Cubic Sieve Congruence of the Discrete Logarithm Problem, and Fractional Part Sequences ⋆

Srinivas Vivek *

University of Luxembourg, Luxembourg

C. E. Veni Madhavan

Department of Computer Science and Automation, Indian Institute of Science, Bangalore, India

Abstract

The Cubic Sieve Method for solving the Discrete Logarithm Problem in prime fields requires a nontrivial solution to the Cubic Sieve Congruence (CSC) $x^3 \equiv y^2 z \pmod{p}$, where p is a given prime number. A nontrivial solution must also satisfy $x^3 \neq y^2 z$ and $1 \leq x, y, z < p^\alpha$, where α is a given real number such that $\frac{1}{3} < \alpha \leq \frac{1}{2}$. The CSC problem is to find an efficient algorithm to obtain a nontrivial solution to CSC. CSC can be parametrized as $x \equiv v^2 z \pmod{p}$ and $y \equiv v^3 z \pmod{p}$. In this paper, we give a deterministic polynomial-time ($O(\ln^3 p)$ bit-operations) algorithm to determine, for a given v, a nontrivial solution to CSC, if one exists. Previously it took $\widetilde{O}(p^\alpha)$ time in the worst case to determine this. We relate the CSC problem to the gap problem of fractional part sequences, where we need to determine the non-negative integers N satisfying the fractional part inequality $\{\theta N\} < \phi$ (θ and ϕ are given real numbers). The correspondence between the CSC problem and the gap problem is that determining the parameter z in the former problem corresponds to determining N in the latter problem. We also show in the $\alpha = \frac{1}{2}$ case of CSC that for a certain class of primes the CSC problem can be solved deterministically in $\widetilde{O}\left(p^{\frac{1}{3}}\right)$ time compared to the previous best of $\widetilde{O}\left(p^{\frac{1}{2}}\right)$. It is empirically observed that about one out of three primes is covered by the above class.

Key words: computational number theory, cryptanalysis, Diophantine equation, discrete logarithm problem, fractional part sequence
1991 MSC: [2010] 11D79, 11Y16, 11Y50

1. Introduction

The Cubic Sieve is a variant of the Index Calculus Method for the Discrete Logarithm Problem (DLP) in fields of prime order Coppersmith et al. (1986); Das (1999); Das and Veni Madhavan (2005); Lenstra and Lenstra Jr. (1990); Menezes et al. (1997); Schirokauer et al. (1996). It was first proposed in Coppersmith et al. (1986). Working of the cubic sieve method requires a nontrivial solution (in positive integers) to a Diophantine equation called the Cubic Sieve Congruence (CSC, for short) $x^3 \equiv y^2 z \pmod{p}$, where p is a given prime number. A nontrivial solution to CSC must satisfy

$$x^3 \equiv y^2 z \pmod{p}, \quad x^3 \neq y^2 z, \quad 1 \leq x,\, y,\, z < p^{\alpha}, \tag{1}$$

where α is a given real number that satisfies $\frac{1}{3} < \alpha \leq \frac{1}{2}$. Henceforth the above equation will be referred to as CSC (1). Note that CSC (1) cannot be satisfied if $1 \leq x,\, y,\, z \leq p^{\frac{1}{3}}$. When x, y, and z are of the order $O(p^{\alpha})$, then the heuristic expected running time of the cubic sieve is $L_p\left[\gamma = \frac{1}{2},\, c = \sqrt{2\alpha}\right] = \exp\left((c + o(1))\,(\ln p)^{\gamma}\,(\ln \ln p)^{1-\gamma}\right)$, where $\ln p$ denotes the natural logarithm of p. Hence smaller values of α lead to faster running times. It is important to note that this estimate of the running time of cubic sieve does not take into account the time required for finding a nontrivial solution to CSC. Therefore, an important open problem concerning the cubic sieve method is to develop an efficient algorithm to determine a nontrivial solution to CSC, given p and α. We shall refer to this problem as the *CSC problem*.

The Number Field Sieve is the current best algorithm for DLP in prime fields with the heuristic expected running time of $L_p\left[\frac{1}{3},\, \left(\frac{64}{9}\right)^{\frac{1}{3}}\right]$. Hence the cubic sieve method is mostly of theoretical interest to cryptography. Apart from the cryptographic connection, the CSC problem is a challenging problem in computational number theory and is interesting in its own right. Some attempts to solve this problem have been made in Das (1999); Das and Veni Madhavan (2005); Maitra et al. (2009). Recently, the parametrization $x \equiv v^2 z \pmod{p}$ and $y \equiv v^3 z \pmod{p}$ (Equation (2)) was introduced by Maitra et. al. Maitra et al. (2009).

In this paper, we make further progress towards finding an efficient algorithm for the CSC problem by showing that we can determine in deterministic polynomial time whether a solution to CSC (Equation (2)) exists for a given v ($1 \leq v < p$). If one exists, we show that we can also compute it efficiently. Previously, the only way to determine this was to check all the values of z from 1 to p^{α}. We were able to accomplish this by relating the above problem to the *gap problem* of fractional part sequences Slater (1950, 1967). As a consequence, we show in the $\alpha = \frac{1}{2}$ case of CSC (1) that for primes "close" to i^{ϵ} (integer i, real $\epsilon \in [3, 4]$), a solution to CSC exists and it can be computed deterministically in $\widetilde{O}\left(p^{\frac{1}{3}}\right)$ time [1], while the previous best is $\widetilde{O}\left(p^{\frac{1}{2}}\right)$. Interestingly, we

---

⋆ Abstract of this work appeared in the third Workshop on Mathematical Cryptology (WMC 2012) held at CIEM-Castro Urdiales, Spain, on 9-11 July 2012.

* Corresponding Author. Postal address: University of Luxembourg, FSTC, 6 rue Richard Coudenhove-Kalergi, L-1359 Luxembourg. Tel: +352 46 66 44 6224. Fax: +352 46 66 44 5500.

Email addresses: srinivasvivek.venkatesh@uni.lu (Srinivas Vivek), cevm@csa.iisc.ernet.in (C. E. Veni Madhavan).

[1] The running times of the algorithms related to the CSC problem reflect the total number of bit operations required. In order to avoid cluttering the running time expressions with logarithmic factors, we often use the soft-oh notation $\widetilde{O}$ Cormen et al. (2001, pp. 59). The implicit logarithmic factor is $\ln^3 p$.

Algorithm 1 Solving CSC (1) given p, α and δ ($\delta > 0$).

(1) For $x \leftarrow 1$ to $\left\lfloor p^{\frac{1}{3}+\delta} \right\rfloor$
  (a) For $y \leftarrow 1$ to $\left\lfloor p^{\frac{1}{3}+\delta} \right\rfloor$
    (i) $z \leftarrow x^3 y^{-2} \pmod p$
    (ii) If (x, y, z) satisfies CSC (1), then Return (x, y, z).

have empirically observed that about one-third of all the primes are covered by the above class.

The rest of the paper is organized as follows. In Section 2, we briefly discuss the previous results on the CSC problem. In Section 3, we generalize a heuristic algorithm described in Maitra et al. (2009) for the $\alpha = \frac{1}{2}$ case of CSC to a generic α $\left(\frac{1}{3} < \alpha \leq \frac{1}{2}\right)$. Later in that section, we make some remarks on the non-applicability of the LLL and other lattice basis reduction algorithms for solving the CSC problem. Previous results on the distribution of the non-negative integers N satisfying the fractional part inequality $\{\theta N\} < \phi$ (rational θ, real ϕ are given) is presented in Section 4, and we shall also see there how to efficiently compute the least such N. In Section 5, we will extend the results of Section 4 to efficiently determine the least common N satisfying both $\{\theta N\} < \phi$ and $\left\{\hat{\theta} N\right\} < \hat{\phi}$ (both θ and $\hat{\theta}$ are rational), when certain conditions on θ, $\hat{\theta}$, ϕ, $\hat{\phi}$ and N are satisfied. As a consequence we shall see how, given any v, we can efficiently determine a solution to CSC. The existence of solutions for primes "close" to i^ϵ, and consequently lesser time to compute them, is presented in Section 6. We finally conclude in Section 7.

2. Previous Work

Let $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{N}$ denote, respectively, the set of real numbers, the set of integers and the set of positive integers. Throughout this paper, the variable p represents a prime number, $\alpha \in \mathbb{R}$, $\frac{1}{3} < \alpha \leq \frac{1}{2}$, and by $n \pmod p$ (for $n \in \mathbb{Z}$) we mean the least non-negative remainder obtained on dividing n by p. The symbols $\lfloor . \rfloor$, $\lceil . \rceil$ and $\{.\}$ denote the floor, ceiling and fractional part, respectively, of a real value.

When primes are close to (but less than) perfect cubes, then we can directly get the solution $x = \lceil p^{\frac{1}{3}} \rceil$, $y = 1$ and $z = x^3 - p$, satisfying CSC (1). Since this method will not work for many primes, we need a systematic approach. The simplest algorithm to compute a solution to CSC (1) is to vary x and y from 1 to p^α, and check if (x, y) satisfies CSC (1). Clearly, the worst-case running time of this algorithm is $\widetilde{O}\left(p^{2\alpha}\right)$.

The first non-trivial (heuristic) algorithm for the CSC problem is due to Das (1999); Das and Veni Madhavan (2005). It is based on a heuristic estimate that the number of solutions to CSC (1) is approximately $p^{3\alpha-1}$. An evidence for the estimate is obtained by observing that the probability of $z \equiv x^3 y^{-2} \pmod p$ being less than p^α is $p^{\alpha-1}$ Maitra et al. (2009). Interestingly, the question of non-emptiness of the solution set of CSC (1) for all but finitely many primes is still open. We now obtain Algorithm 1 for the CSC problem.

In Algorithm 1, $\delta > 0$ must be sufficiently large to ensure that there are "enough" solutions. Clearly, the running time of Algorithm 1 is $\widetilde{O}\left(p^{\frac{2}{3}+o(1)}\right)$ when $\delta = o(1)$. Note that the x, y and z we get as a solution are of magnitude $O\left(p^{\frac{1}{3}+o(1)}\right)$ and are independent

Algorithm 2 Solving CSC (2) given p and α.

(1) For $v \leftarrow 1$ to $p-1$
  (a) For $z \leftarrow 1$ to $\lceil p^{\alpha} \rceil - 1$
    (i) $x \leftarrow v^2 z \pmod p$, $y \leftarrow v^3 z \pmod p$
    (ii) If $(v,\, z)$ satisfies CSC (2), then
      (A) Return $(x,\, y,\, z)$.

of α. By assuming that the solutions of CSC (1) are uniform randomly distributed in the range $1 \leq x,\, y < p^{\frac{1}{3}+\delta}$, and consequently the probability that a randomly selected pair $(x,\, y)$ $\left(1 \leq x,\, y < p^{\frac{1}{3}+\delta}\right)$ satisfies CSC (1) being $\frac{p^{3\left(\frac{1}{3}+\delta\right)-1}}{p^{2\left(\frac{1}{3}+\delta\right)}} = p^{\left(\frac{1}{3}+\delta\right)-1}$, we get the (heuristic) expected running time of Algorithm 1 to be $\widetilde{O}\left(p^{1-\left(\frac{1}{3}+\delta\right)}\right) = \widetilde{O}\left(p^{\frac{2}{3}-o(1)}\right)$. However, note that even when we give a value of x for which there is a solution to CSC (1), we cannot efficiently determine a corresponding value of y, and vice-versa. This serves as the motivation for us to study the $(v,\, z)$-parametrization of CSC introduced in Maitra et al. (2009).

The next major attempt at solving the CSC problem was by Maitra et al. (2009). They parametrized $x^3 \equiv y^2 z \pmod p$ as

$$\left(\frac{y}{x}\right)^2 \equiv \frac{x}{z} \equiv v^2 \pmod p \quad \Leftrightarrow \quad x \equiv v^2 z \pmod p,\ y \equiv v^3 z \pmod p.$$

Hence CSC (1) can be equivalently written as

$$x \equiv v^2 z \pmod p,\ y \equiv v^3 z \pmod p,\ x^3 \neq y^2 z,\ 1 \leq x,\, y,\, z < p^{\alpha},\ 1 \leq v < p. \qquad (2)$$

We refer to the above equation as CSC (2).

Based on CSC (2), we obtain Algorithm 2. The worst-case running time of Algorithm 2 is $\widetilde{O}\left(p^{1+\alpha}\right)$ and the (heuristic) expected running time is $\widetilde{O}\left(p^{2-2\alpha}\right)$. Note that the worst-case and the expected running time of Algorithm 2 is worse than that of Algorithm 1.

Throughout Maitra et al. (2009), only the $\alpha = \frac{1}{2}$ case is dealt. It is shown for $v < p^{\frac{1}{2}}$ that we can optimize the inner loop of Algorithm 2. This is made possible by exploiting the properties of solutions to CSC (2) ($\alpha = \frac{1}{2}$). As a consequence they show that the solutions can be efficiently computed for those primes "close" to (but less than) the fourth powers. In the next section, we generalize the optimized version of Algorithm 2 in Maitra et al. (2009) (for the $\alpha = \frac{1}{2}$ case) to a general α $\left(\frac{1}{3} < \alpha \leq \frac{1}{2}\right)$. Hence, in order to avoid repetition, we refrain from further describing the results of Maitra et al. (2009). More details on the efficient computation of solutions for primes close to fourth powers can be found in Section 6.

3. Heuristic Algorithm and Some Remarks

In this section and in Sections 4 and 5, α can take any real value such that $\frac{1}{3} < \alpha \leq \frac{1}{2}$. Throughout the remainder of the paper, we will work with the $(v,\, z)$-parametrization given by CSC (2). The results presented in this section follow in a straightforward manner from those corresponding to the case of $\alpha = \frac{1}{2}$ in Maitra et al. (2009).

Algorithm 3 Solving CSC (2) such that $v < p^{\alpha}$, given p and α.

(1) For $v \leftarrow \left\lfloor p^{\frac{1-\alpha}{2}} \right\rfloor + 1$ to $\lceil p^{\alpha} \rceil - 1$
  (a) For $j \leftarrow 1$ to $\left\lfloor \frac{v^2}{p^{1-\alpha}} \right\rfloor$
    (i) $z \leftarrow \left\lceil \frac{j\,p}{v^2} \right\rceil$
    (ii) $x \leftarrow v^2 z \pmod p$
    (iii) If $(x < \frac{p^{\alpha}}{v})$, then Return $(x,\, y \leftarrow vx,\, z)$.

Proposition 1. *If $x, y, z, v < p^{\alpha}$, $x \equiv v^2 z \pmod p$ and $y \equiv v^3 z \pmod p$, then the condition $x^3 \neq y^2 z$ is equivalent to $x \neq v^2 z$.*

Proof. The condition $v,\, x < p^{\alpha}$ implies that $vx < p$. Since $y \equiv v^3 z \equiv vx \pmod p$, we have $y = vx$. Therefore, $x^3 \neq y^2 z \Leftrightarrow x^3 \neq (vx)^2 z \Leftrightarrow x \neq v^2 z \Leftrightarrow x < v^2 z$. □

We now obtain the following corollaries from Proposition 1 and its proof.

Corollary 2. *If $1 \leq v \leq p^{\frac{1-\alpha}{2}}$ or $p^{\alpha} \leq v \leq p^{1-\alpha}$, then corresponding to v there exists no solution to* CSC (2).

Proof. If $1 \leq v \leq p^{1-\alpha}$, then $y \equiv vx \pmod p$ implies that $y = vx$. If $p^{\alpha} \leq v \leq p^{1-\alpha}$, then $y \geq p^{\alpha}$. Hence there can be no solution. If $\alpha > \frac{1}{3}$ and $1 \leq v \leq p^{\frac{1-\alpha}{2}}$, then from Proposition 1, we have $x^3 = y^2 z$ and hence there can exist no solution to CSC (2). □

Note that when $\alpha = \frac{1}{2}$, then $p^{\alpha} = p^{1-\alpha} = p^{\frac{1}{2}}$.

Corollary 3. *Corresponding to $v < p^{\alpha}$ if there exists a solution to* CSC (2), *then $x < \frac{p^{\alpha}}{v}$.*

Using the above results, we obtain Algorithm 3 for solving CSC (2) for those primes which have a solution for $v < p^{\alpha}$. An example of a prime for which there is no solution to CSC (2) for $v < p^{\alpha}$ $(\frac{1}{3} < \alpha \leq \frac{1}{2})$ is 101.

The step 1.(a).i of Algorithm 3 is an optimized version of the corresponding step 1.(a) of Algorithm 2. The inner loop of Algorithm 2 corresponds to the arithmetic progression $v^2 z$ (varying z for a fixed v). Hence between any two multiples of p, we need to consider only the first term of the progression. The expression $z \leftarrow \left\lceil \frac{j\,p}{v^2} \right\rceil$ in Algorithm 3 precisely corresponds to these terms. The upper bound on the index j is obtained by observing that $j\,p \leq v^2 p^{\alpha}$. The fact that $v^2 \nmid p$ $(1 < v < p^{\alpha})$ and that $j \geq 1$ ensures that $v^2 z > p$.

Since $v^2 < p^{2\alpha} \leq p$, in the worst case, there are exactly $\left\lfloor \frac{v^2}{p^{1-\alpha}} \right\rfloor$ iterations of the inner for-loop corresponding to j. Hence the running time of Algorithm 3 is

$$\widetilde{O}\left(\frac{1}{p^{1-\alpha}} \sum_{v=p^{\frac{1-\alpha}{2}}}^{p^{\alpha}} v^2 \right) = \widetilde{O}\left(\frac{p^{3\alpha}}{p^{1-\alpha}} \right) = \widetilde{O}\big(p^{4\alpha-1}\big)\,.$$

When $\alpha < \frac{1}{2}$, this algorithm is asymptotically faster than the $\widetilde{O}\big(p^{2\alpha}\big)$-algorithm we obtain when z is incremented only by 1 at a time. This algorithm runs in polynomial time for those primes p which have a solution to CSC (2) for $v \approx p^{\frac{1-\alpha}{2}}$. It is shown in the

$\alpha = \frac{1}{2}$ case that there are infinitely many primes which have a solution for $v \approx p^{\frac{1}{4}}$ Maitra et al. (2009). The (heuristic) expected running time of Algorithm 3 is the same as its worst-case running time. This is because the expected number of solutions for $v < p^{\alpha}$ is $p^{4\alpha-2}$, which is at most 1 for $\alpha \leq \frac{1}{2}$. Note that these running times are worse compared to that of Algorithm 1.

In the inner loop of Algorithm 3, we were trying to determine a z ($z < p^{\alpha}$), for a given v ($v < p^{\alpha}$), such that $v^2 z \pmod p < \frac{p^{\alpha}}{v}$, or equivalently $\left\{ \frac{v^2 \pmod p}{p} z \right\} < \frac{1}{p} \left(\frac{p^{\alpha}}{v} \right)$. Using previous results on the gap problem of fractional part sequences, we shall see in the next section that such a (least) z can be computed deterministically in polynomial time, and hence the running time of Algorithm 3 can be reduced to $\widetilde{O}(p^{\alpha})$. The fact that not all primes have a solution to CSC (2) corresponding to $v < p^{\alpha}$, and that the range $\left(p^{\frac{1-\alpha}{2}}, p^{\alpha} \right)$ shrinks to zero length as $\alpha \to \frac{1}{3}$ (for a fixed p), provides us a motivation to pursue the following problem. To find a common z ($z < p^{\alpha}$) simultaneously satisfying the two inequalities $\left\{ \frac{v^2 \pmod p}{p} z \right\} < \frac{p^{\alpha}}{p}$ and $\left\{ \frac{v^3 \pmod p}{p} z \right\} < \frac{p^{\alpha}}{p}$, and also satisfying the condition $x^3 \neq y^2 z$. In Section 5, we provide a deterministic polynomial-time algorithm to this problem by extending the results for the single inequality case, thereby reducing the worst-case running time of Algorithm 2 to $\widetilde{O}(p)$ and the expected running time of Algorithm 2 to $\widetilde{O}\left(p^{2-3\alpha}\right)$.

3.1. Lattice Basis Reduction: Remarks

The problem of finding a common z ($z < p^{\alpha}$) satisfying both $\left\{ \frac{v^2 \pmod p}{p} z \right\} < \frac{p^{\alpha}}{p}$ and $\left\{ \frac{v^3 \pmod p}{p} z \right\} < \frac{p^{\alpha}}{p}$ can be restated as finding pairs (c, d) and ($\hat{c}$, d) such that $1 \leq c, \hat{c}, d < p^{\alpha}$, $c \equiv d r \pmod p$ and $\hat{c} \equiv d \hat{r} \pmod p$, where $r = v^2 \pmod p$, $\hat{r} = v^3 \pmod p$ and $d = z$. Note that all the (c, d) (no restriction on the values of c and d) satisfying $c \equiv d r \pmod p$ form a two dimensional lattice. Similarly, the ($\hat{c}$, $\hat{d}$) satisfying $\hat{c} \equiv \hat{d} \hat{r} \pmod p$ form another lattice. Hence we are looking for a "short" vector on each of the two lattices such that both the vectors have the same value in the second coordinate ($d = \hat{d}$).

The LLL or other lattice basis reduction algorithms do not seem to be of much use in our case, though the shortest vector problem in two dimensions can be exactly solved in deterministic polynomial time (Lenstra Jr., 2008; Micciancio and Goldwasser, 2002). The problem seems to lie in the fact that the condition $x^3 \neq y^2 z$ in CSC (2) does not have a geometric analogue unlike the rest of the conditions, as seen in the previous paragraph. Let us try to examine this issue in the case of $v = 1$ in CSC (2). When $v = 1$, we have $r = \hat{r} = 1$ and the lattices $c \equiv d r \pmod p$ and $\hat{c} \equiv \hat{d} \hat{r} \pmod p$ are now identical to $\mathbb{Z} \times \mathbb{Z}$. But the shortest possible pair of vectors ($c = 1$, $d = 1$) and ($\hat{c} = 1$, $\hat{d} = 1$) fail to satisfy the condition $x^3 \neq y^2 z$. Also, no other pair of (exponentially many) "short" vectors in $\mathbb{Z} \times \mathbb{Z}$ can satisfy CSC (2) because when $v = 1$, then $x = y = z$ and hence $x^3 = y^2 z$. In fact, as we have seen in Corollary 2, there are no solutions to CSC (2) corresponding to $1 \leq v \leq p^{\frac{1-\alpha}{2}}$ and $p^{\alpha} \leq v \leq p^{1-\alpha}$. However if v is sufficiently large, then we may be able to heuristically argue that the condition $x^3 \neq y^2 z$ holds with a high probability. But our goal is to obtain a deterministic polynomial time method to determine whether there exists a solution to CSC (2) for a given value of v. Hence trying to compute short lattice vectors until the condition $x^3 \neq y^2 z$ is satisfied does not seem to work in our case.

4. Solving a Fractional Part Inequality

In the previous section, we saw that the Algorithm 3 would considerably speed up if we could efficiently determine a z such that $\left\{\frac{v^2 \pmod p}{p}\, z\right\} < \frac{1}{p}\left(\frac{p^\alpha}{v}\right)$. Let us consider a more general problem of determining an N (for a given θ and ϕ) such that

$$\{\theta N\} < \phi, \quad \text{where} \quad \theta,\, \phi \in \mathbb{R},\ 0 < \theta,\, \phi < 1,\ N \in \mathbb{N} \cup \{0\}. \tag{3}$$

The restrictions on θ and ϕ will not lead to any loss of generality because $0 \leq \{\theta N\} < 1$ and $\{(m+\theta)N\} = \{\theta N\} \quad \forall\, m \in \mathbb{Z}$. The problem of determining the gaps between the successive N satisfying (3) is known as the *gap problem* Slater (1967). The distribution of the N satisfying (3) was first studied in Slater (1950). It is shown, for both rational and irrational θ, that the successive N satisfying (3) is separated by gaps of at most three different lengths, one being the sum of the other two.

A related problem is the *step problem* Slater (1967). The problem is to determine the steps into which the interval [0, 1] is partitioned when the values $\{1\theta\}$, $\{2\theta\}$, ..., $\{N\theta\}$ are arranged in the ascending order. A result analogous to that of the gap problem is applicable to the step problem. For more details on this and other related problems, we refer the reader to Drobot (1987); Fraenkel and Holzman (1995); Halton (1965); Slater (1964, 1967). When θ is irrational, the sequence $N\theta$ $(N \geq 0)$ is uniformly distributed modulo 1 Graham et al. (1994, pp. 87). Throughout the rest of the paper, we shall confine ourselves to the case of θ being rational.

Let $\theta = \frac{r}{q}$, $r,\, q \in \mathbb{N}$, $r < q$ and $\gcd(r,\, q) = 1$. Solving the inequality $\{\theta N\} < \phi$ for N is equivalent to solving $rN \pmod q < T$, where $T = \lceil \phi q \rceil$. Henceforth, let ϕ be of the form $\phi = \frac{T}{q}$, where $0 < T < q$. Note that the inequality $rN \pmod q < T$ has exactly T solutions for $0 \leq N < q$. Also note that the sequence of fractional parts $\{N\theta\}$ is periodic with period q. From these observations, let us rewrite (3) as follows

$$\{\theta N\} < \phi, \quad \text{where} \quad \theta = \frac{r}{q},\ \phi = \frac{T}{q},\ 1 \leq r,\, T < q,\ \gcd(r,\, q) = 1, \tag{4}$$

$r,\, T,\, q \in \mathbb{N}$, and $N \in \mathbb{N} \cup \{0\}$.

The following preliminary continued fraction formulae will be useful in further discussions. Many of these can be found, for instance, in Hensley (2006, pp. 6). Let θ be as defined in (4). Let the simple continued fraction expansion of θ be

$$\theta = \frac{r}{q} = [0;\, a_1,\, a_2,\, \ldots,\, a_n], \quad \text{where} \quad a_i \in \mathbb{N},\ a_n > 1. \tag{5}$$

The s^{th}convergent to θ is

$$\frac{r_s}{q_s} = [0;\, a_1,\, a_2,\, \ldots,\, a_s], \quad \text{where} \quad \gcd(r_s,\, q_s) = 1,\ 1 \leq s \leq n, \tag{6}$$

$r_0 = 0$ and $q_0 = 1$. Let q_s be the simple continuant of $a_1,\, a_2,\, \ldots,\, a_s$, then it satisfies

$$q_s = a_s\, q_{s-1} + q_{s-2} \quad \text{where} \quad 1 \leq s \leq n,\ q_0 = 1,\ q_{-1} = 0. \tag{7}$$

Note that r_s is the simple continuant of $a_2,\, a_3,\, \ldots,\, a_s$ $(2 \leq s \leq n, r_1 = 1, r_0 = 0)$, $r_n = r$ and $q_n = q$. Let Q_s be the simple continuant of $a_n,\, a_{n-1},\, \ldots,\, a_{n-s+1}$ $(1 \leq s \leq n, Q_0 = 1,$ $Q_{-1} = 0)$. Particular values of Q_i are $Q_n = q_n = q$, $Q_{n-1} = r_n = r$ and $Q_1 = a_n$. The Q_i satisfy

$$Q_{n-s+1} = a_s\, Q_{n-s} + Q_{n-s-1} \quad (1 \le s \le n), \tag{8}$$

$$q_s\, Q_{n-s} + q_{s-1}\, Q_{n-s-1} = q \quad (0 \le s \le n), \tag{9}$$

$$Q_{n-s} = (-1)^{s-1}\,(r\, q_{s-1} - q\, r_{s-1}) \quad (1 \le s \le n+1). \tag{10}$$

Let A_s be the s^{th} complete quotient of θ, where

$$\frac{1}{A_s} = [0;\, a_s,\, a_{s+1},\, \ldots,\, a_n] = \frac{Q_{n-s}}{Q_{n-s+1}} \quad (1 \le s \le n). \tag{11}$$

Remark 4. Most of the results in this section can be found in Slater (1950, Part 1) and the rest can be easily derived from it. There are only a few notational changes we have made when using their results. The variables x, p_i $(1 \le i \le n)$, Z, Z_0 and α in Slater (1950, Part 1) have been replaced by, respectively, θ, r_i $(1 \le i \le n)$, T, T_0 and γ. For the sake of completeness, we have collected the required results in this section. We often refer to Lemma 5, Theorems 6 and 9, Corollaries 7, 8 and 10, and Equations (5) - (13) mentioned here. The ideas of this section are needed in the next section.

The T given in (4) can be uniquely represented as $T = T_0(s,\, b) + c$, as defined by Lemma 5.

Lemma 5. *Any $T \in \mathbb{N}$, $0 < T < q$, may be expressed uniquely as*

$$T = T_0 + c, \tag{12}$$

$$\begin{gathered} \textit{where} \quad T_0 = T_0(s,\, b) = (b+1)\, Q_{n-s} + Q_{n-s-1}, \\ \textit{with} \quad b = 0,\, 1,\, \ldots,\, a_s - 1 \quad \textit{if} \quad s = 2,\, 3,\, \ldots,\, n, \\ \textit{with} \quad b = 0,\, 1,\, \ldots,\, a_1 - 2 \quad \textit{if} \quad s = 1, \\ \textit{and} \quad c = 0,\, 1,\, \ldots,\, Q_{n-s} - 1. \end{gathered} \tag{13}$$

Whenever we write T_0 or $T_0(s,\, b)$ (or, T_0', T_0'', $\hat{T}_0$ and $\hat{T}_0'$), we always refer to the "special numbers" of (13). Unless the parameters s ($\hat{s}$ or s') and b ($\hat{b}$ or b') are explicitly manipulated, say as in $T_0(s,\, b+1)$, by writing $T_0(s,\, b) = T_0$, we always mean that s and b are as uniquely determined according to (13).

Theorem 6 below describes all the N that satisfy (4) for T_0. By writing "(4) for $(\theta,\, T_0)$," we mean that $\theta = \theta$ and $T = T_0$ in (4). If the value of θ is clear from the context, then we will simply write "(4) for T_0."

Theorem 6. *The non-negative N satisfying* (4) *for $T_0(s,\, b)$ are*

$$N(\gamma,\, \beta) = \gamma\, q_{s-1} + \beta\,(q_s - b\, q_{s-1})$$

where, if s is even, $\beta = \gamma = 0$, or $\beta = 1,\, 2,\, 3,\, \ldots$

$$\textit{with} \quad \gamma \in \{\lfloor (\beta - 1)\; B_s \rfloor\,,\; \lfloor (\beta - 1)\; B_s \rfloor + 1,\; \ldots,\; \lfloor \beta\, B_s \rfloor\}\,,$$

where, if s is odd, $\beta = 0,\, 1,\, 2,\, \ldots$

$$\textit{with} \quad \gamma \in \{\lceil \beta\, B_s \rceil\,,\; \lceil \beta\, B_s \rceil + 1,\; \ldots,\; \lceil (\beta+1)\, B_s \rceil\}\,,$$

and $B_s = b + \frac{1}{A_{s+1}}$, define $B_n = b$.

Algorithm 4 Given θ (r, q) and T, to compute the least positive N satisfying (4) for T.

(1) Determine $T_0'(s', b')$ (the least value satisfying (13) such that $T_0' \geq T$) using Lemma 5.
(2) Compute, using Theorem 6, the first two positive values of N, say N_1 and N_2 $(N_1 < N_2)$, satisfying (4) for T_0'.
(3) If N_1 satisfies (4) for T, then Return N_1, else Return N_2.

From the above theorem it follows that in the case of (4) for T_0, there are only two gap-lengths separating the successive N satisfying (4) for T_0 (except when $T_0 = 1$). We also obtain Corollaries 7 and 8 from Theorem 6.

Corollary 7. *The successive N satisfying (4) for $T_0(s, b)$ are separated by only two gap-lengths q_{s-1} and $q_s - b\,q_{s-1}$, and the number of gaps for $0 \leq N \leq q$ are $T_0 - Q_{n-s}$ and Q_{n-s}, respectively. The larger gap-length is $q_s - b\,q_{s-1}$ while the smaller one is q_{s-1}.*

Note that $T_0 - Q_{n-s} = 0$ only when $T_0 = 1$. It is easy to see that for any value of θ in (4), $T = 1$ is always a special number of (13). When $T_0(s, b) > 1$, then $B_s > 0$.

Corollary 8. *When $1 < T_0 < q$, the gap-lengths in* Corollary 7 *are different. If s is even, then the first gap is the larger gap $(q_s - b\,q_{s-1})$, followed by $\lfloor B_s \rfloor$ smaller gaps (q_{s-1}). If s is odd, then the first $\lceil B_s \rceil$ gaps are the smaller gaps, followed by one larger gap.*

Theorem 9 below is a generic version of Theorem 6 which is valid for any value of T $(0 < T < q)$. Theorem 9 is known in the literature as "Slater's three-gap theorem" Fraenkel and Holzman (1995). Corollary 10 follows from Theorem 9.

Theorem 9. *Let $T = T_0(s, b) + c$ be the representation determined by (12). The N satisfying (4) for T are separated by only three gap-lengths q_{s-1}, $q_s - b\,q_{s-1}$ and $q_s - (b+1)\,q_{s-1}$. The number of these gaps, for $0 \leq N \leq q$, are $T - Q_{n-s}$, $Q_{n-s} - c$ and c, respectively. The largest gap-length is $q_s - b\,q_{s-1}$, which is the same as the larger gap-length corresponding to (4) for T_0. The other two gaps of gap-lengths $q_s - (b+1)\,q_{s-1}$ and q_{s-1} are obtained by splitting the larger gap corresponding to (4) for T_0.*

Corollary 10. *Let $T = T_0(s, b) + c$ (by (12)), and $T_0'(s', b')$ be the least value satisfying (13) such that $T_0' \geq T$. If N_1 and N_2 are two consecutive values satisfying (4) for T_0', then N_1 or N_2 (or both) satisfy (4) for T_0, and hence also satisfy (4) for T.*

Corollary 10 suggests that in order to compute the least positive N satisfying (4), then it suffices to compute the first two positive N satisfying (4) for T_0'. These two values of N are in turn computed using Theorem 6. Using this idea we now obtain Algorithm 4.

Proposition 11. *The running time of* Algorithm 4 *is $O\big(\ln^3 q\big)$ bit-operations.*

This follows from the fact that the extended Euclidean algorithm terminates in $O(\ln q)$ steps and requires $O\big(\ln^3 q\big)$ bit-operations when run on the inputs r and q. Hence the length of the continued fraction expansion of θ is $O(\ln q)$. The continuants q_s and Q_s $(1 \leq s \leq n)$ can be computed with $O\big(\ln^3 q\big)$ bit-operations, and so are each of the steps in Algorithm 4.

Using Algorithm 4, we can significantly speed up Algorithm 3. We can replace the inner loop of Algorithm 3 by a call to Algorithm 4 with $\theta = \frac{v^2 \pmod p}{p}$ ($r = v^2 \pmod p$, $q = p$) and $T = \left\lceil \frac{p^\alpha}{v} \right\rceil$. We must also perform a check whether the returned value, say z, satisfies $z < p^\alpha$. The worst-case and the expected running time of Algorithm 3 is now reduced to $\widetilde{O}(p^\alpha)$ from $\widetilde{O}\left(p^{4\alpha-1}\right)$.

5. Solving Simultaneous Fractional Part Inequalities

In the previous section, we saw how to efficiently compute the least positive N satisfying $\{\theta N\} < \phi$, when θ is a rational number. The Algorithm 2 for the CSC problem suggests us to solve a generalization of the above problem. More precisely, we need to efficiently determine the least positive N simultaneously satisfying both $\{\theta N\} < \phi$ and $\left\{\hat{\theta} N\right\} < \hat{\phi}$, for rational θ and $\hat{\theta}$ (θ, $\hat{\theta}$, ϕ and $\hat{\phi}$ are given).

The problem of explicitly determining such an N has not been addressed before. A related existential result is that the successive (non-negative) N satisfying both $\{\theta N\} < \phi$ and $\left\{\hat{\theta} N\right\} < \hat{\phi}$ are separated by finitely many gaps (θ, $\hat{\theta}$ are either rational or irrational). It is easy to show this result for θ and $\hat{\theta}$ both being rational. For more details on this and other related results refer to Fraenkel and Holzman (1995); Slater (1964). As assumed in the previous section, θ and $\hat{\theta}$ will always denote rational numbers in the interval (0, 1).

Consider the two inequalities (the first same as (4))

$$\{\theta N\} < \phi, \quad \text{where} \quad \theta = \frac{r}{q},\ \phi = \frac{T}{q},\ 1 \le r,\ T < q,\ \gcd(r,\ q) = 1, \tag{14}$$

and

$$\left\{\hat{\theta} N\right\} < \hat{\phi}, \quad \text{where} \quad \hat{\theta} = \frac{\hat{r}}{\hat{q}},\ \hat{\phi} = \frac{\hat{T}}{\hat{q}},\ 1 \le \hat{r},\ \hat{T} < \hat{q},\ \gcd(\hat{r},\ \hat{q}) = 1, \tag{15}$$

r, T, q, $\hat{r}$, $\hat{T}$, $\hat{q} \in \mathbb{N}$ (given), and $N \in \mathbb{N} \cup \{0\}$ (to be determined).

A straightforward algorithm to compute the least positive N satisfying both (14) and (15) is to successively compute the N satisfying one of (14) or (15) (using Corollary 10 and Theorem 6), until the other inequality is also satisfied. This approach is not efficient as can be seen from the example where $q = \hat{q} = p$ (prime $p > 2$), $r = 1$, $\hat{r} = p - 1$ and $T = \hat{T} = \frac{p+1}{2}$. In this case there is no common (nontrivial) solution to (14) and (15), but this algorithm will still check $\frac{p+1}{2}$ values of N which are less than p.

Designing a polynomial-time algorithm for the generic case of (14) and (15) appears hard. Fortunately, when we apply the restrictions $T \le \left\lceil q^{\frac{1}{2}} \right\rceil$, $\hat{T} \le \left\lceil \hat{q}^{\frac{1}{2}} \right\rceil$, and $N < \left\lceil (\min(q,\ \hat{q}))^{\frac{1}{2}} \right\rceil$, then we can come up with a deterministic polynomial-time algorithm to compute the least positive common N satisfying both (14) and (15). It is easy to guess that the above restrictions are tailor-made for those corresponding to the problem of determining a z ($z < p^\alpha$), for a given v ($1 \le v < p$), such that $(v,\ z)$ satisfies CSC (2). In order to simplify the description of the algorithm, throughout the rest of the section, we shall only consider the instance of (14) and (15) corresponding to CSC (2). The algorithm for the generic case (with the above mentioned restrictions) can be easily derived from Algorithm 5.

In the case of CSC (2) (given prime p ($p \geq 3$), v ($1 \leq v < p$), and α ($\frac{1}{3} < \alpha \leq \frac{1}{2}$)), the equations (14) and (15) become

$$\{\theta Z\} < \phi, \quad \text{where} \quad \theta = \frac{r}{p},\ \phi = \frac{T}{p},\ r = v^2 \,(\mathrm{mod}\, p),\ T = \lceil p^\alpha \rceil, \tag{16}$$

and

$$\left\{\hat{\theta} Z\right\} < \hat{\phi}, \quad \text{where} \quad \hat{\theta} = \frac{\hat{r}}{p},\ \hat{\phi} = \frac{\hat{T}}{p},\ \hat{r} = v^3 \,(\mathrm{mod}\, p),\ \hat{T} = \lceil p^\alpha \rceil, \tag{17}$$

where $Z \in \mathbb{N} \cup \{0\}$ (to be determined). Note that $\gcd(r,\, p) = \gcd(\hat{r},\, p) = 1$. In (16) and (17), we have replaced N with Z to remind us that we are working in the case of CSC (2). Note that if we require a value of Z satisfying both (16) and (17) to also satisfy CSC (2), then the following two conditions must also be satisfied

$$1 \leq Z < \lceil p^\alpha \rceil, \tag{18}$$

and

$$x^3 \neq y^2 z, \quad \text{where} \quad x \equiv v^2 Z \,(\mathrm{mod}\, p),\ y \equiv v^3 Z \,(\mathrm{mod}\, p),\ z = Z. \tag{19}$$

Let θ, T, $\hat{\theta}$ and $\hat{T}$ be as in (16) and (17). Let

$$T = \lceil p^\alpha \rceil = T_0(s,\, b) + c \tag{20}$$

and

$$\hat{T} = \lceil p^\alpha \rceil = \hat{T}_0(\hat{s},\, \hat{b}) + \hat{c} \tag{21}$$

be the representation of T and $\hat{T}$, determined by (12), corresponding to (16) and (17), respectively. Denote the largest gap-length corresponding to (16) and (17) by g_{max} and $\hat{g}_{max}$, respectively. From Theorem 9, the exact values of g_{max} and $\hat{g}_{max}$ are, respectively, $q_s - b\, q_{s-1}$ and $\hat{q}_{\hat{s}} - \hat{b}\, \hat{q}_{\hat{s}-1}$. We now have the following lemma.

Lemma 12. $g_{max},\ \hat{g}_{max} \geq \lceil p^\alpha \rceil - 1$.

Proof. First, we prove the lemma for g_{max} . Since $T = \lceil p^\alpha \rceil$ and (16) has exactly T gaps for $0 \leq Z \leq p$, we need $\lceil p^\alpha \rceil\, g_{max} \geq p$. Therefore, $g_{max} \geq \frac{p}{\lceil p^\alpha \rceil} \geq \frac{p}{\left\lceil p^{\frac{1}{2}} \right\rceil}$. Using the fact that g_{max} is an integer, we get $g_{max} \geq \left\lfloor p^{\frac{1}{2}} \right\rfloor \geq \lceil p^\alpha \rceil - 1$. Similarly the result follows for $\hat{g}_{max}$. $\square$

Using Theorem 9 (applied to (16)), Lemma 12, and Corollary 8 (applied to (14) for $(\theta,\, T_0)$), we see that when s (in (20)) is even, the first gap corresponding to (16) is the gap of length $q_s - b\, q_{s-1}$ ($= g_{max}$) or $q_s - (b+1)\, q_{s-1}$ ($= g_{max} - q_{s-1}$). (It cannot be q_{s-1}, by Corollary 8 (applied to (14) for $(\theta,\, T''_0(s,\, b+1))$)). Hence there can be at most two values of $Z < \lceil p^\alpha \rceil$ which satisfy (16). Note that there can be exactly two values of $Z < \lceil p^\alpha \rceil$ only when $g_{max} = \lceil p^\alpha \rceil - 1$ and the first (larger) gap of (14) for $(\theta,\, T_0)$ has split. Similarly when $\hat{s}$ (in (21)) is even, there can be at most two values of $Z < \lceil p^\alpha \rceil$ which satisfy (17). Hence when s (or $\hat{s}$) is even, we just need to check if $g_{max} - q_{s-1}$ and g_{max} (or, $\hat{g}_{max} - \hat{q}_{\hat{s}-1}$ and $\hat{g}_{max}$) satisfy (16)-(19). In these (three) cases, we can compute the smallest Z satisfying (16)-(19) in polynomial time.

Let both s and $\hat{s}$ be odd. Using Theorem 9 (applied to (16)), Lemma 12, and Corollary 8 (applied to (14) for $(\theta,\, T_0)$), we see that the first $\lceil B_s \rceil$ gaps corresponding to (16) are of

length q_{s-1}, and then followed by a gap of length g_{max}, or a gap of length q_{s-1} followed by a gap of length $g_{max} - q_{s-1}$. In the case of (17), the first $\left\lceil \hat{B}_{\hat{s}} \right\rceil$ gaps are of length $\hat{q}_{\hat{s}-1}$, and then followed by a gap of length $\hat{g}_{max}$, or a gap of length $\hat{q}_{\hat{s}-1}$ followed by a gap of length $\hat{g}_{max} - \hat{q}_{\hat{s}-1}$.

Let

$$M = \min(\lceil B_s \rceil \; q_{s-1}, \; \left\lceil \hat{B}_{\hat{s}} \right\rceil \; \hat{q}_{\hat{s}-1}) \qquad \text{and} \qquad F = \operatorname{lcm}(q_{s-1}, \, \hat{q}_{\hat{s}-1}). \tag{22}$$

In the range $[0, M]$ there is only one type of gap-length in (16) as well as (17). Now there are two possibilities for M. If $M \geq \lceil p^\alpha \rceil - 1$, then there are exactly $\left\lfloor \frac{\lceil p^\alpha \rceil - 1}{F} \right\rfloor$ values of $Z < \lceil p^\alpha \rceil$ satisfying both (16) and (17). The corresponding values of Z are $j\,F \; \left(1 \leq j \leq \left\lfloor \frac{\lceil p^\alpha \rceil - 1}{F} \right\rfloor\right)$. Note that when $F > \lceil p^\alpha \rceil - 1$, there are no solutions. The other possibility is that $M < \lceil p^\alpha \rceil - 1$. The values of Z up to $M \, (1 \leq M < \lceil p^\alpha \rceil - 1)$ satisfying both (16) and (17) are $j\,F \; \left(1 \leq j \leq \left\lfloor \frac{M}{F} \right\rfloor\right)$. Again, if $M < F$, then there are no solutions up to M. Let $h = q_{s-1}$ or $h = \hat{q}_{\hat{s}-1}$ according as $M = \lceil B_s \rceil \; q_{s-1}$ or not. Since $g_{max}, \, \hat{g}_{max} \geq \lceil p^\alpha \rceil - 1$ (Lemma 12) and $M, \, F \geq 1$, we have $M + g_{max}, \, M + \hat{g}_{max} \geq \lceil p^\alpha \rceil$. Therefore the only possibility of another solution is $Z = M + h$. Hence, even in the case of both s and $\hat{s}$ being odd, we can find a $Z < \lceil p^\alpha \rceil$, if one exists, satisfying both (16) and (17). Since we even require that the Z must satisfy (19), then we need to check all the solutions up to $\lceil p^\alpha \rceil - 1$. When there are exponentially many solutions, as in the case of $v = 1$, then we might end up checking all the solutions but none satisfying (19). This problem can be overcome with the help of the following theorem, which shows that it suffices to check the satisfiability of (19) for $Z = F$.

Theorem 13. *Let s (in (20)) and $\hat{s}$ (in (21)) be both odd, and M, F be as in (22). Consider the common solutions $Z_j = j\,F \; \left(1 \leq j \leq \left\lfloor \frac{min(M, \lceil p^\alpha \rceil - 1)}{F} \right\rfloor\right)$ satisfying (16), (17) and (18). Either all the Z_j satisfy (19) or none of them satisfies (19).*

Proof. Let $\left\lfloor \frac{\min(M, \lceil p^\alpha \rceil - 1)}{F} \right\rfloor \geq 1$, so that there exists at least one common solution. Let $x_j \equiv v^2 Z_j \pmod p$, $y_j \equiv v^3 Z_j \pmod p$ and $z_j = Z_j$. Therefore $x_j \equiv j\,x_1 \pmod p$, $y_j \equiv j\,y_1 \pmod p$ and $z_j = j\,z_1$. Since $j, \, x_1, \, y_1, \, z_1 \leq \lceil p^\alpha \rceil - 1 < p^{\frac{1}{2}}$, we get $x_j = j\,x_1$, $y_j = j\,y_1$ and $z_j = j\,z_1$. Hence $x_j^3 \neq y_j^2 z_j$ if and only if $x_1^3 \neq y_1^2 z_1$. $\square$

Using the above ideas, we obtain Algorithm 5. It determines, for a given v, the least Z (say z) satisfying (16) to (19), i.e. determines the least z such that $(v, \, z)$ satisfies CSC (2), if any exists.

The following proposition follows easily from Proposition 11.

Proposition 14. *The running time of* Algorithm 5 *is $O\big(\ln^3 p\big)$ bit-operations.*

We have implemented Algorithm 5 in PARI/GP on an Intel Pentium-4 single core processor running Ubuntu Linux 9.10. On experimenting (for the $\alpha = \frac{1}{2}$ case of CSC (2)) with 10 randomly chosen 1024-bit primes p and 100 randomly chosen v for each value of p, we got the average running time of Algorithm 5 to be 0.02 seconds.

Using Algorithm 5, we can reduce the worst-case running time of Algorithm 2 to $\widetilde{O}\big(p^1\big)$ from $\widetilde{O}\big(p^{1+\alpha}\big)$, and the expected running time of Algorithm 2 reduces to $\widetilde{O}\big(p^{2-3\alpha}\big)$ from

Algorithm 5 Given v $(1 \leq v < p)$ $(p \geq 3)$, to determine the least positive z, if any, such that $(v,\, z)$ satisfies CSC (2).

(1) Determine the representations $T = \lceil p^{\alpha} \rceil = T_0(s,\, b) + c$ and $\hat{T} = \lceil p^{\alpha} \rceil = \hat{T}_0(\hat{s},\, \hat{b}) + \hat{c}$ by applying Lemma 5 for (16) and for (17), respectively.

(2) If s (or $\hat{s}$) is even, and if $z \leftarrow q_s - (b+1)\, q_{s-1}$ or else $z \leftarrow q_s - b\, q_{s-1}$ (or $\hat{q}_{\hat{s}} - (\hat{b}+1)\, \hat{q}_{\hat{s}-1}$ or else $\hat{q}_{\hat{s}} - \hat{b}\, \hat{q}_{\hat{s}-1}$) satisfies CSC (2) for the given v, then Return z.

(3) Else (s, $\hat{s}$ - both odd)

  (a) If $\lceil B_s \rceil\, q_{s-1} \leq \left\lceil \hat{B}_{\hat{s}} \right\rceil\, \hat{q}_{\hat{s}-1}$, then $M \leftarrow \lceil B_s \rceil\, q_{s-1}$ and $h \leftarrow q_{s-1}$, else $M \leftarrow \left\lceil \hat{B}_{\hat{s}} \right\rceil\, \hat{q}_{\hat{s}-1}$ and $h \leftarrow \hat{q}_{\hat{s}-1}$.

  (b) $F \leftarrow \mathrm{lcm}(q_{s-1},\, \hat{q}_{\hat{s}-1})$

  (c) If $z \leftarrow F$ satisfies CSC (2) for the given v, then Return z.

  (d) If $M < \lceil p^{\alpha} \rceil - 1$ and if $z \leftarrow M + h$ satisfies CSC (2) for the given v, then Return z.

$\widetilde{O}\big(p^{2-2\alpha}\big)$. Note that, for the $\alpha = \frac{1}{2}$ case, the improved worst-case running time of Algorithm 2 equals that of the current best deterministic algorithm (Algorithm 1), and similarly the improved expected running time of Algorithm 2 matches the current best expected running time (Algorithm 1).

In order to make Algorithm 2 even more efficient, we need to be able to predict a small range of values of v in which we are guaranteed a solution. This problem appears to be hard and currently we are even unable to determine whether corresponding to $v = i+1$ a solution to CSC (2) exists, given that $v = i$ has no solutions. Nevertheless, it is important to pursue research in this direction since we are now required to analyze the distribution of solutions of CSC (2) with respect to only one parameter v, unlike two parameters x and y in the case of CSC (1).

The converse problem of determining various primes which have a solution to CSC (2) for a given value of v (say i) is useful to identify classes of primes for which we can find a solution efficiently. This problem is addressed in the next section.

6. Existence of Solutions to CSC

It is shown in Maitra et al. (2009) that for the primes p satisfying $(i-1)^2 i^2 - i + 1 < p < (i-1)^2 i^2$, there exists a solution to CSC (2) $(\alpha = \frac{1}{2})$ and a corresponding $(v,\, z)$ pair is $\big(v = i,\, z = (i-1)^2\big)$. Using the prime number theorem, we see that the (expected) number of primes less than n satisfying the above inequality is $\Theta\left(\frac{n^{\frac{1}{2}}}{\ln n}\right)$. Hence primes close to the fourth powers have a solution for $v \approx p^{\frac{1}{4}}$ $\left(v > p^{\frac{1}{4}}\right)$ and using Algorithm 3 $(\alpha = \frac{1}{2})$ the solution can be efficiently computed. It is easy to see that the above result is based on the following lemma.

Lemma 15. *If* $0 < a^2 b - p < \frac{p^{\frac{1}{2}}}{a}$ *and* $1 \leq a,\, b < p^{\frac{1}{2}}$, *then* $(v = a,\, z = b)$ *satisfies* CSC (2) $(\alpha = \frac{1}{2})$.

Note that the number of primes for which the triple ($x = \lceil p^{\frac{1}{3}} \rceil$, $y = 1$, $z = x^3 - p$) satisfies CSC (1) ($\alpha = \frac{1}{2}$) is $\Theta\left(\frac{n^{\frac{5}{6}}}{\ln n}\right)$.

Let us try to generalize the above result that primes "close" to (but less than) the fourth powers have a solution for $v \approx p^{\frac{1}{4}}$, to determine those primes which have a solution to CSC (2) ($\alpha = \frac{1}{2}$) for a given $v = i$, and that $v \approx p^{\frac{1}{\epsilon}}$ ($\epsilon \in \mathbb{R}$, $3 \leq \epsilon \leq 4$). Throughout this section we will restrict ourselves only to the case $\alpha = \frac{1}{2}$ of CSC (2).

Let $i \in \mathbb{N}$, $i \geq 6$, $\epsilon \in \mathbb{R}$ and $3 \leq \epsilon \leq 4$. Let $v = i$ in CSC (2). Define $z = \left\lfloor i^{\epsilon-2} \right\rfloor$, hence $v^2 z \leq i^\epsilon$. If we choose p such that $(i-1)^\epsilon < p < v^2 z \leq i^\epsilon$ and $v^2 z - p < \frac{p^{\frac{1}{2}}}{v}$, then by Lemma 15 we have (v, z) satisfying CSC (2) for such a p, and also $v \approx p^{\frac{1}{\epsilon}}$. The restriction $(i-1)^\epsilon < p \leq i^\epsilon$ ensures that the primes are in disjoint intervals as i varies for a fixed ϵ. Since $v^2 z = i^2 \left\lfloor i^{\epsilon-2} \right\rfloor = i^\epsilon - \left\{ i^{\epsilon-2} \right\} i^2 \leq i^\epsilon$ and $0 \leq \left\{ i^{\epsilon-2} \right\} i^2 < i^2$, we require $\epsilon \geq 3$, and the restriction $\epsilon \leq 4$ follows from Algorithm 3 ($\alpha = \frac{1}{2}$). Note that when $i \geq 6$, we have $i^\epsilon < 2\ (i-1)^\epsilon$ and hence $v^2 z \pmod p = v^2 z - p$. We need to find those primes p which satisfy the conditions

$$(i-1)^\epsilon < p < i^2 \left\lfloor i^{\epsilon-2} \right\rfloor \tag{23}$$

and

$$i^2 \left\lfloor i^{\epsilon-2} \right\rfloor - p < \frac{p^{\frac{1}{2}}}{i}. \tag{24}$$

The inequality in (24) is quadratic and it can be solved for p (this is the reason for requiring $\alpha = \frac{1}{2}$). On solving (24) for p, and then requiring that it also satisfies (23), we get the solution set

$$P_{\epsilon,\, i} = \left\{ \text{primes}\, p \;\middle|\; i^2 \left\lfloor i^{\epsilon-2} \right\rfloor - \left(\frac{\sqrt{4\, i^4 \left\lfloor i^{\epsilon-2} \right\rfloor} - 1}{2\, i^2} \right) < p < i^2 \left\lfloor i^{\epsilon-2} \right\rfloor \right\}.$$

Proposition 16. *The primes $p \in P_{\epsilon,\, i}$ have $(v = i,\, z = \left\lfloor i^{\epsilon-2} \right\rfloor)$ satisfying* CSC (2) *($\alpha = \frac{1}{2}$), and $v \approx p^{\frac{1}{\epsilon}}$.*

Since $\left(\frac{\sqrt{4\, i^4 \left\lfloor i^{\epsilon-2} \right\rfloor} - 1}{2\, i^2} \right) \approx i^{\frac{\epsilon}{2} - 1}$, the number of primes less than n (for a fixed ϵ) covered by $P_{\epsilon,\, i}$ is $\Theta\left(\frac{n^{\frac{1}{2}}}{\ln n}\right)$. Note that $v \approx p^{\frac{1}{\epsilon}}$, but not really $p \approx v^\epsilon$, as p belongs to an interval (of length $\approx v^{\frac{\epsilon}{2} - 1}$) whose right end is the multiple of v^2 nearest to (and less than or equal to) v^ϵ. We still say that p is "close" to v^ϵ since $\frac{v^\epsilon - p}{v^\epsilon - (v-1)^\epsilon} \to 0$ as $v \to \infty$.

For a given i, the set $\bigcup\limits_{3 \leq \epsilon \leq 4} P_{\epsilon,\, i}$ can be better pictured by considering the interval $\left[i^3,\, i^4 \right]$, dividing it into sub-intervals of length i^2, i.e. intervals of the form $(\, i^3 + (j-1)\, i^2,\, i^3 + j\, i^2\,)$ for $1 \leq j \leq i^2 - i$, and then considering in each sub-interval all the primes in the right most sub-sub-interval of length $\left\lceil \sqrt{i + j} \right\rceil - 1$. It is easy to see that the cardinality of $\bigcup\limits_{3 \leq \epsilon \leq 4} P_{\epsilon,\, i}$ is $\Theta\left(\frac{i^3}{\ln i}\right)$. This approach gives us a fairly accurate algorithm to compute the cardinality of $\bigcup\limits_{\epsilon,\, i} P_{\epsilon,\, i}$.

When $l \geq 3$, we have $l^3 < (l+1)^3 < l^4$ and hence any real number $k \geq 27$ can be written in the form l^ϵ (for some $3 \leq \epsilon \leq 4$ and $l \in \mathbb{N}$) and the number of such representations of

Table 1. Specific values of $count(n)$.

n	$count(n)$	$\pi(n)$	$\frac{count(n)}{\pi(n)}$
2×10^8	3643598	11078937	0.328876
4×10^8	7017151	21336326	0.328882
6×10^8	10300963	31324703	0.328845
8×10^8	13530391	41146179	0.328837
10×10^8	16716041	50847534	0.328748

k is $\Theta\left(k^{\frac{1}{3}} - k^{\frac{1}{4}}\right) = \Theta\left(k^{\frac{1}{3}}\right)$. These ideas suggest that $\bigcup_{\epsilon,\, i} P_{\epsilon,\, i}$ can possibly cover a large proportion of primes. Because the sets $P_{\epsilon,i}$ have too much overlap, calculating the exact proportion of these primes seems to be challenging. Let $count(n)$ denote the number of primes less than or equal to n which are also in $\bigcup_{\epsilon,\, i} P_{\epsilon,\, i}$. It is empirically observed up to one billion that about one in three primes belongs to $\bigcup_{\epsilon,\, i} P_{\epsilon,\, i}$. Table 1 gives the value of $count(n)$ for some values of n. The values of $count(n)$ listed in Table 1 deviate only marginally from the actual values because of the floating-point approximations in their computations. The function $\pi(n)$ denotes the total number of primes less than or equal to n.

From Proposition 16, we conclude that for primes $p \in P_{\epsilon,\, i}$ there is a solution to CSC (2) ($\alpha = \frac{1}{2}$) corresponding to v, where $p^{\frac{1}{4}} < v < p^{\frac{1}{3}} + 1$, and using Algorithm 2 along with Algorithm 5, we can determine a solution in $\widetilde{O}\left(p^{\frac{1}{3}}\right)$ time. It can be easily shown that for these primes the Algorithm 3 takes $\widetilde{O}\left(p^{\frac{1}{2}}\right)$ time in the worst case, the previous best running time.

Using an approach similar to the one in this section, we may be able to identify more classes of primes for which a solution to CSC (2) can be computed more efficiently.

7. Conclusion

We have shown that we can determine in deterministic polynomial time whether a solution to CSC (2) exists for a given v ($1 \leq v < p$), and we can also compute it efficiently, if one exists. An important research direction is to analyze the distribution of solutions with respect to the parameter v and use the analysis to guess a value of v close to the one which has a solution. We have also shown that the primes "close" to i^{ϵ} (integer i, real $\epsilon \in [3,\, 4]$) have a solution to CSC (2) ($\alpha = \frac{1}{2}$). Determining a precise estimate of the proportion of primes covered by this characterization needs to be addressed. Extending this analysis of the distribution of solutions to a general α ($\frac{1}{3} < \alpha \leq \frac{1}{2}$) also needs to be done. Determining whether a solution to CSC (2) exists for a given z ($1 \leq z < p^{\alpha}$) leads to interesting questions on fractional part sequences such as efficiently finding a common N simultaneously satisfying both $\left\{\theta N^2\right\} < \phi$ and $\left\{\theta N^3\right\} < \phi$.

Acknowledgements

We would like to thank Mr. Puttabasavaiah for helping us obtain the papers Slater (1950, 1967). Many thanks to Prof. John H. Halton for mailing his paper Halton (1965), and also to Srikanth Pai for useful initial discussions.

References

Coppersmith, D., Odlzyko, A. M., Schroeppel, R., 1986. Discrete logarithms in $GF(p)$. Algorithmica 1 (1), 1–15.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., Stein, C., 2001. Introduction to algorithms. The MIT press.

Das, A., 1999. Galois Field computations: Implementation of a library and a study of the discrete logarithm problem. Ph.D. thesis, Indian Institute of Science, Bangalore.

Das, A., Veni Madhavan, C. E., 2005. On the cubic sieve method for computing discrete logarithms over prime fields. International Journal of Computer Mathematics 82 (12), 1481–1495.

Drobot, V., 1987. Gaps in the sequence $n^2\vartheta$ (mod 1). International Journal of Mathematics and Mathematical Sciences 10 (1), 131–134.

Fraenkel, A. S., Holzman, R., 1995. Gap problems for integer part and fractional part sequences. Journal of Number Theory 50 (1), 66–86.

Graham, R. L., Knuth, D. E., Patashnik, O., 1994. Concrete Mathematics: a foundation for computer science. Addison-Wesley Reading, MA.

Halton, J. H., 1965. The distribution of the sequence $\{n\xi\}$ $(n = 0, 1, 2, \ldots)$. In: Proceedings of the Cambridge Philosophical Society. Vol. 61. pp. 665–670.

Hensley, D., 2006. Continued Fractions. World Scientific Pub Co Inc.

Lenstra, A. K., Lenstra Jr., H. W., 1990. Handbook of Theoretical Computer Science. MIT Press/Elsevier, Amsterdam, Ch. Algorithms in Number Theory, pp. 675–715.

Lenstra Jr., H. W., 2008. Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography. Cambridge Univ Press, Ch. Lattices, pp. 127–181.

Maitra, S., Rao, Y. V. S., Stanica, P., Gangopadhyay, S., 2009. Nontrivial solutions to the cubic sieve congruence problem: $x^3 \equiv y^2 z \bmod p$. Computación y Sistemas 12 (3), 253–266.

Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A., 1997. Handbook of Applied Cryptography. CRC.

Micciancio, D., Goldwasser, S., 2002. Complexity of lattice problems: a cryptographic perspective. Vol. 671. Springer Netherlands.

Schirokauer, O., Weber, D., Denny, T., 1996. Discrete logarithms: the effectiveness of the index calculus method. In: Proceedings of the Algorithmic Number Theory Symposium II. Springer, pp. 337–361.

Slater, N. B., 1950. The distribution of the integers N for which $\{\theta N\} < \phi$. In: Proceedings of the Cambridge Philosophical Society. Vol. 46. pp. 525–534.

Slater, N. B., 1964. Distribution problems and physical applications. Compositio Math 16, 176–183.

Slater, N. B., 1967. Gaps and steps for the sequence $n\theta$ mod 1. In: Proceedings of the Cambridge Philosophical Society. Vol. 63. pp. 1115–1123.