2004－AL－94　(3)
2004／3／19

合成数の AKS witness に関する実験的研究

瀬川　紘 [*1], 玉木　久夫 [*2]

正整数 n に対して合同式 $(x+a)^n \neq x^n+a \pmod{n, x^r-1}$ を満たしかつ $gcd(a,n)=1$ であるような正整数 r と整数 a の対は n が合成数のときかつそのときに限り存在する。このような対 (r,a) を合成数 n の AKS witness と呼ぶことにする。Agrawal, Kayal と Saxena の決定的多項式時間素数性判定アルゴリズムは、(1) 与えられた n に対して r がある性質を満たすとき、もし n が素数の冪乗でない合成数ならば $1 \leq a \leq O\sqrt{r}\log n$ の範囲の a で (r,a) が n の AKS witness であるものが存在する、(2) その性質を満たす $r = O(\log^5 n)$ が必ず存在する、ことに基づいている。我々は小さい値の AKS witness の存在について実験を行った。結果の一部として、10^{11} 以下のすべての合成数 n および 10^{16} 以下のすべての Carmichael 数 n に対して $(r,1)$ が n の AKS witness であるような r の最小値は $0.49\log_2 n$ 以下、ある $1 \leq a \leq r$ に対して (r,a) が n の AKS witness であるような r の最小値は $0.37\log_2 n$ 以下であることを見出した

Experimental research on AKS witness of the number of composition

Kou SEGAWA[*1] and Hisao TAMAKI[*2]

For any integer $n \geq 2$, congruence $(x+a)^n \neq x^n+a \pmod{n, x^r-1}$ is satisfied by some positive r and a with $gcd(n,a)=1$ if and only if n is a composite number. We call such a pair (r,a) an AKS witness of the composite n. The deterministic polynomial time primality algorithm of Agrawal, Kayal and Saxena is based on the facts: (1)if r satisfies some condition with respect to given n, and if n is a composite but is not a power of a prime, then (r,a) is an AKS witness of n for some $1 \leq a \leq O(\sqrt{r}\log n)$; (2) for every n this condition is satisfied by some $r = O(\log^5 n)$. We have conducted experiments on the existences of AKS witnesses with small values. In particular, we have found that, for every composite $n \leq 10^{11}$ and for every Carmichael number $n \leq 10^{16}$, n has an AKS witness $(r,1)$ with $r \leq 0.49\log_2 n$ and an AKS witness (r,a) for some $1 \leq a \leq r$ with $r \leq 0.37\log_2 n$.

Key Words : Primality testing, AKS algorithm, AKS witness

1. は　じ　め　に

素数とは 1 とその数以外では割り切れない正整数である。与えられた整数が素数であるか否かという素数判定問題は何世紀も前から存在し、素数の数学的性質を安全性の根拠とする RSA 暗号が実用化されてからはさらに熱心に研究が行なわれてきた。

2002 年に Agrawal らにより発表された AKS アルゴリズム [1] は初めての決定的多項式時間素数判定アルゴリズムであり $\tilde{O}(\log^{7.5} n)$ 時間で決定的素数判定を行なうという理論的上界を示した。

AKS アルゴリズムは素数判定問題が多項式時間の計算量クラスに属するかどうかという理論的な問題を解決したという意味でも大変重要なものであるが、応用分野（特に暗号分野）における決定的素数判定アルゴリズムの実用の可能性を示唆している点でも興味深い。画期的なアルゴリズムである AKS アルゴリズムはまだ発表されてから日が浅い事もあり、活発なアルゴリズム改良が続いている [5]。

AKS アルゴリズムは次の合同式を基礎として

[*1] 明治大学大学院理工学研究科基礎理工学専攻
[*1] Computer Science Course,Major in Science,Graduate School of Science and Technology, Meiji University.
[*2] 明治大学理工学部情報科学科
[*2] DepartMent of Computer Science,Meiji University.

いる。

$$(x+a)^n \equiv x^n + a \pmod{n, x^r - 1} \qquad (1)$$

この合同式は、両辺の x に関する多項式が、係数については n を法とし、多項式としては x^r-1 を法として合同であることを意味している。n が素数のときには、この合同式はどのような正整数の対 (r,a) に対しても成立する。一方、n が合成数のときには、この合同式を成立させないような対 (r,a) が存在する。

定義 1.1 n を合成数、a をを $gcd(n,a)=1$ であるような整数、r を任意の正整数とするとき、合同式 *(1)* が成り立つならば *(r,a)* を n の *AKS non-witness* 成り立たないならば (r,a) を n の *AKS witness* と呼ぶ。

合成数 n に対する AKS witness すべてからなる集合を W_n で表す。

Agrawal らは素数の冪でないどのような合成数 n に対しても $r = O(\log^5 n), 1 \le a \le O(\sqrt{r}\log n)$ を満たす AKS witness(r,a) が存在する事を示した。我々は「合成数 n に対して上の上限よりさらに小さい値の AKS witness の存在を保証することができるか？」という問いに興味を持ち、その問いに答えるための手がかりとなる実験データを提供する事を目的とする。

具体的には、次に定義する関数の値を (1)$n < 10^{11}$ の範囲のすべての合成数、(2)$n < 10^{16}$ の範囲のすべての Carmichael 数、(3)$10^{10} \le m \le 10^{10}+10^8$, $10^{20} \le m \le 10^{20}+10^8$, $10^{30} \le m \le 10^{30}+10^8$,$10^{40} \le m \le 10^{40}+10^8$ の範囲の $(6m+1)(12m+1)(18m+1)$ の形をした Carmichael 数に対して求めた。

$$\beta_f^+(n) = \min\{r \mid \exists a, 1 \le a < f(n,r), (r,a) \in W_n \text{ or } r \mid n\}$$
$$\beta_f^-(n) = \min\{r \mid \exists a, 1 \le a < f(n,r), (r,-a) \in W_n \text{ or } r \mid n\}$$

ここで、f は一般には n と r の関数であるが、$f(n,r)=1$、$f(n,r)=r$、$f(n,r)=\log n$ の三つの場合について実験を行った[1]。

実験の結果、(1) の範囲では $\beta_1^+(n) \le 0.49\log n$、$\beta_r^+(n) \le 0.37\log n$、$\beta_{\log n}^+(n) \le 0.37\log n$ が成り立っている。(2) の範囲では $\beta_1^+(n) \le 0.49\log n$、$\beta_r^+(n) \le 0.37\log n$、$\beta_{\log n}^+(n) \le 0.37\log n$ が成り立っている。(3) の範囲では $\beta_1^+(n) \le 0.15\log n$、$\beta_r^+(n) \le 0.15\log n$、$\beta_{\log n}^+(n) \le 0.15\log n$ が成り立っている。

[1] この論文では特に断りの無い限り対数の底は 2 とする

もしもこれらの傾向が一般の n に対しても成り立つならば、AKS witness に基づいた素数性判定アルゴリズムは $\tilde{O}(\log^4 n)$ 時間で実行できることになる。

また、実験を高速化する努力のなかで我々は次の観察を得た。すなわち n を奇合成数とするとき、$(2,1)$ が n の AKS witness であること、$(2,-1)$ が n の AKS witness であること、および n が底 2 の疑素数であることはすべて互いに同値である。この観察を用いて、上の実験において底 2 の疑素数以外の n を実験の対象から排除することにより、実験時間の大幅な短縮が可能となった。

また我々は $(r,-1)$ の形をした AKS witness に関する Agrawal, Kayal と Saxena の予想 (AKS 予想) についての補足的な実験も行った。この実験においては、Kayal と Saxena の公開している実験データの誤り (リストからのデータ欠落) を発見することができた。この発見には、上で述べた観察が大きな役割を果たしている。

さらに、実験結果の観察から上の観察を一般化する次の命題を証明した。

命題 1.2 正整数 $a \le 2$ に対して $(a-1)^n \equiv a-1 \pmod{n}$ かつ $(a+1)^n \equiv a+1 \pmod{n}$ であるならば $(2,a)$ と $(2,-a)$ はどちらも n の *AKS witness* ではない。

2. 準　　備

素数 n は n の倍数以外の任意の整数 a に対して合同式

$$a^{n-1} \equiv 1 \pmod{n}$$

を満す (フェルマーの小定理)。合成数 n が n と互いに素な a に対してこの合同式を満たすとき、n は底 a の擬素数と呼ばれる。n が n と互いに素なすべての a を底とする擬素数であるとき n は Carmichael 数と呼ばれる。

次の定理はフェルマーの小定理の拡張であり、AKS アルゴリズムの基礎をなす。

定理 2.1 a を n と互いに素な数とする。この時 n が素数の時、かつその時に限り

$$(x+a)^n \equiv x^n + a \pmod{n} \qquad (2)$$

が成り立つ。

素数性の判定にこの合同式をそのまま用いてすべての係数を求めるならば指数時間を要する。Agrawal らのアイディアは合同式 (2) の評価を x^r-1 を法として行うことであった。前節での彼らの理論への言及を、AKS witness という言葉を使わずに

言い替えると、「適切に選んだ $O(\log^5 n)$ の大きさの r を用いてもとの合同式を正確に評価することができる」となる。

3. 擬素数と AKS non-witness の関連性について

次の命題は、合同式 (1) の x に 1 を代入することにより得られる。

命題 3.1 もし、(r,a) が合成数 n の *AKS non-witness* ならば $(a+1)^n \equiv a+1 \pmod n$ が成り立つ。

$r=2$ の場合には、逆方向の関係を表す次の命題が成立する。

命題 3.2 奇合成整数 n と正整数 a に対して $(a+1)^n \equiv a+1 \pmod n$ と $(a-1)^n \equiv a-1 \pmod n$ が成り立つならば $(2,a)$ と $(2,-a)$ はともに n の *AKS non-witness* である。

証明

$$O_a = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{2i+1} a^{2i+1}$$

$$E_a = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{2i} a^{2i}$$

とおく。仮定を用いると

$$O_a - E_a = (a-1)^n \equiv a-1 \pmod n$$
$$O_a + E_a = (a+1)^n \equiv a+1 \pmod n$$

より

$$2O_a \equiv 2a \pmod n \tag{3}$$

であり、n は仮定より奇数だから

$$O_a \equiv a \pmod n \tag{4}$$

が成り立つ。同様に

$$E_a \equiv 1 \pmod n \tag{5}$$

が言える。したがって、

$$(x+a)^n \equiv E_a x + O_a \pmod{x^2-1}$$
$$\equiv x^n + a \pmod{n, x^2-1}$$

$$(x-a)^n \equiv E_a x - O_a \pmod{x^2-1}$$
$$\equiv x^n - a \pmod{n, x^2-1}$$

が成り立つ。 □

命題 3.1 と命題 3.2 で $a=1$ とした場合から次の系が成り立つ。

系 3.3 奇合成数 n に対して以下の *3* 条件は互いに同値である。

1. $(2,1)$ は n の *AKS non-witness* である。
2. $(2,-1)$ は n の *AKS non-witness* である。
3. n は底 2 の擬素数である。

時間的には系 3.3 がまず発見されて、実験の高速化に利用された。そののち命題 3.2 が実験結果より示唆され、系 3.3 の証明が一般化された。命題 3.1 は、多くの a に対して合同式 1 が成り立つような n は Carmichael 数である可能性が高いことを示唆しており、Carmichael 数に特化した実験をある程度正当化している。

4. 実　験　結　果

$f(n,r)=1$、$f(n,r)=r$、$f(n,r)=\log n$ のそれぞれの場合についての $\beta_f^+(n)$ の $n<10^{11}$ の範囲のグラフを図 1 に示す。これらのグラフは n については対数スケールであり、また $\beta(n)>\beta(n')$ がすべての $n'<n$ に対して成り立つような n のみをプロットしている。10^{11} 以下の底 2 の擬素数は 38975 個であり、したがってそれ以外の大半の奇合成数に対しては関数値はすべて 2 であることに注意する。また、この範囲の *Carmichael* 数は 3605 個であった。

表 1 は、β の各変種に対して $n<10^{11}$ の範囲で $\beta(n)=r$ となる奇合成数 n の個数を r ごとにまとめている。表 3 と表 2 は、特に $\beta_{\log n}$ の場合に、n が Carmichael 数の場合とそれ以外の場合を分けて示している。$r=2$ に対する振舞いが二つの場合で正反対である理由は前節の命題 3.1 と命題 3.2 が説明している。

Table 1　$\beta(n)=r$ である $n<10^{11}$ の個数

r	β_1^+	β_r^+	$\beta_{\log n}^+$	β_1^-	β_r^-	$\beta_{\log n}^-$
2	★★	★★	35370	★★	★★	35370
3	1042	34196	2069	34196	37165	2069
4	18008	3799	1095	1431	1334	1095
5	18912	888	392	2942	426	392
6	508	42	0	0	0	0
7	457	49	48	367	49	48
8	39	1	1	34	1	1
9	8	0	0	5	0	0
10	1	0	0	0	0	0

表 4 は、$f(n,r)=r$ の場合について $n<10^{16}$ の範囲で $\beta_f^+(n)=r$ となる Carmichael 数 n の個数を r ごとにまとめている。また、$n<10^{16}$ の範囲の Carmichael 数に対する β 関数のグラフを図 2 に示

Fig. 1　$\max \beta_f(n)$

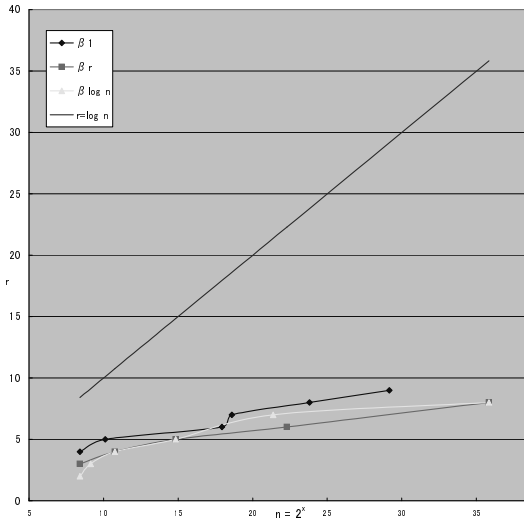

Table 2　Carmichael 数

r	$\beta^+_{\log n}$	$\beta^-_{\log n}$
2	35370	35370
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0

Table 3　非 Carmichael 数

r	$\beta^+_{\log n}$	$\beta^-_{\log n}$
2	0	0
3	2069	2069
4	1095	1095
5	392	392
6	0	0
7	48	48
8	1	1

す。この実験に使用した Carmichael 数のリストは [3] から得た。さらに、$10^{10} \le m \le 10^{10}+10^8$,$10^{20} \le m \le 10^{20}+10^8$, $10^{30} \le m \le 10^{30}+10^8$,$10^{40} \le m \le 10^{40}+10^8$ の範囲の、$(6m+1)(12m+1)(18m+1)$ の形をした Carmichael 数 [4] に対する表を表 5,6,7,8 に示す。

5. AKS 予想に関連した Kayal と Saxena の実験データについて

Agrawal らは [1],[2] で次の予想をしている。

AKS 予想 5.1 もし r が素数で n を割り切らず、

$$(x-1)^n \equiv x^n-1 \pmod{n, x^r-1}$$

が成り立つならば、n は素数であるか、または $n^2 \equiv 1 \pmod r$ である。

この予想が正しければ、与えられた n に対してまず $n^2 \not\equiv 1 \pmod r$ であるような最小の素数 r を求め、この r に対して上の合同式を評価するという単純な手続きにより $\tilde{O}(\log^3 n)$ 時間で素数判定ができることになる。[1],[2] において $r \le 100$,$n \le 10^{10}$ の範囲で実験が行なわれ、予想が正しい事が確かめられたと述べられている。[2] に公開された彼らの実験データには、10^{10} 以下のすべての奇合成数 n と 100 以下の素数 r の対で $(r,-1)$ が n の AKS non-witness となるようなものすべてがリストされている。我々は当初このリストを基に我々の実験を進めようとしたが、その検討課程でこのリストの誤りを発見した。すなわち、このリストからは、$4\cdot 10^9$ 以上の底 2 の擬素数 n に対するエントリ $(n,2)$ が欠落している。これらのエントリが必要であることは、系 3.3 が示している。欠落している n で最もちいさな値は 4004179201、最も大きな値は 9998721001 であり、欠落している底 2 の擬素数の個数は 2156 である。なお、当然ながら不足データは AKS 予想の反例を示すものではない。

6. 終　わ　り　に

本研究では「合成数 n に対して $r = O(\log^5 n)$ よりさらに小さい値の AKS witness の存在を保証することができるか？」という問いに興味を持ち、その問いに答えるための手がかりを求めて実験を行なった。実験した範囲では、$r < \log n$ なる AKS witness が必ず存在しているが、理論的な上界を示さない限り、アルゴリズムの高速化に結びつくことはない。今後は r の値のみならず、この実験で得られた non-witness の構造的性質も調べて理論的な進展に結びつく観察を得ることを目指したい。

文　　献

(1) Manindra Agrawal,Neeraj Kayal and Nitin Saxena.”Primes is in P” available at http://www.cse.iitk.ac.in/primality.pdf

(2) Neeraj Kayal and Nitin Saxena.”Toward a deterministic polynomial-time test”, TechnicalReport,IIT Kanpur,2002, avaibale at http://www.cse.iitk.ac.in/research/btp2001/primality.html together with a separate experimental data file.

(3) Richard G.E. Pinch. Compressed text file carmichael.gz,available at ftp://ftp.dpmms.cam.ac.uk/pub/rgep/Carmichael

(4) Gunter Loh,Wolfagang Niebuhr. ”A New Algorithm for constructing large carmichael numbers”

(5) The American Institute of Mathematics, ”Future directions in algorith-

mic number theory”, 2003, avaibale at http://www.aimath.ord/WWN/primesinp

Table 4　$\beta(n)=r$ である 10^{16} 以下の Carmichael 数の個数

r	$\beta_1^+(r)$	$\beta_r^+(r)$	$\beta_{\log n}^+(r)$	$\beta_1^-(r)$	$\beta_r^-(r)$	$\beta_{\log n}^-(r)$
2	**	**	0	**	**	0
3	565	58087	165152	58087	163494	165152
4	19600	140165	63133	10613	63486	63133
5	194807	44891	16707	156595	17980	16707
6	7039	1822	0	5	0	0
7	22651	1560	1533	19661	1560	1533
8	1583	80	80	1356	80	80
9	351	60	60	301	60	60
10	14	0	0	0	0	0
11	69	17	17	67	17	17
12	2	0	0	1	0	0
13	2	1	1	2	1	1

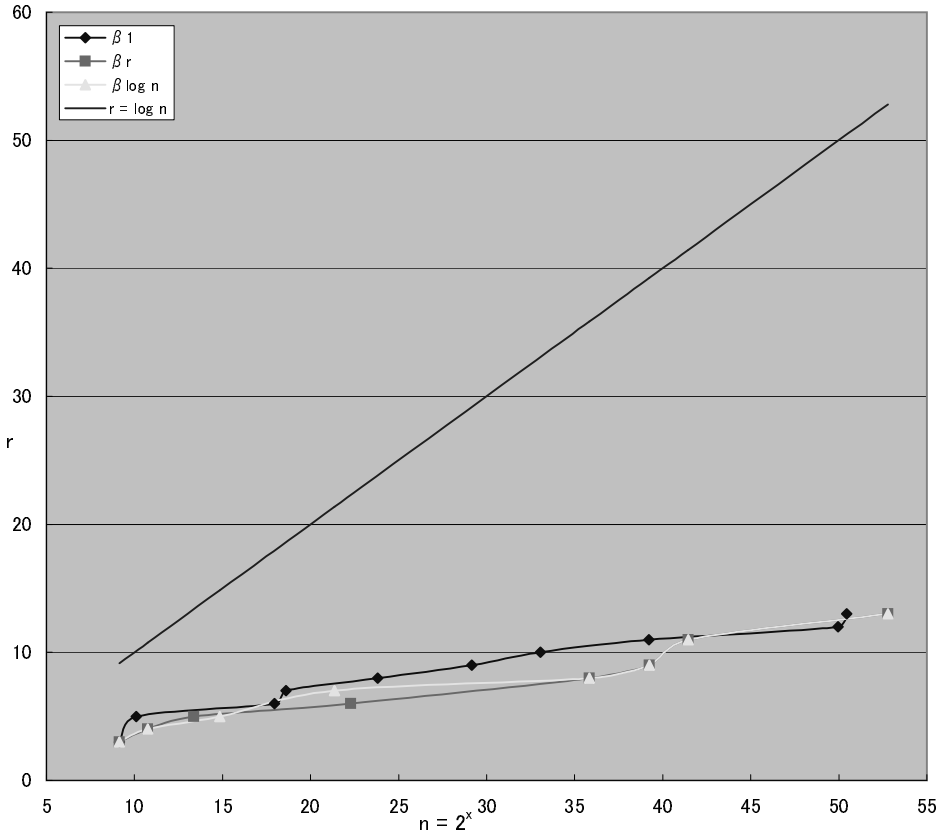

Fig. 2　$\max \beta_f(n)$

$C(m_1,m_2)$: $m_1 \le m \le m_2$ なる m に対して $(6m+1)(12m+1)(18m+1)$ の形をした Carmichael 数の集合

Table 5　$\beta(n)=r$ であるような $n \in C(10^{10},10^{10}+10^8)$ の個数

r	$\beta_1^+(r)$	$\beta_r^+(r)$	$\beta_{\log n}^+(r)$	$\beta_1^-(r)$	$\beta_r^-(r)$	$\beta_{\log n}^-(r)$
2	⋆⋆	⋆⋆	0	⋆⋆	⋆⋆	0
3	0	0	0	0	0	0
4	0	52570	52570	0	52570	52570
5	52001	25570	25570	52001	25575	25575
6	0	0	0	0	0	0
7	39025	19439	19439	39025	19439	19439
8	9839	3281	3281	9839	3281	3281
9	2222	2222	2222	2222	2222	2222
10	0	0	0	0	0	0
11	951	951	951	951	951	951
12	0	0	0	0	0	0
13	105	105	105	105	105	105
14	0	0	0	0	0	0
15	0	0	0	0	0	0
16	10	10	10	10	10	10
17	7	7	7	7	7	7

$\min n = 1296000043196400479919961777332889$

Table 6　$\beta(n)=r$ であるような $n \in C(20^{10},10^{20}+10^8)$ の個数

r	$\beta_1^+(r)$	$\beta_r^+(r)$	$\beta_{\log n}^+(r)$	$\beta_1^-(r)$	$\beta_r^-(r)$	$\beta_{\log n}^-(r)$
2	⋆⋆	⋆⋆	0	⋆⋆	⋆⋆	0
3	0	0	0	0	0	0
4	0	7468	7468	0	7468	7468
5	7499	3729	3729	7499	3729	3729
6	0	0	0	0	0	0
7	5564	2794	2794	5564	2794	2794
8	1427	499	499	1427	499	499
9	299	299	299	299	299	299
10	0	0	0	0	0	0
11	138	138	138	138	138	138
12	0	0	0	0	0	0
13	10	10	10	10	10	10

Table 7　$\beta(n)=r$ であるような $n \in C(10^{30},10^{30}+10^8)$ の個数

r	$\beta_1^+(r)$	$\beta_r^+(r)$	$\beta_{\log n}^+(r)$	$\beta_1^-(r)$	$\beta_r^-(r)$	$\beta_{\log n}^-(r)$
2	⋆⋆	⋆⋆	0	⋆⋆	⋆⋆	0
3	0	0	0	0	0	0
4	0	79	79	0	79	79
5	1278	1204	1204	1278	1204	1204
6	0	0	0	0	0	0
7	867	862	862	867	862	862
8	141	141	141	141	141	141
9	98	98	98	98	98	98
10	0	0	0	0	0	0
11	31	31	31	31	31	31
12	0	0	0	0	0	0
13	3	3	3	3	3	3

Table 8　$\beta(n)=r$ であるような $n \in C(10^{40},10^{40}+10^8)$ の個数

r	$\beta_1^+(r)$	$\beta_r^+(r)$	$\beta_{\log n}^+(r)$	$\beta_1^-(r)$	$\beta_r^-(r)$	$\beta_{\log n}^-(r)$
2	⋆⋆	⋆⋆	0	⋆⋆	⋆⋆	0
3	0	0	0	0	0	0
4	0	33	33	0	33	33
5	551	521	521	551	521	521
6	0	0	0	0	0	0
7	390	387	387	390	387	387
8	56	56	56	56	56	56
9	48	48	48	48	48	48
10	0	0	0	0	0	0
11	15	15	15	15	15	15
12	0	0	0	0	0	0
13	2	2	2	2	2	2