Methods of finding n-th roots of integers and their connection with Cryptography.

by
S. A. Katre
Bhaskaracharya Pratishthana, Pune
Formerly, Savitribai Phule Pune University, Pune

Methods of finding n-th roots of integers and their connection with cryptography

Prof. S. A. Katre

Bhaskaracharya Pratishthana, Pune

Formerly, Savitribai Phule Pune University

Society of Indian Academic in America (SIAA)

Webinar Series 2020-2023

Talk by Prof. S. A. Katre

(20th August 2023 Time 8 pm-9 pm IST, 10.30 am (New York Time)

- Topic: Methods of finding n-th roots of integers and their connection with Cryptography.

Abstract: Aryabhata in his Ganitapada written in 499 AD, gives a systematic method of finding square root and cube root of a given perfect square or a perfect cube. This method is amenable to generalization to finding n-th root. The Indian Human Computer Shakuntaladevi, while finding 23rd root of a 201-digit number apparently used a method which relates to modular arithmetic used in RSA-Cryptography. We shall discuss these methods in the talk.

Society of Indian Academics in America (SIAA)

SIAA Webinar

24 July 2022, Sunday

8 pm - 9 pm IST
(10.30 am New York)

1. Method of Aryabhata of finding n-th roots
2. Shakuntala Devi and her method of finding n-th roots of perfect powers
3. Connection with Cryptography

About the Speaker:

- Prof. S. A. Katre is a retired Professor of Mathematics from Savitribai Phule Pune University, Pune, India. From 2018-23 he was Lokmanya Tilak Chair Professor at S. P. Pune University.
- He is associated with the Mathematics Institution in Pune named Bhaskaracharya Pratishthana

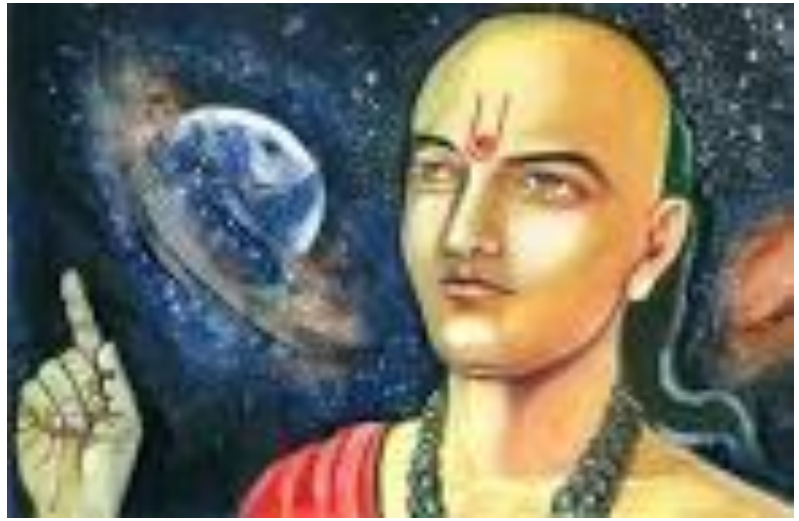
and also with some Mathematical Societies in India viz. The Mathematics Consortium, Indian Academy of Industrial and Applicable Mathematics, Indian Society for History of Mathematics as an office bearer.

Ancient Indian Mathematicians

- Aryabhata (476-550 CE),
- Bhaskaracharya I (c 600-c. 680)
- Mahaveeracharya
- Sridharacharya
- Jayadeva
- Sripati
- Bhaskaracharya II (1114-1185)
- Madhavacharya

See the statue of Aryabhat at IUCAA, Pune

Aryabhata's method of finding square root



- In 499 AD, Aryabhata wrote a book now called Aryabhatiya. It have 4 parts.

The 2nd part is called Ganitapada.

It has 33 verses. Verse 4 deals with finding A square root of a perfect square. The method of Aryabhata used the identity $(a+b)^2 = a^2 + 2ab + b^2$ in an effective way and Aryabhata also uses the power of decimal system to do the calculations involving the digits in the square root.

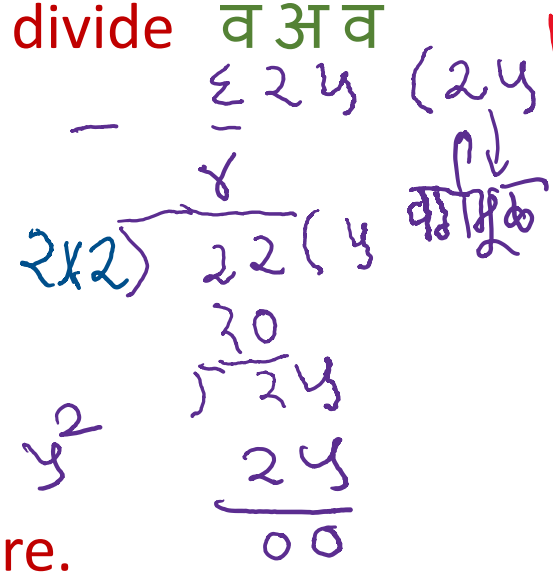
वर्गमूळ साधणे Taking the square root

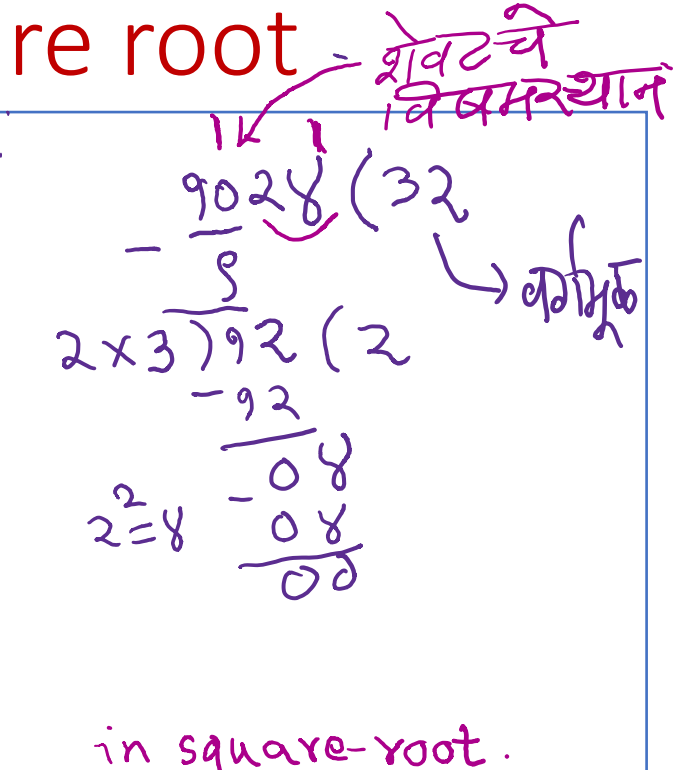
भागं हरेदवर्गान्नित्यं From अवर्ग-place, divide व अ व

द्विगुणेन वर्गमूलेन |by 2x `sqrt'

वर्गाद्वर्गे शुद्धे From वर्ग-place subtract वर्ग

लब्धं स्थानान्तरे मूलम् ॥४॥





When remender is 0, get sqrt elsewhere.

in square-root.

अवर्गात् नित्यं द्विगुणेन वर्गमूलेन भागं हरेत् |

वर्गमूलेन = by square root so far available at the “square root place”

वर्गात् वर्गे शुद्धे, लब्धं स्थानान्तरे मूलम् |

In the above problem there are 2 वर्ग स्थान, so 2 digits in the square root.

Aryabhata's algorithm for square root

- After subtracting the largest square from the last odd place, write its square root at the square root place.
- Always divide the right-hand even place by twice the `square root available', and get the remainder. Then subtract the square of the resulting quotient from the odd place on the right side and place the quotient at the square root place to the right.
- Now this is the square root. If there are more digits left, then the same process should be continued. For division, always use the square root obtained at the square root place.
- Odd space = Square space, Even space = Non-square space

The Recursion of Aryabhata

- शेवटल्या विषम स्थानांतून सर्वांत मोठा वर्ग वजा केल्यावर वर्ग मूळाच्या जागी त्या वर्गाचे मूळ लिहून नेहमी उजव्या बाजूकडील सम स्थानाला (उपलब्ध) वर्गमुळाच्या दुपटीने भागावे.
- मग आलेल्या भागाकाराचा वर्ग उजव्या बाजूकडील विषम स्थानांतून वजा करून तो भागाकार वर्गमुळाच्या जवळ उजवीकडे मांडावा.
- आता हे वर्गमूळ आहे.
- अजून अंक उरले असतील तर हीच क्रिया चालू ठेवावी. भागाकारासाठी वर्गमुळाच्या ठिकाणी असलेले वर्गमूळ वापरावे.
- विषम स्थान = वर्ग स्थान, सम स्थान =अवर्ग स्थान

No. of digits in a square root

- Number of digits in a square root would be the number of वर्ग स्थान or square places.
- A number of 5 digits has 3 square places.
- A number of 6 digits has 3 square places and a number of 4 digits has 2 square places.
- A number with 2n or 2n-1 digits has n square places and has n digits in the square root.

वर्गमूळ काढण्याचे उदाहरण Finding square root

```
                व अ व अ व
               )५ ४ ७ ५ ६(२ ३ ४ वर्गमूळ
२^२             ४
                 --
 २x २=  ४) १  ४  (३
 २x २x३    १  २
           ----
             २  ७  --→
```

[3 square places, so 3 digits in the square root.]

```
 --→                २  ७
३^२                   ९
२  x २३       ४६)१  ८  ५ ( ४
२  x २३x४          १  ८  ४
                   ----------
                      १  ६
४^२                   १  ६
                      ----
                         ०
```

If you know 23^2=529, you could directly subtract 529 from the 2nd वर्ग place and go ahead.

वर्गमूळ काढण्याचे उदाहरण Example of square root

उदाहरण: ५४७५६ या संख्येचे वर्गमूळ काढा. (विषम स्थाने ५ - ७ - ६ = वर्ग स्थान)

व अ व अ व

) ५ ४ ७ ५ ६(२ ३ ४ वर्गमूळ

२^२ ४ a b c

२x २= ४) १ ४ (३ = b

२x २x3 १ २

---

२ ७

३^ २ ९

२ x २३ ४६)१ ८ ५ (४ = c

२ x २३ x ४ १ ८ ४

---

१ ६

४^ २ १ ६

From वर्ग subtract a^2

From अवर्ग Divide by 2a & get b

In the division process 2axb is subtracted.

subtract b^2

Divide by 2ab to get c

In the division process 2(ab)xc is subtracted.

Subtract c^2. Squareroot is abc.

Since there are 3 वर्ग स्थान, the square root has 3 digits.

Patiganit: वर्गमूळ काढण्याचे उदाहरण Finding square root

व अ व अ व

)५ ४ ७ ५ ६(२ ३ ४ वर्गमूळ

२^२ ४

२x २= ४) १ ४ (३

१ २

---

२ ७ --→

3 square places, so 3 digits in the square root.

पाटीगणित

Put the remainder in the original place everytime to save space.

--→ २ ७

३^२ ९

२ x २३ ४६)१ ८ ५ (४

१ ८ ४

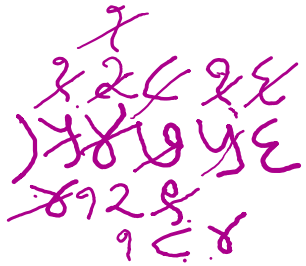
---

१ ६

४^२ १ ६

---

४ ६)५४७५६ (२३४ ०



Aryabhata's formula and recurrence

- $(a+b)^2 = a^2+2ab+b^2$
- $(a+b+c)^2 = a^2+2ab+b^2+2(a+b)c+c^2$
- $(a+b+c+d)^2$

$= a^2+2ab+b^2+2(a+b)c+c^2$

$+2(a+b+c)d+d^2$

- $(a+b+c+d+e)^2$

$= a^2+2ab+b^2+2(a+b)c+c^2$

$+2(a+b+c)d+d^2+2(a+b+c+d)e+e^2$

- If the square root has 5 digits, a,b,c,d,e, from the given cube N Aryabhata is systematically subtracting from appropriate places

$(a+b)^2$, $(a+b+c)^2$, $(a+b+c+d)^2$,

and finally $(a+b+c+d+e)^2$

to get remainder 0 and get the square root.

- Here the digits, as per their place, obtain higher place value.

Aryabhata's method for finding square roots

- The digits a,b,c,d,e in the square root together with place values satisfy the following identities.
- $(a+b)^2 = a^2+2ab+b^2$
- $(a+b+c)^2 = [a^2+2ab+b^2] +2(a+b)c+c^2$

- $(a+b+c+d)^2$

$= [a^2+2ab+b^2+2(a+b)c+c^2]$

$+2(a+b+c)d+d^2$

$(a+b+c+d+e)^2 = [a^2+2ab+b^2+2(a+b)c+c^2]$

$+2(a+b+c)d+d^2+2(a+b+c+d)e+e^2$

- The number of square places is equal to the number of digits in the square root.
- The numbers a,b,c,d,e in the square root are to be interpreted along with place values for the identities and they are considered as digits in the calculations.
- The effect of place value is incorporated in placing the digits at the appropriate place while doing actual calculations.

General algorithm of Aryabhata for square root: “Nondecimal” Useful for Roman Numerals

- N=98 01
- We try arbitrary numbers a,b etc.
- Try a=95, a^2=9025.
- 9801-9025=776.
- Divide by 2a=2x95=190.

  Quotient is b=4
- Subtract from 776 the numbers 2ab and b^2, i.e. 760 and 16

to get the remainder as 0.

So the square root is 95+4=99.

Square root using arbitrary parts

- To find square root of 9801. Take a=21. 9801-441=9360.
- Take b=20. Subtact 2x21x20=840 and 20^2=400 to get 8120.
- a+b=41.
- Take c=39. Subtract 2x41x39=3198 to get 4922.

  Subtract 39^2=1600+1-80 to get 3401.

  a+b+c=80.
- Take d=15. Subtract 2x80x15 + 225 to get 776.

  a+b+c+d=95. Try e=4.
- Subtract 2x95x4 +16=760+16=776 to get 0. Thus, the square root is a+b+c+d+e=95+4=99.(For small a, method of finding b does not work.)
- Since the parts can be arbitrary, the method works in any base.

Base 2 calculations for square root

- 111 =(7), $(7)^2$=(49) =(32+16+1)=11 00 01
- Base 2: 11-01=10. Put 1 at sqrt place. Divide 10 0 by (2)x1=10. Quotient is (2)=10, but you should take it smaller, as 1.
- Subtract from 100 the number (2)x1x1=10. Answer is 10. Take next 0 to get 100. Subtract 1 from100. Answer is 11. Now put 1 after 1 in sqrt place, so at sqrt place we have 11.
- Divide by (2)x11=(6)=110, the number 110. The quotient is 1.
- Subtract 110-110. Remainder is 0. Take next 1. Subtract 1 from it. Remainder is 0. Now put 1 at the sqrt place. We get 111 as square root. We are done.

घनमूळ साधणे To get cube root

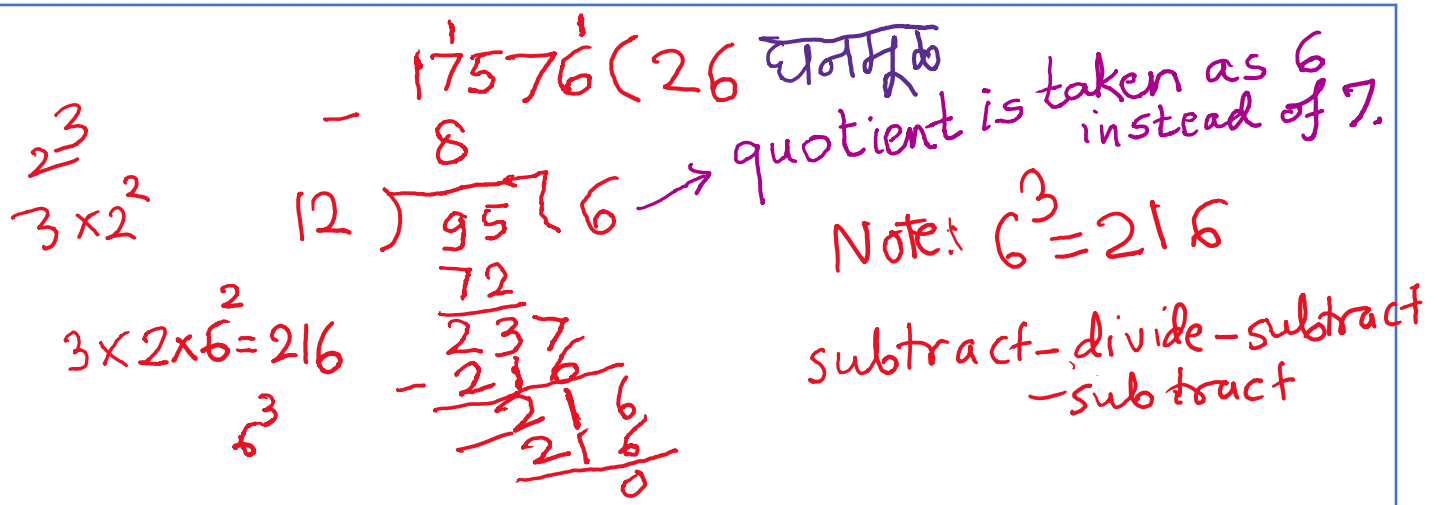
अघनाद् भजेद् द्वितीयात्

त्रिगुणेन घनस्य मूलवर्गेण |

वर्गस्त्रिपूर्वगुणितः

शोध्यः प्रथमाद् घनश्च घनात्॥५॥

(Ganitapada of Aryabhata)



$(a+b)^3 = a^3+3a^2b+3ab^2+b^3$

द्वितीयात् अघनात् "त्रिगुणेन घनस्य मूलवर्गेण" भजेत्| भजेत्=divide पूर्व=mentioned cuberoot

घनस्य मूलवर्गेण=by square of the current obtained cuberoot, available at the cube root place.

प्रथमात् (अघनात्) "त्रिपूर्वगुणितः वर्गः" शोध्यः| घनात् च घनः (शोध्यः)| शोध्यः=subtract

Note that due to further subtractions, it may not be possible to take largest quotient. e.g. it can be 1 less than expected. The number of digits in the cube root = the number of "cube-places".

No. of digits in a cube root and n-th root

In a perfect cube there are places घन, अघन1 and अघन2.

(cube place, noncube place -1 and noncube place -2) serially, starting from the smallest place to the largest place. The number of digits in a cube root is equal to the number of घन (cube) places.

A number with 3n or 3n-1 or 3n-2 digits has n cube places and has n digits in its cube root. Cube places: 1,4,7,10,… starting from unit's place. अघन1: 2,5,8,…, अघन2: 3,6,9,…

If there are k *n-th power* places in a perfect n-th power, then the number of digits in the n-th root is equal to k. The nth power places are places bearing numbers "1+(i-1)n for $i \geq 1$", i.e. 1,n+1,2n+1,…

Finding Cube root

Subtract the largest cube from the last cube place and write its cube root in the cube root row.

Divide, by three times the square of the (current obtained) cube root, the number (in non-cubeplace-2) adjacent to that cube-place and get the remainder.

Then subtract from the next noncube place (non-cube-place-1), the product of three times the “obtained cube root” and the square of the quotient and subtract the cube of the quotient from the next cube-place, and place the quotient on the right side of the cube root line. This should be called (current) cubic root.

If there are still numbers left, the same process should be continued.

6^3

Examples: cube-root, decimal point

$3 \times 56^2 = 3 \times 3136 = 9408$

2536
60

$3 \times 56 \times 1^2 = 168$ 1

$1^3 = 1$

Find the cube root of 17.576 Answer: 2.6

New Problem: Change number and the place of decimal point.

Find the cube root of

176.76 (Approximate Cube Root)

176(5.61

5^3 125

$3x5^2$ 75) 517(6

450

676

$3x5x6^2=540$

$6^3=216$

676

540

1360

216

1144

Put zeros to make groups of 3 digits after decimal point.

9408)11446(1

9408

20320

− 168

201520

− 1

2015190

Finding cube root

शेवटच्या घन स्थानांतून सर्वांत मोठा घन वजा करून त्याचे घनमूळ घनमूळाच्या ओळीत लिहावे.

त्या घनस्थानाच्या लगतच्या अघन स्थानाला “आलेल्या घनमूळा”च्या वर्गाच्या तिपटीने भागावे.

नंतर पुढील अघनस्थानातून, आलेल्या भागाकाराच्या वर्गाला पूर्वीच्या घनमूळाच्या तिपटीने आलेला गुणाकार वजा करावा आणि पुढील घनस्थानांतून भागाकाराचा घन वजा करावा आणि तो भागाकार घनमुळाच्या ओळीत उजव्या बाजूला मांडावा. याला घनमूळ म्हणावे. अजून अंक शिल्लक असतील तर हीच क्रिया पुढे चालू ठेवावी.

घनमूळाचे उदाहरण Example of a cube root

उदाहरण: १८६०८६७ चे घनमूळ काढा.

(घन स्थाने १ - - ० - - ७)

१ ८ ६ ० ८ ६ ७(१२३

१^ ३ १

1 is at cube root place ---

३x १^२ ३) ० ८ (२

६

---

२ ६

३x १x २^२ १ २

---

१ ४ ०

२^ ३ ८

12 is at cube root place ---

३x १२^२ ४३२) १ ३ २ ८(३

३x १२^२ ४३२) १ ३ २ ८(३

१ २ ९ ६

---

० ३ २ ६

३x १२x३^२ ३ २ ४

---

२ ७

३^३ २ ७

---

० Put 3 at the cube root place.

The cube root is 123.

Aryabhata's formula for finding cube roots/n-th roots

- $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$
- $(a+b+c)^3 = [\, a^3+3a^2b+3ab^2+b^3 \,] + 3(a+b)^2c+3(a+b)c^2+c^3$
- $(a+b+c+d)^3 = [a^3+3a^2b+3ab^2+b^3$

$+3(a+b)^2c+3(a+b)c^2+c^3\,]$

$+3(a+b+c)^2d+3(a+b+c)d^2+d^3$

- $(a+b+c+d+e)^3$

$= [\, a^3+3a^2b+3ab^2+b^3$

$+3(a+b)^2c+3(a+b)c^2+c^3\,]$

$+3(a+b+c)^2d+3(a+b+c)d^2+d^3$

$+3(a+b+c+d)^2e+3(a+b+c+d)e^2+e^3$

In this way any nth root can be obtained.

For example, to find the 5th root:

From the given 5th power number,

make groups of 5 digits starting from digit's place onwards.

From the last group, subtract the largest "digit-5^{th}-power" a^5 .

Then take next digit, divide by $5a^4$ and get b (this can be smaller due to extended division, as we have to subtract more terms).

Then take next digit and subtract $10a^3b^2$, take next digit and subtract $10a^2b^3$, take next digit and subtract $5ab^4$, take next digit and subtract b^5, and proceed till 0.

Binomial Theorem and Aryabhata's Recursion

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} ab^{n-1} + b^n.$$

Aryabhata's Recursion: Subtract a^n from "current N", b= $[(N-a^n)/na^{n-1}]$, where [.] is the integral part (b may have to be replaced by a smaller number), where the recurrence is as follows:

Initially a=a1=largest digit such that $a1^n \leq$ largest nth-power-place.

a=a1, Subtract $a1^n$ from N. Obtain b by above method and call it a2.

b=a2, `New a' =a+b, i.e. replace a by a+b, and find new b. Call it a3.

Use binomial theorem while subtracting $(a+b)^n$ from N,

i.e. subtract successively the terms in the binomial expansion of $(a+b)^n$.

a=a1+a2, b=a3

a=a1+a2+a3, b=a4

a= a1+a2+a3+a4, b=a5

…….

To get n-th root by Aryabhata's method

- Make groups of digits in N, of n digits, starting from unit's place. Last group can be of n or less no. of digits.
- No. of groups is equal to the the number of digits in the n-th root.
- From last group subtract a maximum n-th power of a digit, say a.
- The remainder with a next digit is to be divided by na^{n-1}.
- Let the quotient be b. Sometimes we may have to take b-1 instead of b.
- Then subtract $nC1\ a^{n-1}\ b$ (a step in the division), then $nC2\ a^{n-2}\ b^2$, …, b^n , at appropriate decimal places, thus effectively subtracting $(a+b)^n$, actually $(10a+b)^n$. The remainder is to be divided by "$n(a+b)^{n-1}$", that gives the next digit c. Then subtract terms so as to effectively subtract "$(a+b+c)^n$", and so on.

Finding n-th root by Aryabhata's method

From right of the given n-th power (unit's place) call places as n-th power place (npp), non-nth-power-place1,nnpp2,nnpp3,nnpp-`n-1';npp, nnpp1,nnpp2,…

Number of npp's is equal to the number of digits in the n-th root.

From the last npp, subtract maximum n-th power, and write the n-th root of this number say `a' separately in the n-th root place. Then divide the next place (nnpp-`n-1') by nx[(n-1)th power of `a' –which is the n-th root obtained so far- and get the quotient say b. Note that sometimes we may have to consider b-1 as quotient as we have to subtract many terms after this. Find the remainder. Here you are subtracting $nC1a^{n-1}b$.

From the successive places subtract successively $nC2a^{n-2}b^2,\ldots,b^n$, the terms in the binomial theorem, and write b at the end in the n-th root place. Then if still numbers remain, divide the next place (nnpp-`n-1') by nx[(n-1)th power of 'ab' –which is the n-th root obtained so far- and continue till the remainder is 0 (or the required number of digits in the n-th root are obtained –especially for a non-nth-power).

Aryabhata's general method for any base

- Aryabhata tries to write the n-th root as a sum of certain integers a1, a2,…, ak.
- These numbers can be arbitrary, as the binomial theorem and the method tells.
- Aryabhata cleverly takes these numbers as `single digit x a power of 10'.
- If the numbers are written in any base B, then the n-th root can be taken as the sum of numbers of the form `single digit x a power of B'.
- Thus, the method of Aryabhata works in any base.

Shorter Method for an n-th root using last digits

- If N is known to be a perfect n-th power, then it is possible to find the n-th root of N by a shorter method.
- For this we study first the high school method to find square root and cube root.
- We can find the last digit of a square root or a cube root by studying the last digit of the given number N.
- Other digits in the root can be obtained using congruences mod 10, digit by digit.

High School Method to find the square root of a 3 or 4-digit number which is a perfect square

- Number N ends with 5. Then it ends with 25. Leave these digits and look at the initial 1 or 2 numbers available. Write this number C as a(a+1), i.e. the product of 2 consecutive numbers. Then the square root is the 2-digit number a5.
- Proof: $(a5)^2 = (A+5)^2$ where A=10a. So $(a5)^2 = A^2+10A+25 = A(A+10)+25$ ='(a(a+1))25'.
- Shorter method: Find the digit a (largest) such that $a^2 < C$. Then the square root R is (a5). E.g. $\sqrt{625} = 25, \sqrt{5625} = 75, \sqrt{2025} = 45.$
- If the number ends with 0, then the last 2 digits are 00. Find `a' largest such that $a^2 \leq C\ (actually\ a^2 = C)$. Then R=(a0).

E.g. $\sqrt{3600} = 60, \sqrt{6400} = 80.$

Square root of a 3-4 digit perfect square: High School Method

- Last digit d:- $1^2=9^2 \rightarrow 1$, $2^2=8^2 \rightarrow 4$, $3^2=7^2 \rightarrow 9$, $4^2=6^2 \rightarrow 6$, $0^2 \rightarrow 0$, $5^2 \rightarrow 5$.

Last digit of square	1	4	9	6	0	5
Last digit of square root	1,9	2,8	3,7	4,6	0	5

- Method: Find the digit a (largest) such that $a^2 \leq C$. Find the 2 possibilities for the last digit d. If $N>(a5)^2$ then choose larger d, otherwise smaller d, to get the square root (ad).
- Ex. $45^2=2025$, $\sqrt{9801} = 99\ as\ 95^2 = 9025.$
- $\sqrt{1369} = 37\ as\ 35^2 = 1225.$
- $\sqrt{1089} = 33, as\ 35^2 = 1225.$
- The method works only if the given number is a perfect square.

High School Method to find the cube root of a number upto 6 digits which is a perfect cube

- The cubes of numbers with last digits 0 to 9 end with different digits:
- $0^{cube} \rightarrow 0$, $1^{cube} \rightarrow 1$, $2^{cube} \rightarrow 8$, $3^{cube} \rightarrow 7$, $4 \rightarrow 4$, $5 \rightarrow 5$, $6 \rightarrow 6$, $7 \rightarrow 3,8 \rightarrow 2$, $9 \rightarrow 9$.

Hence if a cube has upto 3 digits, then its cube root is a 1-digit number which can be obtained from the above list. (cube=343, Last digit 3, cuberoot =7)

If a number N has 4 to 6 digits, then its cube root has 2 digits.

The last digit (unit's place) is obtained as above. The first digit (10's digit) is a the largest number such that $a^3 \leq C$, where C is obtained from N by deleting the last 3 digits. [To get the last digit we are using congruence mod 10.]

Example: 50653= 50 653= 37^3, 148877= 148 877 = 53^3, 512= 8^3.

Last digit of the cube root can be obtained by the last digit of the cube.

Getting a cuberoot from last 2 digits of N, using congruences, provided N is odd and does not end with 5.

- Write A=10a. Given N, b can be obtained such that $(\grave{}ab')^3 = N$.

$(\grave{}ab')^3 = (A+b)^3 = A^3 + 3A^2b + 3Ab^2 + b^3$=N ≡ 10c+d mod 100 say. (i.e. last 2 digits - 10's and units - of N are c and d.

So $30ab^2 + b^3$ ≡10c +d mod 100.

- If b^3 ≡ 10b'+b''mod 100, then b'' =d. (Here b, b' are taken to be of 1 digit.)

So, $30ab^2$+10b' ≡ $10c\ mod\ 100$, So $3ab^2$+b' ≡ $c\ mod\ 10$.

- If (b,10)=1, then a can be obtained uniquely from this equation.
- Example. 148877= 148 877 = 53^3 . To get cube root using only last 2 digits.

Here b=3. $(10a+3)^3$ ≡77 mod 100, so 30ax9+27 ≡ 77 mod 100

So 30ax9+20 ≡70 mod 100, so 27a+2 ≡7 mod 10, so 7a ≡5 mod 10,

Multiply by 3. So a ≡ 3x5 ≡ 5 mod 10. Thus the cube root is 53.

Shakuntala Devi
Indian Human Computer

In 1977, at Southern Methodist University, Shakuntala Devi gave the 23rd root of a 201-digit number in 50 seconds. Her answer, which was 546,372,891, was confirmed by calculations done at the US Bureau of Standards by the UNIVAC 1101 computer, for which a special program had to be written to perform such a large calculation, which took a longer time than for her to do the same.

Cube root and 7^{th} root

In 1988, Shakuntala Devi travelled to the US to have her abilities studied by Arthur Jensen, a professor of educational psychology at the University of California, Berkeley. Jensen tested her performance at several tasks, including the calculation of large numbers.

Examples of the problems presented to Devi included calculating the cube root of 61,629,875 and the seventh root of 170,859,375. Jensen reported that Devi provided the solution to the above-mentioned problems (395 and 15, respectively) before Jensen could copy them down in his notebook.

61,629,875 has 3 groups of 2+3+3 =8 digits. The cube root has 3 digits. First digit must be 3 as 3^3=27 and 4^3=64. Last digit must be 5. For middle number probably Devi understands that it is close to 64…so answer close to 40, so tries 39. Gets 61,629 >39^3= 59319, answer is 395. Or $(40-1)^3$= 64000-120x39-1 < 64000-120x30=60400< 61629.

As for 7^{th} root, that is easier, there are 2 groups, 2+7=9. The answer is 2-digit, first digit must be 1 looking at 17, and the last digit must be 5, so the answer is 15.

23^{rd} root of a 201 digit number

- The 201 digit number N is to be written using groups of 23 mainly. Thus as 23x8=184, one initial group has 17 digits and the remaining 8 groups are of 23 digits each. Thus the answer has 9 digits. N is:
- 9167486769,2003915809,8660927585,3801624831,0668014430,
- 8622407126,5164279346,5704086709,6593279205,7674808067,
- 9002278301,6354924852,3803357453,1693511190,3596577547,
- 3400756816,8830562082,1016129132,8455648057,8015880677,1

Since N and 23 both are coprime to 10, i.e. are odd and not ending with 5, the 9 digits of the 23^{rd} root can be found just by using the last 9 digits of N by a THEOREM.

Method of Solution: Congruence mod 10

- Last 9 digits of N are 158806771 Ans: R= 546,372,891 : Distinct digits

$N \equiv 1 \ mod\ 10. Since\ 23rd\ root\ mod\ 10\ is\ unique\ it\ must\ end\ with\ 1.$

- $N \equiv (10x+1)^{23} \bmod 100$, so $71 \equiv (230x+1) \bmod 100$, ($71 \equiv 30x + (1)^{23} \bmod 100$)

so $70 \equiv 230x \bmod 100$, so $70 \equiv 30x \bmod 100$ or $7 \equiv 3x \bmod 10$, so x= 9.

So last 2 digits of R are 91. The 3rd digit will be 8. We prodeed as follows:

- $N \equiv (100x+91)^{23} \bmod 1000$, $N \equiv (2300x.91^{22} + 91^{23}) \bmod 1000$,

$\equiv 300x.(90+1)^{22}+(90+1)^{23} \bmod 1000$ ($771 \equiv 300x + 91^{23} \bmod 1000$)

$771 \equiv 300x+1+23.90+(23.22/2)90^2 \bmod 1000$. Subtract 1, divide by 10.

$77 \equiv 30x +207+23.11.810 \bmod 100$, so $70 \equiv 30x+200+3.1.10 \bmod 100$

$7 \equiv 3x+20+3 \bmod 10$, so $3x \equiv -6\ mod\ 10$, so $x \equiv -2 \equiv 8 \bmod 10$, so x=8.

We required only last 3 digits of 91^{23} here in the computation.

Getting all digits in the 23-rd root

- $6771 \equiv (1000x + 891)^{23} \bmod 10000$ [Ans: 546,372,891]

  $\equiv 891^{23} + (23 \times 22/2) \times 891^{22} \times 1000 \bmod 10000$ [N ≡ 158806771]

  $\equiv 891^{23} + 3000x \bmod 10000$, x=2. We required last 4 digits of 891^{23} .
- $06771 \equiv 2891^{23} + 30000x \bmod 100000$, x=7
- $806771 \equiv 72891^{23} + 300000x \bmod 1000000$, x=3
- $8806771 \equiv 372891^{23} + 3000000x \bmod 10000000$, x=6
- $58806771 \equiv 6372891^{23} + 30000000x \bmod 100000000$, x=4
- $158806771 \equiv 46372891^{23} + 300000000x \bmod 1000000000$, x=5

  We required only last 9 digits of 46372891^{23} in this calculation.
- Everytime one is reduced to a congruence mod 10 to be solved.

Theorem for k-th root: Last m digits enough

Let N be coprime to 10. Let k be coprime to 10.

Let the m = no. of digits in the k-th root R of N.

Let $N \equiv N1 \bmod 10^{m}$. (N1 gives the last m digits of N.)

$\phi(10^m)=4 \times 10^{m-1}$ is also coprime to k, as gcd(k,10)=1.

Let k1 = inverse of k mod $\phi(10^m)$. Then $kk1 \equiv 1 \bmod \phi(10^m)$.

i.e. $kk1=1+t.\ \phi(10^m)$. So $R^{kk1} \equiv R^{1+t.\phi(10\wedge m)} \bmod 10^m$.

$N=R^k$, $N^{k1} \equiv R^{kk1} \equiv R \bmod 10^m$ (by Euler's theorem).

But $N^{k1} \equiv N1^{k1} \bmod 10^m$.

So $N1^{k1} \equiv R \bmod 10^m$. R has only m digits, so R is uniquely determined by N1, i.e. the last m digits of N.

k-th root and RSA Cryptography

- The idea that kth root mod N can be obtained by taking k1th power, is a key step in encryption and decryption in RSA cryptography.

- In RSA, encryption is done by raising the message number to kth power reduced modulo N.
- For decryption, one requires k-th root mod N.
- For this, one raises the received number to k1-th power mod N, where k1 is such that $kk1 \equiv 1 \bmod \phi(N)$.
- One gets back the encrypted message.

RSA (Rivest, Shamir and Adleman)

One of the most prominent applications of Mathematics in recent times is RSA cryptography, which is used in online purchases, banking, smart cards and similar gadgets.

Wars were won by effective use of cryptography and were lost due to overconfidence in its effectiveness.

Some classical cryptosystems like Julius Caeser's cipher and permutation cipher are obsolete now. E.g. permutation cipher can be broken using frequency analysis.

Cryptography in 2nd World War

The German Lorenz cipher machine was used in World War II for encryption of very high-level general staff messages. The discovery of Mathematicians such as Turing from Britain, of how to decrypt the messages encrypted using the German machine, ultimately resulted in the defeat of Germany in the 2nd World War. It is always necessary to search for new methods of cryptography.

Conversion of a message into a number string

The message to be sent is converted into a string of numbers using ASCII code, or any pre-decided code.

In ASCII code ‘A’ is represented by 65. Similarly ‘a’ by 97,+ by 43,‘?’ by 63, ‘z’ by 122, ‘{’ by 123, etc. These numbers can be written as 3 digit numbers using zeros.

Using ASCII code, “Gauss is great.” becomes:

071097117115115032105115103114101097116046

The Euler's function

- The number of positive integers less than or equal to n and relatively prime to n is denoted by ϕ(n).
- ϕ(1)=1, ϕ(2)=1, ϕ(3)=2, ϕ(4)=2. If p prime, ϕ(p)=p-1,
- $\phi(p^k) = p^k - p^{k-1}$. E.g. ϕ(25)=25-5=20.
- ϕ(pq)=(p-1)(q-1), if p and q are distinct primes.
- ϕ(mn)=ϕ(m) ϕ(n), if m and n are relatively prime. (multiplicative property)
- Ex.: ϕ(100)= ϕ(25).ϕ(4)=20x2 =40.

n=10

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

φ(10) = 4

φ(100)=40

p prime

1, 2, 3, ..., p-1

φ(p) = p-1

$\varphi(m)$ Euler

$a^{\varphi(m)} \equiv 1 \pmod{m}$ ✓

Gauss introduced ≡

$13 \equiv 1 \pmod{2}$

$4 \equiv 1 \pmod{3}$

$10 \equiv 1 \pmod{9}$

$81 \equiv 1 \pmod{10}$

$13 - 1$ is divisible by 12.

$m \mid (a-b)$

$a \equiv b \pmod{m}$

$c \equiv d \pmod{m}$

$a+c \equiv b+d \pmod{m}$

$(a-b)+(c-d)$ ✓

$ac - bc + bc - bd$ ✓

$ac \equiv bd \pmod{m}$

Inverse modulo n

- If c is relatively prime to n then it can be considered as an element of the group Z_n^* and it has inverse mod n.
- For n=15, the inverse of 2 mod 15 is 8, because $2.8 \equiv 1 (\text{mod } 15)$.
- If (c,n)=1, we can use Euclid's algorithm to write 1=a.c+b.n .
- Thus $a.c \equiv 1 (\text{mod } n)$. If n is large, Euclid's algorithm is useful to find inverse mod n.

Euler's Theorem

- If G is a finite group of order n and a is an element of G then $a^n = id$.
- Euler's Theorem: For every *a* coprime to n,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof: Z_n^* is a group of order $\phi(n)$.

Ex.: $\phi(20)=8$.

Check that $3^8 \equiv 1 \pmod{20}$.

- Note: Powers can be obtained by the method of repeated squaring.
- $3^8=(((3^2)^2)^2)$.

Leonard Euler (1708-1783)

Powering by repeated squaring

To find a^{100} one calculates a.a.a…a and requires 99 multiplications.

To do this efficiently, one uses binary representation of 100.

(1100100)

$100 = 64+32+4 = 2^6+2^5+2^2$.

$a^{100} = (a\text{^}2^6)\cdot (a\text{^}2^5)\cdot (a\text{^}2^2)$.

Since $a\text{^}2^k$ can be obtained by squaring k times, a^{100} can be obtained in 6+2=8 multiplications.

(binary length - 1) + (no. of 1's - 1)

A powering Method of Bhaskaracharya (1114-1185)

Ex.: 100 --> 50--> 25 --> 24 --> 12 --> 6-->3-->2-->1

For even number, divide by 2, and for odd number, subtract 1, till you reach 1.

Find a^{100} by going in the opposite direction व्युत्क्रम :

(Multiply/square: multiply by `a' or by itself, appropriately.)

100 <--50<-- 25 <-- 24 <-- 12<-- 6<--3<--2<--1

a a a a a a a a a

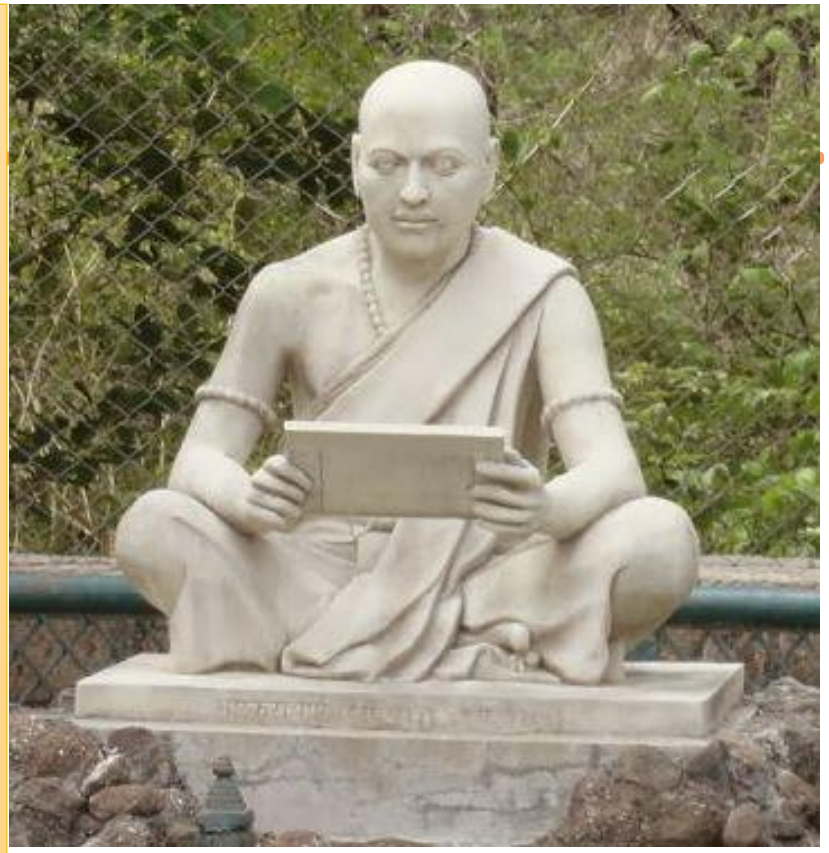
$a, ar, ar^2 + \cdots ar^{n-1}$

$a\left(r^n - 1\right)$

$r - 1$

Using this powerful method of Bhaskaracharya (Leelavati: Verse 125) called गुणवर्ग method, for a 100 digit number k, a^k can be obtained in just 664 multiplications.

(Current Name: Repeated Squaring Method)



It is not well known that such an important method was described by Bhaskaracharya. It was first mentioned in India, by Pingala – 3rd Century BCA.

The principle of RSA cryptography

The computer can multiply two integers exactly, within the blink of an eye, but it can take exorbitant amount of time for factoring a large integer (say of 200 digits or more).

(Quantum computers are expected to do this in a reasonable time.)

- A product of 2 primes is in general more difficult to factorise than a product of 3 or more primes.
- Ex.: A number N of 200 digits which is a product of 4 primes must have a prime factor of 50 or less number of digits. If N=pq, a product of 2 primes, then at least one of p and or q has at most 100 digits.)

Public Keys and Secret Keys

- Let N be a product of two large primes p and q.
- N is called a public key.

- $\phi(N) = (p-1)(q-1)$. Ex. $\phi(91) = \phi(7x13) = 6x12 = 72$.
- Take k to be an integer coprime to $\phi(N)$.

Then k is another public key.

- These two public keys are made public (e.g. by keeping them on one's website).
- Let a positive integer k_1 be the inverse of k in the group $Z_{\phi(N)}^*$. k_1 is called a secret key.

Why is k_1 a secret key

- Although N=pq is public, the primes p,q are difficult to obtain, as factorisation of large numbers is not an easy process.
- Hence $\phi(N) = (p-1)(q-1)$ is difficult to get.
- Thus, finding k_1 such that $k\, k_1 \equiv 1 (\mathrm{mod}\ \phi(N))$ is not possible in a limited time.

Ex. If p=7, q=13, then N=pq=91, $\phi(N)=72$.

If k=29, then $29 \times 5 = 145 \equiv 1 (\mathrm{mod}\ 72)$, so $k_1 = 5$.

k_1 can be found only by the person who knows the factorization of N.

Encrypting the message

- If the message converted to a number string is very long, it is necessary to divide it into smaller number strings so that the resulting numbers are smaller than the public key N.

- If a is such a number, one uses the second key k to get the encrypted message string $b < N$ by $b \equiv a^k \pmod{N}$.

Decrypting the message: Finding k-th root modulo N

- The sent message b, even if intercepted, cannot be understood by a third party, without knowing the secret key k_1.
- Decryption requires finding k-th root mod N. Surprisingly this is achieved by powering.
- To decrypt the received message b, one finds b^{k_1} (mod N). The answer is nothing but the sent message string a.

How does the decryption work?

Find k-th root using powering

- The sent message is $b \equiv a^k \pmod N$. ($0<a<N$.)
- Since $k.k_1 \equiv 1 \pmod{\phi(N)}$, there is an integer t such that $k.k_1 = 1 + t.\phi(N)$.
- If (a, N)=1, i.e. a is in the group Z_n^*, so

  by Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod N$.
- $b^{k_1} \equiv a^{kk_1} \equiv a^{1+t\phi(N)}$

  $\equiv a.\left(a^{\phi(n)}\right)^t \equiv a \pmod N$.

Euler did not now that his theorem will be useful in RSA Cryptography later.

- Thus one gets back the original message. As N=pq, the method works for (a, N) ≠ 1 also.

An example

- Take primes p=3,q=5. Then the first public key is N=3.5=15 . Φ(15)=2.4=8.
- Take k=3 (coprime to 8).

  k is the second public key.
- Let the message string be a=13. Here a is < 15. The encrypted message is
- $b \equiv a^k \pmod{N}$, i.e. $b \equiv 13^3 \pmod{15}$, i.e. b=7.

  Since $3.3 \equiv 1 \pmod{8}$, The secret key $k_1 = 3$. Then $b^{k_1} = b^3 \equiv 7^3 \equiv 13 \pmod{15}$, gives the original message string 13.

Use of Free Software KASH

- The free software KASH helps in exact computations and therefore helps in testing and understanding RSA Cryptography. Using KASH one can find large primes and perform modular operations. KASH also does factorisation of numbers upto 50 digits, but as is expected, factorizations of large numbers, say of 200 digits, are not feasible using even KASH, so decrypting of an RSA-encrypted message is possible with KASH only using the secret key.
- Computations may be done using Mathematica or SAGE also.

Getting Large Primes Using KASH

```
kash> p:= NextPrime(42254657778);
        42254657803
kash> q:= NextPrime(6788989900767);
        6788989900789
kash> N:= p*q;  (Public Key 1)
        286866448858776284470656 7
            (a 25-digit number)
```

Euler's Phi Function

kash>ϕ(N)= $\phi(pq)$=(p-1)*(q-1); (Secret Key 1)

28686644885198306901479 76

(This gives ϕ(N). The Phi function can be computed using the factorisation of the number N.)

kash> k:=4567; (Public Key 2)

4567

(k is a trial number expected to be coprime to Phi(N))

GCD as a combination of the given numbers

Express 1=4567xA + ϕ(N)xB

kash> IntXGcd(4567, ϕ(N));

[1, [626872598980247652456247, -998]]

This says that the gcd of 4567 and Phi(N) is 1.

Also, the gcd 1 is a combination of of the numbers 4567 and ϕ(N).

See the two entries in the inner bracket.

kash> k1:=last[2][1]; (Secret Key 2)

626872598980247652456247 (24 digits)

The Inverse Mod ϕ(N)

- The inverse of k mod ϕ(N) is obtained from the linear combination.

k1= the inverse of k is obtained as follows:

kash> k1:=last[2][1]; (Secret Key 2)

626872598980247652456247

This is the first entry in the inner bracket.

If it happens to be negative, we should add ϕ(N) to it to make it positive.

The Encrypted Message

kash> a:=1234567; (Message to be sent)

1234567

The encrypted message is $a^k \pmod N$.

k:=4567; N=28686644885877628447065 67

kash> b:=IntPowerMod(a,k,N);

3639332525073553736422 82

(This is the Encripted Message. From this one gets no clue what the original message is.)

The Decryption

The decrypted message is $b^{k1} \pmod N$.

k1= 626872598980247652456247

b = 3639332525073553736422 82

N = 28686644885877628447065 67

kash> c:=IntPowerMod(b,k1,N);

1234567 (This is the same as the sent message 'a', as expected.)

New methods such as elliptic curve cryptography have also been developed.

Thank You for Your Patience

Thanks to

Prof. Ravi Kulkarni, Prof. Kishore Kulkarni,

Authorities and friends of SIAA,

and esteemed audience