2005－ＣＳＥＣ－30（７）
2005／7／21

Miller–Rabinテストでの誤判定確率の実験的計測値と理論的上界値との比較

中島 俊哉

(株) 富士通研究所 〒674–8555 兵庫県明石市大久保町西脇 64
E-mail: tossi@jp.fujitsu.com

あらまし Miller–Rabin テストにおける誤判定確率 (強 probable prime が強擬素数である確率) の理論上界を，ビット長 100 以上 300 以下のランダムに生成した奇数について計測した実験値と比較した．その結果，理論での期待値により各ビット長で 16 個程度強擬素数が観測されるはずの強 probable prime の個数について実際には強擬素数は全く観測されなかった．この結果を統計的に解析することにより，300 ビット以下での実際の誤判定確率は 95%の信頼度で現状での最小の理論上界よりも 1/4 以下であろうという推測値を得た．

キーワード 素数判定，Miller–Rabin テスト，誤判定確率，IEEE P1363

Comparison of Error Probabilities of The Miller–Rabin Test by Experimental Measurement Value and Theoretical Upper Bound

Toshiya NAKAJIMA

Fujitsu Laborartories Ltd. Nishiwaki 64, Okubo-cho, Akashi-shi, Hyogo, 674–8555 Japan
E-mail: tossi@jp.fujitsu.com

Abstract We compare theoretical upper bounds of error probability of the Miller–Rabin test(probability that a strong probable prime is a strong pseudoprime) with experimental results for randomly generated odd integers of 100–300 bitlength. The number of strong probable primes we test is the theory–conjectured number in which about sixteen strong pseudoprimes would be found for each bitlength. After the experiment, no strong pseudoprimes were found. Analyzing this result by statistical inference, we estimate with 95% upper confidence limit that the real error probability for the range of tested bitlength is less than 1/4 of the minimum theoretical upper bound.

Key words primality proving, Miller–Rabin test, error probability, IEEE P1363

1. はじめに

確率的素数判定法である Miller–Rabin テストでは，テストを通過した強 probable prime(SPP) のごく一部が合成数 (強擬素数, SPSP) である可能性がある．SPP に対して SPSP が占める割合が誤判定確率であり，この確率の理論的上界値として IEEE P1363 [3] 等に記載されている値が一般に用いられている．しかし実際にはこれよりはるかに低い上界値が理論的に導出されている文献 [1], [2] が存在することから，現時点で最も低い上界値がさらに改良され得るのかが興味の対象になる．本稿では誤判定確率を実験的に計測し理論的上界値と比較することにより，現時点の上界値がより下がる可能性があるかを推測する．

2. 誤判定確率の基本評価式

本稿における誤判定確率は Miller–Rabin テストを通過した奇数 (強 probable prime) が合成数 (強擬素数) である確率を意味する．テスト対象の奇数とそれに対する Miller–Rabin テストの底とをランダムに選ぶものとすると，誤判定確率は条件付き確率を用いて次のように定式化される：

ランダムに選んだ k ビットの奇数 n が合成数であったという事象を C，ランダムに選んだ異なる t 個の底について n がテストを通過したという事象を A とすると，k ビットの奇数全体の平均誤判定確率 $p(k,t)$ は事象 A の後で事象 C が発生する条件付き確率 $\Pr(C|A)$ として表わされる．したがって，

$$p(k,t) = \Pr(C|A) = \Pr(C \cap A) \ / \ \Pr(A) \qquad (1)$$

となる．ここで $\Pr(A)$ は t 個の底全てについて k ビットの奇数

がテストを通過する平均確率，$\Pr(C \cap A)$ は t 個の底全てについて k ビットの合成数がテストを通過する平均確率である．

底の範囲は $[1,\ n-1]$ であり，奇数 n について素数と判定する底の個数を $S(n)$ とすると n が 1 つの底でテストを通過する確率は $S(n)/(n-1)$ であるから，$\Pr(A)$ は次式で表わされる [2]．

$$\begin{aligned}\Pr(A) &= 2^{-(k-2)} \sum_{n \in M_k} \left\{ \frac{S(n)}{n-1} \right\}^t \\ &= 2^{-(k-2)} \left[\sum_{n \in C_k} \left\{ \frac{S(n)}{n-1} \right\}^t + \sum_{n \in P_k} 1 \right]. \end{aligned} \tag{2}$$

ここで M_k, C_k, P_k は各々 k ビットの奇数，合成数，素数の集合．

同様に，$\Pr(C \cap A)$ は次式で表わされる．

$$\Pr(C \cap A) = 2^{-(k-2)} \sum_{n \in C_k} \left\{ \frac{S(n)}{n-1} \right\}^t. \tag{3}$$

以上により $p(k,t)$ の基本評価式

$$\begin{aligned} p(k,t) &= \frac{\sum_{n \in C_k} \left\{ \frac{S(n)}{n-1} \right\}^t}{\sum_{n \in C_k} \left\{ \frac{S(n)}{n-1} \right\}^t + (\pi(2^k) - \pi(2^{k-1}))} \\ &\leqq \sum_{n \in C_k} \left\{ \frac{S(n)}{n-1} \right\}^t / \left(\pi(2^k) - \pi(2^{k-1}) \right) \\ &=: \lambda / \rho \end{aligned} \tag{4}$$

を得る．ここで $\pi(\cdot)$ は素数計数関数．

上式により，λ の上界と ρ の下界とから $p(k,t)$ の上界が求まることになる．なお，$S(n)$ については Monier による公式 [6] があるが，これは n の素因数の情報を用いるため直接的には適用できない．

3. 誤判定確率の各種の上界値

前節で示したとおり，誤判定確率の上界の評価は $\lambda := \sum_{n \in C_k} \{S(n)/(n-1)\}^t$ の上界と $\rho := \pi(2^k) - \pi(2^{k-1})$ の下界との評価に帰着されるため，これらの評価の精密度の差異により [1], [2], [3] などでの各種の上界値が得られることになる．(ただし ρ の下界はこれら全てで共通であり $\rho \geqq 0.71867 \cdot 2^k/k$ と表わされる [2].)

以下，各種の $p(k,t)$ または λ の評価式を示す．

・評価式 1 [3]：

$$p(k,t) < \frac{k^{2/3} \cdot 2^t \cdot 4^{2-\sqrt{tk}}}{\sqrt{t}}. \tag{5}$$

ここで $(k \geqq 21,\ 3 \leqq t \leqq k/9)$ または $(k \geqq 88,\ t = 2)$．

$$p(k,1) < k^2 4^{2-\sqrt{k}}. \tag{6}$$

ここで $k \geqq 2$．

これらの式は計算が簡単であり，実用上十分低い上界が得られるため一般的に用いられている．実際にはこれらの式は [2] からの引用であり，次に示す更に低い上界をもとに導出される．

・評価式 2 [2]：

$$\lambda \leqq 2^{k-2-Mt} + c \cdot 2^{k-2+t} \cdot \sum_{m=3}^{M} \sum_{j=2}^{m} 2^{m(1-t)-j-\frac{k-1}{j}}. \tag{7}$$

ここで $c = 8(\pi^2 - 6)/3$，$3 \leqq M \leqq 2\sqrt{k-1} - 1$，$k \geqq 21$，$t \geqq 1$．$M$ は自由パラメタであり，数値計算では M を変化させて最小の上界を探索することになる．

この式の導出過程を検討すると上界を改良できる余地があることが判る．[2] では導出の途中で $|N(m,k,j)|$ で表される値を次のように評価し，M を有限の範囲に収めるため 2 番目の不等号を用いている：

$$\begin{aligned} |N(m,k,j)| &< 2^k \cdot \frac{\pi^2 - 6}{3} \cdot \frac{2^{m+1-j} - 1}{2^{(k-1)/j} - 1} \\ &\leqq 2^{k+1} \cdot \frac{\pi^2 - 6}{3} \cdot 2^{m-j-(k-1)/j}. \end{aligned}$$

実際には $|N(m,k,j)|$ の評価は最初の不等号で十分であるのでこれを用いると λ の上界は次で計算される．

・評価式 3：

$$\begin{aligned} \lambda &\leqq 2^{k-2-Mt} \\ &\quad + c \cdot 2^{k-3+t} \sum_{m=3}^{M} 2^{-mt} \sum_{j=2}^{m} \frac{2^{m+1-j} - 1}{2^{(k-1)/j} - 1}. \end{aligned} \tag{8}$$

このとき自由パラメタ M は $M \geqq 3$ になり範囲が有限ではないが，実際には $M = 100$ 程度で収束する．

・評価式 4 [1]：

$$\begin{aligned} \lambda &\leqq 2^{k-2-Mt} + 2^{k-1} c_s (2^{t/q} - 1) \\ &\quad \cdot \sum_{m=2+1/q}^{M(\text{step } 1/q)} 2^{-mt} \sum_{j=2}^{\lceil m \rceil} \frac{\lceil 2^{m+1-j} \rceil - 1}{2^{(k-1)/j} - 1}. \end{aligned} \tag{9}$$

ここで $3 \leqq M \leqq 2\sqrt{k-1} - 3$，$q = 4$，
$c_s = (s+1)((\pi^2/6) - \sum_{n=1}^{s}(1/n^2))$，$s = \min\{s_1,\ 30\}$，$s_1 \leqq (2^{(k-1)/j} - 1)2^{j-M-2}$ $(2 \leqq j \leqq M$ であるすべての j について$)$．

この式も評価式 2 を基に改良したものとなる．

これらの各式とは異なる導出方法による評価式として，実数 x 以下の奇数 n に対する Fermat テストの平均誤判定確率 $P(x)$ を用いた式を次に示す．

・評価式 5 [2]：

$$\begin{aligned} \lambda &\leqq \frac{2^{-M_1(t-1)+(k-1)}}{2 + k \ln 2} P(2^k) + k 2^{-M_1(t-1)-2} \\ &\quad + c_1 \frac{2^{k-2+t}}{1 - 2^{1-t}} \sum_{j=2}^{M_1} 2^{-jt-(k-1)/j}. \end{aligned} \tag{10}$$

ここで $c_1 = 8(\pi^2-6)/3$, $k \geqq 2$, $t \geqq 2$, $3 \leqq M_1 \leqq 2\sqrt{k-1}-1$.

$$\lambda \leqq \frac{2^{k-1}}{2+k\ln 2}P(2^k) + \frac{k}{4} . \tag{11}$$

ここで $t=1$, $k \geqq 2$.

これらの $P(2^k)$ は[4]により以下の式で与えられる：

実数 c, L_1, L, L_2, M, l は $\frac{1}{2} < c < 1$, $10 < L_1 < L < L_2 < M/2$, $L^{3/2} \leqq 10M$, $2 \leqq l < L_1$ を満たす自由パラメタとする．このとき任意の $x > L^2$ について次式が成り立つ．

$$\begin{aligned} P(x) \leqq\ & 2(2+\ln x) \\ & \cdot \left\{ \frac{1}{4L_1} + \frac{50}{99}\left(\frac{L_1}{L_2-1}+1\right)\frac{(2+\ln L_1)^2}{L_2-1} \right. \\ & + \frac{1}{x}L_2^2\left(2+\frac{\ln x}{\ln 10}\right)(1+\ln L_1) + \frac{100}{99}\frac{(1+\ln L_1)^2}{M} \\ & + \frac{125}{3564}\frac{(1+\ln L_2)^2}{M-2L_2}(4+\ln L_1)^4 + \frac{50}{99}\frac{(1+\ln L_1)}{L} \\ & + \frac{100K_c}{(1-c)(10^{1+c}-1)}\left(\frac{M}{x}\right)^{1-c}(1+\ln L_1)^2 \\ & \cdot \sum_{i=0}^{j}\frac{1}{i!}\left(2\sum_{p\leqq l}\frac{1}{p}\right)^i\left(1+\ln\frac{L^2L_1}{m_i}\right) \\ & \left. \cdot \exp(2^{-c}\alpha_l f_c(m_i))\right\} . \end{aligned}$$

ここで $\alpha_l = (1-l^{-c})^{-\ln(L^2L_1)/\ln l}$, p_i は i 番目の素数，$m_i = p_1 \cdots p_i$, j は $m_j \leqq L^2L_1 < m_{j+1}$ で定める．また，$f_c(m_i) = \prod_{1\leqq r\leqq i}(1-p_r^{-c})^{-1}$ であり，K_c は次の上界を用いる．

$$\begin{aligned} K_c &\leqq \exp(K_c') , \\ K_c' &= \sum_{i=2}^{11} p_i^{-2c}\left(\frac{1}{2}+\frac{1}{3(p_i^c-1)}\right) \\ &\quad + \frac{1}{2c-1}\left(\frac{1}{2}+\frac{1}{3(37^c-1)}\right)\left(36^{1-2c}-\frac{1}{2}\cdot 37^{1-2c}\right) . \end{aligned}$$

以上の各評価式について実際に計算した結果を表1–表5に，各 $p(k,t)$ についての最小上界値を表6に示す．なお，各表には $p(k,t) \leqq 1/2^y$ と表した場合の y の下界を記述している．

4. 計測方法と結果

4.1 方　　法

本節では表6の $t=1$ での理論上界を基準値として，実験的に誤判定確率を計測する．基本的にはランダムに生成した奇数を Miller–Rabin テストで判定し，テストを通過した場合は確定的素数判定法 (楕円曲線法) により強擬素数かを決定する．$t=1$ であるため底は各 n について1個となる．計測手順を以下に示す．

1) ビット長 k の奇数 n をランダムに1個生成
2) $a \in [1, n-1]$ の整数 a をランダムに1個生成
3) a を底として n に対する Miller–Rabin テストを実行
4) n がテストを通過すれば SPP の観測度数を+1 し，テストを通過しなければ 1) に戻る
5) 楕円曲線法により n が合成数と判定されれば強擬素数の観測度数を+1
6) SPP の観測度数が指定した値になるまで 1)–5) を実行
7) SPP の観測度数に対する強擬素数の観測度数の比率を実験的な誤判定確率とする

上記の手順6) で指定される SPP の観測度数は次のとおり定める：この計測では得られた強擬素数の観測度数と理論値との比較が目的であるため，観測度数を用いた理論値の検定を行う必要があるが，その際二項分布が正規分布で近似できるだけの SPP の観測度数 (標本数) を確保するものとする．標本数を s とすると実用上十分な精度で近似するためには $s \cdot p(k,t) > 5$ かつ $s \cdot (1-p(k,t)) > 5$ が必要とされている[8]ことから，今回の計測では $s \cdot p(k,t) > 16$ となる s を設定する．

4.2 結　　果

以上の方針により，k=100, 150, 200, 250, 300 ビットのケースについて強擬素数の観測度数を計測した結果と，実際の誤判定確率が表6の $t=1$ での上界値に等しいとする仮説を H_0 としてこの計測結果を得る確率 $\Pr(H_0)$ とを表7に示す．全てのケースで強擬素数の観測度数が0であったため結果的に正規分布近似は必要なく，二項分布から直接 $\Pr(H_0) = (1-p(k,1))^s$ となる．なお楕円曲線法のツールとして[7]を，乱数生成ツールとして[5]を用いた．

表7の結果から，$\Pr(H_0)$ がいずれも非常に低い値であるため H_0 は成立せず，$k \leqq 300$, $t=1$ での実際の誤判定確率は表6による値よりも低いと推測できる．この推測を定量的に考察するため，表7の観測度数に対する実際の誤判定確率の区間推定値 (上側信頼限界) を表8に示す．信頼係数を $1-\alpha$ とすると，強擬素数の観測度数0のもとでの上側信頼限界は二項分布から $1-\alpha^{1/s}$ として求められる．

表8の結果と表1・表6の理論値 ($t=1$) を図1にまとめて示す．これらを比較すると，各 s に対応するビット長での理論値はいずれも計測値から推定される99%信頼区間の外側にあることが分る．したがって95%信頼区間で判断すると，$k \leqq 300$, $t=1$ での実際の誤判定確率は現時点で最小の理論値の1/4以下であろうと考えられる．

5. まとめと今後の課題

Miller–Rabin テストを通過した強 probable prime(SPP) が強擬素数 (SPSP) である確率の理論的上界値を実験的な計測値と比較した結果，今回の実験規模での統計的解析では実際の誤判定確率は現状で最小の理論値よりも1/4以下であろうとの推測値を得た．今後の課題として，100ビット以下の領域での SPSP の網羅的探索と，300ビット以上の領域での相対的に少数の SPP 観測度数による統計的解析を実施する予定である．

謝　　辞

本研究の実施にあたり，富士通研究所の伊豆哲也氏・武仲正彦氏には様々な観点から有益な議論とアドバイスをいただきました．ここに深く感謝いたします．

文　献

[1] R.J. Burthe, Jr., "Further Investigations with The Strong Probable Prime Test", Math. Comp., Vol. 65, No. 213 (1996), pp. 373–381.

[2] I. Damgård, P. Landrock, and C. Pomerance, "Average Case Error Estimates for The Strong Probable Prime Test", Math. Comp., Vol. 61, No. 203 (1993), pp. 177–194.

[3] IEEE, Standard Specifications for Public Key Cryptography, IEEE P1363/D13 (1999).

[4] S.H. Kim and C. Pomerance, "The Probability that a Random Probable Prime is Composite", Math. Comp., Vol. 53, No. 188 (1989), pp. 721–741.

[5] 松本・西村, mt19937ar.c (in Mersenne Twister Home Page), http://www.math.sci.hiroshima-u.ac.jp/~m-mat/MT/mt.html

[6] L. Monier, "Evaluation and Comparison of Two Efficient Probablistic Primality Testing Algorithms", Theoret. Comp. Sci., Vol.12 (1980), pp. 97–108.

[7] F. Morain, ECPP, the package (Version 6.4.5), http://www.lix.polytechnique.fr/~morain/Prgms/ecpp.english.html

[8] 東京大学教養学部統計学教室編, 基礎統計学 I 統計学入門, 東京大学出版会 (2004).

表 1　評価式 1 による上界値

Table 1　Upper bounds with estimation 1

$k \setminus t$	1	2	3	4	5	6	7	8	9	10
100	2	12	18	23	26	30	33	36	38	40
150	6	18	25	31	36	40	44	47	51	54
200	8	23	31	38	43	49	53	58	62	65
250	11	27	36	44	50	56	62	67	71	75
300	14	31	41	49	57	63	69	75	80	84
350	16	34	45	55	63	70	76	82	88	93
400	18	38	50	60	68	76	83	89	95	101
450	20	41	54	64	73	82	89	96	102	108
500	22	44	57	69	78	87	95	102	109	115
550	24	47	61	73	83	92	100	108	115	122
600	26	49	64	77	87	97	106	114	121	128

表 2　式評価 2 による上界値

Table 2　Upper bounds with estimation 2

$k \setminus t$	1	2	3	4	5	6	7	8	9	10
100	5	14	20	25	29	33	36	39	41	44
150	8	20	28	34	39	43	47	51	54	57
200	11	25	34	41	47	52	57	61	65	69
250	14	29	39	47	54	60	65	70	75	79
300	16	33	44	53	60	67	73	78	83	88
350	19	37	48	58	66	73	80	86	91	97
400	21	40	53	63	72	80	87	93	99	105
450	23	43	57	68	77	85	93	100	106	112
500	25	46	61	72	82	91	99	106	113	119
550	27	49	64	76	87	96	104	112	119	126
600	29	52	68	80	91	101	110	118	125	132

表 3　評価式 3 による上界値

Table 3　Upper bounds with estimation 3

$k \setminus t$	1	2	3	4	5	6	7	8	9	10
100	5	15	21	26	30	34	37	40	42	45
150	9	20	28	35	40	44	48	52	55	58
200	11	25	34	42	48	53	58	62	66	70
250	14	30	40	48	55	61	66	71	76	80
300	17	34	45	54	61	68	74	79	84	89
350	19	37	49	59	67	74	81	87	93	98
400	21	41	54	64	73	81	88	94	100	106
450	23	44	58	69	78	86	94	101	107	113
500	25	47	61	73	83	92	100	107	114	120
550	27	50	65	77	88	97	105	113	120	127
600	29	53	68	81	92	102	111	119	126	133

表 4 評価式 4 による上界値

Table 4 Upper bounds with estiination 4

$k \diagdown t$	1	2	3	4	5	6	7	8	9	10
100	7	17	23	28	32	35	38	41	44	46
150	11	22	30	36	41	46	50	53	56	60
200	14	27	36	43	49	54	59	63	67	71
250	16	32	42	49	56	62	68	72	77	81
300	19	36	46	55	63	69	75	81	86	90
350	21	39	51	60	69	76	82	88	94	99
400	24	43	55	65	74	82	89	95	101	107
450	26	46	59	70	79	88	95	102	108	114
500	28	49	63	74	84	93	101	108	115	121
550	30	52	67	79	89	98	107	114	121	128
600	31	55	70	83	94	103	112	120	128	135

表 5 評価式 5 による上界値

Table 5 Upper bounds with estimation 5

$k \diagdown t$	1	2	3	4	5	6	7	8	9	10
100	<0	5	20	25	29	33	36	39	41	44
150	<0	17	28	34	39	43	47	51	54	57
200	3	25	34	41	47	52	57	61	65	69
250	10	29	39	47	54	60	65	70	75	79
300	19	33	44	53	60	67	73	78	83	88
350	28	38	49	58	66	73	80	86	91	97
400	37	46	55	64	72	80	87	93	99	105
450	46	54	62	70	78	86	93	100	106	112
500	56	63	71	78	85	93	100	106	113	119
550	65	72	79	86	93	100	107	114	120	126
600	75	82	88	95	102	109	115	122	128	134

表 6 各 $p(k,t)$ の最小上界値

Table 6 Minimum upper bounds for each $p(k,t)$

$k \diagdown t$	1	2	3	4	5	6	7	8	9	10
100	7	17	23	28	32	35	38	41	44	46
150	11	22	30	36	41	46	50	53	56	60
200	14	27	36	43	49	54	59	63	67	71
250	16	32	42	49	56	62	68	72	77	81
300	19	36	46	55	63	69	75	81	86	90
350	28	39	51	60	69	76	82	88	94	99
400	37	46	55	65	74	82	89	95	101	107
450	49	54	62	70	79	88	95	102	108	114
500	56	63	71	78	85	93	101	108	115	121
550	65	72	79	86	93	100	107	114	121	128
600	75	82	88	95	102	109	115	122	128	135

表 7 計測結果

Table 7 Results of the measurement

k	SPP の観測度数	SPSP の観測度数	$\Pr(H_0)$
100	3,000	0	6.0×10^{-11}
150	40,000	0	3.3×10^{-9}
200	300,000	0	1.1×10^{-8}
250	1,100,000	0	5.1×10^{-8}
300	9,000,000	0	3.5×10^{-8}

表 8 誤判定確率の上側信頼限界

Table 8 Upper confidence limit of error probability

SPP の観測度数	99%区間	95%区間	80%区間	67%区間
3,000	9.3	9.9	10.8	11.4
40,000	13.0	13.7	14.6	15.1
300,000	15.9	16.6	17.5	18.0
1,100,000	17.8	18.4	19.3	19.9
9,000,000	20.8	21.5	22.4	22.9

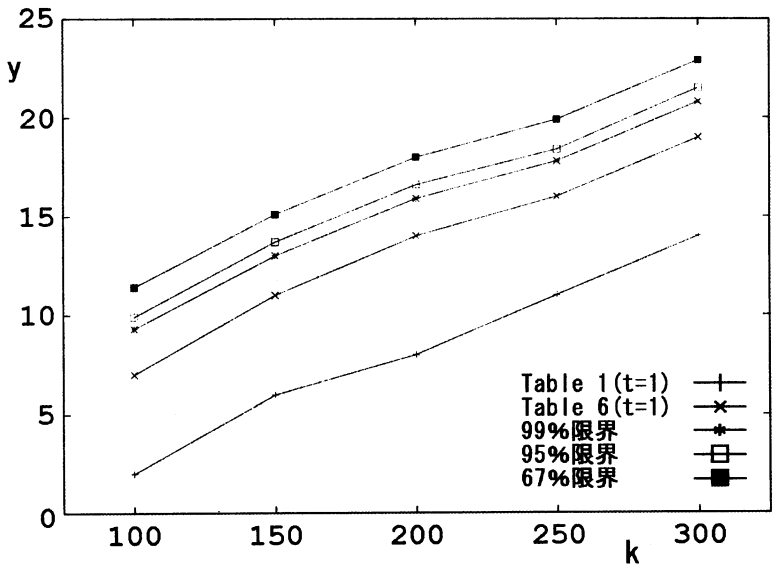

図1 理論と統計による上界

Fig. 1 Upper bounds with theory and statistics