合成数はどこまで素数に近づけるか

山田智宏（大阪大学）

March 21. 2021 / Apr 5. 2021 revised

Introduction

素数と合成数の違い

素数 1 と自分自身以外に約数をもたない

合成数 1 とも自分自身とも異なる約数をもつ

一見明らかな違いに思えるが…

Introduction

素数と合成数の違い

素数 1 と自分自身以外に約数をもたない

合成数 1 とも自分自身とも異なる約数をもつ

一見明らかな違いに思えるが…

したがって、1 より大きな整数 N が素数であるかどうか確かめるには、
$2, 3, \ldots, N-1$ の中に N の約数が存在するかどうか確かめればよい

しかし、$2, 3, \ldots, N-1$ をひとつひとつ確かめるのは非常に時間がかかる

したがって、1 より大きな整数 N が素数であるかどうか確かめるには、
$2, 3, \ldots, N-1$ の中に N の約数が存在するかどうか確かめればよい

しかし、$2, 3, \ldots, N-1$ をひとつひとつ確かめるのは非常に時間がかかる

N より小さい整数が N を割り切るかどうか確かめるにはどの程度の時間を要するか？

1 桁の足し算・引き算・比較・桁移動を 1 単位演算と考えると 2 つの数 $M, N (M < N)$ の引き算に必要な単位演算の回数は、N の桁数の定数倍以下
（コンピューターで計算する場合でも、2 進数で計算するだけで、基本的な方法は変わらない）

N の桁数は $\log N$ にほぼ比例するから、引き算に要する時間は $O(\log N)$

割り算は、引き算と桁移動を N の桁数以内の回数繰り返せば可能だから $O(\log^2 N)$ の演算で可能

実際には $O(\log N \log\log N \log\log\log N)$ で可能なことが知られている
（たとえば Hasselström, 2003）

N より小さい整数が N を割り切るかどうか確かめるにはどの程度の時間を要するか？

1 桁の足し算・引き算・比較・桁移動を 1 単位演算と考えると 2 つの数 $M, N (M < N)$ の引き算に必要な単位演算の回数は、N の桁数の定数倍以下
（コンピューターで計算する場合でも、2 進数で計算するだけで、基本的な方法は変わらない）

N の桁数は $\log N$ にほぼ比例するから、引き算に要する時間は $O(\log N)$

割り算は、引き算と桁移動を N の桁数以内の回数繰り返せば可能だから $O(\log^2 N)$ の演算で可能

実際には $O(\log N \log\log N \log\log\log N)$ で可能なことが知られている
（たとえば Hasselström, 2003）

N より小さい整数が N を割り切るかどうか確かめるにはどの程度の時間を要するか？

1 桁の足し算・引き算・比較・桁移動を 1 単位演算と考えると 2 つの数 $M, N (M < N)$ の引き算に必要な単位演算の回数は、N の桁数の定数倍以下
（コンピューターで計算する場合でも、2 進数で計算するだけで、基本的な方法は変わらない）

N の桁数は $\log N$ にほぼ比例するから、引き算に要する時間は $O(\log N)$

割り算は、引き算と桁移動を N の桁数以内の回数繰り返せば可能だから $O(\log^2 N)$ の演算で可能

実際には $O(\log N \log\log N \log\log\log N)$ で可能なことが知られている
（たとえば Hasselström, 2003）

N より小さい整数が N を割り切るかどうか確かめるにはどの程度の時間を要するか？

1 桁の足し算・引き算・比較・桁移動を 1 単位演算と考えると 2 つの数 $M, N (M < N)$ の引き算に必要な単位演算の回数は、N の桁数の定数倍以下
（コンピューターで計算する場合でも、2 進数で計算するだけで、基本的な方法は変わらない）

N の桁数は $\log N$ にほぼ比例するから、引き算に要する時間は $O(\log N)$

割り算は、引き算と桁移動を N の桁数以内の回数繰り返せば可能だから $O(\log^2 N)$ の演算で可能

実際には $O(\log N \log\log N \log\log\log N)$ で可能なことが知られている
（たとえば Hasselström, 2003）

よって、 $2, 3, \ldots, N-1$ をすべて確かめることは
$O(N \log N \log\log N \log\log\log N)$ 以内に可能

$N = m_1 m_2$ と、1 より大きな 2 つの整数の積であらわされるとき
$m_1 \leq \sqrt{N}$ または $m_2 \leq \sqrt{N}$ だから、実際には 2 以上 $\sqrt{N}$ 以下の整数をすべて確かめれば足りる

よって素数の確認（合成数の場合は、約数の発見）は
$O(\sqrt{N} \log N \log\log N \log\log\log N)$ 以内に可能

$\log N, \log\log N$ などは、どのような小さな正の ϵ をとっても N^{ϵ} より増加が遅いので N が素数かどうかの確認は $N^{1/2+o(1)}$ 以内に可能ともいえる

よって、 $2, 3, \ldots, N-1$ をすべて確かめることは
$O(N \log N \log\log N \log\log\log N)$ 以内に可能

$N = m_1 m_2$ と、1 より大きな 2 つの整数の積であらわされるとき
$m_1 \leq \sqrt{N}$ または $m_2 \leq \sqrt{N}$ だから、実際には 2 以上 $\sqrt{N}$ 以下の整数をすべて確かめれば足りる

よって素数の確認（合成数の場合は、約数の発見）は
$O(\sqrt{N} \log N \log\log N \log\log\log N)$ 以内に可能

$\log N, \log\log N$ などは、どのような小さな正の ϵ をとっても N^{ϵ} より増加が遅いので N が素数かどうかの確認は $N^{1/2+o(1)}$ 以内に可能ともいえる

単に約数を求めるよりやや強く、合成数を素因数分解する問題を考える

- 合成数の素因数分解を求められれば合成数の約数は求められる
- 逆に、合成数の約数を発見する方法があれば、それを素数にたどり着くまで繰り返すことで、素因数分解が得られる

単に約数を求めるよりやや強く、合成数を素因数分解する問題を考える

- 合成数の素因数分解を求められれば合成数の約数は求められる
- 逆に、合成数の約数を発見する方法があれば、それを素数にたどり着くまで繰り返すことで、素因数分解が得られる

素因数分解に要する時間は？

- Shanks, 1971: $N^{1/4+o(1)}$ 以内に可能
- Pollard, 1974 および Strassen, 1976: 拡張リーマン予想が正しければ $N^{1/5+o(1)}$ 以内に可能
- 数体ふるい法（Number Field Sieve, Crandall and Pomerance, 2005, Chapter 6 などを参照）：
  $\exp((C+o(1))\log^{1/3} N(\log\log N)^{2/3})$ 以内に可能と推測されている

最近、125 桁の素数 2 つの積を、もとの素数に分解する問題が解かれたが、のべ 2000 年以上を要した
(https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html)

やはり、合成数の約数を見つけるには時間がかかる！

素因数分解に要する時間は？

Shanks, 1971: $N^{1/4+o(1)}$ 以内に可能

Pollard, 1974 および Strassen, 1976: 拡張リーマン予想が正しければ $N^{1/5+o(1)}$ 以内に可能

数体ふるい法（Number Field Sieve, Crandall and Pomerance, 2005, Chapter 6 などを参照）：
$\exp((C+o(1))\log^{1/3} N(\log\log N)^{2/3})$ 以内に可能と推測されている

最近、125 桁の素数 2 つの積を、もとの素数に分解する問題が解かれたが、のべ 2000 年以上を要した
(https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html)

やはり、合成数の約数を見つけるには時間がかかる！

素因数分解に要する時間は？

Shanks, 1971: $N^{1/4+o(1)}$ 以内に可能

Pollard, 1974 および Strassen, 1976: 拡張リーマン予想が正しければ $N^{1/5+o(1)}$ 以内に可能

数体ふるい法（Number Field Sieve, Crandall and Pomerance, 2005, Chapter 6 などを参照）：
$\exp((C+o(1))\log^{1/3} N(\log\log N)^{2/3})$ 以内に可能と推測されている

最近、125 桁の素数 2 つの積を、もとの素数に分解する問題が解かれたが、のべ 2000 年以上を要した
(https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html)

やはり、合成数の約数を見つけるには時間がかかる！

素因数分解に要する時間は？

Shanks, 1971: $N^{1/4+o(1)}$ 以内に可能

Pollard, 1974 および Strassen, 1976: 拡張リーマン予想が正しければ $N^{1/5+o(1)}$ 以内に可能

数体ふるい法（Number Field Sieve, Crandall and Pomerance, 2005, Chapter 6 などを参照）：
$\exp((C+o(1))\log^{1/3} N(\log\log N)^{2/3})$ 以内に可能と推測されている

最近、125 桁の素数 2 つの積を、もとの素数に分解する問題が解かれたが、のべ 2000 年以上を要した
(https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html)

やはり、合成数の約数を見つけるには時間がかかる！

素因数分解に要する時間は？

Shanks, 1971: $N^{1/4+o(1)}$ 以内に可能

Pollard, 1974 および Strassen, 1976: 拡張リーマン予想が正しければ $N^{1/5+o(1)}$ 以内に可能

数体ふるい法（Number Field Sieve, Crandall and Pomerance, 2005, Chapter 6 などを参照）:
$\exp((C+o(1))\log^{1/3} N(\log\log N)^{2/3})$ 以内に可能と推測されている

最近、125 桁の素数 2 つの積を、もとの素数に分解する問題が解かれたが、のべ 2000 年以上を要した
(https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html)

やはり、合成数の約数を見つけるには時間がかかる！

一方、素数判定は $\log N$ の多項式と同程度の速さで増加する時間内に可能

- Agrawal, Kayal and Saxena, 2002-2004: $\log^{10.5+o(1)} N$ 以内に可能 （理論上 $\log^{7.5+o(1)} N$ でも可能だが、$o(1)$ 部分が具体的に計算できない）
- Lenstra and Pomerance 2005: $\log^{6+o(1)} N$ 以内に可能

300 桁程度の数でも素数か否かの判定は、1 分以内に可能 (PARI-GP 2.13.0, i5-6200U 2.3GHz, 2 core)

一方、素数判定は $\log N$ の多項式と同程度の速さで増加する時間内に可能

Agrawal, Kayal and Saxena, 2002-2004: $\log^{10.5+o(1)} N$ 以内に可能（理論上 $\log^{7.5+o(1)} N$ でも可能だが、$o(1)$ 部分が具体的に計算できない）

Lenstra and Pomerance 2005: $\log^{6+o(1)} N$ 以内に可能

300 桁程度の数でも素数か否かの判定は、1 分以内に可能 (PARI-GP 2.13.0, i5-6200U 2.3GHz, 2 core)

一方、素数判定は $\log N$ の多項式と同程度の速さで増加する時間内に可能

Agrawal, Kayal and Saxena, 2002-2004: $\log^{10.5+o(1)} N$ 以内に可能 （理論上 $\log^{7.5+o(1)} N$ でも可能だが、$o(1)$ 部分が具体的に計算できない）

Lenstra and Pomerance 2005: $\log^{6+o(1)} N$ 以内に可能

300 桁程度の数でも素数か否かの判定は、1 分以内に可能 (PARI-GP 2.13.0, i5-6200U 2.3GHz, 2 core)

一方、素数判定は $\log N$ の多項式と同程度の速さで増加する時間内に可能

Agrawal, Kayal and Saxena, 2002-2004: $\log^{10.5+o(1)} N$ 以内に可能 （理論上 $\log^{7.5+o(1)} N$ でも可能だが、$o(1)$ 部分が具体的に計算できない）

Lenstra and Pomerance 2005: $\log^{6+o(1)} N$ 以内に可能

300 桁程度の数でも素数か否かの判定は、1 分以内に可能 (PARI-GP 2.13.0, i5-6200U 2.3GHz, 2 core)

一方、素数判定は $\log N$ の多項式と同程度の速さで増加する時間内に可能

Agrawal, Kayal and Saxena, 2002-2004: $\log^{10.5+o(1)} N$ 以内に可能 （理論上 $\log^{7.5+o(1)} N$ でも可能だが、$o(1)$ 部分が具体的に計算できない）

Lenstra and Pomerance 2005: $\log^{6+o(1)} N$ 以内に可能

300 桁程度の数でも素数か否かの判定は、1 分以内に可能 (PARI-GP 2.13.0, i5-6200U 2.3GHz, 2 core)

一方、素数判定は $\log N$ の多項式と同程度の速さで増加する時間内に可能

Agrawal, Kayal and Saxena, 2002-2004: $\log^{10.5+o(1)} N$ 以内に可能 （理論上 $\log^{7.5+o(1)} N$ でも可能だが、$o(1)$ 部分が具体的に計算できない）

Lenstra and Pomerance 2005: $\log^{6+o(1)} N$ 以内に可能

300 桁程度の数でも素数か否かの判定は、1 分以内に可能 (PARI-GP 2.13.0, i5-6200U 2.3GHz, 2 core)

素数判定は比較的容易だが、素因数分解が今のところ困難であることは、RSA 暗号に利用される

なお、量子コンピューターを用いれば、素因数分解は $O(\log^2 N \log\log N \log\log\log N)$ 以内に可能 (Shor, 1994)

ただし、量子コンピューターはまだ巨大な数を扱えるところまでは実用化されていない

なお、通常のコンピューターで高速に素因数分解する方法を発見したという報告が最近あったが、正しいと確認されておらず、疑いの声も出ている

素数判定は比較的容易だが、素因数分解が今のところ困難であることは、RSA 暗号に利用される

なお、量子コンピューターを用いれば、素因数分解は
$O(\log^2 N \log\log N \log\log\log N)$ 以内に可能 (Shor, 1994)

ただし、量子コンピューターはまだ巨大な数を扱えるところまでは実用化されていない

なお、通常のコンピューターで高速に素因数分解する方法を発見したという報告が最近あったが、正しいと確認されておらず、疑いの声も出ている

Pseudoprimes

これはどういうことか？

素因数分解をせずに素数かどうかを確かめる方法は存在する！

素数判定や素因数分解の方法についての詳細は Crandall and Pomerance, 2005 などを参照

Pseudoprimes

これはどういうことか？

素因数分解をせずに素数かどうかを確かめる方法は存在する！

素数判定や素因数分解の方法についての詳細は Crandall and Pomerance, 2005 などを参照

Pseudoprimes

これはどういうことか？

素因数分解をせずに素数かどうかを確かめる方法は存在する！

素数判定や素因数分解の方法についての詳細は Crandall and Pomerance, 2005 などを参照

有名な例としては

Wilson の定理 (e.x. Hardy-Wright, Theorem 81)

N が素数 $\Leftrightarrow (N-1)! \equiv -1 \pmod{N}$

$N \geq 5$ が素数、$2 \leq a \leq N-2$ のとき $ab \equiv 1 \pmod{N}$ となる b がとれる、このようにペア (a, b) をとっていくと ± 1 だけ残るから、
$(N-1)! \equiv 1 \times (-1) \equiv -1 \pmod{N}$

なお、N が 4 より大きな合成数の場合 $(N-1)!$ は N の倍数で、$N = 4$ のときは $3! = 6 \equiv 2 \pmod{4}$

しかし、階乗の計算は非常に時間がかかる（管見の限り $O(N)$ より速い方法は見当たらない）ため、現実的ではない！

有名な例としては

Wilson の定理 (e.x. Hardy-Wright, Theorem 81)

N が素数 $\Leftrightarrow (N-1)! \equiv -1 \pmod{N}$

$N \geq 5$ が素数、$2 \leq a \leq N-2$ のとき $ab \equiv 1 \pmod{N}$ となる b がとれる、このようにペア (a, b) をとっていくと ± 1 だけ残るから、
$(N-1)! \equiv 1 \times (-1) \equiv -1 \pmod{N}$

なお、N が 4 より大きな合成数の場合 $(N-1)!$ は N の倍数で、$N = 4$ のときは $3! = 6 \equiv 2 \pmod{4}$

しかし、階乗の計算は非常に時間がかかる（管見の限り $O(N)$ より速い方法は見当たらない）ため、現実的ではない！

有名な例としては

Wilson の定理 (e.x. Hardy-Wright, Theorem 81)

N が素数 $\Leftrightarrow (N-1)! \equiv -1 \pmod{N}$

$N \geq 5$ が素数、$2 \leq a \leq N-2$ のとき $ab \equiv 1 \pmod{N}$ となる b がとれる、このようにペア (a, b) をとっていくと ± 1 だけ残るから、
$(N-1)! \equiv 1 \times (-1) \equiv -1 \pmod{N}$

なお、 N が 4 より大きな合成数の場合 $(N-1)!$ は N の倍数で、$N = 4$ のときは $3! = 6 \equiv 2 \pmod{4}$

しかし、階乗の計算は非常に時間がかかる（管見の限り $O(N)$ より速い方法は見当たらない）ため、現実的ではない！

一方、

Fermat の小定理

p が素数で a が p で割り切れなければ $a^{p-1} \equiv 1 \pmod{p}$

しかし、この逆は一般には成り立たない！

たとえば $2^{340} \equiv 1 \pmod{341}$ だが $341 = 11 \times 31$ は合成数

このように、素数ではないが、Fermat の小定理にあらわれる合同式が成り立ってしまう場合が存在する

擬素数

N が a を底とする擬素数 (pseudoprime): N が合成数で $\gcd(a, N) = 1$ だが $a^{N-1} \equiv 1 \pmod{N}$

2 を底とする擬素数: $341, 561, 645, 1105, 1387, 1729, 1905, 2047 \ldots$ (OEIS A001567)

これらの数については $2^{N-1} \equiv 1 \pmod{N}$ が成り立つので、これだけでは素数と見分けがつかない

しかし、この逆は一般には成り立たない！

たとえば $2^{340} \equiv 1 \pmod{341}$ だが $341 = 11 \times 31$ は合成数

このように、素数ではないが、Fermat の小定理にあらわれる合同式が成り立ってしまう場合が存在する

擬素数

N が a を底とする擬素数 (pseudoprime): N が合成数で $\gcd(a, N) = 1$ だが $a^{N-1} \equiv 1 \pmod{N}$

2 を底とする擬素数: $341, 561, 645, 1105, 1387, 1729, 1905, 2047 \ldots$ (OEIS A001567)

これらの数については $2^{N-1} \equiv 1 \pmod{N}$ が成り立つので、これだけでは素数と見分けがつかない

しかし、この逆は一般には成り立たない！

たとえば $2^{340} \equiv 1 \pmod{341}$ だが $341 = 11 \times 31$ は合成数

このように、素数ではないが、Fermat の小定理にあらわれる合同式が成り立ってしまう場合が存在する

擬素数

N が a を底とする擬素数 (pseudoprime): N が合成数で $\gcd(a, N) = 1$ だが $a^{N-1} \equiv 1 \pmod{N}$

2 を底とする擬素数: $341, 561, 645, 1105, 1387, 1729, 1905, 2047 \ldots$ (OEIS A001567)

これらの数については $2^{N-1} \equiv 1 \pmod{N}$ が成り立つので、これだけでは素数と見分けがつかない

$a \equiv 1 \pmod{N}$ ならば $a^{N-1} \equiv 1 \pmod{N}$ だから、N が擬素数となる底 a は確かに存在する

一方で、与えられた底 a に対して、$a-1$ の約数のような自明なもの以外の擬素数を見つけるのは難しい

Pomerance, 1981: x が大きい時 x 以下の、与えられた底 a に対する擬素数の個数は $x^{1-\log\log\log x/(2\log\log x)}$ より小さい

素数定理より x 以下の素数の個数は $x/\log x$ で近似できるから、擬素数は素数よりずっと少ない

その点で、Fermat の小定理における合同式はほぼ素数固有の性質ということができる

したがって、その性質を素数と共有する擬素数は素数に近い性質をもっている

$a \equiv 1 \pmod{N}$ ならば $a^{N-1} \equiv 1 \pmod{N}$ だから、N が擬素数となる底 a は確かに存在する

一方で、与えられた底 a に対して、$a-1$ の約数のような自明なもの以外の擬素数を見つけるのは難しい

Pomerance, 1981: x が大きい時 x 以下の、与えられた底 a に対する擬素数の個数は $x^{1-\log\log\log x/(2\log\log x)}$ より小さい

素数定理より x 以下の素数の個数は $x/\log x$ で近似できるから、擬素数は素数よりずっと少ない

その点で、Fermat の小定理における合同式はほぼ素数固有の性質ということができる

したがって、その性質を素数と共有する擬素数は素数に近い性質をもっている

$a \equiv 1 \pmod{N}$ ならば $a^{N-1} \equiv 1 \pmod{N}$ だから、N が擬素数となる底 a は確かに存在する

一方で、与えられた底 a に対して、$a-1$ の約数のような自明なもの以外の擬素数を見つけるのは難しい

Pomerance, 1981: x が大きい時 x 以下の、与えられた底 a に対する擬素数の個数は $x^{1-\log\log\log x/(2\log\log x)}$ より小さい

素数定理より x 以下の素数の個数は $x/\log x$ で近似できるから、擬素数は素数よりずっと少ない

その点で、Fermat の小定理における合同式はほぼ素数固有の性質ということができる

したがって、その性質を素数と共有する擬素数は素数に近い性質をもっている

さらに、a が $3, 11, 17$ のいずれでも割り切れないとき $a^{560} \equiv 1 \pmod{561}$ が成り立つ

実際、a が $3, 11, 17$ のいずれでも割り切れないとき $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$

560 は $2, 10, 16$ の公倍数だから $a^{560} \equiv 1 \pmod{3}$, $a^{560} \equiv 1 \pmod{11}$, $a^{560} \equiv 1 \pmod{17}$ より $a^{560} \equiv 1 \pmod{561}$ となる

このように $\gcd(a, N) = 1$ のとき必ず $a^{N-1} \equiv 1 \pmod{N}$ が成り立つような合成数 N （Carmichael 数）が存在する！

さらに、a が $3, 11, 17$ のいずれでも割り切れないとき $a^{560} \equiv 1 \pmod{561}$ が成り立つ

実際、a が $3, 11, 17$ のいずれでも割り切れないとき $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$

560 は $2, 10, 16$ の公倍数だから $a^{560} \equiv 1 \pmod{3}$, $a^{560} \equiv 1 \pmod{11}$, $a^{560} \equiv 1 \pmod{17}$ より $a^{560} \equiv 1 \pmod{561}$ となる

このように $\gcd(a, N) = 1$ のとき必ず $a^{N-1} \equiv 1 \pmod{N}$ が成り立つような合成数 N（Carmichael 数）が存在する！

さらに、a が $3, 11, 17$ のいずれでも割り切れないとき $a^{560} \equiv 1 \pmod{561}$ が成り立つ

実際、a が $3, 11, 17$ のいずれでも割り切れないとき $a^2 \equiv 1 \pmod{3}$, $a^{10} \equiv 1 \pmod{11}$, $a^{16} \equiv 1 \pmod{17}$

560 は $2, 10, 16$ の公倍数だから $a^{560} \equiv 1 \pmod{3}$, $a^{560} \equiv 1 \pmod{11}$, $a^{560} \equiv 1 \pmod{17}$ より $a^{560} \equiv 1 \pmod{561}$ となる

このように $\gcd(a, N) = 1$ のとき必ず $a^{N-1} \equiv 1 \pmod{N}$ が成り立つような合成数 N （Carmichael 数）が存在する！

Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめようとしても、a が N と公約数をもたない限り、合成数とはわからない

a が N と公約数をもっていれば、$\gcd(a, N)$ を求めることで N の約数も見つかるから、Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめるのは、N の約数を見つけるのとほぼ同等に難しいといえる（最大公約数は Euclid の互除法をつかって、比較的容易に求められる）

では、Carmichael 数をどのようにして見つけるか？

Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめようとしても、a が N と公約数をもたない限り、合成数とはわからない

a が N と公約数をもっていれば、$\gcd(a, N)$ を求めることで N の約数も見つかるから、Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめるのは、N の約数を見つけるのとほぼ同等に難しいといえる（最大公約数は Euclid の互除法をつかって、比較的容易に求められる）

では、Carmichael 数をどのようにして見つけるか？

Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめようとしても、a が N と公約数をもたない限り、合成数とはわからない

a が N と公約数をもっていれば、$\gcd(a, N)$ を求めることで N の約数も見つかるから、Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめるのは、N の約数を見つけるのとほぼ同等に難しいといえる（最大公約数は Euclid の互除法をつかって、比較的容易に求められる）

では、Carmichael 数をどのようにして見つけるか？

Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめようとしても、a が N と公約数をもたない限り、合成数とはわからない

a が N と公約数をもっていれば、$\gcd(a, N)$ を求めることで N の約数も見つかるから、Carmichael 数を $a^{N-1} \equiv 1 \pmod{N}$ の形の合同式で素数か合成数か確かめるのは、N の約数を見つけるのとほぼ同等に難しいといえる（最大公約数は Euclid の互除法をつかって、比較的容易に求められる）

では、Carmichael 数をどのようにして見つけるか？

$\varphi(N)$ を $1, 2, \ldots, N-1$ のなかで N と互に素な整数の個数とする

p が素数のときは p^e と互に素とは、 p で割り切れないことと同値だから
$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

より一般に $N = \prod_{i=1}^{r} p_i^{e_i}$ ならば $\varphi(N) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$

$\varphi(N)$ を $1, 2, \ldots, N-1$ のなかで N と互に素な整数の個数とする

p が素数のときは p^e と互に素とは、 p で割り切れないことと同値だから
$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

より一般に $N = \prod_{i=1}^{r} p_i^{e_i}$ ならば $\varphi(N) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$

$\varphi(N)$ を $1, 2, \ldots, N-1$ のなかで N と互に素な整数の個数とする

p が素数のときは p^e と互に素とは、 p で割り切れないことと同値だから
$\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1)$

より一般に $N = \prod_{i=1}^{r} p_i^{e_i}$ ならば $\varphi(N) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$

実際、このとき $a(0 \leq a \leq N-1)$ を各 $p_i^{e_i}$ で割った余りを a_i とおくと

(a) 各 $i = 1, \ldots, r$ について $0 \leq a_i \leq p_i^{e_i} - 1$

(b) $\gcd(a, N) = 1 \Leftrightarrow a$ は いずれの p_i でも割り切れない $\Leftrightarrow$ 各 i について a_i は p_i で割り切れない

(c) $0 \leq a_i \leq p_i^{e_i} - 1$ となる r-組 $(a_1, \ldots, a_r)$ を決定すれば a が定まり、かつ、異なる r-組には異なる a が対応する

(a)(b) から、 a_i の可能な選択は $p_i^{e_i - 1}(p_i - 1)$ 通りであり、(c) から a の可能性は $\prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$ 通り

実際、このとき $a(0 \leq a \leq N-1)$ を各 $p_i^{e_i}$ で割った余りを a_i とおくと

(a) 各 $i = 1, \ldots, r$ について $0 \leq a_i \leq p_i^{e_i} - 1$

(b) $\gcd(a, N) = 1 \Leftrightarrow a$ は いずれの p_i でも割り切れない $\Leftrightarrow$ 各 i について a_i は p_i で割り切れない

(c) $0 \leq a_i \leq p_i^{e_i} - 1$ となる r-組 $(a_1, \ldots, a_r)$ を決定すれば a が定まり、かつ、異なる r-組には異なる a が対応する

(a)(b) から、 a_i の可能な選択は $p_i^{e_i-1}(p_i - 1)$ 通りであり、(c) から a の可能性は $\prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$ 通り

実際、このとき $a(0 \leq a \leq N-1)$ を各 $p_i^{e_i}$ で割った余りを a_i とおくと

(a) 各 $i = 1, \ldots, r$ について $0 \leq a_i \leq p_i^{e_i} - 1$

(b) $\gcd(a, N) = 1 \Leftrightarrow a$ は いずれの p_i でも割り切れない $\Leftrightarrow$ 各 i について a_i は p_i で割り切れない

(c) $0 \leq a_i \leq p_i^{e_i} - 1$ となる r-組 $(a_1, \ldots, a_r)$ を決定すれば a が定まり、かつ、異なる r-組には異なる a が対応する

(a)(b) から、a_i の可能な選択は $p_i^{e_i-1}(p_i - 1)$ 通りであり、(c) から a の可能性は $\prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$ 通り

実際、このとき $a(0 \leq a \leq N-1)$ を各 $p_i^{e_i}$ で割った余りを a_i とおくと

(a) 各 $i = 1, \ldots, r$ について $0 \leq a_i \leq p_i^{e_i} - 1$

(b) $\gcd(a, N) = 1 \Leftrightarrow a$ は いずれの p_i でも割り切れない $\Leftrightarrow$ 各 i について a_i は p_i で割り切れない

(c) $0 \leq a_i \leq p_i^{e_i} - 1$ となる r-組 $(a_1, \ldots, a_r)$ を決定すれば a が定まり、かつ、異なる r-組には異なる a が対応する

(a)(b) から、 a_i の可能な選択は $p_i^{e_i-1}(p_i - 1)$ 通りであり、(c) から a の可能性は $\prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1)$ 通り

特に $\varphi(N) \leq N-1$ **で** N **が素数** $\Leftrightarrow \varphi(N) = N-1$

さらに、Fermat の小定理より一般的な定理が成り立つ！

Fermat-Euler の定理

$\gcd(a, N) = 1$ **ならば** $a^{\varphi(N)} \equiv 1 \pmod{N}$

特に $\varphi(N) \leq N-1$ で N が素数 $\Leftrightarrow \varphi(N) = N-1$

さらに、Fermat の小定理より一般的な定理が成り立つ！

Fermat-Euler の定理

$\gcd(a, N) = 1$ ならば $a^{\varphi(N)} \equiv 1 \pmod{N}$

実際 $1, 2, \ldots, N-1$ のなかで N と互に素な整数全体を $s_1, s_2, \ldots, s_{\varphi(N)}$ とし、as_i を N で割った余りを t_i とおくと

t_i も N と互に素で、$1 \leq t_i \leq N-1$

$t_i = t_j$ ならば $as_i \equiv as_j \pmod{N}$ より $s_i \equiv s_j \pmod{N}$ つまり

$s_i = s_j$

だから $t_1, t_2, \ldots, t_{\varphi(N)}$ は $1, 2, \ldots, N-1$ のなかで N と互に素な整数を 1 回ずつとる

よって $\prod_i t_i = \prod_i s_i$ となり

$$a^{\varphi(N)} \prod_i s_i = \prod_i (as_i) \equiv \prod_i t_i = \prod_i s_i \pmod{N}$$

だが各 s_i は N と互に素だから $\prod_i s_i$ も N と互に素なので

$a^{\varphi(N)} \equiv 1 \pmod{N}$

実際 $1, 2, \ldots, N-1$ のなかで N と互に素な整数全体を $s_1, s_2, \ldots, s_{\varphi(N)}$ とし、as_i を N で割った余りを t_i とおくと

t_i も N と互に素で、 $1 \leq t_i \leq N-1$

$t_i = t_j$ ならば $as_i \equiv as_j \pmod{N}$ より $s_i \equiv s_j \pmod{N}$ つまり

$s_i = s_j$

だから $t_1, t_2, \ldots, t_{\varphi(N)}$ は $1, 2, \ldots, N-1$ のなかで N と互に素な整数を 1 回ずつとる

よって $\prod_i t_i = \prod_i s_i$ となり

$$a^{\varphi(N)} \prod_i s_i = \prod_i (as_i) \equiv \prod_i t_i = \prod_i s_i \pmod{N}$$

だが各 s_i は N と互に素だから $\prod_i s_i$ も N と互に素なので

$a^{\varphi(N)} \equiv 1 \pmod{N}$

実際 $1, 2, \ldots, N-1$ のなかで N と互に素な整数全体を $s_1, s_2, \ldots, s_{\varphi(N)}$ とし、as_i を N で割った余りを t_i とおくと

t_i も N と互に素で、 $1 \leq t_i \leq N-1$

$t_i = t_j$ ならば $as_i \equiv as_j \pmod{N}$ より $s_i \equiv s_j \pmod{N}$ つまり

$s_i = s_j$

だから $t_1, t_2, \ldots, t_{\varphi(N)}$ は $1, 2, \ldots, N-1$ のなかで N と互に素な整数を 1 回ずつとる

よって $\prod_i t_i = \prod_i s_i$ となり

$$a^{\varphi(N)} \prod_i s_i = \prod_i (as_i) \equiv \prod_i t_i = \prod_i s_i \pmod{N}$$

だが各 s_i は N と互に素だから $\prod_i s_i$ も N と互に素なので

$a^{\varphi(N)} \equiv 1 \pmod{N}$

実際 $1, 2, \ldots, N-1$ のなかで N と互に素な整数全体を $s_1, s_2, \ldots, s_{\varphi(N)}$ とし、as_i を N で割った余りを t_i とおくと

t_i も N と互に素で、 $1 \leq t_i \leq N-1$

$t_i = t_j$ ならば $as_i \equiv as_j \pmod{N}$ より $s_i \equiv s_j \pmod{N}$ つまり

$s_i = s_j$

だから $t_1, t_2, \ldots, t_{\varphi(N)}$ は $1, 2, \ldots, N-1$ のなかで N と互に素な整数を 1 回ずつとる

よって $\prod_i t_i = \prod_i s_i$ となり

$$a^{\varphi(N)} \prod_i s_i = \prod_i (as_i) \equiv \prod_i t_i = \prod_i s_i \pmod{N}$$

だが各 s_i は N と互に素だから $\prod_i s_i$ も N と互に素なので

$a^{\varphi(N)} \equiv 1 \pmod{N}$

実際 $1, 2, \ldots, N-1$ のなかで N と互に素な整数全体を $s_1, s_2, \ldots, s_{\varphi(N)}$ とし、as_i を N で割った余りを t_i とおくと

t_i も N と互に素で、 $1 \leq t_i \leq N-1$

$t_i = t_j$ ならば $as_i \equiv as_j \pmod{N}$ より $s_i \equiv s_j \pmod{N}$ つまり

$s_i = s_j$

だから $t_1, t_2, \ldots, t_{\varphi(N)}$ は $1, 2, \ldots, N-1$ のなかで N と互に素な整数を 1 回ずつとる

よって $\prod_i t_i = \prod_i s_i$ となり

$$a^{\varphi(N)} \prod_i s_i = \prod_i (as_i) \equiv \prod_i t_i = \prod_i s_i \pmod{N}$$

だが各 s_i は N と互に素だから $\prod_i s_i$ も N と互に素なので
$a^{\varphi(N)} \equiv 1 \pmod{N}$

さらに、Carmichael 関数 $\lambda(N)$ を次のように定める

Carmichael 関数

- p が素数のとき、$p = 2, e \geq 3$ のときを除いて $\lambda(p^e) = p^{e-1}(p-1)$ とし $e \geq 3$ のときは $\lambda(2^e) = 2^{e-2}$ とする
- 一般的には $N = \prod_{i=1}^{r} p_i^{e_i}$ に対して $\lambda(N)$ を各 $\lambda(p_i^{e_i})$ の最小公倍数とする

このとき Fermat の小定理の一般化として $\gcd(a, N) = 1$ ならば $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

また、やはり N が素数 $\Leftrightarrow \lambda(N) = N - 1$

実際、先に考察した 561 の例のように、各 i に対して、$a^{\lambda(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$（$p_i$ が奇数のときは Euler の定理からすぐにわかる、$p_i = 2$ のときは演習問題）だから $a^{\lambda(N)} \equiv 1 \pmod{p_i^{e_i}}$ も各 i に対して成り立つので、結局 $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

さらに、Carmichael 関数 $\lambda(N)$ を次のように定める

Carmichael 関数

- p が素数のとき、$p = 2, e \geq 3$ のときを除いて $\lambda(p^e) = p^{e-1}(p-1)$ とし $e \geq 3$ のときは $\lambda(2^e) = 2^{e-2}$ とする
- 一般的には $N = \prod_{i=1}^{r} p_i^{e_i}$ に対して $\lambda(N)$ を各 $\lambda(p_i^{e_i})$ の最小公倍数とする

このとき Fermat の小定理の一般化として $\gcd(a, N) = 1$ ならば $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

また、やはり N が素数 $\Leftrightarrow \lambda(N) = N - 1$

実際、先に考察した 561 の例のように、各 i に対して、$a^{\lambda(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$（$p_i$ が奇数のときは Euler の定理からすぐにわかる、$p_i = 2$ のときは演習問題）だから $a^{\lambda(N)} \equiv 1 \pmod{p_i^{e_i}}$ も各 i に対して成り立つので、結局 $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

さらに、Carmichael 関数 $\lambda(N)$ を次のように定める

Carmichael 関数

- p が素数のとき、$p = 2, e \geq 3$ のときを除いて $\lambda(p^e) = p^{e-1}(p-1)$ とし $e \geq 3$ のときは $\lambda(2^e) = 2^{e-2}$ とする
- 一般的には $N = \prod_{i=1}^{r} p_i^{e_i}$ に対して $\lambda(N)$ を各 $\lambda(p_i^{e_i})$ の最小公倍数とする

このとき Fermat の小定理の一般化として $\gcd(a, N) = 1$ ならば $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

また、やはり N が素数 $\Leftrightarrow \lambda(N) = N - 1$

実際、先に考察した 561 の例のように、各 i に対して、$a^{\lambda(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$（$p_i$ が奇数のときは Euler の定理からすぐにわかる、$p_i = 2$ のときは演習問題）だから $a^{\lambda(N)} \equiv 1 \pmod{p_i^{e_i}}$ も各 i に対して成り立つので、結局 $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

さらに、Carmichael 関数 $\lambda(N)$ を次のように定める

Carmichael 関数

- p が素数のとき、$p = 2, e \geq 3$ のときを除いて $\lambda(p^e) = p^{e-1}(p-1)$ とし $e \geq 3$ のときは $\lambda(2^e) = 2^{e-2}$ とする
- 一般的には $N = \prod_{i=1}^{r} p_i^{e_i}$ に対して $\lambda(N)$ を各 $\lambda(p_i^{e_i})$ の最小公倍数とする

このとき Fermat の小定理の一般化として $\gcd(a, N) = 1$ ならば $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

また、やはり N が素数 $\Leftrightarrow \lambda(N) = N - 1$

実際、先に考察した 561 の例のように、各 i に対して、$a^{\lambda(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$ （p_i が奇数のときは Euler の定理からすぐにわかる、$p_i = 2$ のときは演習問題） だから $a^{\lambda(N)} \equiv 1 \pmod{p_i^{e_i}}$ も各 i に対して成り立つので、結局 $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

さらに、Carmichael 関数 $\lambda(N)$ を次のように定める

Carmichael 関数

- p が素数のとき、$p = 2, e \geq 3$ のときを除いて $\lambda(p^e) = p^{e-1}(p-1)$ とし $e \geq 3$ のときは $\lambda(2^e) = 2^{e-2}$ とする
- 一般的には $N = \prod_{i=1}^{r} p_i^{e_i}$ に対して $\lambda(N)$ を各 $\lambda(p_i^{e_i})$ の最小公倍数とする

このとき Fermat の小定理の一般化として $\gcd(a, N) = 1$ ならば $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

また、やはり N が素数 $\Leftrightarrow \lambda(N) = N - 1$

実際、先に考察した 561 の例のように、各 i に対して、$a^{\lambda(p_i^{e_i})} \equiv 1 \pmod{p_i^{e_i}}$ （p_i が奇数のときは Euler の定理からすぐにわかる、$p_i = 2$ のときは演習問題） だから $a^{\lambda(N)} \equiv 1 \pmod{p_i^{e_i}}$ も各 i に対して成り立つので、結局 $a^{\lambda(N)} \equiv 1 \pmod{N}$ が成り立つ

$\lambda(N)$ が $N-1$ の約数ならば、先に考察した 561 の例と同様にして、$\gcd(a,N)=1$ となる a に対しては $a^{N-1}\equiv 1 \pmod{N}$ がつねに成り立ち、N は Carmichael 数となることがわかる！

最初の数個の Carmichael 数は $561, 1105, 1729, 2465, 2821, 6601, \ldots$
OEIS A002997

$\lambda(N)$ が $N-1$ の約数ならば、先に考察した 561 の例と同様にして、$\gcd(a,N)=1$ となる a に対しては $a^{N-1}\equiv 1 \pmod{N}$ がつねに成り立ち、N は Carmichael 数となることがわかる！

最初の数個の Carmichael 数は $561, 1105, 1729, 2465, 2821, 6601, \ldots$
OEIS A002997

$N > 2$ と $\lambda(N)$ が互に素ならば N は奇数で平方因子をもたない、また p が N の素因数のとき N は $ap + 1$ の形の素因数をもたない

(a) N が 2 より大きな偶数ならば 4 または奇素数で割り切れ、$\lambda(N)$ も偶数となる

(b) N が p^2 で割り切れると $\lambda(N)$ は p で割り切れるので N と $\lambda(N)$ はともに p で割り切れる

(c) $p, ap + 1$ がともに素数で N が $p, ap + 1$ で割り切れると $\lambda(N)$ は $(ap + 1) - 1 = ap$ で割り切れるから、 N と $\lambda(N)$ はともに p で割り切れる

よって、Carmichael 数も奇数で平方因子をもたず、また $p, ap + 1$ がともに素数ならば Carmichael 数は、$p, ap + 1$ で同時に割り切れない

$N > 2$ と $\lambda(N)$ が互に素ならば N は奇数で平方因子をもたない、また p が N の素因数のとき N は $ap + 1$ の形の素因数をもたない

(a) N が 2 より大きな偶数ならば 4 または奇素数で割り切れ、$\lambda(N)$ も偶数となる

(b) N が p^2 で割り切れると $\lambda(N)$ は p で割り切れるので N と $\lambda(N)$ はともに p で割り切れる

(c) $p, ap + 1$ がともに素数で N が $p, ap + 1$ で割り切れると $\lambda(N)$ は $(ap + 1) - 1 = ap$ で割り切れるから、 N と $\lambda(N)$ はともに p で割り切れる

よって、Carmichael 数も奇数で平方因子をもたず、また $p, ap + 1$ がともに素数ならば Carmichael 数は、$p, ap + 1$ で同時に割り切れない

Adleman, Pomerance, and Granville, 1994

x が大きいとき x 以下の整数 N で、$\lambda(N)$ が $N-1$ の約数となるようなもの（先述のとおり Carmichael 数となる）の個数は $x^{2/7}$ より大きい（$2/7$ は $5(1-1/(2\sqrt{e}))/12 = 0.290306\cdots$ より小さな任意の数に置換可能）

一方、Carmichael 数は素数よりもずっと少ないことが知られている

Pomerance, 1981

x が大きいとき x 以下の Carmichael 数の個数は $x^{1-\log\log\log x/\log\log x}$ より小さい

Adleman, Pomerance, and Granville, 1994

x が大きいとき x 以下の整数 N で、$\lambda(N)$ が $N-1$ の約数となるようなもの（先述のとおり Carmichael 数となる）の個数は $x^{2/7}$ より大きい（$2/7$ は $5(1-1/(2\sqrt{e}))/12 = 0.290306\cdots$ より小さな任意の数に置換可能）

一方、Carmichael 数は素数よりもずっと少ないことが知られている

Pomerance, 1981

x が大きいとき x 以下の Carmichael 数の個数は $x^{1-\log\log\log x/\log\log x}$ より小さい

ところで…

$\lambda(N)$ は $\varphi(N)$ の約数であるが、では N が合成数だが $\varphi(N)$ が $N-1$ の約数となることはあるか？（もちろんその場合 $\lambda(N)$ も $N-1$ の約数だから N は Carmichael 数となる）

そのような合成数は存在しないと予想されている (Lehmer, 1932) が、未だ解決されていない（後述）！

ところで…

$\lambda(N)$ は $\varphi(N)$ の約数であるが、では N が合成数だが $\varphi(N)$ が $N-1$ の約数となることはあるか？（もちろんその場合 $\lambda(N)$ も $N-1$ の約数だから N は Carmichael 数となる）

そのような合成数は存在しないと予想されている (Lehmer, 1932) が、未だ解決されていない（後述）！

Miller-Rabin test

Fermat の小定理に関する考察から、次の問題が生じる

Proposition

Carmichael 数を合成数と見破るにはどうすればよいか？

そこで、Fermat の小定理を少し変形した合同式と、やはりその合同式を成立させてしまう合成数について考える

Miller-Rabin test

Fermat の小定理に関する考察から、次の問題が生じる

Proposition

Carmichael 数を合成数と見破るにはどうすればよいか？

そこで、Fermat の小定理を少し変形した合同式と、やはりその合同式を成立させてしまう合成数について考える

Miller-Rabin test

Fermat の小定理に関する考察から、次の問題が生じる

Proposition

Carmichael 数を合成数と見破るにはどうすればよいか？

そこで、Fermat の小定理を少し変形した合同式と、やはりその合同式を成立させてしまう合成数について考える

Fermat の小定理から、次のことがわかる:

Proposition

$N-1=2^s t$ となる整数 $s \geq 0$ と奇数 t をとる
N が素数で a が N で割り切れなければ、次のどちらかが成り立つ:

(a) $a^t \equiv 1 \pmod{N}$,

(b) $a^{2^k t} \equiv -1 \pmod{N}$ となる k が存在する

実際 $a^{2^s t} \equiv 1 \pmod{N}$ であるから $a^{2^\ell t} \equiv 1 \pmod{N}$ となる最小の整数 $\ell \geq 0$ がとれる
$\ell = 0$ のとき (a) が成り立ち、$\ell > 0$ のとき $k = \ell - 1$ について (b) が成り立つ

Fermat の小定理から、次のことがわかる:

Proposition

$N-1=2^s t$ となる整数 $s \geq 0$ と奇数 t をとる
N が素数で a が N で割り切れなければ、次のどちらかが成り立つ:

(a) $a^t \equiv 1 \pmod{N}$,

(b) $a^{2^k t} \equiv -1 \pmod{N}$ となる k が存在する

実際 $a^{2^s t} \equiv 1 \pmod{N}$ であるから $a^{2^\ell t} \equiv 1 \pmod{N}$ となる最小の整数 $\ell \geq 0$ がとれる
$\ell = 0$ のとき (a) が成り立ち、$\ell > 0$ のとき $k = \ell - 1$ について (b) が成り立つ

Fermat の小定理から、次のことがわかる:

Proposition

$N-1=2^s t$ となる整数 $s \geq 0$ と奇数 t をとる
N が素数で a が N で割り切れなければ、次のどちらかが成り立つ:

(a) $a^t \equiv 1 \pmod{N}$,

(b) $a^{2^k t} \equiv -1 \pmod{N}$ となる k が存在する

実際 $a^{2^s t} \equiv 1 \pmod{N}$ であるから $a^{2^\ell t} \equiv 1 \pmod{N}$ となる最小の整数 $\ell \geq 0$ がとれる
$\ell = 0$ のとき (a) が成り立ち、$\ell > 0$ のとき $k = \ell - 1$ について (b) が成り立つ

例

$N = 561$ のとき

$$2^{140} \equiv 67 \pmod{561}, 2^{280} \equiv 1 \pmod{561}$$

なので、(a), (b) のいずれも成り立たない、このことは 561 が合成数であることを示している（前者は

$$2^{140} \equiv 1 \pmod{3}, 2^{140} \equiv 1 \pmod{11}, 2^{140} \equiv 2^4 \equiv 16 \pmod{17}$$

から手計算で確かめられる）

つまり、561 は単純な Fermat の小定理の合同式はすり抜けてしまうが、(a)(b) で合成数であることがわかってしまう

(a), (b) のいずれも成り立たない数 a は N が合成数であることの証人 (witness) といえる

例

$N = 561$ のとき

$$2^{140} \equiv 67 \pmod{561}, 2^{280} \equiv 1 \pmod{561}$$

なので、(a), (b) のいずれも成り立たない、このことは 561 が合成数であることを示している（前者は

$$2^{140} \equiv 1 \pmod{3}, 2^{140} \equiv 1 \pmod{11}, 2^{140} \equiv 2^4 \equiv 16 \pmod{17}$$

から手計算で確かめられる）

つまり、561 は単純な Fermat の小定理の合同式はすり抜けてしまうが、(a)(b) で合成数であることがわかってしまう

(a), (b) のいずれも成り立たない数 a は N が合成数であることの証人 (witness) といえる

例

$N = 561$ のとき

$$2^{140} \equiv 67 \pmod{561}, 2^{280} \equiv 1 \pmod{561}$$

なので、(a), (b) のいずれも成り立たない、このことは 561 が合成数であることを示している（前者は

$$2^{140} \equiv 1 \pmod{3}, 2^{140} \equiv 1 \pmod{11}, 2^{140} \equiv 2^4 \equiv 16 \pmod{17}$$

から手計算で確かめられる）

つまり、561 は単純な Fermat の小定理の合同式はすり抜けてしまうが、(a)(b) で合成数であることがわかってしまう

(a), (b) のいずれも成り立たない数 a は N が合成数であることの証人 (witness) といえる

残念ながら N が合成数で $\gcd(a, N) = 1$ だが (a), (b) のいずれかが成り立ってしまう場合は存在する

m が素数のとき $2^{m-1} - 1 \equiv 0 \pmod{m}$ であるから $2^{m-1} - 1 = dm$ とおくと

$$2^{2^{m-1}-1} \equiv 2^{dm} \equiv (2^m)^d \equiv 1 \pmod{2^m - 1}$$

より、$N = 2^m - 1, a = 2$ に対して (a) が成り立つ

しかし、 m が素数でも $2^m - 1$ が合成数の場合がある

残念ながら N が合成数で $\gcd(a, N) = 1$ だが (a), (b) のいずれかが成り立ってしまう場合は存在する

m が素数のとき $2^{m-1} - 1 \equiv 0 \pmod{m}$ であるから $2^{m-1} - 1 = dm$ とおくと

$$2^{2^{m-1}-1} \equiv 2^{dm} \equiv (2^m)^d \equiv 1 \pmod{2^m - 1}$$

より、$N = 2^m - 1, a = 2$ に対して (a) が成り立つ

しかし、 m が素数でも $2^m - 1$ が合成数の場合がある

残念ながら N が合成数で $\gcd(a, N) = 1$ だが (a), (b) のいずれかが成り立ってしまう場合は存在する

m が素数のとき $2^{m-1} - 1 \equiv 0 \pmod{m}$ であるから $2^{m-1} - 1 = dm$ とおくと

$$2^{2^{m-1}-1} \equiv 2^{dm} \equiv (2^m)^d \equiv 1 \pmod{2^m - 1}$$

より、$N = 2^m - 1, a = 2$ に対して (a) が成り立つ

しかし、 m が素数でも $2^m - 1$ が合成数の場合がある

たとえば $m = 11$ のとき $2047 = 23 \times 89, 2047 - 1 = 2 \times 1023$ であるが、$2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}$ となる

さいわい $3^{1023} \equiv 1565 \pmod{2047}$（これは $3^{1023} \equiv 3^{11} \equiv 1 \pmod{23}$ および $3^{1023} \equiv 3^{55} \equiv -3^{11} \equiv 52 \pmod{89}$ から手計算で確かめられる）だから 3 が 2047 が合成数であることの証人となる

強擬素数

N が合成数 だが (a), (b) のいずれかが成り立ってしまう場合、 N を a を底とする強擬素数 (strong pseudoprime) という

2 を底とする強擬素数: $2047, 3277, 4033, 4681, 8321, \ldots$ (OEIS A001262)

たとえば $m = 11$ のとき $2047 = 23 \times 89, 2047 - 1 = 2 \times 1023$ であるが、$2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}$ となる

さいわい $3^{1023} \equiv 1565 \pmod{2047}$（これは $3^{1023} \equiv 3^{11} \equiv 1 \pmod{23}$ および $3^{1023} \equiv 3^{55} \equiv -3^{11} \equiv 52 \pmod{89}$ から手計算で確かめられる）だから 3 が 2047 が合成数であることの証人となる

強擬素数

N が合成数 だが (a), (b) のいずれかが成り立ってしまう場合、 N を a を底とする強擬素数 (strong pseudoprime) という

2 を底とする強擬素数: $2047, 3277, 4033, 4681, 8321, \ldots$ (OEIS A001262)

たとえば $m = 11$ のとき $2047 = 23 \times 89, 2047 - 1 = 2 \times 1023$ であるが、$2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}$ となる

さいわい $3^{1023} \equiv 1565 \pmod{2047}$（これは $3^{1023} \equiv 3^{11} \equiv 1 \pmod{23}$ および $3^{1023} \equiv 3^{55} \equiv -3^{11} \equiv 52 \pmod{89}$ から手計算で確かめられる）だから 3 が 2047 が合成数であることの証人となる

強擬素数

N が合成数 だが (a), (b) のいずれかが成り立ってしまう場合、 N を a を底とする強擬素数 (strong pseudoprime) という

2 を底とする強擬素数: $2047, 3277, 4033, 4681, 8321, \ldots$ (OEIS A001262)

たとえば $m = 11$ のとき $2047 = 23 \times 89, 2047 - 1 = 2 \times 1023$ であるが、$2^{1023} = (2^{11})^{93} \equiv 1 \pmod{2047}$ となる

さいわい $3^{1023} \equiv 1565 \pmod{2047}$（これは $3^{1023} \equiv 3^{11} \equiv 1 \pmod{23}$ および $3^{1023} \equiv 3^{55} \equiv -3^{11} \equiv 52 \pmod{89}$ から手計算で確かめられる）だから 3 が 2047 が合成数であることの証人となる

強擬素数

N が合成数 だが (a), (b) のいずれかが成り立ってしまう場合、 N を a を底とする強擬素数 (strong pseudoprime) という

2 を底とする強擬素数: $2047, 3277, 4033, 4681, 8321, \ldots$ (OEIS A001262)

561 の例から期待されるように、単純に Fermat の小定理を直接用いる場合よりも、合成数を発見しやすくなる

Rabin, 1980

N が合成数ならば $1, 2, \ldots, N-1$ のなかで、N と互に素な数のうち少なくとも $3/4$ は証人となる

よって N が合成数だが $\gcd(a, N) = 1$ となるすべての底 $a = 1, 2, \ldots, N-1$ について強擬素数となるということは起きず、さらに

Burthe, 1997

N が合成数ならば $N^{1/(6\sqrt{e})+o(1)}$ より小さい証人が存在する

したがって、$N^{1/(6\sqrt{e})+o(1)}$ より小さい証人が存在するかどうか確かめることで素数かどうか確かめられる

561 の例から期待されるように、単純に Fermat の小定理を直接用いる場合よりも、合成数を発見しやすくなる

Rabin, 1980

N が合成数ならば $1, 2, \ldots, N-1$ のなかで、N と互に素な数のうち少なくとも $3/4$ は証人となる

よって N が合成数だが $\gcd(a, N) = 1$ となるすべての底 $a = 1, 2, \ldots, N-1$ について強擬素数となるということは起きず、さらに

Burthe, 1997

N が合成数ならば $N^{1/(6\sqrt{e})+o(1)}$ より小さい証人が存在する

したがって、$N^{1/(6\sqrt{e})+o(1)}$ より小さい証人が存在するかどうか確かめることで素数かどうか確かめられる

561 の例から期待されるように、単純に Fermat の小定理を直接用いる場合よりも、合成数を発見しやすくなる

Rabin, 1980

N が合成数ならば $1, 2, \ldots, N-1$ のなかで、N と互に素な数のうち少なくとも $3/4$ は証人となる

よって N が合成数だが $\gcd(a, N) = 1$ となるすべての底 $a = 1, 2, \ldots, N-1$ について強擬素数となるということは起きず、さらに

Burthe, 1997

N が合成数ならば $N^{1/(6\sqrt{e})+o(1)}$ より小さい証人が存在する

したがって、$N^{1/(6\sqrt{e})+o(1)}$ より小さい証人が存在するかどうか確かめることで素数かどうか確かめられる

最小の証人が k となる最小の合成数を N_k とおくと

Table: N_k (OEIS A006945, OEIS A089825)

k	N_k	k	N_k
2	9	15	3034679039109989281
3	2047	17	3474749660383
5	1373653	19	449841468253905 1
6	134670080641	22	160430839158166628 41
7	25326001	23	341550071728321
10	307768373641	37	3825123056546413051
11	3215031751	41	3186658578340311511674 61
12	150240184974717624 1	43	3317044064679887385961981
13	2152302898747	47	$\leq$ 6003094289670105800312596501
14	1478868544880821	53	$\leq$ 5927636107559557326344633010 1

しかし、残念なことにどのような定数 K をとっても、 $2, 3, \ldots, K$ のいずれの底についても強擬素数となる合成数は無数に存在する！

Adleman, Granville, Pomerance, 1994

X が十分大きいとき X 以下の合成数 N で、最小の証人が $(\log N)^{1/(3 \log\log\log N)}$ より大きなものが少なくとも $X^{1/(35 \log\log\log X)}$ 存在する

一方、拡張リーマン予想が正しければ、必ず比較的小さな証人が存在することが知られている

Miller, 1976 (see also Bach, 1985)

拡張リーマン予想が正しいとき N が合成数ならば $2\log^2 N$ より小さな証人が存在する

よって、拡張リーマン予想が正しいならば $2\log^2 N$ 以下の数の中に証人が存在するかどうか確かめることにより $\log^{4+o(1)} N$ 以下の時間で素数であるかどうかの判定が可能となる

しかし、残念なことにどのような定数 K をとっても、 $2, 3, \ldots, K$ のいずれの底についても強擬素数となる合成数は無数に存在する！

Adleman, Granville, Pomerance, 1994

X が十分大きいとき X 以下の合成数 N で、最小の証人が $(\log N)^{1/(3 \log\log\log N)}$ より大きなものが少なくとも $X^{1/(35 \log\log\log X)}$ 存在する

一方、拡張リーマン予想が正しければ、必ず比較的小さな証人が存在することが知られている

Miller, 1976 (see also Bach, 1985)

拡張リーマン予想が正しいとき N が合成数ならば $2\log^2 N$ より小さな証人が存在する

よって、拡張リーマン予想が正しいならば $2\log^2 N$ 以下の数の中に証人が存在するかどうか確かめることにより $\log^{4+o(1)} N$ 以下の時間で素数であるかどうかの判定が可能となる

以上のことから…

- N が合成数の場合、N と互に素な数すべてについて (a)(b) をすり抜けることは不可能
- 一方、$(\log N)^{1/(3 \log\log\log N)}$ 以下の数すべてについて (a)(b) をすり抜けてしまう数は無数に存在する
- 拡張リーマン予想が正しければ $2\log^2 N$ より小さな範囲内で合成数であることがわかってしまう
- また、1 から $N-1$ までででランダムに選んだ数について (a)(b) を確かめるという作業を k 回繰り返して、合成数 N がそれらの判定をすべてすり抜ける確率は $1/4^k$ 以下とみることができる
- この原理に基づく素数判定を Miller-Rabin 判定法という

Giuga's conjecture

N が素数のとき Fermat の小定理から

$$1^{N-1} + 2^{N-1} + \cdots + (N-1)^{N-1} + 1 \equiv 0 \pmod{N} \tag{1}$$

が成り立つ

Giuga, 1950

この合同式が成り立つ合成数は存在するか？（存在しないと予想）

Giuga's conjecture

N が素数のとき Fermat の小定理から

$$1^{N-1} + 2^{N-1} + \cdots + (N-1)^{N-1} + 1 \equiv 0 \pmod{N} \tag{1}$$

が成り立つ

Giuga, 1950

この合同式が成り立つ合成数は存在するか？（存在しないと予想）

Giuga's conjecture

N が素数のとき Fermat の小定理から

$$1^{N-1} + 2^{N-1} + \cdots + (N-1)^{N-1} + 1 \equiv 0 \pmod{N} \tag{1}$$

が成り立つ

Giuga, 1950

この合同式が成り立つ合成数は存在するか？（存在しないと予想）

N が合成数で、この合同式が成り立つことは N のすべての素因数 p について $p(p-1)$ が $\frac{N}{p}-1$ を割り切ることと同値

N のすべての素因数 p について p が $\frac{N}{p}-1$ を割り切る数を Giuga 数という

Giuga 数: $30, 858, 1722, 66198, \ldots$ (OEIS A007850)

奇数の Giuga 数は存在しないと予想されているが、未解決

N が合成数で、この合同式が成り立つことは N のすべての素因数 p について $p(p-1)$ が $\frac{N}{p}-1$ を割り切ることと同値

N のすべての素因数 p について p が $\frac{N}{p}-1$ を割り切る数を Giuga 数という

Giuga 数: $30, 858, 1722, 66198, \ldots$ (OEIS A007850)

奇数の Giuga 数は存在しないと予想されているが、未解決

なお、つぎの 3 つは同値

- N が Giuga 数
- $1^{\varphi(N)} + 2^{\varphi(N)} + \cdots + (N-1)^{\varphi(N)} \equiv -1 \pmod{N}$
- $\sum_{p|N} \frac{1}{p} - \prod_{p|N} \frac{1}{p}$ が整数

また、

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} x^m$$

により定まる Seki-Bernoulli 数 B_m について

Agoh, 1995

合同式 (1) が成り立つ $\Leftrightarrow NB_{N-1} \equiv -1 \pmod{N}$

N が合成数で、合同式 (1) が成り立つ $\Leftrightarrow$ N が Giuga 数で、かつ N のすべての素因数 p について $p-1$ が $\frac{N}{p}-1$ を割り切る

$p-1$ が $\frac{N}{p}-1$ を割り切ることは $p-1$ が $N-1=p\left(\frac{N}{p}-1\right)+(p-1)$ を割り切ることと同値なので

N が合成数で、合同式 (1) が成り立つ $\Leftrightarrow$ N が Giuga 数かつ Carmichael 数

ここから、N が合成数で、合同式 (1) が成り立つならば

- N は奇数で平方因子をもたず、p が N の素因数ならば N は $ap+1$ の形の素因数をもたない
- $\sum_{p|N} \frac{1}{p} > 1$

がわかる

Benocchi, 1985 や Borwein, Maitland, and Skerritt 2013 はこの条件が成り立つ素因数のパターンを調べ、次の結果に至った

Borwein, Maitland, and Skerritt 2013

N が合成数で、合同式 (1) が成り立つならば N は少なくとも 4771 個の素因数をもち、$N > 10^{19907}$

ここから、N が合成数で、合同式 (1) が成り立つならば

- N は奇数で平方因子をもたず、p が N の素因数ならば N は $ap+1$ の形の素因数をもたない
- $\sum_{p|N} \frac{1}{p} > 1$

がわかる

Benocchi, 1985 や Borwein, Maitland, and Skerritt 2013 はこの条件が成り立つ素因数のパターンを調べ、次の結果に至った

Borwein, Maitland, and Skerritt 2013

N が合成数で、合同式 (1) が成り立つならば N は少なくとも 4771 個の素因数をもち、$N > 10^{19907}$

AKS test

先に述べたように、素数判定は $\log^c N$ 以内に可能

Agrawal, Kayal, and Saxena, 2002-2004

$N \geq 2, r$ を $g > 0, N^g \equiv 1 \pmod{r}$ ならば $g > (\log N / \log 2)^2$ となるようにとり N は $\sqrt{\varphi(r)} \log N / \log 2$ 以下の素因数をもたないとする

このとき N が素数 $\Leftrightarrow 0 \leq a \leq \sqrt{\varphi(r)} \log N / \log 2$ となるすべての整数 a について

$$(x + a)^N \equiv x^N + a \pmod{(x^r - 1, N)} \tag{2}$$

が成り立つ（合同式は、多項式を $x^r - 1$ で割って、さらに係数を N で割った余りを比較する）

上記のような r として比較的小さなものが取れることが知られており、この方法により、素数判定は $\log^c N$ 以内に可能であることが証明された！

Agrawal, Kayal, and Saxena, 2002-2004

$N \geq 2, r$ を $g > 0, N^g \equiv 1 \pmod{r}$ ならば $g > (\log N / \log 2)^2$ となるようにとり N は $\sqrt{\varphi(r)} \log N / \log 2$ 以下の素因数をもたないとする

このとき N が素数 $\Leftrightarrow 0 \leq a \leq \sqrt{\varphi(r)} \log N / \log 2$ となるすべての整数 a について

$$(x + a)^N \equiv x^N + a \pmod{(x^r - 1, N)} \tag{2}$$

が成り立つ（合同式は、多項式を $x^r - 1$ で割って、さらに係数を N で割った余りを比較する）

上記のような r として比較的小さなものが取れることが知られており、この方法により、素数判定は $\log^c N$ 以内に可能であることが証明された！

Agrawal, Kayal, and Saxena, 2002-2004

$N \geq 2, r$ を $g > 0, N^g \equiv 1 \pmod{r}$ ならば $g > (\log N / \log 2)^2$ となるようにとり N は $\sqrt{\varphi(r)} \log N / \log 2$ 以下の素因数をもたないとする

このとき N が素数 $\Leftrightarrow 0 \leq a \leq \sqrt{\varphi(r)} \log N / \log 2$ となるすべての整数 a について

$$(x + a)^N \equiv x^N + a \pmod{(x^r - 1, N)} \tag{2}$$

が成り立つ（合同式は、多項式を $x^r - 1$ で割って、さらに係数を N で割った余りを比較する）

上記のような r として比較的小さなものが取れることが知られており、この方法により、素数判定は $\log^c N$ 以内に可能であることが証明された！

そこで、次の問題が生じる

(2) が成り立つような小さな整数 a と合成数 N はどのようなものが存在するか？（容易に確認できる特殊例を除いて存在しないならば、(2) の形の合同式を 1 つ検証し、特殊例を検証するだけで素数判定ができる）

予想 (Agrawal, Kayal, and Saxena, 2002-2004)

r が N を割り切らない素数で

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

ならば N は素数か、または $N^2 \equiv 1 \pmod{r}$

この予想が正しければ、$N(N-1)(N+1)$ を割り切らない素数 r をとり、1 つ合同式を検証するだけで素数判定ができることになる

Lenstra and Pomerance, 2003 はこの予想を誤りと考えているが、いまだ解決されていない

そこで、次の問題が生じる

(2) が成り立つような小さな整数 a と合成数 N はどのようなものが存在するか？（容易に確認できる特殊例を除いて存在しないならば、(2) の形の合同式を 1 つ検証し、特殊例を検証するだけで素数判定ができる）

予想 (Agrawal, Kayal, and Saxena, 2002-2004)

r が N を割り切らない素数で

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

ならば N は素数か、または $N^2 \equiv 1 \pmod{r}$

この予想が正しければ、$N(N-1)(N+1)$ を割り切らない素数 r をとり、1 つ合同式を検証するだけで素数判定ができることになる

Lenstra and Pomerance, 2003 はこの予想を誤りと考えているが、いまだ解決されていない

そこで、次の問題が生じる

(2) が成り立つような小さな整数 a と合成数 N はどのようなものが存在するか？（容易に確認できる特殊例を除いて存在しないならば、(2) の形の合同式を 1 つ検証し、特殊例を検証するだけで素数判定ができる）

予想 (Agrawal, Kayal, and Saxena, 2002-2004)

r が N を割り切らない素数で

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

ならば N は素数か、または $N^2 \equiv 1 \pmod{r}$

この予想が正しければ、$N(N-1)(N+1)$ を割り切らない素数 r をとり、1 つ合同式を検証するだけで素数判定ができることになる

Lenstra and Pomerance, 2003 はこの予想を誤りと考えているが、いまだ解決されていない

一方、これに代わる予想として

予想 (Popovych, 2008)

r が N を割り切らない素数で

$$(x-1)^N \equiv x^N - 1, (x+2)^N \equiv x^N + 2 \pmod{(x^r - 1, N)}$$

ならば N は素数か、または $N^2 \equiv 1 \pmod{r}$

これが正しければ、 $N(N-1)(N+1)$ を割り切らない素数 r をとり、2 つ合同式を確かめれば素数判定ができることになる）

Lehmer's conjecture

では N が合成数だが $\varphi(N)$ が $N-1$ の約数となることはあるか？

予想 (Lehmer, 1932)

$\varphi(N)$ が $N-1$ を割り切るとき N は素数でなければならない

Lehmer's conjecture

では N が合成数だが $\varphi(N)$ が $N-1$ の約数となることはあるか？

予想 (Lehmer, 1932)

$\varphi(N)$ が $N-1$ を割り切るとき N は素数でなければならない

$\omega(N)$ を N の相異なる素因数の個数とする

Lehmer, 1932

N が合成数で $\varphi(N)$ が $N-1$ を割り切るとき

(a) N は奇数

(b) N は平方因子をもたない

(c) $\omega(N) \geq 7$

実際、この場合 $\lambda(N)$ も $N-1$ を割り切るので、$\lambda(N)$ と N は互に素だから (a)(b) はすぐにわかる

(c) は N の素因数のパターンから比較的容易に示される

$\omega(N)$ を N の相異なる素因数の個数とする

Lehmer, 1932

N が合成数で $\varphi(N)$ が $N-1$ を割り切るとき

(a) N は奇数

(b) N は平方因子をもたない

(c) $\omega(N) \geq 7$

実際、この場合 $\lambda(N)$ も $N-1$ を割り切るので、$\lambda(N)$ と N は互に素だから (a)(b) はすぐにわかる

(c) は N の素因数のパターンから比較的容易に示される

$\omega(N)$ を N の相異なる素因数の個数とする

Lehmer, 1932

N が合成数で $\varphi(N)$ が $N-1$ を割り切るとき

(a) N は奇数

(b) N は平方因子をもたない

(c) $\omega(N) \geq 7$

実際、この場合 $\lambda(N)$ も $N-1$ を割り切るので、$\lambda(N)$ と N は互に素だから (a)(b) はすぐにわかる

(c) は N の素因数のパターンから比較的容易に示される

その後の発展

- Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$
- Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$
- Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

- Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$
- Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$
- Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$

Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$

Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$

Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$

Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

- Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$
- Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$
- Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

- Pomerance, 1977: $V(x) = O(x^{1/2}\log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$
- Luca and Pomerance, 2011: $V(x) < x^{1/2}\log^{-1/2+o(1)} x$
- Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

- Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$
- Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$
- Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

- Pomerance, 1977: $V(x) = O(x^{1/2}\log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$
- Luca and Pomerance, 2011: $V(x) < x^{1/2}\log^{-1/2+o(1)} x$
- Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$

Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$

Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$

Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$

Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$

Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$

Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$

Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$

Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$

Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$

Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$

Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$

Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$

Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$

Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, さらに $\omega(N) \leq r$ ならば $N \leq r^{2^r}$

Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$

Burek and Żmija, 2016: $\omega(N) \leq r$ ならば $N \leq 2^{2^r} - 2^{2^{r-1}}$

その後の発展

Cohen and Hagis, 1980: $\omega(N) \geq 14$, $N > 10^{20}$

Renze's notebook: $\omega(N) \geq 15$, $N > 10^{26}$

Pinch, research page: $N > 10^{30}$

さらに $V(x)$ を $\varphi(N)$ が $N-1$ を割り切る合成数 $N \leq x$ の個数とすると

Pomerance, 1977: $V(x) = O(x^{1/2} \log^{3/4} x)$, **さらに $\omega(N) \leq r$ ならば** $N \leq r^{2^r}$

Luca and Pomerance, 2011: $V(x) < x^{1/2} \log^{-1/2+o(1)} x$

Burek and Żmija, 2016: $\omega(N) \leq r$ **ならば** $N \leq 2^{2^r} - 2^{2^{r-1}}$

$\varphi(N)$ が $N-1$ を割り切る合成数が存在するかどうかは知られていないが、やや弱い条件を考えると…

- $\varphi(561) = 2 = 320$ は 560^2 を割り切る
- $\varphi(N)$ が $(N-1)^2$ を割り切る N: $561, 1105, 1729, 2465, \ldots$ (OEIS A173703).

$\varphi(N)$ が $N-1$ を割り切る合成数が存在するかどうかは知られていないが、やや弱い条件を考えると…

$\varphi(561) = 2 = 320$ は 560^2 を割り切る

$\varphi(N)$ が $(N-1)^2$ を割り切る N: $561, 1105, 1729, 2465, \ldots$ (OEIS A173703).

N が k-Lehmer: N が合成数で $\varphi(N)$ が $(N-1)^k$ を割り切る

McNew, 2013

各 k に対し x 以下の k-Lehmer 数 N の個数は $O(x^{1-1/(4k-1)})$
また、x 以下の整数 N である k について $\varphi(N)$ が $(N-1)^k$ を割り切るものの個数は $x\exp(-(1+o(1))\log x \log\log\log x/\log\log x)$.

McNew and Wright, 2016

$k \geq 3$ のとき x 以下の整数 N で $(k-1)$-Lehmer でないが k-Lehmer であるものが少なくとも $x^{1/(k-1)+o(1)}$ 存在する
（この証明には特殊な素数のパターンに関する非常に証明の難しい結果が用いられている）

2-Lehmer 数 $\varphi(N)$ が $(N-1)^2$ を割り切る合成数 N が無限に多く存在するかは未解決

N が k-Lehmer: N が合成数で $\varphi(N)$ が $(N-1)^k$ を割り切る

McNew, 2013

各 k に対し x 以下の k-Lehmer 数 N の個数は $O(x^{1-1/(4k-1)})$
また、x 以下の整数 N である k について $\varphi(N)$ が $(N-1)^k$ を割り切るものの個数は $x\exp(-(1+o(1))\log x \log\log\log x/\log\log x)$.

McNew and Wright, 2016

$k \geq 3$ のとき x 以下の整数 N で $(k-1)$-Lehmer でないが k-Lehmer であるものが少なくとも $x^{1/(k-1)+o(1)}$ 存在する
（この証明には特殊な素数のパターンに関する非常に証明の難しい結果が用いられている）

2-Lehmer 数 $\varphi(N)$ が $(N-1)^2$ を割り切る合成数 N が無限に多く存在するかは未解決

N が k-Lehmer: N が合成数で $\varphi(N)$ が $(N-1)^k$ を割り切る

McNew, 2013

各 k に対し x 以下の k-Lehmer 数 N の個数は $O(x^{1-1/(4k-1)})$
また、x 以下の整数 N である k について $\varphi(N)$ が $(N-1)^k$ を割り切るものの個数は $x\exp(-(1+o(1))\log x \log\log\log x/\log\log x)$.

McNew and Wright, 2016

$k \geq 3$ のとき x 以下の整数 N で $(k-1)$-Lehmer でないが k-Lehmer であるものが少なくとも $x^{1/(k-1)+o(1)}$ 存在する
（この証明には特殊な素数のパターンに関する非常に証明の難しい結果が用いられている）

2-Lehmer 数 $\varphi(N)$ が $(N-1)^2$ を割り切る合成数 N が無限に多く存在するかは未解決

N が k-Lehmer: N が合成数で $\varphi(N)$ が $(N-1)^k$ を割り切る

McNew, 2013

各 k に対し x 以下の k-Lehmer 数 N の個数は $O(x^{1-1/(4k-1)})$
また、x 以下の整数 N である k について $\varphi(N)$ が $(N-1)^k$ を割り切るものの個数は $x\exp(-(1+o(1))\log x \log\log\log x/\log\log x)$.

McNew and Wright, 2016

$k \geq 3$ のとき x 以下の整数 N で $(k-1)$-Lehmer でないが k-Lehmer であるものが少なくとも $x^{1/(k-1)+o(1)}$ 存在する
（この証明には特殊な素数のパターンに関する非常に証明の難しい結果が用いられている）

2-Lehmer 数 $\varphi(N)$ が $(N-1)^2$ を割り切る合成数 N が無限に多く存在するかは未解決

さらに、Lehmer の条件に近づけることはできるか？

Almost Lehmer numbers (Yamada, submitted)

(a) N が 1-nearly Lehmer: N が合成数で $N-1$ のある素因数 ℓ をとれば $\varphi(N)$ は $\ell(N-1)$ を割り切る

(b) N が almost Lehmer: N が合成数で $N-1$ のある平方因子をもたない約数 ℓ をとれば $\varphi(N)$ は $\ell(N-1)$ を割り切る

たとえば、Ramanujan のタクシー数 $1729 = 7 \times 13 \times 19$ について、$\varphi(1729) = 6 \times 12 \times 18 = 1296 = 1728 \times (3/4)$ は 1728 は割り切らないが 3×1728 を割り切るので 1729 は 1-nearly Lehmer

さらに、Lehmer の条件に近づけることはできるか？

Almost Lehmer numbers (Yamada, submitted)

(a) N が 1-nearly Lehmer: N が合成数で $N-1$ のある素因数 ℓ をとれば $\varphi(N)$ は $\ell(N-1)$ を割り切る

(b) N が almost Lehmer: N が合成数で $N-1$ のある平方因子をもたない約数 ℓ をとれば $\varphi(N)$ は $\ell(N-1)$ を割り切る

たとえば、Ramanujan のタクシー数 $1729 = 7 \times 13 \times 19$ について、$\varphi(1729) = 6 \times 12 \times 18 = 1296 = 1728 \times (3/4)$ は 1728 は割り切らないが 3×1728 を割り切るので 1729 は 1-nearly Lehmer

さらに、Lehmer の条件に近づけることはできるか？

Almost Lehmer numbers (Yamada, submitted)

(a) N が 1-nearly Lehmer: N が合成数で $N-1$ のある素因数 ℓ をとれば $\varphi(N)$ は $\ell(N-1)$ を割り切る

(b) N が almost Lehmer: N が合成数で $N-1$ のある平方因子をもたない約数 ℓ をとれば $\varphi(N)$ は $\ell(N-1)$ を割り切る

たとえば、Ramanujan のタクシー数 $1729 = 7 \times 13 \times 19$ について、$\varphi(1729) = 6 \times 12 \times 18 = 1296 = 1728 \times (3/4)$ は 1728 は割り切らないが 3×1728 を割り切るので 1729 は 1-nearly Lehmer

1-nearly Lehmer 数の例 (OEIS A338998)

$1729, 12801, 5079361, 34479361, 3069196417, \ldots$

2^{32} 以下のものはこの 5 つだけしかない（Carmichael 数は 1729 と 3069196417 のみ）

Almost Lehmer 数の例 (OEIS A337316)

$$1729, 12801, 247105, 1224721, 2704801, 5079361, 8355841, \ldots$$

2^{32} 以下のものは 38 個ある（そのうち 14 個が Carmichael 数）

Theorem (Yamada, submitted)

x 以下の 1-nearly Lehmer 数の個数は

$$O((x \log x)^{2/3} (\log \log x)^{8/3})$$

より小さく x 以下の almost Lehmer 数の個数は

$$x^{4/5} \exp\left(\left(\frac{4}{5} + o(1)\right) \frac{\log x \log \log \log x}{\log \log x}\right)$$

より小さい

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）
たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる
$\{p_1^2 p_2^2\}, \{p_1^2 p_2, p_2\}, \{p_1 p_2^2, p_1\}, \{p_1^2, p_2^2\}, \{p_1^2, p_2, p_2\}, \{p_2^2, p_1, p_1\},$
$\{p_1 p_2, p_1 p_2\}, \{p_1 p_2, p_1, p_2\}, \{p_1, p_1, p_2, p_2\}.$

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）
たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる
$\{p_1^2 p_2^2\}$, $\{p_1^2 p_2, p_2\}$, $\{p_1 p_2^2, p_1\}$, $\{p_1^2, p_2^2\}$, $\{p_1^2, p_2, p_2\}$, $\{p_2^2, p_1, p_1\}$, $\{p_1 p_2, p_1 p_2\}$, $\{p_1 p_2, p_1, p_2\}$, $\{p_1, p_1, p_2, p_2\}$.

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）

たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる

$\{p_1^2 p_2^2\}, \{p_1^2 p_2, p_2\}, \{p_1 p_2^2, p_1\}, \{p_1^2, p_2^2\}, \{p_1^2, p_2, p_2\}, \{p_2^2, p_1, p_1\},$
$\{p_1 p_2, p_1 p_2\}, \{p_1 p_2, p_1, p_2\}, \{p_1, p_1, p_2, p_2\}.$

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）
たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる
$\{p_1^2 p_2^2\}, \{p_1^2 p_2, p_2\}, \{p_1 p_2^2, p_1\}, \{p_1^2, p_2^2\}, \{p_1^2, p_2, p_2\}, \{p_2^2, p_1, p_1\},$
$\{p_1 p_2, p_1 p_2\}, \{p_1 p_2, p_1, p_2\}, \{p_1, p_1, p_2, p_2\}.$

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）

たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる

$\{p_1^2 p_2^2\}, \{p_1^2 p_2, p_2\}, \{p_1 p_2^2, p_1\}, \{p_1^2, p_2^2\}, \{p_1^2, p_2, p_2\}, \{p_2^2, p_1, p_1\},$
$\{p_1 p_2, p_1 p_2\}, \{p_1 p_2, p_1, p_2\}, \{p_1, p_1, p_2, p_2\}.$

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）

たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる

$\{p_1^2 p_2^2\}, \{p_1^2 p_2, p_2\}, \{p_1 p_2^2, p_1\}, \{p_1^2, p_2^2\}, \{p_1^2, p_2, p_2\}, \{p_2^2, p_1, p_1\},$
$\{p_1 p_2, p_1 p_2\}, \{p_1 p_2, p_1, p_2\}, \{p_1, p_1, p_2, p_2\}.$

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）

たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる

$\{p_1^2 p_2^2\}, \{p_1^2 p_2, p_2\}, \{p_1 p_2^2, p_1\}, \{p_1^2, p_2^2\}, \{p_1^2, p_2, p_2\}, \{p_2^2, p_1, p_1\},$
$\{p_1 p_2, p_1 p_2\}, \{p_1 p_2, p_1, p_2\}, \{p_1, p_1, p_2, p_2\}.$

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）

たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる

$\{p_1^2 p_2^2\}$, $\{p_1^2 p_2, p_2\}$, $\{p_1 p_2^2, p_1\}$, $\{p_1^2, p_2^2\}$, $\{p_1^2, p_2, p_2\}$, $\{p_2^2, p_1, p_1\}$, $\{p_1 p_2, p_1 p_2\}$, $\{p_1 p_2, p_1, p_2\}$, $\{p_1, p_1, p_2, p_2\}$.

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）

たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる

$\{p_1^2 p_2^2\}$, $\{p_1^2 p_2, p_2\}$, $\{p_1 p_2^2, p_1\}$, $\{p_1^2, p_2^2\}$, $\{p_1^2, p_2, p_2\}$, $\{p_2^2, p_1, p_1\}$, $\{p_1 p_2, p_1 p_2\}$, $\{p_1 p_2, p_1, p_2\}$, $\{p_1, p_1, p_2, p_2\}$.

$\tau(s)$: $s = s_1 s_2 \cdots s_r, 1 < s_1 \leq s_2 \leq \cdots s_r$ の形に整数の積へと分解する方法の総数（$\tau(s)$ の値は OEIS A001055 を参照）
たとえば $s = p_1^2 p_2^2$ のとき、次の分解から $\tau(s) = 9$ とわかる
$\{p_1^2 p_2^2\}$, $\{p_1^2 p_2, p_2\}$, $\{p_1 p_2^2, p_1\}$, $\{p_1^2, p_2^2\}$, $\{p_1^2, p_2, p_2\}$, $\{p_2^2, p_1, p_1\}$,
$\{p_1 p_2, p_1 p_2\}$, $\{p_1 p_2, p_1, p_2\}$, $\{p_1, p_1, p_2, p_2\}$.

Erdős, Granville, Pomerance, and Spiro, 1990, (3.1)

任意の正の整数 s と $x > 3$ について

$$\sum_{q \leq x, q \equiv 1 \pmod{s}} \frac{1}{q} < \frac{c_1 \log\log x}{s} \tag{3}$$

となる絶対定数（s, x によらない） c_1 が存在する

q は $q \leq x, q \equiv 1 \pmod{s}$ となる素数全体を動く

これをもとにして

Lemma 1

x 以下の整数 N で $\varphi(N)$ が s で割り切れるものの個数は

$$\frac{\tau(s) x (c_1 \log\log x)^{\Omega(s)}}{s} \tag{4}$$

より小さい（c_1 は絶対定数）

がわかる

Erdős, Granville, Pomerance, and Spiro, 1990, (3.1)

任意の正の整数 s と $x > 3$ について

$$\sum_{q \leq x, q \equiv 1 \pmod{s}} \frac{1}{q} < \frac{c_1 \log\log x}{s} \tag{3}$$

となる絶対定数（s, x によらない） c_1 が存在する

q は $q \leq x, q \equiv 1 \pmod{s}$ となる素数全体を動く

これをもとにして

Lemma 1

x 以下の整数 N で $\varphi(N)$ が s で割り切れるものの個数は

$$\frac{\tau(s) x (c_1 \log\log x)^{\Omega(s)}}{s} \tag{4}$$

より小さい（c_1 は絶対定数）

がわかる

Oppenheim, 1927

$x \to \infty$ のとき

$$\sum_{s \le x} \tau(s) = \frac{(1+o(1))xe^{2\sqrt{\log x}}}{2\sqrt{\pi}\log^{3/4} x} \tag{5}$$

をつかって

Lemma 2

$x \to \infty$ のとき

$$\sum_{s \le x} \frac{\tau(s)}{s} < \frac{(1+o(1))e^{2\sqrt{\log x}}\log^{1/4} x}{2\sqrt{\pi}} \tag{6}$$

がわかる

Oppenheim, 1927

$x \to \infty$ のとき

$$\sum_{s \le x} \tau(s) = \frac{(1+o(1))xe^{2\sqrt{\log x}}}{2\sqrt{\pi}\log^{3/4} x} \tag{5}$$

をつかって

Lemma 2

$x \to \infty$ のとき

$$\sum_{s \le x} \frac{\tau(s)}{s} < \frac{(1+o(1))e^{2\sqrt{\log x}}\log^{1/4} x}{2\sqrt{\pi}} \tag{6}$$

がわかる

$\tau(s)$ 自体は $s^{1-o(1)}$ まで大きくなることがある

Canfield, Erdős, and Pomerance, 1983

Highly factorable な整数 s (OEIS A033833) について

$\tau(s) = s \exp(-(1+o(1)) \log s \log\log\log s / \log\log s)$

$\tau(s)$ 自体は $s^{1-o(1)}$ まで大きくなることがある

Canfield, Erdős, and Pomerance, 1983

Highly factorable な整数 s (OEIS A033833) について

$\tau(s) = s \exp(-(1+o(1)) \log s \log\log\log s / \log\log s)$

以下

- $U_1(x)$: x 以下の 1-nearly Lehmer 数の個数
- $U_\infty(x)$: x 以下の almost Lehmer 数の個数
- $S(s;x)$: x 以下の整数 n で $\varphi(n)$ が s で割り切れる物の個数

とおく

Lemma 1 から

$$S(s;x) \leq \frac{\tau(s)x(c_1 \log\log x)^{\Omega(s)}}{s}$$

以下

- $U_1(x)$: x 以下の 1-nearly Lehmer 数の個数
- $U_\infty(x)$: x 以下の almost Lehmer 数の個数
- $S(s;x)$: x 以下の整数 n で $\varphi(n)$ が s で割り切れる物の個数

とおく

Lemma 1 から

$$S(s;x) \leq \frac{\tau(s)x(c_1 \log\log x)^{\Omega(s)}}{s}$$

x: 十分大きな実数

N: 1-nearly Lehmer あるいは almost Lehmer

とすると $(N-1)/\varphi(N) = k/\ell, \gcd(k,\ell) = 1$ とあらわしたとき

ℓ は $N-1$ の約数で平方因子をもたず、さらに N が 1-nearly Lehmer の場合は素数

また N が合成数で、$\gcd(\varphi(N), N) = 1$ なので N は奇数で平方因子をもたないことは先に触れたとおり

x: 十分大きな実数

N: 1-nearly Lehmer あるいは almost Lehmer

とすると $(N-1)/\varphi(N) = k/\ell, \gcd(k,\ell) = 1$ とあらわしたとき

ℓ は $N-1$ の約数で平方因子をもたず、さらに N が 1-nearly Lehmer の場合は素数

また N が合成数で、$\gcd(\varphi(N), N) = 1$ なので N は奇数で平方因子をもたないことは先に触れたとおり

x: 十分大きな実数

N: 1-nearly Lehmer あるいは almost Lehmer

とすると $(N-1)/\varphi(N) = k/\ell, \gcd(k,\ell) = 1$ とあらわしたとき

ℓ は $N-1$ の約数で平方因子をもたず、さらに N が 1-nearly Lehmer の場合は素数

また N が合成数で、$\gcd(\varphi(N), N) = 1$ なので N は奇数で平方因子をもたないことは先に触れたとおり

$N = md$ とおくと、N は平方因子をもたないので
$\ell(md-1) = k\varphi(N) = k\varphi(m)\varphi(d)$ となるから

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_0} \right), \ell_0 = \gcd(\ell, \varphi(d)) \tag{7}$$

$\ell_0 \mid \ell \mid (N-1)$ だから $\varphi(d)/\ell_0, \ell_0$ はともに $N-1 = md-1$ の約数
よって ℓ_2 を 「ℓ_0 の素因数のうち、 $\varphi(d)$ を 2 回以上割り切る素数全体の積」とおくと

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_2} \right) \tag{8}$$

また、 ℓ_2^2 は $\varphi(d)$ を割り切るので $\ell_2 \leq \sqrt{\varphi(d)} < \sqrt{d}$ となる

$N = md$ とおくと、N は平方因子をもたないので
$\ell(md-1) = k\varphi(N) = k\varphi(m)\varphi(d)$ となるから

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_0}\right), \ell_0 = \gcd(\ell, \varphi(d)) \tag{7}$$

$\ell_0 \mid \ell \mid (N-1)$ だから $\varphi(d)/\ell_0, \ell_0$ はともに $N-1 = md-1$ の約数
よって ℓ_2 を 「ℓ_0 の素因数のうち、 $\varphi(d)$ を 2 回以上割り切る素数全体の積」とおくと

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_2}\right) \tag{8}$$

また、 ℓ_2^2 は $\varphi(d)$ を割り切るので $\ell_2 \leq \sqrt{\varphi(d)} < \sqrt{d}$ となる

$N = md$ とおくと、N は平方因子をもたないので
$\ell(md-1) = k\varphi(N) = k\varphi(m)\varphi(d)$ となるから

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_0}\right), \ell_0 = \gcd(\ell, \varphi(d)) \tag{7}$$

$\ell_0 \mid \ell \mid (N-1)$ だから $\varphi(d)/\ell_0, \ell_0$ はともに $N-1 = md-1$ の約数
よって ℓ_2 を 「ℓ_0 の素因数のうち、 $\varphi(d)$ を 2 回以上割り切る素数全体の積」とおくと

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_2}\right) \tag{8}$$

また、 ℓ_2^2 は $\varphi(d)$ を割り切るので $\ell_2 \leq \sqrt{\varphi(d)} < \sqrt{d}$ となる

$N = md$ とおくと、N は平方因子をもたないので
$\ell(md-1) = k\varphi(N) = k\varphi(m)\varphi(d)$ となるから

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_0}\right), \ell_0 = \gcd(\ell, \varphi(d)) \tag{7}$$

$\ell_0 \mid \ell \mid (N-1)$ だから $\varphi(d)/\ell_0$, ℓ_0 はともに $N-1 = md-1$ の約数
よって ℓ_2 を 「ℓ_0 の素因数のうち、 $\varphi(d)$ を 2 回以上割り切る素数全体の積」とおくと

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_2}\right) \tag{8}$$

また、 ℓ_2^2 は $\varphi(d)$ を割り切るので $\ell_2 \leq \sqrt{\varphi(d)} < \sqrt{d}$ となる

$N = md$ とおくと、N は平方因子をもたないので
$\ell(md-1) = k\varphi(N) = k\varphi(m)\varphi(d)$ となるから

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_0}\right), \ell_0 = \gcd(\ell, \varphi(d)) \tag{7}$$

$\ell_0 \mid \ell \mid (N-1)$ だから $\varphi(d)/\ell_0, \ell_0$ はともに $N-1 = md-1$ の約数
よって ℓ_2 を 「ℓ_0 の素因数のうち、 $\varphi(d)$ を 2 回以上割り切る素数全体の積」とおくと

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_2}\right) \tag{8}$$

また、 ℓ_2^2 は $\varphi(d)$ を割り切るので $\ell_2 \leq \sqrt{\varphi(d)} < \sqrt{d}$ となる

$N = md$ とおくと、N は平方因子をもたないので
$\ell(md-1) = k\varphi(N) = k\varphi(m)\varphi(d)$ となるから

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_0}\right), \ell_0 = \gcd(\ell, \varphi(d)) \tag{7}$$

$\ell_0 \mid \ell \mid (N-1)$ だから $\varphi(d)/\ell_0, \ell_0$ はともに $N-1 = md-1$ の約数
よって ℓ_2 を 「ℓ_0 の素因数のうち、 $\varphi(d)$ を 2 回以上割り切る素数全体の積」とおくと

$$md \equiv 1 \left(\mathrm{mod}\ \frac{\varphi(d)}{\ell_2}\right) \tag{8}$$

また、 ℓ_2^2 は $\varphi(d)$ を割り切るので $\ell_2 \leq \sqrt{\varphi(d)} < \sqrt{d}$ となる

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}$, $N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

* Y_1 を $x^{1/3}$ より大きな実数、 $Y_2 = Y_1^2$ とおく
* N は Y_2 より大きな素数では割り切れない、実際 $N = mp, p > Y_2$ とすると 先の考察から $m \equiv 1 \pmod{(p-1)/\ell_2}, \ell_2^2 \mid (p-1)$ となるが $m \geq 1 + \sqrt{p-1} > \sqrt{p}, N > p^{3/2} > Y_2^{3/2} = Y_1^3$ となって矛盾する
* N が Y_1 より大きな素因数をもたないとき, Y_1 以上の最小の N の約数を d とおくと $Y_1 \leq d \leq Y_1^2 = Y_2$
* N が $Y_1 \leq p \leq Y_2$ の範囲に素因数 p をもつとき N は $Y_1 \leq d \leq Y_2$ となる約数 $d = p$ をもつ
* よって n は $Y_1 \leq d \leq Y_2$ の範囲に約数 d をもつ

各 d について $md \equiv 1 \pmod{\varphi(d)/\ell_2}$ となる整数 $md \le x$ の個数は 多くとも $1 + \lfloor \ell_2 x/(d\varphi(d)) \rfloor$

先に触れたことから $\ell_2 \le \sqrt{\varphi(d)} \le Y_1$

Hardy-Wright, Theorem 328 などから

$d/\varphi(d) < (e^\gamma + o(1)) \log\log d \ll \log\log x$

よって x 以下の、almost Lehmer 数あるいは 1-nearly Lehmer 数の個数は多くとも

$$\begin{aligned} &\sum_{\ell_2 \le Y_1} \sum_{Y_1 \le d \le Y_2, \ell_2^2 \mid \varphi(d)} \left(1 + \frac{\ell_2 x}{d\varphi(d)}\right) \\ &\ll \sum_{\ell_2 \le Y_1} \left(S(\ell_2^2; Y_2) + \sum_{Y_1 \le d \le Y_2, \ell_2^2 \mid \varphi(d)} \frac{\ell_2 x \log\log x}{d^2} \right), \end{aligned} \tag{9}$$

almost Lehmer 数の場合、ℓ_2 は平方因子をもたない数を、1-nearly Lehmer 数の場合 ℓ_2 は 1 および素数を動く

各 d について $md \equiv 1 \pmod{\varphi(d)/\ell_2}$ となる整数 $md \le x$ の個数は 多くとも $1 + \lfloor \ell_2 x/(d\varphi(d)) \rfloor$

先に触れたことから $\ell_2 \le \sqrt{\varphi(d)} \le Y_1$

Hardy-Wright, Theorem 328 などから

$d/\varphi(d) < (e^\gamma + o(1)) \log\log d \ll \log\log x$

よって x 以下の、almost Lehmer 数あるいは 1-nearly Lehmer 数の個数は多くとも

$$\sum_{\ell_2 \le Y_1} \sum_{Y_1 \le d \le Y_2, \ell_2^2 \mid \varphi(d)} \left(1 + \frac{\ell_2 x}{d\varphi(d)}\right) \ll \sum_{\ell_2 \le Y_1} \left(S(\ell_2^2; Y_2) + \sum_{Y_1 \le d \le Y_2, \ell_2^2 \mid \varphi(d)} \frac{\ell_2 x \log\log x}{d^2} \right), \tag{9}$$

almost Lehmer 数の場合、ℓ_2 は平方因子をもたない数を、1-nearly Lehmer 数の場合 ℓ_2 は 1 および素数を動く

各 d について $md \equiv 1 \pmod{\varphi(d)/\ell_2}$ となる整数 $md \le x$ の個数は 多くとも $1 + \lfloor \ell_2 x/(d\varphi(d)) \rfloor$

先に触れたことから $\ell_2 \le \sqrt{\varphi(d)} \le Y_1$

Hardy-Wright, Theorem 328 などから

$d/\varphi(d) < (e^\gamma + o(1)) \log\log d \ll \log\log x$

よって x 以下の、almost Lehmer 数あるいは 1-nearly Lehmer 数の個数は多くとも

$$\begin{aligned} &\sum_{\ell_2 \le Y_1} \sum_{Y_1 \le d \le Y_2, \ell_2^2 \mid \varphi(d)} \left(1 + \frac{\ell_2 x}{d\varphi(d)}\right) \\ &\ll \sum_{\ell_2 \le Y_1} \left(S(\ell_2^2; Y_2) + \sum_{Y_1 \le d \le Y_2, \ell_2^2 \mid \varphi(d)} \frac{\ell_2 x \log\log x}{d^2} \right), \end{aligned} \tag{9}$$

almost Lehmer 数の場合、ℓ_2 は平方因子をもたない数を、1-nearly Lehmer 数の場合 ℓ_2 は 1 および素数を動く

1-nearly Lehmer

この場合 ℓ_2 は 1 または素数だから $\tau(\ell_2^2) \leq 2$ なので Lemma 1 から

$$U_1(x) \ll \sum_{\ell_2 \leq Y_1} \left(\frac{Y_2 (c_1 \log\log x)^{\Omega(\ell_2)}}{\ell_2^2} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2)+1}}{Y_1 \ell_2} \right) \tag{10}$$
$$\ll \left(Y_2 (c_1 \log\log x)^{2r} + \frac{x (\log x)(c_1 \log\log x)^{2r+1}}{Y_1} \right).$$

$Y_1 = (x \log x \log\log x)^{1/3}$ とおくことで、定理の前半が証明できる

この場合 ℓ_2 は 1 または素数だから $\tau(\ell_2^2) \leq 2$ なので Lemma 1 から

$$\begin{aligned} U_1(x) &\ll \sum_{\ell_2 \leq Y_1} \left(\frac{Y_2 (c_1 \log\log x)^{\Omega(\ell_2)}}{\ell_2^2} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2)+1}}{Y_1 \ell_2} \right) \\ &\ll \left(Y_2 (c_1 \log\log x)^{2r} + \frac{x (\log x)(c_1 \log\log x)^{2r+1}}{Y_1} \right). \end{aligned} \tag{10}$$

$Y_1 = (x \log x \log\log x)^{1/3}$ とおくことで、定理の前半が証明できる

1-nearly Lehmer

この場合 ℓ_2 は 1 または素数だから $\tau(\ell_2^2) \leq 2$ なので Lemma 1 から

$$\begin{aligned} U_1(x) &\ll \sum_{\ell_2 \leq Y_1} \left(\frac{Y_2 (c_1 \log\log x)^{\Omega(\ell_2)}}{\ell_2^2} + \frac{x (c_1 \log\log x)^{\Omega(\ell_2)+1}}{Y_1 \ell_2} \right) \\ &\ll \left(Y_2 (c_1 \log\log x)^{2r} + \frac{x (\log x)(c_1 \log\log x)^{2r+1}}{Y_1} \right). \end{aligned} \tag{10}$$

$Y_1 = (x \log x \log\log x)^{1/3}$ とおくことで、定理の前半が証明できる

$\ell_2^2 \mid \varphi(d)$ なので Hardy-Wright の定理 328 を再び用いて

$$\varphi(d)/\ell_2 \geq \sqrt{\varphi(d)} \gg (d/\log\log d)^{1/2}$$

よって (9) のかわりに

$$\begin{aligned} \#U_\infty(x) &\ll \sum_{\ell_2 < Y_1} \left(S(\ell_2^2; Y_2) + \sum_{Y_1 \leq d \leq Y_2, \ell_2^2 \mid \varphi(d)} \frac{x(\log\log x)^{1/2}}{d^{3/2}} \right) \\ &\ll \sum_{\ell_2 \leq Y_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \left(Y_2 (c_1 \log\log x)^{\Omega(\ell_2)} + \frac{x(c_1 \log\log x)^{\Omega(\ell_2)+1/2}}{Y_1^{1/2}} \right) \end{aligned} \tag{11}$$

$\ell_2^2 \mid \varphi(d)$ なので Hardy-Wright の定理 328 を再び用いて

$$\varphi(d)/\ell_2 \geq \sqrt{\varphi(d)} \gg (d/\log\log d)^{1/2}$$

よって (9) のかわりに

$$\begin{aligned} \#U_\infty(x) &\ll \sum_{\ell_2 < Y_1} \left(S(\ell_2^2; Y_2) + \sum_{Y_1 \leq d \leq Y_2, \ell_2^2 \mid \varphi(d)} \frac{x(\log\log x)^{1/2}}{d^{3/2}} \right) \\ &\ll \sum_{\ell_2 \leq Y_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \left(Y_2 (c_1 \log\log x)^{\Omega(\ell_2)} + \frac{x(c_1 \log\log x)^{\Omega(\ell_2)+1/2}}{Y_1^{1/2}} \right) \end{aligned} \tag{11}$$

$\ell_2 \le Y_2^{1/2}$ だから

$$\Omega(\ell_2^2) = 2\omega(\ell_2) < \frac{(1+o(1))\log Y_2}{\log\log x} \tag{12}$$

なので Lemma 2 より

$$\sum_{\ell_2<Y_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \le \sum_{s<Y_2} \frac{\tau(s)}{s} \ll e^{2\sqrt{\log x}} \log^{1/4} x. \tag{13}$$

$\ell_2 \le Y_2^{1/2}$ だから

$$\Omega(\ell_2^2) = 2\omega(\ell_2) < \frac{(1+o(1))\log Y_2}{\log\log x} \tag{12}$$

なので Lemma 2 より

$$\sum_{\ell_2 < Y_1} \frac{\tau(\ell_2^2)}{\ell_2^2} \le \sum_{s < Y_2} \frac{\tau(s)}{s} \ll e^{2\sqrt{\log x}} \log^{1/4} x. \tag{13}$$

(12), (13) を (11) に代入して

$$\#U_\infty(x) \ll e^{(1+o(1))\log Y_2 \log\log\log x/\log\log x}\left(Y_2 + \frac{x}{Y_1^{1/2}}\right) \tag{14}$$

$Y_1 = x^{2/5}$ とすることで定理の後半も証明できる

(12), (13) を (11) に代入して

$$\#U_\infty(x) \ll e^{(1+o(1))\log Y_2 \log\log\log x/\log\log x}\left(Y_2 + \frac{x}{Y_1^{1/2}}\right) \tag{14}$$

$Y_1 = x^{2/5}$ とすることで定理の後半も証明できる

2 階線形再帰数列

P, Q を $P^2 \neq 4Q$ となる整数、とし

$$\begin{aligned} U_0 =& 0, U_1 = 1, U_{n+2} = PU_{n+1} - QU_n, \\ V_0 =& 2, V_1 = P, V_{n+2} = PV_{n+1} + QV_n \end{aligned} \tag{15}$$

により $U_n = U_n(P, Q), V_n = V_n(P, Q)(n = 0, 1, \ldots)$ を定める

$D = P^2 - 4Q, \alpha = (P + \sqrt{D})/2, \beta = (P - \sqrt{D})/2$ を $x^2 - Px + Q = 0$ の 2 つの解とすると

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, V_n = \alpha^n + \beta^n \tag{16}$$

が成り立つ

2 階線形再帰数列

P, Q を $P^2 \neq 4Q$ となる整数、とし

$$\begin{aligned} U_0 =& 0, U_1 = 1, U_{n+2} = PU_{n+1} - QU_n, \\ V_0 =& 2, V_1 = P, V_{n+2} = PV_{n+1} + QV_n \end{aligned} \tag{15}$$

により $U_n = U_n(P, Q), V_n = V_n(P, Q)(n = 0, 1, \ldots)$ を定める

$D = P^2 - 4Q, \alpha = (P + \sqrt{D})/2, \beta = (P - \sqrt{D})/2$ を $x^2 - Px + Q = 0$ の 2 つの解とすると

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, V_n = \alpha^n + \beta^n \tag{16}$$

が成り立つ

例

$P = 1, Q = -1$ のとき $U_n : 0, 1, 1, 2, 3, 5, \ldots$ は Fibonacci 数と、
$V_n : 2, 1, 3, 4, 7, 11, \ldots$ は Lucas 数と一致する
$P = 3, Q = -2$ のとき $U_n = 2^n - 1, V_n = 2^n + 1$

例

$P = 1, Q = -1$ のとき $U_n : 0, 1, 1, 2, 3, 5, \ldots$ は Fibonacci 数と、
$V_n : 2, 1, 3, 4, 7, 11, \ldots$ は Lucas 数と一致する
$P = 3, Q = -2$ のとき $U_n = 2^n - 1, V_n = 2^n + 1$

Fermat の定理の一般化として、つぎの定理が知られている

Ribemboim, 1996, 2.IV

p を P, Q, D のいずれも割り切らない奇素数とすると p は $U_{p-(D/p)}$ を割り切る、また $p \mid V_{(p-(D/p))/2} \Leftrightarrow (Q/p) = -1$

やはり、この逆は成り立たない！

例

$P = 1, Q = -1$ とおくと $D = 5, (5/323) = -1$ かつ
$U_{18} = 2584 = 2^3 \times 323$ より 323 は $U_{323-(5/323)} = U_{324}$ を割り切る（m が n の約数ならば U_m は U_n の約数となる）が、$323 = 17 \times 19$

$U_{n-(D/n)}$ を割り切る合成数 n は 2 階線形再帰数列 U_n に対応する擬素数といえる！

Fibonacci 数に対応する擬素数は $323, 377, 1891, 3827, 4181, \ldots$ (OEIS A081264)

やはり、この逆は成り立たない！

例

$P = 1, Q = -1$ とおくと $D = 5, (5/323) = -1$ かつ
$U_{18} = 2584 = 2^3 \times 323$ より 323 は $U_{323-(5/323)} = U_{324}$ を割り切る（m が n の約数ならば U_m は U_n の約数となる）が、$323 = 17 \times 19$

$U_{n-(D/n)}$ を割り切る合成数 n は 2 階線形再帰数列 U_n に対応する擬素数といえる！

Fibonacci 数に対応する擬素数は $323, 377, 1891, 3827, 4181, \ldots$ (OEIS A081264)

やはり、この逆は成り立たない！

例

$P = 1, Q = -1$ とおくと $D = 5, (5/323) = -1$ かつ
$U_{18} = 2584 = 2^3 \times 323$ より 323 は $U_{323-(5/323)} = U_{324}$ を割り切る（m が n の約数ならば U_m は U_n の約数となる）が、$323 = 17 \times 19$

$U_{n-(D/n)}$ を割り切る合成数 n は 2 階線形再帰数列 U_n に対応する擬素数といえる！

Fibonacci 数に対応する擬素数は $323, 377, 1891, 3827, 4181, \ldots$ (OEIS A081264)

未解決問題（Selfridge-Wagstaff-Pomerance の 620 ドル問題）

2 を底とする擬素数で、かつ Fibonacci 擬素数である、$5k \pm 2$ の形の数は存在するか？
（言い換えると、 $n \equiv \pm 3 \pmod{10}$ かつ、$2^{n-1} - 1$ と $U_n(P = 1, Q = -1)$ をともに割り切る n は存在するか？）

この問題への懸賞金:

- 条件をすべて満足する n: Selfridge 500$, Wagstaff 100$, Pomerance 20$
- 条件をすべて満足する n が存在しないことの証明: Selfridge 20$, Wagstaff 100$, Pomerance 500$

未解決問題（Selfridge-Wagstaff-Pomerance の 620 ドル問題）

2 を底とする擬素数で、かつ Fibonacci 擬素数である、$5k \pm 2$ の形の数は存在するか？
（言い換えると、 $n \equiv \pm 3 \pmod{10}$ かつ、$2^{n-1} - 1$ と $U_n(P = 1, Q = -1)$ をともに割り切る n は存在するか？）

この問題への懸賞金:

条件をすべて満足する n: Selfridge 500$, Wagstaff 100$, Pomerance 20$

条件をすべて満足する n が存在しないことの証明: Selfridge 20$, Wagstaff 100$, Pomerance 500$

また、つぎのような定理も知られている

Ribemboim, 1996, 2.IV

p が素数ならば $V_p(P,Q) \equiv P \pmod{p}$

一方で、$P=1, Q=-1$ のとき $n = 705, 2465, 2737, 3745, \ldots$ (OEIS A005845) に対しても $V_n \equiv 1 \pmod{n}$ が成り立つ！

また、つぎのような定理も知られている

Ribemboim, 1996, 2.IV

p が素数ならば $V_p(P,Q) \equiv P \pmod{p}$

一方で、$P=1, Q=-1$ のとき $n = 705, 2465, 2737, 3745, \ldots$ (OEIS A005845) に対しても $V_n \equiv 1 \pmod{n}$ が成り立つ！

さらに任意の P について $V_n(P,-1) \equiv P \pmod{n}$ が成り立つ合成数 n（強 Fibonacci 擬素数）が存在する: $443372888629441, 58292008086312 1, 39671149333495681, 842526563598720001, \ldots$ (OEIS A299799)

Lidl, Müller, Oswald, 1990

N が強 Fibonacci 擬素数 $\Leftrightarrow$ N が平方因子をもたない奇数で、 p が N の素因数ならば $N \equiv 1$ または $p \pmod{(p^2-1)/2}$

よって 強 Fibonacci 擬素数は Carmichael 数でもある

さらに任意の P について $V_n(P,-1) \equiv P \pmod{n}$ が成り立つ合成数 n（強 Fibonacci 擬素数）が存在する: $443372888629441, 58292008086312 1,$ $3967114933349568 1, 84252656359872000 1, \ldots$ (OEIS A299799)

Lidl, Müller, Oswald, 1990

N が強 Fibonacci 擬素数 $\Leftrightarrow$ N が平方因子をもたない奇数で、 p が N の素因数ならば $N \equiv 1$ または $p \pmod{(p^2-1)/2}$

よって 強 Fibonacci 擬素数は Carmichael 数でもある

任意の P について $V_N(P,1) \equiv P \pmod N$ が成り立つ数も存在する:
$7056721, 79397009999, 443372888629441, 582920080863121, \ldots$ (OEIS A175530)

Müller, Oswald, 1991

任意の P について $V_N(P,1) \equiv P \pmod n$ が成り立つ $\Leftrightarrow$ N が平方因子をもたず p が N の素因数ならば $N \equiv \pm 1 \pmod{p-1}$ かつ
$N \equiv \pm 1 \pmod{p+1}$

このことから N が 強 Fibonacci 擬素数 $\Leftrightarrow$ N が Carmichael 数で、かつ任意の P について $V_N(P,1) \equiv P \pmod n$ が成り立つ、ということがわかる

任意の P について $V_N(P,1) \equiv P \pmod N$ が成り立つ数も存在する: $7056721, 79397009999, 443372888629441, 582920080863121, \ldots$ (OEIS A175530)

Müller, Oswald, 1991

任意の P について $V_N(P,1) \equiv P \pmod n$ が成り立つ $\Leftrightarrow$ N が平方因子をもたず p が N の素因数ならば $N \equiv \pm 1 \pmod{p-1}$ かつ $N \equiv \pm 1 \pmod{p+1}$

このことから N が 強 Fibonacci 擬素数 $\Leftrightarrow$ N が Carmichael 数で、かつ任意の P について $V_N(P,1) \equiv P \pmod n$ が成り立つ、ということがわかる

さらに、任意の整数 P と N と互に素な任意の整数 Q について
$V_N(P,Q) \equiv P \pmod N$ が成り立つ超強 Dickson 擬素数が存在する:
$443372888629441, 39671149333495681, 84252656359872001,$
$2380296518909971201, \ldots$ (OEIS A175531)

Müller, Oswald, 1992

N が超強 Dickson 擬素数 $\Leftrightarrow$ N が平方因子をもたず p が N の素因数ならば $N \equiv 1$ または $p \pmod{p^2-1}$

超強 Dickson 擬素数は無限に多く存在すると予想されているが (Howe, 2000) 未解決

さらに、任意の整数 P と N と互に素な任意の整数 Q について
$V_N(P,Q) \equiv P \pmod N$ が成り立つ超強 Dickson 擬素数が存在する:
443372888629441, 3967114933495681, 84252656359872001,
$2380296518909971201, \ldots$ (OEIS A175531)

Müller, Oswald, 1992

N が超強 Dickson 擬素数 $\Leftrightarrow$ N が平方因子をもたず p が N の素因数ならば $N \equiv 1$ または $p \pmod{p^2-1}$

超強 Dickson 擬素数は無限に多く存在すると予想されているが (Howe, 2000) 未解決

さらに、任意の整数 P と N と互に素な任意の整数 Q について $V_N(P,Q) \equiv P \pmod{N}$ が成り立つ超強 Dickson 擬素数が存在する:
$443372888629441, 39671149333495681, 84252656359872001, 238029651890997120 1, \ldots$ (OEIS A175531)

Müller, Oswald, 1992

N が超強 Dickson 擬素数 $\Leftrightarrow$ N が平方因子をもたず p が N の素因数ならば $N \equiv 1$ または $p \pmod{p^2-1}$

超強 Dickson 擬素数は無限に多く存在すると予想されているが (Howe, 2000) 未解決

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (A-Bed)

Agoh, 1995:

Takashi Agoh, On Giuga's conjecture, Manuscripta Math. **87** *(1995), 501–510*

Agrawal, Kayal, and Saxena 2002-2004:

Manindra Agrawal, Neeraj Kayal, and Nitin Saxena, PRIMES is in P, Ann. of Math. **160** *(2004), 781–793.*

Bach, 1985:

Eric Bach, Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms, An ACM Distinguished Dissertation 1984, The MIT Press, 1985.

Bedocchi, 1985:

Edmondo Bedocchi Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma (4) **11** *(1985), 229–236.*

References (Ben-Bure)

Bender, 1974:

Edward A. Bender, Partitions of multisets, Disc. Math. **9** *(1974), 301–311.*

Borwein, Maitland, and Skerritt, 2013:

Jonathan Borwein, Christopher Maitland, and Matthew Skerritt, Computation of an improved lower bound to Giuga's primality conjecture, INTEGERS **13** *(2013), A67, 14 pages.*

Burek and Żmija, 2016:

Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, Int. J. Number Theory **15** *(2016), 1463–1468.*

References (Ben-Bure)

Bender, 1974:

Edward A. Bender, Partitions of multisets, Disc. Math. **9** *(1974), 301–311.*

Borwein, Maitland, and Skerritt, 2013:

Jonathan Borwein, Christopher Maitland, and Matthew Skerritt, Computation of an improved lower bound to Giuga's primality conjecture, INTEGERS **13** *(2013), A67, 14 pages.*

Burek and Żmija, 2016:

Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, Int. J. Number Theory **15** *(2016), 1463–1468.*

References (Ben-Bure)

Bender, 1974:

Edward A. Bender, Partitions of multisets, Disc. Math. **9** *(1974), 301–311.*

Borwein, Maitland, and Skerritt, 2013:

Jonathan Borwein, Christopher Maitland, and Matthew Skerritt, Computation of an improved lower bound to Giuga's primality conjecture, INTEGERS **13** *(2013), A67, 14 pages.*

Burek and Żmija, 2016:

Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, Int. J. Number Theory **15** *(2016), 1463–1468.*

References (Ben-Bure)

Bender, 1974:

Edward A. Bender, Partitions of multisets, Disc. Math. **9** *(1974), 301–311.*

Borwein, Maitland, and Skerritt, 2013:

Jonathan Borwein, Christopher Maitland, and Matthew Skerritt, Computation of an improved lower bound to Giuga's primality conjecture, INTEGERS **13** *(2013), A67, 14 pages.*

Burek and Żmija, 2016:

Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, Int. J. Number Theory **15** *(2016), 1463–1468.*

References (Ben-Bure)

Bender, 1974:

Edward A. Bender, Partitions of multisets, Disc. Math. **9** *(1974), 301–311.*

Borwein, Maitland, and Skerritt, 2013:

Jonathan Borwein, Christopher Maitland, and Matthew Skerritt, Computation of an improved lower bound to Giuga's primality conjecture, INTEGERS **13** *(2013), A67, 14 pages.*

Burek and Żmija, 2016:

Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, Int. J. Number Theory **15** *(2016), 1463–1468.*

References (Ben-Bure)

Bender, 1974:

Edward A. Bender, Partitions of multisets, Disc. Math. **9** *(1974), 301–311.*

Borwein, Maitland, and Skerritt, 2013:

Jonathan Borwein, Christopher Maitland, and Matthew Skerritt, Computation of an improved lower bound to Giuga's primality conjecture, INTEGERS **13** *(2013), A67, 14 pages.*

Burek and Żmija, 2016:

Dominik Burek and Błażej Żmija, A new upper bound for numbers with the Lehmer property and its application to repunit numbers, Int. J. Number Theory **15** *(2016), 1463–1468.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (Burt-C)

Burthe, 1997:

Ronald Joseph Burthe Jr. Upper bounds for least witnesses and generating sets, Acta Arith. **35** *(1997), 311–326.*

Canfield, Erdős, and Pomerance, 1983:

E. R. Canfield, P. Erdős, and C. Pomerance, On a problem of Oppenheim concerning "Factorisatio Numerorum", J. Number Theory **17** *(1983), 1–28.*

Crandall and Pomerance, 2005:

Richard Crandall and Carl Pomerance, Prime Numbers. A Computational Perspective, 2nd ed. Springer, New York, 2005.

Cohen and Hagis 1980:

G. L. Cohen and P. Hagis Jr., On the number of prime factors of n if $\varphi(n) \mid (n-1)$, Nieuw Arch. Wisk. (3) **28** *(1980), 177–185.*

References (E-G)

EGPS, 1990:

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, 1990, 165–204.

Giuga, 1950:

Giuseppe Giuga, Su una presumibile proprietá caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3) **14 (83)** *(1950), 511–528.*

Grau and Oller-Marcén, 2012:

José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, Integers **12** *(2012), #A37.*

References (E-G)

EGPS, 1990:

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, 1990, 165–204.

Giuga, 1950:

Giuseppe Giuga, Su una presumibile proprietá caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3) **14 (83)** *(1950), 511–528.*

Grau and Oller-Marcén, 2012:

José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, Integers **12** *(2012), #A37.*

References (E-G)

EGPS, 1990:

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, 1990, 165–204.

Giuga, 1950:

Giuseppe Giuga, Su una presumibile proprietá caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3) **14 (83)** *(1950), 511–528.*

Grau and Oller-Marcén, 2012:

José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, Integers **12** *(2012), #A37.*

References (E-G)

EGPS, 1990:

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, 1990, 165–204.

Giuga, 1950:

Giuseppe Giuga, Su una presumibile proprietá caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3) **14 (83)** *(1950), 511–528.*

Grau and Oller-Marcén, 2012:

José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, Integers **12** *(2012), #A37.*

References (E-G)

EGPS, 1990:

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, 1990, 165–204.

Giuga, 1950:

Giuseppe Giuga, Su una presumibile proprietá caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3) **14 (83)** *(1950), 511–528.*

Grau and Oller-Marcén, 2012:

José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, Integers **12** *(2012), #A37.*

References (E-G)

EGPS, 1990:

P. Erdős, A. Granville, C. Pomerance, and C. Spiro, On the normal behavior of the iterates of some arithmetic functions, Analytic Number Theory, Proceedings of a Conference in Honor of Paul T. Bateman, Birkhäuser, 1990, 165–204.

Giuga, 1950:

Giuseppe Giuga, Su una presumibile proprietá caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3) **14 (83)** *(1950), 511–528.*

Grau and Oller-Marcén, 2012:

José María Grau and Antonio M. Oller-Marcén, On k-Lehmer numbers, Integers **12** *(2012), #A37.*

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. ***69*** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, https://aimath.org/WWN/primesinp/articles/html/50a/

References (H-Le)

Hardy-Wright:

G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 6th edition, revised by D. R. Heath-Brown and J. H. Silverman, Oxford University Press, 2008.

Howe, 2000:

Everett W. Howe, Higher-ordeer Carmichael Numbers, Math. Comp. **69** *(2000), 1711–1719.*

Lehmer, 1932:

D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. **38** *(1932), 745–751.*

Lenstra and Pomerance, 2003:

Remarks on Agrawal's Conjecture, `https://aimath.org/WWN/primesinp/articles/html/50a/`

References (Li-Mc)

Lidl, Müller, Oswald, 1990:

Rudolf Lidl, Winfried B. Müller, and Alan Oswald, Some remarks on strong Fibonacci pseudoprimes, Appl. Alg. Eng. Comm. Comput. **1** *(1990), 59–65.*

Luca and Pomerance, 2011:

Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (3) **17** *(2011), 13–21.*

McNew, 2013:

Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, Int. J. Number Theory **9** *(2013), 1215–1224.*

References (Li-Mc)

Lidl, Müller, Oswald, 1990:

Rudolf Lidl, Winfried B. Müller, and Alan Oswald, Some remarks on strong Fibonacci pseudoprimes, Appl. Alg. Eng. Comm. Comput. **1** *(1990), 59–65.*

Luca and Pomerance, 2011:

Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (3) **17** *(2011), 13–21.*

McNew, 2013:

Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, Int. J. Number Theory **9** *(2013), 1215–1224.*

References (Li-Mc)

Lidl, Müller, Oswald, 1990:

Rudolf Lidl, Winfried B. Müller, and Alan Oswald, Some remarks on strong Fibonacci pseudoprimes, Appl. Alg. Eng. Comm. Comput. **1** *(1990), 59–65.*

Luca and Pomerance, 2011:

Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (3) **17** *(2011), 13–21.*

McNew, 2013:

Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, Int. J. Number Theory **9** *(2013), 1215–1224.*

References (Li-Mc)

Lidl, Müller, Oswald, 1990:

Rudolf Lidl, Winfried B. Müller, and Alan Oswald, Some remarks on strong Fibonacci pseudoprimes, Appl. Alg. Eng. Comm. Comput. **1** *(1990), 59–65.*

Luca and Pomerance, 2011:

Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (3) **17** *(2011), 13–21.*

McNew, 2013:

Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, Int. J. Number Theory **9** *(2013), 1215–1224.*

References (Li-Mc)

Lidl, Müller, Oswald, 1990:

Rudolf Lidl, Winfried B. Müller, and Alan Oswald, Some remarks on strong Fibonacci pseudoprimes, Appl. Alg. Eng. Comm. Comput. **1** *(1990), 59–65.*

Luca and Pomerance, 2011:

Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (3) **17** *(2011), 13–21.*

McNew, 2013:

Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, Int. J. Number Theory **9** *(2013), 1215–1224.*

References (Li-Mc)

Lidl, Müller, Oswald, 1990:

Rudolf Lidl, Winfried B. Müller, and Alan Oswald, Some remarks on strong Fibonacci pseudoprimes, Appl. Alg. Eng. Comm. Comput. **1** *(1990), 59–65.*

Luca and Pomerance, 2011:

Florian Luca and Carl Pomerance, On composite integers n for which $\varphi(n) \mid n-1$, Bol. Soc. Mat. Mexicana (3) **17** *(2011), 13–21.*

McNew, 2013:

Nathan McNew, Radically weakening the Lehmer and Carmichael conditions, Int. J. Number Theory **9** *(2013), 1215–1224.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (Mc& W-Mü)

McNew and Wright, 2016:

Nathan McNew and Thomas Wright, Infinitude of k-Lehmer numbers which are not Carmichael, Int. J. Number Theory **12** *(2016), 1863–1869.*

Gary L. Miller, 1976:

Riemann's hypothesis and tests for primality, J. Comput. Sys. Sci. **13** *(1976), 300–317.*

Müller, Oswald, 1991:

Winfried B. Müller, and Alan Oswald, Dickson Pseudoprimes and Primality Testing, in Advances in Cryptology - EUROCRYPT '91, Lecture Notes Comput. Sci. **547**, *512–516.*

Müller, Oswald, 1992:

Generalized Fibonacci pseudoprimes and probable primes, in Applications of Fibonacci Numbers **5** *(1992), Springer Science+Business Media, B. V., 459–464.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n for which $\varphi(n) \mid (n-1)$, II, Pacific J. Math. **69** *(1977), 177–186.*

References (O-Pom)

Oppenheim, 1927:

A. Oppenheim, On an arithmetic function II, J. London Math. Soc. **2** *(1927), 123–130.*

Pinch's research page:

Richard G.E. Pinch, Mathematics research page, `http://www.chalcedon.demon.co.uk/rgep/rcam.html`

Pollard, 1974:

J. M. Pollard, Theorems on factorization and primality testing, Proc. Cambridge Philos. Soc. **76** *(1974), 521–528.*

Pomerance, 1977:

Carl Pomerance, On composites n *for which* $\varphi(n) \mid (n-1)$*, II, Pacific J. Math.* **69** *(1977), 177–186.*

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (Pop-R)

Popovych, 2008:

Roman Popovych, A note on Agrawal conjecture, Cryptology ePrint Archive: `https://eprint.iacr.org/2009/008.pdf`

Rabin, 1980:

Michael O. Rabin, Probabilistic algorithm for testing primality, J. Number Theory **12** *(1980), 128–138.*

Renze's notebook:

John Renze, Computational evidence for Lehmer's totient conjecture, `https://library.wolfram.com/infocenter/MathSource/5483/`

Ribenboim, 1996:

The New Book of Prime Number Records, Springer, 1996.

References (S)

Shanks, 1971:

Class Number, a theory of factorization, and genera, in 1969 Number Theory Institute, Proc. Symp. Pure Math. **20** *(1969), 415–440, Amer. Math. Soc., Providence, R.I., 1971.*

Shor, 1994:

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annual Symposium on Fundation of Computer Science, IEEE Comput. Soc., 1994, 124–134.

Strassen, 1976:

Von Volker Strassen, Einige Resultate über Berechnungskomplexität, Jber. Deutsch. Math.-Verein. **78** *(1976/77), 1–8.*

References (S)

Shanks, 1971:

Class Number, a theory of factorization, and genera, in 1969 Number Theory Institute, Proc. Symp. Pure Math. **20** *(1969), 415–440, Amer. Math. Soc., Providence, R.I., 1971.*

Shor, 1994:

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annual Symposium on Fundation of Computer Science, IEEE Comput. Soc., 1994, 124–134.

Strassen, 1976:

Von Volker Strassen, Einige Resultate über Berechnungskomplexität, Jber. Deutsch. Math.-Verein. **78** *(1976/77), 1–8.*

References (S)

Shanks, 1971:

Class Number, a theory of factorization, and genera, in 1969 Number Theory Institute, Proc. Symp. Pure Math. **20** *(1969), 415–440, Amer. Math. Soc., Providence, R.I., 1971.*

Shor, 1994:

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annual Symposium on Fundation of Computer Science, IEEE Comput. Soc., 1994, 124–134.

Strassen, 1976:

Von Volker Strassen, Einige Resultate über Berechnungskomplexität, Jber. Deutsch. Math.-Verein. **78** *(1976/77), 1–8.*

References (S)

Shanks, 1971:

Class Number, a theory of factorization, and genera, in 1969 Number Theory Institute, Proc. Symp. Pure Math. **20** *(1969), 415–440, Amer. Math. Soc., Providence, R.I., 1971.*

Shor, 1994:

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annual Symposium on Fundation of Computer Science, IEEE Comput. Soc., 1994, 124–134.

Strassen, 1976:

Von Volker Strassen, Einige Resultate über Berechnungskomplexität, Jber. Deutsch. Math.-Verein. **78** *(1976/77), 1–8.*

References (S)

Shanks, 1971:

Class Number, a theory of factorization, and genera, in 1969 Number Theory Institute, Proc. Symp. Pure Math. **20** *(1969), 415–440, Amer. Math. Soc., Providence, R.I., 1971.*

Shor, 1994:

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annual Symposium on Fundation of Computer Science, IEEE Comput. Soc., 1994, 124–134.

Strassen, 1976:

Von Volker Strassen, Einige Resultate über Berechnungskomplexität, Jber. Deutsch. Math.-Verein. **78** *(1976/77), 1–8.*

References (S)

Shanks, 1971:

Class Number, a theory of factorization, and genera, in 1969 Number Theory Institute, Proc. Symp. Pure Math. **20** *(1969), 415–440, Amer. Math. Soc., Providence, R.I., 1971.*

Shor, 1994:

P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, Proc. 35th Annual Symposium on Fundation of Computer Science, IEEE Comput. Soc., 1994, 124–134.

Strassen, 1976:

Von Volker Strassen, Einige Resultate über Berechnungskomplexität, Jber. Deutsch. Math.-Verein. **78** *(1976/77), 1–8.*

MANY THANKS FOR YOUR ATTENTION

Tomohiro Yamada
Center for Japanese language and culture
Osaka University
562-8558
8-1-1, Aomatanihigashi, Minoo, Osaka
Japan
e-mail: tyamada1093@gmail.com