 암호에서는 암호 알고리즘을 공개하도록 하고 있다. 1883년 Auguste Kerckhoff는 암호 시스템의 안전성에 대해 '키 이외에 암호 시스템의 모든 것이 공개되어도 안전해야 한다'고 했는데 이것을 Kerckhoff's principle이라고 한다. 이렇게 함으로써 암호 방식의 안전성을 공개적으로 검토하게 하여 안전성을 확인하는 것이다.
표준화된 암호와 표준화된 컴퓨팅 기기들을 사용하는 현대 암호에서는 암호 알고리즘을 감추

기가 매우 어렵다. 또한 암호 알고리즘을 감춘다고 해서 암호의 보안성이 높아지는 것도 아니다. 비밀로 다루어진 암호 알고리즘이 일단 공개되고 나면 그 안전성에 문제가 발견되는 사례가 많다. 그러므로 암호 분야에서는 어떤 암호 알고리즘이 많은 암호 학자들에 의해 장기간 세부적으로 수행된 분석에서도 잘 견디어 낼 때까지는 그 알고리즘을 안전하다고 인정하지 않는다. 즉, 암호 체계는 '무죄가 증명될 때까지는 유죄'이다.

4) 차세대 암호

- 양자내성암호

격자 기반 격자 위에서 계산하는 문제의 어려움에 기반하는 암호 시스템
코드 기반 일반적인 선형 코드를 디코딩하는 어려움에 기반하는 암호 시스템
다변수 기반 유한체 위에서 계산하는 다변수함수 문제의 어려움에 기반하는 암호 시스템
해시 기반 해시 함수의 안전성을 기반으로 한 전자 서명 시스템
아이소제니 기반 순서가 같은 두 타원 곡선 사이에 존재하는 아이소제니를 구하는 문제의 어려움에 기반하는 암호 시스템

- 동형암호

암호문을 이용하여 계산을 할 수 있도록 해주는 공개키 암호화 방식. 암호화된 데이터들을 이용하여 게산한 결과를 복호화하면 암호화되지 않은 상태로 계산한 값과 일치하는 암호화 방식이다. 국내에서는 정수 환(Ring) 기반의 동형암호 알고리즘이 개발되었으며, 국외 IBM, Microsoft 등은 다수의 동형암호 알고리즘을 개발하고 의료 분야 등 다양한 응용 서비스 적용 기술을 개발 중이다.

- 형태보존암호

암호문이 평문이 가지고 있는 형태를 그대로 유지한 암호화 방식. 암호화된 데이터들을 이용하여 계산한 결과를 복호화하면 암호화되지 않은 상태로 계산한 값과 일치하는 암호화 방식이다.
작은 크기의 평문에 대한 암호화가 가능하며, 안전성에 문제가 발생하지 않도록 추가적인 입력 정보인 트윅을 사용한다.
데이터의 길이가 보존되어 추가적인 저장 공간 구매가 불필요하며, DB 스키마 변경도 불필요하기 때문에 암호화 시스템 구축 비용이 절감된다.
신용카드, 주민등록번호, 사회보장번호 등과 같이 특정 형태의 암호화에 효율적으로 사용할 수 있다.

- 경량암호

경량 암호는 사물인터넷(IoT) 등을 스마트 디바이스 상에 탑재, 운용하기 위해 개발된 암호화 방식이다.

라. 우리의 암호

탐구 순서(방법)

1. 암호의 특성을 활용해 각자 직접 만들어본다.
2. 직접 만든 암호를 해석해본다.
3. 해석한 후 우드락에 우리가 만든 암호를 정리한다

III 결론

암호의 기능은 점점 더 다양해지고 있다. 전자산업이 발달함에 따라 다양한 기능을 가진 암호체계를 필요로 하는 경우가 폭발적으로 늘어나고 있으며, 이미 암호는 현대인의 일상생활 곳곳에서 쉽게 찾을 수 있다. 아파트 현관이나 회사의 출입문의 시건 장치, 컴퓨터의 패스워드로부터 은행계좌나 신용카드의 비밀번호, 전자우편이나 휴대전화 내용의 암호화에 이르기까지 이루 헤아릴 수가 없다. 전자화폐, 전자입찰, 전자투표 등에서도 핵심은 암호기술이다.

예를 들어 전자 입찰을 생각해보자. 나의 입찰가를 암호화해서 제출했을 때, 다른 입찰자가 나의 입찰가를 몰라야 할 뿐만 아니라 나의 입찰가보다 조금 높은 금액의 암호문을 만들 수 없어야 한다. 또 낙찰된 후에 내가 애초의 입찰가를 부인할 수 없어야 한다. 더 나아가 입찰시행기관의 누구도 입찰이 마감되기 전에 나의 입찰가를 미리 알아내어 다른 입찰자에게 알려줄 수 없어야 한다. 전자투표의 경우도 마찬가지이다. 각 투표자가 투표지를 암호화하여 제출했을 때, 투표자 외에는 어느 누구도 그 내용을 몰라야 하고 또 변조할 수도 없어야 한다. 두 번 이상 투표할 수 없도록 해야하며, 부정 투표자가 있어도 안되며, 그러면서도 정확한 집계가 이루어져야 하고 그 결과에 잘못이 없음을 확인할 수 있어야 한다.

새로운 암호의 응용은 위에서 언급한 것들 외에도 무수히 많다. 인터넷상에서 음악이나 영상 등의 디지털제품 판매에도 가장 시급한 과제는 암호기술이다. 중요한 비밀정보를 다루는 기관의 컴퓨터시스템에 대한 해킹과 방어는 전쟁이나 다름없으며 이러한 네트웍보안의 핵심도 암호기술이다. 암호의 새로운 응용에 대하여 최근에 대표적인 것 두 가지만 더 예를 들어보자.

이러한 조건들은 단순히 암호문을 주고받을 수 있는 암호체계로는 도저히 만족시킬 수 없는 조건들로서, 이러한 까다로운 조건들을 모두 만족시킬 수 있는 암호체계를 만들기 위해서는 고급 수학이론의 도움이 절대적이다.

정보화시대를 맞아 암호의 중요성이 대두되고 있다. 우리는 산업적인 측면에서의 필요성을 주로 언급하였지만 국가안보의 관점에서 보게되면 암호이론과 기술의 수준은 국가의 존망과 직결되는 문제가 된다. 암호이론과 기술의 수준에서 뒤쳐지면, 평화시에는 정보속국 내지는 정보식민지로 전락하게 될 것이고 전시에는 패망하게 될 것이기 때문이다. 우리는 다음 중 어디에 해당되는가? 정보화시대에 항상 염두에 두어야 할 질문이다.

워터파크 속 수학원리

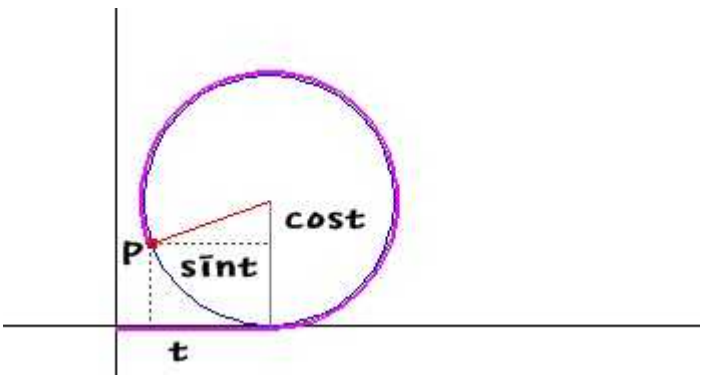
분야 : 주제탐구
10115 박서혜, 10123 이서영, 10127 이지윤, 10310 김지수

1. 사이클로이드

▲ 사이클로이드 미끄럼틀

1) 개념 : 구르는 원 위에 있는 한 정점이 그리는 자취

2) 수학적 표현 : 원점과 접해있던 반지름이 1인 원이 x축을 따라 t만큼 굴러갔을 때 원점과 접해있던 점이 P라고 정의한다. 점 P를 방정식으로 나타내면 x=t−sint, y=1−cost



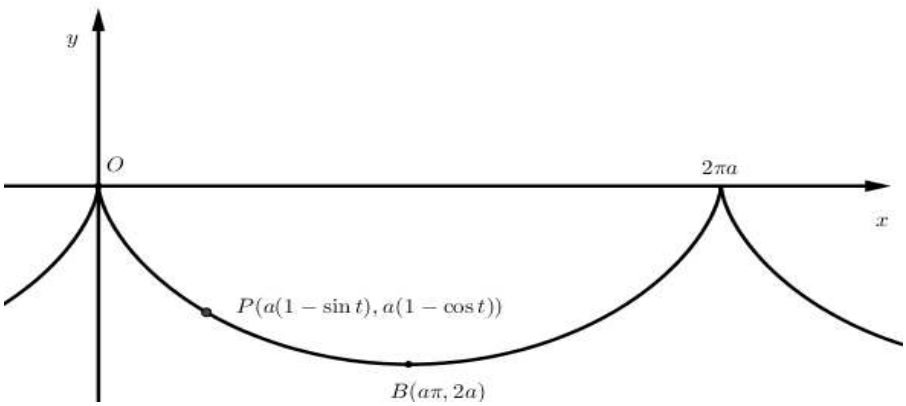
3) 역사 : 사이클로이드는 17세기 수학자들 사이에서 빈번히 논쟁을 야기하여 헬렌의 기하학이라고 불린다. '움직이는 원 위의 한 점에 의하여 생성되는 곡선'이 문헌에 최초로 언급된 것은 1501년 부벨이 원의 넓이를 구하는 과정에서 그러한 곡선을 이용했다는 것이다. '사이클로이드 (cycloid)' 라는 이름은 1599년 갈릴레오가 명명하였다. 그는 사이클로이드의 한 아치 아랫부분의 넓이를 구하는 수학적 방법을 찾으려고 하였으나 성공하지 못했다. 그리고 실제로 금속판으로 생성원과 사이클로이드 모양을 만들어 무게를 비교하여 사이클로이드 아치의 넓이와 생성원의 넓이의 비율이 대충 3:1이라는 것을 발견했지만 비율이 무리수의 분수로 직교구적법이 불가능하다고 부정확하게 결론지었다. 1673년 네덜란드의 물리학자 호이겐스는 '진자시계'라는 저서에서 진자의 궤적이 원의 호가 아니라 사이클로이드 곡선이 되어야 진자의 주기가 정확히 일정하게 된다는 것을 증명하고, 이러한 성질을 이용해 진자시계를 만들었다. 1675년에 호이겐스는 가느다란 나선형의 금속스프링이 감겼다 풀렸다 할 때 진동의 주기가 일정한 것을 응용한 시계를 고안하였다. 이 시기에 과학자들은 용수철에 매달린 물체와 진자의 운동에 관심을 갖고 연구하였고, 그 결과들은 근대적인 시계의 발명, 표준 도량형의 정립 등으로 이어지며 자연을 수량화하여 연구하는 기초가 되었다. 1696년에는 요한 베르누이가 지면에 수직인 한 평면에 놓인 두 점 사이를 연결하는 어떤 경로를 따라 공이 중력에 의하여 굴러 내려올 때 최단시간이 걸리도록 하는 경로의 곡선을 찾는 사이클로이드의 의문을 풀어주는 최속강하선 증명을 사용했다.

4) 성질 :

① 등시곡선 : 중력의 영향으로 어떤 곡선을 따라서 물체가 그 곡선의 가장 낮은 곳으로 마찰이 없이 굴러 떨어진다고 할 때, 그 곡선의 어떤 점에서 물체를 굴리더라도 가장 낮은 곳까지 굴러 떨어지는데 걸리는 시간이 같은 곡선.

② 최단시간 강하곡선 : 사이클로이드를 x에 대칭이동하면 아래와 같은 식을 얻을 수 있다.
x=a(t−sint),y=a(1−cost)x=a(t−sin t),y=a(1−cos t)

점 P에 미치는 중력을 고려하면 원점 O에서 바닥점 B에 도착하는 시간이 가장 빠른 곡선이다.



2. 워터슬라이드 속 사이클로이드

1) 사이클로이드 미끄럼틀의 효과 : 사이클로이드의 최단강하라는 성질을 이용해서 같은 거리의 선으로 만든 경로 중 도착점에 가장 빠르게 도달하는 곡선으로 효율성과 사용자의 스릴감을 높인다.

2) 탐구 목적 및 준비물
사이클로이드 미끄럼틀 모형을 제작해 실험함으로써 원리를 이해하고자 한다.
재료: 전지2장, 50cm자, 줄자, 각도기, 컴퍼스, 접착제(풀,목공풀), 구슬,
카메라

3. 파도풀 속 소금물 농도

1) 사람이 뜰 수 있게 하는 소금의 양 계산
밀도 = 질량/부피
사람의 밀도가 소금물 밀도보다 작아야 사람이 물에 뜰 수 있다.
예를 들어 보면, 1톤의 물 = 1000kg = 1000L 이므로,
1000L의 부피를 구해 보면 1000L×0.001 = 1m^3
소금물의 밀도는 (1000+x)kg/m^3
사람의 부피를 1.03g/cm^3이라고 하면, 1.03g/cm^3 = 1030kg/m^3이다.
앞서 말했듯 사람의 밀도가 소금물 밀도보다 작아야 하므로, x는 최소한 30kg은 넘어야 한다.

2) 농도와 밀도

용액의 부피가 그대로이다고 가정했을 때 소금(조작변인)을 더 넣으면 용액의 질량만 증가하기 때문에 용액의 밀도가 증가한다.

4. 사이클로이드의 실생활 활용

1) 우리나라 전통가옥의 기와지붕

지붕을 덮고 있는 암기와와 그 끝에 얹힌 암막새의 곡선은 사이클로이드에 가깝다. 빗물이 기와에 스며들어 목조 건물이 부식되는 것을 막기 위해서는 가능한 빗물이 기와에 머무는 시간을 줄여야 한다. 그러기 위해서는 빗물이 기와를 가장 빨리 통과하도록 사이클로이드 모양으로 기와를 만드는 것이 효과적이기 때문에 사이클로이드 곡선 형태로 만든다.

2) 미끄럼틀

간혹 보면 미끄럼틀에서 떨어지는 속도를 높여 스릴감을 높이기 위해 미끄럼틀의 모양을 사이클로이드 형태로 만든다.

(3) 미국 텍사스 주의 킴벨 미술관의 지붕

킴벨 미술관의 지붕 같은 경우, 기와 같이 빗물을 신속하게 통과시키는 기능적인 이유보다는 아름다움을 얻기 위해 사이클로이드 형태로 만든다.

(4) 매의 비행경로

매는 사냥감을 포착하면 빠르게 잡아채기 위해 사이클로이드 곡선 모양으로 비행하며 사냥한다.

(5) 사이클로콥터

최근에 개발된 사이클로콥터라는 헬리콥터가 있다. 사이클로이드 곡선을 응용하여 만든 것인데 소음이 적고 에너지 효율이 뛰어나 기존 헬리콥터를 대체할 새로운 비행체로 각광받고 있다. 그리고 여기에 사용된 기술은 수력 및 풍력 발전에도 적용할 수 있어 친환경 에너지 사업에도 기대되고 있다.

수학 도시를 건설하다.

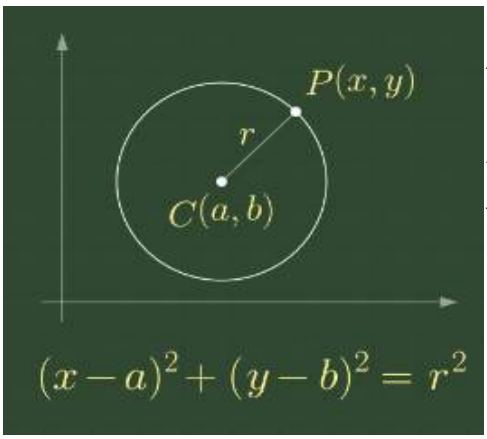
분야 : 주제탐구
10411 박성은, 10524 이소슬

주제 선정

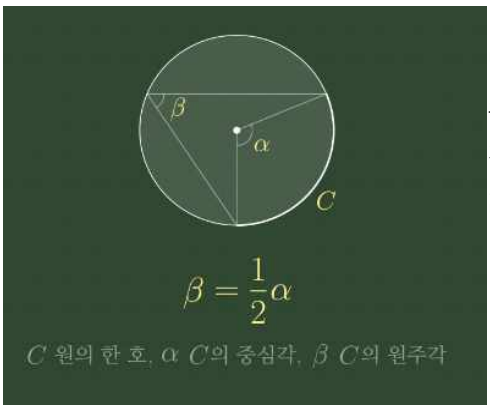
현대 사회에서 주거 환경이 더 중요해지는 상황에서 친환경적이고 생태적인 도시를 만들어보자는 취지로 주제를 선정하였고 이것을 수학과 접목시켜 안전성과 효율성을 보완할 수 있게 하였다. 또한 건물과 다리 공원 등 도시의 모든 부분에 수학적 원리를 담았기 때문에 작품명을 이와 어울리게 수학 도시라 지었다.

원형 빌딩

수학 도시의 전체적인 형태는 좌표평면의 모양으로 이루어져 있고
도시에는 원의 방정식과 일차 함수 모양의 다리가 있다

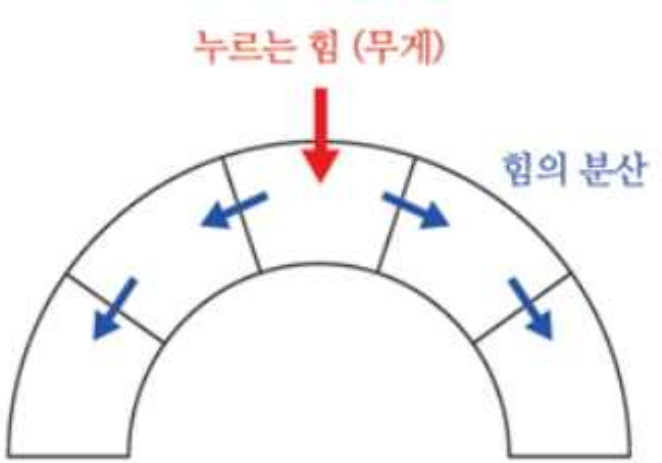


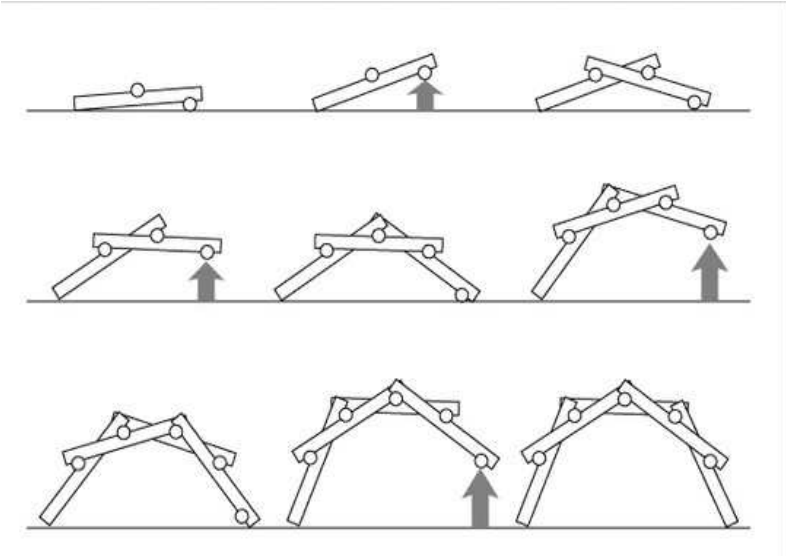
원의 방정식과 좌표평면은 수학 건축물 중 원기둥 모양의 빌딩을 위에서 내려다 봤을 때 찾아볼 수 있다.원의 방정식 공식은 좌표평면에서 원의 중심의 좌표와 반지름으로 원의 방정식을 표현하는 공식이다.



빌딩 옥상의 정원에서 찾아볼 수 있는 원주각 정리는 원 위의 주어진 호에 대한 원주각과 중심각의 관계를 나타낸 정리이다. 원주각 정리에 따르면 원주각은 중심각의 절반이라는 것이다.

다빈치 다리





다빈치 다리는 서로 얽혀 있는 나무 막대들로 이루어진 다리를 말한다. 다빈치 다리는 아치형 구조와 트러스 구조로 이루어져 있는데 삼각형이 단위공간인 트러스 구조는 위에서 힘을 가해도 변형이 일어나지 않는다.그리고 아치형 구조로 만들면 힘은 접점의 접선방향을 향하게 되어 힘을 분산한다.

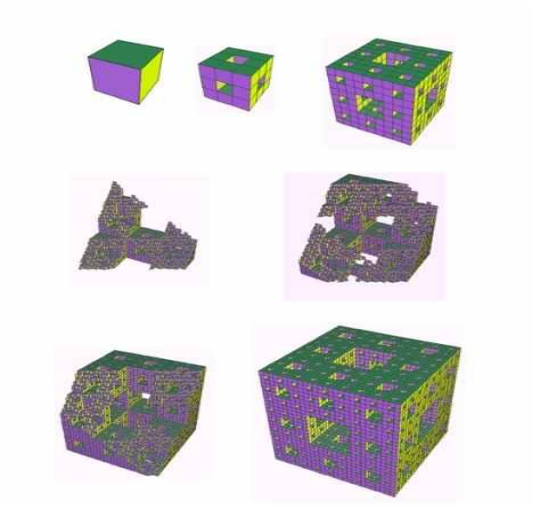
전쟁터에서 통나무를 이용하여 빠르게 다리를 만들어 강을 건널수 있게 하였고, 서로 교차되어 상호 지지대가 만들어져 끈으로 고정하지 않아도 견고하다. 아치형 다리는 아치형 모양이 위에서 누르는 힘을 옆으로 전달하여 아래쪽으로 향하는 힘을 줄여주는 원리를 가지고 있다. 따라서 힘이 분산되어 접착제 등이 없어도 무게를 효과적으로 버틸 수 있다.

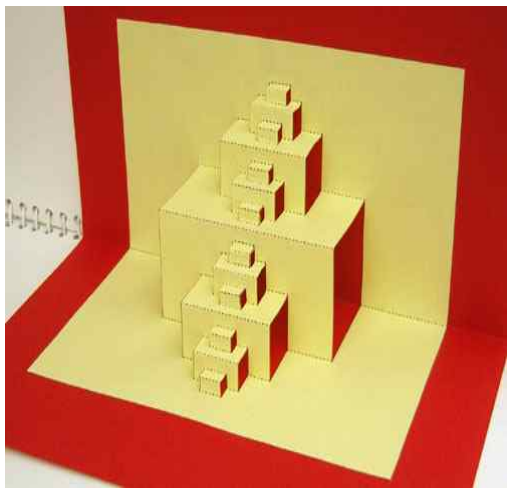
도형의 각을 이용한 빌딩

정사각형의 각(360도/한 각이 90도)이 일정한 각도(30도씩) 회전하게 하여 총 12개의 사각형을 이어붙여서 다시 원래의 위치로 돌아오게 되는 것을 도형의 각으로 표현하였다. 또한 구조를 나선형 구조로 하여 단단히 하여 구조적 안정성을 갖게 하여 지진 같은 자연재해에 효과적으로 예방, 대응할 수 있게 하였다.

전시 구조물(건물)

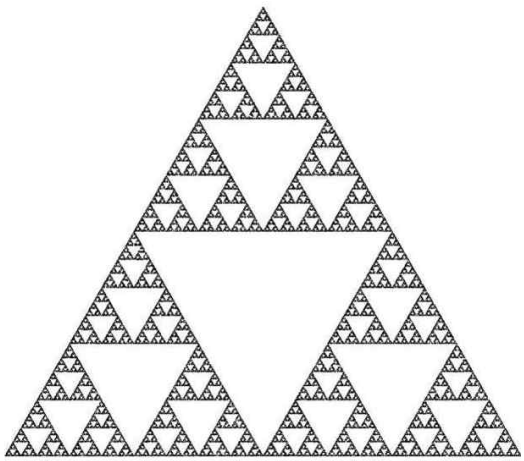
'맹거스펀지'는 크기가 같은 정사각형 6개로 이루어진 정육면체를 떠올려 보자. 각 면을 9개의 정사각형으로 나누면 하나의 정육면체는 총 27개의 작은 정육면체로 쪼개진다. 큰 정육면체의 중심에 있는 작은 정육면체 7개를 빼면, 앞에서 만든 주사위처럼 중간에 구멍이 뚫린 정육면체 모양이 만들어진다. 이와 같은 모양이 무한히 반복된 입체 도형이 바로 '멩거 스펀지'이다.
정육면체에 이 방법을 한 번 사용한 멩거 스펀지를 '1단계', 두 번 사용한 멩거 스펀지를 '2단계'라고 한다. 즉, 방법을 적용한 횟수에 따라 차례대로 이름을 붙인다. 앞에서 만든 '멩거 스펀지 주사위'는 바로 멩거 스펀지 1단계이다. 1개의 정육면체가 20개의 정육면체로 계속 쪼개지기 때문에, 단계가 높아질수록 멩거 스펀지를 이루는 정육면체의 개수는 매우 빠르게 늘어난다.





'시어핀스키 삼각형(Sierpinski triangle)'은 폴란드의 수학자 바츨라프 시어핀스키(Waclaw Sierpinski, 1882~1969)의 이름을 딴 프랙탈 도형이다. 주어진 정삼각형의 각 변의 중점을 이으면 합동인 4개의 작은 정삼각형이 만들어지는데, 이때 가운데 있는 정삼각형을 제거하여 3개의 정삼각형만 남긴다. 남아 있는 3개의 정삼각형에 대해서도 이런 과정을 반복하면 시어핀스키 삼각형을 얻을 수 있다.
이렇게 특정한 규칙을 가지고 0단계도형에 적용시켜 그 부분이 전체가 되어 계속 똑같은 규칙

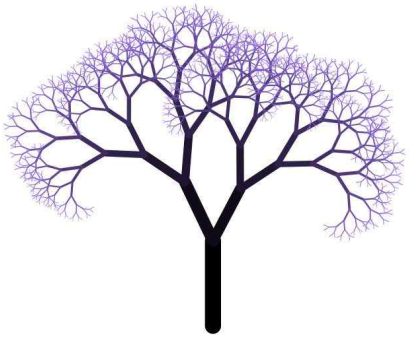
을 계속 적용시켜 그린다. 즉 부분이 전체와 닮음의 관계를 가지는 도형을 프랙탈 도형이라고 한다. 시어핀스키 삼각형은 대표적인 프랙탈 도형이다.



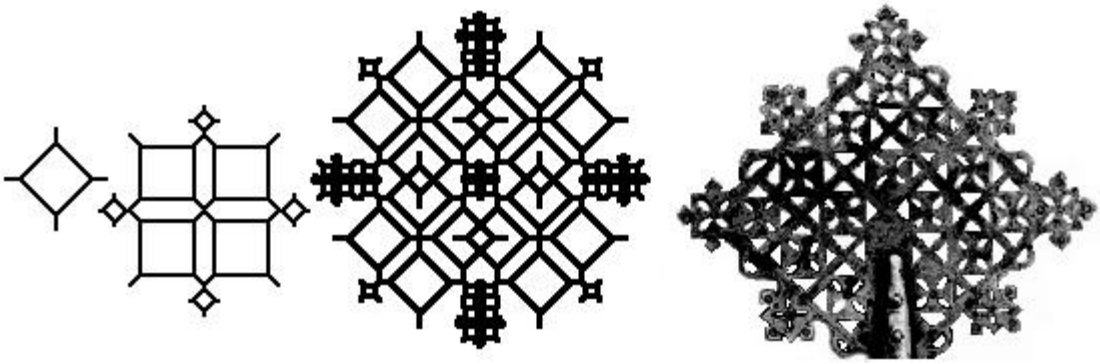
프랙탈(fractal) (나무)

프랙탈이란 부분과 전체가 똑같은 모양을 하고 있다는 자기 유사성 개념을 기하학적으로 푼 구조를 말한다. 프랙탈은 단순한 구조가 끊임없이 반복되면서 복잡하고 묘한 전체 구조를 만드는 것으로, 즉 '자기 유사성(self-similarity)'과 '순환성(recursiveness)'이라는 특징을 가지고 있다.

이 용어는 프랑스 수학자 **만델브로트**(Benoit B. Mandelbrot) 박사가 1975년 '쪼개다'라는 뜻을 가진 라틴어 '프랙투스(frāctus)'에서 따와 처음 만들었다. 해안선이나 눈꽃송이처럼 같은 모양이 반복되는 구조를 '프랙탈'이라고 부르기 시작하였다.



▶수학 도시 속 자연물에서 발견한 프랙탈



▶도시의 건축물 문양에서 발견할 수 있는 프랙탈

호수 위 배의 돛

‘스트링아트’에서는 일대일대응을 찾아볼 수 있다.

스트링 아트란 19세기 영국의 수학자 메리 에베레스트 불이 수학을 가르치기 위해 고안한 것이다. 스트링 아트는 두 점을 이어 하나의 직선을 만들고, 이 수많은 직선들이 하나의 곡선을 만들어내는 시각적 효과를 표현하는 예술작품을 말하는데 직선을 일정한 함수 규칙에 따라 그어주면 그 직선의 접점들이 모여서 곡선을 이루어내는데, 광장히 체계화된 기하학적 요소가 숨어있다.

미리 일정한 간격으로 점을 찍고 점마다 번호를 매긴 후 차례대로 일정한 수를 더하며 이어주면 이를 더해서 나온 수가 총점 개수보다 크면 이 두수의 차와 연결하고 마지막 수까지 모두 연결한다.
점이 많아질수록 숫자가 커지고 이 공식도 더 복잡해지고요, 또한 원, 정사각형 등 어떤 도형에서 시작하느냐에 따라서도 다양한 모양을 만들 수 있다.

여기서 찾아볼 수 있는 일대일 대응이란 두 집합 A,B의 원소를 서로 대응시킬 때, A의 한 원소에 B의 단 하나의 원소가 대응하고, B의 임의의 한 원소에 A의 원소가 단 하나 대응하도록

할 수 있는 대응으로 G.칸토어가 무한의 문제를 해결하기 위해 1900년경 최초로 수학에서의 기본개념으로 사용하였다.
A의 한 원소에 B의 단 하나의 원소가 대응하는 일대일 함수에 B의 임의의 한 원소에 A의 원소가 단 하나 대응한다로 조건이 강해지면 치역과 공역의 원소의 개수가 동일해지며 바로 일대일 대응이 된다.

수학 도시 바닥

‘쪽매맞춤’은 평면 도형을 겹치지 않으면서 빈틈이 없게 모으는 것이다. **테셀레이션**(tessellation)이라고도 한다. 정다각형 중 쪽 맞추기가 가능한 정다각형은 정삼각형, 정사각형, 정육각형이 있다. 우리 주변에서 볼 수 있는 테셀레이션의 경우는 천정, 건물, 옷감, 융단, 벽지 등이 있다. 테셀레이션은 정규 테셀레이션과, 준정규 테셀레이션, 비정규 테셀레이션의 종류가 있다. 우리말로는 '쪽매맞춤'이라 한다.

합동의 성질을 활용하여 같은 모양의 조각들을 서로 겹치거나 틈이 생기지 않게 늘어놓아 새로운 모양을 만드는 기법이다. 테셀레이션에 사용된 모든 도형들은 합동이며 평행이동, 대칭이동 등과 같은 합동의 성질을 이용하여 만들 수 있다.

이때 정삼각형, 정사각형, 정육각형은 테셀레이션이 가능하나 정오각형이나 원과 같은 도형은 어떠한 방법으로도 빈틈이 생기거나 내부가 겹치게 되어 테셀레이션이 불가능하다.

암호 알고리즘

분야 : 주제탐구
20113 이명진, 20119 정혜교, 20209 박은성

Ⅰ 탐구 배경 및 목적

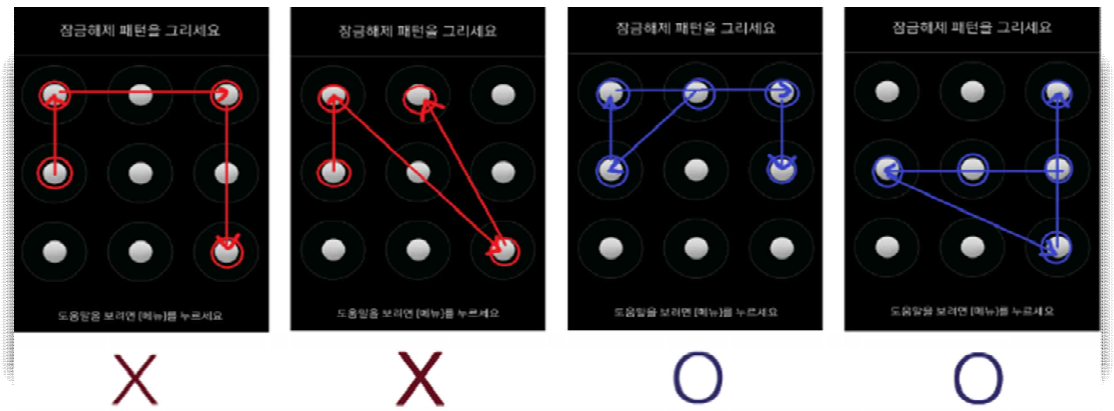
□ 실생활 속 암호

가. 암호의 시작

암호(cryptography)라는 용어의 어원은 그리스어의 비밀이란 뜻을 가진 크립토스(Cryptos)로 알려져 있다. 통신문의 내용을 제 3자가 판독할 수 없는 글자, 숫자, 부호 등으로 변경시킨 것으로 로마시대 이후부터 널리 사용되고 있는데 일상생활 속 우리의 생활에도 많이 사용되고 있다. 흔히 가정에서 볼 수 있는 현관 비밀번호, 사물함 자물쇠 등 숫자를 이용한 암호는 보편적으로 사용되고 있다. 최근 들어서는 지문 인식, 홍채인식 등 신체를 상용화하는 암호 체계가 만들어지고 있는데 이처럼 암호는 우리 삶에서 중요한 부분을 차지하고 있다. 그렇다면, 이 암호는 도대체 어떻게 만들어지는 것일까? 현재 가장 보안률이 높은 암호는 무엇일까? 사람들이 암호를 만드는 이유는 무엇일까? 지금부터 하나하나 알아가도록 하자.

나. 패턴 속 암호의 경우의 수

우리 주변에서 쉽게 볼 수 있는 암호에는 뭐가 있을까? 지금 당장 손에 쥐고있는 휴대폰을 껐다 켜보면 우리에게 매우 익숙한 암호를 볼 수 있을 것이다. 바로 패턴이다. 최소 점 4개~ 최대 점 9개를 사용하는 패턴(휴대폰 암호)의 경우 같은 숫자를 지날 수 없다는 것 (ex)1-3-2-1(x))과 같은 모양의 패턴이더라도 다른 곳에서 시작할 시 다른 패턴으로 인식한다는 것을 고려해보자. (ex) 1-4-5-6 ≠ 6-5-4-1)



$$\sum_{4}^{9}(9Cn\times n!)$$
$$=(9C4\times 4!)+(9C5\times 5!)+(9C6\times 6!)+(9C7\times 7!)$$
$$+(9C8\times 8!)+(9C9\times 9!)$$
$$=(9\times 8\times 7\times 6)+(9\times 8\times 7\times 6\times 5)+(9\times 8\times 7\times 6\times 5\times 4)$$
$$+(9\times 8\times 7\times 6\times 5\times 4\times 3)+(9\times 8\times 7\times 6\times 5\times 4\times 3\times 2)$$
$$+(9\times 8\times 7\times 6\times 5\times 4\times 3\times 2\times 1)$$
$$=3024+15120+60480+181440+362880+362880$$
$$=985824$$

이전의 결과에서 아래와 같은 경우의 수를 뺀다.

(1,3),(3,1),(4,6),(6,4),(7,9),(9,7),(1,7),(7,1),(2,8),(8,2),(3,9),(9,3),(1,9),(9,1),(3,7),(7,3)

중복된 수를 제외하고 각 점의 수로 가능한 패턴의 수는

4개 : 1624

5개 : 7125

6개 : 26016

7개 : 72912

8개 : 140704

9개 : 140704

이를 모두 더하면 389,112 가지의 경우의 수가 나온다. 따라서 우리가 실질적으로 이용 가능한 패턴의 수는 무려 389,112가지나 되는 것이다. 이렇듯 경우의 수가 많으면 많을수록 암호는 더더욱 어려워지고 보안성이 더 좋아지게 된다.

다. 번호 자물쇠의 비밀번호는 왜 4개일까?

우리가 학교에서 흔히 볼 수 있는 8개의 경우의 수가 있는 자물쇠는 항상 비밀번호가 4자리이다. 어째서일까?

먼저 1부터 8까지 8개의 숫자로 이루어진 자물쇠에서 n개의 숫자를 비밀번호로 정했을 때 가능한 경우의 수를 구해보자.

비밀번호 자릿수	경우의 수	비밀번호 자릿수	경우의 수
1	8	5	$\frac{8\times 7\times 6\times 5\times 4}{5\times 4\times 3\times 2\times 1}=56$
2	$\frac{8\times 7}{2\times 1}=28$	6	$\frac{8\times 7\times 6\times 5\times 4\times 3}{6\times 5\times 4\times 3\times 2\times 1}=28$
3	$\frac{8\times 7\times 6}{3\times 2\times 1}=56$	7	$\frac{8\times 7\times 6\times 5\times 4\times 3\times 2}{7\times 6\times 5\times 4\times 3\times 2\times 1}=8$
4	$\frac{8\times 7\times 6\times 5}{4\times 3\times 2\times 1}=70$	8	1

다음을 보면 알 수 있듯 비밀번호가 4개일 때 경우의 수가 70개로 가장 많다. 즉, 가장 풀기 어려운 암호라는 뜻이다. 따라서 우리가 평소 쓰는 8개의 숫자로 이루어진 자물쇠의 비밀번호가 4재리인 것이다.

II 탐구 내용

□ 암호의 역사

가. 카마수트라

B OBDFSOBDLNLBC, ILXS B QBLCDSV MV B QMSD, LE B OBXSV MH QBDDSVCE.

LH FLE QBDDSVCE BVS OMVS QSVOBCSCD…

위의 제시문처럼 의식 없이 마구잡이로 섞어놓은 것 같은 문자의 나열을 대치 암호라고 한다.

대치 암호란, 모든 알파벳 문자를 다른 알파벳 문자로 대치하여 사용하는 암호이다. a를 P로 해석하듯이 말이다. 대치 암호를 정보 수신자와 전송자가 모두 알고 있다면 메시지 해독할 수 있지만, 다른 이들에는 의미 없는 문자들의 나열일 뿐이다.

이런 암호 형태 중 가장 단순한 형태는 갈리아 전쟁 중 장군들의 소통 수간, 카이사르 암호이다. 카이사르 암호에서 각 문자는 일정한 간격만큼 떨어진 문자로 대치한다. 예를 들어, 간격이 3이라면 a는 D, b는 E. 이런 식으로 각 문자를 같은 간격만큼 이동시키면 암호의 종류는 25가지밖에 생성되지 않아, 메시지 해독이 쉽다.

카사이르 암호에서 한층 더 발전하여 교묘하게 만들어진 암호가 카마수트라 경전에 소개되어 있다. 카마수트라는 a를 어떤 알파벳으로 바꿀지 선택 가능한 경우가 26가지이다. 또한, 각 선택에 대해서 b를 어떤 알파벳으로 설정할지에 대해 25가지의 선택이 가능하다. 이로써, a와 b를 암호화 하는 데에도 26×25가지의 경우의 수가 나타난다. 모든 알파벳을 암호화하는 경우의 수는 26!이다. 여기서, a를 A로 대체하는 것은 암호화가 아니므로 1을 제외해야 한다. 그렇다면, 총 경우의 수는 403,291,461,126,605,635,583,999,999. 한 종루의 암호를 검사하는 데에 1초가 걸리는 컴퓨터가 있다고 가정하고, 130억 년 전 대폭발이 일어난 순간부터 암호를 확인하기 시작해도 지금까지 진행해야 하는 어마어마한 결과가 나온다.

	a	b	c	d	e	f	g	h	i	j	k	l	m
%	8	2	3	4	13	2	2	6	7	0	1	4	2
	n	o	p	q	r	s	t	u	v	w	x	y	z
%	7	8	2	0	6	6	9	3	1	2	0	2	0

최초로 암호 해독을 학문으로 발전시킨 이들은 아바스 왕조 시대의 아랍인들이다. 9세기의 이슬람 학자 야쿱 알킨디는 위의 표가 보여주는 것처럼 글로 쓴 문서에서 어떤 문자들은 자주 나타나는 반면, 어떤 문자들은 매우 드물게 나타난다는 점 발견했다.

문자로 쓰인 책에서 모든 문자에는 특유의 개성이 있으며 어떤 문자의 개성은 문자가 다른 기호로 표현될 때도 변하지 않는다는 점이 알킨디가 분석한 내용의 핵심이다. 이를 참고하여 다른 표를 분석하면,

	A	B	C	D	E	F	G	H	I	J	K	L	M
%	1	10	5	12	7	6	3	2	2	1	0	8	5
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
%	2	4	0	3	0	13	1	1	7	0	1	0	1

표에서 S는 13%의 빈도로 나타나며, 다른 문자의 빈도보다 높으므로 가장 많이 쓰이는 알파벳 e를 암호화하는 데 쓰인 문자일 가능성이 크다는 사실을 알 수 있다. 그 다음으로, 암호문에서 가장 많이 나오는 글자는 D로, 빈도는 12%이다. 영어에서 두 번째로 가장 많이 쓰이는 문자는 t이며, 따라서 D에 대치되었다고 생각해 볼 수 있다. 암호문에서 세 번째로 가장 높은 빈도수인 10%를 차지하는 문자는 B로 영어에서 세 번째로 가장 흔히 쓰이는 알파벳 a를 의미할 가능성이 크다. 이 문자들을 암호문에 대치시키고 어떤 결과가 나오는지 보면,

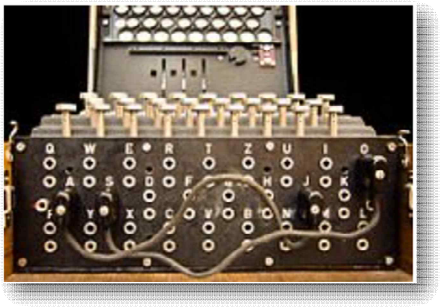
a OatFeOatLNLaC, ILXe a QaLCteV MV a QMet, LE a OaXeV MH QatteVCE.
LH FLE QattaVCE…

문자 a가 홀로 여러 번 나왔다는 점에서 옳게 해독한 것으로 볼 수 있다. 그리고 tFE라는 단어가 자주 보이는데, 이는 the를 의미할 확률이 크다. 실제로 문자 F는 암호문에서 6%를 차지하고, h라는 단어는 영문에서 6%의 비율로 똑같이 나타난다. Lt처럼 두 번째 글자만 해독되어도 그 단어가 무엇을 의미하는지 알 수 있다. t로 끝나는 두 글자 단어는 at, it로 두 가지 밖에 없다. a는 이미 해독했기 때문에 L은 i일 가능성이 크며, 빈도를 보아도 그렇다. L은 암호문에서 8%의 비율로 나타나며, i는 영어에서 이와 거의 유사한 7%의 빈도로 나타나기 때문이다. 이처럼 영어에서 나타나는 알파벳의 비율과 제시문의 알파벳 비율만 알 수 있다면, 여러 가지 경우의 수를 시도하여 해독할 수 있다.

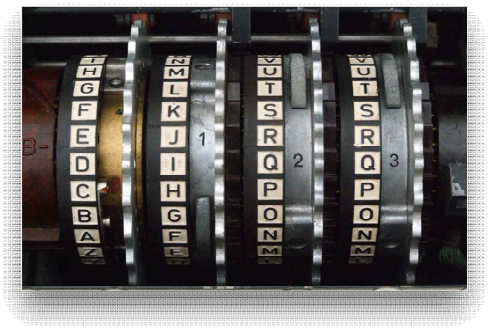
나. 전쟁 속 암호

대치 암호의 약점이 드러나자, 암호 사용자들은 문자 세기에 기초한 공격의 허를 찌르는 더 독창적인 방법들을 고안하기 시작했는데, 그중 하나가 바로 대치암호를 다양화하는 것이었다. 예를 들어 글 전체를 하나의 대치 암호로 암호화하지 않고, 두 가지 대치 암호를 교대로 사용하는 식이었다. 이렇게 하면, beef와 같은 단어를 암호화할 시 문자 e는 매번 다른 방식으로 암호화되는데, 처음의 e와 두 번째 e를 각각 다른 문자로 암호화하기 때문이다. 따라서 beef는 PORK로 암호화되게 되는 것이다. 더 많은 암호들을 순환시킬수록 메시지의 보안도 더욱 강화된다. (물론 가장 안전한 종류의 암호로, 원문에 나타난 모든 글자마다 다른 대치 암호를 적용하는 1회용 암호표가 있다. 이렇게 작성된 암호문은 이해를 돕는 단서가 전혀 없기 때문에 해독이 거의 불가능하다. 하지만, 메시지의 글자마다 다른 대치 암호를 써야 하므로 전혀 실용적이지 않다.)

16세기 프랑스 외교관 블레즈 드 비제네르는 몇 가지의 대치 암호를 순환시키면 모든 종류의 빈도 분석을 충분히 막을 수 있다고 믿었다. 그렇게 탄생한 '비제네르 암호'는 매우 강력한 암호 작성법이었으나, 해독 불가능한 것은 아니었고, 결국 영국의 수학자 찰스 배비지가 해독방법을 밝혀내게 된다. 비제네르 암호가 해독되자, 메시지를 안전하게 암호화하는 새로운 방법에 관한 연구가 시작되었다.



그리하여 1920년대 독일에서 '에니그마'가 발명되었을 때 많은 사람은 해독 불가능한 궁극의 암호가 탄생했다고



믿었다.'에니그마'는 매번 한 글자가 암호화될 때마다 대치암호를 바꾸는 원리를 바탕으로 작동한다. 만약 내가 문자열 aaaaaa를 암호화하고 싶다면(내가 배고프다는 신호를 보내기 위해) 각 a는 다른 방식으로 암호화될 것이다. 에니그마의 아름다움은 한 대치 암호에서 다음 대치 암호로 넘어가는 변화가 매우 효율적이게끔 기계화되었다는 점에 있다. 메시지를 살펴보자. 메시지는 자판을 통해 입력된다. 자판 위로는 제2의 문자판인 '전구판'이 있어서, 자판 위의 한 키를 누르면 전구판의 한 글자에서 불이 들어오면서 암호 글자를 표시한다. 그러나 자판은 전구판에 직접 연결되어 있지 않고 내부에 미로처럼 전선이 얽혀있는 회전 가능한 세 원판을 통해 연결된다. 에니그마가 어떻게 작동하는지 생각해보기 위한 가장 좋은 방법은 회전하는 세 드럼으로 구성된 거대한 원통을 떠올려보는 것이다. 원통의 윗면에는 둘레를 따라 26개의 구멍이 뚫려 있으며 각 구멍에는 알파벳의 한 글자가 붙어 있다. 글자를 암호화할 때 그 글자에 해당하는 구멍에 공을 넣는다. 공은 첫 번째 드럼으로 떨어지며, 첫 번째 드럼의 윗면과 아랫면 역시 둘레에 26개의 구멍이 뚫려 있다. 위와 아래의 구멍들은 관으로 연결된다. 그러나 관은 구부러지고 휘어졌기 때문에, 드럼을 통과한 공은 단순히 위에서 아래로 직접 내려가지 않고 전혀 다른 위치에서 튀어나오게 된다. 중간과 마지막 드럼 역시 유사하지만 위와 아래 구멍들을 연결하는 방식이 다르다. 세 번째 드럼의 밑면을 통과한 공은 마지막으로 알파벳의 각 글자들이 붙어 있는 원통 밑면의 26개의 구멍 중 하나를 빠져나온다. 그러나 이 기계가 정지 상태에 있다면, 에니그마는 대치 암호를 복잡하게 재생산하는 기계에 불과하다. 에니그마 암호기가 천재적인 까닭은 따로 있다.

매번 공이 원통을 통과할 때마다 첫 번째 드럼은 $\frac{1}{26}$만큼 회전한다. 따라서 다음 공이 떨어질 때, 첫 번째 드럼은 그 공을 완전히 다른 경로로 보내게 된다. 예를 들어 글자 a는 처음에는 C로 암호화되지만, 첫 번째 드럼이 한 칸 이동하면, a구멍에 넣은 공은 밑면에서 C와 다른 글자가 적힌 구멍을 통과할 것이다. '에니그마'도 마찬가지이다. 첫 번째 글자가 암호화된 뒤에, 첫 번째 회전 디스크는 딸깍하고 다음 위치로 이동한다.

회전 디스크들은 자동차 계기판의 미터계와 비슷하다. 일단 첫 번째 디스크가 26개의 위치를 모두 돌았다면, 시작 위치로 돌아오는 동안 두 번째 디스크가 $\frac{1}{26}$만큼 회전한다. 따라서 글자를 변경시키는 방법은 26x26x26 가지가 있다. 그뿐만 아니라 에니그마의 조작자가 원판의 순서를 변경할 수도 있기 때문에 가능한 대치 암호의 수에 6(세 개의 원판을 배열하는 경우의 수 = 3!)이 추가로 곱해진다. 기계를 조작하는 사람은 매일 암호책을 보고 메시지를 암호화하기 위해 세 개의 원판을 어떻게 배치해야 할지 결정했다. 수신자도 암호책에 나온 대로 설치하여 메시지를 해독했다. 에니그마가 설치되는 과정에서 복잡한 사항들이 계속해서 도입되었고, 결국 기계 설정 방법의 수는 무려 1억 5천 8백만의 백만 배의 백만 배를 넘었다.

1931년, 이 독일 기계의 설계도를 발견한 프랑스 정부는 충격을 받는다. 중간에 메시지를 가로챈다 하더라도 그 날의 원판의 배치를 알 수 없어 메시지를 해독할 수 없었기 때문이다. 그러나 프랑스 정부는 폴란드와 협약하여 암호 해독에 관한 지식들을 공유했고, 독일의 침략 위협에 놓인 폴란드인은 암호 해독 연구에 집중했다.

폴란드 수학자들은, 원판의 배치가 저마다 고유한 특징을 띠며 그 패턴들을 활용하면 암호문을 거꾸로 돌려서 해독할 수 있다는 사실을 깨달았다. 예를 들어 조작자가 a를 자판에 입력했다면, 원판들이 어떻게 배열되었는지에 따라 그 글자는 이를테면 D로 암호화된다. 첫 번째 원판은 이때$\frac{1}{26}$바퀴를 돌아간다. 또 다른 a가 자판에 입력되면 Z로 암호화되고, D는 디스크들이 설정된 방식에 따라 Z와 어떠한 관계를 맺는다. 우리는 이 관계를 상상의 기계를 통해 조사할 수 있다. 드럼을 재설정하고 각 글자에 대해 차례로 두 번씩 공을 넣으면, 모든 글자에 대해 다음과 같은 식의 관계표를 얻는다.

원래의 문자	a	b	c	d	e	f	g	h	i	j	k	l	m
첫 번째 공	D	T	E	R	F	A	Q	Y	S	I	P	B	N
두 번째 공	Z	S	B	Q	X	G	L	V	K	A	J	D	Y
원래의 문자	n	o	p	q	r	s	t	u	v	w	x	y	z
첫 번째 공	C	G	Z	J	H	M	U	X	K	O	W	L	V
두 번째 공	H	C	W	E	O	I	M	T	P	F	N	R	U

각각의 글자는 한 행마다 꼭 한 번씩만 나타나는데 각 행은 하나의 대치 암호에 대응하기 때문이다. 폴란드 수학자들은 어떻게 이 관계를 활용했을까?

날마다 독일의 모든 에니그마 조작자들은 암호책에 나온 그 날의 설정에 따라 에니그마를 똑같이 설정했다. 그다음에는 자신만의 설정을 선택하여 암호책에서 나온 원래의 설정을 이용하여 그 설정 정보를 보냈다. 그들은 안전을 위해 두 번씩 입력해서 보냈다. 그러나 안전은커녕, 이러한 행동은 치명적인 실수였다. 폴란드인은 이를 토대로 원판들이 글자들을 어떻게 연결하는지에 대한 힌트, 다시 말해 에니그마가 그날 어떻게 설정되었는지에 대한 단서를 얻었다. 옥스퍼드와 케임브리지 중간에 있는 블레츨리 파크의 한 시골 저택을 근거지로 삼은 수학자 집단은 폴란드 수학자들이 발견한 패턴을

연구하였고, 자신들이 만든 봄베라는 기계를 사용하여 자동으로 설정 방식을 찾는 방법을 발견했다. 일설에 따르면 이 수학자들 덕분에 제2차 세계대전의 기간이 2년 단축됨으로써 수많은 생명이 목숨을 구했다고 한다. 또한 그들이 만든 기계는 훗날 현대 생활의 필수품인 컴퓨터를 탄생시켰다. 이처럼 암호는 인류의 존속과 크나큰 연관이 있는 것이다.

다. RSA 암호

최근 우리가 사용하게 된 암호 체제에는 지문, 안면인식, 홍채인식 등 인체와 관련된 암호가 상용화되고 있다. 즉, 사람 고유의 특성을 통한 새로운 암호체계가 사용되고 있는데 인터넷상에서 인체와 관련된 암호를 사용하기 어려운 상황에서 최근 활용되고 있는 암호에는 RSA가 있다. RSA 암호는 리베스트(Rivest, R.), 샤미르(Shamir, A.), 에이들먼(Adleman, L.)이 1977년에 개발한 암호 체계(crypto system)이다. RSA는 공개키 암호시스템의 하나로, 암호화뿐만 아니라 전자서명이 가능한 최초의 알고리즘으로 알려져 있다. RSA가 갖는 전자서명 기능은 인증을 요구하는 전자 상거래 등에 RSA의 광범위한 활용을 가능하게 하였으며 최근 대표적으로 사용되고 있는 공개키 암호 체계이다. RSA는 소인수 분해의 난해함을 이용하여 암호화한다. 암호화하는 방법은 이와 같다.

1. 두 개의 소수 p,q를 선택한다. (p,q 는 서로 다른 수)

2. n = p · q를 계산한다.

3. ϕ(n) = (p − 1)(q − 1)을 계산한다.

4. gcd(e, ϕ(n)) = 1인 공개키 e를 선택한다.

5. d · e ≡ 1 mod ϕ(n)를 만족하는 d를 찾는다.

이 때, 공개되는 키는 e, n이다.

예를 들어 A가 p=11, q=3을 선택하였다고 하자. 그럼 n=33이 되며 ϕ(n)=20이 된다, 그 다음, e를 선택하게 되는데 e는 ϕ(n)와 서로소인 수를 나타내며 이 때 가능한 e 값은 1,3,7,11,13,17,19 이다. 이 중 A는 3을 선택하였다고 하자. 다음, e*d (mod ϕ(N))=1 인 d를 구한다. (ϕ(n)로 나누었을 때, 나머지가 1이 되는 e*d를 의미한다.) 이 중 A는 d 값을 7을 선택하였다고 하자. 이제 A가 B에게 e=3 과 n=33을 알려준다. 이후 상대방은 이 수를 가지고 복호화 가정을 거쳐 구할 수 있게 되는데, 복호화 과정은 이러한 방법으로 이루어진다.

1. 암호화하려는 문장을 정해진 규칙에 따라 숫자화한다.
2. 숫자로 바뀐 문장(평문)을, 적당한 크기의 블록으로 나누어 $m_1, m_2, \ldots, m_k$ 라고 한다. 각각의 블록은 n 보다 작은 수가 되도록 한다. 너무 짧은 블록은 적당한 수로 채운다.
3. 공개키 e 를 사용하여 $m1^e$, $m2^e$,...을 계산한다.
4. 법 n 에 대한 m_i 을 r_i 라고 하자. 즉, $r_i \equiv m_i^e \pmod{n}$ 이다.
5. 암호문 $r_1, r_2, \ldots, r_k$ 를 전송한다.

이를 통해 상대방은 암호를 복호화 할 수 있는데 이 때, m_i*e는 큰 수가 되지만 컴퓨터로는 쉽게 구현할 수 있어 유용하게 사용된다. 또, n이 인터넷상에서 이루어질 수 있는 큰 수에도 적용될 수 있어 활용화 되고 있다.

Ⅲ 게임-저널리스트

□ 저널리스트(Journalist)

가. 게임 기본 배경

20XX년, 기자들은 큰 난관에 봉착하게 된다. 거기서 거기인 내용의 기사들이 넘치게 되며 가면 갈수록 신문의 독자들이 줄어간 것이다. 이에 기자들은 각자의 신문 내용의 유출을 막으려 '암호'를 사용하기로 한다. 제 1차 기자대전의 서막이었다. 그들은 기존의 여러 암호들을 사용하여 자신들의 신문의 헤드라인을 비밀로 부치려 했으나 쉽게 뚫리고 만다. 결국 그들은 차세대 암호라 불리던 RSA암호를 사용하기로 한다.

나. 게임 설명

게임에 참가한 4명의 플레이어들은 암호의 비밀을 풀어내어 서로의 헤드라인을 빼앗아 기자대전에서 살아남아야 한다.

플레이어 수 : 4명(적정인원) + 사회자
적정 연령 : 고등학교 1학년~
예상 플레이 시간 : 30~50분

1. 게임 시작 시 플레이어들은 각각 p바구니와 q바구니에서 키워드를 하나씩 뽑는다. (이때 p는 헤드라인에서의 주어, q는 목적어+서술어를 의미하며 문장이 매끄럽지 않더라도 상관없다. (예) p : A 국회의원이, q : 기자회견을 가졌다.)

2. 사회자는 플레이어들의 헤드라인을 확인한 후 플레이어들이 공개키 e, 즉 ϕ(n)의 서로소들을 알려주면 그에 맞는 숫자들이 적힌 패를 배분한다. 또한 각 플레이어의 p와 q의 대소를 비교하여 파랑 또는 빨강의 색깔 패(파랑의 경우 p>q, 빨강의 경우 p<q)를 각 플레이어에게 나눠준 뒤 그를 모든 플레이어에게 잘 보이도록 각자의 앞에 놓게 한다.
이때 ϕ(n) = (p - 1)(q - 1)이다.
(예) p=21, q=2인 경우 20 x 1=20, 즉 ϕ(n)은 20이 된다. e는 ϕ(n)와 서로소인 수를 나타내며 이 때 가능한 e 값은 1,3,7,11,13,17,19가 된다. 사회자는 e가 적어도 6개가 넘도록 플레이어의 헤드라인을 조정해주어야 하며, 플레이어 또한 자신의 헤드라인의 e

가 6개가 넘지 않는다면 다시 뽑도록 한다.)

3. 플레이어들은 공개키 e들을 자신만 볼 수 있도록 나열하며, 나열할 시 플레이어 시선 기준 왼쪽부터 오른쪽으로 갈수록 큰 숫자를 순서대로 나열한다.
(예) 1,7,3,11,17,19,13 의 경우 1,3,7,11,13,17,19 순으로 왼쪽부터 나열한다. 이때 자신의 공개키 패가 다른 플레이어들에게 보이지 않도록 조심한다.)

4. 처음 추리를 할 플레이어를 가위 바위 보를 통해 정한 뒤, 순서대로 자신을 제외한 플레이어들 중 한명을 선택하여 패 하나를 손가락으로 가리킨 뒤 공개키를 추리해낸다. 만약 공개키 추리에 성공했다면 지목당한 플레이어는 그 공개키를 알리고 패를 모두에게 보이도록 한다. 만약 추리에 실패했다면 처음 지목을 한 플레이어는 자신의 공개키에 포함되지 않는 숫자를 말한다.
(예) 플레이어 A가 플레이어 B,C,D 중 한 명을 고른다. 예로 플레이어 C를 고른 경우 나열되어있는 패 중 하나를 선택하여 자신이 생각한 숫자를 말한다. 만약 지목된 패가 13이었을 경우 맞춘다면 플레이어 C는 그 패를 모두에게 보이도록 뒤집고, 13이 아니었을 경우 플레이어 A는 자신의 공개키 수를 제외한 수 중 하나를 말한다. 이때 말하는 수는 자신의 공개키들 중 가장 큰 수 보다 작아야 한다. 만약 더 이상 말할 수 있는 수가 없다면 더 이상 공개할 수가 없다는 것을 밝힌다.)

5. 각자의 공개된 e를 통해 다른 기자들의 $\phi(n)$을 추리하고 이를 통해 p, q를 추리한다. 마지막까지 헤드라인이 공개가 안 되고 살아남은 플레이어가 승리한다.

다. 게임 팁

만약 자신에게 p=11, q=3이 주어졌다면 $n=11\times3=33$이고, $\phi(n)=(11-1)(3-1)=20$이다. $\phi(n)$는 오일러 함수로 쉽게 말하면 n과 서로소인 정수 집합의 원소의 개수를 뜻한다. $\phi(n)$이 20이므로 본인은 20의 서로소인 1, 3, 7, 9, 11, 13, 17, 19를 본인만 볼 수 있도록 나열해야 한다.
나열한 후, 다른 기자들의 e를 맞추어 $\phi(n)$을 유추해야 한다. 만약 상대방의 공개된 e가 1, 2, 4, 7, 8, 11, 13, 14라면 상대의 $\phi(n)$은 15, 17, 19…이 될 수 있다. 가능한 $\phi(n)$이 매우 많기 때문에 $\phi(n)$의 범위를 정하여 공개하면 수월하다. $\phi(n)$이 15라고 한다면 1×15, 3×5가 가능하므로 p=1, q=15 또는 p=3, q=5가 가능하다. (이때, $p<q$이거나 $p>q$라고 정해놓아야 한다.)
구해낸 두 가지 경우의 p, q가 말이 되는지, 안 되는지를 통해 다른 플레이어의 헤드라인을 맞춘다. 마지막까지 살아남는 플레이어가 승리한다.

라. 암호를 사용한 추가적인 수학 공식

게임 내에서 가능한 $\phi(n)$은 20~30으로 제한된다.

$20 = 2^2 \times 5$ / 3,7,9,11,13,17,19
$21 = 3 \times 7$ / 2,4,5,6,8,10,11,13,16,17,19,20
$22 = 2 \times 11$ / 3,5,7,9,13,15,17,19,21
$23 = 1 \times 23$ / 2,3,4,5,6...21,22
$24 = 2^3 \times 3$ / 5,7,11,13,17,19,23
$25 = 5^2$ / 2,3,4,6,7,8,9,11,12...23,24
$26 = 2 \times 13$ / 3,5,7,9,11,15,17...23,25
$27 = 3^3$ / 2,4,5,7,8,10,11...25,26
$28 = 2^2 \times 7$ / 3,5,9,11,13,15,17...25
$29 = 1 \times 29$ / 2,3,4,5,6,7,8...27,28
$30 = 2 \times 3 \times 5$ / 7,11,13,17,19,23,29

다음과 같이 서로의 공개키를 유추하여 ϕ(n)을 추리한 뒤 p,q를 맞추는 능력이 필요한 저널리스트. 공개키의 수가 다르기 때문에 게임이 쉽게 끝날 것을 고려하여 각자에게는 허위 패가 하나씩 주어진다. 각 플레이어는 허위 패를 어디에 둘지 정할 수 있으며 원한다면 놓지 않는 경우도 있다. 이를 통해 숫자를 통한 ϕ(n)추리는 불가능하게 규정되어있으며, p,q에는 20~30까지의 약수들이 있다. 참가자들이 뽑은 패의 ϕ(n)가 20~30에 포함되지 않는 경우 사회자의 감독 아래 나올 때 까지 다시 뽑는다.

Ⅳ 기대효과 및 후기

□ 암호의 전망

암호는 고대부터 현재까지 꾸준히 사용되어지고 있다. 과거에는 단순 상대방과의 정해진 암호를 통해 메시지를 주고받는 형태였다면 이는 발전하여 오늘날에는 일상생활 속 잠금장치와 같이 다양한 형태로 모두가 대상이 될 수 있는 암호 체제가 사용되는 경우가 많다. 그러나 암호의 형태를 보면 항상 경우의 수가 최대가 되도록 하여 보안성을 높인다는 공통점이 있다. 이처럼 암호는 비밀이라는 의미를 가진 만큼 최적화된 방향으로 상용화되어왔다. 최근에 들어서는 신체의 일부를 사용하여 개개인의 고유한 암호를 사용하기도 하는데 홍채 인식, 지문 인식이 대표적이다. 이를 통해 암호는 항상 고유의 형태를 뛰어 보안성을 더욱 높이는 형태로 발전해왔으며 앞으로 어떠한 암호 체제가 생겨날지는 예측할 수 없다. 과거의 전쟁 암호로부터 시작하여 현재의 전자상거래까지, 미래의 어떤 상황에서 무슨 형태로 새로운 암호가 탄생할지 암호에 대한 발전은 기대된다. 암호가 우리의 사회에서 사라지는 날이 올까? 아마 절대 오지 않을 것이다. 우리는 하나하나 암호화되는 사회에서 어떻게 살아남아야 하는 것일까? 언제까지 그저 제공되는 암호에 만족하며 안이한 삶을 살 것인가? 분명 우리가 사용하는 암호는 언젠가 해독될 것이고, 그렇다면 우리는 빠르게 새로운 암호를 찾아야 한다. 그러기 위해서는 암호가 어떻게 만들어졌는지에 대해 잘 알고 있어야 할지 않을까? 시대가 변해도 사라지기는커녕 복잡한 방식으로 발전할 수학의 산물, 그것이 바로 암호이다.

□ 탐구 후기

이번 수학 탐구는 다양한 암호에 대해서도 알아보았지만 암호의 원리에 대해서도 생각해볼 수 있는 시간이었다. 왜 우리가 사용하는 잠금 장치는 4자리 수인지, 우리의 생활뿐만이 아닌 전자상거래에서도 보안 장치로 암호가 사용되고 있는 사실 등 암호에 대해 깊이 탐구해 볼 수 있었다. 이어 암호의 원리를 활용하여 나만의 게임을 만들면서 기존에 있던 암호 체제를 변형하여 학생들의 눈높이에 단순화시키고 활용할 수 있어 뜻깊은 시간이었다.