TCS-TR-A-19-83

TCS Technical Report

Taking Discrete Roots in the Field $\mathbb{Z}_p$ and in the Ring $\mathbb{Z}_{p^e}$

by

Thomas Zeugmann

Division of Computer Science

Report Series A

June 15, 2019

Hokkaido University
Graduate School of
Information Science and Technology

Email: thomas@ist.hokudai.ac.jp

Phone: +81-011-706-7684
Fax: +81-011-706-7684

Taking Discrete Roots in the Field $\mathbb{Z}_p$ and in the Ring $\mathbb{Z}_{p^e}$

Thomas Zeugmann
Division of Computer Science
Hokkaido University
N-14, W-9, Sapporo 060-0814
Japan
thomas@ist.hokudai.ac.jp

Abstract

The present paper studies the problem of taking discrete roots in the field $\mathbb{Z}_p$ and in the ring $\mathbb{Z}_{p^e}$, where p is a prime number and e is a positive natural number. After surveying the state of the art, the paper presents several generalizations of Tonelli–Shanks and Adleman–Manders–Miller like approaches. In particular, it shown that there is a generalization of the generalized Adleman–Manders–Miller algorithm which allows one to compute directly discrete qth roots with respect to the modulus p^e.

The second part is devoted to lifting algorithms. Here the main emphasis is completeness; i.e., we present lifting algorithms for all possible cases depending on the prime p, the root q and the greatest common divisor of p and q. As a byproduct, we also present a proof of one of Tonelli's (1891) lifting algorithms.

1. Introduction

The problem of solving discrete quadratic equations has been studied for at least a millennium. We refer the reader to Dickson [6, Binomial Congruences, pp. 204 ff] for a comprehensive exposition. Some of the algorithms obtained found renewed interest after public key cryptography emerged. Examples comprise e.g. Tonelli [24] and Cipolla [5].

In the present paper we are mainly interested in taking discrete roots in the the field $\mathbb{Z}_p$ and in the $\mathbb{Z}_{p^e}$, where p is a prime number and e is a positive natural number. So our equations have the form $x^q \equiv a \mod p$, where p is a prime and q is a positive natural number or, more generally, of the form $x^q \equiv a \mod p^e$ for positive natural numbers e.

We start with a very general theorem characterizing the existence of such discrete roots for under the assumption that the corresponding multiplicative group $\mathbb{Z}_n^*$ is

cyclic (cf. Theorem 11). Though the proof of this theorem is constructive, it does not yield efficient algorithms in general. Here by efficient we mean that the corresponding algorithms achieve a running time that is polynomial in the length of the input.

Therefore, we then turn our attention to efficient algorithms with a focus of Tonelli's [24, 25] algorithms and the generalization obtained by Adleman, Manders, and Miller [1]. As far as this part is concerned our main result is a generalization of their algorithm, which allows for a direct computation of general qth roots in the ring $\mathbb{Z}_{p^e}$.

In the second part of the present paper we provide a detailed exposition of algorithms that allow to lift a qth root obtained with respect to the modulus p to moduli p^e. This comprises a proof and an improvement of a lifting proposed without proof by Tonelli [24], and the group of algorithms commonly known as Hensel [11] lifting. In this way, the complexity of the algorithms obtained becomes easily comparable. Whenever appropriate, also examples are included.

2. Preliminaries

Let $\mathbb{N} = \{0, 1, 2, , \ldots\}$ denote the set of all *natural numbers*. We set $\mathbb{N}^+ =_{df} \mathbb{N} \setminus \{0\}$. By $\mathbb{Z}$ we denote the set of all *integers*. Furthermore, we use $\mathbb{Q}$ and $\mathbb{R}$ for the set of all *rational numbers* and *real numbers*, respectively.

For all real numbers y we define $\lfloor y \rfloor$, the *floor function*, to be the greatest integer less than or equal to y. Similarly, $\lceil y \rceil$ denotes the smallest integer greater than or equal to y, i.e., the *ceiling function*. Furthermore, for all numbers $y \in \mathbb{R}$ we write $|y|$ to denote the *absolute value* of y.

Throughout this report we write $\log n$ to denote the *logarithm to the base* 2, $\ln n$ to denote the *logarithm to the base* e (where e is the Euler number), and $\log_c n$ to denote the *logarithm to the base* c.

Let $a, b \in \mathbb{Z}$ be given. We say that a *divides* b (or b is *divisible* by a) if there exists a $d \in \mathbb{Z}$ such that $b = ad$. If a divides b we write $a|b$, and a is called a *divisor* of b. Hence, divisibility is a binary relation. Furthermore, we call greatest number $d \in \mathbb{N}$ dividing both a and b the *greatest common divisor* of a and b and write $d = \gcd(a, b)$. It is convenient to set $\gcd(0, 0) = 0$. Also, $\gcd(a, 0) = a$ and $\gcd(a, a) = a$ for all $a \in \mathbb{N}$.

The gcd of two numbers a and b can be efficiently computed by using the *extended Euclidean algorithm* (abbr. ECLA). Note that the ECLA also computes $x, y \in \mathbb{Z}$ such that $d = ax+by$, where $d = \gcd(a, b)$. This is also known as Lamé's [16] theorem. We refer the reader to Shallit [21] for a detailed discussion of the origins of the analysis of the Euclidean algorithm by French mathematicians and to Schreiber [20] for a German source from the 16th century noticing the worst-case of the Euclidean algorithm. For further information concerning algorithms computing the gcd we refer the reader to Knuth [13].

Let $m \in \mathbb{N}^+$, and let $a, b \in \mathbb{Z}$; we write $a \equiv b \bmod m$ if m divides $a - b$ (abbr. $m|(a-b)$). Thus, $a \equiv b \bmod m$ if and only if a and b have the *same* remainder when divided by m. If $a \equiv b \bmod m$ then we say that a is *congruent* b modulo m, and we refer to "$\equiv$" as the *congruence relation*. The symbol "$\equiv$" was introduced by Gauss [9], who studied congruences thoroughly. We also write $a \bmod m$ to denote the remainder r obtained when a is divided by m. For $m = 1$ we obtain the *zero ring* consisting of the set $\{0\}$ and the only possible addition and multiplication $0 + 0 = 0$ and $0 \cdot 0 = 0$, respectively.

It is easy to see that the congruence relation is an equivalence relation, i.e., it is *reflexive, symmetric* and *transitive*. Therefore, we may consider the equivalence classes $[a] =_{df} \{x \mid x \in \mathbb{Z},\ a \equiv x \mod m\}$, where $a \in \mathbb{Z}$. Consequently, we directly obtain that $[a] = [b]$ iff $a \equiv b \mod m$. Hence, there are precisely the m equivalence classes $[0], [1], \ldots, [m-1]$. We set $\mathbb{Z}_m =_{df} \{[0], [1], \ldots, [m-1]\}$.

We define addition and multiplication of these equivalence classes by

$$\begin{aligned} [a] + [b] &=_{df} [a + b] \quad \text{and} \\ [a] \cdot [b] &=_{df} [a \cdot b]\ . \end{aligned}$$

In order to simplify notation, we usually omit the brackets, i.e., instead of $[a]$ we shortly write just a.

Furthermore, the following theorem establishes some useful rules for performing calculations with congruences:

Theorem 1. *Let $m \in \mathbb{N}^+$, let $a, b, c, d \in \mathbb{Z}$ be such that $a \equiv b \mod m$ and $c \equiv d \mod m$, and let $n \in \mathbb{N}$. Then we have the following:*

(1) $a + c \equiv b + d \mod m$;

(2) $a - c \equiv b - d \mod m$;

(3) $ac \equiv bd \mod m$;

(4) $a^n \equiv b^n \mod m$.

The following theorem completely characterizes the existence of modular inverses:

Theorem 2. *Let $m \in \mathbb{N}^+$, and let $a \in \mathbb{Z}$. The congruence $ax \equiv 1 \bmod m$ is solvable if and only if $\gcd(a, m) = 1$. Moreover, if $ax \equiv 1 \mod m$ is solvable, then the solution is uniquely determined.*

Hence we conclude that $(\mathbb{Z}_m, +, \cdot)$ is a field iff m is a prime number.

Furthermore, it is not difficult to show the following:

Theorem 3. *Let $a, c \in \mathbb{Z}$ and let $b \in \mathbb{N}$, $b \geqslant 2$. Then the* linear congruence $ax \equiv c \bmod b$ *is solvable if and only if $\gcd(a, b)$ divides c. Moreover, if $d = \gcd(a, b)$ and $d|c$ then there are precisely d solutions in $\mathbb{Z}_b$ for $ax \equiv c \bmod b$.*

Taking Theorem 2 into account it is appropriate to consider the multiplicative group $\mathbb{Z}_m^*$, where $m \in \mathbb{N}^+$ and $\mathbb{Z}_m^* =_{df} \{a \mid a \in \{1, \ldots, m-1\},\ \gcd(m, a) = 1\}$.

Let $m \in \mathbb{N}^+$; by $\varphi(m) =_{df} |\mathbb{Z}_m^*|$ we denote *Euler's [7] totient function* (also called *Euler's phi-function*), where one assumes by definition that $\varphi(1) = 1$. Furthermore, a function $f\colon \mathbb{N} \to \mathbb{N}$ is said to be *multiplicative* if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$ whenever $\gcd(m, n) = 1$.

The following theorem summarizes some basic properties of Euler's totient function:

Theorem 4 (Euler [7]). *For all $m, n \in \mathbb{N}^+$ we have*

(1) $\varphi(mn) = \varphi(m)\varphi(n)$ *if* $\gcd(m, n) = 1$;

(2) $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ *if p is prime and $\alpha \geqslant 1$;*

(3) $\varphi(p) = p - 1$ *if and only if p is prime.*

We refer the reader to Koblitz [14] for a proof.

We shall need frequently the following theorems:

Theorem 5 (Euler's [7] Theorem). *Let $n \in \mathbb{N}$, $n \geqslant 2$; then $a^{\varphi(n)} \equiv 1 \bmod n$ for all $a \in \mathbb{Z}_n^*$.*

Theorem 5 covers the following important special case which was first discovered by Pierre de Fermat [23, pp. 206–212].

Theorem 6 (Fermat's Little Theorem). *Let $p \in \mathbb{N}$ be any prime number. Then we have $a^{p-1} \equiv 1 \mod p$ for all $a \in \mathbb{Z}_p^*$.*

Recall that a group G is cyclic if it contains an element g generating all the elements of the group; i.e., $G = \{a^n \mid n = 1, \ldots, |G|\}$. We refer to such elements g as a *generator* or a *primitive root*.

In order to achieve the desired level of generality we recall the following theorem, which completely characterizes the cyclic groups $\mathbb{Z}_n^*$:

Theorem 7 (Primitive Root Theorem (cf. Gauss [9, Article 92])). *The group $\mathbb{Z}_n^*$ is cyclic if and only if n is 1, 2, 4, p^e, or $2p^e$ for some odd prime number p and $e \in \mathbb{N}^+$.*

Furthermore, as far as the necessary background concerning group theory, rings and fields is concerned, we refer the reader to Bach and Shallit [2, Chapter 2] and the references therein. In particular, we shall need the following theorem:

Theorem 8. *Let $\mathbb{F}$ be any Abelian field, and let $p \in \mathbb{F}[x]$ be a polynomial such that $p \neq 0$. Then the polynomial p possesses at most d zeros, where $d = \deg p$.*

Next, we shall presents general results concerning the existence, multiplicity, and computation of discrete roots in fields $\mathbb{Z}_p$, where p is any prime or in rings $\mathbb{Z}_n$, where n is such that $\mathbb{Z}_n^*$ is cyclic. Then we turn our attention to the problem of how to lift solutions obtained in $\mathbb{Z}_p$ to solutions in the ring $\mathbb{Z}_{p^e}$, where $e \in \mathbb{N}^+$.

3. Computing Roots in the Ring $\mathbb{Z}_n$

In this section we almost always assume that $n \in \mathbb{N}^+$ is such that $\mathbb{Z}_n^*$ is cyclic. Next, let $a \in \mathbb{Z}_n^*$ and let $n \in \mathbb{N}^+$. Our main goal is to study the solvability of the congruence $x^q \equiv a \bmod n$. However, it is already known for the case that $q = 2$ that the congruence $x^2 \equiv a \bmod p$ may or may not have a solution (cf., e.g., Koblitz [14, Chapter 2]). So it is appropriate to have the following definition:

Definition 1 (qth Residue, qth Nonresidue)**.** Let Let $m \in \mathbb{N}$, $m \geqslant 2$ be any number, let $a \in \mathbb{Z}_m^*$, and let $q \in \mathbb{N}^+$. Then the element a is said to be a *qth residue* modulo m if $x^q \equiv a \mod m$ is solvable in $\mathbb{Z}_m^*$. If a is not a qth residue modulo m, then we call a a *qth nonresidue* modulo m.

Remark. If $q = 2$ then we refer to a qth residue and a qth nonresidue as a *quadratic residue* and a *quadratic nonresidue*, respectively.

3.1. *A Particular Easy Case*

We start to look at the problem of taking discrete roots for a particular easy case. Let $p \in \mathbb{N}$ be any prime, let $q \geqslant 1$, and let $a \in \mathbb{Z}_p$ be arbitrarily fixed. We aim to solve $x^q \equiv a \bmod p$. Then we have the following theorem:

Theorem 9. *Let p be any prime and let $q \in \mathbb{N}^+$ be such that $\gcd(q, p-1) = 1$, and let $a \in \mathbb{Z}_p$ be arbitrarily fixed. Then the congruence $x^q \equiv a \bmod p$ has a uniquely determined solution.*

Proof. If $a \equiv 0 \bmod p$ then $x = 0$ is the unique solution and we are done. Next, we assume that $a \not\equiv 0 \bmod p$. Since $\gcd(q, p-1) = 1$, by Theorem 2 we know that the modular inverse d of q in $\mathbb{Z}_{p-1}^*$ exists and it is uniquely determined.

Claim 1. $x =_{df} a^d \bmod p$ *is a solution of* $x^q \equiv a \bmod p$.

Since $qd \equiv 1 \bmod p-1$, there is a $k \in \mathbb{Z}$ such that $dq = 1 + (p-1) \cdot k$. Thus we obtain

$$\begin{aligned} x^q \equiv \left(a^d\right)^q &\equiv a^{dq} \equiv a^{1+(p-1)\cdot k} \\ &\equiv a \cdot a^{(p-1)\cdot k} \equiv a \cdot 1^k \quad \text{(by Theorem 6)} \\ &\equiv a \mod p\,, \end{aligned}$$

and Claim 1 is shown.

Claim 2. *The solution of* $x^q \equiv a \bmod p$ *is uniquely determined.*

Suppose that there are solutions x_1 and x_2 of $x^q \equiv a \bmod p$. As the proof of Claim 1 shows we have $z^{qd} \equiv z \bmod p$ for all $z \in \mathbb{Z}_p^*$. Thus, we obtain

$$\begin{aligned} x_1 &\equiv x_1^{qd} \equiv (x_1^q)^d \equiv a^d \\ &\equiv (x_2^q)^d \equiv x_2^{qd} \equiv x_2 \mod p \ ; \end{aligned}$$

i.e., x_1 and x_2 are the same modulo p, and Claim 2 is shown.

Claim 1 and 2 directly yield the theorem. ∎

Theorem 9 directly allows for the following corollary:

Corollary 1. *Let* p *be any prime and let* $q \in \mathbb{N}^+$ *be such that* $\gcd(q, p-1) = 1$. *Then every element* $a \in \mathbb{Z}_p$ *is a* q*th residue modulo* p.

Remarks. First, we note that the proof of Theorem 9 is constructive; i.e., we also have an efficient method to compute the qth root in case that the assumptions of Theorem 9 are satisfied.

Second, we note that it suffices to consider qth roots for $q \in \{1, \ldots, p-1\}$. This observation is directly implied by the fact that we have computed the modular inverse of $q \in \mathbb{Z}_{p-1}^*$, i.e., it was sufficient to consider q reduced modulo $p-1$. As a matter of fact, this observation generalizes to arbitrary polynomials, since we have the following theorem:

Theorem 10. *Let* p *be a prime, let* $n \in \mathbb{N}$, *and let* $f(x) = \sum_{i=0}^{n} a_i x^i$, *where* $a_i \in \mathbb{Z}_p$ *for all* $i = 0, \ldots, n$. *Then the congruence* $f(x) \equiv 0 \bmod p$ *is equivalent to a congruence* $\hat{f}(x) \equiv 0 \bmod p$, *where* $\deg \hat{f} \leqslant p-1$.

Proof. Let the polynomial f be arbitrarily fixed. If $\deg f \leqslant p-1$ we are already done. Otherwise, we divide f by $x^p - x$ and obtain

$$f(x) = (x^p - x)Q(x) + R(x) \ ,$$

where $\deg R \leqslant p-1$. By Theorem 6 we know that $x^p \equiv x \bmod p$, and therefore we have $x^p - x \equiv 0 \bmod p$. Consequently, we see that $(x^p - x)Q(x) \equiv 0 \bmod p$, and thus $f(x) \equiv R(x) \bmod p$. ∎

3.2. *A General Characterization Theorem*

At this point it is only natural to ask what we can say concerning the solvability of $x^q \equiv a \bmod p$ in case that the condition $\gcd(p-1, q) = 1$ is not satisfied. We shall answer this question in a more general context. As we shall see the theory of qth residues is clearly arranged provided the multiplicative group $\mathbb{Z}_n^*$ is cyclic. Recall that the primitive root theorem completely characterizes the cyclicity of $\mathbb{Z}_n^*$ (cf. Theorem 7). The following theorem goes back to Gauss [9, Article 60–63]:

Theorem 11. *Let $q \in \mathbb{N}^+$, let $n \in \mathbb{N}^+$ be such that $\mathbb{Z}_n^*$ is cyclic. Furthermore, let $b = \gcd(\varphi(n), q)$. Then we have the following:*

(1) *An element $a \in \mathbb{Z}_n^*$ is a qth residue if and only if $a^{\varphi(n)/b} \equiv 1 \bmod n$.*

(2) *There are precisely $\varphi(n)/b$ many qth residues in $\mathbb{Z}_n^*$.*

(3) *If $a \in \mathbb{Z}_n^*$ is a qth residue in $\mathbb{Z}_n^*$ then the congruence $x^q \equiv a \bmod n$ possesses precisely b solutions.*

Proof. Let $n \in \mathbb{N}^+$ be such that $\mathbb{Z}_n^*$ is cyclic, and let $b = \gcd(q, \varphi(n))$. Assume that $x^q \equiv a \bmod n$ is solvable, and let x_0 be a solution, i.e., we have $x_0^q \equiv a \bmod n$. Using Theorem 5 and taking into account that $q/b \in \mathbb{N}$, we conclude that

$$a^{\varphi(n)/b} \equiv (x_0^q)^{\varphi(n)/b} \equiv \left(x_0^{\varphi(n)}\right)^{q/b} \equiv 1 \mod n\,.$$

and the necessity of Assertion (1) is shown.

For the sufficiency of Assertion (1) we assume that $a^{\varphi(n)/b} \equiv 1 \bmod n$. We have to show that $x^q \equiv a \bmod n$ is solvable.

Recall that $a \in \mathbb{Z}_n^*$. By Theorem 7 we know that $\mathbb{Z}_n^*$ possesses a generator g. Let $y \in \{1, \ldots, \varphi(n)\}$ be such that $a \equiv g^y \bmod n$. Using $a^{\varphi(n)/b} \equiv 1 \bmod n$ and the transitivity of the congruence relation, we see that

$$1 \equiv a^{\varphi(n)/b} \equiv (g^y)^{\varphi(n)/b} \equiv \left(g^{\varphi(n)}\right)^{(y/b)} \mod n$$

holds. Since g is a generator of $\mathbb{Z}_n^*$ this implies that $y/b \in \mathbb{N}$ must hold. We conclude that y is a multiple of b, i.e., we obtain that $y = z \cdot b$ for some $z \in \mathbb{N}^+$. Furthermore, since $b = \gcd(q, \varphi(n))$, there are numbers $s, t \in \mathbb{Z}$ such that $b = s \cdot q + t\varphi(n)$. We continue with the following claim:

Claim 1. *$x =_{\mathrm{df}} g^{z \cdot s}$ is a solution of $x^q \equiv a \bmod n$.*

This can be seen as follows:

$$\begin{aligned} x^q &\equiv (g^{z \cdot s})^q \equiv g^{z \cdot s \cdot q} \equiv g^{z \cdot s \cdot q} \cdot 1 \equiv g^{z \cdot s \cdot q} \cdot g^{\varphi(n) t \cdot z} \\ &\equiv g^{z(s \cdot q + \varphi(n) t)} \equiv g^{z \cdot b} \quad (\text{since } b = s \cdot q + t\varphi(n)) \\ &\equiv g^y \qquad (\text{since } z \cdot b = y) \\ &\equiv a \qquad (\text{since } a \equiv g^y \bmod n)\,. \end{aligned}$$

Hence we have shown Claim 1, and thus the sufficiency of Assertion (1).

In order to show Assertion (2) we start with the following claim:

Claim 2. *Let $\zeta =_{\mathrm{df}} g^{\varphi(n)/b}$. Then $\zeta, \ldots, \zeta^b$ are the pairwise different solutions of $x^q \equiv 1 \bmod n$.*

Clearly, $x^q \equiv 1 \bmod n$ is solvable. Recall that $b = \gcd(q, \varphi(n))$. Hence, there is a $d \in \mathbb{N}^+$ such that $q = d \cdot b$. So we have

$$\begin{aligned} \zeta^q &\equiv \left(g^{\varphi(n)/b}\right)^q \equiv g^{\varphi(n)q/b} \equiv g^{\varphi(n)d\cdot b/b} \equiv g^{\varphi(n)d} \\ &\equiv \left(g^{\varphi(n)}\right)^d \equiv 1^d \equiv 1 \mod n\,. \end{aligned}$$

Here we used Theorem 5, i.e., $g^{\varphi(n)} \equiv 1 \bmod n$. Consequently, ζ is a qth root of $x^q \equiv 1 \bmod n$. Taking into account that $\left(\zeta^k\right)^q \equiv (\zeta^q)^k \equiv 1^k \equiv 1 \bmod n$ for all $k = 1, \ldots, b$, we see that $\zeta, \ldots, \zeta^b$ are solutions of $x^q \equiv 1 \bmod n$. Furthermore, since g is a generator of $\mathbb{Z}_n^*$, we conclude that these solutions are pairwise incongruent.

It remains to show that there are no other solutions of $x^q \equiv 1 \bmod n$. Recall that $1 = g^{\varphi(n)}$. Let x be any solution of $x^q \equiv 1 \bmod n$. Then there is a uniquely determined $\ell \in \{1, \ldots, \varphi(n)\}$ such that $x = g^\ell$. Since $x^q \equiv g^{\ell\cdot q} \bmod n$, we conclude that $q \cdot \ell \equiv \varphi(n) \bmod \varphi(n)$ must hold. By Theorem 3 we know that the latter congruence is solvable in ℓ iff $b = \gcd(q, \varphi(n))$ divides $\varphi(n)$. This is clearly the case. Therefore, by Theorem 3 we also know that there are precisely b solutions. Consequently, $x^q \equiv 1 \bmod p$ possesses exactly b pairwise incongruent solutions, and Claim 2 is shown.

Claim 3. *Let x be a solution of $x^q \equiv a \bmod n$. Then all solutions of $x^q \equiv a \bmod n$ are obtained as $x \cdot \zeta$, where ζ is any solution of $x^q \equiv 1 \bmod n$.*

From $x^q \equiv a \bmod n$ and $\zeta^q \equiv 1 \bmod n$ we directly obtain $(x \cdot \zeta)^q \equiv a \bmod n$ (cf. Theorem 1). We note that for incongruent ζ_1 and ζ_2 we obtain incongruent solutions $x \cdot \zeta_1$ and $x \cdot \zeta_2$ modulo n. Hence, by Claim 2 there are at least b pairwise distinct solutions of $x^q \equiv a \bmod b$. On the other hand, there are also at most b pairwise distinct solutions of $x^q \equiv a \bmod p$. This can be seen as above: Suppose we have another solution $\hat{x} \in \mathbb{Z}_n^*$ of $x^q \equiv a \bmod n$. Recall that $a \equiv g^y \bmod n$ and let $\hat{x} = g^\ell \bmod n$. Then the congruence $q \cdot \ell \equiv y \bmod \varphi(n)$ must be satisfied and in case it is, there are exactly $b = \gcd(q, \varphi(n))$ many solutions.

Consequently, there are exactly b pairwise distinct solutions of $x^q \equiv a \bmod n$, and Assertion (3) is shown. ∎

Remarks. The proof of Theorem 11 is also constructive. So, if we can compute $\varphi(n)$, can find a generator g of $\mathbb{Z}_n^*$ and can solve the discrete logarithm problem for a, then we can compute qth roots efficiently. While the computation of $\varphi(n)$ in general is difficult, since all known algorithms require the factorization of n, here the situation is much easier, since we have only the cases for n shown in Theorem 7. For these cases, $\varphi(n)$ can be efficiently computed. However, finding a generator and solving the discrete logarithm problem for a are considered to be difficult.

Furthermore, we may restrict ourselves to moduli of the form p^e, where p is prime and $e \in \mathbb{N}^+$, since the case $n = 2p^e$ can be handled by using the Chinese remainder theorem.

Note that Theorem 11 still achieves the necessary level of generality for these cases. In contrast many authors restrict themselves to the cases $\gcd(p-1, q) = 1$ or $q|(p-1)$ (cf., e.g., [1, 4] and references therein). We shall come back to this point later.

3.3. *Further Easy Cases*

We continue with the exploration of more efficient algorithms for the rings $\mathbb{Z}_{p^e}$, where p is an odd prime and $e \in \mathbb{N}^+$. Inspired by Johnston [12] and the proof of Theorem 9 we found an algorithm that efficiently solves the qth root problem in $\mathbb{Z}_{p^e}^*$ provided p is an odd prime, and $b = \gcd(\varphi(p^e), q)$ is such that $\gcd(\varphi(p^e)/b, q) = 1$. Note that $\gcd(\varphi(p^e)/b, q) = 1$ implies that b divides $\varphi(p^e)$ exactly ones.

Theorem 12. *Let p be an odd prime, let $e, q \in \mathbb{N}^+$, let $b = \gcd(\varphi(p^e), q)$ be such that $\gcd(\varphi(p^e)/b, q) = 1$, and let $a \in \mathbb{Z}_p^*$. Then one can efficiently compute a solution of $x^q \equiv a \bmod p^e$.*

Proof. First, in accordance with Assertion (1) of Theorem 11 we have to check whether or not $a^{\varphi(p^e)/b} \equiv 1 \bmod p^e$. If this is not the case, then there does not exist any solution of $x^q \equiv a \bmod p^e$, and we are done.

Otherwise, we aim to determine a $z \in \mathbb{N}^+$ such that $(a^z)^q \equiv a \bmod p^e$. The latter condition is equivalent to $a^{zq-1} \equiv 1 \bmod p^e$, and thus we conclude that

$$zq - 1 \equiv 0 \mod \frac{\varphi(p^e)}{b} \tag{1}$$

must hold; i.e., the desired z must be the modular inverse of q with respect to the modulus $\varphi(p^e)/b$. Since $\gcd(\varphi(p^e)/b, q) = 1$, Theorem 2 ensures that z exists and that it is uniquely determined.

We claim that $x = a^z \bmod p^e$ is a solution of $x^q \equiv a \bmod p^e$. This can be seen as follows: Since $\gcd(\varphi(p^e)/b, q) = 1$, we know that there exists an integer $\ell \in \mathbb{Z}$ such that $zq = \ell \cdot \varphi(p^e)/b + 1$. Consequently, we obtain

$$\begin{aligned} a^{zq} &\equiv a^{\ell \cdot \varphi(p^e)/b + 1} \\ &\equiv \left(a^{\varphi(p^e)/b}\right) \cdot a \\ &\equiv 1 \cdot a \equiv a \mod p^e , \end{aligned}$$

where we used that $a^{\varphi(p^e)/b} \equiv 1 \bmod p^e$.

Having the knowledge that the modulus n is either a prime or a prime power, one can check in time $O\left((\log n)^3\right)$ which of the two cases occurs. This algorithm also finds p and e, and thus $\varphi(p^e)$ can be efficiently computed. The rest is a gcd calculation and the computation of a modular inverse. Hence, the theorem is shown. ∎

The proof of Theorem 12 is telling us how to compute efficiently *one* solution of the congruence $x^q \equiv a \bmod p^e$. The remaining $b-1$ solutions can then be easily obtained

provided we have a qth nonresidue η modulo p^e. Using Theorem 11 we then have $\eta^{\varphi(p^e)/b} \not\equiv 1 \bmod p^e$ By Theorem 5 we furthermore know that $\eta^{\varphi(p^e)} \equiv 1 \bmod p^e$. Consequently, if $q = \ell \cdot b$ then we directly obtain

$$\left(\eta^{\varphi(p^e)/b}\right)^q \equiv \left(\eta^{\varphi(p^e)/b}\right)^{b\cdot\ell} \equiv \left(\eta^{\varphi(p^e)}\right)^{\ell} \equiv 1 \mod p^e .$$

Hence, we found a solution of $x^q \equiv 1 \bmod p$. Using *mutatis mutandis* the same arguments as in the proof of Claim 2 in the demonstration of Theorem 11 we see that for $\zeta =_{df} \eta^{\varphi(p^e)/b} \bmod p^e$ the powers $\zeta^2, \ldots, \zeta^b$ are the pairwise different b solutions of $x^q \equiv 1 \bmod p^e$. The rest is then done as in Claim 3.

Example 1. We take the prime 8929 and try to solve $x^{217} \equiv 97 \bmod 8929$. Computing $b = \gcd(8928, 217) = 31$ and $8928/31 = 288$ yields that we have to check whether or not $97^{288} \equiv 1 \bmod 8929$. This is true and so we have to compute $\gcd(288, 217)$, which is 1. Therefore, now we solve $z \cdot 217 \equiv 1 \bmod 288$. We obtain $z = 73$ and hence the solution is $97^{73} \equiv 7174 \bmod 8929$. A quick check is in order here, and we verify that $7174^{217} \equiv 97 \bmod 8929$.

Theorem 11, Assertion (3) is telling us that there are precisely 31 solutions. So we randomly choose a number η and and check whether or not $\eta^{288} \not\equiv 1 \bmod 8929$. If it is, then we have found a 217th nonresidue. Let us take $\eta = 29$. We easily verify that $29^{288} \equiv 3891 \bmod 8929$ and that $3891^{217} \equiv 1 \bmod 8929$. Consequently, we have $\zeta = 3891$.

Next, we compute $\zeta^2, \ldots, \zeta^{31}$, and thus obtain

$$\begin{aligned} &5226,\ 3033,\ 6194,\ 1483,\ 2219,\ 8715,\ 6652,\ 6690,\ 2755,\ 4905,\\ &4082,\ 7300,\ 1151,\ 5112,\ 5909,\ 8673,\ 3952,\ 1494,\ 375,\ 3698\\ &4299,\ 3392,\ 1210,\ 2527,\ 1728,\ 111,\ 3309,\ 8630,\ 6290,\ 1 . \end{aligned}$$

Finally, we multiply our solution 7174 with each of these numbers to compute the remaining thirty solutions of $x^{217} \equiv 97 \bmod 8929$, which are

$$\begin{aligned} &7382,\ 7698,\ 5052,\ 4603,\ 7628,\ 552,\ 4872,\ 685,\ 4493,\ 8210,\\ &6077,\ 1615,\ 6878,\ 2085,\ 5203,\ 2830,\ 2073,\ 3156,\ 2621,\ 1393,\\ &260,\ 2683,\ 1552,\ 2828,\ 3220,\ 1633,\ 5484,\ 6863,\ 6223,\ 1980 . \end{aligned}$$

Here the last entry, i.e., 1980 is obtained by multiplying our solution 7174 with 3891, i.e., ζ, since we have already the solution 7174.

Note that 29 is *not* a generator of $\mathbb{Z}^*_{8929}$, since $29^{8928/3} \equiv 1 \bmod 8929$.

Of course, in the case of square roots Theorem 12 is just corresponding to the primes satisfying $p \equiv 3 \bmod 4$. Then $2|(p-1)$ but no higher power of 2 divides $p-1$. Since the modular inverse of 2 is $(p+1)/4$ with respect to the modulus $(p-1)/2$, we thus directly obtain that $a^{(p+1)/4} \bmod p$ is a solution of $x^2 \equiv a \bmod p$ provided a is a quadratic residue. This was already shown by Lagrange [15, page 500].

We finish this part by pointing out another easy case. Looking at the proof of Theorem 12 we see that we also can compute a qth root provided that a is also a qth residue for the highest power k of b dividing $\varphi(p^e)$. The resulting algorithm is almost the same except that we now compute the modular inverse of z with respect to the modulus $\varphi(p^e)/b^k$. Hence, we have the following corollary:

Corollary 2. *Let p be an odd prime, let $e, q \in \mathbb{N}^+$, and let $b = \gcd(\varphi(p^e), q)$ and $a \in \mathbb{Z}_p^*$ be such that $a^{\varphi(p^e)/b^k} \equiv 1 \bmod p^e$ for the highest power k of b dividing $\varphi(p^e)$ and $\gcd(\varphi(p^e)/b^k, q) = 1$. Then a solution of $x^q \equiv a \bmod p^e$ can be efficiently computed.*

Example 2. Let us solve the congruence $x^{39} \equiv 541 \bmod 8929^2$. Taking into account that $\gcd(8928, 39) = 3$ and that 3^2 also divides 8928 but 3^3 does not divide 8928, we have to compute $8929 \cdot 8928/9$ which is 8857568. Next, we verify that $\gcd(8857568, 39) = 1$. It remains to check whether or not $541^{8857568} \equiv 1 \bmod 8929^2$. Since this condition is satisfied, we compute the modular inverse of 39 with respect to the modulus 8857568, which is 7040631. Then we proceed as before, i.e., we compute $541^{7040631} \equiv 51594947 \bmod 8929^2$ and a quick check shows that we indeed have found a solution, since $51594947^{39} \equiv 541 \bmod 8929^2$.

The rest is *mutatis mutandis* done as before, i.e., we randomly choose $\eta \in \mathbb{Z}^*_{8929^2}$ until we find a 39th nonresidue, e.g., let us choose $\eta = 17$. Consequently, we have to compute $17^{8929 \cdot 8928/3} \equiv 54453631 \bmod 8929$, and thus verify that η is a 39th nonresidue modulo 8929.

Hence, now $\zeta = 54453631$ and $\zeta^2 = 25273409$. Therefore we directly obtain the three solutions $x_1 = 51594947$, $x_2 = 73511649$, and $x_3 = 34347486$.

3.4. *Square Roots*

We continue with another well-studied case, i.e., the computation of discrete square roots. In this regard, the Tonelli–Shanks algorithm, which was found by Tonelli [24], and reinvented by Shanks [22] with a small modification, is of particular interest as we shall show later. This algorithm was also generalized to the Adleman–Manders–Miller [1] algorithm. Here we follow Bach and Shallit [2].

Algorithm Tonelli 1

Input. An odd prime p, and an $a \in \mathbb{Z}_p^*$.

Output. The two solutions of $x^2 \equiv a \bmod p$ if a is a quadratic residue modulo p or *no solution* if a is quadratic nonresidue modulo p.

***Step* 1.** Check whether or not $a^{(p-1)/2} \equiv 1 \bmod p$. If this is not the case, then output *no solution* and stop.

Otherwise, execute the following steps:

***Step* 2.** Choose randomly an $\eta \in \mathbb{Z}_p^*$ until a quadratic nonresidue modulo p is found.

***Step* 3.** Let $p - 1 = 2^s \cdot t$, where t is odd.

***Step* 4.** Initialize $\varepsilon := 0$;

For $i = 2$ to s do

if $(a\eta^{-\varepsilon})^{(p-1)/2^i} \not\equiv 1 \bmod p$ then $\varepsilon := \varepsilon + 2^{i-1}$.

***Step* 5.** Compute $h := a\eta^{-\varepsilon}$;

$x_0 := \eta^{\varepsilon/2} \cdot h^{(t+1)/2} \bmod p$.

Output $\pm x_0 \bmod p$.

Theorem 13. *Algorithm Tonelli 1 is correct.*

Proof. By Theorem 11 we know that the output *no solution* is correct.

Next, assume that a is a quadratic residue. In Step 4 we have initially $\varepsilon = 0$ and thus $\eta^0 = 1$. Therefore the first test is to check whether or not $a^{(p-1)/4} \equiv 1 \mod p$. Since a is a quadratic residue we know that $a^{(p-1)/2} \equiv 1 \mod p$. Consequently, we know that $a^{(p-1)/4} \equiv \pm 1 \mod p$ (cf. Theorem 8).

Recall that $p - 1 = 2^s \cdot t$, and assume that $a^{(p-1)/4} \equiv -1 \mod p$; i.e., then ε is set to be 2, and we have

$$a^{2^{s-2} \cdot t} \equiv -1 \mod p \tag{2}$$

$$\eta^{-\varepsilon \cdot 2^{s-2} \cdot t} \equiv \eta^{-2^{s-1} \cdot t} \mod p\,. \tag{3}$$

Hence, multiplying (2) and (3) yields

$$(a\eta^{-\varepsilon})^{2^{s-2} \cdot t} \equiv (-1) \cdot \eta^{-2^{s-1} \cdot t} \mod p\,. \tag{4}$$

Since η is a quadratic nonresidue, we obtain $\eta^{-2^{s-1} \cdot t} \equiv \eta^{-(p-1)/2} \equiv -1 \bmod p$. Therefore, after updating ε in the loop of Step 4 we have

$$(a\eta^{-\varepsilon})^{2^{s-2} \cdot t} \equiv 1 \mod p\,.$$

Inductively we thus obtain that $(a\eta^{-\varepsilon})^{2^{s-i} \cdot t} \equiv 1 \bmod p$, and after the loop is finished, we know that

$$(a\eta^{-\varepsilon})^t \equiv 1 \mod p\,. \tag{5}$$

Finally, assume that $x_0 = \eta^{\varepsilon/2} \cdot h^{(t+1)/2} \bmod p$ is output. It remains to show that $x_0^2 \equiv a \bmod p$. Recall that $h = a\eta^{-e}$. Then we have

$$\begin{aligned} x_0^2 &\equiv \eta^{\varepsilon} \cdot h^{(t+1)} \equiv \eta^{\varepsilon} \cdot (a\eta^{-\varepsilon})^{t+1} \\ &\equiv \eta^{\varepsilon} a^{t+1} (\eta^{-\varepsilon})^{t+1} \equiv \eta^{\varepsilon} a^{t+1} (\eta^{-\varepsilon})^{t} \eta^{-\varepsilon} \\ &\equiv a^{t+1} (\eta^{-\varepsilon})^{t} \equiv a \cdot a^{t} (\eta^{-\varepsilon})^{t} \\ &\equiv a \cdot (a\eta^{-\varepsilon})^{t} \\ &\equiv a \mod p\,; \end{aligned}$$

where we used $(a\eta^{-\varepsilon})^t \equiv 1 \bmod p$ (cf. (5)). Hence, the theorem is shown. ∎

We note that Algorithm Tonelli 1 is a Las Vegas algorithm, since the desired quadratic nonresidue is found by randomly choosing an element $\eta \in \mathbb{Z}_p^*$ and then one applies Theorem 11. Since half of the elements of $\mathbb{Z}_p^*$ are quadratic residues and the other half are quadratic nonresidues, the expected number of executions of Step 2 is two. The rest of the algorithm is deterministic.

Claim 2. *The Algorithm Tonelli 1 executes* $O\left((\log p)^4\right)$ *bit operations.*

Proof. In each loop of Step 4 one has to perform a modular exponentiation. The maximum number of executions of this loop is given by the highest exponent of 2 dividing $(p-1)$ which is at most $\log p$. Finally, Step 5 requires two modular exponentiations. Since each modular exponentiation needs $O\left((\log p)^3\right)$ bit operations, Claim 2 is shown. ∎

Tonelli [25] derived an algorithm to solve the congruence $x^2 \equiv a \bmod p^e$, where p is an odd prime and $e \in \mathbb{N}^+$. We include this algorithm here, thereby using the same modifications Bach and Shallit [2] used for Tonelli's [24] algorithm.

Algorithm Tonelli 2

Input. An odd prime p, an $e \in \mathbb{N}^+$, and an $a \in \mathbb{Z}_{p^e}^*$.

Output. The two solutions of $x^2 \equiv a \bmod p^e$ if a is a quadratic residue modulo p^e or *no solution* if a is quadratic nonresidue modulo p^e.

***Step* 1.** Check whether or not $a^{(p-1)/2} \equiv 1 \bmod p$. If this is not the case, then output *no solution* and stop.

Otherwise, execute the following steps:

***Step* 2.** Choose randomly an $\eta \in \mathbb{Z}_p^*$ until a quadratic nonresidue modulo p is found.

***Step* 3.** Let $\varphi(p^e) = p^{e-1}(p-1) = 2^s \cdot t$, where t is odd.

***Step* 4.** Initialize $\varepsilon := 0$;

For $i = 2$ to s do

if $(a\eta^{-\varepsilon})^{(p-1)/2^i} \not\equiv 1 \bmod p$ then $\varepsilon := \varepsilon + 2^{i-1}$.

***Step* 5.** Compute $h := a\eta^{-\varepsilon} \bmod p^e$;

$x_0 := \eta^{\varepsilon/2} \cdot h^{(t+1)/2} \bmod p^e$.

Output $\pm x_0 \bmod p^e$.

We observe that $c \equiv \pm 1 \bmod p$ iff $c^{p^{e-1}} \equiv \pm 1 \bmod p^e$, where $c \in \mathbb{Z}$ is arbitrarily fixed. Consequently, the correctness of Algorithm Tonelli 2 can be shown *mutatis mutandis* as for Algorithm Tonelli 1. We omit the details.

Example 3. Let $p = 41$, let $e = 3$, and let $a = 5321$. We use Algorithm Tonelli 2 to solve $x^2 \equiv 5321 \bmod 41^e$. Note that $5321 \equiv 32 \bmod 41$.

In Step 1 we check whether or not $32^{20} \equiv 1 \bmod 41$. Since this is the case, we randomly choose $\eta = 17$ and verify that η is a quadratic nonresidue. Next, in Step 3 we compute $\varphi\left(41^3\right) = 2^3 \cdot 8405$, i.e., $s = 3$ and $t = 8405$.

In the first execution of the loop of Step 4 we find that $32^{10} \not\equiv 1 \bmod 41$. Consequently, we obtain $\varepsilon = 2$ and continue with $i = 3$.

We find that $\left(32 \cdot 17^{-2}\right)^5 \equiv 4 \bmod 41$. Hence, ε remains unchanged and we enter Step 5. We obtain $h = 5321 \cdot 18840 \equiv 36506 \bmod 41^3$. Since $(t+1)/2 = 4203$ we thus have $36506^{4203} \equiv 10984 \bmod 41^3$, and finally arrive at $17 \cdot 10984 \equiv 48886 \bmod 41^3$. Therefore, the output is 48886 and 20035.

A quick check is in order here, and we verify that $48886^2 \equiv 5321 \bmod 41^3$ and also that $20035^2 \equiv 5321 \bmod 41^3$.

Remark. Another remark is in order here. One may combine the Tonelli algorithms as described above with any of the easy cases given in Theorems 9 and 12 or Corollary 2 provided the corresponding assumptions are satisfied. Suppose we have to solve the congruence $x^q \equiv a \bmod p^e$. Then we use Theorem 11 to find out whether or not a is a qth residue. Next, we compute $b = \gcd(\varphi(p^e), q)$. Since we aim to apply one of the Tonelli algorithms, this gcd should be 2. Consequently, there is an $m \in \mathbb{N}^+$ such that $b = 2m$. If m is such that one of the easy cases is applicable, then we can directly compute a solution of $x^m \equiv a \bmod p^e$. Let x_0 be the solution found. Subsequently, we solve $y^2 \equiv x_0 \bmod p^e$, say we obtain $\pm y_0$. Then we know that $\left(y_0^2\right)^m \equiv a \bmod p^e$, i.e., $\pm y_0$ are solutions of $x^q \equiv a \bmod p^e$ and by Theorem 11 we know that there are no other solutions.

Example 4. Let $p = 8929$ and consider $x^{34} \equiv 140 \bmod 8929$. Furthermore, we have $2 = \gcd(8928, 34)$ and $\gcd(8928, 17) = 1$. Thus, Theorem 9 is applicable, and we find the solution 5113 of $x^{17} \equiv 140 \bmod 8929$. Using Algorithm Tonelli 1, we solve the congruence $y^2 \equiv 5113 \bmod 8929$ and obtain ± 7392.

Remark. The theory developed so far is sufficient to solve general quadratic congruences. Let $a', b', c' \in \mathbb{Z}_p^*$, and let the congruence $a'x^2 + b'x + c' \equiv 0 \bmod p$ be given, where p is an odd prime. In the first step we multiply both sides with the modular inverse c_a of a in $\mathbb{Z}_p^*$. We therefore obtain the congruence

$$x^2 + bx + c \equiv 0 \mod p \ ,$$

where $b \equiv b' \cdot c_a \bmod p$ and $c \equiv c' \cdot c_a \bmod p$.

Next, let c_2 and c_4 denote the modular inverses of 2 and 4, respectively, in Z_p^*. Then we directly obtain

$$x^2 + bx + c \ \equiv \ x^2 + bx + b^2c_4 - b^2c_4 + c \equiv (x + b \cdot c_2)^2 - \left(b^2c_4 - c\right) \mod p \ .$$

The reader should check that $c_2^2 \equiv c_4 \bmod p$.

Consequently, the congruence $x^2 + bx + c \equiv 0 \bmod p$ is equivalent to the congruence $(x + b \cdot c_2)^2 \equiv \left(b^2 c_4 - c\right) \bmod p$. The latter congruence is solvable iff $b^2 c_4 - c$ is a quadratic residue modulo p.

3.5. *Solving* $x^q \equiv a \mod p$ *for Odd Primes* p

Next, we turn our attention to find efficient algorithms for the solution of congruences of the form $x^q \equiv a \bmod p$, where p is an odd prime.

Nishihara et al. [18] studied the computation of cubic roots and considered the particular settings of the generalized Adleman–Manders–Miller [1] algorithm for this case. However, Bach and Shallit [2, pp. 160–163] contains already a complete description of the generalized Adleman–Manders–Miller [1] algorithm for the case that q is a prime divisor of $p - 1$. Since Theorem 11 is more general, it is only natural to ask whether or not one can generalize the Adleman–Manders–Miller [1] algorithm even further. We continue with an affirmative answer.

Let us start with $b = \gcd(p - 1, q)$. Then one can write $p - 1 = b^s \cdot t$ and has to distinguish the cases $\gcd(b, t) \neq 1$ and $\gcd(b, t) = 1$. As we shall see soon, the second case does not cause major problems. In order to see that the first case may occur, consider $p = 29$ and $q = 14$. Then we have $\gcd(28, 14) = 14$ and thus $28 = 14 \cdot 2$, i.e., we have $b = 14$ and $t = 2$. Hence, $\gcd(14, 2) \neq 1$.

Now, we can proceed *mutatis mutandis* as in Example 4. Dividing 14 by 2 yields 7, and thus one has to decompose the problem of finding a 14th root into the problem of computing first a 7th root and then the square root of the solution obtained for the 7th root. If all solutions are desired, then it is also beneficial to compare the amount of time used for the different problems. In the given setting it is easy to find all the seven roots of the 7th root problem once one root has been computed. But then we have to run the square root algorithm seven times. Alternatively, if one starts with the square roots, then one has to run the algorithm to find a 7th root two times. This may be more efficient.

Note that this technique can be easily generalized. If $\gcd(b, t) \neq 1$ then one has to divide b the gcd obtained and considers $\tilde{b} = b/\gcd(b, t)$. In turn, one then computes $p-1 = \tilde{b}^{\tilde{s}} \cdot \tilde{t}$. If $\gcd(\tilde{b}, \tilde{t}) \neq 1$, this technique is iterated. So, in the following we may assume that $\gcd(b, t) = 1$. Furthermore, without loss of generality we may assume that $0 \leqslant q \leqslant p - 1$ (cf. Theorem 6).

In the general case considered here, the basic idea can be described as follows: We assume that a is a qth residue modulo p, i.e., by Theorem 11 we have

$$a^{(p-1)/b} \equiv 1 \mod p \,, \tag{6}$$

where $b = \gcd(p-1, q)$. Moreover, we assume that $p-1 = b^s \cdot t$, where $\gcd(b, t) = 1$ and thus $\gcd(q, t) = 1$. In order to avoid the cases already handled in Theorem 12

and Corollary 2 we also assume that

$$a^{(p-1)/b^k} \not\equiv 1 \mod p \quad \text{for } k = 2, \ldots, s \,. \tag{7}$$

Hence, since $(p-1)/b = b^{s-1}t$ we also have

$$a^{b^{s-1}\cdot t} \equiv 1 \mod p. \tag{8}$$

Taking into account that $\gcd(q,t) = 1$ there is an $\ell \in \mathbb{N}^+$ such that $t|(q\ell-1)$. Hence, there exists an $m \in \mathbb{Z}$ such that $q\ell - 1 = mt$. The Congruence (8) implies

$$a^{b^{s-1}\cdot mt} \equiv 1 \mod p \,, \tag{9}$$

and thus we also have

$$\left(a^{q\ell-1}\right)^{b^{s-1}} \equiv 1 \mod p \,.$$

Consequently, we know that

$$\left(\left(a^{q\ell-1}\right)^{b^{s-2}}\right)^{b} \equiv 1 \mod p. \tag{10}$$

Next, let η be a qth nonresidue modulo p. Then Theorem 11 directly implies that $\eta^{(p-1)/b} \not\equiv 1 \bmod p$, and by Theorem 6 we know that $\left(\eta^{(p-1)/b}\right)^{b} \equiv 1 \bmod p$. Hence we conclude that $\eta^{(p-1)/b}$ is a bth root of unity. As already said above, then for $\zeta =_{df} \eta^{(p-1)/b}$ we know that $\zeta, \ldots, \zeta^{b-1}$ and $\zeta^0 =_{df} 1$ are pairwise different. Furthermore, since $q = bu$ for some $u \in \mathbb{N}^+$ we also have

$$\left(\eta^{(p-1)/b}\right)^{bu} \equiv 1 \mod p \,. \tag{11}$$

Using $(p-1)/b = b^{s-1}t$ we thus have

$$\left(\left(\eta^{t}\right)^{b^{s-1}}\right)^{b} \equiv 1 \mod p \,. \tag{12}$$

Moreover, by (10) we also know that $\left(a^{q\ell-1}\right)^{b^{s-2}}$ is also a bth root of unity.

We note that, if α is a bth root of unity, then α^{-1} is also a bth root of unity, since we easily verify that $(\alpha - 1)^b \equiv \left(\alpha^b\right)^{-1} \equiv 1 \bmod p$. Furthermore, the product of two bth roots of unity is a bth root of unity, and clearly, 1 is the neutral element with respect to multiplication. And multiplication modulo p is commutative. Hence, the bth roots of unity form an Abelian group.

Consequently, we can express all bth roots of unity as

$$U_j = \left(\eta^{t}\right)^{j\cdot b^{s-1}} \mod p \,, \quad j = 0, \ldots, b-1 \,. \tag{13}$$

Therefore, there is a uniquely determined $j_1 \in \{0, \ldots, b-1\}$ such that

$$\left(a^{q\ell-1}\right)^{b^{s-2}} \cdot \left(\eta^{t}\right)^{j_1\cdot b^{s-1}} \equiv 1 \mod p \,.$$

Using the group structure of the bth roots of unity, we thus conclude that there is a uniquely determined $j_2 \in \{0, \ldots, b-1\}$ such that

$$\left(a^{q\ell-1}\right)^{b^{s-3}} \cdot \left(\eta^t\right)^{j_1 \cdot b^{s-2}} \cdot \left(\eta^t\right)^{j_2 \cdot b^{s-1}} \equiv 1 \mod p .$$

Iterating this process, we find the remaining j_k, $k = 3, \ldots, s-1$, and arrive at

$$a^{q\ell-1} \cdot \left(\eta^t\right)^{j_1 \cdot b} \cdot \ldots \cdot \left(\eta^t\right)^{j_{s-1} \cdot b^{s-1}} \equiv 1 \mod p . \tag{14}$$

This in turn implies that

$$\begin{aligned} a^{q\ell} \cdot \left(\eta^t\right)^{j_1 \cdot b} \cdot \ldots \cdot \left(\eta^t\right)^{j_{s-1} \cdot b^{s-1}} &\equiv a \mod p \\ a^{q\ell} \cdot \left(\left(\eta^t\right)^{j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2}}\right)^b &\equiv a \mod p . \end{aligned} \tag{15}$$

Recalling that $b = \gcd(p-1, q)$ we know that there is a $y \in \mathbb{N}^+$ and a $z \in \mathbb{Z}$ such that $b = qy + (p-1)z$. This enables us to replace the b's in the exponents of (15) by $qy + (p-1)z$. Thus, we obtain the additional factors $\left(\left(\eta^t\right)^{p-1}\right)^z$ which are, by Theorem 6, congruent 1 modulo p. That is, we finally have

$$\left(a^\ell\right)^q \cdot \left(\left(\eta^t\right)^{(j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2})y}\right)^q \equiv a \mod p . \tag{16}$$

Thus, the solution x_0 of $x^q \equiv a \bmod p$ obtained by this computation can be directly read off; i.e., it is

$$x_0 = a^\ell \cdot \left(\eta^t\right)^{(j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2})y} \mod p . \tag{17}$$

Note that the computation of x_0 can be simplified by reducing the exponents ℓ and $(j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2})y$ modulo $p-1$.

We refer to the resulting algorithm as AMMG 1 for short. The AMMG 1 is a Las Vegas algorithm, since we have to choose randomly elements from $\mathbb{Z}_p^*$ until we have found a qth nonresidue.

Theorem 14. *Let p be an odd prime, let $q \in \mathbb{N}^+$, and let $a \in \mathbb{Z}_p^*$ such that a is a qth residue modulo p. Furthermore, let $b = \gcd(p-1, q$ be such that for $p-1 = b^s \cdot t$ the condition $\gcd(b, t) = 1$ is satisfied. Then the Algorithm* AMMG 1 *correctly computes a solution of $x^q \equiv a \bmod p$. The time complexity of the Algorithm* AMMG 1 *is $O\left(b(\log p)^4\right)$.*

Proof. The correctness was shown above. As far as the time complexity of the AMMG 1 is concerned, we note that the gcd computations and the modular exponentiations can be performed in time $O\left((\log p)^3\right)$. The difficult part is the computation of the numbers $j_1, \ldots, j_{s-1}$. This is actually a discrete logarithm problem, and if b is large then one may consider to use one of the well-known algorithms (cf., e.g., Menezes, van Oorschot and Vanstone [17]). If b is small, then just trying the possible values for j is feasible. So the overall complexity is $O\left(b(\log p)^4\right)$. ∎

Example 5. Let $p = 3001$ be the given prime modulus, and let us try to solve the congruence $x^{35} \equiv 19 \bmod 3001$. We obtain $\gcd(3000, 35) = 5$ and $3000 = 5^3 \cdot 24$. Next, we verify that $\gcd(24, 5) = 1$, and thus we can apply the algorithm described above.

First, we check $19^{600} \equiv 1 \bmod 3001$, which is true. The, we conclude that 19 is a 35th residue modulo 3001. Furthermore, we also have $19^{120} \not\equiv 1 \bmod 3001$, and thus we are not in the trivial case. Since we also need a 35th nonresidue, we randomly choose an element from the group $\mathbb{Z}^*_{3001}$, say 157 and have $157^{600} \equiv 2204 \bmod 3001$. By Theorem 11 we conclude that 157 is a 35th nonresidue.

The next step is the computation of ℓ. Using the ECLA we find $35 \cdot 11 - 1 = 16 \cdot 24$, i.e., we have $\ell = 11$. Note that $35 \cdot 11 - 1 = 384$. So we calculated $b = 5$, $s = 3$, $t = 24$, and also $q\ell - 1 = 384$.

Now, we have to find j_1 and j_2 as described above. First, we compute $a^{q\ell-1}$ and obtain $19^{384} \equiv 2012 \bmod 3001$. Since $s = 3$, we need $2012^5 \equiv 1125 \bmod 3001$. We continue with our 35th nonresidue and obtain $157^{24} \equiv 2996 \bmod 3001$. Note that we have $b^{s-1} = 25$. So, we try $j_1 = 0, 1, \ldots$ and find that for $j_1 = 2$ the desired condition $1125 \cdot 2996^{2 \cdot 25} \equiv 1 \bmod 3001$ is satisfied. Next, we proceed as described above and find $j_2 = 4$. That is, we have

$$\begin{aligned} 19^{384} \cdot \left(157^{24}\right)^{2 \cdot 5} \cdot \left(157^{24}\right)^{4 \cdot 25} &\equiv 2012 \cdot 371 \cdot 674 \\ &\equiv 1 \mod 3001 \,. \end{aligned}$$

In order to compute the solution, we use the ECLA and find the desired $y = 2743$, i.e., we obtain $5 = 35 \cdot 2743 - 3000 \cdot 32$. Consequently, our solution is

$$\begin{aligned} x_0 &\equiv 19^{11} \cdot 157^{24(2+4\cdot 5)\cdot 2743 \bmod 3000} \\ &\equiv 536 \mod 3001 \,. \end{aligned}$$

A quick check is in order here, and we verify that $536^{35} \equiv 19 \bmod 3001$.

Of course, one can also compute the remaining four solutions by using the 35th nonresidue *mutatis mutandis* as described in Example 1. By (12) we know that $(\eta)^{t \cdot b^{s-1}}$ is a bth root of unity. Hence we compute $\zeta =_{df} 2996^{25} \equiv 2204 \bmod 3001$ and also ζ^2, ζ^3, ζ^4 modulo 3001 and then multiply the already obtained solution 536 with $\zeta, \ldots, \zeta^4$. This gives us the remaining four solutions, which are 1951, 2572, 2800, and 1144.

Next we ask whether or not one can generalize the AMMG 1 along the lines yielding Algorithm Tonelli 2 from Algorithm Tonelli 1. This is indeed possible.

3.6. *Solving* $x^q \equiv a \mod p^e$ *for Odd Primes* p

In this section we shall provide the Algorithm AMMG 2, which can be used to directly solve $x^q \equiv a \bmod p^e$, where p is an odd prime, $e \in \mathbb{N}^+$, and $q \in \mathbb{N}^+$ is such that

$\gcd(p, q) = 1$. The case that $\gcd(p, q) \neq 1$ deserves special attention and will be considered in Section 4.5.

First, we note that $a \in \mathbb{Z}_{p^e}^*$ is a q residue modulo p^e if and only if it is a qth residue modulo p. This will be shown in Section 4.4.

Next, we outline the necessary modifications to obtain Algorithm AMMG 2. By Theorem 4 we know that $\varphi(p^e) = p^{e-1}(p-1)$. We assume that a is a qth residue modulo p^e, i.e., by Theorem 11 we have

$$a^{p^{e-1}(p-1)/b} \equiv 1 \mod p^e , \tag{18}$$

where $b = \gcd(\varphi(p^e), q)$. Again, we assume that $\varphi(p^e) = b^s \cdot t$, where $\gcd(b, t) = 1$ and thus $\gcd(q, t) = 1$. In order to avoid the cases already handled in Theorem 12 and Corollary 2 we also assume that

$$a^{\varphi(p^e)/b^k} \not\equiv 1 \mod p^e \quad \text{for } k = 2, \ldots, s . \tag{19}$$

Hence, since $\varphi(p^e)/b = b^{s-1}t$ we also have

$$a^{b^{s-1} \cdot t} \equiv 1 \mod p^e. \tag{20}$$

So, we have here a different t and therefore also a different ℓ; i.e., since $\gcd(q, t) = 1$ we can compute $\ell \in \mathbb{N}^+$ and $m \in \mathbb{Z}$ such that $q\ell - 1 = mt$.

The rest remains unchanged except that all computations have to be done modulo p^e, until we have reached the point shown in (15). Here we have to change the computation of y as follows: Using $b = \gcd(\varphi(p^e), q)$ we apply the ECLA to find a $y \in \mathbb{N}^+$ and a $z \in \mathbb{Z}$ such that $b = qy + \varphi(p^e)z$. Now we can replace the b's in the exponents of (15) by $qy + \varphi(p^e)z$. This yields the extra factors $\left((\eta^t)^{\varphi(p^e)}\right)^z$ which are, by Theorem 5, congruent 1 modulo p^e. That is, we finally have

$$\left(a^\ell\right)^q \cdot \left(\left(\eta^t\right)^{(j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2})y}\right)^q \equiv a \mod p^e . \tag{21}$$

Consequently, the solution x_0 of $x^q \equiv a \bmod p^e$ is

$$x_0 = a^\ell \cdot \left(\eta^t\right)^{(j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2})y} \mod p^e . \tag{22}$$

And of course we can again simplify the computation by reducing the exponents ℓ and $(j_1 + j_2 \cdot b + \cdots + j_{s-1} \cdot b^{s-2})y$ modulo $\varphi(p^e)$.

Hence, we have shown the following theorem:

Theorem 15. *Let p be an odd prime, let $e, q \in \mathbb{N}^+$, and let $a \in \mathbb{Z}_{p^e}^*$ such that a is a qth residue modulo p^e. Furthermore, let $b = \gcd(\varphi(p^e), q$ be such that for $\varphi(p^e) = b^s \cdot t$ the condition $\gcd(b, t) = 1$ is satisfied. Then the Algorithm* AMMG 2 *correctly computes a solution of $x^q \equiv a \bmod p^e$.*

Remarks. As far as the time complexity is concerned, we have to distinguish the cases that p^e is given as input and the p and e are given as input, respectively. In the first case, the time complexity is $O\left(b(\log p^e)^4\right)$. In the second case the time complexity of the Algorithm AMMG 2 crucially depends on the size of p^e and of a. If a has roughly the same size as p^e then the running time is as in the first case. However, if a and p are n bit numbers then one has to assume that $e \leqslant n^c$, where c is a constant. Then the length of the output is bounded by $O(n^2)$ many bits. Alternatively, one may require that a is n bit number and that p and e have at most n^c many bits, where c is again a constant.

The reader may wonder why we have to compute the numbers $j_1, \ldots, j_{s-1}$ modulo p^e. The reason is that these numbers may be different from the ones obtained modulo p (cf. Example 6).

Example 6. We use the same setting as in Example 5 except that we add the exponent 2 to the modulus 3001, i.e., we aim to solve $x^{35} \equiv 19 \bmod 3001^2$. Using Theorem 4 we obtain $\varphi(3001^2) = 9003000$, and thus $\varphi(3001^2) = 5^3 \cdot 72024$.

Therefore, we have $t = 72024$ and furthermore, $\ell = 12347$. Recall that ℓ is obtained by the ECLA applied to 72024 and 35; i.e., $\gcd(72024, 35) = 1 = 12347 \cdot 35 - 6 \cdot 72024$.

Hence, we obtain $35 \cdot 12347 - 1 = 432144$. We take the same 35th nonresidue as before and compute $157^{72024} \equiv 5611865 \bmod 3001^2$. Now we are in a position to compute j_1.

We have to compute the following:

$$\begin{aligned} \left(19^{432144}\right)^5 &\equiv 6015129 \mod 3001^2 , \\ \left(157^{72024}\right)^{25} &\equiv 5761123 \mod 3001^2 . \end{aligned}$$

Since $6015129 \cdot 5761123 \equiv 3980000 \bmod 3001^2$ we continue with $j_1 = 2$ and obtain $5761123^2 \equiv 2255749 \bmod 3001^2$. We verify that $6015129 \cdot 2255749 \equiv 1 \bmod 3001^2$ and therefore we have $j_1 = 2$.

It remains to compute j_2. Taking into account that

$$\begin{aligned} 19^{432144} &\equiv 7208038 \mod 3001^2 , \\ \left(157^{72024}\right)^{10} &\equiv 6530547 \mod 3001^2 , \end{aligned}$$

we check whether or not $7208038 \cdot 6530547 \equiv 1 \bmod 3001^2$. Since this congruence is satisfied, we know that $j_2 = 0$. Note that the j_2 obtained here is different from the one obtained in Example 5.

All what is left is to compute $y = 8488543$ and

$$\begin{aligned} x_0 &= 19^{12347} \cdot 5611865^{2 \cdot 8488543 \bmod \varphi(3001^2)} \\ &\equiv 1073013 \cdot 4128196 \equiv 6382698 \mod 3001^2 . \end{aligned}$$

And indeed we have $6382698^{35} \equiv 19 \bmod 3001^2$.

For the sake of completeness we also include the remaining solutions here, which are obtained as before. That is, we know that 5761123 is a 35th root of unity in $\mathbb{Z}^*_{3001^2}$. Consequently, the other four solutions are 6166854, 5922117, 7467024, and 1079310.

4. Lifting Algorithms

This section deals with algorithms allowing to compute solutions to the problems considered in $\mathbb{Z}^*_{p^e}$ provided we already have a solution of the problem modulo p, where p is a prime number, and $e \in \mathbb{N}^+$. We start this section with a decomposition of $\mathbb{Z}^*_{p^e}$, which will be helpful to show a lifting result for discrete square roots.

4.1. *A Decomposition of $\mathbb{Z}^*_{p^e}$*

Let p be a prime, and let $e \in \mathbb{N}^+$, $e \geqslant 2$. Following Hasse [10, Chapter 4] we decompose the group $\mathbb{Z}^*_{p^e} = G \times H$, where the set G is isomorphic to $\mathbb{Z}^*_p$ and the set H is defined as $H =_{df} \{r \mid r \in \mathbb{Z}^*_{p^e},\ r \equiv 1 \bmod p\}$. Now, it is easy to see that $|H| = p^{e-1}$ and that $|G| = p - 1$. Consequently, $|G \times H| = (p-1) \cdot p^{e-1} = \varphi(p^e)$.

So we are in a position to define the wanted group homomorphism $\alpha\colon \mathbb{Z}^*_p \to \mathbb{Z}^*_{p^e}$ for our decomposition $G \times H$. We set

$$\alpha(r) \quad =_{df} \quad r^{p^{e-1}} \mod p^e \quad \text{for all } r \in \mathbb{Z}^*_p\ . \tag{23}$$

Claim 1. *α is injective.*

Let r_1 and r_2 be any elements from $\mathbb{Z}^*_p$ such that $\alpha(r_1) = \alpha(r_2)$. We have to show $r_1 = r_2$. By assumption we have

$$r_1^{p^{e-1}} \quad = \quad r_2^{p^{e-1}} \mod p^e$$

and thus we also know that

$$r_1^{p^{e-1}} \quad = \quad r_2^{p^{e-1}} \mod p\ . \tag{24}$$

Observe that it suffices to show that

$$r^{p^{e-1}} \equiv r \mod p \quad \text{for all } r \in \mathbb{Z}^*_p\ . \tag{25}$$

This can be seen as follows: We have

$$(p-1)(p^{e-2} + \cdots + p + 1) + 1 \quad = \quad p^{e-1}\ . \tag{26}$$

Moreover, by Theorem 6 we know that $r^{p-1} \equiv 1 \bmod p$ and therefore we can conclude that $\left(r^{p-1}\right)^{(p^{e-2}+\cdots+1)} \equiv 1 \bmod p$. Since $r \equiv r \bmod p$, by (26) and by Theorem 1 we obtain $r^{(p-1)(p^{e-2}+\cdots+1)} \cdot r \equiv r^{p^{e-1}} \equiv r \bmod p$, and Claim 1 is shown.

Claim 2. *α is a group homomorphism.*

We have to show $\alpha(a \cdot b) = \alpha(a) \cdot \alpha(b)$ for all $a, b \in \mathbb{Z}_p^*$. By the definition of α we have

$$\alpha(a) \cdot \alpha(b) \equiv a^{p^{e-1}} b^{p^{e-1}} \equiv (ab)^{p^{e-1}} \mod p^e \,. \tag{27}$$

Let $k \equiv ab \bmod p$, where $k \in 1, \ldots, p-1$. Hence, there exists an $\ell \in \mathbb{Z}$ such that $k = ab + \ell p$. Using the binomial theorem we see that

$$\begin{aligned} k^{p^{e-1}} &= (ab + \ell p)^{p^{e-1}} = \sum_{i=0}^{p^{e-1}} \binom{p^{e-1}}{i} (ab)^{p^{e-1}-i} (\ell p)^i \\ &\equiv (ab)^{p^{e-1}} \mod p^e \end{aligned}$$

if and only if

$$\sum_{i=1}^{p^{e-1}} \binom{p^{e-1}}{i} (ab)^{p^{e-1}-i} (\ell p)^i \equiv 0 \mod p^e \,. \tag{28}$$

Since p is prime we conclude that p^{e-1} is only divisible by p. Furthermore, the products $\binom{p^{e-1}}{i} p^i$ are all divisible by p^e provided $i \geqslant 1$. Hence (28) is valid and Claim 2 is shown.

Remarks. If $i = 1$ then we obtain $\binom{p^{e-1}}{1} p = p^e$. Therefore, we see that we could not have used any power smaller than p^{e-1} in the definition of the group homomorphism α (cf. (23)).

Note that (25) directly implies that the mapping α is also surjective. Thus, the mapping α is bijective. Together with Claim 2 we conclude that α is an isomorphism. Therefore, we define

$$G =_{df} \operatorname{im}(\alpha) = \left\{ r^{p^{e-1}} \bmod p^e \mid r \in \mathbb{Z}_p^* \right\} \,. \tag{29}$$

Putting this all together we obtain the following algorithm computing the decomposition of $\mathbb{Z}_{p^e}^*$:

Algorithm DECOMP

Input: Any $a \in \mathbb{Z}_{p^e}^*$;

Output: $c_1 \in G$ and $c_2 \in H$ such that $a \equiv c_1 c_2 \bmod p^e$;

***Step* 1.** compute $r := a \bmod p$;

***Step* 2.** compute $c_1 := \alpha(r) = r^{p^{e-1}} \mod p^e$;

***Step* 3.** compute the modular inverse c_1^{-1} of c_1 in $\mathbb{Z}_{p^e}^*$.

***Step* 4.** compute $c_2 := a c_1^{-1} \mod p^e$.

It remains to show that the Algorithm DECOMP is correct.

Theorem 16. *Let $a \in \mathbb{Z}_{p^e}^*$, and let c_1, c_2 be the numbers returned by the Algorithm* DECOMP. *Then we have $c_1 \in G$, $c_2 \in H$ and $c_1 c_2 \equiv a \bmod p^e$.*

Proof. By construction we see that $c_1 \in G$. Furthermore, $c_2 \in \mathbb{Z}_{p^e}^*$ and thus it suffices to show that $c_2 \equiv 1 \bmod p$. Since $c_1 c_1^{-1} \equiv 1 \bmod p^e$, we conclude $c_1 c_1^{-1} \equiv 1 \bmod p$. By (25) and by construction we know that $c_1 \equiv r \equiv a \bmod p$ and therefore we arrive at $c_2 \equiv a c_1^{-1} \equiv r c_1^{-1} \equiv c_1 c_1^{-1} \equiv 1 \bmod p$.

Finally, $c_1 c_2 \equiv c_1 a c_1^{-1} \equiv c_1 c_1^{-1} a \equiv a \bmod p^e$, and the theorem is shown. ∎

It remains to say something about the time complexity of the Algorithm DECOMP. A closer look at this algorithm directly reveals that it crucially depends on the size of p^e and of a. So, if a has roughly the same size as p^e then the running time is polynomial in the length of the input. This can be achieved by assuming that a is an n-bit number and that p and e are less than or equal to n^c, where c is a constant. Or one allows p to be an n-bit number and requires $e \leqslant n^c$, where c is again a constant. Then a may have $O\left(n^2\right)$ many bits.

In the following we shall always assume one of these two settings.

4.2. *Lifting the Modular Inverse Modulo a Prime Power*

Since Algorithm DECOMP involves the computation of the modular inverse, it is only natural to ask whether or not there is also a lifting algorithm for this computation. We continue with the affirmative answer.

Let p be a prime, let $e \in \mathbb{N}^+$ be such that $e \geqslant 2$, and let $a \in \mathbb{Z}_{p^e}^*$. We assume that we know the modular inverse a^{-1} of a modulo p and aim to compute the modular inverse of a modulo p^e. Then the following iterative method can be used (cf. von zur Gathen [8]):

Algorithm INV

Input. Any $a \in \mathbb{Z}_{p^e}^*$ and $a^{-1} \in \mathbb{Z}_p^*$ such that $a a^{-1} \equiv 1 \bmod p$;

Output. $\tilde{a}^{-1} \in \mathbb{Z}_{p^e}^*$ such that $a \tilde{a}^{-1} \equiv 1 \bmod p^e$;

***Step* 1.** initialize $c_0 := a^{-1} \bmod p$;

***Step* 2.** for $i := 1$ to $i := \lceil \log e \rceil$ compute $c_i := \left(2c_{i-1} - a c_{i-1}^2\right) \bmod p^{2^i}$;

***Step* 3.** let $m := \lceil \log e \rceil$; output $c_m \bmod p^e$.

Theorem 17. *Let $a \in \mathbb{Z}_{p^e}^*$, let $a^{-1} \in \mathbb{Z}_p^*$ be such that $a a^{-1} \equiv 1 \bmod p$, and let c_m be the number returned by the Algorithm* INV. *Then we have $a c_m \equiv 1 \bmod p^e$.*

Proof. We show by induction on i that $ac_i \equiv 1 \bmod p^{2^i}$. By the assumption of the theorem and the initialization of the Algorithm INV we have $ac_0 \equiv 1 \bmod p$.

For $i \geqslant 1$ we have the induction hypothesis that $ac_{i-1} \equiv 1 \bmod p^{2^{i-1}}$. Consequently, we know that $p^{2^{i-1}} | (ac_{i-1} - 1)$. Hence, we directly obtain

$$\begin{aligned} ac_i &= 2ac_{i-1} - a^2c_{i-1}^2 = -\left(a^2c_{i-1}^2 - 2ac_{i-1} + 1\right) + 1 = -(ac_{i-1} - 1)^2 + 1 \\ &\equiv 1 \mod p^{2^i}, \quad (\text{since } p^{2^{i-1}} | (ac_{i-1} - 1)), \end{aligned}$$

and by the choice of m the theorem is shown. ∎

Remark. Comparing the method of Algorithm INV with the quadratic Newton iteration obtained for $f(x) =_{df} a - 1/x$, we see that there is a striking similarity. The technique used here is a special case of a more general result known as Hensel's lemma named after Kurt Hensel [11]. For more information about the history of this lemma we refer the reader to Roquette [19].

4.3. *Lifting Discrete Square Roots*

Let us start this subsection by showing the correctness of Tonelli's [24] formula to lift a solution of $x^2 \equiv a \bmod p$ to a solution of $x^2 \equiv a \bmod p^e$. Assume that x_0 is a solution, i.e., we have $x_0^2 \equiv a \bmod p$. Let

$$x_1 =_{df} x_0^{p^{e-1}} \cdot a^{(p^e - 2p^{e-1}+1)/2} \mod p^e ; \tag{30}$$

and let us show that $x_1^2 \equiv a \bmod p^e$. Tonelli [24] did not include a proof of (30). The correctness of (30) is shown as follows: Since $x_0^2 \equiv a \bmod p$, we also know that

$$x_0^2 \cdot a^{-1} \equiv 1 \mod p , \tag{31}$$

where a^{-1} denotes the modular inverse of a modulo p. Therefore, we apply the isomorphism α from our Algorithm DECOMP to the Congruence (31) and conclude that

$$\left(x_0^2 \cdot a^{-1}\right)^{p^{e-1}} \equiv 1^{p^{e-1}} \equiv 1 \mod p^e . \tag{32}$$

Next, using Theorem 4 we know that $\left|\mathbb{Z}_{p^e}^*\right| = \varphi(p^e) = p^e - p^{e-1}$, and by Theorem 5 we obtain

$$\begin{aligned} x_1^2 &\equiv \left(x_0^{p^{e-1}}\right)^2 \cdot a^{(p^e - 2p^{e-1}+1)} \\ &\equiv \left(x_0^{p^{e-1}}\right)^2 \underbrace{a^{p^e - p^{e-1}}}_{\equiv 1 \bmod p^e} \cdot a^{-p^{e-1}} \cdot a \\ &\equiv \left(x_0^2\right)^{p^{e-1}} \cdot \left(a^{-1}\right)^{p^{e-1}} \cdot a \\ &\equiv \left(x_0^2 \cdot a^{-1}\right)^{p^{e-1}} \cdot a \equiv 1 \cdot a \equiv a \mod p^e , \end{aligned}$$

where the last step is due to (32).

The correctness proof given above allows for the following corollary:

Corollary 3. *Let p be any odd prime, let $a \in \mathbb{Z}_p^*$, let $e \in \mathbb{N}^+$, and let x_0 be a solution of $x^2 \equiv a \bmod p$. Then*

$$x_1 \;=\; x_0^{p^{e-1}} \cdot a^{(1-p^{e-1})/2} \mod p^e$$

is a solution of $x^2 \equiv a \bmod p^e$.

Proof. Squaring x_1 modulo p yields $\left(x_0^{p^{e-1}}\right)^2 \cdot a^{(1-p^{e-1})} \bmod p^e$ and we are back to line 2 in the proof given above. ∎

It is also obvious that every solution of $x^2 \equiv a \bmod p^e$, $e \geqslant 2$, satisfies the congruence $x^2 \equiv a \bmod p$. This directly implies that the congruence $x^2 \equiv a \bmod p^e$ is solvable if and only if the congruence $x^2 \equiv a \bmod p$ is solvable. Hence, it remains to ask whether or not there may be more than two solutions of $x^2 \equiv a \bmod p^e$. In order to answer this question we proceed as follows:

Let p be any odd prime, let $e \in \mathbb{N}$ be such that $e \geqslant 2$, and assume that the congruence $x^2 \equiv a \bmod p$ is solvable. Furthermore, let x_0 be any fixed solution of $x^2 \equiv a \bmod p$. Then there is a uniquely determined solution x of $x^2 \equiv a \bmod p^e$ such that $x \equiv x_0 \bmod p$.

As we have already seen, there is a always such a solution x of $x^2 \equiv a \bmod p^e$. So it remains to show that it is uniquely determined. Suppose to the contrary that there are x_1 and y_1 such that $x_1^2 \equiv a \bmod p^e$ and $y_1^2 \equiv a \bmod p^e$, and that furthermore the condition $x_1 \equiv y_1 \equiv x_0 \bmod p$ is satisfied. Then we have $x_1^2 - y_1^2 \equiv 0 \bmod p^e$ (cf. Theorem 1). Consequently, we obtain

$$(x_1 - y_1)(x_1 + y_1) \;\equiv\; 0 \mod p^e\,. \tag{33}$$

Since $x_1 \equiv y_1 \equiv x_0 \bmod p$, we see that $x_1 + y_1 \equiv 2x_0 \bmod p$. Taking into account that $2 \in \mathbb{Z}_p^*$ and $x_0 \in \mathbb{Z}_p^*$, we conclude that $2x_0 \in \mathbb{Z}_p^*$. Since $\mathbb{Z}_p^*$ is the multiplicative group of the field $\mathbb{Z}_p$, we know that the modular inverse $(x_1 + y_1)^{-1}$ of $(x_1 + y_1)$ in $\mathbb{Z}_p^*$ exists. By Theorem 17 we thus know that $(x_1 + y_1)$ has a modular inverse in $\mathbb{Z}_{p^e}^*$. Multiplying both sides of the Congruence (33) with this modular inverse directly yields $x_1 - y_1 \equiv 0 \bmod p^e$, and we are done.

Summarizing, we have the following theorem:

Theorem 18. *Let p be any odd prime, let $e \in \mathbb{N}$ be such that $e \geqslant 2$, and let $a \in \mathbb{Z}_p^*$. Then we have the following:*

(1) *The element a is a quadratic residue modulo p^e if and only if it is a quadratic residue modulo p;*

(2) *if a is a quadratic residue modulo p^e then the congruence $x^2 \equiv a \bmod p^e$ has two solutions and these solutions are of the form $\pm x \bmod p^e$.*

However, Tonelli's [24] lifting method is not the only one, and it seems difficult to generalize it to higher roots. So it is appropriate to include a further method here, which maybe interesting in its own right.

The idea is to lift a solution available modulo p^e to a solution modulo p^{2e}. Then, by iterating this method one obtains a quite efficient method. In order to see of how to obtain such a method, we make the following approach: Assume that we have a solution x_0; i.e.,

$$x_0^2 \equiv a \mod p^2 . \tag{34}$$

The Congruence (34) implies that $1 - x_0^2 \cdot a^{-1}$ is divisible by p^e, where a^{-1} is the modular inverse of $a \mod p^e$. Hence, we know that $\left(1 - x_0^2 \cdot a^{-1}\right)^2$ is divisible by p^{2e}. Since we are looking for an x_1 such that $x_1^2 \equiv a \bmod p^{2e}$, we set $x_1 =_{df} x_0(1 + tp^e)$. The parameter $t \in \mathbb{Z}^*_{p^{2e}}$ has to be determined such that $x_1^2 \cdot a^{-1} \equiv 1 \bmod p^{2e}$, where a^{-1} is the modular inverse of a modulo p^{2e}. Putting this together we have

$$x_1^2 \cdot a^{-1} \equiv 1 \equiv 1 + \left(1 - x_0^2 \cdot a^{-1}\right)^2 \mod p^{2e} . \tag{35}$$

Since $x_1^2 \equiv x_0^2(1 + tp^e)^2 \equiv x_0^2(1 + 2tp^e) \bmod p^{2e}$, we obtain from (35) that

$$\begin{aligned} x_0^2 \cdot a^{-1}(1 + 2tp^e) &\equiv 1 + \left(1 - x_0^2 \cdot a^{-1}\right)^2 \\ &\equiv 2 + x_0^2 \cdot a^{-1}(x_0^2 \cdot a^{-1} - 2) \mod p^{2e} \end{aligned} \tag{36}$$

must hold. Multiplying both sides of this congruence with the modular inverse $\left(x_0^2 \cdot a^{-1}\right)^{-1}$ of $x_0^2 \cdot a^{-1}$ modulo p^{2e} yields

$$1 + 2tp^e \equiv 2 \cdot \left(x_0^2 \cdot a^{-1}\right)^{-1} + x_0^2 \cdot a^{-1} - 2 \mod p^{2e} .$$

From the latter congruence we conclude that the modular inverse of x_0^2 has to be congruent to $1 + 2tp^e$. Consequently, we arrive at

$$\begin{aligned} 1 + 2tp^e &\equiv 2(1 + 2tp^e) + x_0^2 \cdot a^{-1} - 2 \mod p^{2e} \\ 1 + 2tp^e &\equiv 2 - x_0^2 \cdot a^{-1} \mod p^{2e} \\ tp^e &\equiv \left(1 - x_0^2 a^{-1}\right) 2^{-1} \mod p^{2e} . \end{aligned} \tag{37}$$

So we need the modular inverse of 2 modulo p^{2e}. Recall that p is odd. Hence, $p^{2e} + 1$ is even. Since $(p^{2e} + 1) \equiv 1 \bmod p^{2e}$, it is advantageous to replace (37) by

$$tp^e \equiv \left(1 - x_0^2 a^{-1}\right) \cdot \frac{p^{2e} + 1}{2} .$$

Finally, in order to obtain the desired lifting algorithm we also have to update the modular inverse of a in each iteration. This is done by using Step 2 of the Algorithm INV. Thus, we shall use $c_{a,i}$ to denote the modular inverse of a modulo p^{2i}. Alternatively, one may use the Algorithm ECLA to compute the modular inverse modulo p^e and then reduce it modulo p^{2i}. For sequential computations both methods seem feasible. But if one aims to perform parallel computations, then the first method is more appropriate.

Summarizing, we thus have the following lifting algorithm:

Algorithm LIFT1

Input. An odd prime p, an integer $e \geqslant 2$, a quadratic residue $a \in \mathbb{Z}_{p^e}^*$, $c_{a,0}$, and a solution x_0 of $x^2 \equiv a \bmod p$.

Output. $x_m \in \mathbb{Z}_{p^e}^*$ such that $x_m^2 \equiv a \bmod p^e$ and $x_m \equiv x_o \bmod p$.

***Step* 1.** for $i = 1, 2, \ldots, \lceil \log e \rceil$ compute $c_{a,i} := \left(2c_{a,i-1} - ac_{a,i-1}^2\right) \bmod p^{2^i}$ and

$$x_i \equiv \left(x_{i-1} + x_{i-1}\left(1 - x_{i-1}^2 c_{a,i}\right) \cdot \left(p^{2^i} + 1\right)/2\right) \mod p^{2^i} .$$

***Step* 2.** Let $m = \lceil \log e \rceil$. Output $x_m \bmod p^e$.

As described above, the Algorithm LIFT1 needs $\lceil \log e \rceil$ many iterations of Step 1. On the other hand, each iteration is easy to compute and does not involve any modular exponentiation as Tonelli's [24] lifting technique does.

We continue with the case $p = 2$, which deserves special attention by at least two reasons. First, observe that in all the cases considered so far we have $\gcd(p, 2) = 1$, where 2 is the degree of the polynomial. Since 2 is even, a new situation arises, i.e., $\gcd(2, 2) = 2$. Second, we have to clarify how many solutions may occur. For example, the congruence $x^2 \equiv 3 \bmod 2$ is equivalent to $x^2 \equiv 1 \bmod 2$, which has precisely one solution, i.e., $x = 1$. But $x^2 \equiv 3 \bmod 2^2$ and $x^2 \equiv 3 \bmod {}^2$ do not have any solution as a quick check reveals. Moreover, $x^2 \equiv 1 \bmod 2^2$ possesses the two solutions $x_1 = 1$ and $x_2 = 3$ and the congruence $x^2 \equiv 1 \bmod 2^3$ possesses the four solutions $x_1 = 1$, $x_2 = 3$, $x_3 = 5$, and $x_4 = 7$.

So, it is no longer true that $x^2 \equiv a \bmod 2^e$ is solvable iff $x^2 \equiv a \bmod 2$ is solvable, provided $e \geqslant 2$. We have also seen that 1 is the *only* quadratic residue modulo 8. So, it also no longer true that *half* of the elements of $\mathbb{Z}_{2^e}^*$ are quadratic residues and *half* of them are quadratic nonresidues.

We also observe that the solutions of $x^2 \equiv 1 \bmod 2^3$ can be written as $x_1 = 1$, $x_4 = -x_1 \bmod 2^3$, $x_3 = (x_1 + 2^2) \bmod 2^3$, and $x_2 = (-x_1 + 2^2) \bmod 2^3$.

Let us check the latter observation for the modulus p^4. We already know that $\mathbb{Z}_{2^4}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$. Squaring all these elements we obtain

$$\begin{aligned} 1^2 &\equiv 1 \mod 2^4 , & 9^2 &\equiv 1 \mod 2^4 , \\ 3^2 &\equiv 9 \mod 2^4 , & 11^2 &\equiv 9 \mod 2^4 , \\ 5^2 &\equiv 9 \mod 2^4 , & 13^2 &\equiv 9 \mod 2^4 , \\ 7^2 &\equiv 1 \mod 2^4 , & 15^2 &\equiv 1 \mod 2^4 . \end{aligned}$$

This directly shows that the quadratic residues of $\mathbb{Z}_{2^4}^*$ are 1 and 9, i.e., $a \in \mathbb{Z}_{2^4}^*$ is a quadratic residue iff $a \equiv 1 \bmod 8$. We also see that $x_1 = 3$, $x_2 = -x_1 = 13$, $x_3 = (x_1 + 2^3) \equiv 11 \bmod 2^4$, and $x_4 = (x_2 + 2^3) \equiv 5 \bmod 2^4$ are the solutions of $x^2 \equiv 9 \bmod 2^4$. The four solutions of $x^2 \equiv 1 \bmod 2^4$ can be analogously represented.

Next, we provide a lifting method for moduli of the form 2^e, where $e \geqslant 4$ (cf. Zeugmann [27]). The cases $e = 1, 2, 3$ are trivial and thus omitted.

Algorithm LIFT2

Input. A natural number $e \geqslant 4$, and a quadratic residue $a \in \mathbb{Z}^*_{2^e}$.

Output. The four solutions of $x^2 \equiv b \bmod 2^e$.

***Step* 1.** Compute an x_0 such that $x_0^2 \equiv a \bmod 2^4$ and initialize $d = 3$.

***Step* 2.** Assume that we are given a solution x of $x^2 \equiv a \bmod 2^{d+1}$.

Compute the modular inverse $c_{a,2d}$ of a modulo 2^{2d}. Then calculate

$$\hat{x} \;:=\; \left(x + x(1 - x^2 \cdot c_{a,2d})/2\right) \mod 2^{2d} \;.$$

Set $d := 2d - 1$, and iterate the construction until the exponent $2d$ reaches e. That means, from x_0 we calculate $x_1 \bmod 2^6$, then $x_2 \bmod 2^{10}$, a.s.o.

***Step* 3.** Let x_m be the last iterate obtained. Then output $x_m \bmod 2^e$, $-x_m \bmod 2^e$, $\left(x_m + 2^{e-1}\right) \bmod 2^e$, and $\left(-x_m + 2^{e-1}\right) \bmod 2^e$.

Here we left it open how the modular inverses are computed. One could use our Algorithm INV, Euler's theorem 5, or the ECLA.

It remains to show the correctness of the Algorithm LIFT2. This is done inductively as follows: By assumption we possess a solution of $x^2 \equiv a \bmod 2^{d+1}$; i.e., we know that $2^{d+1} \mid (1 - x^2 \cdot c_{a,2d})$. Consequently, $2^d \mid (1 - x^2 \cdot c_{a,2d})/2$. This in turn implies that 2^{2d} divides $\left((1 - x^2 \cdot c_{a,2d})/2\right)^2$. We have to show that $\hat{x}^2 \equiv a \mod 2^{2d}$. Squaring $\hat{x}$ yields

$$\begin{aligned} \hat{x}^2 &\equiv x^2 + 2x^2\left(1 - x^2 \cdot c_{a,2d}\right)/2 + \underbrace{\left((1 - x^2 \cdot c_{a,2d})/2\right)^2}_{\equiv 0} \\ &\equiv x^2 + x^2\left(1 - x^2 c_{a,2d}\right) \mod 2^{2d} \;. \end{aligned} \tag{38}$$

At this point we need an idea of how to proceed, *et voilà*, here it comes. It suffices to show that $\hat{x}^2 \cdot c_{a,2d} - 1 \equiv 0 \bmod p^{2d}$. Using (38) we thus have

$$\begin{aligned} \hat{x}^2 \cdot c_{a,2d} - 1 &\equiv x^2 \cdot c_{a,2d} + x^2 \cdot c_{a,2d}\left(1 - x^2 \cdot c_{a,2d}\right) - 1 \\ &\equiv -\left(1 - x^2 \cdot c_{a,2d}\right) + x^2 \cdot c_{a,2d}\left(1 - x^2 \cdot c_{a,2d}\right) \\ &\equiv -\left(1 - x^2 \cdot c_{a,2d}\right)^2 \\ &\equiv 0 \mod 2^{2d} \;, \end{aligned}$$

where the last step is due to $2^{2d} \mid \left(1 - x^2 \cdot c_{a,2d}\right)$.

Clearly, if x is a solution of $x^2 \equiv a \bmod 2^e$ the so is $-x$. Taking into account that $\left(x + 2^{e-1}\right)^2 \equiv x \bmod 2^e$ we see that the four elements output are indeed solutions. Hence, the correctness is shown.

Moreover, if $x^2 \equiv a \bmod 2^e$ for any $e \geqslant 4$ then we also know that $x^2 \equiv a \bmod 2^3$. Consequently, if there is a solution modulo 2^e then we have $a \equiv 1 \mod 2^3$, since 1 is the only quadratic residue modulo 2^3.

Hence, it remains to show that there are no other solutions. If $x \in \mathbb{Z}_{2^e}^*$ then x must be odd. Consequently, suppose we have $x^2 \equiv y^2 \equiv a \bmod 2^e$. Then we directly obtain $x^2 - y^2 \equiv 0 \bmod 2^e$; i.e., we know that

$$(x+y)(x-y) \equiv 0 \mod 2^e \ . \tag{39}$$

Since both x and y are odd and since $(x+y)+(x-y) = 2x$ we conclude that either $(x+y)$ or $(x-y)$ is divisible by 4. The Congruence (39) thus implies that the factor which is divisible by 4 must be even divisible by 2^{e-1}. That means we have just four possibilities; i.e., $x \equiv y \bmod 2^e$, $x \equiv y + 2^{e-1} \bmod 2^e$, $x \equiv -y \bmod 2^e$, and also $x \equiv -y + 2^{e-1}$. Consequently the Algorithm LIFT2 computes all solutions. It is also easy to see that these four solutions are pairwise incongruent modulo 2^e.

Summarizing, we thus have the following theorem:

Theorem 19. *Let $p = 2$, let $e \in \mathbb{N}$ be such that $e \geqslant 3$, and let $a \in \mathbb{Z}_p^*$. Then we have the following:*

(1) *The element a is a quadratic residue modulo 2^e if and only if $a \equiv 1 \bmod 8$;*

(2) *if a is a quadratic residue modulo 2^e then the congruence $x^2 \equiv a \bmod 2^e$ has exactly four solutions and these solutions are of the form $x \bmod 2^e$, $-x \bmod 2^e$, $\left(x + 2^{e-1}\right)$, and $\left(-x + 2^{e-1}\right)$.*

4.4. *Lifting Discrete qth Roots*

At this point it is only natural to ask whether or not we can generalize our lifting methods to qth roots. The affirmative answer is presented below. We follow here Zeugmann [27]. As in the case of discrete square roots we have to distinguish the cases whether or not the exponent and the modulus have a nontrivial common factor. We start with the case that $\gcd(p, q) = 1$.

Theorem 20. *Let p be any prime, let $e \in \mathbb{N}^+$, let $q \in \mathbb{N}^+$ be such that $\gcd(p, q) = 1$, and let $a \in \mathbb{N}^+$ and $x_0 \in \mathbb{Z}_p^*$ be such that $x_0^{q \bmod (p-1)} \equiv a \bmod p$. Then one can lift this solution x_0 to a uniquely determined solution x_1 of $x^q \equiv a \bmod p^e$.*

Proof. First, we compute the modular inverses $c_{a,0}$ and $c_{q,0}$ in $\{1, \ldots, p-1\}$ of a and q modulo p, respectively, and set $x_{0,0} = x_0$. Then start Algorithm LIFT3.

Algorithm LIFT3

Input. A prime p, a natural number $e \geqslant 2$, $q \in \mathbb{N}^+$ such that $\gcd(p, q) = 1$, a qth residue $a \in \mathbb{Z}_{p^e}^*$, an initial solution $x_{0,0}$ of $x_0^q \equiv a \bmod p$, and the modular inverses $c_{a,0}$ and $c_{q,0}$ modulo p.

Output. The solution x_1 of $x^q \equiv b \bmod p^e$ such that $x_1 \equiv x_{0,0} \bmod p$.

***Step* 1.** For $i = 1, 2, \ldots \lceil \log e \rceil$ compute

$$\begin{aligned} c_{a,i} &:= \left(2 \cdot c_{a,i-1} - a \cdot c_{a,i-1}^2\right) \mod p^{2^i} \\ c_{q,i} &:= \left(2 \cdot c_{q,i-1} - q \cdot c_{q,i-1}^2\right) \mod p^{2^i} \\ x_{0,i} &:= \left(x_{0,i-1} + x_{0,i-1}\left(1 - x_{0,i-1}^q c_{a,i}\right) c_{q,i}\right) \mod p^{2^i} . \end{aligned}$$

(Note that $c_{a,i}$ and $c_{q,i}$ are the modular inverses of a and q modulo p^{2^i})

***Step* 2.** Let $m = \lceil \log e \rceil$. Output $x_1 := x_{0,m} \bmod p^e$.

It remains to show the correctness of this algorithm. Since $a \in \mathbb{Z}_{p^e}^*$, we know that its modular inverse modulo p^e exists. By assumption we also know that $\gcd(p, q) = 1$, and thus the modular inverse of q modulo p^e exists, too. Furthermore, the computation of $c_{a,i}$ and $c_{q,i}$, respectively, are just done as in Algorithm INV, and thus correct.

In order to show that x_1 is a solution of $x^q \equiv a \bmod p^e$, it suffices to prove that $x_{0,i}^q c_{a,i} \equiv 1 \bmod p^{2^i}$ for $i = 0, \ldots, \lceil \log e \rceil$. This is done inductively.

The induction basis is clear by construction. Assuming the induction hypothesis that $p^{2^{i-1}} \mid \left(1 - x_{0,i-1}^q c_{a,i-1}\right)$ the induction step is done as follows:

$$\begin{aligned} x_{0,i}^q c_{a,i} &\equiv c_{a,i}\left(x_{0,i-1} + x_{0,i-1}\left(1 - x_{0,i-1}^q c_{a,i}\right) c_{q,i}\right)^q \\ &\equiv x_{0,i-1}^q c_{a,i}\left(1 + \left(1 - x_{0,i-1}^q c_{a,i}\right) c_{q,i}\right)^q \\ &\equiv x_{0,i-1}^q c_{a,i} \sum_{\nu=0}^{q} \binom{q}{\nu} \left(1 - x_{0,i-1}^q c_{a,i}\right)^\nu c_{q,i}^\nu \\ &\equiv x_{0,i-1}^q c_{a,i} + x_{0,i-1}^q c_{a,i}\left(1 - x_{0,i-1}^q c_{a,i}\right) \mod p^{2^i} , \end{aligned}$$

where the latter step results from the fact that, in accordance with the induction hypothesis, we have $p^{2^{i-1}} \mid \left(1 - x_{0,i-1}^q c_{a,i-1}\right)$. Hence, we see that $p^{2^i} \mid \left(1 - x_{0,i-1}^q c_{a,i-1}\right)^\nu$ for every $\nu \geqslant 2$. Moreover, we have $\binom{q}{1} = q$ and $c_{q,i} q \equiv 1 \bmod p^{2^i}$.

Thus, finally we obtain

$$\begin{aligned} x_{0,i}^q c_{a,i} &\equiv x_{0,i-1}^q c_{a,i} - \left(1 - x_{0,i-1}^q c_{a,i} - 1\right)\left(1 - x_{0,i-1}^q c_{a,i}\right) \\ &\equiv x_{0,i-1}^q c_{a,i} + 1 - x_{0,i-1}^q c_{a,i} - \left(1 - x_{0,i-1}^q c_{a,i}\right)^2 \\ &\equiv 1 \mod p^{2^i} . \end{aligned}$$

Consequently, x_1 is a solution of $x^q \equiv a \bmod p^e$. So, it also satisfies the congruence $x_1^q \equiv a \bmod p$. Since $x_0^q \equiv a \bmod p$ by assumption, we have $x_1 - x_0 \equiv 0 \bmod p$. Therefore, x_1 and x_0 are, when taken modulo p, the same. ∎

Remarks. By Theorem 20 we know how to efficiently lift one given solution x_0 of the congruence $x_0^{q \bmod (p-1)} \equiv a \bmod p$ to a solution x_1 of the congruence $x^q \equiv a \bmod p^e$. On the other hand, if $b = \gcd(p-1, q)$ then the congruence $x_0^{q \bmod (p-1)} \equiv a \bmod p$ possesses precisely b many solutions (cf. Theorem 11). Taking into account that $\varphi(p^e) = p^{e-1}(p-1)$ and that $\gcd(p, q) = 1$, we conclude that $\gcd(\varphi(p^e), q) = b$, too. Thus, the congruence $x^q \equiv a \bmod p^e$ also has precisely b many solutions.

Therefore, it is only natural to ask whether or not one has to lift each solution obtained modulo p to its corresponding solution modulo p^e or if we can compute the remaining solutions modulo p^e more efficiently.

Looking at the proof of Theorem 11, we see that we can use the same algorithm to find the remaining solutions; i.e., by computing a solution ζ of $x^q \equiv 1 \bmod p^e$, then calculating $\zeta^2, \ldots, \zeta^{b-1}$, and finally by multiplying x_1 with each of the obtained values $\zeta, \ldots, \zeta^{b-1}$. Note that ζ can be found as before. We randomly pick an element $\eta \in \mathbb{Z}_{p^e}^*$ until we find a qth nonresidue.

4.5. *The Case* $\gcd(p, q) \neq 1$

Next, we have to solve the case that $\gcd(p, q) \neq 1$. Since we have already studied the subcase $p = 2$, it remains to handle the case that the prime p is odd. First, we consider the case that $p = q$, and then we shall consider the general case.

Mutatis mutandis we have to overcome the same problems mentioned before presenting the Algorithm LIFT2. In particular, it is no longer true that $x^p \equiv a \bmod p^e$ is solvable if and only if $x^p \equiv a \bmod p$ is solvable. In particular, Theorem 6 implies that $x^p \equiv a \bmod p$ has the uniquely determined solution $x = a$. In contrast, provided that a is a pth residue modulo p^e, then we always have p solutions.

Theorem 21. *Let p be any odd prime, let $e \in \mathbb{N}^+$, and let $a \in \mathbb{N}^+$. Then one can (efficiently) compute all solutions of $x^p \equiv a \bmod p^e$.*

Proof. First, if $a = 0$ or a is such that p divides a then $x = 0$ is the only solution, and we are done.

Second, if $a \in \mathbb{N}^+$ and p does not divide a then we distinguish the following cases:

Case 1. $e = 1$.

Then, we know that $\gcd(p, a) = 1$, and so $a \in \mathbb{Z}_p^*$. Consequently $x_0 := a \bmod p$ is the only solution of $x^p \equiv a \bmod p$, and the theorem is shown.

Case 2. $e > 1$.

We note that Theorem 11 is applicable. Since $b = \gcd(\varphi(p), p) = p$ we have to check whether or not a is a pth residue modulo p^e. If it is not, then there is no solution.

If a is a pth residue modulo p^e, then we know by Theorem 11, Assertion (3), that there are precisely p solutions. So, it remains to show how these solutions are computed. This is done as follows:

Note that if a is a pth residue modulo p^e then it is also a pth residue modulo p^k for all $k = 1, \ldots, e-1$. This is a direct consequence of Theorem 11, Assertion (1). Then we also know that $a \in \mathbb{Z}^*_{p^e}$. Our strategy is to find a solution modulo p^2. Having the latter solution we lift it to a solution modulo p^3. Afterwards, we shall use a modification of the Algorithm LIFT2. This ensures that the number of lifting steps is bounded by $O(\log e)$.

Next, we take $x_1 := (a + p) \bmod p^2$, and show the following claim:

Claim 1. x_1 *is a solution of* $x^p \equiv a \bmod p^2$.

We have to compute x_1^p. Note that $p^{p-\nu}$ is divisible by p^2 for all $\nu \leqslant p-2$. Hence, we have

$$\begin{aligned} x_1^p &\equiv (a+p)^p \equiv \sum_{\nu=0}^{p} a^\nu p^{p-\nu} \\ &\equiv \binom{p}{p-1} a^{p-1} \cdot p + a^p \equiv a^p \mod p^2 , \end{aligned}$$

since $\binom{p}{p-1} = p$. Recall that a is a pth residue modulo p^2. Using Theorem 11, Assertion (1), and $\varphi(p^2) = (p-1)p$, we obtain $a^{\varphi(p^2)/p} \equiv a^{p-1} \equiv 1 \bmod p^2$, where the latter step is due to Theorem 6. Consequently, $a^p \equiv a \bmod p^2$, and therefore $x_1^p \equiv a \bmod p^2$. So, Claim 1 is shown.

So, if $e = 2$ then the p solutions are $(x_1 + t \cdot p) \bmod p^2$ for $t = 0, \ldots, p-1$. We shall prove that these values are indeed solutions of $x^p \equiv a \bmod p^2$ below in more generality. If $e \geqslant 3$, we continue as follows:

We compute the modular inverse $c_{a,3}$ of a modulo p^3 and set

$$x_2 := (x_1 + x_1 (1 - x_1^p \cdot c_{a,3})/p) \mod p^3 .$$

Claim 2. x_2 *is a solution of* $x^p \equiv a \bmod p^3$.

Since $x_1^p \equiv a \bmod p^2$, we also know that $x_1^p \cdot c_{a,3} - 1 \equiv 0 \bmod p^2$. Consequently, we see that $(1 - x_1^p \cdot c_{a,3})/p \in \mathbb{Z}$.

Now, it suffices to show that $x_2^p \cdot c_{a,3} \equiv 1 \bmod p^3$. We obtain

$$\begin{aligned} x_2^p \cdot c_{a,3} &\equiv c_{a,3} \cdot (x_1 + x_1 (1 - x_1^p \cdot c_{a,3})/p)^p \\ &\equiv c_{a,3} \cdot x_1^p (1 + (1 - x_1^p \cdot c_{a,3})/p)^p \\ &\equiv c_{a,3} \cdot x_1^p \sum_{\nu=0}^{p} \binom{p}{\nu} ((1 - x_1^p \cdot c_{a,3})/p)^\nu \\ &\equiv x_1^p \cdot c_{a,3} \left(1 + \binom{p}{1} (1 - x_1^p \cdot c_{a,3})/p\right) \\ &\equiv x_1^p \cdot c_{a,3} + x_1^p \cdot c_{a,3} (1 - x_1^p \cdot c_{a,3}) \\ &\equiv x_1^p \cdot c_{a,3} - (1 - x_1^p \cdot c_{a,3} - 1)(1 - x_1^p \cdot c_{a,3}) \\ &\equiv x_1^p \cdot c_{a,3} + 1 - x_1^p \cdot c_{a,3} - (1 - x_1^p \cdot c_{a,3})^2 \\ &\equiv 1 \mod p^3 . \end{aligned}$$

Note that we used $p|\left((1-x_1^p\cdot c_{a,3})/p\right)$ in order to go from line 3 to line 4. Therefore, $\binom{p}{p-2}\left((1-x_1^p\cdot c_{a,3})/p\right)^2$ is divisible by p^3 and $\left((1-x_1^p\cdot c_{a,3})/p\right)^\nu$ is itself divisible by p^3 for all $\nu\geqslant 3$. The first part of the latter observation also shows that we cannot directly lift x_1 to a solution modulo p^4. Finally, in line 7 we used the fact that $x_1\cdot c_{a,3}-1\equiv 0 \bmod p^2$. Thus, Claim 2 is shown.

Consequently, if $e=3$ then we are done. We output $x_2+t\cdot p^2$ for $t=0,\ldots,p-1$.

If $e\geqslant 4$ then we use the following Algorithm LIFT4, which is a modification of Algorithm LIFT2. We denote the modular inverse of a modulo p^k by $c_{a,k}$. Analogously, we write $x_{0,0}$ for the initial solution x_0 and $x_{0,k}$ for the solution lifted to p^k. Note that we skip below the formulae for the computation of the modular inverse, since it is the same as in the Algorithm INV.

Algorithm LIFT4

Input. An odd prime p, a natural number $e\geqslant 3$, a pth residue $a\in\mathbb{Z}_p^*$, and an initial solution $x_1\in\mathbb{Z}_{p^3}^*$ of $x^p\equiv a \bmod p^3$.

Output. The $\varphi(p^e)/p$ solutions of $x^p\equiv b \bmod p^e$.

***Step* 1.** Initialize $d=2$ and $x_{0,2}=x_1$.

***Step* 2.** Compute the modular inverse $c_{a,2d}$ of a modulo p^{2d}. Then calculate

$$x_{0,2d} \;:=\; (x_{0,d}+x_{0,d}(1-x_{0,d}^p\cdot c_{a,2d})/p) \mod p^{2d}\ .$$

Set $d:=2d-1$, and iterate the construction until the exponent $2d$ reaches e. That means, from $x_{0,0}$ we calculate $x_{0,4} \bmod p^4$, then $x_{0,6} \bmod p^6$, a.s.o.

***Step* 3.** Let x_m be the last iterate computed. Output the following p solutions: $x_m \bmod p^e$, $\left(x_m+p^{e-1}\right) \bmod p^e$, $\left(x_m+2\cdot p^{e-1}\right) \bmod p^e$, …, $\left(x_m+(p-1)p^{e-1}\right) \bmod p^e$.

The correctness proof for x_m is *mutatis mutandis* the same as the proof of Claim 2, and the small modifications are done as in the demonstration of Theorem 19. We therefore omit it here.

It remains to show the correctness and completeness of the solutions output. Since for $e\geqslant 2$ we have $\gcd(\varphi(p^e),p)=p$, we conclude from Theorem 11 that there are always p solutions. So, it remains to show that the p solutions given are correct. Here we assume that $x_m \bmod p^e$ is a correct solution. Taking into account that $\binom{p}{p-1}=p$ and that $\left(p^{e-1}\right)^{p-\nu}$ is divisible by p^e for $\nu=0,\ldots,p-2$, we obtain for $\ell=1,\ldots,p-1$ that

$$\begin{aligned}\left(x_m+\ell\cdot p^{e-1}\right)^p &\equiv \sum_{\nu=0}^{p}\binom{p}{\nu}x_m^\nu\cdot\left(\ell\cdot p^{e-1}\right)^{p-\nu}\\ &\equiv x_m^p\equiv a \mod p^e\ ,\end{aligned}$$

and we are done.

Finally, the Algorithm LIFT4 requires mainly one modular exponentiation and the computation of a modular inverse. Hence, the algorithm is efficient provided that a and p^e have roughly the same number of bits. Furthermore, it is also efficient if $e \leqslant \max\{\log a, \log p\}$, since then p^e has at most $O\left(\max\{\log a, \log p\}^2\right)$ many bits. ∎

Some more remarks are mandatory here, and so we continue with them.

Remarks. As we mentioned above, the congruence $x^p \equiv a \bmod p$ possesses always precisely one solution. This is also directly implied by Theorem 11, Assertion (3), since $b = \gcd(p-1, p) = 1$ and $a^{p-1} \equiv 1 \bmod p$ for every $a \in \mathbb{Z}_p^*$.

On the other hand, if $e = 2$ then $\varphi(p^2) = (p-1)\cdot p$ (cf. Theorem 4). Consequently, now we know that there are precisely $p-1$ many pth residues in $\mathbb{Z}_{p^2}^*$. And for each of them there are precisely seven solutions. And if $e > 2$ then we always have seven solutions. Furthermore, since p itself does not possess a modular inverse in $\mathbb{Z}_{p^e}^*$ for all $e \geqslant 2$, we have do perform the division by p in our Algorithm LIFT4. This is the reason that we always take the solution modulo p^{e+1} and interpret it as a solution modulo p^e. This guarantees that the resulting quotient is always an integer. Furthermore, the example shows that it may be beneficial to perform the lifting steps with the smallest solution available.

Note that Theorem 21 generalizes to the case that $\gcd(p, q) = p$ but $q \neq p$, where p is any odd prime. Let us start with the case that $q = p^k$, where p is an odd prime and $k \in \mathbb{N}^+$, $k \geqslant 2$. The idea is to iterate the computation of the roots as described in the proof of Theorem 21. First, let $k = 2$; then we have to solve the congruence $z^{p^2} \equiv a \mod p^e$, where $e \in \mathbb{N}^+$.

The key observation is the following: Assume that a is a qth residue modulo p^e. This can be checked by using Theorem 11, Assertion (1). If a is a qth residue modulo p, we know that $a^{\varphi(p^e)/b} \equiv 1 \bmod p^e$, where $b = \gcd(\varphi(p^e), q)$. Now, recalling that $q = p^2$ we thus have $b = p^2$, since $q \neq p$. Hence, we obtain

$$1 \equiv 1^p \equiv \left(a^{\varphi(p^e)/p^2}\right)^p \equiv a^{\varphi(p^e)/p} ;$$

i.e., a is also a pth residue modulo p^e.

Consequently, we can use the algorithm presented in the proof of Theorem 21 and compute a solution x_0 of $x^p \equiv a \bmod p^e$. Thus, we know that $x_0 = \sqrt[p]{a}$. Now, we iterate the computation and solve $y^p \equiv x_0 \bmod p^e$. Therefore, for every solution y of $y^p \equiv x_0 \bmod p^e$ we know that $(y^p)^p \equiv a \bmod p^e$. Since there are p solutions of $x^p \equiv a \bmod p^e$, we obtain p^2 solutions of $z^{p^2} \equiv a \bmod p^e$, and Theorem 11 it telling us that we have found all possible solutions.

Now, it is easy to see that these ideas nicely generalize to the case that $q = p^k$, where $k \geqslant 2$. However, if we increment k and if e is larger, then the amount of the necessary computations grows exponentially in k.

Furthermore, the general case that $q = \ell \cdot p^k$, where $\gcd(\ell, p) = 1$ can be handled *mutatis mutandis*. Now, one has to take the ℓth root, and then we are back to the case that q is a power of p.

Finally, we provide an example.

Example 7. Let $a = 324$, let $q = 49$, let $p = 7$ and $e = 4$. The reader should verify that 324 is a 49th residue modulo 7^4. Using our algorithm from the proof of Theorem 21 we find $x_1 = 863$ and verify that $863^7 \equiv 324 \bmod 7^4$.

Next, we solve $y^7 \equiv 863 \bmod 7^4$ by using the same algorithm. So the solution modulo 7 is 2, the solution modulo 7^2 is 37, and then we obtain $c_{863,3} = 312$ and

$$y_{3,1} \;:=\; \left(37 + 37\left(1 - 37^7 \cdot 312\right)/7\right) \mod 7^3 \;=\; 156\,.$$

The final step yields $c_{863,4} = 1341$ and

$$y_{4,1} \;:=\; \left(156 + 156\left(1 - 156^7 \cdot 1341\right)/7\right) \mod 7^4 \;=\; 793\,.$$

A quick check shows that $793^{49} \equiv 324 \bmod 7^4$. The seven solutions obtained from 793 are thus

$$793,\ 1136,\ 1479,\ 1822,\ 2165,\ 107,\ 450\,.$$

Repeating the calculations for $x_2 := (863 + 7^3) \bmod 7^4 = 1206$ results in the seven solutions

$$842,\ 1185,\ 1528,\ 1871,\ 2214,\ 156,\ 499\,.$$

Next, we take $x_3 := (863 + 2 \cdot 7^3) \bmod 7^4 = 1549$, $x_4 = 1892$, $x_5 = 2235$, $x_6 = 177$, and $x_7 = 520$ in order to find the remaining 35 solutions, which are

$$\begin{aligned}
&1920,\ 2263,\ 205,\ 548,\ 891,\ 1234,\ 1577,\\
&1969,\ 2312,\ 254,\ 597,\ 940,\ 1283,\ 1626,\\
&2018,\ 2361,\ 303,\ 646,\ 989,\ 1332,\ 1675,\\
&2067,\ 9,\ 352,\ 695,\ 1038,\ 1381,\ 1724,\\
&744,\ 1087,\ 1430,\ 1773,\ 2116,\ 58,\ 401\,.
\end{aligned}$$

It should be noted that only the last lifting step has to be repeated in all these calculations. We leave it to the reader to figure out why this is so.

5. Conclusions and Open Problems

In this paper we have studied the problem to take discrete qth roots in the field $\mathbb{Z}_p$ and the ring $\mathbb{Z}_{p^e}$. In a first step we showed a generalization of the generalized Adleman, Manders, and Miller [1] algorithm, which solves this problem modulo p (cf. Algorithm

AMMG 1). Second, we generalized the obtained algorithm to solve the problem of taking discrete qth root directly in the ring $\mathbb{Z}_{p^e}$ resulting in the Algorithm AMMG 2.

The computational difficult part in these two algorithms is a discrete logarithm problem. The present algorithms solve this problem by computing the b-adic representation of the desired discrete logarithm digit-wise. Recall that $b = \gcd(p-1, q)$.

However, looking at the Congruence shown in (14) it is easy to see that we just have to find an $m \in \mathbb{N}^+$ such that $a^{q\ell-1} \cdot (\eta^t)^m \equiv 1 \bmod p$. This problem looks easier than the general strategy presented in the proof of Theorem 11 by at least two reasons. First, we do not need a generator, just a qth nonresidue η. Though we have choose randomly an element from $\mathbb{Z}_p^*$ until a qth residue is found, the advantage is the *verification* by using Assertion (1) of Theorem 11. As far as I am aware of, there is no comparable method to check whether or not an element from $\mathbb{Z}_p^*$ is a generator. Of course, these remarks directly apply to the Algorithm AMMG 2, too. So it would be nice to know whether or not improvements are possible, e.g., along the lines explored by Bernstein [3].

Furthermore, for several years I have been interested in lifting algorithms and have studied algorithms as presented in Section 4 and also some that allowed for a lifting an element given modulo p to a corresponding element modulo p^e (cf. Zeugmann [26, 27]). The lifting algorithms obtained are well-suited for parallel computations provided p and e are bounded by n^c, c constant, where n is the number of bits of the remaining inputs. Note that all these algorithms strictly avoid modular exponentiation.

On the other hand, the lifting algorithms included in Algorithm Tonelli 2, presented as Tonelli's [24] lifting in Section 4.3, and included in the Algorithm AMMG 2, all use modular exponentiation to achieve the lifting. This indicates the strength and usefulness of modular exponentiation. On the other hand, so far I am not aware of any optimal or close to optimal parallel modular exponentiation algorithm.

References

[1] Leonard Adleman, Kenneth Manders, and Gary Miller. On taking roots in finite fields. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science, Providence, Rhode Island, 31 October - 1 November 1977*, pages 175–178. IEEE Computer Society Press, 1977.

[2] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Volume 1: Efficient Algorithms*. The MIT Press, MIT, Cambridge, Massachussetts, 1996.

[3] Daniel J. Bernstein. Faster square roots in annyoing finite fields. Technical report, available from `http://cr.yp.to/papers/sqroot.pdf`, 2001.

[4] Zhengjun Cao, Qian Sha, and Xiao Fan. Adleman–Manders–Miller root extraction method revisited. In Chuan-Kun Wu, Moti Yung, and Dongdai Lin,

editors, *Information Security and Cryptology, 7th International Conference, Inscrypt 2011, Beijing, China, November 30 – December 3, 2011. Revised Selected Papers*, volume 7537 of *Lecture Notes in Computer Science*, pages 77–85, Berlin, Heidelberg, 2012. Springer.

[5] Michele Cipolla. Un metodo per la risoluzione della congruenza di secondo grado. *Rendiconto dell'Accademia delle Scienze Fisiche e Matematiche Napoli*, 9:154–163, 1903.

[6] Leonard Eugene Dickson. *History of the Theory of Numbers*, volume 1. Carnegie Institution of Washington, Washington, 1919.

[7] Leonhard Euler. Theoremata arithmetica nova methodo demonstrata. *Novi commentarii academiae scientiarum imperialis Petropolitanae*, 8:74–104, 1763.

[8] Joachim von zur Gathen. Computing powers in parallel. *SIAM Journal on Computing*, 16(5):930–945, 1987.

[9] Carl Friedrich Gauss. *Disquisitiones Arithmeticae*. Springer-Verlag, Berlin, Heidelberg, New York, (translated by Arthur A. Clarke), English edition, 1966.

[10] Helmut Hasse. *Number Theory*, volume 229 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, New York, Berlin, Heidelberg, 1980.

[11] Kurt Hensel. *Theorie der algebraischen Zahlen*. Druck und Verlag von B.G. Teubner, Leipzig und Berlin, 1908.

[12] Anna M. Johnston. A generalized q^{th} root algorithm. In Robert Endre Tarjan and Tandy J. Warnow, editors, *Proceedings of the Tenth Annual ACM-SIAM Symposium on Discrete Algorithms, 17-19 January 1999, Baltimore, Maryland, USA.*, pages 929–930, Philadelphia, PA, USA, 1999. Society for Industrial and Applied Mathematics.

[13] Donald E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, third edition, 1998.

[14] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 1994.

[15] Joseph-Louis Lagrange. Sur la solution des problèmes indéterminés du second degré. In *Œuvres complètes*, volume 2, pages 377–535. Gauthier-Villars, Paris, 1868. originally published in Mémoires de l'Académie Royale des Sciences et Belles-lettres de Berlin, tome XXIII, 1769.

[16] Gabriel Lamé. Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers. *Comptes rendus des séances du l'Académie des Sciences*, 19:867–870, 1844.

[17] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Inc., 1996.

[18] Nozomu Nishihara, Ryuichi Harasawa, Yutaka Sueyoshi, and Aichi Kudo. A remark on the computation of cube roots in finite fields. Technical Report Report 2009/457, IACR Cryptology ePrint Archive, 2013.

[19] Peter Roquette. History of valuation theory. In Franz-Viktor Kuhlmann, Salma Kuhlmann, and Murray Marshall, editors, *Valuation Theory and Its Applications, Volume I*, Fields Institute Communications, The Fields Institute for Mathematical Sciences, pages 291–355. American Mathematical Society, 2002.

[20] Peter Schreiber. A supplement to J. Shallit's paper "Origins of the analysis of the Euclidean algorithm". *Historia Mathematica*, 22(4):422–424, 1995.

[21] Jeffrey Shallit. Origins of the analysis of the Euclidean algorithm. *Historia Mathematica*, 21(4):401–419, 1994.

[22] Daniel Shanks. Five number theoretic algorithms. In Robert S. D. Thomas and Hugh C. Williams, editors, *Proceedings of the Second Manitoba Conference on Numerical Mathematics, October 5-7, 1972*, pages 51–70, Winnipeg, 1973. Utilitas Mathematica Pub.

[23] Paul Tannery and Charles Henry, editors. *Oeuvres de Fermat, Tome Deuxième: Correspondance*. Gauthier-Villars et fils, Paris, 1894.

[24] Alberto Tonelli. Bemerkung über die Auflösung quadratischer Congruenzen. *Nachrichten von der Königlichen Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen*, 1891(10):344–346, 1891.

[25] A. Tonelli. Sulla risoluzione della congruenza $x^2 \equiv c \bmod p^\lambda$. *Atti Della Reale Accademia Dei Lincei, Rendiconti*, 5(1):116–120, 1892.

[26] Thomas Zeugmann. Improved parallel computations in the ring $\mathbb{Z}_{/p^\alpha}$. *Elektronische Informationsverarbeitung und Kybernetik*, 25:543–547, 1989.

[27] Thomas Zeugmann. Highly parallel computations modulo a number having only small prime factors. *Information and Computation*, 96(1):95–114, 1992.