$999\cdots9$ を素数で割ると

東北大学理学部オープンキャンパス数学クイズ

黒木 玄

2009 年 6 月 15 日　 編集者に送った生原稿*

はじめに

私は 2005 年度から 2008 年度にかけて 4 年連続で東北大学理学部オープンキャンパスの数学クイズを担当しました. しかし, 4 年分のネタのすべてを紹介し切れませんし, 話の都合で実際に出した問題を少し変えて紹介したり, 異なる年に出した問題をあたかも同じ年に出したかのように説明してしまうことがあるかもしれません. しかし実際の数学クイズの雰囲気は正しく伝わるように説明するつもりなので御了承お願い致します. (実際に出した問題は [1] で公開してあります.)

1　明日は数学クイズの日だ!

大学が夏休みに入った直後の某年某月某日. 東北大学理学部では毎年オープンキャンパスを開催しており, 数学科では研究室見学や体験授業の他に数学クイズを実施している. 数学クイズはオープンキャンパスにやって来たお客さんたちに数学のクイズを解いてもらうという企画である. 実は今年も数学クイズの係に当たってしまった. 主なお客さんは高校生. 1 年生もやって来る. 高校 1 年生でも解ける問題でしかも数学の世界の面白さの一端に触れることができる問題を出さなければいけない. これは大変だ. 正直言って自信がない. 係に当たってしまったものは仕方がない. なんとかしなければいけない.

出す問題はもう決めてある.

問題 1. 10^{222} を 23 で割った余りを求めよ.

問題 2. 99999 のように 9 だけがならんでいる数が 19 で割り切れるためには 9 をいくつならべればよいか?

問題 3 (お持ち帰り問題). 正の整数 n, e を

$$n = 116232311005172322403$$

$$e = 48154933114927891117$$

と定める. 10 文字以内の文を下のコード表にしたがって数字 m に変換する. m の暗号化 c を $c =$ (m^e を n で割った余り) と定める.

$$c = 26827231170163415492$$

であるとき, 暗号を破ってもと文を解読せよ. 実際の解読は手計算ではほとんど不可能だろう. 自宅や高校に帰った後にパソコンなどを使って問題を解くことに挑戦して欲しい.

たとえば文 "うなぎをたべたい" に対応する数字 m はどうなるか. コード表にしたがって各文字が

$$う \to 22,\ な \to 40,\ ぎ \to 76,\ を \to 64,$$
$$た \to 35,\ べ \to 93,\ た \to 35,\ い \to 21$$

と変換されるので $m = 2240766435933521$ となる. このとき m の暗号化 c は m^e を n で割った余りであり, $c = 16338511021545418035$ となる.

コード表

	0	1	2	3	4	5	6	7	8	9
0		ー	「	」	（	）	、	。	！	？
1	0	1	2	3	4	5	6	7	8	9
2	あ	い	う	え	お	か	き	く	け	こ
3	さ	し	す	せ	そ	た	ち	つ	て	と
4	な	に	ぬ	ね	の	は	ひ	ふ	へ	ほ
5	ま	み	む	め	も	や	ゆ	よ	ら	り
6	る	れ	ろ	わ	を	ん	ぁ	ぃ	ぅ	ぇ
7	ぉ	っ	ゃ	ゅ	ょ	が	ぎ	ぐ	げ	ご
8	ざ	じ	ず	ぜ	ぞ	だ	ぢ	づ	で	ど
9	ば	び	ぶ	べ	ぼ	ぱ	ぴ	ぷ	ぺ	ぽ

1.1　合同式

問題のヒントとして以下のように合同式について説明しておく予定になっている.

*数学セミナー 2009 年 8 月号に掲載.

a, b は整数であり, n は正の整数であるとする. $a-b$ が n で割り切れるとき,

$$a \equiv b \pmod n$$

と書き, a と b は n を法として合同であると言う. たとえば $1 \equiv 4 \pmod 3$, $2 \equiv -3 \pmod 5$ である. $a \equiv b \pmod n$ は a と b を n で割った余りが互いに等しいということだと考えてもよい.

合同式の便利な点は足し算や掛け算の計算において $\equiv \ (\mathrm{mod}\ n)$ をあたかも普通の等号のように扱って構わないことである. より正確には次の通り.

一般に $a \equiv a' \pmod n$ かつ $b \equiv b' \pmod n$ のとき $a+b \equiv a'+b' \pmod n$ と $ab \equiv a'b' \pmod n$ が成立する. 実際 $a-b$ と $a'-b'$ が n で割り切れ, $a-a' = kn$, $b-b' = ln$ と表わされているとき, $(a+b)-(a'+b') = a-a'+b-b' = kn+ln = (k+l)n$ であり, $ab-a'b' = (a'+kn)(b'+ln)-a'b' = a'ln+kb'n+kln^2 = (a'l+kb'+kln)n$ となるので, $(a+b)-(a'+b')$ も $ab-a'b'$ も n で割り切れることがわかる.

たとえば $8 \equiv 1 \pmod 7$ なので $8^3 \equiv 1^3 \pmod 7$ となる. 実際に 8^3 を計算してそれを 7 で割った余りを求めるのは面倒だが, 1^3 を計算するのは超やさしい. 合同式について知っていれば 8^3 を計算せずに 8^3 を 7 で割った余りが 1 になることがわかる. (この考え方は問題 1 の大ヒントになっている.)

1.2 合同式の応用

せっかくなので数学クイズの時間に合同式の別の応用も紹介しておくことにしよう. たとえば次の事実が知られている.

与えられた数が 3 で割り切れるかどうかはその数のすべての桁を足し上げた結果が 3 で割り切れるかどうかで判定可能である.

たとえば 534 のすべての桁を足し上げると $5+3+4 = 12$ であり, 12 は 3 で割り切れる. よって 534 も 3 で割り切れる.

このような判定法は合同式の考え方を使えば容易に導き出せる. 10 を 3 で割ると余りが 1 なので $10 \equiv 1 \pmod 3$ である. よって $\equiv \ (\mathrm{mod}\ 3)$ をあたかも等号のごとく扱って良いという事実を使うと

$$534 \equiv 5 \cdot 10^2 + 3 \cdot 10 + 4 \equiv 5+3+4 \pmod 3$$

が成立することがわかる. 3 を法とした合同式では 10 を 1 で置き換えることが許され, その結果 10^2 も $1^2 = 1$ で置き換えられる.

このことに気付けば 3 で割り切れるかどうかだけではなく, 3 で割った余りを少ない手間で計算する方法も得られる.

与えられた数とその数のすべての桁を足しあげた結果を 3 で割った余りは互いに等しい.

実際の計算では全ての桁を足し上げるときに 3 の倍数を無視して構わない. たとえば 1234567 を 3 で割った余りを求めるためには 1 から 7 までの数を 3 の倍数はゼロだとみなして足しあげた結果を求めればよい. $1+2$ や 3 や $4+5$ や 6 は 3 の倍数なのでゼロとみなされるので, 最後の 7 を 3 で割った余りの 1 が答になる.

$10 \equiv 1 \pmod 9$ なので 9 で割った余りについても 3 で割った余りとまったく同様の結果が成立している.

さらに $7 \cdot 11 \cdot 13 = 1001$ を使えば次の結果を導くこともできる.

6 桁の数 a の上 3 桁を b と書き, 下 3 桁を c と書くと, a と $-b+c$ を $7, 11, 13$ で割った余りには等しくなる.

証明は次の通り. 1001 が $7, 11, 13$ で割り切れることより, n が $7, 11, 13$ のどれかならば $1001 \equiv 0 \pmod n$ である. この両辺から 1 を引けば $1000 \equiv -1 \pmod n$ が得られる. この式は $n = 7, 11, 13$ を法とした合同式において 1000 を -1 で置き換えて構わないことを意味している. したがって $n = 7, 11, 13$ のとき $a \equiv 1000b + c \equiv -b + c \pmod n$. この合同式は a と $-b+c$ を $n = 7, 11, 13$ で割った余りが互いに等しくなることを意味している.

たとえば 175342 と $-175+342 = 167$ を $7, 11, 13$ で割った余りは互いに等しい. $7, 11, 13$ で割った余りはそれぞれ $6, 2, 11$ となる.

実際には $n = 11$ の場合には $10 \equiv -1 \pmod{11}$ を使った方が簡単だ. 11 を法とする合同式では 10^k を $(-1)^k$ で置き換えて構わない. たとえば $175342 \equiv -1+7-5+3-4+2 \equiv 2 \pmod{11}$. このように計算した方が上の方法を使うより簡単である.

1.3 フェルマーの小定理

問題 2 は特別な道具を使わなくても直接計算すれば解けるはず. どの程度手間がかかるかを確認するために実際に計算してみよう. (しばらくのあいだ計算が続く. 計算がへたくそなので結構時間がかかってしまう.) できた! この程度の計算なら数学科のオープンキャンパスを見学に来てくれた高校生はやってくれるだろう. しかも実際の計算してみた人だけが

味わえる興奮もある.

しかし, 当日印刷して配布する解答と解説ではフェルマーの小定理に触れておくべきだろう.

フェルマーの小定理. p が素数ならば p で割り切れない任意の整数 a に対して $a^{p-1} \equiv 1 \pmod{p}$.

たとえば $p = 7$, $a = 3$ のとき $3^6 = 729 = 700 + 28 + 1$ なので確かに $3^6 \equiv 1 \pmod{7}$ が成立している.

フェルマーの小定理を $p = 19$, $a = 10$ の場合に適用すれば問題 2 の答が容易に得られ, $p = 23$, $a = 10$ の場合に適用すれば問題 1 を解くための大ヒントが得られる.

興味が湧いた人は他の数字の例でも確認してみるのが良いだろう. 証明を知りたい人は大学生向けの代数学の教科書を見たり, 教わっている高校の数学の先生に聞いて欲しい.

1.4 RSA 暗号

問題 3 の方式の暗号は RSA 暗号と呼ばれていることにも触れておかなければいけない. パソコンによる計算では Maxima という無料で使える数式処理ソフトが便利であることも紹介しておこう. (RSA 暗号と Maxima については後の方で解説をつけます.)

明日が楽しみになって来た. 明日は数学クイズの日だ! (仙台の夏はそんなに暑くありません. 快適な夏の夜のあいだ延々と様々なことを考え続けることになりました.)

2 数学クイズ当日

数学クイズは午後の出し物である. 今年の数学科のオープンキャンパスに訪れた人はすでにン百人を突破したらしい (正確な数字は忘れましたが事実です). ここ数年, 数学の人気が高まっているのか?

数学クイズの会場の教室に高校生とその付き添いの人らしき方々がたくさん入っている. 問題とヒントは数学棟にやって来たお客さんにすでに配布してある.

午後 2 時. 数学クイズの時間の始まりだ. 教室はほとんど満員.

問題 1 または問題 2 を解けた人は手を上げて下さい. 正解できた人には飲み物を配ります.

問題 3 は持ち帰り問題なので自宅もしくは高校に帰ってからじっくり考えて下さい.

スケジュールの都合でこの教室を出て行きたい方は自由にそうして下さい. ただし, 出口そばのテーブルに数学クイズの解答と解説が印刷された紙があるので忘れずに持って帰って下さい.

質問がある人は大学生もしくは大学院生のお兄さんとお姉さんに自由に聞いて下さい.

……などと説明をしながら手が上がるのを待つ.

2.1 問題 1 について

問題 1 を最後までやり遂げた人は少なかった. 10^{22} を 23 で割った余りが 1 になることがわかれば合同式の使い方に関するヒントからすぐに答が求まる. $10^{22} \equiv 1 \pmod{23}$ より $10^{220} \equiv (10^{22})^{10} \equiv 1 \pmod{23}$. よって $10^{222} \equiv 10^{220} \cdot 10^2 \equiv 100 \equiv 8 \pmod{23}$. すなわち 10^{222} を 23 で割った余りは 8 である.

問題は $10^{22} \equiv 1 \pmod{23}$ をどのように導くかである. フェルマーの小定理を $p = 23$, $a = 10$ に適用すればこの結果はただちに得られる. フェルマーの小定理を使わずに直接計算する場合には 22 を $22 = 2 + 4 + 16$ と表わしておき, $10^2 \equiv 8 \pmod{23}$, $10^4 \equiv (10^2)^2 \equiv 8^2 \equiv 18 \equiv -5 \pmod{23}$, $10^8 \equiv (10^4)^2 \equiv (-5)^2 \equiv 2 \pmod{23}$, $10^16 \equiv (10^8)^2 \equiv 2^2 \equiv 4 \pmod{23}$ と $10^2, 10^4, 10^{16}$ について計算し, $10^{22} \equiv 10^2 \cdot 10^4 \cdot 10^{16} \equiv 8 \cdot (-5) \cdot 4 \equiv -160 \equiv 70 \equiv 1 \pmod{23}$ と計算すれば手間をかなり減らせる.

もちろん, このような工夫をしなくても地道に $10, 10^2, 10^3, \ldots$ を 23 で割った余りを合同式を使って求めてもよい. (実際そのような計算で答を出した人もいました.)

2.2 問題 2 について

問題 2 はまじめに挑戦した人のうちかなりの人ができたようだ. 多数派は「9 の個数を増やしながら 19 による割り算の筆算を割り切れるまで続ける」という私が昨晩試してみたのと同じ方法を使っていた. 答は「9 を 18 個ならべると 19 で割り切れる」である.

問題 2 は小学校レベルの問題に見えるかもしれない. しかし, 9 を 18 個ならべて 19 で割る筆算をやり切った人には以下で説明する事実を指摘して楽しんでもらうことができた.

9 の個数を増やしながら 19 で割る筆算を続けた人は結果的に $9, 99, 999, 9999, 99999, \ldots$ を 19 で割った余りを順番に計算したことになる. 9 が 18 個ならんだところで余りがちょうど 0 になる. 割り切れたと

いうことだ．そのあいだに出て来る余りを順番に書くと次のようになる:

$$\begin{array}{ccccccccc} 9, & 4, & 11, & 5, & 2, & 10, & 14, & 16, & 17, \\ 8, & 13, & 6, & 12, & 15, & 7, & 3, & 1, & 0. \end{array}$$

この数列には明らかな規則性がある．まず, 0 から 17 までの数がちょうど一回づつ登場する．さらに i 番目の余りと $i+9$ 番目の余りを足すと (上の余りの表で縦に足すと) すべて 17 になる．これは偶然か?

もちろんこれらの規則性は偶然ではない．偶然でない理由も重要だが, 数学クイズを出す私の立場から見て重要なことはこんなところにも数学の世界の美しい法則が隠れていることである．

数学者は結局のところ「十分に解明されていない数学の世界の美しい法則を明らかにする」という仕事をしている．どこかの偉い先生が提出した難しい数学の問題を一所懸命解いているだけではないのだ．そこに何か普遍的で価値のある法則が隠れているからそれを明らかにしようとしているのである．

$9, 99, 999, 9999, 99999, \dots$ を 19 で割った余りを実際に筆算で計算してみた方々に上の規則性について説明すると目の色が変わる．やはり自分の力でやり遂げた計算結果に驚くべき規則性が隠れていることを知ると誰でも感動してしまうようだ．そういう感動を貴重なことだと感じる人には是非とも数学科に来てもらいたいと私は思うのである．

しばらくのあいだ p は $2, 5$ 以外の素数であるとする．9 を k 個ならべてできる数は $10^k - 1$ に等しい．$10^k - 1$ が p で割り切れることは $10^k \equiv 1 \pmod p$ を意味している．さらに $10, 10^2, 10^3, \dots, 10^{p-1}$ を p で割った $p-1$ 個の余りについて考えよう．フェルマーの小定理から $10^{p-1} \equiv 1 \pmod p$ が成立するので最後の 10^{p-1} を p で割ると余りは 1 である．これ以外に余りが 1 になるものがないと仮定する．そのとき $p = 19$ の場合に見た規則性がそのまま成立していることを示せる (証明は略)．すなわち, 長さが $p-1$ 個の余りの中に 1 から $p-1$ までの数がちょうど一回づつ登場し, i 番目の余りと $i + (p-1)/2$ 番目の余りを足すとすべて p になる．

i 番目の余りと $i + (p-1)/2$ 番目の余りを足すと p になるということは $10^i + 10^{i+(p-1)/2} = 10^i(1 + 10^{(p-1)/2})$ が p で割り切れることを意味する．p は $2, 5$ 以外の素数なのでこれは $10^{(p-1)/2} \equiv -1 \equiv p-1 \pmod p$ を意味する．だから二つ目の規則性を確認するためには $10^{(p-1)/2}$ を p で割った余りが $p-1$ になることを確認するだけで十分である．

興味のある方は $p = 7, 17$ や問題 1 に登場した $p = 23$ の場合を計算して実際に規則性が成立していることを確認してみると良いだろう．

さらに興味が湧いた人は 10 のべきを素数で割った余りを求めるだけではなく, 任意の数のべきを素数で割った余りを求めてどのような規則性があるかを観察してみるのが良いだろう．そこには平方剰余の相互法則のような驚くべき法則が隠れている．

2.3 問題 3 について (RSA 暗号)

問題 3 を手計算で解くのはほぼ不可能なのでお持ち帰り問題とした．パソコンを使ったとしても, どのような手続きで暗号を破るのか, そのために使えるソフトは何か, などに関する知識が無ければ難しい．お持ち帰りの問題 3 には以下の説明を加えておいた．

問題 3 は本質的に $c = (m^e$ を n で割った余り$)$ から逆に m を求める問題である．ここで n は n は二つの異なる素数 p, q の積であり, e は $(p-1)(q-1)$ と互いに素な数であるとする．このような問題は次の手続きで解くことができる．

1. n を素因数分解して p, q を求める．
2. $p-1$ と $q-1$ の最小公倍数 r を求める．
3. $de \equiv 1 \pmod r$ を満たす r 未満の正の整数 d を求める．
4. $m = (c^d$ を n で割った余り$)$ でもとの m を解読できる．
5. m をコード表にしたがって文に直す．

なお手続きのステップ 2 で $r = (p-1)(q-1)$ としてもよいが, r は $p-1$ と $q-1$ の最小公倍数とした方が効率的である．以上の手続きで問題が解けることを理解するためには RSA 暗号について勉強する必要がある．RSA 暗号に関する詳しい説明については文献 [2] などを参照して欲しい．

実際の計算にはパソコンが必要だろう．そのために使用できるおすすめのソフトは Maxima である．Maxima は誰でも無料で利用できる数式処理ソフトであり, ソースコードもすべて公開されている．Maxima に関する詳しい説明については横田博史氏のウェブサイト [3] が詳しい．

まず Maxima を入手して手もとのパソコンで使えるようにし, Maxima を起動する．最小公倍数を計算するために函数 `lcm()` を使いたいので次のように入力する:

```
load ("functs");
```

公開鍵 n, e と暗号化の結果 c を入力する．

```
n:116232311005172322403;
e:48154933114927891117;
c:16338511021545418035;
```

上で説明した手続きの方法によって暗号化前の m を計算する．

```
f:ifactors(n);
p:f[1][1];
q:f[2][1];
d:inv_mod(e,lcm(p-1,q-1));
m:power_mod(c,d,n);
```

この場合は n が素数 p, q の積に素因数分解されるので容易に解読可能である．コード表を用いて最後の出力結果 $m = 2240766435933521$ を文章になおすと "うなぎをたべたい" になる。逆に m の暗号化は次のようにして行なう．

```
power_mod(m,e,n);
```

この計算結果は当然最初の c に一致している．Maxima の詳細については Maxima の help やマニュアルを参照して欲しい．Maxima を使えばかなり高級な数学も気楽に利用できるようになる．

さて, 問題 3 の元ネタは RSA 暗号である．現代のパソコンでは 20 桁程度の数の素因数分解は瞬時に可能なので問題 3 程度の暗号は誰でも解読できる．しかし最初に与える n を数百桁の 2 つの異なる素数の積とした場合には素因数分解があまりにも大変なので実際上暗号解読は不可能だと考えられている．

RSA 暗号が便利なのは暗号化の方法が公開されていてもよいことである (公開鍵暗号)．たとえば私が n と e を公開して, あなたに「秘密にした文章を数字 m に変換し, e 乗して n で割った余り c を計算して送ってくれ」と頼んだとしよう．n や e のような暗号化のために必要な情報が第三者に漏れ, しかも通信途中で数 c を盗み見られたとしても, あなたは安心して秘密の文章が秘密のまま私に送られたことを信じて大丈夫だと考えてよい．

暗号は我々のデジタル社会でプライバシーを守るために必須の基本技術である．その技術の根幹に n の素因数分解の話や数のべきを n で割った余りの話 (問題 1,2 は 10 のべきを素数で割った余りの話だった) が出て来ることは個人的に結構面白いことだと思う．

3　後日談

数年後．私は数学クイズを実施したのと同じ教室で数学科 3 年生向けの代数学の演習を行なっていた．その演習では午前の講義で習ったことをすぐ使えるような簡単な問題を出すことにしてる．午前の講義ではフェルマーの小定理の証明をやったようだ．

私は以前出した数学クイズの問題をそのまま出すことにした．「99999 のように 9 だけがならんでいる数が 19 で割り切れるためには 9 をいくつならべればよいか?」

すると女子学生のひとりと男子学生のひとりが「数学クイズでその問題を出したときいました」と言った．そして演習時間終了後に思い出ばなしに花が咲く．私は忘れていたが, そのうちの一人は数学クイズのときに「$10, 10^2, 10^3, \ldots$ を素数で割った余りの順序はどのような法則で決まっているのか?」という質問をしてくれたようだ．あと数学クイズのときの雑談で私は「無限に広い平面に描かれた放物線は地平線に接する楕円に見える」というような話もしたらしい．

数学科 3 年生の方々に上の問題 (と他 1 問) を解いてもらって解答を提出してもらったのだが, フェルマーの小定理を使った簡潔な解答を書いた後に実際に 9 を 18 個ならべた数を 19 で割る筆算を計算して余りとして 0 から 17 までの数がすべて出て来るという規則性を確認した方もいた．

数学科の数学は抽象的になり過ぎて難しくなりすぎるということがよくあるので, たまには数学クイズの教訓 (こんなところにも美しい規則性が!) を思い出して, 授業に活かすのも悪くないなと私は思った．も数学科に来て欲しいと思っていたタイプの方が実際に入学して来ているのを知って私はうれしかった．

数は世界を作る！

ところで読者の中に問題 3 を解けた方はどれだけいるだろうか?

参考文献

[1] http://www.math.tohoku.ac.jp/~kuroki/LaTeX/#OpenCampus

[2] 佐藤篤, 素数と暗号 — 初等整数論と RSA 暗号系入門, 2005 年 8 月 26 日, http://www.math.tohoku.ac.jp/~atsushi/Jarticle/crypto.pdf

[3] http://www.bekkoame.ne.jp/~ponpoko/