

A study on Cubic Sieve Congruence

A dissertation submitted in partial fulfilment
of the requirements of M.Tech.(Computer Science)
degree of the Indian Statistical Institute, Kolkata

by

Subba Rao Y. V.

under the supervision of

**Subhamoy Maitra
Applied Statistical Unit**

**Indian Statistical Institute
Kolkata-700 108.**

10th July 2003

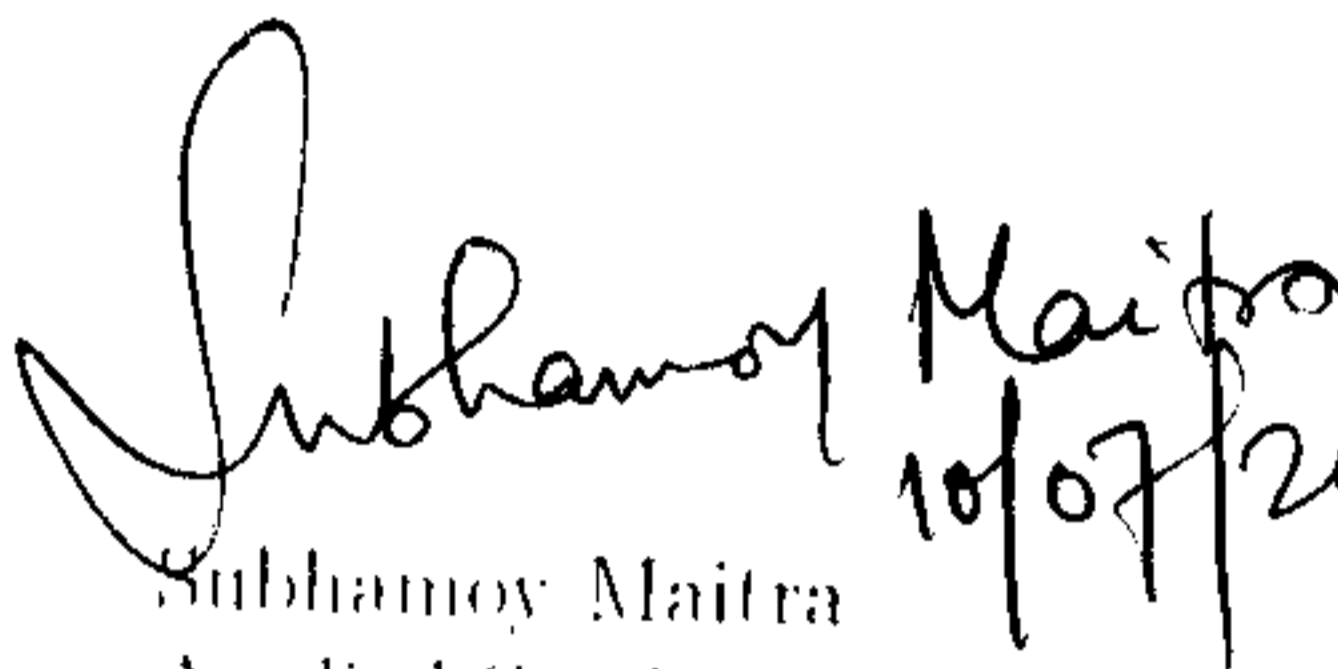
Indian Statistical Institute

203, Barrackpore Trunk Road,

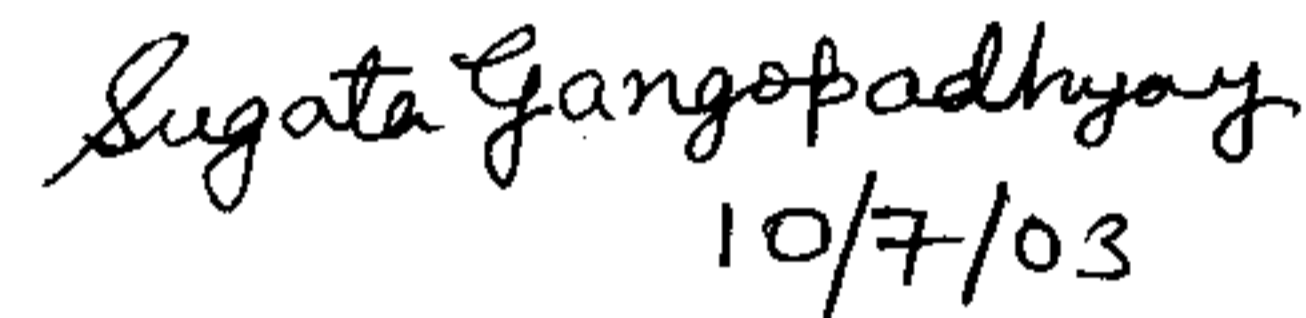
Kolkata-700 108.

Certificate of Approval

This is to certify that this thesis titled "A study on Cubic Sieve Congruence" submitted by **Subba Rao Y. V.** towards partial fulfilment of requirements for the degree of M.Tech. in Computer Science at Indian Statistical Institute, Kolkata embodies the work done under my supervision.


Subhamoy Maitra
10/07/2003

Subhamoy Maitra
Applied Statistical Unit
Indian Statistical Institute
Kolkata-700 108.


10/7/03

External Expert
Lecturer, BITS Pilani

Acknowledgments

I take pleasure in thanking Dr. Subhamoy Maitra for his friendly guidance throughout the dissertation period. His pleasant and encouraging words have always kept my spirits up.

I take the opportunity to thank Prof. R. Tandon, University of Hyderabad, India. I also thank my friends A. Rajani Kanth, M. Raja Sekhar, my classmates and my family for their encouragement to finish this work.

Subba Rao Y. V.

Abstract

In this dissertation we first explained the importance of cubic sieve congruence problem in the context of Cryptology. We justified an heuristic estimate of cardinality of S_a , set of solutions for cubic sieve congruence problem with x , y and z of order p^n , using some statistical methods. Then we presented an algorithm to solve the problem in time better than $O(p)$. Then we gave a method, which can solve the problem in log time, but only for few primes. Finally, we suggested further possible improvements to our proposed algorithm.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 1.1 | Discrete logarithm problem. | 1 |
| 1.2 | Some known algorithms for DLP. | 1 |
| 1.3 | Cubic Sieve Congruence problem | 2 |
| 2 | Existence of solution to CSC. | 3 |
| 2.1 | An Heuristic Estimate. | 3 |
| 2.2 | Verification of conjecture. | 4 |
| 3 | An Algorithm to solve CSC. | 7 |
| 3.1 | CSC in Parametric form. | 7 |
| 3.2 | Some Observations | 8 |
| 3.3 | Usefulness of this Algorithm. | 10 |
| 4 | Extensions. | 15 |
| 4.1 | A polynomial time Algorithm. | 15 |
| 4.2 | Further improvements to consider. | 16 |
| | Bibliography | 16 |

Chapter 1

Introduction

1.1 Discrete logarithm problem.

Let F_p be a prime field with cardinality p . Let g be a generator of the cyclic multiplicative group F_p^* . Given an element $a \in F_p^*$, there exists a unique integer $0 \leq x \leq p-2$ such that $a = g^x$ in F_p . Such an integer x is called as discrete logarithm or index of a in F_p with respect to g and is denoted by $ind_g(a)$. Determination of x from known p , g and a is the discrete logarithm problem (DLP).

The known difficulty in computation of DLP with easily computable inverse, discrete exponentiation makes DLP, a problem of high interest in Cryptology. As a simple example of this, we can look an instance of ElGamal Crypto System $-(p, \alpha, \beta)$, where α is a generator of F_p^* and $\beta = \alpha^a$, for some secret $a \in \{0, 1, 2, \dots, p-2\}$.

In this, encoding function

$$C_k : F_p^* \longrightarrow F_p^* \times F_p^*$$

is defined as, for $x \in F_p^*$ we define

$$C_k(x) = (y_1, y_2)$$

where $y_1 = \alpha^k$ (k is again secret value known only to sender) and $y_2 = x\beta^k$. It is decoded by simple function defined as

$$D_k(y_1, y_2) = y_2(y_1)^{-a}$$

As noted above, hardness of DLP makes this Cryptosystem reliable.

1.2 Some known algorithms for DLP.

It can be easily seen that DLP can be solved using linear search in $O(p)$ time and $O(1)$ space or by precomputing g^x for all x , it can be solved in $O(1)$ time and $O(p)$ space.

A good trade-off of time and space can be obtained in **Shank's algorithm**. This can be implemented in $O(m)$ time and $O(m)$ space, where $m = \lfloor (p-1)^{1/2} \rfloor$. **Pohlig - Hellman**

algorithm requires factoring $p-1$ into its prime factors, which is again a known hard problem.

Index calculus method appears to be more applicable in solving DLP. In [1], chapter 3, three variants of this method are discussed. These variants are Basic method, Linear Sieve method and The Cubic Sieve method. In this last method, i.e., cubic sieve method, we need a 'known' solution of the Diophantienne equation

$$x^3 \equiv y^2 z \pmod{p} \tag{1.1}$$

such that $x^3 \neq y^2 z$ with x, y, z of the order p^α for some $1/3 \leq \alpha \leq 1/2$.

1.3 Cubic Sieve Congruence problem

The remaining part of this dissertation focuses on understanding the above Diophantienne equation and its solutions. From now we refer to this problem as Cubic Sieve Congruence problem and is denoted as CSC. In Chapter 2 we make an attempt to show that for sufficiently large α CSC has non empty solution set. In Chapter 3, we describe an algorithm to solve CSC that takes lesser than $O(p)$ time for almost all primes. In Chapter 4, we suggest some possible lines of thought to extend this work.

Chapter 2

Existence of solution to CSC.

2.1 An Heuristic Estimate.

We begin this section by defining few notations. Let

$$S = \{(x, y, z) | x^3 \equiv y^2 z \pmod{p}, 1 \leq x, y, z < p\} \quad (2.1)$$

$$S_{=} = \{(x, y, z) | (x, y, z) \in S \text{ and } x^3 = y^2 z\} \quad (2.2)$$

$$S_{\neq} = \{(x, y, z) | (x, y, z) \in S \text{ and } x^3 \neq y^2 z\} \quad (2.3)$$

$$S_{\alpha} = \{(x, y, z) \in S | 1 \leq x, y, z \leq p^{\alpha}\} \quad (2.4)$$

In [1], Chapter 5 it is shown that

$$\#S = (p-1)^2 = \Theta(p^2) \quad (2.5)$$

$$\#S_{=} \leq \frac{3}{2}(p-1)\ln(p-1) + (3\gamma - \frac{3}{2})(p-1) + O(\sqrt{p}) = O(p \ln p) \quad (2.6)$$

and

$$\#S_{=} \geq \frac{3}{2}p + O(p^{\frac{2}{3}}) \quad (2.7)$$

i.e.

$$\#S_{=} = \Omega(p) \quad (2.8)$$

[Here γ represents Euler's constant defined as $\gamma = \lim_{n \rightarrow \infty} (1 + \frac{1}{2} + \dots + \frac{1}{n} - \ln(n)) = 0.57721566\dots$]
Since S is the disjoint union of $S_{=}$ and S_{\neq} , from above equations we have,

$$\#S_{\neq} \geq (p-1)^2 - \frac{3}{2}(p-1)\ln(p-1) + O(p) \quad (2.9)$$

$$\#S_{\neq} \leq (p-1)^2 - \frac{3}{2}p + O(p^{\frac{2}{3}}). \quad (2.10)$$

In particular,

$$\#S_{\neq} = \Theta(p^2). \quad (2.11)$$

From this it is clear that partial CSC problem, ignoring the bounds on x, y and z has approximately p^2 number of solutions.

We are more interested in knowing the value of $\#S_\alpha$, which is estimated by the following conjecture.

Conjecture 2.1 *The expected cardinality of S_α is asymptotically equal to $\chi p^{3\alpha-1}$ for all $0 < \alpha \leq 1$ and for some constant $\chi \approx 1$.*

Good number of experimental verifications with various sizes of primes ranging from 15bits to 32bits, do support above conjecture. Few such results are included in next section.

2.2 Verification of conjecture.

As our first step, as in [1], we tabulated results for various primes. Two such results are given here as Table 2.1 and Table 2.2. In this first column is the value of α , second column is the number of solutions with x, y , and z with order p^α , third column is value of $\frac{2}{3}p^{3\alpha-1}$ and fourth column is value of $p^{3\alpha-1}$. These results indicate that as α increases the number of solutions get closer to $p^{3\alpha-1}$ and also for sufficiently large α depending on the size of prime (in case of 32bit primes this α is 0.41) $\frac{2}{3}p^{3\alpha-1}$ gives us a lower bound to number of solutions.

To continue our verification, we calculated

$$\frac{\text{Number of solutions of order } p^\alpha}{p^{3\alpha-1}}$$

for α ranging from .34 to .50 for fifty randomly chosen primes. Then in Table 2.3 we tabulated information as α in first column, mean of above fifty fractions for that α in second column and in last column standard deviation of the same values are given. Results here indicate that as α is increasing to .50 we see that mean is getting closer to 1.0 and standard deviation getting closer to 0.0, this justifies the above conjecture.

| α | # of solutions | $\frac{2}{3}p^{3\alpha-1}$ | $p^{3\alpha-1}$ |
|----------|----------------|----------------------------|-----------------|
| 0.340000 | 0 | 0 | 1 |
| 0.350000 | 0 | 2 | 3 |
| 0.360000 | 2 | 3 | 5 |
| 0.370000 | 6 | 7 | 11 |
| 0.380000 | 16 | 14 | 22 |
| 0.390000 | 27 | 28 | 43 |
| 0.400000 | 69 | 56 | 84 |
| 0.410000 | 154 | 109 | 164 |
| 0.420000 | 283 | 212 | 319 |
| 0.430000 | 573 | 413 | 620 |
| 0.440000 | 1135 | 804 | 1206 |
| 0.450000 | 2223 | 1564 | 2347 |
| 0.460000 | 4407 | 3043 | 4565 |
| 0.470000 | 8639 | 5919 | 8879 |
| 0.480000 | 16910 | 11513 | 17270 |
| 0.490000 | 33179 | 22392 | 33589 |
| 0.500000 | 65137 | 43552 | 65329 |

Table 2.1: Prime : 4268002919

| α | # of solutions | $\frac{2}{3}p^{3\alpha-1}$ | $p^{3\alpha-1}$ |
|----------|----------------|----------------------------|-----------------|
| 0.340000 | 0 | 0 | 1 |
| 0.350000 | 2 | 2 | 3 |
| 0.360000 | 4 | 3 | 5 |
| 0.370000 | 5 | 7 | 11 |
| 0.380000 | 13 | 14 | 22 |
| 0.390000 | 27 | 28 | 43 |
| 0.400000 | 54 | 56 | 84 |
| 0.410000 | 126 | 108 | 163 |
| 0.420000 | 257 | 211 | 317 |
| 0.430000 | 547 | 412 | 618 |
| 0.440000 | 1080 | 800 | 1201 |
| 0.450000 | 2150 | 1557 | 2336 |
| 0.460000 | 4235 | 3028 | 4543 |
| 0.470000 | 8300 | 5888 | 8832 |
| 0.480000 | 16427 | 11448 | 17172 |
| 0.490000 | 32244 | 22258 | 33387 |
| 0.500000 | 63262 | 43274 | 64911 |

Table 2.2: Prime : 4213586771

| α | Mean | Std.Div |
|----------|-----------|-----------|
| 0.34 | 0.2800000 | 0.6074369 |
| 0.35 | 0.4100000 | 0.5115004 |
| 0.36 | 0.5340000 | 0.4082616 |
| 0.37 | 0.6622222 | 0.4120630 |
| 0.38 | 0.7054902 | 0.3139408 |
| 0.39 | 0.7988400 | 0.2547877 |
| 0.40 | 0.8296789 | 0.1910907 |
| 0.41 | 0.8618105 | 0.1410821 |
| 0.42 | 0.8903438 | 0.1060304 |
| 0.43 | 0.9261365 | 0.0804415 |
| 0.44 | 0.9389463 | 0.0643277 |
| 0.45 | 0.9533673 | 0.0441644 |
| 0.46 | 0.9686826 | 0.0338940 |
| 0.47 | 0.9745897 | 0.0261893 |
| 0.48 | 0.9799228 | 0.0207219 |
| 0.49 | 0.9840180 | 0.0138331 |
| 0.50 | 0.9883767 | 0.0111183 |

Table 2.3: Verification of conjecture

Chapter 3

An Algorithm to solve CSC.

3.1 CSC in Parametric form.

To have a better understanding of the problem, we tried to express it in parametric form as

$$x \equiv v^2 z \pmod{p} \text{ and } y \equiv vz \pmod{p} \quad (3.1)$$

here condition $x^3 \neq y^2 z$ in CSC can be rewritten as $x \neq v^2 z$. We shall denote this problem as CSCP.

Lemma 3.1 *Problem CSC is equivalent to problem CSCP.*

Proof : Given a solution (x_0, y_0, z_0, v_0) of CSCP we can see that (x_0, y_0, z_0) is a solution of CSC, because

$$\begin{aligned} y_0^2 z_0 &\equiv v_0^2 x_0^2 z_0 \quad (\because y_0 \equiv v_0 x_0 \pmod{p}) \\ &\equiv x_0^2 v_0^2 z_0 \\ &\equiv x_0^2 x_0 \quad (\because x_0 \equiv v_0^2 z_0 \pmod{p}) \\ &\equiv x_0^3 \pmod{p} \end{aligned}$$

Similarly, given (x_1, y_1, z_1) a solution of CSC, we have (x_1, y_1, z_1, v_1) where $v_1 \equiv \frac{y_1}{x_1}$, as solution of CSCP. This is true, because

$$v_1^2 z_1 \equiv \frac{y_1^2 z_1}{x_1^2} \equiv \frac{x_1^3}{x_1^2} \equiv x_1 \pmod{p}$$

and

$$v_1 x_1 \equiv \frac{y_1 x_1}{x_1} \equiv y_1 \pmod{p}$$

So we have the equivalence as needed.

For the remaining part of this chapter we focus only on CSCP problem in a restated form along with bounding condition of CSC problem. ■

3.2 Some Observations

We restate CSCP problem along with bounding condition of CSC as

$$x \equiv v^2 z \pmod{p} \quad \text{and} \quad y \equiv vx \pmod{p}$$

with $x \neq v^2 z$ and $0 \leq x, y, z \leq p^{0.5}$. Our aim is to solve this problem with its conditions. As seen in the previous section this is same as CSC problem with $\alpha = 0.5$. Henceforth we write $v = p^\alpha$ (this α has nothing to do with upper bound of x, y and z) and $z = p^\beta$ for some real α, β .

Lemma 3.2 $\alpha > 0.25$ for all valid solutions (x, y, z, v) of CSCP.

Proof : This is easy to see because if $v = p^\alpha \leq p^{0.25}$ then both of our congruence relations become equalities as

$$x = v^2 z, \quad \text{since } 2\alpha + \beta \leq 2(0.25) + 0.5 = 1.$$

Also

$$y = vx, \quad \text{since } x < p^{0.5} \text{ and } v \leq p^{0.25}.$$

This violates our requirement. So $\alpha > 0.25$.

Lemma 3.3 For any fixed $v = p^\alpha$ with $\alpha \leq 0.5$, we have (if it exists) $x < p^{0.5-\alpha}$.

Proof : This follows from the fact that $vx \equiv y < p^{0.5}$. But as $\alpha \leq 0.5$ and $x < p^{0.5}$, this congruence is an equality i.e. $vx = y$.

From this we have, $vx < p^{0.5}$, therefore $x < \frac{p^{0.5}}{v} = p^{0.5-\alpha}$ as needed.

So having,

$$v, z < p^{0.5} \text{ and } x = v^2 z < p^{0.5-\alpha}$$

immediatly gives us suitable solution with $y = vx < p^{0.5}$. These observation along with above two lemmas form the basis of our Algorithm. Here for each fixed v in the range $p^{0.25}$ to $p^{0.5}$, we vary z (using information provided by the following lemma) and compute x for each pair (v, z) . Once the suitable x is found we stop by giving the corresponding solution as output. In next section we try to look at the applicabilty of the algorithm.

Unless stated otherwise, from now onwards we work with $v = p^\alpha$ with $0.25 < \alpha < 0.5$.

Lemma 3.4 For a fixed $v = p^\alpha$ that is part of a solution (x, y, z, v) , we have $z \geq p^{1-2\alpha}$.

Proof : From the fact that $p^{0.25} < v < p^{0.5}$ we have $p^{0.5} < v^2 < p$.

Now if we assume that $z < p^{1-2\alpha}$, then we have (with out taking modular operations)

$$p^{0.5} < v^2 z = p^{2\alpha} z < p^{2\alpha} p^{1-2\alpha} = p.$$

Therefore $x \equiv v^2 z$ can not be of order $p^{0.5}$.

This proves that $z \geq p^{1-2\alpha}$, as needed.

From this lemma, we can see that for fixed v , smallest z that can be considered is $\lceil p^{1-2\alpha} \rceil$. We represent this as z_1 and also write $z_1 = p^{\beta_1}$ for some real $\beta_1 < 0.5$.

For this z_1 , we have

$$v^2 z_1 = p^{2\alpha + \beta_1} = p + k_1 \quad (3.2)$$

for some $0 \leq k_1 < p$.

Now we have two possible cases, they are

Case 1: $k_1 < p^{0.5-\alpha}$

In this case our problem is solved by letting $x = k_1$. Because, from earlier discussion we know that if $v, z < p^{0.5}$ and $x < p^{0.5-\alpha}$ then we can have a solution just by taking $y = vx$.

Case 2: $k_1 \geq p^{0.5-\alpha}$

In this case we may try for 'next suitable' z in the increasing order. Let that be $z_2 = p^{\beta_2}$ of the form $z_2 = z_1 + t_1$. Also we need z_2 to be such that

$$v^2 z_2 = p^{2\alpha + \beta_2} = p + k_2 \quad (3.3)$$

for some $0 \leq k_2 < p$.

We shall look this more closely, because

$$\begin{aligned} v^2 z_2 &= 2p + k_2 \\ \Rightarrow v^2(z_1 + t_1) &= 2p + k_2 \end{aligned}$$

This gives us,

$$\begin{aligned} v^2 t_1 &= 2p + k_2 - v^2 z_1 \\ &= 2p + k_2 - (p + k_1) \\ &= (p - k_1) + k_2. \end{aligned}$$

From this we have,

$$t_1 = \frac{(p - k_1) + k_2}{v^2}.$$

Since our aim is to minimize k_2 , we can take

$$t_1 = \lceil \frac{(p - k_1)}{v^2} \rceil.$$

Again as above, we have two cases as,

Case 1: $k_2 < p^{0.5-\alpha}$, this leads to a solution.

Case 2: $k_2 \geq p^{0.5-\alpha}$, we can continue to next z , say $z_3 = z_2 + t_2$ where $t_2 = \lceil \frac{(p - k_2)}{v^2} \rceil$.

We can repeat this process until it terminates by giving us a 'valid' solution or it reaches a stage as $z_r > p^{0.5}$ in some r^{th} cycle. If z_r becomes larger, we can restart with $v = v + 1$ till $v < p^{0.5}$.

All this leads to an Algorithm as below.

```

I       $Min = p^{0.25}$ 
II      $Max = p^{0.5}$ 
III    Start with  $v = Min$ 
IV     while( $v < Max$ ) {
IVa     $z = \lceil \frac{p}{v^2} \rceil$ 
IVb     $k \equiv (v^2 z) \pmod{p}$ 
IVc    if ( $k < \frac{p^{0.5}}{v}$ ) {
        Output solution as ( $x = k, y = kv, z = z, v = v$ )
        STOP
    }
IVd     $t = \lceil \frac{p-k}{v^2} \rceil$ 
IVe     $z = z + t$ 
IVf    While ( $z < p^{0.5}$ ) {
         $k \equiv (v^2 z) \pmod{p}$ 
        if ( $k < \frac{p^{0.5}}{v}$ ) {
            Output solution as ( $x = k, y = kv, z = z, v = v$ )
            STOP
        }
         $t = \lceil \frac{p-k}{v^2} \rceil$ 
         $z = z + t$ 
    }
IVg     $v = v + 1$ 
}
V      Output (No solutions in range  $p^{0.5}$  as  $x, y, z, v < p^{0.5}$  ).
VI     STOP.

```

3.3 Usefulness of this Algorithm.

We shall give here few of our results in using this Algorithm,

prime : 145678132176163

$$\begin{aligned}
 p^{0.25} &= 3475 \\
 p^{0.5} &= 12069719 \\
 v &= 27009 \\
 x &= 17 \\
 y &= 459153 \\
 z &= 9785284
 \end{aligned}$$

prime : 145678132176162513743

$$\begin{aligned} p^{0.25} &= 109863 \\ p^{0.5} &= 12069719639 \\ v &= 115472 \\ x &= 18609 \\ y &= 2148818448 \\ z &= 10925491628 \end{aligned}$$

prime : 23456543676548754325781

$$\begin{aligned} p^{0.25} &= 391351 \\ p^{0.5} &= 153155292682 \\ v &= 1440247 \\ x &= 48034 \\ y &= 69180824398 \\ z &= 147005442243 \end{aligned}$$

prime : 66666555558888899999267

$$\begin{aligned} p^{0.25} &= 508133 \\ p^{0.5} &= 258198674587 \\ v &= 11225651 \\ x &= 16104 \\ y &= 180777883704 \\ z &= 117974951645 \end{aligned}$$

To assert that this algorithm is useful, we need to prove that for every given prime, there exists a solution (x, y, z, v) with all of order $p^{0.5}$. But in reality it is not true, as we managed to see some primes (eg: 17011, 741799451) with no such solutions. But still, though it is not 'complete', this algorithm is effective, as seen by our statistical observations. Table:3.1(for 25 primes of size 30bits) is normalized distribution of α 's in intervals of length 0.05 in range 0.25 to 1.00. Each cell in this table is $\frac{\# \text{ of } \alpha\text{'s in that interval}}{\text{Actual length on real line}} * 2^{15}$. Here we can see a larger mass in most cases is in some interval in the range 0.25 to 0.50 as we need it. Table:3.2 gives the actual number of α 's in each interval in above range.

| .3 | .35 | .4 | .45 | .5 | .55 | .6 | .65 | .7 | .75 | .8 | .85 | .9 | .95 | 1 |
|--------|-------|--------|-------|-------|------|------|------|------|------|------|------|------|------|------|
| 210.10 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.70 | 0.88 | 1.02 | 1.06 | 1.09 | 1.10 | 1.12 | 1.10 |
| 0.00 | 0.00 | 0.00 | 5.81 | 2.12 | 0.77 | 0.56 | 0.72 | 1.19 | 1.15 | 1.22 | 1.34 | 1.33 | 1.32 | 1.31 |
| 0.00 | 0.00 | 32.92 | 0.00 | 0.00 | 0.00 | 1.18 | 0.97 | 1.14 | 1.12 | 1.45 | 1.41 | 1.39 | 1.40 | 1.34 |
| 0.00 | 0.00 | 14.23 | 5.11 | 0.00 | 1.32 | 1.42 | 0.77 | 1.01 | 1.33 | 1.17 | 1.21 | 1.17 | 1.18 | 1.14 |
| 0.00 | 36.49 | 25.95 | 4.61 | 0.00 | 0.58 | 0.41 | 1.55 | 0.94 | 1.25 | 1.10 | 1.02 | 1.04 | 1.04 | 1.04 |
| 99.65 | 35.27 | 0.00 | 0.00 | 0.00 | 2.21 | 1.37 | 0.55 | 0.74 | 1.07 | 0.95 | 0.97 | 1.01 | 1.02 | 0.99 |
| 0.00 | 37.78 | 0.00 | 4.82 | 0.00 | 2.46 | 0.66 | 1.02 | 0.87 | 1.10 | 1.11 | 1.10 | 1.08 | 1.09 | 1.07 |
| 115.61 | 0.00 | 0.00 | 10.97 | 3.97 | 1.44 | 2.86 | 1.04 | 1.16 | 1.20 | 1.51 | 1.37 | 1.20 | 1.25 | 1.24 |
| 0.00 | 0.00 | 0.00 | 5.29 | 0.00 | 0.69 | 1.99 | 0.98 | 1.74 | 1.00 | 1.29 | 1.22 | 1.16 | 1.18 | 1.21 |
| 101.43 | 0.00 | 0.00 | 0.00 | 0.00 | 0.57 | 1.01 | 1.08 | 0.92 | 1.00 | 1.01 | 0.97 | 1.08 | 1.01 | 1.01 |
| 0.00 | 0.00 | 42.62 | 10.21 | 1.83 | 0.66 | 1.66 | 0.85 | 1.25 | 1.23 | 0.98 | 1.16 | 1.14 | 1.17 | 1.17 |
| 0.00 | 87.13 | 0.00 | 40.39 | 12.60 | 0.76 | 1.67 | 2.02 | 2.65 | 1.01 | 1.26 | 1.39 | 1.30 | 1.32 | 1.33 |
| 0.00 | 36.27 | 12.89 | 0.00 | 0.00 | 2.31 | 0.62 | 0.95 | 1.22 | 0.95 | 1.06 | 1.07 | 1.02 | 1.03 | 1.05 |
| 734.57 | 89.42 | 16.33 | 0.00 | 0.00 | 0.80 | 1.74 | 0.85 | 1.05 | 1.37 | 1.40 | 1.47 | 1.44 | 1.39 | 1.37 |
| 0.00 | 0.00 | 0.00 | 0.00 | 1.83 | 0.00 | 0.94 | 0.68 | 1.25 | 1.07 | 1.23 | 1.13 | 1.20 | 1.16 | 1.15 |
| 119.52 | 43.49 | 0.00 | 0.00 | 0.00 | 0.00 | 0.28 | 1.01 | 1.58 | 1.50 | 1.34 | 1.24 | 1.39 | 1.33 | 1.33 |
| 0.00 | 0.00 | 26.43 | 4.71 | 1.68 | 0.60 | 0.21 | 0.30 | 1.05 | 0.91 | 1.06 | 1.06 | 1.13 | 1.09 | 1.07 |
| 115.07 | 0.00 | 0.00 | 5.45 | 0.00 | 0.71 | 0.77 | 1.49 | 1.05 | 1.29 | 1.10 | 1.32 | 1.27 | 1.26 | 1.26 |
| 0.00 | 35.09 | 0.00 | 4.39 | 0.00 | 0.55 | 0.39 | 0.55 | 1.55 | 1.13 | 1.01 | 0.99 | 0.96 | 0.99 | 0.99 |
| 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 2.03 | 1.46 | 0.70 | 1.08 | 1.32 | 1.12 | 1.18 | 1.14 | 1.20 | 1.18 |
| 302.54 | 0.00 | 50.71 | 4.49 | 0.00 | 0.00 | 2.00 | 1.92 | 1.08 | 1.10 | 1.19 | 0.99 | 1.02 | 1.03 | 1.00 |
| 345.19 | 41.62 | 30.12 | 0.00 | 0.00 | 1.43 | 0.52 | 1.49 | 0.91 | 1.27 | 1.13 | 1.19 | 1.26 | 1.23 | 1.25 |
| 0.00 | 0.00 | 200.87 | 20.65 | 1.86 | 1.34 | 1.44 | 1.64 | 1.37 | 1.31 | 1.20 | 1.10 | 1.11 | 1.18 | 1.18 |
| 0.00 | 45.13 | 49.50 | 0.00 | 0.00 | 0.00 | 2.36 | 2.26 | 1.30 | 1.17 | 1.18 | 1.40 | 1.36 | 1.34 | 1.38 |
| 0.00 | 74.29 | 79.42 | 4.72 | 3.36 | 1.20 | 1.28 | 1.60 | 1.49 | 1.06 | 0.93 | 0.98 | 1.08 | 1.10 | 1.09 |

Table 3.1: Distribution of α 's of v

| Prime | < .3 | < .35 | < .4 | < .45 | < .5 |
|------------|------|-------|------|-------|------|
| 895917131 | 2 | 0 | 0 | 0 | 0 |
| 593554447 | 0 | 0 | 0 | 1 | 1 |
| 551556059 | 0 | 0 | 2 | 0 | 0 |
| 774712823 | 0 | 0 | 1 | 1 | 0 |
| 961344259 | 0 | 1 | 2 | 1 | 0 |
| 1052502491 | 1 | 1 | 0 | 0 | 0 |
| 877166131 | 0 | 1 | 0 | 1 | 0 |
| 669150091 | 1 | 0 | 0 | 2 | 2 |
| 721235807 | 0 | 0 | 0 | 1 | 0 |
| 997165739 | 1 | 0 | 0 | 0 | 0 |
| 777782111 | 0 | 0 | 3 | 2 | 1 |
| 601873567 | 0 | 2 | 0 | 7 | 6 |
| 976974643 | 0 | 1 | 1 | 0 | 0 |
| 561998999 | 6 | 2 | 1 | 0 | 0 |
| 784308199 | 0 | 0 | 0 | 0 | 1 |
| 604718867 | 1 | 1 | 0 | 0 | 0 |
| 920692687 | 0 | 0 | 2 | 1 | 1 |
| 678600491 | 1 | 0 | 0 | 1 | 0 |
| 1066913867 | 0 | 1 | 0 | 1 | 0 |
| 741799451 | 0 | 0 | 0 | 0 | 0 |
| 1014893507 | 3 | 0 | 4 | 1 | 0 |
| 678813823 | 3 | 1 | 2 | 0 | 0 |
| 759828683 | 0 | 0 | 14 | 4 | 1 |
| 548375899 | 0 | 1 | 3 | 0 | 0 |
| 917289047 | 0 | 2 | 6 | 1 | 2 |

Table 3.2: Number of v 's

We also tried to look at the distribution of v 's from 0 to $p - 1$. For this we made the total length into 10 parts as $\frac{i-1}{10}p$ to $\frac{i}{10}p$ for $i \in \{1, 2, \dots, 10\}$ and calculated the value $\frac{\# \text{ of } v\text{'s in an interval}}{\text{Total } \# \text{ of } v\text{'s}}$. We tabulated the mean and standard deviation of this values for above primes in Table:2.3. Results here show that v 's are uniformly distributed.

| Upper Bd | Mean | Std.Div. |
|----------|---------|----------|
| .1p | 0.10067 | 0.00176 |
| .2p | 0.10059 | 0.00206 |
| .3p | 0.10053 | 0.00220 |
| .4p | 0.10013 | 0.00179 |
| .5p | 0.09914 | 0.00260 |
| .6p | 0.10032 | 0.00184 |
| .7p | 0.09893 | 0.00229 |
| .8p | 0.10035 | 0.00195 |
| .9p | 0.10004 | 0.00222 |
| p | 0.09930 | 0.00209 |

Table 3.3: Distribution of v 's

Chapter 4

Extensions.

4.1 A polynomial time Algorithm.

Here we present another method to solve CSCP, but applicable to 'few' primes only. Let p be given prime then take $n = \lfloor p^{\frac{1}{3}} \rfloor$. So we have

$$n^3 < p < (n + 1)^3.$$

Now let $k = (n + 1)^3 - p$. If $k < \frac{p^{0.5}}{n+1}$, by letting $v = n + 1$ and $z = n + 1$, we have the required solution as seen earlier. Likewise, we can also consider values such as $n^2(n + 1)$, $n^2(n + 2)$, $(n + 1)^2n$, $n^2(n + 3)$. All these values are of the form a^2b where a^2 is the perfect square part of the product and b is the remaining part, they all lie between n^3 and $(n + 1)^3$. Say if any particular a^2b satisfies the following two conditions,

- i) $a^2b > p$
- ii) $k = a^2b - p < \frac{p^{0.5}}{a}$

Then we have a solution by taking $v = a$ and $z = b$.

Though this method takes time polynomial in $\log(p)$, it is applicable only to primes that are 'slightly' smaller than perfect cubes or values of the form a^2b as described above. One can improve this method by looking at more dense set of numbers of the form a^2b than the one described above.

we can see few examples to see the simplicity of this method and also observe how rarely this can be used. We shall consider the primes between 1600^3 and 1601^3 solvable by this method, they are 4098559973, 4098559991, 4098559999, 4101119977, 4101119993, 4101121567, 4103684779. We can see a solution of CSCP when $p = 4098559999$, here $p < 1600^2 \cdot 1601$ and $k = 1$. So by taking $v = 1600$ and $z = 1601$ we have $x = 1$ and $y = 1600$. In a similar way it is easy to solve other primes listed above. In brief, the solutions are given in Table:4.1

But this is very small number of total number of primes in this interval. In the interval from 10^3 to 11^3 , we can use this method only for 2 of the 49 primes.

| Prime | v | z | k or x |
|------------|------|------|------------|
| 4098559973 | 1600 | 1601 | 17 |
| 4098559991 | 1600 | 1601 | 9 |
| 4101119993 | 1600 | 1602 | 7 |
| 4101121567 | 1601 | 1600 | 33 |
| 4101119977 | 1600 | 1602 | 23 |
| 4103684779 | 1601 | 1601 | 22 |

Table 4.1: Solutions

4.2 Further improvements to consider.

As described earlier, algorithm in Chapter.3 uses gap in 'suitable z ' for a fixed v . In a similar way we can try to work with gap in 'suitable v ' for a fixed z . But, we believe to have good improvement by finding a 'better' (v_1, z_1) pair for given (v_0, z_0) pair that is not part of any solution. Here by 'better' we aim at having $k_1 < k_0$ where $v_1^2 z_1 = l_1 p + k_1$ and $v_0^2 z_0 = l_0 p + k_0$.

We can also transform CSC to a quadratic form by taking $y_1 \equiv x^{-1} y z \pmod{p}$. After this, the new relation is

$$y_1^2 \equiv x z \pmod{p} \tag{4.1}$$

But in this transformation one has to work on understanding how the bounding condition, x , y and z are of order p^α for $\frac{1}{3} \leq \alpha \leq \frac{1}{2}$, is transformed.

Bibliography

- [1] A. Das. Galois Field Computations: Implementation of a library and a study of the discrete logarithm problem. *Ph.D. Thesis*, Indian Institute of Science, Bangalore, India, 1999.
- [2] A. K. Lenstra and H. W. Lenstra, Algorithms in Number Theory, In *Handbook of Theoretical Computer Science*, pages 675-715, 1990.
- [3] A. K. Lenstra and H. W. Lenstra, Eds, The development of the Number Field Sieve, *Lecture Notes in Mathematics #1554*, Springer-Verlag, 1993.
- [4] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge University Press, 1994.
- [5] A. Odlyzko, Discrete logarithms and their Cryptographic significance, In *Eurocrypt'84*, *Lecture Notes in Computer Science #209*, pages 224-314, Springer-Verlag, 1985.
- [6] D. R. Stinson, *Cryptography Theory and Practice*. 2nd Edition, CRC Press, 2002.