

モジュラス N の因数分解

今泉 克己¹

概要 : 合成数なら $p-1$ で $n-1$ が割れるという Korselt の Criterion を SageMathCell で実装した。概略は次の通りである。

(1) p と q を作る。 $p = \text{random_prime}(2^{1024}-1, \text{False}, 2^{1023})$, q も同様。(2) q が p より大きい場合は p と q を入れ替える。(3) $n-1$ に対する mod 演算を $p-1$ を含む p で行い, 結果を配列に格納し変数名を与える。(4) 上記配列には $q-1$ 続けて $p-1$ が並ぶ。(5) 配列上の mod 演算の結果を x とし $\text{gcd}(n, x+1)$ が 2 以上の場合は x から n の約数が見つかる (n は除外する)。Korselt と Carmichael 数には, 互いに素な素数が 2 つか 3 つ以上かの違いがある。Carmichael 数は 3 つ以上の素数に因数分解できなければならないため Korselt の Criterion とした。 $n+1-\phi(n) = p+q$ を $q =$ に変形し $n = p \cdot q$ に代入し 2 次方程式を解くと p が得られたが, $\phi(n) = (p-1)(q-1)$ の場合に限られ $\text{euler_phi}(n)$ は解が戻らない。素数計数関数も n が大きく振動項があり近似であることなど課題がある。

キーワード : Korselt's Criterion, Carmichael 数, $\text{euler_phi}(n)$, 素数計数関数

Factoring the modulus N

Katsumi Imaizumi¹

Abstract: Korselt's Criterion on SageMathCell. (1) Make p and q with $\text{random_prime}(2^{1024}-1, \text{False}, 2^{1023})$. (2) Make an array like $aa = [n-1 \% (x-1)]$ for x in $\text{range}(p, p+100)$. (3) An array aa contains headed $q-1, p-1$. (4) if $\text{gcd}(n, aa[y]+1) \geq 2$ it is a factor of n (except n). Korselt's Criterion has in minimum two prime numbers. With $\phi(n) = (p-1)(q-1)$, transform $n+1-\phi(n) = p+q$ to $q =$, then substitute $n = p \cdot q$ with q . then solved quadratic equation on p . $\text{euler_phi}(n)$ do not answer because n is large.

Keywords: Korselt's Criterion, Carmichael Number, $\text{euler_phi}(n)$, Prime-Counting Function

1. はじめに

Shor や Grover のアルゴリズムをクラウド上にある量子コンピュータのシミュレータや実機で実行でき, 例えば $15 = 3 \times 5$ といった因数分解や検索の動作をデスクトップ環境からでも web ブラウザを用いてでも試すことができるようになった。確かに実行できたことを確認した後, Post-Quantum Cryptography (PQC) についても調査研究を始めたが, 古典計算での公開鍵暗号の堅牢性について, 改めて確認を行ってみたことが, 本研究の始まりである。

驚くべきことに, 例えばスマートフォンの web ブラウザなどからでも SageMathCell は使うことができる。計算が所定の時間内で終わらなければ, タイムアウトする。その点 OS 上の暗号 API や openssl のように利用者の端末でも現用の公開鍵暗号は計算可能であり経済的とも言える。

2. 計算機実験の概略

$p-1$ で $n-1$ が割れるという Korselt's Criterion を SageMathCell [7][8] 上に実装した。概略は次の通りである。

(1) P と Q を作る

$p = \text{random_prime}(2^{1024}-1, \text{False}, 2^{1023})$ とする。 q も同様。 random_prime の引数については, 2 つ目の引数は, proof が False の場合は $\text{pseudo-primality test}$ を行うが, $\text{proof of primality}$ は得られない。 3 つ目の引数は, 得た素数の lower bound を指定する。もし $\text{proof of primality}$ が必要ならば, Pocklington Test を Coq で別途行うことは可能だが計算時間が必要である。なお $\text{gcd}(p-1, q-1) > 2$ ならば再度 p, q を作り直すことで互いに素とする。 p, q が奇素数なら偶数同士の gcd で, その値は 2 かそれ以上である。

(2) mod 演算を行い配列に格納する

中国の剰余定理 (Chinese remainder theorem) の応用で, $n-1$

¹ 凸版印刷株式会社
Toppan Printing Co., Ltd.

に対する mod 演算を p の前後のある範囲で行い、結果を配列に格納。`print [560 % (x-1) for x in [3,11,17]]` は `[0,0,0]` となる。`print 3*11*17` は 561 となる。1 つ目の処理の 3,11,17 を p の前後の一定の範囲とし、配列として変数名を与える。例えば以下とする。

```
aa=[n-1 % (x-1) for x in range(p,p+100)]
```

なお、上記の 561 を得る CRT の演算例と配列の使い方は、[14]の p122 を参考として得た。

配列 `aa` は、 $(n-1)\%(p-1), (n-1)\%p, (n-1)\%(p+1), \dots$ が格納される。最初と次の配列要素には p, q の大きさを予め整合してあれば ($p > q$ とし、 $p < q$ なら入れ替える)、常に $p-1, q-1$ が格納される。特に数論的な意味はなく単純な計算の結果である。配列 `aa` は処理の都合によって任意の長さとしてよい。

(3) 配列の要素の観察

上記配列はループ駆動で作成しているので、配列要素には p と q の 2 つと残りは式によって出力された値の場合、整数が並ぶ場合があり、整数が並ぶ場合には、 p か q が擬素数だった場合が含まれそうである。しかし当初はそのようなカーマイケル数なども含む処理を行っていたが、最終的には p と q の間に congruence がなく、あらかじめ gcd で p と q を検査するようにした。配列には mod 演算の結果が入っているので、`x[m]` などとして 1 つずつ取り出し、それらと `gcd(n, x[m]+1)` を行い、 x から n の約数が見つかった。

3. 考察

3.1 SageMathCell で行った演算の意味

中国の剰余定理を RSA 暗号[21]に使うことは広く知られているが、Korselt と Carmichael 数には、互いに素な素数が 2 つか 3 つ以上かの違いがある。Carmichael 数は 3 つ以上の素数に因数分解できなければならないため、Korselt's Criterion[4][5]とした。 p あるいは q は素数なら（擬素数でなければ）原始根をもつが、原始根の性質を調べていくと、 pq については剰余群 $(\mathbb{Z}/pq\mathbb{Z})^*$ が巡回群となるか否かという問題が見つかり、巡回群になるとは言えない（巡回群ではない、すなわち原始根を持たない）という結果を [18]から学んだので、記しておく。また[23]では Proposition 2.1.5.に、

Let $GLL(\mathbb{R})$ be the set of invertible elements of $Zorn(\mathbb{R})$. Then $GLL(\mathbb{R})$ is a Moufang loop. という命題と (p23), inverse element, $GLL(\mathbb{Z}/pq\mathbb{Z})$ (p11, p27)が見受けられるので、これらの意味を研究している。なお、演算の結果得られる配列の先頭には、今回の条件では必ず p か q が順に現れる。ただし擬素数を含め 2 因数ではない条件に緩和した場合には、配列の要素の様相は変わると考えている。

3.2 モジュラー

円分体のガロア拡大[19]などの別の方向性も考えてみる

必要がある。[20]では 1.5. Applications of Modular Forms として、10 のモジュラーに関するさまざまな方向性を述べている。[27]では Pomerance, Li の Artin の予想の一般化を漸近公式がない場合の対応として述べ、その他の Artin 予想の拡張として関数体, Carlitz Modules, Drinfeld Modules などを挙げている。[27]の筆者は、[28]でさらに

素数計数関数である $\pi(x)$ についても考察を進める。[39]では p.33 で Hecke と isogeny について、[38]では pp.78-80 で REMARKS ON ISOGENIES としている。[35]では Ch.4, Sec.7 として pp.65-68 に Lattices of Rational Integers, Canonical Basis としている。

3.3 モジュラス N から p, q についてゼロ知識で因数分解できるための条件の考察

Euler の ϕ 関数が 2 通りの方法で計算でき、 n を指数とする SageMathCell であれば `euler_phi(n)` と、`phi(n)=(p-1)*(q-1)` の 2 通りである。モジュラス N からゼロ知識で因数分解できるとすれば、`euler_phi(n)` であるが、悉皆的に計数している場合には、計算がタイムアウトするだけでなく、解が現実的な時間の中で得ることができないことが想定される。

[29]が、素数計数関数を扱っていることを知らなかったが、執筆中に偶然手に取るチャンスを得、中身を読んで驚いている。`euler_phi(n)` が実際の計算で 2048 ビットモジュラスでは解を返せないとすれば、なんらかの数論的な関数を探ることができる。ただしその実際の計算を行う計算機ハードウェアや計算環境とする処理ソフトウェアがどのような実装をしているかは別問題であり、いくつかの処理系で試してみたものの、よく知られた素数計数の記録値を超えるような実装は筆者には見出すことができなかった。

$p+q=n$ の形に式を変形して $n=p*q$ に代入した後に p について 2 次方程式を解くと、 $\phi(n)$ の値が必要なだけ正確に取ればという条件がつくが、 n だけから p と q を求めることができる。実際に $(p-1)*(q-1)$ で得た値では可能であった。また SageMathCell で実際に数値実験したところ、素数を `euler_phi` に与えると p ならば $p-1$ が返り計算は早いと p と q から作成した $n(n=p*q)$ では内部で因数分解しているためか長い n であるほど解は得にくくなる。

4. おわりに

p と q が大きくなるほど、素数の分布は減っていくために、ループする範囲をひろくとらないと p と q を見つけられないし、ちょうど n となる 2 つの素数を見出すことも簡単なことではない。そのため GNFS や楕円曲線を使う方法など考え付くことはおよそ一通り試してはいるのだが、正攻法でどこがもっとも問題になるのかを計算実験を行いながら確認することができた。その上で、どうしても簡単には克服できそうにもない点が、リーマンの素数公式の構成に

は振動項があり、ゼータ関数の零点と深い関係を持っているという点である。Discrete Log の問題から出発し、Dirichlet Character/Eisenstein, Hasse-Weil Zeta (合同ゼータ), Langrands Program, Chebyshev's Bias, Gauss's Primes as Random Walk, といったこれまでの研究を一通り踏査してみたが、納得のいく解決策は見つけられなかった。この点については、一通り上記で見つかる主な文献を確認したあと、[50]を読むとある程度まとまった理解が得やすい。チューリング, PP341-375, コブリッツ, PP484-495, シルヴァーマン, PP493-495, 量子のドラマ/クラドニ図形/モンゴメリ/オドリツコ/ランダウ/ウィグナー/ダイソン, PP493-495 などが記されているが、とりわけマイケル・ベリー [53], P544 の意味での量子カオス (Quantum chaology, not quantum chaos [54]) と自身の論文でベリーは述べている) がこの書物の示す終着駅である。Hasse-Weil Zeta については [48], P.126, Theorem 1.1, [30] の第 8 章から文献をたどることができる。Witt Vector [51] あるいは Witt Ring [49], PP.50-61. については、脱稿直前に気がついた。

GRH が真ならばという仮定がつく計算ソフトウェアは Common Lisp 上に実装されたものなど他にもあるが、計算できる桁数に言語仕様では限界がないと言われていても、搭載メモリや処理系 (およびその実装仕様) の側では現実には限界があることは否定しない。素数を扱う上で桁数や型などに限界があるのは避けたいことなので、Common Lisp 上のある実装を確認したあとに Haskell 上に全桁を処理できるような実装を試み、Haskell を用いて、巨大な (50 万ビット, 150515 桁) の素数を求めるプログラムの投稿 [33] を参考にして現状 5 位の素数 $2^{43112609}-1$ (12,978,189 桁) の桁数が実行した環境では扱えた。Haskell は素数や巨大整数の処理に有用であった。

四元数と八元数についてはまったく研究が足りていない。モノイドを中心に表される絶対数学 [30] や Moufang Loop, quasi-group [26] についても追うことができなかった。今後の研究としたい。[40], p211 では、 N が合成数である (しかも、2つの素数 p, q の積である) ことはすでにわかっているのに、その素数の値がわからないということの安全性の根拠としているという根源的な指摘を行っている。本稿では、乱数で p と q を生成しあたかも知らなかったかのように、モジュラス N から出発して p, q を導きたかったが、それは実現できず、たとえ ROCA [41] のような計算量が大幅に削減できる条件だとしても、現実に SageMathCell や CUI の Sage 上で ROCA の POC コード [42] を実行し確認したが、2048 ビットのモジュラスの因数分解は筆者の環境では行えなかった。執筆途上で RSA の malleability の議論についても気がついて調査しながら執筆したが、Raw RSA is malleable owing to the homomorphic property [43] という指摘がある。しかしそれでも OAEP と PKCS (padding) のあとに、padding oracle attack という攻撃が RSA 暗号標準 PKCS#1

v1.5 に対しても報告 [44] されている。本稿でのべた内容は、 p と q から作成したモジュラス N の因数分解について述べており、とりわけ N は無平方で、 p と q は互いに素である素数である前提の議論に限定した。

謝辞 研究計画を承認し支えてくださった方々、とりわけ 2 度ほど相談に伺いこちらでの発表を勧めて頂いた先生には匿名になってしまい大変申し訳ありませんが、記してここに感謝申し上げます。ありがとうございました。

参考文献

- [1] 武田邦敬, 甲斐博, 野田松太郎, 代数的アルゴリズムに対する量子計算, 数理解析研究所講究録 1335, 2003, p.119-126. <http://www.jssac.org/~mura0/rims-ws/rims02/KKroku/Pdf/117-takeda.pdf>, (参照 2019-08-01)
- [2] 高木剛, 耐量子計算機暗号の標準化動向, 第 19 回情報セキュリティ・シンポジウム, 日本銀行金融研究所情報技術研究センター, 2018. https://www.imes.boj.or.jp/citecs/symp/19/ref4_takagi.pdf, (参照 2019-08-01).
- [3] "Post-Quantum Cryptography Standardization". <https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization>, (参照 2019-08-01).
- [4] "Korselt's Criterion". <http://mathworld.wolfram.com/KorseltsCriterion.html>, (参照 2019-08-01).
- [5] Conrad, K., Carmichael numbers and Korselt's criterion, expository paper (2016), p.1-3. <https://kconrad.math.uconn.edu/blurbs/ugradnumthy/carmichaelkorselt.pdf>, (参照 2019-08-01).
- [6] Borwein, D.; Borwein, J. M.; Borwein, P. B.; and Girgensohn, R., "Giuga's Conjecture on Primality." *Amer. Math. Monthly* **103**, 40-50, 1996. <https://carma.newcastle.edu.au/db90/pdfs/db90-109.00.pdf>, (参照 2019-08-01).
- [7] "Publications Citing SageMath", <http://www.sagemath.org/library-publications.html#CiteSage>, (参照 2019-08-01).
- [8] Stein, W. and Joyner, D., "SAGE: System for Algebra and Geometry Experimentation", *ACM SIGSAM Bulletin*, Vol.39, No. 2, June 2005. <https://dl.acm.org/citation.cfm?id=1101889>, (参照 2019-08-01). http://www.sagemath.org/files/sage_stein2005.pdf, (参照 2019-08-01).
- [9] Wong, D., "How to Backdoor Diffie-Hellman", June 2016. <https://eprint.iacr.org/2016/644.pdf>, (参照 2019-08-01). https://github.com/mimoo/Diffie-Hellman_Backdoor, (参照 2019-08-01).
- [10] Wong, D., "How to Backdoor Diffie-Hellman: quick explanation", <https://www.cryptologie.net/article/360/how-to-backdoor-diffie-hellman-quick-explanation/>, (参照 2019-08-01).
- [11] "coqprime", <https://github.com/they/coqprime>, (参照 2019-08-01).
- [12] Laurent Théry, Guillaume Hanrot. Primality Proving with Elliptic Curves. *TPHOL 2007*, Sep 2007, Kaiserslautern, Germany. pp.319-333. <https://hal.inria.fr/inria-00138382/en>, (参照 2019-08-01).
- [13] "Computational Mathematics with SageMath",

- <http://sagebook.gforge.inria.fr/english.html>,(参照 2019-08-01).
- [14] Zimmermann,P., et al., Computational Mathematics with SageMath, Society for Industrial & Applied Mathematics,December 2018.
<https://epubs.siam.org/doi/10.1137/1.9781611975468>(参照 2019-08-01).
<http://dl.lateralis.org/public/sagebook/sagebook-ba6596d.pdf>,(参照 2019-08-01).
- [15] Witno,A.,” The Primitive Root Theorem”, April 2012.
<http://www.philadelphia.edu.jo/math/witno/250313.htm>,(参照 2019-08-01).
<https://www.philadelphia.edu.jo/math/witno/notes/won5.pdf>,(参照 2019-08-01).
- [16] “Primitive Root”,
<http://mathworld.wolfram.com/PrimitiveRoot.html>,(参照 2019-08-01).
- [17] 桂利行,“R S A 暗号”,高校生のための現代数学講座, 2009 年度「素数の世界」, 東京大学玉原国際セミナーハウス,2009.
<http://www.ms.u-tokyo.ac.jp/tambara/lectures-for-highschool/14h2009.html>,(参照 2019-08-01).
<http://www.ms.u-tokyo.ac.jp/tambara/docs/14h20090731-2katsura.pdf>,(参照 2019-08-01).
- [18] 村田玲音,剰余位数の分布について,明治学院大学経済研究 (145),55-66 (2012-01-31)
<http://econ.meijigakuin.ac.jp/research/publication/pdf/145-4.pdf>,(参照 2019-08-01).
- [19] 上野孝司,“響きあうガロアとガウスー正 17 角形の作図問題 (第 2 版)”,December 2016.
<http://hooktail.org/misc/index.php?%B4%F3%B9%C6>,(参照 2019-08-01).
<http://hooktail.sub.jp/contributions/galoire32160913tu.pdf>,(参照 2019-08-01).
- [20] Stein, W.A., Modular Forms:A Computational Approach., Graduate Studies in Mathematics Volume 79,2007.
<https://bookstore.ams.org/gsm-79/>,(参照 2019-08-01).
<https://wstein.org/books/modform/stein-modform.pdf>(参照 2019-08-01).
- [21] Rivest, R.L., Shamir, A. and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM CACM Homepage archive Volume 21 Issue 2, February 1978,p.120-126.
<https://dl.acm.org/citation.cfm?id=359342>,(参照 2019-08-01).
<https://people.csail.mit.edu/rivest/Rsapaper.pdf>,(参照 2019-08-01).
- [22] Stein, W.A., “Primality Testing”,
<https://wstein.org/edu/2007/spring/ent/ent-html/node26.html>,(参照 2019-08-01).
- [23] Wells, A.,T.,“Zorn vector matrices over commutative rings and the loops arising from their construction” (2010). *Graduate Theses and Dissertations*. 11830.
<https://lib.dr.iastate.edu/etd/11830>,(参照 2019-08-01).
<https://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=2900&context=etd>,(参照 2019-08-01).
- [24] Kinyon, M.,K., Smith, J.,D.,H. and Vojtěchovský, P., “Sylow Theory for Quasigroups II: Sectional Action“, Journal of Combinatorial Designs, Volume25, Issue4, April 2017, P.59-184 First published: 20 September 2016.
<https://doi.org/10.1002/jcd.21535>,(参照 2019-08-01).
<https://cs.du.edu/~mathfiles/preprints/nsm-math-preprint-1607.pdf>,(参照 2019-08-01).
- [25] Siu,Y.,T.,”Prime-Counting Function and Zeros of Riemann Zeta Function”, Math 213a (Fall 2018).
http://www.math.harvard.edu/~siu/math213a/prime_counting_func tion_and_zeros_of_riemann_zeta_function_parts1&2.pdf,(参照 2019-08-01).
- [26] “Algebraic loop 冪 quasigroup”
http://pantodon.shinshu-u.ac.jp/topology/literature/algebraic_loop.html,(参照 2019-08-01).
- [27] Felix, A.,T., Variations on Artin’s primitive root conjecture, Ph.D. thesis, Queen’s University (2011).
https://qspace.library.queensu.ca/bitstream/1974/6635/1/Felix_Adam_T_201108_PhD.pdf,(参照 2019-08-01).
- [28] Felix, A. T., and Murty, M. R.,A problem of Fomenko's related to Artin's conjecture. International Journal of Number Theory, 8(7), p.1687-1723,2012. doi:10.1142/S1793042112500984.
<http://www.cs.uleth.ca/~felix/fomenko.pdf>,(参照 2019-08-01).
- [29] Wiener, N., The Fourier Integral and Certain of Its Applications, Dover.,also available bellow.,especially on p104,Chap.III, SPECIAL TAUBERIAN THEOREMS.
https://books.google.co.jp/books?id=L1U4AAAIAAJ&pg=PA104&lpg=PA104&dq=wiener+the+fourier+integral+and+certain+of+its+applications+Special+tauberian&source=bl&ots=cYK5aHfXoC&sig=ACfU3U3vQIgHPvgKiUZ3MzNaTfv4pJLNUA&hl=ja&sa=X&ved=2ahUKEwiMuLnAmOHjAhXMG6YKHf_6BkQQ6AEwCxoECEUQAQ#v=onepage&q=wiener%20the%20fourier%20integral%20and%20certain%20of%20its%20applications%20Special%20tauberian&f=false,(参照 2019-08-01).
- [30] 黒川信重,小山信也,リーマン予想のこれまでとこれから, December 2009,日本評論社.
- [31] 足立恒雄, フェルマーの大定理,第 3 版,June 1996,日本評論社.
- [32] 小島寛之, 世界は素数でできている, August 2017,角川新書.
- [33] Takusagawa,K.,“[qqcvkken] Million-bit RSA”, January 2019.
<http://kenta.blogspot.com/2019/01/qqcvkken-million-bit-rsa.html>,(参照 2019-08-01).
- [34] “The Coq Proof Assistant”,
<https://coq.inria.fr/>,(参照 2019-08-01).
- [35] Cohn, H.,Advanced Number Theory,1980,Dover.
- [36] Ribenboim, P.,The Little Book of Big Primes, 1991,Springer.
- [37] 足立恒雄, 類体論へ至る道, 1982,日本評論社.
- [38] Birch, B.J. and Kuyk,W. editors., Modular functions of one variable IV, 1975, Springer, Lecture Notes in Mathematics, Vol.,476.
<https://rd.springer.com/book/10.1007/2FBFb0097580>,(参照 2019-08-01).
- [39] Gross,B.,Arithmetic on elliptic curves with complex multiplication,1980, Springer, Lecture Notes in Mathematics, Vol.,776.
<https://rd.springer.com/book/10.1007/BFb0096754caasddsZ>
- [40] 野崎昭弘,「 $P \neq NP$ 」問題 : 現代数学の超難問,ブルーバックス,B-1933, September 2015,講談社.
- [41] Nemeč,M., Sys,M., Svenda,P., Klinec,D., and Matyas,V., The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli, In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17),.pp.1631-1648, 2017.
<https://dl.acm.org/citation.cfm?id=3133969>,(参照 2019-08-01).
https://crocs.fi.muni.cz/_media/public/papers/nemeč_roca_ccs17_p_reprint.pdf,(参照 2019-08-01).
- [42] <https://github.com/brunoproduit/roca/blob/master/src/roca.sage> (参照 2019-08-01).
- [43] Oswald,E., Smart,N., “COMS30124 : Making and Breaking RSA”,http://resist.isti.cnr.it/free_slides/cryptography/oswald/Part_V.pdf,(参照 2019-08-01).
- [44] Bardou, R., Focardi, R., Kawamoto, Y., Simionato,L., Steel G.,and Tsay, J.K.,暗号ハードウェアに対する効率的なパディングオ

- ラケル攻撃,2013年 暗号と情報セキュリティシンポジウム (SCIS 2013) January, 2013.
<https://researchmap.jp/mu17ed99n-1781481/>, (参照 2019-08-01).
- [45] “リーマンの素数公式を可視化する”,
<http://tsujimotter.hatenablog.com/entry/2014/06/29/002109>, (参照 2019-08-19).
- [46] Gidney,C., Ekerå ,M.,“How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”, May 2019.
<https://arxiv.org/pdf/1905.09749.pdf>, (参照 2019-08-19).
- [47] Henry,R.,Goldberg,I.,”Solving Discrete Logarithms in Smooth-Order Groups with CUDA”,In the 5th Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems (SHARCS 2012), March 2012 (Washington, DC).,
<http://homes.sice.indiana.edu/henry/publications/sharcs12.pdf>, (参照 2019-08-19).
- [48] Koblitz,N., Algebraic Aspects of Cryptography,1998,Springer.
<https://rd.springer.com/book/10.1007%2F978-3-662-03642-6>, (参照 2019-08-19).
- [49] Demazure,M., Lectures on p-Divisible Groups,1972,Springer.
<https://rd.springer.com/book/10.1007%2FBFB0060741> (参照 2019-08-19).
- [50] マーカス・デュ・ソーテイ,素数の音楽,Oct 2013,新潮社.
- [51] Bourgeois,G., Faugère,J.,C., “Algebraic attack on NTRU using Witt vectors and Gröbner bases”, Journal of Mathematical Cryptology, 3(3), pp. 205-214, doi:10.1515/JMC.2009.011, (参照 2019-08-19).,
<https://www.degruyter.com/view/j/jmc.2009.3.issue-3/jmc.2009.011/jmc.2009.011.xml>, (参照 2019-08-19).
- [52] Lattore,J.,I.,Sierra,G.,” There is entanglement in the primes”, Quant.Inf.Comput..15 (2015),622-676.,arXiv:1403.4765v2 [quant-ph].
<http://arxiv.org/abs/arXiv:1403.4765>, (参照 2019-08-21).
<https://arxiv.org/pdf/1403.4765.pdf>, (参照 2019-08-21).
- [53] Berry,M.,V.,” Hearing the music of the primes: auditory complementarity and the siren song of zeta”,2012, J. Phys. A 45, 382001.
<https://michaelberryphysics.files.wordpress.com/2013/06/berry454.zip>, (参照 2019-08-21).
<https://www.semanticscholar.org/paper/Hearing-the-music-of-the-primes%3A-auditory-and-the-Berry/a98a22daed846dfa2a9bf5027d52b38b8de9e619>, (参照 2019-08-21).
- [54] Berry,M.,V.,” Quantum chaology, not quantum chaos”,Physica Scripta, Vol.40,Number 3.1989.
<https://iopscience.iop.org/article/10.1088/0031-8949/40/3/013/meta>, (参照 2019-08-21).