高校生のための現代数学講座
「素数の世界」
講義 (3)　寺杣　友秀

東京大学
玉原国際セミナーハウス
2009 年 7 月 25 日

「合同式の計算」

1　剰余による合同式と加法と乗法

- m を 2 以上の整数とする。ふたつの整数 a_1 と a_2 が m を法とし合同である、というのを $a_1 - a_2$ が m で割り切れることであると定義する。このとき

$$a_1 \equiv a_2 \pmod{m}$$

と書く。

- 整数の集合 $\mathbf{Z}$,m の倍数の集合を $m\mathbf{Z}$ と書く。上の定義は

$$a_1 \equiv a_2 \pmod{m} \Longleftrightarrow a_1 - a_2 \in m\mathbf{Z}$$

と書くと簡潔に書ける。

- m を法として合同であるときに" 仲間であるとして分類する。" これは数学用語で同値類別と呼ばれる。その一つ一つのグループを同値類という。r を整数とするとき m を法として r と合同であるもの $[r]$ は一つの同値類である。今の場合、この同値類を m を法とする剰余類という。

- 整数 r に対して $r \equiv r_0 \pmod{m}$ であり $0 \leq r_0 \leq m-1$ なる整数 r_0 がただ一つ定まる。従って m を法とする剰余類の個数は m 個である。剰余類全体の記号を $\mathbf{Z}/m\mathbf{Z}$ と書く。従って

$$\mathbf{Z}/m\mathbf{Z} = \{[0], [1], \ldots, [m-1]\}$$

となる。

- a_1 と a_2 が m を法として合同、b_1 と b_2 が m を法として合同なら $a_1 + b_1$ と $a_2 + b_2$ が m を法として合同となる。これから剰余類 $[a_1]$ と $[a_2]$ の和 $[a_1] + [a_2]$ が $a_1 + a_2$ が含まれる類として定義できる。$[a_1] + [a_2] = [a_3]$ は $a_1 + a_2 \equiv a_3 \pmod{m}$ と同じ意味である。

- 差、及び掛け算についても上と同様のことが成り立つ。

- 合同関係式は和、差、掛け算は剰余類の和、差、掛け算と解釈できるので、どのタイミングで合同な数で置き換えても答えはかわらない。

$$\begin{aligned}
10! &\equiv 1 \cdot 2 \cdot \cdots \cdot 10 \pmod{11} \\
&\equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdot 3 \cdot (-3) \cdot 4 \cdot (-4) \cdot 5 \cdot (-5) \pmod{11} \\
&\equiv (-1) \cdot 1 \cdot 4 \cdot 9 \cdot 16 \cdot 25 \pmod{11} \\
&\equiv (-1) \cdot 1 \cdot 4 \cdot (-2) \cdot 5 \cdot 3 \pmod{11} \\
&\equiv (-3) \cdot 4 \pmod{11} \\
&\equiv -1 \pmod{11}
\end{aligned}$$

2　合同式の除法

- $[a]$,$[b]$ を m を法とする剰余類として $[a]$ の $[b]$ による割り算はいつできるのか？つまり

$$a \equiv cb \pmod{m}$$

なる c は存在するか？またそのような c はただ一つか？

- $[b]$ による割り算がいつでもできるためには $[b]$ の逆元 $[x]$ が存在しなくてはならない。（逆数ではなく、ここではあえて逆元といった。）つまり

$$1 \equiv bx \pmod{m}$$

逆に逆元が存在すればいつでも $[b]$ による割り算ができる。これは $my + bx = 1$ なる x, y が存在することと同等である。つまり b と m が互いに素であることが同等である。$[0]$ には逆元がない。

- m を法とする b の逆数を求めるにはユークリッドの互除法を用いればよい。

- 鶴と亀がいる。足の数を合わせたものを 9 で割ると 3 余り、頭の数を合わせてものを 9 で割ると 4 あまる。鶴の数は 9 で割ると何匹余るか？

- m を法とした剰余類 $\mathbf{Z}/m\mathbf{Z}$ において $[0]$ でない類が必ず逆元を持つ条件はなんだろうか？

3　合同式の指数、アルゴリズム

- 次に指数は定義できるか？m を 2 以上の整数として $[a]^p$ は自然数 p に対して

$$[a]^p = \underbrace{[a] \cdot [a] \cdots [a]}_{p \text{ 個}}$$

として定義される。さらに、$[a]$ に逆元があるときに $[a]^{-p} = ([a]^{-1})^p$ とおく。

- 自然数で考えると指数がちょっと大きくなると、答えはすぐに大きくなる。

$$3^{113} = 8216782349860225013320438177913146043582421707992003 23$$

それでも計算機はかなり早く計算してくれる。

- x^p の指数計算の速いアルゴリズム $(x \neq 0)$

(1) p を 2 進展開する。

$$(a_1 a_2 \cdots a_n)_2 = (\cdots((a_1 \times 2 + a_2) \times 2 + a_3) \cdots \times 2 + a_n$$

ただし $a_1 = 1$, $a_i = 0$ または 1. たとえば 113 を 2 進展開をすると次のようになる。だから

$$\begin{aligned} 113 &= (1110001)_2 = 2^6 + 2^5 + 2^4 + 1 \\ &= (((1 \times 2 + 1) \times 2 + 1) \times 2 \times 2 \times 2 \times 2 + 1 \end{aligned}$$

(2) 次の様にして数列 b_n を定める。

$$b_1 = x^{a_1}(= x), \quad b_2 = b_1^2 \times x^{a_2}, \ldots, b_n = b_{n-1}^2 \times x^{a_n}$$

たとえば上の例の場合

$$\begin{aligned}
&b_1 = 3, b_2 = b_1^2 \times 3 = 27, b_3 = b_2^2 \times 3 = 2187,\\
&b_4 = b_3^2 = 4782969,\\
&b_5 = b_4^2 = 22876792454961,\\
&b_6 = b_5^2 = 523347633027360537213511521,\\
&b_7 = b_6^2 \times 3 = 821678234986022501332043817791314604358242170799200323
\end{aligned}$$

(3) b_n が求めるものである。

- なぜこのようなアルゴリズムで求められるのだろうか？
- 合同剰余の場合も全く同じ方法でもとめられる。m を法とする計算では必ず答えは各段階で $m-1$ より小さくなるので、桁数もそれ以上にはならない。
- 指数に関しては指数法則が成り立つ。

$$[a]^p \times [a]^q = [a]^{p+q}$$

$$([a]^p)^q = [a]^{pq}$$

$[a]$ に逆元があれば上の法則は $p, q \in \mathbf{Z}$ で成立する。

4 合同式の指数の法則

- $x_0 = 1, x_n = x_{n-1} \cdot [a]$ という $\mathbf{Z}/m\mathbf{Z}$ での列（数列）を考えると、剰余類は有限個しかないので、いつかはそれまでに出てきた類に一致する。従って

$$[a]^p = [a]^{p+q}$$

なる $0 < p$, $0 < q$ が存在する。$p+q$ が最小になるような q を考えると、$[a]^p$ は p に関して q を周期にもつ列となる。

- さらに $[a]$ に逆元があるときには上の式に $[a]^{-p}$ を掛けて $[a]^q = 1$ となることになる。
- 周期にはどのような規則性があるだろうか？話を単純化するために a には逆元があるときに試してみよう。

(1) m を固定して逆元をもつような $[a]$ を動かしたとき、周期はどのようにかわるだろうか？

(2) 次に m を動かして考える。m が素数のとき (1) で予想される量ははどうなっているだろうか？

(3) m が合成数のときはどうだろうか？

(4) m が二つの互いに素な整数 m_1, m_2 の積 $m_1 m_2$ となっているとき、(1) で予想される量はどうなっているだろうか？

- (2) で予想されるような m が素数のときの結果はフェルマーの小定理と呼ばれる。
- m が素数であることが解っている場合、$[a]$ の逆元をすばやく求める方法はないだろうか？
- m が素数であることが解っている場合、$[a]^b$ と b が解っている場合、$[a]$ をすばやく求める方法はないだろうか？b としてはどのようなどのような条件を課したらよいだろうか？