東北大学オープンキャンパス2008 数学クイズ問題と解答

黒木玄@東北大学大学院理学研究科数学専攻

1 問題

どうしても問題が解けなければ後の節にある大ヒントも参照して下さい.

[**0**] 以下にある問題 [**1**], [**2**], [**3**], [**5**], [**6**] で求めるべき数 A, B, C, D, E, F を並べたもの $ABCDEF$ を次のページのコード表にしたがって言葉に変換すると何になるか? たとえばコード表によって $45 \to$ “は”, $40 \to$ “な” と変換されるので 4540 という数字の並びは “はな” という言葉に変換される. [解答: $ABCDEF = 343222 \to$ “そすう”] □

[**1**] $141A387$ の形の数 (百四十一万 A 千三百八十七, A は 0 から 9 の整数) が 9 で割り切れるような A を求めよ. (ヒント: $1+4+1+A+3+8+7$) [解答: $A = 3$] □

[**2**] $564B628$ の形の数 (五百六十四万 B 千六百二十八, B は 0 から 9 の整数) が 11 で割り切れるような B を求めよ. (ヒント: $5-6+4-B+6-2+8$) [解答: $B = 4$] □

[**3**] $1C39D6$ の形の数 (十 C 万三千九百 D 十六, C, D は 0 から 9 の整数) が 101 で割り切れるような C, D を求めよ. (ヒント: $1C - 39 + D6$) [解答: $C = 3$, $D = 2$] □

[**4**] 2^6 を 7 で割った余りを求めよ. [解答: 1] □

[**5**] 2^{91} を 7 で割った余り E を求めよ. (ヒント: $91 = 15 \cdot 6 + 1$ と上の問題の結果を使う.) [解答: $E = 2$] □

[**6**] 2^{91} を 11 で割った余り F を求めよ. (ヒント: 2^{10} を 11 で割った余りは? $91 = 9 \cdot 10 + 1$) [解答: $F = 2$] □

[**7**] 2^{91} を 77 で割った余りを求めよ. (ヒント: 問題 [**5**], [**6**] の結果を使う.) [解答: 2] □

[**8**] 13 乗して 77 で割った余りが 2 になる 77 未満の正の整数を求めよ. (ヒント: $7 \cdot 13 = 91$ なので $(2^7)^{13} = 2^{91}$ である. 問題 [**7**] の結果を利用せよ.) [解答: $2^7 = 128$ を 77 で割った余りの 51] □

次の問題を解くためにはパソコンが必要になる. だから次の問題はお持ち帰りの問題とする. 自宅に帰った後に時間をかけてゆっくり解く準備をして欲しい.

[**9**] **(お持ち帰り問題)** $n = 116232311005172322403$, $e = 48154933114927891117$ とおく. 10 文字以内の文を次ページ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. たとえば文 “うなぎをたべたい” に対応する数字はコード表にしたがって各文字が

$$\text{う} \to 22,\ \text{な} \to 40,\ \text{ぎ} \to 77,\ \text{を} \to 64,\ \text{た} \to 35,\ \text{べ} \to 93,\ \text{た} \to 35,\ \text{い} \to 21$$

と変換されるので $m = 2240776435933521$ になる. このとき m の暗号化 c は m^e を n で割った余りであり, $c = 52738287526667312929$ となる.

$c = 26827231170163415492$ であるとき, 暗号を破ってもと文の解読せよ. [解答: n の素因数分解 $n = pq$, $p = 6335678101$, $q = 18345678103$, $p-1$ と $q-1$ の最小公倍数 $r = 19372051830081827700$, $\bmod r$ での e の逆数 $d = 19102163426605063453$, c^d を n で割った余り $m = 258245332521643727 60$, m を文に直すと “かずはせかいをつくる”] □

この方式の暗号はRSA暗号と呼ばれており, 実際に使われている. しかし実用的に使われる n は巨大な (100桁以上の) 二つの異なる素数の積に取る. 巨大な二つの素数の積の素因数分解はコンピューターを用いても非常に難しい. そのおかげで n が十分に大きな二つの素数の積であれば, 暗号化の方法を指定するデータ n, e と暗号化の結果 c が公開されていても現実的な時間では解読不可能だと考えられている. しかし上のお持ち帰り問題の n は比較的小さいのでパソコンを使えば容易に素因数分解できる. したがって大ヒントにある手続きで暗号を破ることができる.

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

2 大ヒント

問題 [**1**], [**2**], [**3**] は以下の事実を知っていれば暗算で解くことができる:

(1) $141A387$ が 9 で割り切れるための必要十分条件は $1+4+1+A+3+8+7$ が 9 で割り切れることである.

(2) $564B628$ が 11 で割り切れるための必要十分条件は $5-6+4-B+6-2+8$ が 11 で割り切れることである.

(3) $1C39D6$ が 101 で割り切れるための必要十分条件は $1C-39+D6$ が 101 で割り切れることである.

これらの事実の証明は以下で説明する合同式を使えば容易である. n は正の整数であるとする. このとき「整数 a, b が n を法として合同である」とは $a-b$ が n のある整数倍になることであると定める. そのとき $a \equiv b \pmod{n}$ と書く. $a \equiv 0 \pmod{n}$ と a が n で割り切れることは同値であり, $a \equiv b \pmod{n}$ と a, b のそれぞれを n で割った余りが互いに等しいことは同値である. さらに以下が成立している:

(a) **反射律:** $a \equiv a \pmod{n}$.

(b) **対称律:** $a \equiv b \pmod{n}$ ならば $b \equiv a \pmod{n}$.

(c) **推移律:** $a \equiv b \pmod{n}$ かつ $b \equiv c \pmod{n}$ ならば $a \equiv c \pmod{n}$.

(d) $a \equiv a' \pmod n$ かつ $b \equiv b' \pmod n$ ならば
$a + a' \equiv b + b' \pmod n$ かつ $aa' \equiv bb' \pmod n$.

最後の (d) は $a \equiv a' \pmod n$ かつ $b \equiv b' \pmod n$ ならば $\bmod n$ の合同式の計算において a, b のそれぞれに a', b' を代入することが許されることを意味している. 以上の結果を使えば (1) は次のようにして証明される. $10 \equiv 1 \pmod 9$ なので $\bmod 9$ の合同式の計算で 10 に 1 を代入することが許される. よって

$$\begin{aligned} 141A387 &= 1 \cdot 10^6 + 4 \cdot 10^5 + 1 \cdot 10^4 + A \cdot 10^3 + 3 \cdot 10^2 + 8 \cdot 10 + 7 \\ &\equiv 1 + 4 + 1 + A + 3 + 8 + 7 \pmod 9. \end{aligned}$$

すなわち $141A387$ と $1+4+1+A+3+8+7$ のそれぞれを 9 で割った余りは互いに等しい. したがって $141A387$ が 9 で割り切れることと $1+4+1+A+3+8+7$ が 9 で割り切れることは同値である. 以上の証明の本質をひとことで言うと次のようになる. $\bmod 9$ の目で眺めている人は $10, 100, 1000, \ldots$ がすべて 1 に見える! (2), (3) も $10 \equiv -1 \pmod{11}$, $100 \equiv -1 \pmod{101}$ を使えばまったく同様に証明できる.

問題 [**4**] は直接の計算ですぐに解ける. 実はより一般に次の定理が成立することが知られている (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 $a^{p-1} \equiv 1 \pmod p$.

この定理の証明については自分の数学の先生に聞いて欲しい. 様々な証明がある.

問題 [**5**], [**6**] は次の考え方を使う. $a^k \equiv 1 \pmod n$ かつ $e = kl + 1$ のとき, $\bmod n$ の合同式の計算で a^k に 1 を代入することができ, $a^e = a^{kl+1} = a(a^k)^l$ なので $a^e \equiv a \pmod n$ である.

問題 [**7**] は問題 [**5**], [**6**] の結果を使えばすぐに解ける. $2^{91} - r$ が 7 と 11 で割り切れるならば 77 でも割り切れるので, 2^{91} を 7, 11 で割った余りがともに r であれば 2^{91} を 77 で割った余りも r になる.

問題 [**8**] は次の考え方で解ける. 問題 [**7**] が解けていれば 2^{91} を 77 で割った余り r はすでにわかっている. よって $(2^7)^{13} = 2^{91} \equiv r \pmod{77}$ である. 2^7 を 77 で割った余りを m と書くと $2^7 \equiv m \pmod{77}$ であるから, $m^{13} \equiv (2^7)^{13} \pmod{77}$ である. よって m を 13 乗して 77 で割った余りは r になる.

[**9**] 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. この問題は次の手続きで解くことができる.

1. n を素因数分解する. n は二つの異なる素数 p, q の積に素因数分解されたとする.
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.

問題 [**8**] にもこの手続きを適用できることに注意せよ. 実は [**8**] のヒントはこの手続きがもとになっている. なおステップ 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次の文書を参照して欲しい:

- 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`
- 赤間陽二, 暗号, 計算機数学 A, 2006 年 11 月 27 日, `http://www.math.tohoku.ac.jp/akama/2006/RSA.pdf`

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.

- 公式サイト: `http://maxima.sourceforge.net/`
- 入手方法: 公式サイトから Download をクリックして説明を読む.
- 日本語による説明: Google などで Maxima について検索すればたくさん見つかる.

Maxima は以下のように利用できる. 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:527382875266673129 29;
```

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 $m = 2240776435933521$ 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. Maxima のようなソフトを自由に使いこなせるような高校生は将来自分の数学的才能をどのように活かすかを真剣に考えるべきだと思う.

3 最後に

帰宅後に問題をどうしても解けない場合には, まず自分の数学の先生に相談して下さい. それでも疑問が残った場合には私のメールアドレス `kuroki@math.tohoku.ac.jp` 宛に相談のメールを下さい. 目標に応じてヒントや文献を紹介することができます. 1 週間以上返事がない場合には携帯電話宛の `integrable-system@h.vodafone.ne.jp` に催促の短いメールを下さい.