QUADRATIC MAPS AS DYNAMICAL SYSTEMS ON THE P-ADIC NUMBERS

MONICA NEVINS AND THOMAS D. ROGERS

ABSTRACT. We describe the trajectories of the successive iterates of the square map and its perturbations on the field of p-adic numbers. We show that the cycles of the square map on $\mathbb{Q}_p$ arise from cycles of the square map on $\mathbb{F}_p$, and that all nonperiodic trajectories in the unit disk densely define a compact open subset. We find that the maps $x \mapsto x^2 + \varepsilon$, with ε inside the unit circle, have similar dynamics to $x \mapsto x^2$, but that each fundamental cycle arising from $\mathbb{F}_p$ can further admit harmonic cycles, for different choices of p and ε. In contrast, the cycles of the maps $x \mapsto x^2 + \varepsilon$, with ε on the boundary of the unit circle, are no longer tied to those of the square map itself. In all cases we give a refined algorithm for computing the finitely many periodic points of the map.

1. INTRODUCTION

We are interested in dynamics over the p-adic fields $\mathbb{Q}_p$, for p a prime. Our starting point in this study — inspired by the development of the corresponding problem on the real and complex numbers over the past 30 years — is the analysis of the dynamics of the algebraically simplest of nonlinear systems, namely, the family of quadratic maps $f_\varepsilon(x) = x^2 + \varepsilon$ for $|\varepsilon|_p \leq 1$. In this paper, we give a complete global description of the trajectories of elements $x \in \mathbb{Q}_p$ under the iterates of f_ε.

Denote the norm on $\mathbb{Q}_p$ by $|\cdot|_p$ (*cf.* Section 2) and write $f_\varepsilon^k = f_\varepsilon \circ \cdots \circ f_\varepsilon$ (k times) for the kth iterate of f_ε. Our main result is the following (Theorems 3.4 and 4.3).

Theorem. *Let $f_\varepsilon \colon \mathbb{Q}_p \to \mathbb{Q}_p$ be given by $f_\varepsilon(x) = x^2 + \varepsilon$, with $|\varepsilon|_p < 1$ (including $\varepsilon = 0$). Then f_ε admits exactly two fixed points $\delta_{p,\varepsilon}$ and $\mu_{p,\varepsilon}$, with $|\delta_{p,\varepsilon}|_p = |\mu_{p,\varepsilon} - 1|_p = |\varepsilon|_p$. If $x \in \mathbb{Q}_p$ satisfies $|x|_p > 1$, then the trajectory of $f_\varepsilon^k(x)$, $k = 0, 1, 2, \ldots$, diverges to infinity; whereas if $|x|_p < 1$, the trajectory converges to $\delta_{p,\varepsilon}$. If $p = 2$, then the trajectory of every x on the unit circle $|x|_p = 1$ converges to $\mu_{p,\varepsilon}$. For any other prime p, if $|x|_p = 1$, then x is either a periodic point, or its trajectory is eventually quasiperiodic. Further, there are only finitely many periodic points, and we give an algorithm to compute them (in all but a few "nongeneric" cases).*

In particular, one finds that the domains of attraction in $\mathbb{Q}_p$ are easily defined. See Definition 3.3 for the notion of quasiperiodicity. When $\varepsilon = 0$, the fixed points are evidently $\delta_{p,\varepsilon} = 0$ and $\mu_{p,\varepsilon} = 1$.

We actually prove a far more precise result about the structure of the orbit space, as encapsulated in the pseudo-algorithm found in Part F of the proof of Theorem 4.3. In particular, we prove that each cycle of the square map $x \mapsto x^2$ on the finite field with p elements $\mathbb{F}_p$ gives rise to a so-called *fundamental cycle* of $f = f_0$ on $\mathbb{Q}_p$ of equal (primitive) period, and that these are the *only* finite orbits of the square map on $\mathbb{Q}_p$. When we consider instead the trajectories of those maps f_ε on $\mathbb{Q}_p$ with $|\varepsilon|_p < 1$ and $\varepsilon \neq 0$, we find, for all but some "exceptional primes" (*cf.* Table 6.1), corresponding fundamental cycles; furthermore, when $|\varepsilon|_p < 1$, these fundamental cycles may (as p and ε vary) admit additional *harmonics*. Here we define a harmonic cycle to be a finite orbit $\mathcal{H}$

Date: March 22, 2000.

The first named author is supported by the Killam Trust.

of f_ε whose period is a multiple of that of the corresponding fundamental cycle $\mathcal{F}$ (and a multiple of the order of 2 modulo p) and whose elements share leading coefficients with elements of $\mathcal{F}$. We apply a general theorem of Pezda [Pe] (see Theorem 4.1), to deduce the maximum possible length of a harmonic cycle of f_ε. Finally, we use a generalization of a result of Thiran, Verstegen and Weyers in [TVW] to identify some maps f_ε and fundamental cycles $\mathcal{F}$ which admit no harmonics at all.

The paper is organized as follows. In Section 2, we set our notation and review basic facts about the p-adic numbers, including Hensel's Lemma and the definition of the exponential map in a p-adic field. In Section 3 we use these ideas to analyse the dynamics of the square map $f(x) = x^2$, with a view towards the general case. The analysis culminates, in Section 4, with a description of the trajectories of $f_\varepsilon(x) = x^2 + \varepsilon$, for $|\varepsilon|_p < 1$. In Section 5, we give a brief summary of the possible dynamics of the "boundary" case $f_\varepsilon(x) = x^2 + \varepsilon$, with $|\varepsilon|_p = 1$, and describe how our analysis may be applied to compute cycles of these maps. Finally, in Section 6, we discuss some of the (possibly open) questions raised by our analysis, including the dynamics of f_ε on $\mathbb{Q}_p$ for an exceptional prime p. We also discuss the existence of the nongeneric cases of our algorithm, which firmly resist the application of either Hensel's lemma or the limiting result of [TVW].

There are a number of papers on related questions of dynamics of polynomial maps, and quadratic maps in particular. In particular, the paper [TVW] of Thiran, Verstegen and Weyers (and, closely related, the earlier, but unpublished paper [B] of Ben-Menahem) provide significant forays into the dynamics of quadratic maps on $\mathbb{Q}_p$. In [TVW], they prove that f_a, with $|a|_p > 1$, exhibits chaotic behaviour, and also consider some examples of the dynamics of f_ε, $|\varepsilon|_p \leq 1$. Where our paper overlaps with theirs, ours is both more general and contains more complete proofs.

In [TVW] it is proven that f_ε is topologically conjugate to a linear map in a certain neighbourhood of an "indifferent" fixed point (and hence that f_ε is quasiperiodic in that neighbourhood), and point out that the result can be generalized to a properly defined indifferent (or neutral) cycle. It is this generalization that we use in our analysis (although we do not include the proof).

Finally, note that [TVW] discusses the quasiperiodicity of f_ε in general as well, using the argument in the appendix of [B]. Our proof of quasiperiodicity is quite different, and much simpler, taking advantage of our restrictions on ε.

Other important papers which consider quadratic maps of the form $x \mapsto x^2 + a$ (over number fields as well as p-adic fields) include [Mo], [Na], [Si], and [WR]. An analysis of techniques which apply to a broad class of p-adic analytic maps is studied by Lubin in [L]. In particular, he defines notions of unipotency and instability which bear close relation to the nongeneric cases of our algorithm. Also, he introduces the "Lie logarithm" as a linearization tool, and as such it suggests that it might be possible to derive a far more general analysis of linearity near periodic points than that presented in [TVW].

Last, but certainly not least, is a deep paper of Pezda [Pe], in which he proves an upper bound for the possible periods of cycles of polynomial maps with coefficients in the unit circle of $\mathbb{Q}_p$ (or indeed in the integer ring of any algebraic number field). Pezda's paper seems fundamental to the generalization of our results to other polynomial mappings, or to algebraic extensions of the fields $\mathbb{Q}_p$ — a topic which the authors hope to return to in a subsequent paper.

2. p-adic Numbers

Let p be a prime number. If $n \in \mathbb{Z}^*$ is a nonzero integer, then its p-adic valuation, denoted $\mathrm{val}(n)$, is the largest integral power of p dividing n. Extend this valuation to all rational numbers $m/n \in \mathbb{Q}$ by setting $\mathrm{val}(m/n) = \mathrm{val}(m) - \mathrm{val}(n)$ if $m \neq 0$ and $\mathrm{val}(0) = \infty$. Then the p-adic norm

is defined by

$$|x|_p = p^{-\mathrm{val}(x)}$$

for any $x \in \mathbb{Q}$. This norm is nonarchimedean, meaning that we have in place of the triangle inequality the relation $|x+y|_p \leq min\{|x|_p, |y|_p\}$. Consequently (and in stark contrast to the euclidean norm), the p-adic norm does not permit the accumulation of error, in the sense that, if each of k elements $\{x_1, x_2, \ldots, x_k\}$ have p-adic norm at most ϵ, then $|x_1 + x_2 + \cdots + x_k|_p \leq \epsilon$ as well. This property justifies our extensive use of modular arithmetic in Sections 3 and 4.

Completing the field of rational numbers with respect to this norm yields the field of p-adic numbers, denoted $\mathbb{Q}_p$. A concrete realization of $\mathbb{Q}_p$ is as the set of all formal Laurent series in p with coefficients in the set $\{0, 1, 2, \ldots, p-1\}$:

$$\mathbb{Q}_p = \{x = \sum_{n=N}^{\infty} a_n p^n \mid N \in \mathbb{Z},\ a_n \in \{0, 1, 2, \ldots, p-1\}\ , a_N \neq 0\},$$

with addition and multiplication performed by starting at the lowest power of p, and "carrying" successively higher powers of p. (Thus, for example, $-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots$.) For $x \in \mathbb{Q}_p$ as above, $|x|_p = p^{-N}$. Two p-adic numbers are thus "close" with respect to the norm if their coefficients a_n agree for all $n < M$, for some "large" M. In this sense, the norm on $\mathbb{Q}_p$ is equivalent to that conventionally used in symbolic dynamics [D], that is, maps on sequence spaces (which traditionally carry no algebraic structure). [1]

The field $\mathbb{Q}_p$ is unordered and, since it contains $\mathbb{Q}$ as a subfield, has characteristic 0. Moreover, in this topology, $\mathbb{Q}$ is a dense, proper subset of $\mathbb{Q}_p$; $\mathbb{Q}$ embeds into $\mathbb{Q}_p$ as the set of elements whose p-adic coefficients are eventually periodic (much in the same way that $\mathbb{Q}$ embeds into $\mathbb{R}$).

The distinguished subring of $\mathbb{Q}_p$ defined by $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$ is called the *integer ring*. It is an integral domain. The set of invertible elements in $\mathbb{Z}_p$, called the *group of units* and denoted $\mathbb{Z}_p^*$, consists of those elements of $\mathbb{Z}_p$ for which $a_0 \neq 0$. The ring $\mathbb{Z}_p$ contains a unique maximal ideal $p\mathbb{Z}_p = \{x \in \mathbb{Z}_p \mid |x|_p < 1\}$, the set-theoretic complement of $\mathbb{Z}_p^*$. The quotient of $\mathbb{Z}_p$ by its maximal ideal gives a field, which we identify with the finite field of p elements $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ in the obvious way. (Similarly, we can identify $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$ for any positive integer n.) In this context, we call $\mathbb{F}_p$ the *residue field* (or *residue class field*) of $\mathbb{Q}_p$.

Topologically, $\mathbb{Q}_p$ is a Cantor set: totally disconnected but not discrete. Moreover, if two open balls (with respect to the p-adic norm) in $\mathbb{Q}_p$ intersect, then one must contain the other. Algebraically, the p-adics are also full of holes: there is no finite field extension of $\mathbb{Q}_p$ which is algebraically closed. Not surprising, therefore, is the sparseness of the set of periodic points under f_ε in $\mathbb{Q}_p$.

Nevertheless, finding roots of polynomials in $\mathbb{Q}_p$ is often quite simple, with the help of Hensel's Lemma.

Theorem 2.1 (Hensel's Lemma). *Suppose $g(x)$ is a polynomial with coefficients in $\mathbb{Z}_p$. If $a \in \mathbb{Z}_p$ is an approximate root of g in the sense that*

$$g(a) \equiv 0 \mod p^{2m+1}, \qquad \textit{where } m = val(g'(a))$$

and $g'(a) \neq 0$, then there is a unique root b of g near a in the sense that

$$g(b) = 0 \qquad \textit{and} \qquad b \equiv a \mod p^{m+1}.$$

[1] Another algebraic structure on this set can be imposed via component-wise addition mod p (that is, identifying it with the field $\mathbb{F}_p((t))$ of formal Laurent series in an indeterminate t); this has been considered in, for example, [SR1] and [SR2].

Remark 2.2. In the special case where $g'(a)$ has a *constant* leading term (so $\mathrm{val}(g'(a)) = 0$), Hensel's Lemma implies that it suffices to solve the polynomial equation in the residue field $\mathbb{F}_p$ in order to ensure the existence of a solution in $\mathbb{Z}_p$.

Hensel's Lemma is well-known and true in the more general setting of local rings; see, for example, [E, Thm.7.3]. We will make use of a slight extension of Hensel's Lemma, as follows:

Theorem 2.3. *Suppose $g(x)$ is a polynomial with coefficients in $\mathbb{Z}_p$, $p \neq 2$. If $a \in \mathbb{Z}_p$ is an approximate root of g in the sense that*

$$g(a) \equiv 0 \mod p^{2r+1}, \qquad \text{where } r \geq val(g'(a))$$

and $g'(a) \neq 0$, then there is a unique root b of g near a in the sense that

$$g(b) = 0 \qquad \text{and} \qquad b \equiv a \mod p^R,$$

where $R = r+1$ if $r = val(g'(a))$ and $R = 2r - val(g'(a))$ if $r > val(g'(a))$.

Proof. The existence and uniqueness of the root b of g is given by Hensel's Lemma; what remains in question is the accuracy to which the approximate root a estimates b, when $r > \mathrm{val}(g'(a)) = m$. Consider Taylor's expansion of the polynomial g:

$$g(b) = g(a+h) = g(a) + hg'(a) + \frac{1}{2}h^2 g''(a) + O(h^3).$$

By Hensel's Lemma, $\mathrm{val}(h) \geq m+2$. Suppose $\mathrm{val}(h) = k < 2r+1-m$; then as $\mathrm{val}(g(a)) \geq 2r+1$ and $\mathrm{val}(\frac{1}{2}h^2 g''(a)) \geq 2k$ (and all other terms have valuation at least $3k-1$, even accounting for $\mathrm{val}(\frac{1}{n!})$), we deduce that the only term with valuation less than $m+k+1$ is $hg'(a)$. But as $g(a+h) = 0$, and $\mathrm{val}(g'(a)) = m$, we must have $\mathrm{val}(h) > k$. □

We remark that the stated existence is not merely abstract — one can explicitly compute the solution b to any desired precision. As a particular and important example, consider the polynomial $g(x) = x^{p-1} - 1$. Then $g'(x) = (p-1)x^{p-2}$, so $|g'(x)|_p = |p-1|_p \, |x|_p^{p-2} = |x|_p^{p-2}$. Thus, for any $a \in \mathbb{Z}_p^*$, we have $g'(a) \in \mathbb{Z}_p^*$. It follows by Remark 2.2 that we should look for roots a of g in the residue field $\mathbb{F}_p$. Since, by Fermat's Little Theorem, every $a \in \{1, 2, 3, \ldots, p-1\}$ satisfies the equation $g(a) \equiv 0 \mod p$, we deduce by Hensel's Lemma that each a gives rise to a unique root $\sigma_a \in \mathbb{Z}_p$ of g with constant term equal to a.

Example. Let $p = 3$, so that $g(x) = x^2 - 1$. First let $a = 1$. As $a^2 = 1$ in $\mathbb{Z}_3$, it is already a root; so $\sigma_1 = 1$. Now let $a = 2$, which is no longer an exact root. By Hensel's Lemma, we know that σ_2 takes the form $\sigma_2 = 2 + b'p + b''p^2 + \cdots$ and satisfies $\sigma_2^2 = 1$. We compute:

$$\begin{aligned} \sigma_2^2 - 1 &\equiv (2+b'p)^2 - 1 \mod p^2 \\ &\equiv 2^2 + 2(2)(b'p) + (b'p)^2 - 1 \mod p^2 \\ &\equiv (1+p) + (1+p)(b'p) + b'^2 p^2 - 1 \mod p^2 \\ &\equiv (1+b')p \mod p^2. \end{aligned}$$

Setting this last equal to 0 (modulo p^2) yields $b' = 2$. We continue in this way and eventually find

$$\sigma_2 = 2 + 2p + 2p^2 + 2p^3 + \cdots = -1,$$

as expected. □

The roots of the polynomial $f(x) = x^{p-1} - 1$ are called the *Teichmüller representatives* of $\{1, 2, \ldots, p-1\}$. Together with 0, they give another canonical choice of representatives in $\mathbb{Z}_p$ of the conjugacy classes of $p\mathbb{Z}_p$ in $\mathbb{Z}_p$. The advantage of this choice is that the elements $\{\sigma_1, \sigma_2, \ldots, \sigma_{p-1}\}$ form a group under multiplication (isomorphic to $\mathbb{F}_p^*$) in $\mathbb{Q}_p$. We will make use of these in Section 3.

Another tool we would like to introduce now for use in Section 3 is the p-adic exponential map, as defined by its Taylor series

$$\exp(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots .$$

Recall that over the real numbers, exp is everywhere-convergent, and gives a bijection of $\mathbb{R}$ with $\mathbb{R}_+$, the positive real line. A moment's thought reveals that the exponential map cannot be nearly so well-behaved in $\mathbb{Q}_p$: if $x = p^{-1}$, for example, then each successive partial sum of $\exp(x)$ has *strictly increasing* norm and hence the series cannot converge in $\mathbb{Q}_p$. Moreover, $|(n!)^{-1}|_p$ itself increases with n, so it is not *a priori* clear that one can choose x small enough to compensate. Nevertheless, using the fact that in $\mathbb{Q}_p$, a series converges if and only if its terms tend to 0, we have the following well-known theorem, proven, for example, in [K, IV.1.].

Theorem 2.4. *The functions* exp *and* $\log(1+x) = x + \frac{1}{2}x + \frac{1}{3}x^2 + \cdots$ *give mutually inverse isomorphisms (and homeomorphisms) between the multiplicative group* $1 + p^n\mathbb{Z}_p$ *and the additive group* $p^n\mathbb{Z}_p$*, for any* $n \geq 1$ *if* p *is odd, and* $n \geq 2$ *if* $p = 2$.

For more detail on the p-adic numbers — their arithmetic, their algebra, or their topology — see, for example, [S] or [K].

3. The Square Map on $\mathbb{Q}_p$

In this section we study the iterates of the square map $f(x) = x^2$ on $\mathbb{Q}_p$ (or $\mathbb{Q}_p^*$). Let us first treat the special (and simple) case of $p = 2$ before proceeding to $p > 2$, which analysis forms the bulk of this section.

Suppose $p = 2$. We can construct a group isomorphism

$$\phi\colon \mathbb{Z} \times \{\pm 1\} \times 2^2\mathbb{Z}_2 \to \mathbb{Q}_2^* \tag{3.1}$$

given by $\phi(n, \epsilon, x) = p^n \epsilon \exp(x)$. Giving $\mathbb{Z}$ and the finite group the discrete topology, and $2^2\mathbb{Z}_2$ the topology it inherits as a subset of $\mathbb{Z}_2$, ϕ becomes a homeomorphism as well. Following the commutative diagram

$$\begin{array}{ccc} \mathbb{Q}_2^* & \xrightarrow{f} & \mathbb{Q}_2^* \\ \uparrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \phi} \\ \mathbb{Z} \times \{\pm 1\} \times 2^2\mathbb{Z}_2 & \xrightarrow{g_1 \otimes g_2 \otimes g_3} & \mathbb{Z} \times \{\pm 1\} \times 2^2\mathbb{Z}_2 \end{array}$$

we see that the square map is conjugate to $\phi^{-1} \circ f \circ \phi = g_1 \otimes g_2 \otimes g_3$, where $g_1\colon \mathbb{Z} \to \mathbb{Z}$ and $g_3\colon 2^2\mathbb{Z}_2 \to 2^2\mathbb{Z}_2$ are given by multiplication by 2, and g_2 is the trivial map $g_2(\epsilon) = 1$ for $\epsilon \in \{\pm 1\}$. Note that none of maps g_i, $i = 1, 2, 3$ are surjective; in particular, the image of g_3 is $2^3\mathbb{Z}_2 \subset 2^2\mathbb{Z}_2$, and each successive iterate of g_3 shrinks this set even more. Thus, regardless of the values of $\epsilon \in \{\pm 1\}$ and $x \in 2\mathbb{Z}_2$, we have

$$\lim_{t\to\infty} \phi(g_1^t(n), g_2^t(\epsilon), g_3^t(x)) = \begin{cases} \infty & \text{if } n > 0, \\ 0 & \text{if } n < 0, \\ 1 & \text{if } n = 0. \end{cases}$$

Hence, 0 and 1 are attractive fixed points, with domains of attraction $2\mathbb{Z}_2$ and $1+2\mathbb{Z}_2$, respectively. All remaining elements of $\mathbb{Q}_2$ have p-adic norm greater than 1, and their trajectories diverge to infinity. There are consequently no dense trajectories of f on $\mathbb{Q}_2$, and no periodic points save the fixed points 0 and 1.

The dynamics of f on $\mathbb{Q}_p$, for $p > 2$, are far more interesting.

Suppose for the remainder of this section that p is odd. We consider the well-known isomorphism of groups and homeomorphism of topological spaces (*cf.* 3.1)

$$\phi\colon \mathbb{Z} \times \mathbb{F}_p^* \times p\mathbb{Z}_p \to \mathbb{Q}_p^*, \tag{3.2}$$

given by $\phi(n, a, x) = p^n \sigma_a \exp(x)$, where again σ refers to the Teichmüller representatives in $\mathbb{Z}_p$. Following the commutative diagram

$$\begin{array}{ccc} \mathbb{Q}_p^* & \xrightarrow{\ f\ } & \mathbb{Q}_p^* \\ \uparrow{\scriptstyle \phi} & & \uparrow{\scriptstyle \phi} \\ \mathbb{Z} \times \mathbb{F}_p^* \times p\mathbb{Z}_p & \xrightarrow{g_1 \otimes g_2 \otimes g_3} & \mathbb{Z} \times \mathbb{F}_p^* \times p\mathbb{Z}_p \end{array}$$

we see that the square map $f(x) = x^2$ is conjugate to $\phi^{-1} \circ f \circ \phi = g_1 \otimes g_2 \otimes g_3$, where $g_1\colon \mathbb{Z} \to \mathbb{Z}$ and $g_3\colon p\mathbb{Z}_p \to p\mathbb{Z}_p$ are given by multiplication by 2, and g_2 is the square map $g_2(x) = x^2$ on $\mathbb{F}_p^*$. While the first two maps are linear, and do not give rise to periodic orbits, the map g_2 does admit a complex orbit structure. The Decomposition Theorem of [R], applied to the cyclic group $\mathbb{F}_p^*$, allows us to deduce the orbit picture of the map $g_2(x) = x^2$, as follows.

For each odd divisor d of $p-1$, let $\mathrm{ord}_d 2$ denote the order of 2 modulo d, and $\varphi(d)$ the Euler phi function at d. (So $\varphi(d)$ is the number of numbers less than d relatively prime to d.) Set $\mathrm{ord}_1 2 = 1$. Then there are $\varphi(d)/\mathrm{ord}_d 2$ cycles of period $\mathrm{ord}_d 2$, for each distinct d. Furthermore, for any $x \in \mathbb{F}_p^*$ which is not itself a periodic point of g_2, the iterate $g_2^k(x)$ *is* periodic, where k is chosen such that 2^k is the largest even divisor of $p-1$.

Hence, passing back to $\mathbb{Q}_p$ via the isomorphism (3.2), we deduce that all periodic orbits of f on $\mathbb{Q}_p$ lie in the finite subgroup of the Teichmüller representatives, and that further the orbit structure of f admits an explicit description for all p.

For the remainder of this section, let us give a full account of the quasiperiodic (*cf.* Definition 3.3) behaviour of the doubling map g_3. We are motivated in part by practical considerations; in applications, the inevitable finiteness of storage space requires us to consider the "truncated" p-adics $\mathbb{Q}_p$ modulo $p^n\mathbb{Z}_p$, for various degrees of precision n. (As mentioned in Section 2, *no* artifacts or errors are introduced in doing so.) Thus it is important to understand the dynamics on this set.

To this end, let us consider the action of $g_3(x) = 2x$ on the *strata* of $\mathbb{Q}_p$, that is, on the open sets of the form $p^r\mathbb{Z}_p^*$ (or, equally, their images in $\mathbb{Q}_p$ modulo $p^n\mathbb{Z}_p$ for any $n \geq r$).

First, identify the space $p\mathbb{Z}_p/p^2\mathbb{Z}_p$ with $\mathbb{F}_p$, the finite field with p elements. The element 0 is fixed by multiplication by 2. The orbit of the doubling map through an element $a \in \mathbb{F}_p^*$ is

$$\mathcal{O} = \{a, 2a, 2^2a, 2^3a, \ldots 2^{n-1}a\},$$

where n is the order of 2 modulo p. It follows that $p\mathbb{Z}_p/p^2\mathbb{Z}_p$ decomposes under g_3 into $(p-1)/n$ cyclic orbits of period n, and one fixed point. Case-by-case computation for the odd primes $p < 100$ yields the data in Table 3.1.

We would next like to understand the structure of the orbits of the doubling map g_3 on $p\mathbb{Z}_p/p^{k+1}\mathbb{Z}_p$ (which we naturally identify with $\mathbb{Z}_p/p^k\mathbb{Z}_p \simeq \mathbb{Z}/p^k\mathbb{Z}$ via division by p) for $k \geq 2$.

Proposition 3.1. *Let p be an odd prime, and let n be the order of 2 in $\mathbb{Z}/p\mathbb{Z}$. If $val(2^n - 1) = r$, then the order of 2 in $\mathbb{Z}/p^k\mathbb{Z}$ is n if $k \leq r$ and np^{k-r} if $k > r$. Consequently, the possible periods of cycles of the square map $f(x) = x^2$ on sets of the form $\mathbb{Z}_p/p^s\mathbb{Z}_p$ ($s \geq 1$) are:*

$$\{c, lcm(n,c)p^{k-r} \mid 0 \leq k < s - r,\ c = 1 \text{ or } c = ord_d 2 \text{ for some odd divisor } d \text{ of } p-1\},$$

p	$\mathrm{ord}_p 2 = n$	# cycles $= (p-1)/n$	p	$\mathrm{ord}_p 2 = n$	# cycles $= (p-1)/n$	p	$\mathrm{ord}_p 2 = n$	# cycles $= (p-1)/n$
3	2	1	29	28	1	61	60	1
5	4	1	31	5	4	67	66	1
7	3	2	37	36	1	71	35	2
11	10	1	41	20	2	73	9	8
13	12	1	43	14	3	79	39	2
17	8	2	47	23	2	83	82	1
19	18	1	53	52	1	89	11	8
23	11	2	59	58	1	97	48	2

TABLE 3.1. Primes p, the order of 2 modulo p, and the number of cycles of the doubling map on $\mathbb{F}_p^*$.

where $lcm(n, c)$ is the least common integer multiple of n and c.

Proof. The case of $k \leq r$ is obvious, so let $k > r$ and proceed by induction on k. Suppose we have proven that the order of 2 in $\mathbb{Z}/p^{k-1}\mathbb{Z}$ is np^{k-r-1}, and that $\mathrm{val}(2^{np^{k-r-1}} - 1) = k - 1$. Let m denote the order of 2 in $\mathbb{Z}/p^k\mathbb{Z}$. Then in particular, $2^m \equiv 1 \mod p^{k-1}$, so there exists a positive integer s such that $m = s(np^{k-r-1})$. Write

$$2^{np^{k-r-1}} \equiv 1 + ap^{k-1} \mod p^k,$$

with $a \neq 0$ by hypothesis. We apply the binomial expansion

$$(1 + ap^{k-1})^s = 1 + sap^{k-1} + \frac{s(s-1)}{2}a^2p^{2(k-1)} + \cdots$$

and note that all but the first two terms have valuation at least k. Hence $2^m = (2^{np^{k-r-1}})^s \equiv 1 \mod p^k$ if and only if $sa \equiv 0 \mod p$. Thus by the minimality of m we deduce that $s = p$. In other words, the order of 2 in $\mathbb{Z}/p^k\mathbb{Z}$ is np^{k-r} and the valuation of $(2^{np^{k-r}} - 1)$ in $\mathbb{Z}_p$ is exactly k.

Now consider the possible periods of cycles of the square map on $\mathbb{Z}_p/p^s\mathbb{Z}_p$. We have already remarked that there are exact cycles of period c in the set of Teichmüller representatives. Furthermore, any approximate cycles of g_3 on the stratum $p\mathbb{Z}_p/p^s\mathbb{Z}_p$ exponentiate to give approximate cycles (of the same periods) of the square map on $1 + p\mathbb{Z}_p/p^s\mathbb{Z}_p$. Now $p\mathbb{Z}_p/p^s\mathbb{Z}_p$ contains the strata

$$p^k\mathbb{Z}_p/p^s\mathbb{Z}_p \simeq \mathbb{Z}_p/p^{s-k}\mathbb{Z}_p$$

for each $k \in \{1, 2, \ldots s\}$; g_3 preserves these strata, leaving cycles of period equal to the order of 2 modulo p^{s-k}. Reconstructing the full map $f(x) = x^2$ via the isomorphism (3.2) yields the desired result. □

Remark 3.2. Those primes p for which the value of r in Proposition 3.1 is strictly greater than 1 are called *Wieferich primes*. To date, extensive search (see [CDP], for example) has revealed only two Wieferich primes — 1093 and 3511 — and each of these gives only $r = 2$. Nevertheless, there is as yet no indication that these are the only such, and in fact it seems possible that there be infinitely many Wieferich primes!

Let us now proceed to give a "global picture" of the orbit space of the square map on $\mathbb{Q}_p$, for p odd. By this we mean an understanding of the behaviour of the trajectory of any point $x_0 \in \mathbb{Q}_p$ under repeated applications of the square map. Use the notation $x_1 = x_0^2$, $x_2 = x_1^2$, ..., and x_t for the t-th iterate of x_0 under f.

Definition 3.3. An element x_0 is *quasiperiodic* (or *recurrent*) if it is not periodic and, for every neighbourhood U of x_0, there exists a $t > 0$ such that $x_t \in U$.

We can now state our Theorem.

Theorem 3.4. *The square map on $\mathbb{Q}_p$ has two fixed points, 0 and 1. If x_0 satisfies $|x_0|_p > 1$, then its trajectory diverges to infinity; if $|x_0|_p < 1$, its trajectory converges to 0.*

Let $|x_0|_p = 1$; then $|x_t|_p = 1$ for all t. If $p = 2$, then this trajectory converges to 1; for $p > 2$, 1 is not attractive. If x_0 lies in the subgroup of Teichmüller representatives, its trajectory becomes periodic in finite time; otherwise, its eventually quasiperiodic trajectory is dense in some compact open subset of $\mathbb{Q}_p$.

Proof. It remains for us to prove that, for $p > 2$, 1 is non-attractive, and that the trajectory of an element x_0 on the unit circle is dense in a compact open subset of $\mathbb{Q}_p$. We do this with the help of the commutative diagram

$$\begin{array}{ccc} p\mathbb{Z}_p & \xrightarrow{z \mapsto 2z} & p\mathbb{Z}_p \\ {\scriptstyle \log}\uparrow & & \downarrow{\scriptstyle \exp} \\ 1+p\mathbb{Z}_p & \xrightarrow{u \mapsto u^2} & 1+p\mathbb{Z}_p, \end{array}$$

where the vertical arrows are isomorphisms and homeomorphisms.

Let n be the order of 2 in $\mathbb{F}_p^*$, and choose r maximal with the property that $2^n \equiv 1 \mod p^r$. For any $z \in p\mathbb{Z}_p$, write $m = \mathrm{val}(z)$, and define

$$V(z) = \bigcup_{l=0}^{n} (2^l z + p^{m+r}\mathbb{Z}_p),$$

a union of open sets contained in the stratum $p^m\mathbb{Z}_p$.

Lemma 3.5. *The trajectory of $z \in p\mathbb{Z}_p$ under the doubling map is dense in $V(z)$.*

Proof. This is an application of Proposition 3.1. $V(z)$ evidently contains the full trajectory of z under the doubling map. Let M be any integer (greater than $m + r$, say). It suffices to show that the trajectory of z meets every neighbourhood $z' + p^M\mathbb{Z}_p$, where $z' \in V(z)$. Now $V(z) \subseteq p^m\mathbb{Z}_p$; identify $p^m\mathbb{Z}_p/p^M\mathbb{Z}_p \simeq \mathbb{Z}_p/p^{M-m}\mathbb{Z}_p$. By Proposition 3.1, the iterates $2^l z$ take on np^{M-m-r} distinct values in this set. Yet this is precisely the number of elements in $V(z) \mod p^M\mathbb{Z}_p$: each of the n distinct open sets $2^l z + p^{m+r}\mathbb{Z}_p$ of $V(z)$ contain p^{M-m-r} elements modulo $p^M\mathbb{Z}_p$. □

We are now ready to address the trajectories of an element $u \in 1 + p\mathbb{Z}_p$ under the square map. First define

$$\mathcal{V}(u) = \exp(V(\log(u))).$$

Following the commutative diagram above, we conclude that the trajectory of u under the square map lies in this set $\mathcal{V}(u)$, and further, by Lemma 3.5, that this trajectory is dense. In particular, this proves that 1 is not an attractive fixed point.

Finally, we turn to the general case of $|x_0|_p = 1$. Use the isomorphism (3.2) to write $x_0 = \phi(0, a_0, z)$, with $a_0 \in \mathbb{F}_p^*$ and $z \in p\mathbb{Z}_p$. By [R], replacing x_0 with some iterate x_t if necessary, we may assume that a_0 is an element of a cycle of the square map in $\mathbb{F}_p^*$. Enumerate this cycle as $S' = \{a_0, a_1, \ldots, a_{q-1}\} \subseteq \mathbb{F}_p^*$, where q is the order of 2 modulo d, for some odd divisor d of $p - 1$ [R]. Then the trajectory of x_0 lies densely in some subset of the open set $S' \times V(z) \subseteq \mathbb{F}_p^* \times p\mathbb{Z}_p$, since the trajectory of z is dense in $V(z)$, and S' is finite.

More explicitly, set $b = gcd(q, n)$ to be the greatest common divisor of the periods of the two cycles (squares of a_0 and powers of 2 modulo p). Then $S' \times V(z) \subseteq \mathbb{F}_p^* \times p\mathbb{Z}_p$ can be partitioned into

b open subsets such that each contains a dense trajectory of one of its elements. This completes the proof. □

Example 1. Let $p = 7$, and $x_0 = \sigma_2 \exp(p)$, where σ_2 is the Teichmüller representative. Here $z = p$, $n = 3$ (and $r = 1$); and since $S' = \{\sigma_2, \sigma_4\}$, $q = 2$. Hence $b = 1$, and

$$S' \times V(p) = \{\sigma_2, \sigma_4\} \times \{p + p^2\mathbb{Z}_p, 2p + p^2\mathbb{Z}_p, 4p + p^2\mathbb{Z}_p\}.$$

Given any $x' \in \sigma_r(s + p\mathbb{Z}_p)$ in this set and $M > 0$, we can find a value $t > 0$ such that $x_t \equiv x' \mod p^M$ — simply take the least common multiple of those values which sufficed in each of the sets S' and $\mathcal{V}(1)$ separately. □

Example 2. Let $p = 11$ and $x_0 = \sigma_4 \exp(p)$. Then $n = 10$ (and $r = 1$); moreover $S' = \{\sigma_4, \sigma_5, \sigma_3, \sigma_9\}$, so $q = 4$. Hence $b = 2$, and the set $S' \times V(p)$ splits into 2 distinct open sets, such that the trajectory of x_0 is dense only in one:

$$\{\sigma_4, \sigma_3\} \times \{2^{2k}p + p^2\mathbb{Z}_p | 0 \le k \le 4\} \cup \{\sigma_5, \sigma_9\} \times \{2^{2k+1}p + p^2\mathbb{Z}_p | 0 \le k \le 4\};$$

the other open set in $S' \times V(p)$ evidently contains the dense trajectory of $\sigma_4 \exp(2p)$, for example. □

4. Iterates of $f_\varepsilon(x) = x^2 + \varepsilon$, $|\varepsilon|_p < 1$

In this section we consider the dynamics of the map $f_\varepsilon(x) = x^2 + \varepsilon$, where ε is "small" in the sense that $|\varepsilon|_p < 1$. Let us first recall a theorem of Pezda (noting that f_ε satisfies the hypothesis). Denote by $*$-cycle any primitive cycle of a polynomial contained entirely in an open set of the form $x + p\mathbb{Z}_p$, $x \in \mathbb{Z}_p$.

Theorem 4.1 ([Pe]). *Let f be a polynomial with coefficients in $\mathbb{Z}_p$. Suppose first that $p > 3$. If f admits a cycle of period n, then*

$$n = ab, \qquad \text{where } a \mid (p-1) \text{ and } b \le p. \tag{4.1}$$

Furthermore, the period of any $*$-cycle of f must divide $p - 1$.

If $p = 3$, then the possible periods of cycles are $\{1, 2, 3, 4, 6, 9\}$, and $*$-cycles cannot have period 6 or 9. If $p = 2$ then the possible periods of cycles are just $\{1, 2, 4\}$, and $*$-cycles cannot have period 4.

Pezda proves this result as a corollary to his more general theorem, which gives an upper bound on the possible lengths of cycles of polynomial maps on algebraic extensions of $\mathbb{Q}_p$. His proof, which is quite technical and clever, involves first reducing to $*$-cycles in the prime ideal (*eg* $p\mathbb{Z}_p$ in $\mathbb{Q}_p$), and then showing that the periods of such cycles are highly constrained. To show further, for $\mathbb{Z}_p$, which cycle periods are possible, he constructs from any given cycle a series of determinants whose valuations must be multiples of the period.

We next have the following theorem, which appears in a less general form in [TVW].

Theorem 4.2. *Let $f_\varepsilon(x) = x^2 + \varepsilon$, with $|\varepsilon|_p \le 1$. Suppose $p > 2$, and that f_ε admits a primitive cycle $\mathcal{O} = \{a_0, a_1, \ldots, a_{c-1}\}$. Set $z = (f_\varepsilon^c)'(a_0)$, and let t be the least positive integer such that $z^t \equiv 1 \mod p$. Let $\beta = val(z^t - 1)$, and set α to be the least integer greater than β/t. Then the only periodic points in the union of the neighbourhoods $a_i + p^\alpha\mathbb{Z}_p$, $0 \le i < c$, are those of the cycle $\mathcal{O}$.*

[TVW] prove this for the case of $c = 1$, by demonstrating that f_ε is topologically conjugate to the linear map $x \mapsto zx$ (where $z = f_\varepsilon'(a_0)$) in such a neighbourhood. It is a straightforward substitution to replace the map f_ε in their proof with the iterate f_ε^c, and the derivative $f_\varepsilon'(a_0)$ with its more general form $z = (f_\varepsilon^c)'(a_0)$.

Let us now proceed to the main result of this section. Note first that since f_ε is not a homomorphism of multiplicative groups, the isomorphims (3.2) and (3.1) are of no help here. Nevertheless, we have the following theorem, which shows that f_ε, $|\varepsilon|_p < 1$, can be interpreted as a perturbation of the original square map.

Theorem 4.3. *There are two fixed points of f_ε, $\delta_{p,\varepsilon}$ and $\mu_{p,\varepsilon}$, with $|\delta_{p,\varepsilon}|_p = |\mu_{p,\varepsilon} - 1|_p = |\varepsilon|_p < 1$. If x is a point such that $|x|_p > 1$, then its trajectory diverges to infinity; whereas if $|x|_p < 1$, its trajectory converges to $\delta_{p,\varepsilon}$.*

If $p = 2$, then the trajectory of every x such that $|x|_p = 1$ converges to $\mu_{p,\varepsilon}$. For all other p, if $|x|_p = 1$, then x is either a periodic point, or its trajectory is eventually quasiperiodic. In many cases, one can algorithmically determine the finitely many periodic points, and calculate them to any degree of precision. In the remaining, very special, cases, the algorithm may fail to terminate, leaving only an approximate picture of the orbit space.

More precisely, let n denote the order of 2 modulo p. Given a primitive c-cycle $\mathcal{O}$ of the square map in $\mathbb{F}_p$, if n does not divide c, then there exists a unique corresponding fundamental c-cycle of f_ε with leading coefficients in $\mathcal{O}$. Any other periodic element of f_ε with leading coefficient in $\mathcal{O}$ is a harmonic cycle, and must have a period which is a multiple of both c and n.

Proof. **A. Existence of fixed points:** A fixed point $x = f_\varepsilon(x)$ must satisfy

$$x = \frac{1 \pm \sqrt{1 - 4\varepsilon}}{2}.$$

If $p \neq 2$, then $\mathrm{val}(4\varepsilon) \geq 1$, and so the square root of $1 - 4\varepsilon$ exists in $\mathbb{Q}_p$ by Hensel's Lemma, since 1 has a square root in $\mathbb{F}_p$. One obtains $\sqrt{1 - 4\varepsilon} = \pm(1 + \varepsilon u)$, for some $u \in \mathbb{Z}_p^*$, so the two fixed points are

$$\delta_{p,\varepsilon} = -\frac{\varepsilon u}{2} \qquad \text{and} \qquad \mu_{p,\varepsilon} = 1 + \frac{\varepsilon u}{2} \qquad (p \neq 2).$$

Similarly, if $p = 2$, then $\mathrm{val}(4\varepsilon) \geq 3$, so we may again apply Hensel's Lemma to deduce the existence of a square root; here it takes the form $1 + 2\varepsilon u$, for some $u \in \mathbb{Z}_p^*$. Hence the two fixed points are

$$\delta_{2,\varepsilon} = -\varepsilon u \qquad \text{and} \qquad \mu_{2,\varepsilon} = 1 + \varepsilon u \qquad (p = 2).$$

B. Trajectories for $|x|_p \neq 1$: It is clear that $|x|_p > 1$ implies $|f_\varepsilon(x)|_p = |x|_p^2 > |x|_p$; hence the trajectory of such an x diverges to infinity. Now suppose that $|x|_p < 1$. It follows that

$$|f_\varepsilon(x)|_p = |x^2 + \varepsilon|_p \begin{cases} = |x|_p^2 & \text{if } |x|_p^2 > |\varepsilon|_p; \\ = |\varepsilon|_p & \text{if } |x|_p^2 < |\varepsilon|_p; \\ \leq |\varepsilon|_p & \text{if } |x|_p^2 = |\varepsilon|_p. \end{cases}$$

Since the norm on $\mathbb{Q}_p$ is discrete, we deduce that $|f_\varepsilon^n(x)|_p = |\varepsilon|_p$ for all n sufficiently large. We show that from this point on, the trajectory approximates $\delta_{p,\varepsilon}$.

Let $m = \mathrm{val}(\varepsilon) \geq 1$. Then since $f_\varepsilon^{n+1}(x) = (f_\varepsilon^n(x))^2 + \varepsilon$, and $\mathrm{val}(f_\varepsilon^n(x))^2 = 2m$, we have $f_\varepsilon^{n+1}(x) \equiv \varepsilon \mod p^{2m}$. This last equality holds also for the fixed point $x = \delta_{p,\varepsilon}$; hence in fact $f_\varepsilon^{n+1}(x) \equiv \delta_{p,\varepsilon} \mod p^{2m}$. To prove that $f_\varepsilon^n(x)$ comes arbitrarily close to $\delta_{p,\varepsilon}$ as $n \to \infty$, we have only to note the following. Given any $y \in \mathbb{Q}_p$ such that $y \equiv \delta_{p,\varepsilon} \mod p^k$ (and thus $y \equiv 0 \mod p^m$), it follows that $y^2 \equiv \delta_{p,\varepsilon}^2 \mod p^{k+m}$. Hence $f_\varepsilon(y) \equiv \delta_{p,\varepsilon}^2 + \varepsilon \mod p^{k+m}$; but as $\delta_{p,\varepsilon}$ is a fixed point of f_ε, we conclude that $f_\varepsilon(y) \equiv \delta_{p,\varepsilon} \mod p^{k+m}$. Clearly then, $\delta_{p,\varepsilon}$ is an *attractive* fixed point, with basin of attraction equal to $p\mathbb{Z}_p$.

C. Outline of strategy for the case of $|x|_p = 1$: In the following sections, we will construct a (potentially non-terminating) algorithm for determining the existence of a cycle of given period c. We proceed in three parts.

In Part D, we consider the special case of $p = 2$, where we find no periodic points besides the attractive fixed points. Thereafter we consider only odd primes p.

In Part E, we determine the applicability of Hensel's Lemma to the c-th iterate of f_ε, or rather, to the function

$$g(x) = f_\varepsilon^c(x) - x.$$

For $r \geq 0$ to be determined, choose $z_0 \in \mathbb{Z}_p^*$ such that $g(z_0) \equiv 0 \mod p^{2r+1}$. Write $z_1, z_2, z_3, \ldots$ for the iterates of z_0 under f_ε. Then by the chain rule,

$$g'(z_0) = f_\varepsilon'(z_0) f_\varepsilon'(z_1) \cdots f_\varepsilon'(z_{c-1}) - 1 = 2^c z_0 z_1 \cdots z_{c-1} - 1. \tag{4.2}$$

To conclude by Hensel's Lemma that there is an exact root of g (generally, a c-cycle of f_ε) near z_0, r must satisfy $r \geq \mathrm{val}(g'(z_0))$. Predicting this value is the object of much of Part E.

In Part F, we summarize an algorithm which, in most cases, allows one to compute all cycles of f_ε on $\mathbb{Q}_p$.

D. Determination of the orbit space for $p = 2$: If $p = 2$, then $\mathrm{val}(g'(z_0)) = 0$ for all $c > 0$. Hensel's Lemma implies that for any c, there exists a unique $x \in \mathbb{Z}_2$ such that $x \equiv z_0 \equiv \mod 2$ and $g(x) \equiv 0 \mod 2$. Since $x = \mu_{2,\varepsilon}$ fits this criterion, we deduce that, for $p = 2$, there are no periodic points of f_ε besides the fixed points. Let us prove that $\mu_{2,\varepsilon}$ is also attractive.

Let $x = 1 + s$, with $s \in 2\mathbb{Z}_2$, be an arbitrary element of $\mathbb{Z}_2^*$. If $\mathrm{val}(s) < \mathrm{val}(\varepsilon)$, then $f_\varepsilon(x) = 1 + 2s + s^2 + \varepsilon = 1 + s'$, with $\mathrm{val}(s') = \mathrm{val}(s) + 1$. On the other hand, if $\mathrm{val}(s) > \mathrm{val}(\varepsilon)$, then the same calculation yields $\mathrm{val}(s') = \mathrm{val}(\varepsilon)$. Hence, replacing x with $f_\varepsilon^n(x)$ $(n > 0)$ if necessary, we may assume that $\mathrm{val}(s) = \mathrm{val}(\varepsilon)$, and thus that $x \equiv 1 + \varepsilon \mod 2^{m+1}$. Similarly, we deduce that $\mu_{2,\varepsilon} \equiv 1 + \varepsilon \mod 2^{m+1}$. It thus suffices to prove that if $y \in \mathbb{Z}_2$ satisfies $y \equiv \mu_{2,\varepsilon} \mod 2^k$, then $f_\varepsilon(y) \equiv \mu_{2,\varepsilon} \mod 2^{k+1}$. Write $y - \mu_{2,\varepsilon} = 2^k u$, for some $u \in \mathbb{Z}_2^*$. Then $(y - \mu_{2,\varepsilon})^2 = 2^{2k} u^2$, which implies

$$y^2 + \mu_{2,\varepsilon}^2 = 2\mu_{2,\varepsilon} y + 2^{2k} u^2 = 2\mu_{2,\varepsilon}(\mu_{2,\varepsilon} + 2^k u) + 2^{2k} u^2 = 2\mu_{2,\varepsilon}^2 + 2^{k+1} \mu_{2,\varepsilon} u'$$

for some $u' \in \mathbb{Z}_2^*$. Subtract $2\mu_{2,\varepsilon}^2$ to deduce that $f_\varepsilon(y) - \mu_{2,\varepsilon} \equiv 0 \mod 2^{k+1}$, as required.

E. Prediction of $\mathrm{val}(g'(z_0))$ when p odd: For the remainder, suppose $p \neq 2$. Then

$$z_0 z_1 \cdots z_{c-1} \equiv z_0 z_0^2 z_0^4 \cdots z_0^{2^{c-1}} \equiv z_0^{2^c - 1} \equiv 1 \mod p, \tag{4.3}$$

where the first of these equivalences uses that $|\varepsilon|_p < 1$, and the last that z_0 is periodic of order c (modulo p) under the map f_ε. Thus, if $2^c \not\equiv 1 \mod p$ — *i.e.* if n does not divide c — then $r = \mathrm{val} g'(z_0) = 0$. By Hensel's Lemma, there exists a *unique* $x \in \mathbb{Z}_p$ such that $g(x) = 0$ and $x \equiv z_0 \mod p$. Thus, for such c, it is necessary and sufficient to find a primitive c-cycle of the square map f_0 on $\mathbb{F}_p^*$ to prove the existence of a primitive c-cycle of f_ε in $\mathbb{Z}_p$. Moreover, the uniqueness of this x implies that, for any c' not divisible by n, there are no cycles of f_ε of period c' through *any* element with leading coefficient equal to z_0. Thus, any harmonic cycles of this fundamental c-cycle (that is, cycles having the same leading coefficients but longer period) must have period divisible by both c and n.

Next consider those c for which n divides c, that is,

$$2^c = 1 + p^r v, \tag{4.4}$$

for some $v \in \mathbb{Z} \cap \mathbb{Z}_p^*$, and $r > 0$. Expanding the expression (4.2) for $g'(z_0)$ yields

$$g'(z_0) = 2^c z_0 z_1 \cdots z_{c-1} - 1 = 2^c (z_0^{2^c - 1} + \varepsilon u) - 1,$$

for some $u \in \mathbb{Z}_p$. By (4.3), $z_0^{2^c-1} \equiv 1 \mod p$; apply (4.4) to this exponent to get $z_0^{p^r v} \equiv 1 \mod p$. Since $b^p \equiv b \mod p$ for all $b \in \mathbb{F}_p$, it follows that already $z_0^v \equiv 1 \mod p$. Writing $z_0^v = 1 + y$ for some $y \in p\mathbb{Z}_p$, and applying the binomial theorem to $z_0^{p^r v} = (1+y)^{p^r}$, we deduce that in fact $z_0^{2^c-1} \equiv 1 \mod p^{r+1}$. Write $z_0^{2^c-1} = 1 + p^{r+1}u'$, for some $u' \in \mathbb{Z}_p$. Then

$$g'(z_0) = 2^c(z_0^{2^c-1} + \varepsilon u) - 1 = (1 + p^r v)(1 + \varepsilon u + p^{r+1}u') - 1. \tag{4.5}$$

Thus, for most cases, $\mathrm{val}(g'(z_0)) \leq r$, and is equal to r if $\mathrm{val}(\varepsilon u) \geq r+1$.

Now we compute the trajectories of the map f_ε on a set of representatives of $\mathbb{Z}_p/p^{2r+1}\mathbb{Z}_p$. One such set is

$$\mathcal{R}_r = \{n \in \mathbb{Z} \mid 1 \leq n \leq p^{2r+1}\}. \tag{4.6}$$

If there exists an element $z_0 \in \mathbb{Z}_p$ whose orbit under f_ε in $\mathcal{R}_r$ has period c, i.e., such that $g(z_0) \equiv 0 \mod p^{2r+1}$, then Theorem 2.3 ensures that there is an exact root x of g such that $x \equiv z_0 \mod p^{r+1}$. We must take care, however, as the primitive period of this root x need not necessarily be c: as a consequence of Theorem 2.3, if y is an element of a cycle of f_ε of period dividing c, then every element y' in the coset $y + p^{r+1}\mathbb{Z}_p$ will satisfy $g(y') = 0$ as well. Hence we must eliminate all these as possibilities before we can conclude that we have discovered a c-cycle.

If no z_0 of period c can be found in $\mathcal{R}_r$, then no c-cycle exists.

Note that when $\mathrm{val}(\varepsilon u) = r$, it is possible that cancellations may produce $\mathrm{val}(p^r v + \varepsilon u) > r$. Thus, whenever $\mathrm{val}(\varepsilon) \leq r$ and a potential cycle through an element z_0 is found, we must evaluate $\mathrm{val}(g'(z_0))$ directly. Should the result be greater than r, we must restart our search for z_0 with respect to the new value of r (and potentially arrive at this same juncture, with a slightly different value of z_0, but with the same problem, *ad infinitum*). These circumstances define what we term the *nongeneric case* of the algorithm.

F. Summary of algorithm (p odd): Let $c \geq 1$ be the period of the cycle $\mathcal{O} = \{a_0, a_1, \ldots a_{c-1}\}$ in $\mathbb{F}_p$. Thus c is the order of 2 modulo d, for some odd divisor d of $p-1$. Applying Theorem 4.1 and the above analysis, we see that the possible periods of cycles of f_ε in $\mathbb{Z}_p$ (with leading coefficients in $\mathcal{O}$) are as follows. Set $l = \mathrm{lcm}(c, n)$ to be the least common multiple of c and $n = \mathrm{ord}_p 2$. The denotations "first" and "second" harmonic are suggestive of the heirarchy of the generic case only; they correspond to different values of r in the above analysis. In particular, the existence of a second harmonic is independent of that of a first harmonic.

- If $p = 3$, then $c = 1$. We have:
  — the fundamental cycle is the fixed point $\mu_{3,\varepsilon}$;
  — the first harmonics (if any) have periods 2 or 4.
  otherwise, for $p > 3$
- If $c = 1$, then:
  — there exists a fixed point in $\mathbb{Z}_p^*$, which is a fundamental cycle;
  — the periods of the first harmonics, if any, have the form kn, with k dividing $(p-1)/n$.
- If $c \neq 1$, $c \mid (p-1)$, and $2^c \not\equiv 1 \mod p$:
  — there exists a fundamental cycle of period c;
  — the periods of the first harmonics (if any) have the form kl, for some $1 \leq k < p$;
  — the periods of the second harmonics (if any) have the form pkl, for $1 \leq k < p$ satisfying $kl \mid (p-1)$.
- If $c \nmid (p-1)$ and $2^c \not\equiv 1 \mod p$:
  — there exists a fundamental cycle of period c;
  — the periods of the first harmonics (if any) have the form kl, with $1 \leq k < p$, such that kl admits a factorization of the form (4.1).

- If $c \mid (p-1)$ and $2^c \equiv 1 \mod p$:
  — there may be a fundamental cycle of period c;
  — if there is no fundamental cycle, there may be first harmonics of periods kc, for $2 \le k < p$;
  — the periods of the second harmonics, if any, have the form pkc, for some $1 \le k < p$ such that k divides $\frac{p-1}{c}$.
- If $c \nmid (p-1)$ and $2^c \equiv 1 \mod p$:
  — there may be a fundamental cycle of period c;
  — if there is no fundamental cycle, there may be first harmonics of periods kc, for $2 \le k < p$ such that kc admits a factorization of the form (4.1).

Those primes for which either of these final two cases arise are the *exceptional primes* alluded to in the introduction and discussed in section 6.

To find a cycle of f_ε of a given period σ from the list above, let r be the estimate of $\mathrm{val}(g'(z_0))$ given in (4.4), and locate a c-cycle in $\mathcal{R}_r$. If none are found we may conclude that no σ-cycles exist. Otherwise, given a candidate z_0, we must

(a) verify that $\mathrm{val}(g'(z_0)) \le r$ and
(b) verify that $z_0 \mod p^{r+1}$ does not coincide with the leading coefficients of some shorter cycle.

The failure of (a) leads to a new estimate of r (and potential disaster, as remarked above); the failure of (b) (on all candidates z_0) implies that no c-cycle exists.

There are a number of potential optimizations to this procedure, however, that curb the polynomial growth of computations with p and r. They are as follows:

i. Linearity in a Neighbourhood: Let x be an exact periodic point of f_ε of period σ. In practice, only the first few digits of x will be known as a result of the preceding steps.

Let t be the order of 2^σ modulo p and write $2^\sigma = 1 + p^r v$ for some $v \in \mathbb{Z}_p^*$. If $r = 1$, compute $x \mod p^2\mathbb{Z}_p$ (and set $s = 1$ below); otherwise, compute at least the first two nonzero digits of x; that is, compute either $x \mod p^2$ or, more generally, $x \mod p^{s+1}$ where $s = \mathrm{val}(x - (x \mod p))$. Write $\tilde{x}$ for this approximation to x. Let z be the product

$$z = (\tilde{x} f_\varepsilon(\tilde{x}) \dots f_\varepsilon^{c-1}(\tilde{x}))^t.$$

Set $\beta = \mathrm{val}(2^{ct}z - 1)$; if $\beta = \min\{r, s\}$, then no cancellations occurred, implying that β is indeed equal to $\mathrm{val}(g'(x) - 1)$. Thus we set α to be the least integer greater than β/t.

Otherwise, the limited precision of our approximation $\tilde{x}$ allows us to conclude only that $\mathrm{val}(g'(x)-1) > \beta$ and that $\alpha > \beta/t$. To obtain a more precise estimate of α, we must improve our estimate $\tilde{x}$ to at least the p^β digit, and recalculate z and α (possibly *ad infinitum*).

Now suppose we have computed α. Then f_ε^c is conjugate to a linear map in the neighbourhood $x + p^\alpha\mathbb{Z}_p$, and consequently, no periodic points of f_ε intersect the union

$$x + p^\alpha\mathbb{Z}_p \ \cup \ f_\varepsilon(x) + p^\alpha\mathbb{Z}_p \ \cup \cdots \cup \ f_\varepsilon^{c-1}(x) + p^\alpha\mathbb{Z}_p. \tag{4.7}$$

If α is sufficiently small (and thus the neighbourhood is large), this eliminates the possibility of any further harmonics, and we are done. Note that this is quite common, as $\beta = 1$ except for the nongeneric case, and $t > 1$ except for the exceptional primes.

Moreover, in any case where α can be computed, we can eliminate the set (4.7) from the search for harmonic cycles.

ii. Equivalence to the Square Map: Note that f_ε acts as $x \mapsto x^2$ on the set $\mathbb{Z}_p/\varepsilon\mathbb{Z}_p$. Write $m = \mathrm{val}(\varepsilon)$; the possible periods of the cycles of $x \mapsto x^2$ on the set $\mathbb{Z}_p/p^m\mathbb{Z}_p$ were determined in Proposition 3.1. Thus, if m is sufficiently large (and ε is sufficiently small), we may eliminate some of the possible periods of harmonics from the list above (for example, all those with multiple $k > 1$) for any case where $2r + 1 \le m$.

iii. Elimination of Echoes of Smaller Cycles: Let $y_0, y_1, \dots y_{\sigma'-1}$ be a previously discovered σ'-cycle, with $\sigma' \mid \sigma$ and $\mathrm{val}(f_\varepsilon^{\sigma'}(y_0)) = s$. Then each element of the open set

$$y_0 + p^{2r+1-s}\mathbb{Z}_p \cup y_1 + p^{2r+1-s}\mathbb{Z}_p \cup \cdots \cup y_{\sigma-1} + p^{2r+1-s}\mathbb{Z}_p$$

will be a solution to $f_\varepsilon^\sigma(x) \equiv x \mod p^{2r+1}\mathbb{Z}_p$, by Theorem 2.3, but the corresponding exact solutions given by the theorem will be just $y_0, y_1, \dots y_{\sigma'-1}$ again. Hence we can eliminate these sets from consideration as well. Doing this from the outset neatly sidesteps the complication (b) mentioned above.

G. Quasiperiodicity: Finally, consider the case where $|x|_p = 1$ and x is not periodic. Replacing x with some iterate under f_ε if necessary, we may assume that its constant term a_0 is an element of a cycle in the finite field; denote the elements of this cycle by $a_0, a_1, \cdots a_{c-1}$. We wish to show that x is a quasiperiodic point. Take a neighbourhood U of x; then U contains a basic open set of the form $x + p^n\mathbb{Z}_p$, for some $n > 0$. Consider the trajectories of f_ε on the set of all cosets of $p^n\mathbb{Z}_p$ whose representatives have constant term among $a_0, a_1, \cdots, a_{c-1}$. By Hensel's Lemma, f_ε^{-1} exists on this set, and moreover it is unique, since $f_\varepsilon(x) \equiv f_\varepsilon(y) \mod p^n$ implies $x^2 \equiv y^2 \mod p^n$. The constant terms are nonzero and have by definition unique square roots among the $a_0, a_1, \cdots a_{c-1}$, so we deduce that $x \equiv y \mod p^n$. Hence, the trajectories of f_ε on this coset space are cycles, and in particular there is some $N > 0$ such that $f_\varepsilon^N(x) \in x + p^n\mathbb{Z}_p$.

□

5. Iterates of $f_\varepsilon(x) = x^2 + \varepsilon$, $|\varepsilon|_p = 1$

The orbit space of these maps are drastically different from those of the preceding two sections; nevertheless, much of the analysis which permitted us a global general picture there carries over to this boundary case.

As noted in [TVW], if $|x|_p > 1$, then the trajectory of f_ε through x diverges to infinity. Thus the question reduces again to a consideration of the trajectories in $\mathbb{Z}_p$.

Consider first the trajectories of f_ε on the residue field $\mathbb{F}_p$. As f_ε is not equivalent to the square map in this case, there is no known general, uniform description of this orbit space. For example, not all f_ε admit fixed points, since $\sqrt{1-4\varepsilon}$ may or may not exist in $\mathbb{Q}_p$. However, the finiteness of $\mathbb{F}_p$ implies the existence of *some* cycles. Insofar as concerns us, they fall into two categories.

The first kind of cycle is one which contains the element $0 \in \mathbb{F}_p$. (This is called an *attractive cycle* in [TVW].) Denote the elements of this cycle $\{a_0, a_1, \dots, a_{c-1}\}$ (with some $a_i = 0$) and consider $g(x) = f_\varepsilon^c(x) - x$. From (4.2), we deduce that $\mathrm{val}(g'(a_0)) = 0$, since the product $a_0a_1 \cdots a_{c-1}$ is 0 modulo p. Hence there exists a unique c-cycle of f_ε with these leading coefficients; even more, this uniqueness (together with the exactness of approximation modulo p) implies that there are *no other cycles* (of any period) with these leading coefficients. In the terminology of the preceding sections: this case gives rise to a single fundamental cycle, with no harmonics.

The second kind of cycle is one which lies entirely in $\mathbb{F}_p^*$, and is similar to those encountered in the proof of Theorem 4.3. For $|\varepsilon|_p = 1$, however, the product $a_0a_1 \cdots a_{c-1}$ is *not* necessarily equal to 1 modulo p, since the analysis of (4.3) does not apply. Hence the valuation of $g'(a_0)$ depends on the entire term in (4.2). We have no *a priori* estimate of $\mathrm{val}(g'(a_0))$ in this case.

Nevertheless, a coarser version of the anaylsis of Part E of the proof can be applied. If $\mathrm{val}(g'(a_0)) = 0$, then the cycle gives rise, via Hensel's Lemma, to a unique c-cycle in $\mathbb{Z}_p$. The only other possible periods of cycles with leading coefficients in the set $\{a_0, a_1, \dots, a_{c-1}\}$ are cm, where m is a multiple of the order of $2^c a_0a_1 \cdots a_{c-1}$ modulo p, and where, by Pezda's Theorem 4.1, cm admits a factorization of the form (4.1). To find a cycle of period σ, one considers the dynamics

of f_ε on sets of the form $\mathbb{Z}/p^{2s+1}\mathbb{Z}$; each time a candidate z_0 is found, we verify that $\mathrm{val}(g'(z_0)) \leq s$. If this fails to be true, we increase s and try again.

Note that the quasiperiodicity argument in Part G of the proof of Theorem 4.3 goes through unchanged for $|\varepsilon|_p = 1$ and hence that under f_ε, all points in $\mathbb{Z}_p$ are either periodic or eventually quasiperiodic. Moreover, as suggested by [TVW], the limiting result Theorem 4.2 holds for $|\varepsilon|_p = 1$ as well, indicating that in some circumstances one can prove the nonexistence of cycles of longer period in a neighbourhood of a given cycle.

6. Open Questions

In Section 3 we laid the foundations for the theory of fundamental cycles. One is immediately struck by some open number-theoretic questions.

For one: how do we determine the order n of 2 in $\mathbb{F}_p^*$? The distribution of these orders is well-known, up to the Generalized Riemann Hypothesis; but determining the value of n in any given case remains difficult. Using the Legendre symbol, one knows that $2^{\frac{p-1}{2}} \equiv 1 \mod p$ if and only if $p \equiv \pm 1 \mod 8$ [S, Ch.1]; but this is not enough to determine n completely.

For another: whereas a formula (in terms of the order of 2 modulo odd divisors of $p-1$) for the number and period of the orbits of the square map on $\mathbb{F}_p$ is known, several related questions remain open. For example, set $c(p)$ equal to the number of cycles of the square map on $\mathbb{F}_p$. On what values, if any, is the map c infinite-to-one? It is conjectured that $c(p) = 2$ is such a value (Artin primes); and but that $c(p) = 1$ is not (Fermat primes) [R]. What effect does it have to replace c with the number of cycles of f_ε, $\varepsilon \in \mathbb{Z}$, as p varies? Or with the maximum number of cycles over all ε?

Related to this is the following more detailed question. For which exceptional primes p (see Table 6.1) does there exist a cycle of the square map on $\mathbb{F}_p$ which fails to induce a corresponding fundamental cycle of f_ε on $\mathbb{Q}_p$? Is there a choice of ε such that there are *no* cycles (fundamental or harmonic) in $\mathbb{Z}_p$ arising from the problematic $\mathrm{ord}_d 2$-cycle in $\mathbb{F}_p$?

For example, the least such prime is $p = 251$. Under the square map, $\mathbb{F}_p$ admits a cycle of period $r_{125} = 100$, but there is no corresponding fundamental cycle of $f_p(x) = x^2 + p$ in $\mathbb{Z}_p$.

The consideration of this class of (large, easily characterized) primes is potentially of interest in its own right. In the context of this paper, it seems that these primes are the ones for which the dynamics of the square map $x \mapsto x^2$ are *least* stable under perturbations.

Another open question, which seems more analytic than number-theoretic in nature, is the existence of an nongeneric pair (p, ε) for which the algorithm of Part F of the proof fails to terminate on some $x_0 \in \mathbb{Q}_p$. Two sets of circumstances can lead to an infinite recursion, but both arise from the conjectural existence of a cycle of f_ε on $\mathbb{Q}_p$, say through the elements $\{x_0, x_1, \ldots x_{c-1}\}$, for which

$$((f_\varepsilon^c)')^t = (2^c x_0 x_1 \cdots x_{c-1})^t = 1 \tag{6.1}$$

exactly for some $t > 0$. If $t = 1$, the algorithm cannot prove or disprove the existence of this cycle in finite time, as necessarily the estimate r of the valuation of the derivative $2^c x_0 x_1 \cdots x_{c-1} - 1$ would never be sufficient to apply Hensel's Lemma. (In fact, Hensel's Lemma is empty when the derivative is identically zero.)

Furthermore, for any t, even if the existence of such a cycle is proven or assumed, the algorithm we describe for isolating a neighbourhood on which f_ε^c has only one fixed point will never terminate.

We can understand why this must occur, as follows. Suppose $p \neq 2$ and write

$$f_\varepsilon^c(x_0 + h) = f_\varepsilon^c(x_0) + h(f^c)'(x_0) + \frac{1}{2}h^2(f^c)''(x_0) + \cdots$$

for the Taylor expansion of the polynomial at x_0. As $f_\varepsilon^c(x_0) = 0$, and $(f^c)'(x_0) = \mu_t$, a t-th root of unity, we can rewrite this as $f_\varepsilon^c(x_0 + h) \equiv x_0 + h\mu_t \mod h^2\mathbb{Z}_p$. Now iterate this expression t times, using the relations $f^c(f^c(x_0 + h)) \equiv f^c(x_0 + h\mu_t) \equiv x_0 + h\mu_t^2 \mod h^2\mathbb{Z}_p$. We conclude that for all h,

$$f_\varepsilon^{ct}(x_0 + h) \equiv x_0 + h \mod h^2\mathbb{Z}_p.$$

This holds for any $h \in \mathbb{Z}_p$; in other words, f_ε^{ct} behaves approximately as its linearization – the identity. However, as f_ε has only finitely many periodic points, achieving a topological conjugacy between the two maps is not possible.

Unfortunately, neither of these cases can be distinguished from one in which the equation (6.1) holds only modulo $p^s\mathbb{Z}_p$, for some large $s > 0$, except in special circumstances (as below). One might begin to justify our use of the suggestive term "non-generic" by remarking that these pairs (p, ε) are defined by a condition which is far from stable under perturbations of p or of ε.

Example. Let $p = 3$ and consider the map f_ε, with $\varepsilon = \frac{3}{4} = \frac{p}{1+p}$. The fixed point $x_0 = \mu_{3,\varepsilon} = 1 - \frac{1}{2}p$ satisfies $(2x_0)^2 = 1$ exactly. Hence this is an example of an "nongeneric" case. □

We are left with many unanswered questions. In what sense does the behaviour of f_ε around x_0 differ from its behaviour in the generic case? Does every prime p admit some choice of ε for which there is a cycle satisfying (6.1)? How can we find such ε? Do we dare imagine that they are in some sense boundary values, such that the behaviour of the quadratic maps f_δ can be predicted by the relation of δ to ε?

References

[A] ARIBAS, written by Otto Forster. See, for example, *The HP-UX Porting and Archive Center* (Maths/Misc., 1999) http://boss.cae.wisc.edu/.

[B] S. Ben-Menahem, "p-adic Iterations," preprint Tel-Aviv UP (1988) 1627–88.

[CDP] Richard Crandall, Karl Dichler and Carl Pomerance, "A Search for Wieferich and Wilson Primes," Mathematics of Computation **66**, No. 217 (1997), 433–449.

[D] Robert L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed., Addison-Wesley, 1989.

[E] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*. Springer-Verlag, New York, 1995.

[K] Neal Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Second Edition. Springer-Verlag, New York, 1984.

[L] Jonathan Lubin, "Nonarchimedean dynamical systems," Compositio Math., **94** no. 3 (1994), 321–346.

[Mo] Patrick Morton, "Arithmetic properties of periodic points of quadratic maps," Acta Arithmetica, LXII.4 (1992) 343–372.

[Na] W. Narkiewicz, "Arithmetics of Dynamical Systems, A Survey," Tatra Mountains Math. Publ. **11** (1997) 69–75. 1998.

[Pe] T. Pezda, "Polynomial cycles in certain local domains," Acta Arithmetica, LXVI.1 (1994) 11–22.

[R] Thomas D. Rogers, "The Graph of the Square Mapping on the Prime Fields," Discrete Mathematics **148** (1996) 317–324.

[S] Jean-Pierre Serre, *A Course in Arithmetic*, Springer-Verlag, New York, 1973.

[Si] Joseph H. Silverman, "Rational Functions with a Polynomial Iterate," Journal of Algebra **180** (1996) 102–110.

[SR1] M. Shirvani and T.D.Rogers, "Ergodic Endomorphisms of Compact Abelian Groups," Commun. Math. Phys. **118** (1988) 401–410.

[SR2] M. Shirvani and T.D.Rogers, "On Ergodic One-Dimensional Cellular Automata," Commun. Math. Phys. **136** (1991) 599–605.

[TVW] E. Thiran, D. Verstegen and J. Weyers, "p-adic Dynamics," Journal of Statistical Physics, Vol. 54, Nos 3/4 (1989) 893–913.

[V] D. Verstegen, "p-adic Dynamical Systems," in *Number Theory and Physics* (J.-M. Luck, P.Moussa and M. Waldschmidt, eds.) Springer Proceedings in Physics, Springer (Berlin), Vol. 47 (1990) 235–242.

[WR] Ralph Walde and Paula Russo, "Rational Periodic Points of the Quadratic Function $Q_c(x) = x^2 + c$," Amer. Math. Monthly, Vol 101 (1994) 318–331.

E-mail address: mnevins@alum.mit.edu, tdrogers@gpu.srv.ualberta.ca

Department of Mathematical Sciences, University of Alberta, Edmonton, Alberta, Canada T6G 2G1

p	d	$\phi(d)$	$n = \mathrm{ord}_p(2)$	$\mathrm{ord}_d 2$
251	125	100	50	100
1459	729	486	486	486
5419	2709	1512	42	42
39367	19683	13122	2187	13122
54001	3375	1800	180	900
110251	55125	25200	350	2100
116381	29095	20240	5060	5060
148997	37249	37056	772	18528
181549	45387	29520	164	7380
213751	106875	54000	1125	4500
246241	7695	3888	108	108
268501	67125	35600	100	8900
446473	55809	33696	351	1404
730021	182505	93104	2116	23276
1299079	649539	393660	6561	196830
2010583	1005291	571536	1701	47628
3037501	759375	405000	202500	202500
3618757	904689	559872	324	1944
4390021	1097505	565152	10092	70644
5419387	2709693	1522152	4374	126846
5521693	1380423	821280	236	102660
5746001	359125	249600	520	7800
5840251	2920125	1435200	650	89700
6049243	3024621	2012040	4374	1006020
6561001	820125	437400	54675	218700
6876901	1719225	913680	1620	76140
8039359	4019679	2629224	8427	1314612
9106063	4553031	2542512	329	45402
10113049	1264131	759360	339	47460
13357177	1669647	931896	5547	77658
17231831	8615915	5100480	8855	106260
17360407	8680203	4960116	413343	826686
22366891	11183445	4717440	78	156
26558929	1659933	962280	24057	240570
27338681	3417335	2666400	2020	333300
28934011	14467005	6613488	13122	551124
29327761	1832985	728640	7590	15180
34229539	17114769	9730224	57918	115836
35175001	4396875	1980000	7500	82500
47904049	2994003	1942056	26973	107892
48912491	24456245	17012160	110	1063260
56337751	28168875	12700800	3675	44100
74967931	37483965	19990800	810	4997700
96468751	48234375	22050000	459375	1837500

TABLE 6.1. The exceptional primes up to 1×10^8, calculated with the aid of the software package ARIBAS [A].