第98回数学教育実践研究会　レポート発表

整数論でOne more thing

北海道札幌南高等学校教諭　長尾良平

平成28年8月6日　小樽桜陽高等学校

1　はじめに

黒岩祐治氏の著書 [1] の中には, 恩師である橋本武氏の授業風景についての記述がある. そこでは, 中勘助「銀の匙」を題材にどんどん**（意味のある）脱線**をしていく様子が紹介されている.

数学の授業でも, 関連する事柄であればどんどん取り込んでいきたいと考えている筆者にとっては, 大変印象深い内容であった. 本レポートでは, 数学Aの「整数の性質」の単元において, 寄り道しながらの授業実践を紹介していきたい.

2　素数について

大学の代数学の授業で紹介された未解決問題や予想の話が印象深かったので, 授業で紹介してみた. 整数の話は, **（難問であっても）主張は伝わりやすい**ので, 高校生にも紹介できるところが良いと考えている. 扱った内容は以下の通り.

(1) 双子素数の予想
   ☜ 100以下の範囲における全ての組

(2) ゴールドバッハ予想
   ☜ 幾つかの偶数を奇素数の和に分解

(3) メルセンヌ数 2^n-1
   ☜ n が合成数の時に素数にならない理由
   ☜ n が素数の時に素数かどうかを確認

(4) ディリクレの算術級数の素数定理
   ☜ $6k-1$ について, $k=1,\ldots,10$ に対して素数になるかどうか確認

また, 最大のメルセンヌ素数 $2^{57885161}-1$ や, 最大の双子素数の組 $3756801695685\cdot 2^{666669}\pm 1$ など（2013年現在）は, **「今まで生徒が触れてきたであろう数の範囲を完全に超越している」**ため, それだけで大きな刺激を与えることになる.

また, **「十分大きな数に対して予想が成り立っていても, 数学では証明にならない」**ことも数学の厳密性の例として取り上げることができるだろう.

3　LCM(10,12)について

$\mathrm{LCM}(10,12)=60$ に関連して, 一般教養を深めて欲しいと思い, 十干十二支の話題を取り上げた. まず, 十干十二支を順に書かせてみる.

十　干：甲, 乙, 丙, 丁, 戊, 己, 庚, 辛, 壬, 癸
十二支：子, 丑, 寅, 卯, 辰, 巳, 午, 未, 申, 酉, 戌, 亥

そして, **六十干支**による年の表し方を紹介し, 西暦から六十干支に変換させて, その年に何があったのか考えさせた.

西暦から六十干支への変換

西暦を

- 10で割った余りが0：庚　→　9：己
- 12で割った余りが0：申　→　11：未

として対応させる.

(1) 1868 年

- 10 で割った余りが 8：戊
- 12 で割った余りが 8：申

となるので, **「戊辰戦争」**勃発.

(2) 1924 年

- 10 で割った余りが 4：甲
- 12 で割った余りが 4：子

となるので, **「甲子園球場」**開場.

生徒は,「本当だ, 凄い！」,「中学校の時に教えて欲しかった！」との声を上げていました.

4 合同式の応用

発展扱いであるが合同式が教科書で扱われるようになり, その応用例である **ISBN コード**と **RSA 暗号**について授業でとりあげた. ISBN コードの実践については, [2] を参照していただくことにして, ここでは, RSA 暗号についての実践を紹介する.

RSA 暗号による暗号化と復号の手順

M で原文（Message）を数値化した文字列, C で暗号文（Code）を表すとする.

○暗号化

(1) 原文を数値化する.

(2) p, q を素数とし, $n = pq$ を計算する.

(3) $\mathrm{GCD}(e, (p-1)(q-1)) = 1$ を満たす正整数 e を用意する.
☜ n, e を公開鍵として公開する.

(4) $\mathrm{C} \equiv \mathrm{M}^e \pmod{n}$ で暗号化する

○復号

(1) $de \equiv 1 \pmod{(p-1)(q-1)}$ を満たす正整数 d を用意する.
☜ d が秘密鍵になる.

(2) $\mathrm{C}^d \equiv \mathrm{M} \pmod{n}$ が成り立つので, 元のメッセージ M に復号できる.

実際の計算はかなり面倒なので, 1 回だけ合同式の計算を行い, [3] の Web サイトを参考にして**早見表を利用する**方式をとった. 早見表を利用することで暗号化と復号が簡単にできるので, 生徒達は RSA の雰囲気は感じとってくれたと思っている.

「暗号化したコメントを年賀状に入れるのもオシャレかもね」と授業で話したところ, 実際に暗号文入りの年賀状を出してくれた生徒がいた.

また, 次に扱う予定であるユークリッド互除法を意識して, **素因数分解の困難性**についても触れた. 実際の RSA 暗号では 600 桁程度の整数 n が用いられており, 仮に 1 秒間に 1 億回の四則演算ができるコンピュータを用いたとしても, 単純に素因数分解していくと**莫大な時間**がかかる. そのため, **素因数分解は現在でも数学の研究対象**になっていることを取り上げ, The RSA Factoring Challenge（現在は終了）や NTT セキュアプラットフォーム研究所の Web ページ [9][10] の内容を紹介した.

最後におまけとして, ガウスが 15 歳で発見した（と言われる）**素数定理**

素数定理

x 以下の素数の個数を $\pi(x)$ と表すとき, $\pi(x)$ は $\dfrac{x}{\log x}$ で近似される.

も紹介し, [11] も使いながらその様子を確認した.

5 互除法に関連して

小学校以来, 最大公約数を求めるには素因数分解をするのが標準的な方法だった. しかし, 2 数が大きくなると RSA 暗号の場面で見たように素因数分解が難しくなる. そこで,

- 4 桁同士の互いに素な 2 数
- 桁数の大きい 2 数

などに対して互除法を利用することにより, その優位性を体感させた. また, 次の**ラメの定理**の定理により, そのアルゴリズムの**効率の良さ**がよく分かる.

ラメの定理

$a > b$ とする．GCD(a, b) を互除法で求めるとき, 最悪でも b の桁数の 5 倍以下の回数の除算で終了する．

定理の証明から, a, b がフィボナッチ数列の隣接する 2 項のときが最悪なケースだと分かる．そこで, GCD$(1597, 987)$ を計算させた（987 が 3 桁：$3 \times 5 = 15$ 回かかるケース）．また, GCD$(12345678, 87654321)$ は最悪でも, $8 \times 5 = 40$ 回で終了するのでやってみるように指示した（実際は 6 回で終了する）．後者は素因数分解で GCD を求めるのは大変である．

6　基数の変換

10 進法で表された数を n 進法で表す処理については,

(1) どんどん余りを出しながら割り算を進め

(2) 余りを逆順に並べる

方法が一般的であるが, その意味を両替をイメージしながら説明をすすめた．

例　$45_{(10)}$ を 2 進法で表す．

1 円玉①：45 枚をどんどん両替していく．

両替対象硬貨	②	④	⑧	⑯	㉜	㊹
交換可能枚数	22	11	5	2	1	0
交換不可枚数	1	0	1	1	0	1
最終使用硬貨	①	②	④	⑧	⑯	㉜

以上の流れから, $45_{(10)} = 101101_{(2)}$ となる．

また, 小数の基数を変換する際, 変換後に循環小数になる例を取り上げた．2 進法で表された数を 10 進法で表すには,

(1) 2 倍して整数部分を比較し

(2) 確定した部分は取り除く

これを繰り返していくことになる．

例　$0.8_{(10)}$ を 2 進法で表す．

$$0.8 = \frac{a}{2} + \frac{b}{4} + \frac{c}{8} + \frac{d}{16} + \dots$$

2 倍して $\underline{1}.6 = \underline{a} + \dfrac{b}{2} + \dfrac{c}{4} + \dfrac{d}{8} + \dots$

2 倍して $\underline{1}.2 = \underline{b} + \dfrac{c}{2} + \dfrac{d}{4} + \dfrac{e}{8} + \dots$

2 倍して $\underline{0}.4 = \underline{c} + \dfrac{d}{2} + \dfrac{e}{4} + \dots$

2 倍して $\underline{0}.8 = \underline{d} + \dfrac{e}{2} + \dfrac{f}{4} + \dots$

これで, 最初の状態に戻ったので, 以下循環する．よって, $0.8_{(10)} = 0.\dot{1}100\dot{}_{(2)}$ となる．

7　百五減算

不定方程式の整数解の問題については,

- 因数分解で積のかたちに
- 不等式で評価する
- 余りで分類（合同式等）
- 拡張ユークリッド互除法

といった手法が用いられる．授業では, 代表的な問題を扱ってこの単元を締めくくったが, 最後に扱ったのが次の問題である．

百五減算

3 で割ると 2 余り・・・①
5 で割ると 1 余り・・・②
7 で割ると 2 余る・・・③
ような 2 桁の自然数を求めよ．

生徒には,「実は江戸時代の**塵劫記**という本に既に取り上げられていてね・・・」という話をすると, とても意外な顔をする．付け加えて, 当時のベストセラーであることを告げると, 当時の人の知的好奇心の高さに驚いていた．

また, 通常は①と③の（共通な）整数解を求め, さらに②との共通解を考えるが,「ガウスは全く違う観点で解く方法を発見してね・・・」とさらっとその解法を紹介すると, 次の日には Web で情報を見つけた生徒が「詳しく説明してくだ

さい」と質問に来ました. 授業では何かとガウスを取り上げるので,**「嗚呼, ガウスになりたい！」**とのつぶやきが複数の生徒から・・・.

8　終わりに

橋本先生の国語の授業は**教科横断的**. 現在の**総合学習**のはしりかもしれない. 駄菓子を食べたり凧揚げをしたり, **教科の枠に縛られず, 興味の赴くままにどこまでも・・・**. その行程を経て得られたものは, **断片的ではなく互いに結びついていて**, それこそ**「知識」と呼ぶに値する**ものだと思う.

以前から,**「大学で学んだことや興味のあることをどう授業に取り入れていくか」**をテーマに実践をし, レポートを作成している. 学生時代のノートを取り出したり, 参考文献に当たったり, Web ページの作成者に連絡をとってみたり・・・. 言うなれば**大人の総合学習**である.**「知識が繋がっていく」のがとても楽しい**.

生徒達にも, そんな感覚を味わって欲しいと思う. そのためにも, 教材研究をさらに進めていきたい.

参考文献等

[1] 黒岩祐治「恩師の条件－あなたは「恩師」と呼ばれる自信がありますか？」リヨン社

[2] 長尾良平「余りものには福がある」
第 73 回数学教育実践研究会レポート

[3] サルにも分かる RSA 暗号
https://www.maitou.gr.jp/rsa/

[4] 早苗雅史「高校生のための暗号論入門」
第 41 回数学教育実践研究会レポート

[5] 林雄一郎「RSA 暗号と因数分解」
第 81 回数学教育実践研究会レポート

[6] 西村昴介「素数から暗号へ」
第 92 回数学教育実践研究会レポート

[7] サイモン・シン著　青木薫訳「暗号解読」
新潮社

[8] 一松信「暗号の数理　作り方と解読の原理」
講談社ブルーバックス

[9] The RSA Factoring Challenge
http://japan.emc.com/
emc-plus/rsa-labs/historical/
the-rsa-factoring-challenge.htm

[10] NTT ニュースリリース
http://www.ntt.co.jp/news2010/1001/
100108a.html

[11] 真実のみを記述する会「素数表 150000 個」
暗黒通信団

[12] 中村滋「フィボナッチ数の小宇宙」
日本評論社

[13] 吉田光由「塵劫記」岩波書店

「素数」にまつわる話題

1. 素数は無限に存在する
- 紀元前3世紀にユークリッドが証明（背理法を利用）.

2. 双子素数の予想
- 差が2である2つの素数の組は無限に存在するか？
- 100以下の双子素数の組を全て挙げてみよう.
- _____

- 現在分かっている最大の双子素数は, _____

3. ゴールドバッハ予想
- 6以上の任意の偶数は、2つの奇素数の和で表せるか？
- 例えば, $28 =$ ___ $+$ ___ , $50 =$ ___ $+$ ___ , $88 =$ ___ $+$ ___

4. メルセンヌ素数
- n を自然数として, $2^n - 1$ の形で表される数をメルセンヌ数といい, 特に素数となるものをメルセンヌ素数という.
- n が合成数のときは, メルセンヌ数は素数にならない（説明できますか？）

- n が素数のときは, メルセンヌ数は素数になったりならなかったり・・・.
- $2^2-1=$ _, $2^3-1=$ _, $2^5-1=$ ___, $2^7-1=$ ____, $2^{11}-1=$ _____

- 現在分かっている最大のメルセンヌ素数は, _____

5. ディリクレの算術級数の素数定理
- GCD$(a,b)=1$ のとき, 集合 $\{ak+b \mid k$ は自然数$\}$ は無数の素数を含む
- 例えば, $a=6, b=-1$ として, $6k-1$ $(k=1,2,3,\ldots)$ を考えると,

k	1	2	3	4	5	6	7	8	9	10
$6k-1$										
素数か否か										

LCM(10,12) = 60 に関連して

「十干」と「十二支」

- 十　干：_____
- 十二支：_____

十干と十二支を組み合わせて, 年を表すことがあります. 丙子, 庚辰, ・・・

十干と十二支による年の表し方（「六十干支」という）

- 西暦を10で割った余りが0：庚　→　9：己
- 西暦を12で割った余りが0：申　→　11：未

として計算ができます.

LCM(10,12) = 60 だから, 60年で1周する. だから, 60歳を _____ という.

問　次の年にどんな出来事があったのか, 六十干支に直して考えてみよう.

1. 1868年

2. 672年

3. 1911年

4. 1924年

mod 33 で考える 暗 号 早 見 表

1乗から25乗までの範囲で

文字	数値化	1乗	2乗	3乗	4乗	5乗	6乗	7乗	8乗	9乗	10乗	11乗	12乗	13乗	14乗	15乗	16乗	17乗	18乗	19乗	20乗	21乗	22乗	23乗	24乗	25乗
A	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
B	2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32
C	3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12
D	4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1
E	5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23
F	6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21
G	7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10
H	8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32
I	9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12
J	10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
K	11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
L	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
M	13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10
N	14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23
O	15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12
P	16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1
Q	17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32
R	18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21
S	19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10
T	20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23
U	21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21
V	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
W	23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23
X	24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21
Y	25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1
Z	26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23
.	27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12
,	28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10
!	29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32
?	30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21
スペース	31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1
	32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32

スパイになった気分で・・・RSA暗号の紹介

公開鍵暗号

- **暗号化する鍵をどうやって相手に伝えるか**が, 古来からの悩み.
  ☜ 鍵がばれてしまっては, 暗号にならない.
- 公開鍵暗号は**暗号化するための鍵を公開**する新しい方式.
  ☜ 暗号化するための鍵と復号（元に戻す）するための鍵が**別になっている**.
  ☜ 公開してしまうので, **鍵の輸送の問題が解決**できる.

RSA暗号

- MITのリベスト, シャミア, エードルマンが考案した**公開鍵暗号**
  ☜ インターネットでの秘密通信にも使われている.
  ☜ その理論的背景に, **互除法**や**合同式**がある

RSA暗号による暗号化と復号の手順

Mで原文（Message）を数値化した文字列, Cで暗号文（Code）を表すとする.

○暗号化

1. 原文を数値化する.
2. p, q を素数とし, $n = pq$ を計算する.
3. 正整数 e として, $\mathrm{GCD}(e, (p-1)(q-1))$ を満たすものを用意する.
   ☜ n, e を公開鍵として公開する.
4. $\mathrm{C} \equiv \mathrm{M}^e \pmod{n}$ で暗号化する

○復号

1. 正整数 d として, $de \equiv 1 \pmod{(p-1)(q-1)}$ を満たすものを用意する.
   ☜ d が秘密鍵であり, 他人に知られないようにする.
2. $\mathrm{C}^d \equiv \mathrm{M} \pmod{n}$ が成り立つので, 元のメッセージMに復号できる.

文字→数値　の換算表

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	.	,	!	?	
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

＿＿組 ＿＿＿番 ＿＿＿＿＿＿＿＿＿＿

例　I LOVE YOU. を暗号化してみる. また, 復号して原文に戻ることを確認する.

暗号化

1. 原文を数値化する

原文	I		L	O	V	E		Y	O	U	.
数値化											

2. $p =$ ＿＿, $q =$ ＿＿ とすると, $n = pq =$ ＿＿

3. 正整数 e を $\mathrm{GCD}(e, (p-1)(q-1)) = \mathrm{GCD}(e,$ ＿＿$) = 1$ となるように選ぶ.
   ☜ 例えば, $e =$ ＿＿ とする.

4. $\mathrm{C} \equiv \mathrm{M}^e \pmod{n}$ で暗号化する.
   ☜ 早見表を利用する.

   暗号文は, 次のようになる.

原　文	I		L	O	V	E		Y	O	U	.
数値化											
暗号文											

復号

1. 正整数 d を $de \equiv 1 \pmod{(p-1)(q-1)}$ として求める.
   ☜ 今は, 数値が小さいので目の子で見つけられる. $d =$ ＿＿
   ☜ 実際は, **拡張ユークリッド互除法**が利用される.

2. $\mathrm{M} \equiv \mathrm{C}^d \pmod{n}$ で復号する.
   ☜ 早見表を利用する.

暗号文											
復　号											
原　文											

実例から・・・

amazonのWebサイトで用いられている公開鍵nの値
16進法で512桁 → 2進法で2048桁 → 10進法で617桁

○16進法表記（amazonのWebサイトから）

```
b7 0d 56 20 a9 13 a2 f5 90 7b 89 2e 59 48 16 31 63 9a 41 95 7a e0 97 1d
66 a6 23 f9 82 2e fc d9 22 6f 8a bc ec 7d d7 49 52 53 d0 2f dc e0 2a ee
f1 f5 c8 8e 80 16 fc 49 51 7d 7c 0f a1 31 fb 46 2c bc 9f b5 95 bb 6d d3
99 79 b6 b4 b1 98 d4 ae 82 71 eb 64 34 3f a5 2a da 9f a7 31 ee ae 37 01
47 3c 1f eb 56 f2 f3 4e a2 d6 d4 99 0d 51 b0 78 d6 00 33 de 92 ac 32 02
31 61 1a a8 ee a1 71 aa ed ff a8 96 38 10 04 20 9a 15 7a 98 c7 8a aa d8
2d 9b 27 63 16 a4 73 30 6b 29 d0 5c 69 14 cb 79 88 c6 1e b2 47 8e a3 ae
88 1a af 87 9b 27 1a b8 16 6d 83 e0 25 6c 14 93 e5 3e 2c 0d 54 5b 33 39
e5 9b a7 c2 5b 69 ff 7d 0b f8 f6 00 eb 46 1b 9b 9d f1 b1 02 d0 60 eb 1f
5e 3b 6f 32 1e 0c 4f 3a 90 6c 1d 7f 0d 5a 2a c6 54 a3 ec d2 0f 08 8c 5a
67 16 a6 c7 30 4f 67 bb 6a e1 ff d5 b5 82 02 79
```

○10進法表記（MacOSXのbcで変換）

```
23108186250418140377406809438455149911472461326698612855219
17240133815018828563136990025269394808310419260580801198967
30046271654200811700684368160252964742205430906094320627072
00120377859873970269873603684376373759639254546606000328635
83630867538185908790359601910452925123246657304899503830344
02742448761516403872645555172774624176765170052775063198365
25728849134576390828774819494643018590986126994640443567849
14615675070572475913372810446978219202634574916640812051794
62701366978998174045887621688575850676684009060624324095869
26592509208413010052545271003319067067049906564675648483181
46801825910489721
```

だから, p, qとしては**300桁程度の素数**が選ばれています. また, もう1つの公開鍵eの値は, $65537 = 2^{16} + 1$が使われています.

秘密鍵dを持たない第3者が解読するためには, $ed \equiv 1 \pmod{(p-1)(q-1)}$を解かなければならないが, nが**数百桁の素数の積**なので$n = pq$に**素因数分解することは非常に困難**である. 従って, $p-1, q-1$の値を求めることも困難であり, 秘密鍵dを入手することは**事実上不可能**である（**不可能なわけではない**）.

_____組 _____番 _____

もし, 600桁の整数を**全ての素数で割れるかどうか**で素因数分解をするならば・・・

素数定理によると・・・
☎ ガウスとルジャンドルが予想
☎ ド・ラ・ヴァレー・プッサンとアダマールが証明

$\sqrt{10^{600}} = 10^{300}$までの素数の個数は, およそ_____個

高性能のコンピュータを利用して, 1秒間に1億$= 10^8$個の約数かどうかの判定ができるとすると,

1年間では, $10^8 \times \_\_ \times \_\_ \times \_\_ \times \_\_\_\_ =$ _____ $\fallingdotseq$ _____個

したがって, 全てのチェックを終える（最悪の場合）ためには,

_____ かかる・・・

素数定理

ガウスは**素数の載った表を眺め, 統計的に考える**ことによってx以下の素数の個数$\pi(x)$が$\dfrac{x}{\log x}$に大体等しいことを発見しています（**15歳で！**）.

☎ $\log x$は数学IIIで出てくる**自然対数**です.

☆確認してみましょう☆

x	10	100	1000
$\log x$	2.3	4.6	6.9
$\dfrac{x}{\log x}$			
$\pi(x)$			

☎ 数値表があります