東北大学オープンキャンパス2006 数学クイズ解答

黒木玄　(東北大学大学院理学研究科数学専攻)

2006年7月28日(木)〜29日(金)

1　問題と解答

a, b は整数であり, n は 0 でない整数であるとする. $a-b$ 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ことにする. 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ことだと考えてもよい.

問題 1 以上の準備のもとで以下の問題に挑戦せよ.

1. $n = 7, 11, 13$ のとき $175342 \equiv -175 + 342 \pmod{n}$ が成立することを両辺を $n = 7, 11, 13$ で割った余りを実際に計算することによって確認せよ.
2. 一般に, 6 桁の数 a の上位 3 桁と下位 3 桁のれぞれを b, c と書く ($a = 1000b + c$). このとき 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証明せよ. □

ヒント. 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 $a - a' = kn$, $b - b' = ln$ のとき, $a + b - (a' + b') = a - a' + b - b' = kn + ln = (k + l)n$ であり, $ab - a'b' = (a' + kn)(b' + ln) - a'b' = a'ln + kb'n + kln^2 = (a'l + kb' + kln)n$ である. したがって $a \equiv b \pmod{n}$ をあたかも通常の等号のごとく扱って構わない. □

解答. 1. 175342, $-175 + 342 = 167$ を 7 で割った余りはともに 6 になり, 11 で割った余りはともに 2 になり, 13 で割った余りはともに 11 になる.

2 の証明. $7 \cdot 11 \cdot 13 = 1001$ であるから $n = 7, 11, 13$ のとき $1000 \equiv -1 \pmod{n}$ である. よって $1000b \equiv -b \pmod{n}$ である. したがって $a = 1000b + c \equiv -b + c \pmod{n}$. □

問題 2 10^{222} を 23 で割った余りを求めよ. □

解答. 直接的計算もしくはフェルマーの小定理より $10^{22} \equiv 1 \pmod{23}$ であることがわかる. (直接的計算で $10^k \equiv 1 \pmod{23}$ となる k を見付けるためには $10, 100, 1000, 10000, \ldots$ を 23 で割った余りが 1 になるまで計算を続けて最後に 0 の個数を数えればよい. 筆算による割り算の計算で余りが 1 にならないとき割られる数の一番右に 0 を追加して計算を続けることは易しいので, 実際にやってみれば見掛けより手間がかからないこともわかる. フェルマーの小定理を知っていれば面倒な計算抜きで $10^{22} \equiv 1 \pmod{23}$ であることがわかる. フェルマーの小定理については解説の節を見よ.)

$10^{22} \equiv 1 \pmod{23}$ を使って

$$10^{222} \equiv (10^{22})^{10} \cdot 10^2 \equiv 1^{10} \cdot 10^2 \equiv 100 \equiv 8 \pmod{23}.$$

したがって 10^{222} を 23 で割った余りは 8 である. □

問題 3 $9, 99, 999, 9999$ のように 9 だけが並んでいる数を素因数分解してみよう:

$$9 = 3^2, \quad 99 = 3^2 \cdot 11, \quad 999 = 3^3 \cdot 37, \quad 9999 = 3^2 \cdot 11 \cdot 101,$$
$$99999 = 3^2 \cdot 41 \cdot 271, \quad 999999 = 3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37, \quad \ldots\ldots$$

これで 9 だけが並んだ数の素因数として少なくとも $3, 7, 11, 13, 37, 41, 101, 271$ が現われることがわかった. (9 だけが並んだ数は $2, 5$ で割り切れないので $2, 5$ が現われないのは当然である.) 13 の次の素数 17 やその次の素数 19 で割り切れる 9 だけが並んでいる数は存在するだろうか? さらにそれ以降の素数についてはどうなっているのだろうか?

1. 17 で割り切れる 9 だけが並んでいる数をひとつ見付けよ.
2. 19 で割り切れる 9 だけが並んでいる数をひとつ見付けよ.
3. 2 と 5 以外の任意の素数 p に対して, p で割り切れる 9 だけが並んでいる数が存在することを証明せよ. □

解答. 1, 2 の解答. $9, 99, 999, 9999, \ldots$ を 17 (もしくは 19) で割った余りを次々に計算し, 余りが 0 で無ければ一番右側に 9 を追加して桁数を一つ増やし (割り算の筆算の途中で一番右側に 9 を追加することは易しい), 割り切れるまで計算を続行すれば良い. その結果, 9999999999999999 = (9 が 16 個並んだ数) は 17 で割り切れ, 99999999999999999 = (9 が 18 個並んだ数) は 19 で割り切れることがわかる.

3 の証明. p で割った余りの可能性は $0, 1, \ldots, p-1$ の p 通りしかないので, $p+1$ 個の数 $1, 10, 10^2, \ldots, 10^p$ を p で割った余りを考えると, それらのうちどれか 2 つの余りは一致している (鳩の巣論法). それらを 10^i, 10^j, $i < j$ と書くことにする. 10^i と 10^j を p で割った余りは一致しているので $10^j - 10^i = 10^i(10^{j-i} - 1)$ は p で割り切れる. p は 2 と 5 以外の素数なので $10^{j-i} - 1 =$ (9 が $j - i$ 個並んだ数) が p で割り切れなければいけない.

実は完全に同じ方法によってより一般的に次が成立していることを示せる.

4. 2 つの自然数 a と n の最大公約数が 1 ならばある正の整数 k で $a^k - 1$ が n で割り切れるものが存在する (オイラーの定理の弱形).

証明. n で割った余りの可能性は $0, 1, \ldots, n-1$ の n 通りしかないので, $n+1$ 個の数 $1, a, a^2, \ldots, a^n$ を n で割った余りを考えると, それらのうちどれか 2 つの余りは一致している. それらを a^i, a^j, $i < j$ と書くことにする. a^i と a^j を n で割った余りは一致しているので $a^j - a^i = a^i(a^{j-i} - 1)$ は n で割り切れる. a と n の最大公約数は 1 であると仮定したので $a^{j-i} - 1$ が n で割り切れなければいけない.

より強い形の本来のオイラーの定理については解説の節を見よ. 上の弱形では k として具体的にどのような数が取れるかわからないが, もともとのオイラーの定理ではその点が明らかになっている.

1, 2, 3 の別解. フェルマーの小定理より p が 2 と 5 以外の素数ならば $10^{p-1} - 1 =$ (9 が $p-1$ 個並んだ数) は p で割り切れることがわかる. 特に (9 が 16 個並んだ数) は 17 で割り切れ, (9 が 18 個並んだ数) は 19 で割り切れる. フェルマーの小定理については解説の節を見よ. □

2 解説

2.1 問題 1 について

問題 1 の解答と同様にして,

$$1000^k a_k + \cdots + 1000a_1 + a_0 \equiv (-1)^k a_k + \cdots - a_1 + a_0 \pmod{n}, \quad n = 7, 11, 13$$

が成立することがわかる. 特に自然数 a が $n = 7, 11, 13$ で割り切れるための必要十分条件は a を下位から 3 桁ごとに区切ってそれらを交互に ± 1 倍して足し上げた結果が $n = 7, 11, 13$ で割り切れることである. 3 桁以上の数の足し算と引き算を高速にできる人は $n = 7, 11, 13$ で割った余りを容易に計算できることになる.

$n = 3, 9$ のとき $10 \equiv 1 \pmod{n}$ なので問題 1 の解答と同様にして

$$10^k a_k + \cdots + 10a_1 + a_0 \equiv a_k + \cdots + a_1 + a_0 \pmod{n}, \quad n = 3, 9$$

が成立することもわかる. 特に自然数 a が $n = 3, 9$ で割り切れるための必要十分条件は a のすべての桁を足し上げた結果が $n = 3, 9$ で割り切れることである. $n = 3, 9$ で割り切れるかどうかに関するこの判定法は有名である. しかしその判定法が常に成立することの理由 (証明) について知っている人はどれだけいるだろうか? 合同式 $a \equiv b \pmod{n}$ を導入すればその証明は非常に簡単になる.

$n = 3, 9$ で割り切れるかどうかの楽な判定法や $n = 7, 11, 13$ で割り切れるかどうかの上の判定法を知っていれば計算が楽になる. そして計算を楽にする方法の裏には合同式 $a \equiv b \pmod{n}$ に関する一般論という数学的一般法則が隠されている. 大学の数学科ではそのような**裏に隠された数学的一般法則**について学ぶことになる.

数学の歴史は数千年以上あるのだが, そのあいだに多くの数学的一般法則が明らかにされ, 努力さえすれば誰にでも利用できるように整備されている. (しかも無料で好きなだけ使える!)

我々のデジタル文明社会においては生活のあらゆる場面で数学的一般法則が利用されている. たとえば CD を聴いている人は CD のデジタル符号化や誤り訂正の基礎になる数学的一般法則を利用しており, 携帯電話を使っている人も同様である. そのようなデジタル機器で利用されている数学的一般法則の多くは問題 1 で使われた合同式の話を発展させたものになっている. たとえば次の節で説明するフェルマーの小定理は最も基礎的な一般法則としてよく使われている.

2.2 問題 2 について

10^{222} を 23 で割った余りを直接計算しようとした方がいたとすれば**御苦労様!**

数学において重要なのは「楽をするための方法」である. しかも特定の場合ごとに楽をするための方法を見付けることよりも広い範囲に適用できる**裏に隠された数学的一般法則**を見付けることが重要である. 数学の研究とはまだ発見や証明がされていないそのような法則を発見したり証明したりすることである.

問題 2 の解答で使われているそのような一般法則は問題 1 のヒントに書かれている合同式の計算に関する一般法則と次のフェルマーの小定理であると考えて良い. もちろんフェルマーの小定理を知らなくても直接的計算で $10^{22} \equiv 1 \pmod{23}$ を確認できるがかなり面倒である. 次のフェルマーの小定理を知っていれば計算抜きで $10^{22} \equiv 1 \pmod{23}$ であることがわかる.

フェルマーの小定理. p が素数であり, a が p で割り切れない整数であれば $a^{p-1} \equiv 1 \pmod{p}$ が成立している. □

たとえば $2^6 \equiv 1 \pmod{7}$, $4^4 \equiv 1 \pmod{5}$ が成立していることは容易に確かめられる. 他の場合についても色々計算してみよ.

フェルマーの小定理の証明を知りたければ, 大学生向けの数学の教科書を参照したり, インターネットで「フェルマーの小定理 証明」を検索してみたり, 自分が数学を習っている先生に参考書を紹介してもらうのが良いだろう. もちろん大学の数学科に入学するまで待つという手もあるが, 興味を持ったことは自分の力を使ってすぐに調べてみた方が良い.

あなたが利用できる書籍, 資料, 人脈, コンピューターのすべてがあなたの力である. 数学の研究も自分自身が利用できるすべての力を用いて行なわれている.

注意. フェルマーの小定理と次のフェルマーの最終定理を混同しないようにして欲しい.

フェルマーの最終定理. n が 3 以上の整数のとき $X^n+Y^n = Z^n$ を満たす正の整数 X, Y, Z は存在しない. □

フェルマー (1601–65) はこの定理を実際に証明できたと思っていたようだが実際には証明できていなかったので, この定理は「フェルマー予想」と呼ばれることが多い. 「フェルマー予想」はアンドリュー・ワイルスによって証明された. ワイルスは谷山豊によって予想された有理数体上の楕円曲線のモジュラー性を証明することフェルマー予想を証明した. フェルマー予想は楕円曲線のモジュラー性という谷山が予想した数学的一般法則から導かれるのである.

2.3 問題 3 について

問題 3 も本質的にフェルマーの小定理の応用問題だと考えて構わない. 計算を楽にするためにはフェルマーの小定理を積極的に使うべきである.

問題 3 の解答ではオイラーの定理の弱形を紹介・証明しているが, 強い形の本来のオイラーの定理は次のように述べられる.

オイラーの定理. n は正の整数であるとする. n の素因数分解を $n = p_1^{e_1} \cdots p_r^{e_r}$ (p_i は互いに異なる素数, e_i は正の整数) と書き, オイラー函数 $\varphi(n)$ を

$$\varphi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdots (p_r^{e_r} - p_1^{e_r-1}) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

と定める. このとき整数 a と n の最大公約数が 1 ならば $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

たとえば $n = 11^2$ のとき $\varphi(n) = 11^2 - 11 = 110$ であるから, オイラーの定理より $10^{110} - 1$ は 11^2 で割り切れる. (実際には $10^{22} \equiv 1 \pmod{11^2}$ が成立している.)

$n = p =$ (素数) のとき $\varphi(n) = \varphi(p) = p - 1$ であるからオイラーの定理はフェルマーの小定理の一般化になっていることもわかる.

n が 2 でも 5 でも割り切れない正の整数であるとき, オイラーの定理を $a = 10$ に適用すれば $10^{\varphi(n)} - 1 =$ (9 が $\varphi(n)$ 個並んだ数) が n で割り切れることがわかる.

群論を使えばオイラーの定理の証明はかなり易しくなる. 実際の証明を知りたい人はフェルマーの小定理の証明と同様に自分の力で色々調べてみて欲しい.