New polynomials producing absolute pseudoprimes with many factors

NAKAMULA, Ken (Tokyo Metropolitan University)
with Tsumura, H. and Komai, H.

10 June, 2005 (Fri.) at TU-Berlin

Def. An odd composite N is an absolute pseudoprime or a Carmichael number

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

Basic Criterion. [Korselt: L'intermédiaire Math. (1899)]

An odd composite N is an absolute pseudoprime

$\Leftrightarrow$ N is square-free and
$p - 1 \mid N - 1 \qquad (\forall p$: prime; $p \mid N)$

Cor. An odd composite N is an absolute pseudoprime

$$\Leftrightarrow \quad a^{N} \equiv a \pmod{N} \qquad (\forall a \in \mathbb{Z})$$

e.g. $561 = 3 \cdot 11 \cdot 17$ ... the least absolute pseudoprime

$1729 = 7 \cdot 13 \cdot 19, \quad 16046641 = 13 \cdot 37 \cdot 73 \cdot 457$

Def. [Chernick: Bull. AMS (1939)]

$$U_k(M) = \prod_{i=1}^{k} (a_i M + b_i) \quad (a_i \in \mathbb{N}, b_i \in \mathbb{Z}; k \geq 3)$$

is a universal form of absolute pseudoprimes

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

e.g. $\mathfrak{U}_3(M) = (6M+1)(12M+1)(18M+1)$

... universal form

$\mathfrak{U}_3(1) = 7 \cdot 13 \cdot 19 = 1729$ ... absolute pseudoprime

$\mathfrak{U}_3(2) = 13 \cdot 25 \cdot 37$ ... NOT absolute pseudoprime

$\mathfrak{U}_3(3) = 19 \cdot 37 \cdot 55$ ... NOT absolute pseudoprime

...

$\mathfrak{U}_3(6) = 37 \cdot 73 \cdot 109 = 294409$

... absolute pseudoprime

Prob. Does $\{\mathfrak{U}_3(M);\ M \in \mathbb{N}\}$ contain infinitely many absolute pseudoprimes? ... Still open unless we assume the prime linear triplet conjecture.

Main Result Let $\mathbf{a}_r = (a_1, a_2, \ldots, a_r) \in \mathbb{N}^r$ $(r \geq 3)$ be satisfying the following conditions:

(1) $a_1 < a_2 < \cdots < a_r$,

(2) $a_1 + a_2 + \cdots + a_{r-1} = a_r$,

(3) $a_j \,|\, 2a_r \quad (1 \leq j \leq r)$,

(4) $\mathrm{GCD}(a_1, a_2, \cdots, a_r) = 1$.

For each $k \geq r$, put

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

Further set $m = M$ or $m = 2^{k-r-1} M$ respectively when $k = r$ or $k > r$. Then $U_k(m; \mathbf{a}_r)$ is a universal form with respect to M.

Namely, we can **directly** construct a universal form U_r with an **arbitraly fixed** r linear factors if there is an r-tuple of natural numbers satisfying the simple conditions (1) to (4).

As will be seen in examples below, it is obvious that such an r-tuple exists for each r.

We also give a precise conjecture, together with numerical computation by Dubner's method (2002), on the number of absolute pseudoprimes generated by some of our universal forms.

Rem. Condition (4) is unnecessary, but without it only a subset of that satisfying condition (4) is produced.

Thm. A [Chernick: Bull. AMS (1939)]
If there is an absolute pseudoprime with k prime factors, then we can construct a universal form with k linear factors from it.

e.g. From $7 \cdot 13 \cdot 31$, $11 \cdot 31 \cdot 41 \cdot 61$, universal forms

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

are constructed.

Thm. B [Chernick: Bull. AMS (1939)]
For $k \in \mathbb{N}$ ($k \geq 3$), if there is an universal form U_k with k linear factors, then we can construct a universal form U_{k+1} with $k+1$ linear factors.

e.g. From $\mathfrak{U}_3$ above, we can inductively define $\mathfrak{U}_4$, $\mathfrak{U}_5, \cdots$. Indeed, for a general $k \geq 4$, we define

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

and, if we put $m = 2^{k-4}M$ for $k \geq 4$, then $\mathfrak{U}_k(2^{k-4}M)$ is a universal form.

Rem. It is almost certain that there exist an absolute pseudoprime with any number k of prime factors by the Hardy-Littlewood Conj. below. But, it is still unsolved and no definite algorithm to find it for each fixed k. So, it is impossible to construct a universal form with an arbitraly number of linear factors directly by Chernick's method.

Rem. There are two main methods to obtain an absolute pseudoprime with many factors as is summarized by Granville and Pomerance (2002). One is Chernick's method above. The other is by Erdős (1956). Starting from a highly composite natural number L, we consider the set of primes p with $p - 1 \mid L$. If the produt N of some of those p's are congruent to $1 \bmod L$, then N is an absolute pseudoprime.

History

Let k-APSP imply "absolute pseudoprime with k prime factors":

· 1939 Chernick $\cdots$ Find 7-APSP by the method above
· 1978 Yorinaga, M. $\cdots$ Table of 13- to 18-APSP
· 1992 Zhang $\cdots$ Find 1305-APSP
· 1993 Pinch $\cdots$ Table of absolute pseudoprimes $< 10^{15}$
· 1994 Alford-Granville-Pomerance
  $\cdots$ Existance of infinitely many absolute pseudoprimes
· 1996 Lőh-Niebuhr $\cdots$ Find 1101518-APSP

A conjecture by Erdős giving a lower bound of the number of absolute pseudoprimes not exceeding X (1956), and a precise study by Granville and Pomerance (2002).

Let $P_k(M) = \prod_{i=1}^{k}(a_i M + b_i)$ denote a universal form with k linear factors.

Hardy-Littlewood Conj. (1923)

$$\#\{M \leq X \mid P_k(M) \text{is an absolute pseudoprime}\}$$
$$\sim C(P_k)\ \frac{X}{(\ln X)^k}\ (X \to \infty).$$

Here $C(P_k)$ is an constant computable from $\{a_i, b_i\}_{i=1}^{k}$.

Making this discussion more in detail, Dubner has computed a conjectural value of the number of absolute pseudoprimes of the form $(6M+1)(12M+1)(18M+1)$ and compared with the actual value in the range $M \leq 10^9$ (2002). $\cdots$ It really gives a very precise conjecture!

e.g. The triple $\mathbf{a}_3 = (a_1, a_2, a_3) = (1, 2, 3)$ satisfies (1) to (4) and gives $U_3(M, \mathbf{a}_3) = \mathfrak{U}_3(M)$ (Chernick's form).

For $k > 3$, also $U_k(m, \mathbf{a}_3) = \mathfrak{U}_k(m)$.

As a generalization of this, for $r \geq 3$, if we put

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

then, the r-tuple $\mathbf{a}_r = (a_1, \ldots, a_r)$ satisfies (1) to (4).

For $k \geq r$, put $\mathfrak{U}_{k,r}(m) = U_k\left(m; \mathbf{a}_r\right) =$

$$\left(2^{r-2}\left(2^{r-2}m+1\right)+1\right)\left(2^{2r-4}\left(2^{r-2}m+1\right)+1\right)$$

$$\times\prod_{i=1}^{k-2}\left(2^{r+i-3}\left(2^{r-2}+1\right)^2 m+1\right).$$

Then $\mathfrak{U}_{k,r}$ is a universal form. In particular $\mathfrak{U}_{k,3}(M) = \mathfrak{U}_k(M)$. Namely $\mathfrak{U}_{k,r}$ is a genralization of Chernick's $\mathfrak{U}_k$.

In general, $\mathfrak{U}_{r,r}(M)$ is a universal form with r factors.

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

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

$$\begin{aligned}\mathfrak{U}_{6,6}(M) &= (272M+1)(4352M+1)\\ &\times (4624M+1)(9248M+1)\\ &\times (18496M+1)(36992M+1)\end{aligned}$$

$$\begin{aligned}\mathfrak{U}_{7,7}(M) &= (1056M+1)(33792M+1)\\ &\times (34848M+1)(69696M+1)\\ &\times (139392M+1)(278784M+1)\\ &\times (557568M+1)\end{aligned}$$

$$
\begin{tikzcd}
{} & {} & {} & {} & {} & \\
\mathfrak{U}_{8,3} \arrow[u] \arrow[r] & \mathfrak{U}_{8,4} \arrow[u] \arrow[r] & \mathfrak{U}_{8,5} \arrow[u] \arrow[r] & \mathfrak{U}_{8,6} \arrow[u] \arrow[r] & \mathfrak{U}_{8,7} \arrow[u] \arrow[r] & {} \\
\mathfrak{U}_{7,3} \arrow[u] \arrow[r] & \mathfrak{U}_{7,4} \arrow[u] \arrow[r] & \mathfrak{U}_{7,5} \arrow[u] \arrow[r] & \mathfrak{U}_{7,6} \arrow[u] \arrow[r] & \mathfrak{U}_{7,7} \arrow[u] & \\
\mathfrak{U}_{6,3} \arrow[u] \arrow[r] & \mathfrak{U}_{6,4} \arrow[u] \arrow[r] & \mathfrak{U}_{6,5} \arrow[u] \arrow[r] & \mathfrak{U}_{6,6} \arrow[u] & & \\
\mathfrak{U}_{5,3} \arrow[u] \arrow[r] & \mathfrak{U}_{5,4} \arrow[u] \arrow[r] & \mathfrak{U}_{5,5} \arrow[u] & & & \\
\mathfrak{U}_{4,3} \arrow[u] \arrow[r] & \mathfrak{U}_{4,4} \arrow[u] & & & & \\
\mathfrak{U}_{3,3} \arrow[u] & & & & &
\end{tikzcd}
$$

e.g. The quadruple $\mathbf{a}_4 = (a_1, a_2, a_3, a_4) = (1, 3, 8, 12)$ satisfies (1) to (4) and gives

$$\mathfrak{V}_k(m) = U_k(m, \mathbf{a}_4) =$$
$$(24m+1)(72m+1)(192m+1)(288m+1)$$
$$\times \prod_{i=1}^{k-4} \left(288 \cdot 2^i m + 1\right) \quad (k \geq 4).$$

Then $\mathfrak{V}_4(M) = (24M+1)$ and $\mathfrak{V}_k(2^{k-5}M)$ $(k \geq 5)$ are universal forms:

$$\mathfrak{V}_4(M) = (24M+1)(72M+1)(192M+1)(288M+1)$$
$$\mathfrak{V}_5(M) = (24M+1)(72M+1)(192M+1)$$
$$\times (288M+1)(576M+1)$$
$$\mathfrak{V}_6(2M) = (48M+1)(144M+1)(384M+1)$$
$$\times (576M+1)(1152M+1)(2304M+1)$$

Another Form

By the same method as the main result, we can prove

Prop. For $k \geq 3$, put

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

Then, setting $m = 3^{k-3}M$, we obtain a universal form $\mathcal{W}_k\left(3^{k-3}M\right)$ with k linear factors.

e.g.

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

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

Expected Value

In the range $M \leq X$, let us now compute the expected value $E(X)$ of the number of M for which absolute pseudoprimes are generated by these universal forms. For $\mathfrak{U}_{4,4}(M)$, $\mathfrak{U}_{5,5}(M)$, $\mathcal{W}_4(3M)$, we compare the values with actual numbers.

Our discussion are based on the fact that the probability of a natural number N to be a prime is about $1/\ln(N)$.

We compute the conditional probability that all linear factors of the universal form are simultaneously primes.

$$\mathrm{Li}(x) := \int_2^x \frac{dt}{\ln(t)}.$$

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

$$E(X) \sim \frac{A}{6a_X X}\Big\{ \mathrm{Li}(a_X X) - \mathrm{Li}(a_X) - \frac{a_X X}{\ln(a_X X)} - \frac{a_X X}{\ln^2(a_X X)} - \frac{2a_X X}{\ln^3(a_X X)} \Big\}.$$

Here a_X is a constant defined by

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

and $A \sim 41.51196$.

Precisely $A = (2.5)^4\, C_1\, C_2\, C_3$, where

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

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

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

These appears from the conditional probability.

Actual Value

Let $N(X)$ be the number of $M \leq X$ for which strong pseudoprimes are generated by these universal forms. We can enumerate it easily by the sieving method.

We have made a computer experiment in the range $X \leq 10^9$ for the $\mathfrak{U}_{4,4}(M)$, $\mathfrak{U}_{5,5}(M)$, $\mathcal{W}_4(3M)$ above.

The results are seen in the table from the next slides.

$\mathfrak{U}_{4,4}(M)$

X	$E(X)$	$N(X)$	$E(X)/N(X)$
10^3	2	2	1.00000
10^4	16	17	0.94118
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

$\mathfrak{U}_{5,5}(M)$

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

$\mathcal{W}_4(3M)$

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

References

[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] A. Korselt, Problème chinois, *L'intermédiaire Math.* **6** (1899), 143.

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

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