素数の逆数の不思議

小学校では

$$\frac{1}{2}=0.5,\quad \frac{1}{3}=0.333\cdots,\quad \frac{1}{5}=0.2$$

などのように分数を小数に直すということをよくやっていたと思います. ところが, 中学校では「数値計算は分数でとめるように」と教わって以来, 数学の世界では小数はあまり顔を出さなくなりました. 「しょうすう」なだけに彼らは数学の世界で肩身を狭くしていると思います. そんな小数ですが, 少し目を向けると面白い世界が見えてきます. では, 問題です.

$$\frac{1}{12377}\text{の小数第 6193 桁目の値を求めよ.}$$

毎年東北大学理学部数学科のオープンキャンパスではイベントとして数学クイズを行っています. 解けたらジュースがもらえるというご褒美つきです. 上の問題は黒木先生（黒木さん）が 2009 年に出題されたものです (注釈にある URL からダウンロードできます) [*1]. 電卓をたたけば頑張れますがこれはナンセンスです. もちろん出題者もそのように解くことを意図していません. 問題を解くためにいくつかヒントが与えられており, ヒントを用いるとちゃんと解けるようになっています. しかし, ヒントが正しいことの証明が問題文中では与えられていません. 実はこのヒントに隠れているカラクリがとても面白く, 証明には整数論における有名な定理をつかいます. このノートはヒントとして書かれている事実に対して証明を与えることを目的に書いてあります. 代数学における群論の初歩と整数論の合同式の性質の知識があれば読めるようになっています.

循環小数

以下の小数は「142857」という数の列が周期的にずっとならぶものになっています. このような小数は循環小数 と呼ばれています.

$$0.142857142857142857\cdots$$

「142857」という列をこの小数の**循環節**と呼ぶことにします. これは 1/7 の値ですが, 循環節だけを用いて

$$\frac{1}{7}=0.\dot{1}42857\dot{}$$

と表記する方法もありましたね. 循環節の数の長さを**循環節の長さ**とよびましょう. 例えば, 1/7 の場合は循環節の長さは 6 です. 以下, 分母に来る数は 2, 5 以外の素数に限定します. 問題として挙げた 12377 も計算すれば素数になることがわかります. 一つ命題を挙げておきます.

命題. p を 2, 5 以外の素数とする. このとき $1/p$ は循環小数になる.

Proof. p は 2, 5 以外の素数なので, 10 と互いに素になることに注意する. 10 の $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ の乗法群 $\mathbb{F}_p^\times$ における位数を e とおく. つまり, e を

$$10^e\equiv 1 \mod p.$$

をみたす最小の正の数のこととします. このとき $10^e-1=pa$ という正の整数 a が存在するので

$$\frac{1}{p}=\frac{a}{pa}=\frac{a}{10^e-1}=\frac{a}{10^e}\frac{1}{1-\left(\frac{1}{10^e}\right)}=\frac{a}{10^e}+\frac{a}{10^{2e}}+\frac{a}{10^{3e}}+\cdots.$$

$a<ap<10^e$ からこれは $1/p$ が循環小数になることを意味する. 例えば $a=123, 10^e=1000$ を考えると第一項は 0.123 で第二項目は 0.000123 となる. 第三項目も同様. □

上で述べた命題から 2, 5 以外の素数の逆数は必ず循環小数になることがわかりました. 前命題の証明をよくみると e は循環節の長さになっていることがわかります. 有限群の一般論によって e は $p-1$ の約数になることがわかります.

[*1] http://www.math.tohoku.ac.jp/ kuroki/LaTeX/OpenCampus2009-Problem.pdf

ヒント (1)

オープンキャンパスのヒント (1) を紹介します. このことは直前に述べたことから明らかです.

ヒント (1)

2, 5 以外の素数 p について $1/p$ を循環小数で表示したとき, 循環節の長さは必ず $p-1$ の約数になる.

高校の教科書数 I を読むと「有理数は小数に直すと有限小数か循環小数になることが知られている」という記述がありますが, 上の命題は特殊な場合の主張になっています. 余力があれば一般の場合に対しての証明を考えてみてください. 逆に循環小数は分数の形に直せるというのは数 III のテキストを見るとわかります.

ヒント (2)

さて, 前ページにもありましたように

$$\frac{1}{7} = 0.\dot{1}42857\dot{}$$

が成り立っていました (電卓をたたかずに手計算で確かめてください). 142857 が循環節ですが, 特に長さが偶数と言うことに注意しておきましょう. 前半の数列「142」を普通の数「ひゃくよんじゅうに」, 後半の数列「857」を普通の数「はっぴゃくごじゅうなな」とおもいましょう. 簡単な計算で

$$142 + 857 = 999$$

となります. ありゃまー不思議! (と思ってください). 電卓をたたいてもいいので $p = 11, 13$ などで成立するかどうかもためしてください:

例 1.

$$\begin{aligned}
1/11 &= 0.\dot{0}\dot{9}\ , \\
1/13 &= 0.\dot{0}76923\dot{}\ , \\
1/17 &= 0.\dot{0}588235294117647\dot{}\ , \\
1/19 &= 0.\dot{0}52631578947368421\dot{}\ .
\end{aligned}$$

ヒント (2) は以下の通りです.

ヒント (2)

p を 2, 5 以外の $1/p$ の循環節の長さが偶数のとき, 循環節を前半, 後半に分けてそれぞれを a, b と書くと $a + b = 99\cdots9$ が成立する.

• ヒント (2) の証明. e を $\mathbb{F}_p^\times$ における 10 の位数とする. e は偶数なので $e = 2e'$ と置くと, $10^{e'}$ は

$$x^2 \equiv 1 \mod p$$

の解ということから $10^{e'} \equiv -1 \mod p$ が成立する. よって

$$\frac{10^{e'} + 1}{p}$$

は整数となる. $1/p$ を少数であらわして

$$\frac{1}{p} = 0.\dot{a_1}a_2\cdots a_{e'}a_{e'+1}\cdots a_{e-1}\dot{a_e}$$

とする. このとき

$$\frac{10^{e'}}{p} = a_1a_2\cdots a_{e'}.a_{e'+1}\cdots a_{e-1}a_e\cdots$$

となるから $1 = 0.999\cdots$ という事実を認めれば $a_n + a_{e'+n} = 9$ $(n = 1, 2, \ldots, e')$ がしたがう. □

注意. 値が少ない素数だけでみると 2, 5 以外の全ての素数の逆数の循環節は偶数！と思いたくなりますが, 一般に正しくはないです. 簡単な反例として $p=3$ や $p=37$ の場合です. 実際,$1/3=0.\dot{3}$ $1/37=0.\dot{0}2\dot{7}$ です. すこし長くなる例として $p=31$ があります. 実際. $1/p=31=0.\dot{0}32258064516129\dot{0}$ となって循環節の長さは 15 です.

ヒント (2) に続いてヒント $(2')$ が用意されています.

ヒント $(2')$

p を $2,5$ でない素数とする. $1/p$ を小数で表し, 小数点第 $(p-1)$ 桁までを前半 a と 後半 b にわけたとする. このとき, 後半の最初の桁が 9 ならばヒント (2) と同様に $a+b=99\cdots9$ が成立する.

「$((p-1)/2+1)$ 桁目が 9」となるときはどんな時？という疑問が出ますが, そのこたえはヒント (3) を見ればわかります. ヒント $(2')$ の証明は後回しにしてつぎにすすむことにします.

ヒント (3)

次のヒントは素数の情報から 特定の桁の値が決定できる ことを述べています.

ヒント (3)

p を 11 以上の素数とする. $1/p$ の小数第 $((p-1)/2+1)$ 桁目は 0 または 9 になる. もっと言うと次が成り立つ:

$$p\equiv 1,3,9,13,27,31,37,39 \mod 40 \iff 1/p \text{ の小数第 } ((p-1)/2+1) \text{ 桁目は } 0\ .$$
$$p\equiv 7,11,17,19,21,23,29,33 \mod 40 \iff 1/p \text{ の小数第 } ((p-1)/2+1) \text{ 桁目は } 9\ .$$

ヒント (3) を証明するためにいくつか整数論で有名な定理を持ちだしましょう.

Legendre symbol

定義. p を奇素数 (すなわち, 2 以外の素数) とします. a を p と互いに素な整数とする.Legendre symbol $\left(\frac{a}{p}\right)$ を以下のように定義します:

$$\left(\frac{a}{p}\right):=\begin{cases}1 & x^2=a \mod p \text{ という整数 } x \text{ が存在する }, \\ -1 & x^2=a \mod p \text{ という整数 } x \text{ が存在しない.}\end{cases}$$

Legendre symbol の諸定理

命題. p を奇素数とする. p と互いに素な $a,b\in\mathbb{Z}$ について次が成り立つ.

$$a\equiv b \mod p \Longrightarrow \left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)\ .$$
$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ .$$
$$\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \mod p \quad \text{(Euler の規準).}$$

定理. $p,\ q$ を異なる奇素数 (2 以外の素数) とするこの時, 次がなりたつ.

$$\text{(平方剰余の相互法則) } \left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\ .$$
$$\text{(第一補充法則) } \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1 & p\equiv 1 \mod 4\ , \\ -1 & p\equiv -1 \mod 4\ .\end{cases}$$
$$\text{(第二補充法則) } \left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & p\equiv \pm 1 \mod 8\ , \\ -1 & p\equiv \pm 3 \mod 8\ .\end{cases}$$

では, ヒント (3) を解くための準備として

$$\left(\frac{10}{p}\right) = 1$$

が成り立つ必要十分条件を見つけましょう. ただし, ここでは p は 5 以外の奇素数としましょう.

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) \equiv p^2 \mod 5 = \begin{cases} 1 & p \equiv \pm 1 \mod 5, \\ -1 & p \equiv \pm 2 \mod 5 \end{cases}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \mod 8, \\ -1 & p \equiv \pm 3 \mod 8. \end{cases}$$

従って,

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right) = 1$$

に注意すると

$$\begin{cases} p \equiv a \mod 5, \\ p \equiv b \mod 8 \end{cases}$$

という合同式の連立方程式を満たす素数 p を求める計算がどうしても必要です. 中国式剰余定理の一般論から上の条件を満たす p は 40 を法としてさだまり, 具体的には $-24a + 25b \mod 40$ が求めたい値になります. ちまちま計算していけば次の結果を得るはずです.

計算結果

p を 2, 5 以外の素数とする.

$$p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \mod 40 \quad \Leftrightarrow \quad \left(\frac{10}{p}\right) = 1 \quad \Leftrightarrow \quad 10^{\frac{p-1}{2}} \equiv 1 \mod p.$$

$$p \equiv 7, 11, 17, 19, 21, 23, 29, 33 \mod 40 \quad \Leftrightarrow \quad \left(\frac{10}{p}\right) = -1 \quad \Leftrightarrow \quad 10^{\frac{p-1}{2}} \equiv -1 \mod p.$$

が成立する.

• ヒント (3) の証明. $10^{(p-1)/2}$ を p で割った余り $10^{(p-1)/2} \mod p$ を計算する. これは x に関する方程式 $x^2 \equiv 1 \mod p$ の解なので $10^{(p-1)/2} \mod p \equiv \pm 1$ がわかる.

- $10^{\frac{p-1}{2}} \equiv 1 \mod p$ の場合.
  循環節の長さは $(p-1)/2$ の約数になる. 小数点第 $(p-1)/2$ 桁目の値を $\oplus$ と置く. $1/p$ を小数で表示したとき

$$\frac{1}{p} = 0.\underbrace{0\cdots}_{\text{循環節}}\underbrace{0\cdots}_{\text{循環節}} \cdots \underbrace{0\cdots\oplus}_{\text{循環節}}\underbrace{0\cdots}_{\text{循環節}}\cdots$$

  となっていることを意味する (p が 11 以上の素数なので小数点 1 桁目が 0 になっていることに注意したい). よって小数点第 $(p-1)/2+1$ 桁目の値は 0 となる.

- $10^{\frac{p-1}{2}} \equiv -1 \mod p$ の場合. 次の合同式が成り立つことに注意する:

$$10^{\frac{(p-1)}{2}} \equiv -1 \equiv p-1 \mod p, \quad 10^{\frac{(p-1)}{2}+1} \equiv -10 \equiv p-10 \mod p.$$

  一方, $p - 10 > 0$ ということと, われわれが 少数第 $\frac{p-1}{2}+1$ 桁目を筆算するときに

$$(p-1)10 - pa_{\frac{p-1}{2}+1} = p - 10$$

  という計算を実行していることに注意する. これから $a_{\frac{p-1}{2}+1} = 9$. がわかる.
  後は上の計算結果と合わせると主張が得られる.

□

上の証明から次のことがすぐ分かります. これはヒント (3') として与えられています.

ヒント (3')

p を $2,5$ 以外の素数とする.

$p \equiv 1,3,9,13,27,31,37,39 \mod 40 \iff 1/p$ の循環節の長さは $(p-1)/2$ の約数.

$p \equiv 7,11,17,19,21,23,29,33 \mod 40 \iff 1/p$ の循環節の長さは $(p-1)/2$ の約数でない.

最後に, ヒント (2') の証明を与えましょう.

ヒント (2') の証明

Proof. p は 11 以上の素数としてよい. $1/p$ の小数第 $(p-1)/2+1$ 桁目が 9 ならば, 今までの考察によって

$$10^{\frac{p-1}{2}} \equiv -1 \mod p$$

でないといけない.

$$\frac{1}{p} = 0.a_1 a_2 \dots a_{\frac{p-1}{2}} a_{\frac{p-1}{2}+1} \cdots a_{p-1} \cdots$$

とすると, ヒント (2) の証明における e' の部分を $\frac{p-1}{2}$ に置き換えた結果によれば

$$a_n + a_{\frac{p-1}{2}+n} = 9 \quad \left(n = 1, 2, \dots, \frac{p-1}{2}\right).$$

□

補足

実は 11 以上の素数で小数第 $((p-1)/2+1)$ 桁目が 9 ならば, 循環節の長さは偶数となる ことがわかります.

Proof. ヒント $(3')$ によって $1/p$ の循環節の長さを e としたとき, e は $p-1$ の約数でかつ $(p-1)/2$ の約数でないということがわかります.

$$a := \frac{p-1}{2} = 2^{k_0} q_1^{k_1} \dots q_r^{k_r}$$

と素因数分解する. ただし, $q_1, \dots, q_r$ は奇素数で, $k_0 \geq 0, k_1, \dots, k_r \geq 1$ である. このとき

$$p-1 = 2^{k_0+1} q_1^{k_1} \dots q_r^{k_r}$$

となる. e は $p-1$ の約数なので e は

$$e = 2^{f_0} q_1^{f_1} \dots q_r^{f_r}$$

と書ける. これから

$$\begin{cases} f_0 \leq k_0 + 1 & \cdots (1) \\ f_i \leq k_i \quad (1 \leq i \leq r) & \cdots (2) \end{cases}$$

が成り立つことに注意しよう. 一方で, e は a の約数でないので $f_j > k_j$ となる $j \in \{0, 1, \dots, r\}$ が存在しないといけないが, 上の $\cdots (2)$ から $j = 0$ でないといけないことが分かる. これは $0 \leq k_0 < f_0$, 故に, $1 \leq f_0$ を意味するので, e が偶数であることが分かる. □

注意. 11 以上の素数で小数第 $((p-1)/2+1)$ 桁目が 9 でない (つまり 0 のである) ときでも循環節の長さは偶数になる時はあります. 例えば $p = 13, 89, 157$ の場合です (40 で割った余りを考えヒント (3) と照らし合わせてみましょう). これらの循環節の長さはそれぞれ 6, 44, 78 になります.

Appendix 1：パソコンで確かめてみよう

p が大きくなると通常の電卓では対応できません．C++ で $1/p$ を少数にするプログラム[*2]を作りました．

```
#include<iostream.h>
int quotient(int,int);//a をｂで割ったときの商をもとめる。
int main(void)
{
int p ;
cout<<"これは１/p を小数展開するプログラムです．割る数 p を入力してください．"<<endl;
cout<<"p"<<endl;
cin>>p ;//割る数を p とおく。
cout<<"少数第何桁までを出したいですか？ただし、１０万桁までが限界です．"<<endl;
int m ;//出力する桁数を m とおく。
cin>> m ;
int Q[100000] ;//出力した値を入れる箱
int q=quotient(10,p);
int r=10%p ;
for(int i=0;i<m+1;i++)
{
Q[i]=q;
q=quotient(10*r,p);
r=(10*r)%p;
}//我々人間が筆算をする手続きを再現している。a%b で a を b で割った余りを表す。
cout<<"結果は"<<endl;
cout<<"1/p=0.";
for(int i=0 ; i<m ; i++)
{cout<<Q[i] ;}//最終的な結果を出力する
cout<<""<<endl;
cout<<"ちなみに第"<<m<<"桁目は"<<Q[m-1]<<"である．"<<endl;//桁数を出す
return 0;
}

int quotient(int a,int b)
{int s;
s=(a-(a%b))/b ;
return s ;
}
```

[*2] プログラムに関してはあまり詳しくないので無駄な表記があったりするかもしれません．

Appendix 2：Legendre symbol の諸定理の証明

ここでは Legendre symbol の証明を与えることにします.

命題 (Euler 規準)**.** p を奇素数とする. p と互いに素な $a \in \mathbb{Z}$ に対して

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p.$$

Proof. $a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$ であるから次を示せば十分:

Claim.

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} = 1 \mod p.$$

実際, $x^2 \equiv a \mod p$ という $x \in \mathbb{Z}$ が存在したとする. x と p は互いに素なので, フェルマーの小定理から

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p.$$

逆に, $a^{\frac{p-1}{2}} = 1 \mod p$ のとき, g を $\mathbb{F}_p^\times$ の原始根とし, $a = g^r \mod p$ となっているとする.

$$g^{r\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \mod p.$$

となる. よって, $r(p-1)/2$ は $p-1$ の倍数. よって $r/2$ は整数. これは a の g に関する指数 r が偶数と言うことを意味している. ゆえに

$$\left(\frac{a}{p}\right) = 1.$$

□

したがって, Legendre symbol を次のように定義し直すことも可能です:

定義. p を奇素数として, a を p と互いに素な 整数とする. このとき,

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \mod p$$

と定める.

命題. p を奇素数とする. a, b を p と互いに素な整数とする. このとき,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Proof. Euler 規準から

$$\text{L.H.S} = (ab)^{\frac{p-1}{2}} \mod p = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \mod p = \text{R.H.S}\ .$$

□

以上で「Legendre symbol の諸定理」で述べた前半の命題の証明が終わりました. 以下, 補充法則, および相互法則を三角関数を用いた Serre の数論講義 (岩波書店) にのっとって示していきます. 後半の証明のために次に述べる「Gauss の補題」を示します. そのためにます, 記号の準備からはじめていきましょう. p を奇素数とします.

$$S := \left\{1, 2, \cdots, \frac{p-1}{2}\right\},\ -S := \left\{-1, -2, \cdots, -\frac{p-1}{2}\right\}$$

と置いて, $\mathbb{F}_p^\times$ の完全代表系を $S \cup (-S)$ でとることにします. $\mathbb{F}_p^\times = S \cup -S$ のもとで, $a \in \mathbb{F}_p^\times, s \in S$ に対し $as \equiv e_s(a)s_a \mod p$ という $e_s(a) \in \{\pm 1\}, s_a \in S$ が一意に定まることに注意しましょう.

補題 (Gauss の補題)**.** 奇素数 p と互いに素な $a \in \mathbb{Z}$ について

$$\left(\frac{a}{p}\right) = \prod_{s \in S} e_s(a).$$

Proof.

Claim. $a \in \mathbb{Z}$, $s, s' \in S$ $(s \neq s')$ について $s_a \neq s'_a$.

実際, $s_a = s'_a$ ならば

$$as \equiv \pm s_a = \pm s'_a \equiv \pm as'(\text{複合任意})$$

となる. $s \neq s'$ だから $s = -s'$ を要請するが,

$$s, s' \in S = \left\{1, 2, \cdots, \frac{p-1}{2}\right\}$$

を考えると, これはあり得ないということがわかる. これで **Claim.** の証明が終わった.

以上で

$$S \ni s \longmapsto s_a \in S$$

の対応が全単射となることがわかった. よって

$$a^{\frac{p-1}{2}} \left(\prod_{s \in S} s\right) = \prod_{s \in S} as = \prod_{s \in S} e_s(a) s_a = \left(\prod_{s \in S} e_s(a)\right)\left(\prod_{s \in S} s_a\right) = \left(\prod_{s \in S} e_s(a)\right)\left(\prod_{s \in S} s\right).$$

$$\therefore \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \left(\prod_{s \in S} e_s(a)\right).$$

□

命題 (第二補充法則)**.** p を奇素数とするこのとき, つぎがなりたつ:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8, \\ -1 & \text{if } p \equiv \pm 5 \mod 8. \end{cases}$$

Proof. $p = 3$ の場合はすぐにわかるので $p \geq 5$ の場合を証明する. $s \in S$ に対して

$$2s \leq \frac{p-1}{2} \equiv e_s(2) = 1$$

なので

$$n(p) = \left| \left\{ s \in \mathbb{Z}\,;\, \frac{p-1}{2} < 2s \leq p-1 \right\} \right|$$

とおく. Gauss の補題から

$$\left(\frac{2}{p}\right) = \prod_{s \in S} e_s(2) = \prod_{\frac{p-1}{2} < 2s \leq p-1} (-1) = (-1)^{n(p)}$$

が従う. $n(p)$ がどうなるかで $\left(\frac{2}{p}\right)$ の値がわかるので, $n(p)$ の振る舞いを調べることにする. 素数 p が 8 を法として 1, 5, -1, -5 のどれかと合同になる. 各々の場合について次が成り立つことに注意しよう.

$$\begin{aligned}
p \equiv 1 \mod 8 &\Longrightarrow p = 8l+1\ (^\exists l \in \mathbb{Z}\,) \Longrightarrow p = 4k+1 \quad (k = 2l), \\
p \equiv 5 \mod 8 &\Longrightarrow p = 8l+5\ (^\exists l \in \mathbb{Z}\,) \Longrightarrow p = 4k+1 \quad (k = 2l+1), \\
p \equiv -1 \mod 8 &\Longrightarrow p = 8l-1\ (^\exists l \in \mathbb{Z}\,) \Longrightarrow p = 4k+3 \quad (k = 2l-1), \\
p \equiv -5 \mod 8 &\Longrightarrow p = 8l-5\ (^\exists l \in \mathbb{Z}\,) \Longrightarrow p = 4k+1 \quad (k = 2(l-1))
\end{aligned}$$

Claim. 5 以上の素数 p に対して,

- $p = 4k+1$ ($^\exists k \in \mathbb{Z}$) $\Longrightarrow n(p) = k$,
- $p = 4k+3$ ($^\exists k \in \mathbb{Z}$) $\Longrightarrow n(p) = k+1$.

実際

- $p = 4k+1$ ($^\exists k \in \mathbb{Z}$) の場合

$$\frac{p-1}{2} < 2s \leq p-1 \Longleftrightarrow 2k < 2s \leq 4k \Longleftrightarrow k < s \leq 2k. \qquad \therefore n(p) = k.$$

- $p = 4k+3$ ($^\exists k \in \mathbb{Z}$) の場合

$$\frac{p-1}{2} < 2s \leq p-1 \Longleftrightarrow 2k+1 < 2s \leq 4k+2 \Longleftrightarrow k+1 \leq s \leq 2k+1. \qquad \therefore n(p) = k+1.$$

よって **Claim.** が示された. このことから

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \mod 8, \\ -1 & \text{if } p \equiv \pm 5 \mod 8. \end{cases}$$

がわかる. この分岐条件は $(-1)^{\frac{p^2-1}{8}}$ と一致することは容易にわかる. □

命題 (第一補充法則)**.**

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4, \\ -1 & \text{if } p \equiv -1 \mod 4. \end{cases}$$

Proof. 定義から

$$e_s(-1) = -1 \ \forall s \in S$$

がわかるので, Gauss の補題から

$$\left(\frac{-1}{p}\right) = \prod_{s \in S}(-1) = (-1)^{\frac{p-1}{2}}$$

となる. $(-1)^{\frac{p-1}{2}}$ が条件式と一致するのは容易にわかる. □

いよいよ平方剰余の相互法則の証明をみていこう. 次の三角法の補題が Key になる.

命題 (三角法の補題)**.** q を正の奇数とする. このとき次の恒等式が成り立つ:

$$\frac{\sin(qx)}{\sin x} = (-4)^{\frac{q-1}{2}} \prod_{t=1}^{\frac{q-1}{2}} \left(\sin^2 x - \sin^2\left(\frac{2\pi t}{q}\right)\right).$$

三角法補題の証明のために次の補題を示す.

補題. 正の整数 n に対して, 最高次係数が $(-4)^n$ の整数係数 n 次多項式で, 次の条件を満たす $\Phi_n(X) \in \mathbb{Z}[X]$ が存在する:

$$\frac{\sin(2n+1)x}{\sin x} = \Phi_n(\sin^2 x).$$

Proof. オイラーの公式によって

$$\begin{aligned} e^{i(2n+1)x} &= (\cos x + i \sin x)^{2n+1} = \cos((2n+1)x) + i \sin((2n+1)x) \\ &= \sum_{j=0}^{2n+1} \binom{2n+1}{j} (\cos x)^{2n+1-j} (i \sin x)^j \end{aligned}$$

j が偶数か奇数かで場合分けする.

$$= \sum_{j=0}^{n} \binom{2n+1}{2j} (\cos x)^{2n+1-2j} (-1)^j \sin^{2j} x + i \sum_{j=0}^{n} \binom{2n+1}{2j+1} (\cos x)^{2n-2j} (-1)^j (\sin x)^{2j+1}$$

となる. 両辺の虚部をとって整理すると

$$\frac{\sin(2n+1)x}{\sin x} = (-1)^n \sum_{j=0}^{n} \binom{2n+1}{2j+1} (\sin^2 x - 1)^{n-j} \sin^{2j} x$$

となる.

Claim.

$$\Phi_n(X) := (-1)^n \sum_{j=0}^{n} \binom{2n+1}{2j+1} (X-1)^{n-j} X^j$$

とおくと, これが求めたい n 次多項式である.

実際,

$$\frac{\sin(2n+1)x}{\sin x} = \Phi(\sin^2 x)$$

は明らかなので, 最高次係数を調べればよい.

$$\begin{aligned}
\Phi(X) \text{ の最高次係数} &= (-1)^n \sum_{j=0}^{n} \binom{2n+1}{2j+1} \\
&= (-1)^n \sum_{j=0}^{n} \left(\binom{2n}{2j} + \binom{2n}{2j+1} \right) \\
&= (-1)^n \sum_{k=0}^{2n} \binom{2n}{k} = (-1)^n 2^{2n} = (-4)^n.
\end{aligned}$$

これで示すべきことが示された.

□

以下, 三角法の補題の証明を示す. $\Phi_(X) := \Phi_{\frac{q-1}{2}}(X)$ と置き,

$$X_t := \sin^2\left(\frac{2\pi t}{q}\right) \text{ for } t = 1, 2, \cdots, \frac{q-1}{2}$$

と置く. 前補題から

$$\Phi(X_t) = \frac{\sin\left(q \cdot \frac{2\pi t}{q}\right)}{\sin\left(\frac{2\pi t}{q}\right)} = 0 \text{ for } t = 1, 2, \cdots, \frac{q-1}{2}$$

ということがわかるので,

$$\Phi(X) = (-4)^{\frac{q-1}{2}} \prod_{t=1}^{\frac{q-1}{2}} \left(X - \sin^2\left(\frac{2\pi t}{q}\right) \right).$$

よって,

$$\frac{\sin(qx)}{\sin x} = \Phi(\sin^2 x) = (-4)^{\frac{q-1}{2}} \prod_{t=1}^{\frac{q-1}{2}} \left(\sin^2 x - \sin^2\left(\frac{2\pi t}{q}\right) \right).$$

□

最後にわれわれの最終目標である平方剰余の相互放送の証明に入る. 三角関数周期性と $\sin(-x) = -\sin x$ という性質をうまく利用することによってによって, Legendre symbol

$$\left(\frac{p}{q}\right)$$

が p と q を入れ換えるときにどれくらいの符号のズレが生じるかを教えてくれる.

定理 (平方剰余の相互法則)**.** p, q を相異なる奇素数とする. このとき, 次が成り立つ:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

Proof.

$$S := \left\{1, 2, \cdots, \frac{p-1}{2}\right\},\ T := \left\{1, 2, \cdots, \frac{q-1}{2}\right\}$$

とおく. $s \in S$ に対して, $qs \equiv e_s(q)s_q \mod p$ より三角関数の周期性を利用すると,

$$\sin\left(\frac{2\pi s}{p}q\right) = e_s(q)\sin\left(\frac{2\pi s_q}{p}\right)$$

となる. 対応 $S \ni s \longmapsto s_q \in S$ の全単射性と Gauss の補題から

$$\left(\frac{q}{p}\right) = \prod_{s\in S} e_s(q) = \prod_{s\in S}\left(\sin\left(\frac{2\pi s}{p}q\right) \Big/ \sin\left(\frac{2\pi s_q}{p}\right)\right) = \prod_{s\in S}\left(\sin\left(\frac{2\pi s}{p}q\right) \Big/ \sin\left(\frac{2\pi s}{p}\right)\right)$$

がわかる. 三角法の補題を適用すれば

$$\begin{aligned}\prod_{s\in S}\left(\sin\left(\frac{2\pi s}{p}q\right) \Big/ \sin\left(\frac{2\pi s}{p}\right)\right) &= \prod_{s\in S}(-4)^{\frac{q-1}{2}} \prod_{t\in T}\left(\sin^2\left(\frac{2\pi s}{p}\right) - \sin^2\left(\frac{2\pi t}{q}\right)\right) \\ &= (-4)^{\frac{q-1}{2}\frac{p-1}{2}} \prod_{s\in S, t\in T}\left(\sin^2\left(\frac{2\pi s}{p}\right) - \sin^2\left(\frac{2\pi t}{q}\right)\right)\end{aligned}$$

$$\therefore \left(\frac{q}{p}\right) = (-4)^{\frac{q-1}{2}\frac{p-1}{2}} \prod_{s\in S, t\in T}\left(\sin^2\left(\frac{2\pi s}{p}\right) - \sin^2\left(\frac{2\pi t}{q}\right)\right).$$

また, 議論の対称性から p, q, S, T の立場を入れ替えることで,

$$\left(\frac{p}{q}\right) = (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{s\in S, t\in T}\left(\sin^2\left(\frac{2\pi t}{q}\right) - \sin^2\left(\frac{2\pi s}{p}\right)\right).$$

がわかる. 積の中身を $A - B$ という形からから $B - A$ に直すことで

$$\begin{aligned}\left(\frac{p}{q}\right) &= (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{s\in S, t\in T}\left(\sin^2\left(\frac{2\pi t}{q}\right) - \sin^2\left(\frac{2\pi s}{p}\right)\right) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}(-4)^{\frac{q-1}{2}\frac{p-1}{2}} \prod_{s\in S, t\in T}\left(\sin^2\left(\frac{2\pi s}{p}\right) - \sin^2\left(\frac{2\pi t}{q}\right)\right) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).\end{aligned}$$

以上でわれわれの示したかったことがすべて証明された. □