Carmichael 数の Universal form について

津村 博文 (東京都立短期大学・経営情報学科)
駒井 洋章 (東京都立大学大学院・理学研究科)
中村　憲　(東京都立大学大学院・理学研究科)

定義　奇数の合成数 N が Carmichael 数

$\Leftrightarrow \quad a^{N-1} \equiv 1 \pmod{N}$ $(\forall a \in \mathbb{Z};\ (a, N) = 1)$

Korselt's criterion (1899)

奇数の合成数 N が Charmichael 数
$\Leftrightarrow$ N が squarefree &
$p - 1 \mid N - 1$ $(\forall p$: 素数; $p \mid N)$

例 $561 = 3 \cdot 11 \cdot 17$ ⋯ 最小の Carmichael 数
$1729 = 7 \cdot 13 \cdot 19$, $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$

定義 [Chernick: Bull. AMS (1939)]
$U_k(M) = \prod_{i=1}^{k} (a_i M + b_i) \quad (a_i, b_i \in \mathbb{N};\ k \geq 3)$
が Carmichael 数の Universal form

$$\Longleftrightarrow U_k(M) \equiv 1 \pmod{a_i M + b_i - 1}$$
$$(\forall M \in \mathbb{Z};\ 1 \leq i \leq k)$$

例 $\mathfrak{U}_3(M) = (6M+1)(12M+1)(18M+1)$
⋯ Universal form

$\mathfrak{U}_3(1) = 7 \cdot 13 \cdot 19 = 1729$ ⋯ Carmichael 数
$\mathfrak{U}_3(2) = 13 \cdot 25 \cdot 37$ ⋯ Carmichael 数でない
$\mathfrak{U}_3(3) = 19 \cdot 37 \cdot 55$ ⋯ Carmichael 数でない
⋮
$\mathfrak{U}_3(6) = 37 \cdot 73 \cdot 109 = 294409$
⋯ Carmichael 数

問題 $\{\mathfrak{U}_3(M);\ M \in \mathbb{N}\}$ は無限個の Carmichael 数を含むか？ ⋯ 未解決

定理**A** [Chernick: Bull. AMS (1939)]

Carmichael 数があれば，それから Univ. form が作れる．

例 $7\cdot 13\cdot 31$, $11\cdot 31\cdot 41\cdot 61$ から

$$(10M-3)(20M-7)(50M-19)$$
$$(12M-1)(36M-5)(48M-7)(72M-11)$$

などが得られる．

定理**B** [Chernick: Bull. AMS (1939)]

$k\in\mathbb{N}$ $(k\geq 3)$ に対し，k 項からなる Univ. form U_k があれば，$k+1$ 項からなる Univ. form U_{k+1} が作れる．

例 上記の $\mathfrak{U}_3$ から帰納的に $\mathfrak{U}_4$, $\mathfrak{U}_5,\cdots$ が定義できる．実際一般の $k\geq 4$ に対し

$$\mathfrak{U}_k(m)=(6m+1)(12m+1)\prod_{i=1}^{k-2}\left(9\cdot 2^i m+1\right)$$

が定義できて，$2^{k-4}\,|\,m$ $(k\geq 4)$ のとき，$m=2^{k-4}M$ とおけば，$\mathfrak{U}_k(2^{k-4}M)$ が Univ. form となる．

注 一般の個数の素因子をもつ Carmichael 数が存在するかは未解決なので, 直接に一般の項数からなる Univ. form を作ることは Chernick の方法では無理. (下から帰納的に作っていくことは可能)

Carmichael 数の発見の歴史的な流れ

k 個の素因子からなる Carmichael 数を k-項数と呼ぶとすると

・1939 Chernick ... 上記の方法で 7 項数の発見
・1978 頼永正孝 ... 13 ~ 18 項数の Table の作成
・1992 Zhang ... 1305 項数の発見
・1993 Pinch ... 大きさ $< 10^{15}$ の Table の作成
・1994 Alford-Granville-Pomerance
... Carmichael 数が無限個存在することの証明
・1996 Lőh-Niebuhr
... 1101518 項数の発見

その他 Erdős による X 以下の Carmichael 数の個数の下限予想 (1956) 等もある.

k 項の Univ. form を一般に

$$P_k(M) = \prod_{i=1}^{k} (a_i M + b_i)$$

と書くとき,

Hardy-Littlewood 予想 (1923)

$$\#\{M \leq X \mid P_k(M) : Carmichael\ Num.\}$$

$$\sim\ C(P_k)\ \frac{X}{(\log X)^k} \quad (X \to \infty)$$

ただし $C(P_k)$ は $\{a_i, b_i\}_{i=1}^{k}$ から計算可能な定数.

Dubner はこの方法を精密化して, $M < X$ の時, $(6M+1)(12M+1)(18M+1)$ の形であらわされる Carmichael 数の個数の予想値を計算し, $M \leq 10^9$ の範囲で実際の個数との比較をした (2002).
... かなり精密な予想になっている.

目標 一般の項数からなる Univ. form を直接的に構成し, Chernick の結果を一般化する. さらに構成したいくつかの Univ. form について, Dubner の方法を用いて精密な個数の予想値を計算する.

主結果 $\mathbf{a}_r = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$ $(r \geq 3)$ が

(1) $a_1 < a_2 < \cdots < a_r$
(2) $a_1 + a_2 + \cdots + a_{r-1} = a_r$
(3) $a_j \mid 2a_r \quad (1 \leq j \leq r)$
(4) $\mathrm{GCD}(a_1, a_2, \cdots, a_r) = 1$

を満たすとき, $k \geq r$ に対し

$$U_k(m; \mathbf{a}_r) := \prod_{j=1}^{r} \left(a_j a_r m + 1\right) \prod_{i=1}^{k-r} \left(2^{i+1} a_r^2 m + 1\right)$$

とおく. このとき $2^{k-r-1} \mid m$ (ただし $k > r$ のとき) となる m に対し, $m = 2^{k-r-1} M$ (ただし $k = r$ の時は $m = M$) とおくと, $U_k(m; \mathbf{a}_r)$ は Universal form となる. すなわち (1) ~ (4) を満たす r 個の自然数の組 (これが各 r ごとに存在することは明らか ... 後で具体例をあげる) があれば, 直接 r 項の Univ. form U_r を作ることができる.

例 $\mathbf{a}_3 = (a_1, a_2, a_3) = (1, 2, 3)$ は (1) ~ (4) を満たし，$U_3(M, \mathbf{a}_3) = \mathfrak{U}_3(M)$ ($\leftarrow$ Chernick's form)．$k > 3$ に対しても，$U_k(m, \mathbf{a}_3) = \mathfrak{U}_k(m)$.

この一般化として，$r \geq 3$ に対し

$$
\begin{aligned}
&a_1 = 1,\ a_2 = 2^{r-2},\\
&a_j = 2^{j-3}\left(2^{r-2}+1\right)\ (3 \leq j \leq r)
\end{aligned}
$$

とおくと，$\mathbf{a}_r = (a_1, \ldots, a_r)$ は (1) ~ (4) を満たす．このとき $k \geq r$ に対し

$$
\begin{aligned}
\mathfrak{U}_{k,r}(m) &= U_k\left(m; \mathbf{a}_r\right)\\
&:= \left(2^{r-2}\left(2^{r-2}m+1\right)+1\right)\\
&\quad \times \left(2^{2r-4}\left(2^{r-2}m+1\right)+1\right)\\
&\quad \times \prod_{i=1}^{k-2}\left(2^{r+i-3}\left(2^{r-2}+1\right)^2 m+1\right)
\end{aligned}
$$

とおくと，$\mathfrak{U}_{k,r}$ は Univ. form を構成する．とくに $\mathfrak{U}_{k,3}(M) = \mathfrak{U}_k(M)$．すなわち $\mathfrak{U}_{k,r}$ は Chernick の $\mathfrak{U}_k$ の一般化と見られる.

定義から

$$\begin{aligned}\mathfrak{U}_{4,4}(M) =&(20M+1)(80M+1)\\ &\times(100M+1)(200M+1)\\ \mathfrak{U}_{5,5}(M) =&(72M+1)(576M+1)(648M+1)\\ &\times(1296M+1)(2592M+1)\end{aligned}$$

一般の $r \geq 3$ に対し，$\mathfrak{U}_{r,r}(M)$ は r 項の Univ. form となる.

主結果と同様の方法で次を得る.

系 $k \geq 3$ に対し

$$\mathcal{W}_k(m) = (6m+1)\prod_{i=1}^{k-2}(4\cdot 3^i m+1) \times(2\cdot 3^{k-1}m+1)$$

とおくと, $3^{k-3} \mid m$ のとき $m = 3^{k-3}M$ とおけば $\mathcal{W}_k\left(3^{k-3}M\right)$ が Univ. form となる.

例 $\mathcal{W}_3(M) = (6M+1)(12M+1)(18M+1)$

$$\mathcal{W}_4(3M) =(18M+1)(36M+1) \times (108M+1)(162M+1)$$

そこで $\mathfrak{U}_{4,4}(M)$, $\mathfrak{U}_{5,5}(M)$, $\mathcal{W}_4(3M)$ について Dubner の方法を用いて、$M < X$ の範囲でこれらの Form から得られる Carmichael 数の個数の予想値を計算して、実際の個数との比較をする.

$$\mathfrak{U}_{4,4}(M) = (20M+1)(80M+1) \times (100M+1)(200M+1)$$

について，$M < X$ の範囲での $\mathfrak{U}_{4,4}(M)$ から得られる Carmichael 数の個数 (の確率的予想値) を $E(X)$ とする．　自然数 N が素数である確率が約 $1/\log(N)$ であることから，$20M+1$，$80M+1$，$100M+1$，$200M+1$ が全て素数になる確率を，(条件付確率を計算することで) 求めると，

$$E(X) \sim \frac{A}{6a_X X}\left\{ \mathrm{Li}(a_X X) - \mathrm{Li}(a_X) - \frac{a_X X}{\log(a_X X)} - \frac{a_X X}{\log^2(a_X X)} - \frac{2a_X X}{\log^3(a_X X)} \right\}$$

ただし $\mathrm{Li}(x) = \int_2^x 1/\log(t)dt$ で，a_X は

$$\log^4(a_X X) = \log(20X+1)\log(80X+1) \times \log(100X+1)\log(200X+1)$$

によって決まる定数．また A は次のように計算できる定数で約41.51196.

詳しくは $A = (2.5)^4\, C_1\, C_2\, C_3$, ただし

$$C_1 = \frac{3}{2} \prod_{p>5} \frac{p(p-2)}{(p-1)(p-1)}$$
$$= 1.4083461\cdots$$

$$C_2 = \frac{3}{4} \prod_{p>5} \frac{p(p-3)}{(p-1)(p-2)}$$
$$= 0.64944352\cdots$$

$$C_3 = \frac{3}{2} \prod_{p>5} \frac{p(p-4)}{(p-1)(p-3)}$$
$$= 1.16188313\cdots$$

これらは条件付確率の計算の過程で現われる.

この漸近公式による予想値 $E(X)$ と実際に存在する個数 $N(X)$ について, $X \leq 10^9$ の範囲で表にすると次のようになる.

$\mathfrak{U}_{4,4}(M)$ について

X	$E(X)$	$N(X)$	$E(X)/N(X)$
10^3	2	2	1.00000
10^4	17	16	1.06250
10^5	90	87	1.03448
10^6	506	487	1.03901
10^7	3021	2959	1.02095
10^8	19143	18960	1.00965
10^9	127204	126997	1.00163

$\mathfrak{U}_{5,5}(M) = (72M+1)(576M+1)(648M+1)$
$\times(1296M+1)(2592M+1)$ について

X	$E(X)$	$N(X)$	$E(X)/N(X)$
10^3	1	2	0.50000
10^4	4	5	0.80000
10^5	19	22	0.86364
10^6	105	107	0.98131
10^7	596	616	0.96753
10^8	3555	3516	1.01109
10^9	22261	22163	1.00442

$\mathcal{W}_4(3M) = (18M+1)(36M+1)$
$\times(108M+1)(162M+1)$ について

X	$E(X)$	$N(X)$	$E(X)/N(X)$
10^3	7	10	0.70000
10^4	30	33	0.90909
10^5	155	149	1.04027
10^6	862	824	1.04612
10^7	5108	5116	0.99843
10^8	32170	32077	1.00290
10^9	212716	213075	0.99832

参考文献

[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.* **140** (1994), 703-722.

[2] J. Chernick, On Fermat's simple theorem, *Bull. Amer. Math. Soc.* **45** (1939), 269-274.

[3] H. Dubner, Carmichael numbers of the form $(6m+1)(12m+1)(18m+1)$, *J. Integer Seq.* **5** (2002), Article 02.2.1, 1-8.

[4] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2002), 883-908.

[5] G. H. Hardy and J. E. Littlewood, Some problems on partitio numerorum III, On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1-70.

[6] G. Lőh and W. Niebuhr, A new algorithm for constructing large Carmichael numbers, *Math. Comp.* **65** (1996), 823-836.

[7] R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** (1993), 381-391.