21411

素数の性質と現代社会との関係

2612　梶原　勇輝　　2510　勝野　皓太　　2613　片山　颯太

要旨

素数の定義は 1 とその数でしか割れない数という単純なものである。しかし、調べていくと自分達が数学の授業でつかっていること以上にさまざまな場面で利用されていることが分かった。自分達はそのことに興味を持ち、基礎知識や基礎性質を学ぶことで、さまざまな種類の素数、素数の詳しい概要、RSA 暗号の仕組み、素数が現代社会にどう使われているか、などを深く追求した。それらを利用して素数の無限性の証明を行った。

目的

素数の知識、性質を学びそれを利用して日常生活とのかかわり、無限性の証明を行う。

本論

Ⅰ，素数の定義

素数とは１とその数自身でしか割ることのできない１を除く自然数。

Ⅱ，いろいろな素数

１，双子素数　ある素数と２だけ離れた素数のペア　3・5　5・7　11・13

現在見つかっている最大の双子素数は 3756801695685・2 の 666669 乗±1

２，いとこ素数　ある素数と４だけ離れた素数のペア　3・7　7・11

３，セクシー素数　ある素数と６だけ離れた素数のペア　5・11　7・13

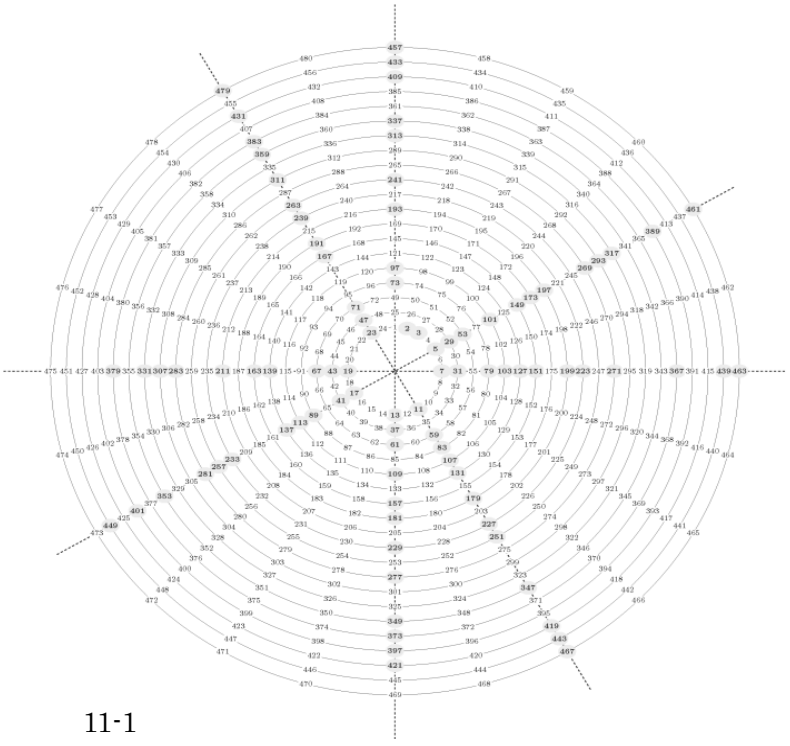
４，フェルマー素数　2^{2^n} であらわせる素数　$3=2^1+1$　$5=2^2+1$　$17=2^4+1$

これらの素数はいずれも無限性があると予想ができるがいまだにはっきりと証明されていない。またこのような素数のペアがあることから素数についての規則性の発見につながるかもしれない。

Ⅲ，素数の規則性

プリヒダの素数円

数字を位置から順に時計回りに円状に並べていき２４ごとに１つ外の円に移るように書く。素数には規則性はないといわれているが、2 と 3 を除いて円の中心から外に向かうように素数が並ぶことが見てみるとわかる。しかし各直線上の現れ方はばらばらでありそこには規則性はないことが見てわかる。結果として一直線状に並んでいるので何らかの規則性があると推測した。



Ⅳ，素数の発見

エラトステネスのふるい

２から１００まで数字を書いた表から二の倍数、三の倍数、五の倍数、七の倍数という順番に数字を消していくと最後は素数だけが表に残ることが分かる（ここでは都合上 1 から 100 までで行っている）

手順①　2 を除く 2 の倍数を表から取り除く。

	11	21	31	41	51	61	71	81	91
2	12	22	32	42	52	62	72	82	92
3	13	23	33	43	53	63	73	83	93
4	14	24	34	44	54	64	74	84	94
5	15	25	35	45	55	65	75	85	95
6	16	26	36	46	56	66	76	86	96
7	17	27	37	47	57	67	77	87	97
8	18	28	38	48	58	68	78	88	98
9	19	29	39	49	59	69	79	89	99
10	20	30	40	50	60	70	80	90	100

手順②　次に大きい素数である、3 を除く 3 の倍数を表から取り除く。

	11	21	31	41	51	61	71	81	91
2									
3	13	23	33	43	53	63	73	83	93
5	15	25	35	45	55	65	75	85	95
7	17	27	37	47	57	67	77	87	97
9	19	29	39	49	59	69	79	89	99

手順③　同じように 5 の倍数、7 の倍数を取り除いていく。

	11		31	41		61	71		91
2									
3	13	23		43	53		73	83	
5		25	35		55	65		85	95
7	17		37	47		67	77		97
	19	29		49	59		79	89	

	11		31	41		61	71		91
2									
3	13	23		43	53		73	83	
5									
7	17		37	47		67			97
	19	29			59		79	89	

これで 1～100 までの素数の判別ができる。

また、これは現在見つかっている最古にして最も素数を正確に求める方法である。

Ⅴ，RSA 法暗号

ロン・リベスト（Rivest)、アディ・シャミア（Shamir)、レン・アドルマン（Adelman）の３人が発明したことからこう呼ばれている。

なお、暗号と呼ばれるものにはすべて、以下のものが存在する。

暗号かぎ・・・与えられた情報を暗号化するもの
復号かぎ・・・その暗号かぎによって暗号化された情報を元の情報に直すもの

１，従来の暗号と RSA 法暗号の違いと利点

従来の暗号 暗号かぎ＝復号かぎ	RSA 法暗号 暗号かぎ≠復号かぎ
・暗号かぎがばれると解読されてしまう ・事前にかつ個人的に、情報を送りたい人に暗号かぎを渡さなくてはならない。	・暗号かぎを持っていても解読できない。 ・渡したい人にも一斉に暗号かぎを渡せる。

２，RSA 法暗号の仕組み

RSA 法暗号は素数によってできている。RSA 法暗号における暗号かぎと復号かぎとは、

・暗号かぎ・・・２つの素数の積で求められる素数　・・・A
・復号かぎ・・・巨大な素数の素因数分解によって求められる素数　・・・B,C

である。つまり、２素数の積を求めることは簡単だが、それを素因数分解することが非常に難しいという素数の性質によって成り立っているのである。

75462131　・・・A＝BC

簡単 ⇑　⇓ 困難

7591　×　9941　・・・B,C

３，暗号化と解読法

暗号の作り方は次の通りである。

ア，暗号かぎと復号かぎの作成

・復号かぎとなる２つの素数 a,b を決める。(よって暗号かぎは ab)

・もうひとつ別の暗号かぎ c を定める。(適当でよい)

・以下の式に代入して、もうひとつの復号かぎ d を求める。

Cd（ mod）(a-1 と b-1 の最小公倍数)＝1

イ，暗号化

・元の文 E から、以下の式に代入して暗号文 F を作成する。

F≡Ec（ mod） ab

ウ，復号

・以下の式に代入して E を求める。

E≡Fd（ mod） ab

Ⅵ，素数の無限性の証明

最大素数Nnが存在するとする。

$$M = (1 \times 2 \times 3 \times 4 \times 5 \times \cdots \times Nn) + 1$$

これは 2～Nn のいずれの素数でも割り切ることはできない。

この矛盾は、最大素数が存在する、という仮定によって生じた。

したがって、最大素数は存在しない。

EX： 最大素数が存在し、それが 5 であるとする。

$$1 \times 2 \times 3 \times 4 \times 5 + 1 = 121$$

$$121 = 11^2$$

$$11 = 1 \times 11$$ ⇒新たな最大素数の発見！！

総括

素数は現代では、暗号としてつかわれることが多い、素数円、素数定理など、規則性に関する予想は多いがいずれも証明されてない。現代社会は、こうした素数の不確定要素によって支えられているのである。

参考文献

ニュートン別冊ゼロと無限と素数と暗号