International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

Theoretical concept of algebraic number theory in particular area

[1]Rupen Chatterjee, [2]Dr Sonal Bharti

[1]*Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, (India)*

ABSTRACT

Algebra is one of the broad parts of mathematics, together with number theory, geometry and analysis.As such, it includes everything from elementary equation solving to the study of abstractions such as groups, rings, and fields. The word algebra is also used in certain specialized ways. A special kind of mathematical object in abstract algebra is called an "algebra", and the word is used, for example, in the phrases linear algebra and algebraic topology. Inthis paper, we discuss primality testingmethods involve arithmetic which are best understood in the context of algebraic number theory.

I INTRODUCTION

Primality testing of large numbers is *very* important in many areas of mathematics, computer science and cryptography. For example, in public-key cryptography, if we can find two large primes p and q, each with 100 digits or more, then we can get a composite

$$n = p * q$$

with 200 digits or more. This composite n can be used to encode a message securely even when n is made public (we call n a *public-key).* The message cannot be decoded without knowledge of the prime factors of n. Of course, we can try to use a modern integer factorization method such as the Elliptic Curve Method to factor n and to get its prime factors p and q, but it would take about 20 million years to complete the job even on a supercomputer. Thus, it is practically impossible to decode the message. Another good example is the searching for amicable numbers. In the following algebraic method for generating amicable numbers,if we can make sure thatthe following four integers p, q, r, s

$p=2^x*g-1$

$q = 2^y + (2^{n+1} - 1) * g$ where $0<x<n$

$r= 2^{n-y}*g*q-1$ $g=2^{n-x}+1$

$S =2^{n-y+x}* g2 * q - 1$ $0<y<n$

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

are all primes, then the pair(m, n) = $(2^n qpr, 2^n qs)$
is an amicable pair. Thus, searching for amicable numbers is often the same as the primalitytesting of some related integers.

Primality testing is one of the oldest problems as well as open problems in mathematics, which goes back to the ancient Greeks about 2000 years ago. The problem can be simply described as follows:

Input: n (n ∈ Natural Numbers and n > 1).

Output: { Yes, if n ∈ Primes,
No, ifn ∈ Composites.

Unfortunately, it is not a simple matter to determine whether or not a random integer *n* is prime,particularly when n is very large. An efficient algorithm for primality testing from the complexitypoint of view would have to run in $O(\log^k n)$ steps, for some fixed *k*. But unfortunately, no such *deterministic* algorithm exists for random integer n, although, for example, Miller [2] showed that n can be checked in $O(\log^5 n)$ steps, assuming the truth of the unproved Extended Riemann Hypothesis (ERH). Recently, many of the modern primality testing algorithms have been incorporated in Computer Algebra Systems (CAS) such as Axiom and Maple (see [3,4] for a reference) as a standard. In this paper, we shall discuss primality testing of large numbers in Maple.

II STRONG PSEUDOPRIMALITY TESTS AND LUCAS TESTS

In this section, we introduce some basic concepts and ideas of probable primes, pseudo primesand pseudoprimality tests, which will be used throughout the paper.

THEOREM 1. (FERMAT'S THEOREM) Ifp is prime and gcd(a,p) = 1, *then*

$$a^{p-1} \equiv 1 (\mathrm{mod} p).$$

Most modern primality testing algorithms depend in some way on the converse (an immediate corollary) of Fermat's Theorem.

COROLLARY 1. (CONVERTE OF FERMAT'S THEOREM-FERMAT TEST) *Let n be an odd positive integer*. Ifgcd(a, n) = 1 *and* then n is composite.

$$a^{n-1} \neq 1 \pmod{n},$$

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

By Corollary 1, we know that if there exists on a with $1 < a < n$, gcd (a, n) = 1 and $a^{n-1} \neq 1 \pmod{n}$, then n must be composite. What happens if we find a number *n* such that $a^{n-1} \equiv \pmod{n-1}$? Can we conclude that n is certainly a prime? The answer is unfortunately not, because n sometimes is indeed a prime, but sometimes is not! This leads to the following important concepts of probable primes and pseudo primes.

DEFINITION 1. If $a^{n-1} \equiv 1 \pmod{n}$, then we call n a (Fermat) probable prime to the base a. A(Fermat) probable prime n to the base a is called a (Fermat) pseudoprime to the base a if n is composite.
For example, $2^{1387-1} \equiv 1 \pmod{1387}$. Thus, 1387 is a Fermat probable prime to the base 2. But since 1387 = 19 * 73 is composite, then it is Fermat pseudoprime to the base 2. A further and immediate improvement over the Fermat test is the strong pseudoprimality test (often called the Miller-Rabin test, or just the strong test). We describe it in the following algorithmic form.

ALGORITHM 1. ***(Strong Pseudoprimality Test)***

[S1] Let n be an odd number, and the base a be a random number in the range $1 < a < n$. Find
j and d with d odd, so that $n - 1 = 2^j d$.

[S2]Compute a d (modn). Ira a (modn) - ±1 (modn), then n is a strong probable prime andoutput "Yes"; stop.

[S3]Square a^d to compute $a^{2d} \pmod{n}$. If $a^{2d} \pmod{n} \equiv 1 \pmod{n}$, then n is composite andoutput "No"; stop. If $a^{2d} \pmod{n} = -1 \pmod{n}$, then n is a strong probable prime and output "Yes"; stop.

[S4]Repeat step S3 with a^{2d} replaced by

$$a^{4d}, a^{8d}, \ldots\ldots, a^{2i-1d}$$

(Note that the sequence is often called the Miller-Rabin sequence.)

$$a^d, a^{2d}, a^{4d}, a^{8d}, \ldots\ldots, a^{2i-1d}$$

[S5] If the procedure has not alreadyterminated, then n is composite and output "No".

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

DEFINITION 2. A positive integer n with n - 1 = d *2^j and *d* odd, is called a strong probableprime to the base *a* if it passes the strong pseudoprimality test described above (i.e., the lastterm in the Miller-Rabin sequence is 1, and the first occurrence of 1either is the first term or ispreceded by -1). A strong probable prime to the base a is called a strong pseudoprime to thebase *a* if it is a composite.

Although very few composites can pass the strong pseudoprimality test, the test itself is notdeterministic, but probabilistic. For example, the composite n = 2047 23 * 89 can pass the strong pseudoprimality test, because n -1 =2^1* 1023, d = 1023 and the Miller-Rabin sequence is $2^{1023}\equiv$l(mod2047), $2^{2046}\equiv$ l(mod2047). So n = 2047 is a *strong pseudoprime to the base 2.*Thus, we cannot conclude that n is prime just by a strong primality test, we will need some other tests as well. One of the other tests is the Lucas (pseudoprimality) test. Noted that there is a special Lucas test (often called *Lucas-Lehmer test)* for Mersenne primes, based on the following theorem.

THEOREM 2. (LUCAS-LEHMER TEST FOR MERSENNE PRIMES) *Let p be an odd prime. Define*the *Lucas sequence* {U_k} *by*

$$\begin{cases} U_0 = 4, \\ U_{k+1} \equiv (U_k^2 - 2) (\mathrm{mod}\, 2^p - 1). \end{cases}$$

Then 2^p - 1 is *prime if and only if* $U_{p-2}\equiv 0$ (mod2^p-1).

For example, suppose we wish to test the primality of 2^7-1. We first compute the Lucassequence {U_k} for 2^7-1 (k = 0, 1 . . . . , p-2 = 5):

Since $U_{p-2}\equiv$0(mod 2^p-1), then 2^7-1 is a prime.

The Lucas test we are interested in here is a more general one. It is an analog of Fermat's theorem for Lucas sequences (see [5] or [6] for a reference).

III PRIMALITY TEST

Maple is a very powerful computer algebra system developed by the Symbolic ComputationGroup at the University of Waterloo and the Institute for Scientific Computing at ETH Zurich. It can manipulate mathematical formulas following the rules of number theory, algebra, geometry, trigonometry, calculus and combinatory. In this section, we are only concerned with the primality test facility in the number theory package of Maple.For example, Pinch at Cambridge [4] tested the numbers in the followinglist y_0 (the first two are Fermat pseudoprimes to the base 2 and the other three axe Carmichaelnumbers):

2152302898747 = 6763 * 10627 * 29947
3474749660383 = 1303 *16927*157543
10710604680091 = 3739 *18691 * 153259
4498414682539051 = 46411 * 232051 * 417691
6830509209595831 = 21319 * 106591 * 3005839

and found that they all can pass the isprime test. That is, Maple declares the above five *composites* to be *prime.* But starting from Maple V Release 3, the isprime test uses a combination of a strong pseudoprimality test and a Lucas test. It is much more powerful and reliable than that in Maple. We tested the five numbers in $y_0$by Maple V Release 3, and found that they cannot pass the isprime test. That is, Maple this time declares the five numbers in y_0 to be composite. As we can see, these numbers are indeed composites, so Maple V Release 3 provides a powerful and reliable approach to the primality test of large numbers.

As mentioned previously; primality testing is a very important operation in searching for amicablenumbers. In a research project on algebraic methods for generating amicable numbers, we have tested three other lists of integers by using the isprime test.

List y_1: Four integers

9288811670405087
145135534866431
313887523966328699903,
455562336787531090452868968512225 27

of p, q, r, s in [1], which generate a new 65-digit amicable pair.

List y_2: 204 integers (see Table 1 in the Appendix) of sixty-eight q, r, s in [11], which generate 68 new large amicable pairs in the 101-122 digit range.

List y_3: Two large 520-digit numbers in [1]

663228553696362109159972051763094684878515990025827353794913905891233290295650_
927164926978078060090008525720971052844194832159866585480713665440902566137427_
066765868827283517939906880431444760818325701672601612024082063487549161697774_
311098436355751715192728637914964348021736278380458303306889299215069309626816_
895201720064738466242877284877638913974106333092215777113364013087483467835695_

*807181754057979471754499144424268957636699060565069202221342263517860285324742_*
923787244296559321526732594386295225522814233907635 1
63274027537892248870181532571417551479496481604059440479935784835126423652640 6_
84528853209002046760281836110112109830416525616015566757905308825067159032230 9_
05755382478644380057820321621487261590967609920694588506018487935727432264499 7_
25424895671478443153848618214154353878300862962156645155092741940774066030448 4_
94502770969677343468753448599526600413485703614810508635450358453899721762146 8_
32745708300340374274713057175105182910078121476677750485567871529434817703395 4_
74581470789757327941332379943242703119819654070271 99

which generates the largest amicable pair with 1041 digits found by HolgerWiethaus inWest Germany.

All the 210 numbers in lists y1, y2, and y3 are found to be prime on Maple. Thetesting only takes about half hour on a parallel Silicon Graphics R4D/340S computer in the University of York Computing Centre. Notice that I have also tested these 210 numbers to be prime in Maple V Release 2 in 1993. As suggested by Bradley Lucier at Purdue University, I have confirmed that all the numbers in y1 and y2 are indeed prime on a Silicon Graphics R4D/340Scomputer in the University of York Computing Centre, by using a deterministic *elliptic curvetest* algorithm ECPP (Elliptic Curve Primality Proving) developed by Atkin and Morain [9]. Asfor the primality of the two large 520-digit numbers in list y3, the confirmation was actuallycompleted by F. Morain in France by using a new version of his ECPP program.

The biggest number we have tested on Maple V Release 3 is a 564-digit prime factor of the11^{th} Fermat number F_{11}:

173462447179147555430258970864309778377421844723664084649347019061363579192879_
108857591038330408837177983810868451546421940712978306134189864280826014542758_
708589243873685563973118948869399158545506611147420216132557017260564139394366_
945793220968665108959685482705388072645828554151936401912464931182546092879815_
733057795573358504982279280090942872567591518912118622751714319229788100979251_
036035496917279912663527358783236647193154777091427745377038294584918917590325_
110939381322486044298573971650711059244462177542540706913047034664643603491382_
441723306598834177

The test only takes about 6 minutes of CPU time on a Silicon Graphics R4D/340S machine.Since no counterexample has been found for the isprime test in Maple V Release 3, we can have the following much stronger definition and result for probable primes.

International Journal of Advance Research in Science and Engineering
Volume No.06, Special Issue No.(01), December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

DEFINITION 4. Let n be a positive integer and n > 1. If n passes the isprimetest in Maple VRelease 3, then n is called a Maple probable prime.

IV CONCLUSION

Inthis paper, we discussedprimality testing methods involve arithmetic which are best understood in the context of algebraic number theory.Since the primality testingfacility isprime in Maple V Release 3 is based on a combined use of a strong pseudoprimality test and a Lucas test, it is a very efficient and reliable test for large numbers. No composite has been found that can pass the isprime test in Maple V Release 3. Our computation experience shows that the Maple primality test results are exactly the same as that obtained by the deterministic elliptic curve test in ECPP. This proves, at least from a practical point of view, that the isprimetest in Maple V Release 3 is reliable. Our experience also shows that the Maple primality test is always far more efficient than ECPP, particularly for large numbers. For example, to test the two large 520-digit numbers in *y*3, Maple only needs a few minutes of CPU time on a Silicon Graphics R4D/340S computer, but ECPP will need several hours. But of course, we usually need to use an elliptic curve test or some other deterministic tests to confirm the results obtained by the Maple test. So we are finally approaching to a more practical and realistic primality test for large numbers (assume *n* is the integer to be tested):

$$\xrightarrow{\text{Maple test}} \begin{cases} n \text{ is composite (100\% correct)} \\ n \text{ is prime (error} \ll 10^{-15}) \end{cases} \xrightarrow{\text{ECPP test}} \begin{cases} n \text{ is composite (100\% correct)} \\ n \text{ is prime (100\% correct)} \end{cases}$$

REFERENCES

1. S.Y. Yan and T.H. Jackson, A new large amicable pair, *Computers Math. Applic.* 27 (6), 1 3 (1994).

2. G.L. Miller, Riemann's hypothesis and tests for primality, *Journal of Computer and System Science* 13, 300-317 (1976).

3. J.H. Davenport, Primality testing revisited, In *Proceedings of International Symposium of Symbolic and Algebraic Computations*, ACM Press, 123-129, (1992).

4. R.G.E. Pinch, Some primality testing algorithms, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, (June 24, 1993).

5. I. Niven, H.S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth edition,John Wiley & Sons, (1991).

6. H. Reisel, *Prime Numbers and Computer Methods for Factorization*, Birkh~user, (1990).

7. R.J. Baillie and S.S. Wagstatf, Jr., Lucas pseudoprimes, *Mathematics of Computation* 35, 1391-1417 (1980).

8. C. Pomerance, J.L. Selfridge and S.S. Wagstaff, Jr., The pseudoprimes to 25.109, *Mathematics of Computation* 35, 1003-1026 (1980).

9. A.O.L. Atkin and F. Morain, Elliptic curves and primality proving, Department of Mathematics, University of Illinois at Chicago, (1991).

10. D.E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*, 2nd edition, Addison-Wesley, (1981).

11. S.Y. Yan, 68 new large amicable pairs, *Computers Math. Applic.* 28 (5), 71-74 (1994).