J. Aust. Math. Soc. **92** (2012), 163–178
doi:10.1017/S1446788712000262

COUNTING FIXED POINTS, TWO-CYCLES, AND COLLISIONS OF THE DISCRETE EXPONENTIAL FUNCTION USING *p*-ADIC METHODS

JOSHUA HOLDEN and MARGARET M. ROBINSON✉

(Received 10 May 2011; accepted 1 February 2012)

Communicated by I. E. Shparlinski

Dedicated to the memory of Alf van der Poorten

Abstract

Brizolis asked for which primes p greater than 3 there exists a pair (g, h) such that h is a fixed point of the discrete exponential map with base g, or equivalently h is a fixed point of the discrete logarithm with base g. Various authors have contributed to the understanding of this problem. In this paper, we use p-adic methods, primarily Hensel's lemma and p-adic interpolation, to count fixed points, two-cycles, collisions, and solutions to related equations modulo powers of a prime p.

2010 *Mathematics subject classification*: primary 11D88; secondary 11A07, 11N37, 11Y16, 94A60.

Keywords and phrases: Brizolis, discrete logarithm, discrete exponential, Hensel's lemma, p-adic interpolation, fixed points, two-cycles, collisions.

1. Introduction

The idea of counting fixed points of discrete exponential functions is usually traced back to Brizolis [12, paragraph F9], who asked whether, given a prime $p > 3$, there is always a pair $(g, x) \in \{1, \ldots, p-1\}^2$ such that g is a primitive root modulo p and

$$g^x \equiv x \bmod p. \tag{1.1}$$

We can regard solutions to this equation as fixed points of a discrete exponential function. Zhang [21] proved that the answer to Brizolis' question is always yes for sufficiently large p; this was rediscovered independently by Cobeli and Zaharescu [6]. Levin (formerly Campbell) proved the result for all primes in [5]. See also [18].

The first-named author thanks the Hutchcroft Fund at Mount Holyoke College for support.

Zhang, and independently Cobeli and Zaharescu, also found a way of estimating the number of pairs (g, x) that satisfy the conditions above and for which x is a primitive root. Specifically, if $N(p)$ is the number of such pairs for a given prime p, we have the following result.

THEOREM 1.1 (See [6, 21]). *Let* $\mathrm{d}(p-1)$ *be the number of divisors of* $p-1$. *Then*

$$\left|N(p) - \frac{\phi(p-1)^2}{p-1}\right| \le \mathrm{d}(p-1)^2\sqrt{p}(1+\ln p).$$

The first-named author [13, 14] investigated the problem of counting the number of solutions to Brizolis' equations when g and x are not necessarily primitive roots. If $F(p)$ is the number of such pairs (g, x), it was conjectured that

$$F(p) \sim p-1$$

as p goes to infinity. The first-named author and Moree [15, Theorem 4.9] proved that this holds for a set of primes of positive relative density. Bourgain *et al.* [3] proved that the conjecture holds for a set of primes of relative density 1. The same authors [4] proved the weaker result that $F(p) = O(p)$ holds for all p, and also that $F(p) \ge (p-1) - o(p)$ for all p.

Our motivation here was to similarly count solutions (g, x) to the equation

$$g^x \equiv x \bmod p^e \tag{1.2}$$

with $g, x \in \{1, \dots, p^e\}$, $p \nmid g$ and $p \nmid x$. Based on numerical evidence, we conjecture that the number of these solutions is asymptotically equivalent to $p^{e-1}(p-1)$ as p goes to infinity, and further that the number of solutions with $g \equiv i$ modulo p is asymptotically equivalent to p^{e-1} for any i as p goes to infinity. We expect that the techniques used to prove the theorems above could also be applied to this case.

We also attempted to investigate the situation as p is held fixed and e goes to infinity. This led naturally to an examination of the function $x \mapsto g^x$ where g is fixed and x ranges through the p-adic integers $\mathbb{Z}_p$, which is carried out in Sections 2 and 3. The (perhaps) surprising discovery is what happens when we look for solutions x to (1.2) not in the set $\{1, \dots, p^e\}$ but rather in the 'correct' set $\{1, \dots, p^e m\}$, where m is the multiplicative order of g modulo p. We show in Section 4 that the number of solutions in this more natural setting is exactly what one would expect from our conjectures, with no error term. (In the case where $e = 1$, [18] observes that it is easy to find fixed points outside the set $\{1, \dots, p\}$ but does not explicitly count them.) Glebsky [9] proves a similar result to ours in the case where $m = p-1$ using a very different method. (We thank Igor Shparlinski for this reference.)

The papers [13–15] also investigated three related questions: the number of two-cycles of the discrete exponential function, or solutions to

$$g^h \equiv a \bmod p \quad \text{and} \quad g^a \equiv h \bmod p, \tag{1.3}$$

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

the number of solutions to a discrete self-power equation

$$x^x \equiv c \bmod p \tag{1.4}$$

for fixed c, and the number of collisions of the discrete self-power function, that is, solutions to

$$h^h \equiv a^a \bmod p. \tag{1.5}$$

It was conjectured in these papers that the number $T(p)$ of solutions to (1.3) with $1 \le g, h, a \le p-1$ and $h \not\equiv a$ modulo p is

$$T(p) \sim p - 1,$$

the number $S(p; c)$ of solutions to (1.4) with $1 \le x \le p-1$ is

$$S(p; c) \sim \sum_{d|(p-1)/m} \frac{\phi(dm)}{dm}$$

where m is the order of c modulo p, and the number $C(p)$ of solutions to (1.5) with $1 \le h, a \le p-1$ and $h \not\equiv a$ modulo p is

$$C(p) \sim \sum_{m|(p-1)} \phi(m) \Bigg(\sum_{d|(p-1)/m} \frac{\phi(dm)}{dm} \Bigg)^2 = \sum_{d|(p-1)} \frac{J_2(d)}{d},$$

where $J_2(n) = n^2 \prod_{p|n}(1 - p^{-2})$ is Jordan's totient function, which counts the number of pairs of integers in $\{1, \dots, n\}$ that, together with n, form a mutually coprime triple. Balog *et al.* [1] established the weaker results that $S(p; c) \le p^{1/3+o(1)} m^{2/3}$ and $S(p; c) \le p^{1+o(1)} m^{-1/12}$, and that $C(p) \le p^{48/25+o(1)}$. No nontrivial theorems on $T(p)$ seem to be known up to this point, although Glebsky and Shparlinski [10] prove some relevant results when g is held fixed.

In Section 5 we investigate the number of solutions to the equations

$$g^h \equiv a \bmod p^e \quad \text{and} \quad g^a \equiv h \bmod p^e, \tag{1.6}$$

where g is fixed and h and a are in $\{1, \dots, p^e m\}$ with much the same results as before. We also indicate how to generalize this to more equations. (Some of these results are also proved in [9].) In Section 6 we similarly investigate the equation

$$x^x \equiv c \bmod p^e \tag{1.7}$$

for fixed c, and x in $\{1, \dots, p^e(p-1)\}$, and in Section 7 we investigate the equation

$$h^h \equiv a^a \bmod p^e \tag{1.8}$$

for h and a in $\{1, \dots, p^e(p-1)\}$.

The use of the discrete exponential function $x \mapsto g^x \bmod p$ for g a primitive root is well known in cryptography; its inverse is commonly referred to as the

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

discrete logarithm and computing it is one of the basic 'hard problems' of public-key cryptography (see [19, Section 3.6]). There are also uses of the function when g is not a primitive root, for example, in the Digital Signature Algorithm (see [19, Section 11.5]). Finally, a few cryptographic algorithms involve the self-power function $x \mapsto x^x \bmod p$, notably variants of the ElGamal signature scheme (see [19, Note 11.71]). The security of these cryptographic algorithms relies on the unpredictability of the inputs to these maps given the outputs. The results cited and those here go some way toward reassuring us that these maps do behave as if the inputs are randomly distributed given only basic facts known about the outputs.

We denote by $|S|$ the cardinality of a set S.

2. Interpolation

Fix $g \in \mathbb{Z}$ and let p be an odd prime. To count solutions to $g^x \equiv x \bmod p^e$, the obvious first step would be to interpolate the function $f(x) = g^x$, defined on $x \in \mathbb{Z}$, to a function on $x \in \mathbb{Z}_p$. Unfortunately, this is not possible unless $g \in 1 + p\mathbb{Z}_p$ (see, for example, [11, Section 4.6] or [17, Section II.2]). However, if we 'twist' the function slightly, then interpolation is possible.

To do this, let $\mu_{p-1} \subseteq \mathbb{Z}_p^\times$ be the set of all $(p-1)$th roots of unity. Then, for an odd prime p, the Teichmüller character

$$\omega : \mathbb{Z}_p^\times \to \mu_{p-1}$$

is a surjective homomorphism. It is known [11, Corollary 4.5.10] that $\mathbb{Z}_p^\times$ has a canonical decomposition as $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, and thus for x in $\mathbb{Z}_p^\times$ we may uniquely write $x = \omega(x)\langle x \rangle$ for some $\langle x \rangle \in 1 + p\mathbb{Z}_p$.

Proposition 2.1 (See [11, Proposition 4.6.3] and [17, Section II.2]). *For an odd prime p, let $g \in \mathbb{Z}_p^\times$ and $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, and let*

$$I_{x_0} = \{x \in \mathbb{Z} : x \equiv x_0 \bmod p - 1\} \subseteq \mathbb{Z}.$$

Then

$$f_{x_0}(x) = \omega(g)^{x_0}\langle g \rangle^x$$

defines a function on $\mathbb{Z}_p$ such that $f_{x_0}(x) = g^x$ whenever $x \in I_{x_0}$.

In fact we can push this a little further.

Proposition 2.2. *For an odd prime p, let m be any multiple of the multiplicative order of g modulo p, such that $m \mid (p-1)$. Let $g \in \mathbb{Z}_p^\times$ and $x_0 \in \mathbb{Z}/m\mathbb{Z}$, and let*

$$I_{x_0} = \{x \in \mathbb{Z} : x \equiv x_0 \bmod m\} \subseteq \mathbb{Z}.$$

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

Then

$$f_{x_0}(x) = \omega(g)^{x_0}\langle g\rangle^x$$

defines a function on $\mathbb{Z}_p$ *such that* $f_{x_0}(x) = g^x$ *whenever* $x \in I_{x_0}$.

Proof. First, $g^m \equiv 1 \bmod p$, and so $\omega(g)^m = \omega(g^m) = 1$. If $x_0, x_0' \in \mathbb{Z}/(p-1)\mathbb{Z}$ and $x_0 \equiv x_0' \bmod m$, then the two functions f_{x_0} and $f_{x_0'}$ given by Proposition 2.1 are equal and agree with g^x on $I_{x_0} \cup I_{x_0'}$. □

Also, for odd primes p, as noted in [11], these functions fit together into a function on $\mathbb{Z}_p \times \mathbb{Z}/m\mathbb{Z}$ defined by $F(x_1, x_0) = f_{x_0}(x_1)$, such that if $x \in \mathbb{Z}$ and $x \equiv x_0 \bmod m$, then $F(x, x) = f_{x_0}(x) = g^x$. Then we have a diagram:

$$\begin{array}{ccc} \mathbb{Z}_p \times \mathbb{Z}/m\mathbb{Z} & \xrightarrow{F} & \mathbb{Z}_p^\times \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/mZ & \xrightarrow{\overline{F}} & (\mathbb{Z}/p^e\mathbb{Z})^\times \end{array}$$

where the vertical arrows are the natural surjections. This commutes as a consequence of the following lemma.

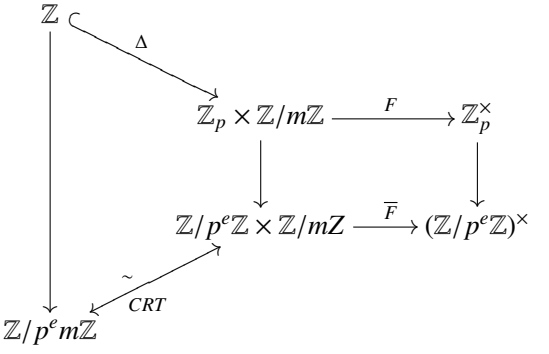
Lemma 2.3 (See [11, Corollary 4.6.2 and just below] or [16, Lemma 2.2.5]). *For any positive integer* k, $(1 + p\mathbb{Z}_p)^k \subseteq 1 + pk\mathbb{Z}_p$.

The lemma implies that $\langle g\rangle^{p^e} \equiv 1 \bmod p^e$, and therefore $\langle g\rangle^x \equiv \langle g\rangle^{x'} \bmod p^e$ when $x \equiv x' \bmod p^e$. (Recall that $\mathbb{Z}_p/p^e\mathbb{Z}_p$ is isomorphic to $\mathbb{Z}/p^e\mathbb{Z}$ for any e.)

For an odd prime p, if we let Δ be the diagonal inclusion map

$$\Delta : \mathbb{Z} \to \mathbb{Z}_p \times \mathbb{Z}/m\mathbb{Z}$$

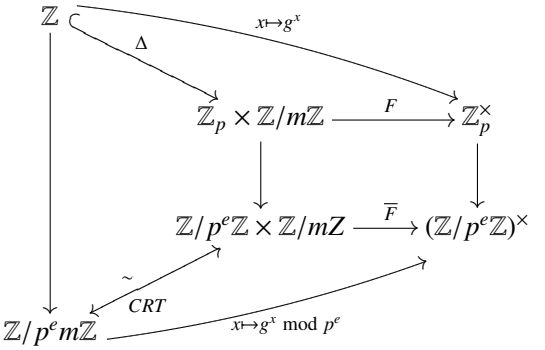
given by the canonical injection $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ and the canonical surjection $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$, then the previous diagram extends nicely to:



where the isomorphism is given by the Chinese remainder theorem. Furthermore, the composition of the maps on the top line is just the map $x \mapsto g^x$ and the composition

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

across the bottom line is the map $x \mapsto g^x \bmod p^e$:



Therefore finding all solutions (x_1, x_0) to $F(x_1, x_0) \equiv x_1 \bmod p^e$, which is the same as finding all solutions to $f_{x_0}(x_1) \equiv x_1 \bmod p^e$ for all possible $x_0 \in \mathbb{Z}/m\mathbb{Z}$, will give us all solutions to $g^x \equiv x \bmod p^e$ as x ranges over $\mathbb{Z}/p^e m\mathbb{Z}$.

3. Hensel's lemma

Definition 3.1 (See [2, Definition III.4.2.2]). A power series $f(x_1, x_2, \ldots, x_n)$ in the ring $\mathbb{Z}_p[[x_1, \ldots, x_n]]$ of formal power series with coefficients in $\mathbb{Z}_p$ is called *restricted* if

$$f(x_1, \ldots, x_n) = \sum_{(\alpha_i)} C_{\alpha_1,\alpha_2,\ldots,\alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$$

and, for every neighborhood V of 0 in $\mathbb{Z}_p$, the number of coefficients $C_{\alpha_1,\alpha_2,\ldots,\alpha_n}$ not belonging to V is finite (in other words, the family $(C_{\alpha_1,\alpha_2,\ldots,\alpha_n})$ tends to 0 in $\mathbb{Z}_p$).

In particular, the series in this paper will be p-adic convergent series such that $\lim_{|\alpha|\to\infty} |C_{\alpha_1,\alpha_2,\ldots,\alpha_n}|_p = 0$ where $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.

In this section, we include two versions of Hensel's lemma. The first version is for n restricted power series in n unknowns.

Proposition 3.2 (See [2, Corollary III.4.5.2]). *Let $f_j(x_1, x_2, \ldots, x_n)$ be a restricted power series in $\mathbb{Z}_p[[x_1, x_2, \ldots, x_n]]$ for $1 \le j \le n$. Let $(a_1, a_2, \ldots, a_n)$ be a vector in $\mathbb{Z}_p^n$ such that the determinant of the Jacobian matrix at $(a_1, a_2, \ldots, a_n)$, that is,*

$$\left| \frac{\partial(f_1, f_2, \ldots, f_n)}{\partial(x_1, x_2, \ldots, x_n)}(a_1, a_2, \ldots, a_n) \right|,$$

is in $\mathbb{Z}_p^\times$ and $f_j(a_1, a_2, \ldots, a_n) \equiv 0 \bmod p$ when $1 \le j \le n$. Then there exists a unique $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_p^n$ for which $x_i \equiv a_i \bmod p$ for $1 \le i \le n$ and $f_j(x_1, x_2, \ldots, x_n) = 0$ in $\mathbb{Z}_p$ for $1 \le j \le n$.

As a corollary we get a generalization of one of the standard formulations of Hensel's lemma to the case of restricted power series.

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

COROLLARY 3.3. *Let $f(x)$ be a restricted power series in $\mathbb{Z}_p[[x]]$ and a be in $\mathbb{Z}_p$ such that $f'(a)$ is in $\mathbb{Z}_p^\times$ and $f(a) \equiv 0 \bmod p$. Then there exists a unique $x \in \mathbb{Z}_p$ for which $x \equiv a \bmod p$ and $f(x) = 0$ in $\mathbb{Z}_p$.*

To discuss collisions below, we will also need a 'lifting lemma' for restricted power series of several variables. This will allow us to count solutions modulo higher powers of p if we know the number of solutions modulo p. The next proposition, which the second-named author learned from Igusa's 1986 'Automorphic Forms' class at Johns Hopkins University, generalizes the version of Hensel's lemma in [16, Lemma III.2.5] to restricted power series, and counts the fibers explicitly.

PROPOSITION 3.4. *Let $f(x_1, x_2, \ldots, x_n)$ be a restricted power series in $\mathbb{Z}_p[[x_1, \ldots, x_n]]$. Let*

$$N_e = \left\{ \overline{\mathbf{a}} \in (\mathbb{Z}_p/p^e\mathbb{Z}_p)^n : \frac{\partial f}{\partial x_i}(\mathbf{a}) \in \mathbb{Z}_p^\times \text{ for some } 1 \le i \le n \text{ and } f(\mathbf{a}) \equiv 0 \bmod p^e \right\}$$

for $e > 0$, where $\overline{\mathbf{a}}$ indicates reduction of $\mathbf{a}$ to the appropriate residue class. Then $\psi : N_{e+1} \to N_e$ is a well-defined canonical surjection with the cardinality of the fiber equal to p^{n-1}.

In particular, a point $\overline{\mathbf{a}} = (a_1, a_2, \ldots, a_n) \in N_e$ can be lifted in p^{n-1} different ways to a point $\overline{\mathbf{b}} = (b_1, b_2, \ldots, b_n) \in N_{e+1}$ such that $b_i \equiv a_i \bmod p^e$ for $1 \le i \le n$, so that the relationship between the cardinalities of the sets is $|N_{e+1}| = p^{n-1}|N_e|$ for $e > 0$.

4. Fixed points

THEOREM 4.1. *For an odd prime p, fix $g \in \mathbb{Z}_p^\times$ and let m be the multiplicative order of g modulo p. Then for every $x_0 \in \mathbb{Z}/m\mathbb{Z}$, there is exactly one solution to the equation*

$$\omega(g)^{x_0}\langle g\rangle^x = x$$

for $x \in \mathbb{Z}_p$.

PROOF. We start by finding solutions modulo p. We know that $\langle g\rangle \equiv 1 \bmod p$, so the equation reduces to

$$\omega(g)^{x_0} \equiv x \bmod p.$$

For fixed g and x_0, this obviously has exactly one solution.

Since we know that $\langle g\rangle$ is in $1 + p\mathbb{Z}_p$, we have that

$$\langle g\rangle^x = \exp(x \log(\langle g\rangle)) = 1 + x \log(\langle g\rangle) + x^2 \log(\langle g\rangle)^2/2! + \text{ higher-order terms in powers of } \log(\langle g\rangle)$$

where from the definition of the p-adic logarithm we know that $\log(\langle g\rangle) \in p\mathbb{Z}_p$. Therefore we have a restricted power series since $|\log(\langle g\rangle)^i/i!|_p \to 0$ as $i \to \infty$ and we can apply Corollary 3.3, which gives us a unique solution in $\mathbb{Z}_p$. □

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

COROLLARY 4.2. *For an odd prime p, fix $g \in \mathbb{Z}$ such that $p \nmid g$ and let m be the multiplicative order of g modulo p. Then there are exactly m solutions to the congruence (1.2), that is,*

$$g^x \equiv x \bmod p^e,$$

for $x \in \{1, 2, \dots, p^e m\}$. Furthermore, these solutions are all distinct modulo p^e and all distinct modulo m.

PROOF. For each $x_0 \in \mathbb{Z}/m\mathbb{Z}$, there is exactly one $x_1 \in \mathbb{Z}/p^e\mathbb{Z}$ such that

$$\omega(g)^{x_0}\langle g\rangle^{x_1} \equiv x_1 \bmod p^e,$$

by Theorem 4.1. By the Chinese remainder theorem, there will be exactly one $x \in \mathbb{Z}/p^e m\mathbb{Z}$ such that $x \equiv x_0 \bmod m$ and $x \equiv x_1 \bmod p^e$. By the interpolation set up, since $x \equiv x_0 \bmod m$, for this x,

$$g^x = \omega(g)^{x_0}\langle g\rangle^x \equiv x \bmod p^e.$$

Finally, since exactly one such x exists for each x_0, we have our m solutions to the congruence. □

5. Two-cycles

DEFINITION 5.1. For a fixed prime p and for some $g \in \mathbb{Z}$ such that $p \nmid g$, the pair (h, a) in $\{1, \dots, p^e(p-1)\}^2$, where $p \nmid h$ and $p \nmid a$, will be called a *two-cycle modulo p^e associated with g* if $h \not\equiv a \bmod p^e$, and (1.6) holds, that is,

$$g^h \equiv a \bmod p^e \quad \text{and} \quad g^a \equiv h \bmod p^e.$$

DEFINITION 5.2. We define the number $|T_e|$ of two-cycles modulo p^e as

$$\begin{aligned}|T_e| = \tfrac{1}{2}|\{&h \in \{1, \dots, p^e(p-1)\},\ p \nmid h :\\ &h \not\equiv a \bmod p^e,\ g^h \equiv a \bmod p^e,\ \text{and } g^a \equiv h \bmod p^e\\ &\text{for some } g \in (\mathbb{Z}/p^e\mathbb{Z})^\times \text{ and } a \in \{1, \dots, p^e(p-1)\},\ p \nmid a\}|.\end{aligned}$$

Thus, when we count *the number of two-cycles modulo p^e*, we will not distinguish between the two-cycle (h, a) and the two-cycle (a, h).

PROPOSITION 5.3. *For an odd prime p and a fixed $g \in \mathbb{Z}_p^\times$, let m be the multiplicative order of g modulo p. Then for every pair $(x_0, y_0) \in (\mathbb{Z}/m\mathbb{Z})^2$, there is exactly one solution $(h, a) \in \mathbb{Z}_p^2$ to the system of equations*

$$\begin{aligned}\omega(g)^{x_0}\langle g\rangle^h &= a,\\ \omega(g)^{y_0}\langle g\rangle^a &= h.\end{aligned}$$

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

PROOF. We start by finding solutions modulo p. If we let

$$f_1(h, a) = \omega(g)^{x_0}\langle g\rangle^h - a,$$
$$f_2(h, a) = \omega(g)^{y_0}\langle g\rangle^a - h,$$

then modulo p this system reduces to

$$f_1(h, a) \equiv \omega(g)^{x_0} - a \bmod p,$$
$$f_2(h, a) \equiv \omega(g)^{y_0} - h \bmod p,$$

which has exactly one solution $(h, a) = (\omega(g)^{x_0}, \omega(g)^{y_0})$ for fixed g, x_0 and y_0. The power series representations for $f_1(h, a)$ and $f_2(h, a)$ are restricted power series and

$$\frac{\partial f_1}{\partial h} = \omega(g)^{x_0}(\log(\langle g\rangle) + h\log(\langle g\rangle)^2 + \cdots) \equiv 0 \bmod p,$$
$$\frac{\partial f_1}{\partial a} = -1 \equiv -1 \bmod p,$$
$$\frac{\partial f_2}{\partial h} = -1 \equiv -1 \bmod p,$$
$$\frac{\partial f_2}{\partial a} = \omega(g)^{y_0}(\log(\langle g\rangle) + a\log(\langle g\rangle)^2 + \cdots) \equiv 0 \bmod p.$$

Thus the determinant of the Jacobian matrix is congruent to -1 modulo p, and by Proposition 3.2 the unique solution modulo p to this system lifts to a unique solution $(h, a) \in \mathbb{Z}_p^2$. □

PROPOSITION 5.4. *For an odd prime p and a fixed $g \in \mathbb{Z}$ such that $p \nmid g$, let m be the multiplicative order of g modulo p. Then if*

$$|T_{e,g}| = \tfrac{1}{2}|\{h \in \{1, \ldots, p^e m\}, p \nmid h : h \not\equiv a \bmod p^e,$$
$$g^h \equiv a \bmod p^e, \text{ and } g^a \equiv h \bmod p^e$$
$$\text{for some } a \in \{1, \ldots, p^e m\}, p \nmid a\}|$$

is the number of two-cycles modulo p^e associated with that particular g,

$$|T_{e,g}| = (m^2 - m)/2.$$

PROOF. Parallel to the proof of Corollary 4.2, for each choice of (x_0, y_0) in $(\mathbb{Z}/m\mathbb{Z})^2$, Proposition 5.3 gives us exactly one pair (h, a) in $(\mathbb{Z}/p^e m\mathbb{Z})^2$ satisfying $g^h \equiv a \bmod p^e$ and $g^a \equiv h \bmod p^e$. Thus there are m^2 such pairs total, but m of them correspond to the case where $h \equiv a \bmod p^e$. Dividing by 2 to account for swapping the roles of h and a gives us the proposition. □

THEOREM 5.5. *For a given odd prime p, the number $|T_e|$ of two-cycles is*

$$|T_e| = \sum_{m|(p-1)} \phi(m)p^{e-1}(p-1)(m-1)/2.$$

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

PROOF. First note that if an h in $\{1, \dots, p^e m\}$ forms part of a two-cycle associated with g and a, then the values in $\{1, \dots, p^e(p-1)\}$ which do the same will be exactly those which are congruent to h modulo p^e and modulo m, and thus modulo $p^e m$. So each element of $T_{e,g}$ gives rise to exactly $(p-1)/m$ elements of T_e in this fashion. On the other hand, if some a in $\{1, \dots, p^e(p-1)\}$ forms part of a two-cycle associated with h and g, then so will an a in $\{1, \dots, p^e m\}$ which is congruent to it modulo $p^e m$. So each element of $T_{e,g}$ gives rise to only one element of T_e in this fashion. Therefore

$$|T_e| = \sum_{g \in (\mathbb{Z}/p^e\mathbb{Z})^\times} \left(\frac{p-1}{m}\right) |T_{e,g}| = \sum_{m|(p-1)} \phi(m) p^{e-1}(p-1)(m-1)/2.$$

This concludes the proof. □

Alternatively, we can count rooted closed walks rather than cycles, a viewpoint which in some ways lends itself better to generalizations.

DEFINITION 5.6. For a fixed prime p and for some $g \in \mathbb{Z}$ such that $p \nmid g$, the ordered tuple $(h_1, \dots, h_k)$ is a *rooted closed walk of length k modulo p^e associated with g* if the following k equations are satisfied:

$$\begin{aligned} g^{h_1} &\equiv h_2 \bmod p^e, \\ g^{h_2} &\equiv h_3 \bmod p^e, \\ &\vdots \\ g^{h_{k-1}} &\equiv h_k \bmod p^e, \\ g^{h_k} &\equiv h_1 \bmod p^e. \end{aligned}$$

Then Corollary 4.2 is equivalent to saying that there are exactly m rooted closed walks of length 1 associated with g in $\{1, 2, \dots, p^e m\}$, and Proposition 5.4 is equivalent to saying that there are m^2 rooted closed walks of length 2 associated with g (including the fixed points) in $\{1, 2, \dots, p^e m\}^2$. In an exactly parallel manner, we can prove the following generalization.

THEOREM 5.7. *For an odd prime p and a fixed $g \in \mathbb{Z}$ such that $p \nmid g$, let m be the multiplicative order of g modulo p. Then there are exactly m^k rooted closed walks of length k modulo p^e associated with g in $\{1, 2, \dots, p^e m\}^k$. Furthermore, any two of these rooted closed walks are distinct modulo p^e and distinct modulo m.*

REMARK 5.8. In the case where $m = p - 1$, this is equivalent to [9, Theorem 1], where it is proved by combinatorial methods. For general m, our statement implies that of [9].

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

6. Self-power solutions

We now turn to the function $x \mapsto x^x \bmod p$, sometimes called the *self-power map*.

The proof of the following elementary lemma was essentially worked out in [8, Theorem 2], and the corollary was also proved by a slightly different method as [20, Theorem 1]. (We thank Lawrence Somer for bringing the latter paper to our attention.)

LEMMA 6.1. *For an odd prime p, fix $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ and let m be the multiplicative order of c modulo p. Also fix $x_0 \in \{0, 1, \ldots, p-2\}$. Then the number of solutions $x \in (\mathbb{Z}/p\mathbb{Z})^\times$ to the equivalence*

$$x^{x_0} \equiv c \bmod p$$

is

$$\begin{cases} \gcd(x_0, p-1) & \text{if } \gcd(x_0, p-1) \mid (p-1)/m, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. For a fixed integer t, the set of tth powers, $P_t = \{x^t : x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$, is a subgroup of index $\gcd(t, p-1)$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then $|P_t| = (p-1)/\gcd(t, p-1)$. If $\gcd(x_0, p-1) \nmid (p-1)/m$, then c is not in P_{x_0}, so $x^{x_0} \equiv c \bmod p$ has no solutions. Otherwise, any element of P_{x_0} is an x_0th power in exactly $\gcd(x_0, p-1)$ ways, so the equivalence has exactly $\gcd(x_0, p-1)$ solutions. □

COROLLARY 6.2. *For an odd prime p, fix $c \in (\mathbb{Z}/p\mathbb{Z})^\times$ and let m be the multiplicative order of c modulo p. Then the number of solutions $x \in \{1, 2, \ldots, p(p-1)\}$ to the equivalence $x^x \equiv c \bmod p$ such that $p \nmid x$ is given by the formula*

$$\sum_{\substack{0 \le x_0 \le p-2 \\ \gcd(x_0, p-1) \mid (p-1)/m}} \gcd(x_0, p-1) = \sum_{d \mid (p-1)/m} d\phi\left(\frac{p-1}{d}\right).$$

PROPOSITION 6.3. *For an odd prime p, fix $c \in \mathbb{Z}_p^\times$ and let m be the multiplicative order of c modulo p. Then for fixed $x_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, the number of solutions to the equation*

$$\omega(x)^{x_0} \langle x \rangle^x = c$$

for $x \in \mathbb{Z}_p^\times$ is

$$\begin{cases} \gcd(x_0, p-1) & \text{if } \gcd(x_0, p-1) \mid (p-1)/m, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. For a fixed x_0, we consider the function

$$f(x) = \omega(x)^{x_0} \langle x \rangle^x - c$$

and look for solutions $x \in \mathbb{Z}_p^\times$ to $f(x) \equiv 0 \bmod p$. Since we know that $\langle x \rangle$ is in $1 + p\mathbb{Z}_p$,

$$\langle x \rangle^x = \exp(x \log(\langle x \rangle)) = 1 + x \log(\langle x \rangle) + x^2 \log(\langle x \rangle)^2/2! + \text{higher-order terms in powers of } x \log(\langle x \rangle)$$

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

where from the definition of the p-adic logarithm we know that $\log(\langle x\rangle) \in p\mathbb{Z}_p$. Now if we consider the power series representation of $f(x)$, we see that

$$f(x) = \omega(x)^{x_0} - c + \omega(x)^{x_0} x \log(\langle x\rangle) \\ + \text{higher-order terms in } p^2\mathbb{Z}_p.$$

Since ω is constant on each of the $p-1$ disjoint cosets of $p\mathbb{Z}_p$ that cover $\mathbb{Z}_p^\times$, or by [17, Proposition 2, Section IV.2],

$$\frac{df}{dx} = \omega(x)^{x_0}[\log(\langle x\rangle) + 1] \equiv \omega(x)^{x_0} \bmod p$$

since $\log(\langle x\rangle) \in p\mathbb{Z}_p$. As $\omega(x)^{x_0} \not\equiv 0 \bmod p$, by Corollary 3.3 the number of solutions in $\mathbb{Z}_p$ is the same as the number of solutions in Lemma 6.1. □

Corollary 6.4. *For an odd prime p, fix $c \in \mathbb{Z}_p^\times$ and let m be the multiplicative order of c modulo p. Then the number of solutions to the congruence (1.7), that is,*

$$x^x \equiv c \bmod p^e,$$

for x such that $x \in \{1, 2, \ldots, p^e(p-1)\}$ and $p \nmid x$ is given by the formula

$$\sum_{\substack{0\le x_0\le p-2 \\ \gcd(x_0,p-1)\mid(p-1)/m}} \gcd(x_0, p-1) = \sum_{d\mid(p-1)/m} d\phi\Big(\frac{p-1}{d}\Big).$$

Proof. The proof is parallel to that of Corollary 4.2. □

7. Collisions

Definition 7.1. The set of solutions $(h, a) \in \{1, 2, \ldots, p(p-1)\}^2$, where $p \nmid h$ and $p \nmid a$, to the equivalence

$$h^h \equiv a^a \bmod p$$

will be denoted C_1 (for *collisions*) and we will use the notation $|C_1|$ for the number of such collisions. More generally, we will denote by $|C_e|$ the number of *collisions* $(h, a) \in \{1, 2, \ldots, p^e(p-1)\}^2$, where $p \nmid h$ and $p \nmid a$, which are solutions to the equivalence

$$h^h \equiv a^a \bmod p^e.$$

Recall that $\overline{x}$ indicates reduction of x to the appropriate residue class.

Lemma 7.2. *For fixed x_0 and $y_0 \in \{0, 1, \ldots, p-2\}$, if*

$$N_1^\times = \{(x, y) \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2 : x^{x_0} - y^{y_0} = 0 \text{ in } \mathbb{Z}/p\mathbb{Z}\},$$

then

$$|N_1^\times| = (p-1)\gcd(x_0, y_0, p-1).$$

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

PROOF. For a fixed integer t the set of tth powers, $P_t = \{x^t : x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$, is a subgroup of index $\gcd(t, p-1)$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, and $|P_t| = (p-1)/\gcd(t, p-1)$. Let $\Im = P_{x_0} \cap P_{y_0}$; then $\Im$ is a subgroup of order

$$|\Im| = \gcd(|P_{x_0}|, |P_{y_0}|) = \frac{(p-1)\gcd(x_0, y_0, p-1)}{\gcd(x_0, p-1)\gcd(y_0, p-1)}.$$

Now, we need to count all the points $(x, y) \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2$ such that $x^{x_0} \equiv y^{y_0} \bmod p$. If $x^{x_0} \equiv y^{y_0} \bmod p$ then x^{x_0} and y^{y_0} are in the set $\Im$ above. Thus,

$$|N_1^\times| = \sum_{i \in \Im} |\{x \in (\mathbb{Z}/p\mathbb{Z})^\times : x^{x_0} \equiv i \bmod p\}| \cdot |\{y \in (\mathbb{Z}/p\mathbb{Z})^\times : y^{y_0} \equiv i \bmod p\}|.$$

If $i \in \Im$, then $|\{x \in (\mathbb{Z}/p\mathbb{Z})^\times : x^{x_0} \equiv i \bmod p\}| = \gcd(x_0, p-1)$, so

$$|N_1^\times| = |\Im| \cdot \gcd(x_0, p-1) \cdot \gcd(y_0, p-1) = (p-1)\gcd(x_0, y_0, p-1),$$

as required. □

PROPOSITION 7.3. *For an odd prime p and for fixed x_0 and y_0 in $\mathbb{Z}/(p-1)\mathbb{Z}$, if we consider the function $f(h, a) = \omega(h)^{x_0}\langle h\rangle^h - \omega(a)^{y_0}\langle a\rangle^a$ for $h, a \in \mathbb{Z}_p^\times$ and let*

$$|N_1^\times| = |\{(\overline{h}, \overline{a}) \in ((\mathbb{Z}_p/p\mathbb{Z}_p)^\times)^2 : f(h, a) \equiv 0 \bmod p\}|,$$

then

$$|N_1^\times| = (p-1)\gcd(x_0, y_0, p-1).$$

PROOF. For a fixed x_0 and y_0, we look for solutions $h, a \in \mathbb{Z}_p^\times$ to $f(h, a) \equiv 0 \bmod p$. Since we know that $\langle h\rangle$ and $\langle a\rangle$ are elements in $1 + p\mathbb{Z}_p$,

$$\langle h\rangle^h = \exp(h\log(\langle h\rangle)) = 1 + h\log(\langle h\rangle) + h^2\log(\langle h\rangle)^2/2! + \text{higher-order terms in powers of } h\log(\langle h\rangle)$$

where $\log(\langle h\rangle) \in p\mathbb{Z}_p$, from the definition of the p-adic logarithm. By considering the number $|N_1^\times|$ of solutions using the power series representation of $f(h, a)$, we see that

$$f(h, a) = \omega(h)^{x_0} - \omega(a)^{y_0} + \text{ higher-order terms in } p\mathbb{Z}_p. \tag{7.1}$$

In this way, we see that

$$|N_1^\times| = |\{(\overline{h}, \overline{a}) \in ((\mathbb{Z}/p\mathbb{Z})^\times)^2 : \omega(h)^{x_0} - \omega(a)^{y_0} \equiv 0 \bmod p\}|.$$

From this expression and Lemma 7.2,

$$|N_1^\times| = (p-1)\gcd(x_0, y_0, p-1).$$

This concludes the proof. □

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

Corollary 7.4. *The number of collisions* $(h, a) \in \{1, 2, \ldots, p(p-1)\}^2$ *such that* $p \nmid h$, $p \nmid a$, *and* $h^h \equiv a^a \bmod p$, *where* p *is an odd prime, is given by the formula*

$$|C_1| = \sum_{0 \le x_0, y_0 \le p-2} (p-1)\gcd(x_0, y_0, p-1) = (p-1)\sum_{d \mid (p-1)} dJ_2((p-1)/d)$$

where $J_2(n) = n^2 \prod_{p \mid n}(1 - p^{-2})$ *is Jordan's totient function.*

Proposition 7.5. *For an odd prime* p *and for fixed* x_0 *and* $y_0 \in \mathbb{Z}/(p-1)\mathbb{Z}$, *if we consider the function* $f(h, a) = \omega(h)^{x_0}\langle h\rangle^h - \omega(a)^{y_0}\langle a\rangle^a$ *for* $h, a \in \mathbb{Z}_p^\times$ *and let*

$$N_e^\times = \{(\overline{h}, \overline{a}) \in ((\mathbb{Z}_p/p^e\mathbb{Z}_p)^\times)^2 : f(h, a) \equiv 0 \bmod p^e\},$$

then

$$|N_e^\times| = p^{e-1}|N_1^\times|.$$

Proof. Considering our series representation for $f(h, a)$ in equation (7.1) shows that

$$f(h, a) = \omega(h)^{x_0} - \omega(a)^{y_0} + \omega(h)^{x_0} h \log(\langle h\rangle) - \omega(a)^{y_0} a \log(\langle a\rangle) + \text{higher-order terms in } p^2\mathbb{Z}_p.$$

Since ω is constant on each of the $p-1$ disjoint cosets of $p\mathbb{Z}_p$ that cover $\mathbb{Z}_p^\times$, or by [17, Proposition 2, Section IV.2],

$$\frac{\partial f}{\partial h} = \omega(h)^{x_0}[\log(\langle h\rangle) + 1] \equiv \omega(h)^{x_0} \bmod p$$

since $\log(\langle h\rangle) \in p\mathbb{Z}_p$. As $\omega(h)^{x_0} \not\equiv 0 \bmod p$, by Proposition 3.4 with $n = 2$,

$$|N_e^\times| = p|N_{e-1}^\times|$$

for $e > 1$, and our proposition follows. □

Corollary 7.6. *For an odd prime* p, *there are exactly* $|C_e| = p^{e-1}|C_1|$ *collisions that are solutions to the congruence (1.8), that is,*

$$h^h \equiv a^a \bmod p^e,$$

for (h, a) *in* $\{1, 2, \ldots, p^e(p-1)\}^2$ *such that* $p \nmid h$ *and* $p \nmid a$.

Proof. The proof is parallel to that of Corollary 4.2. □

Remark 7.7. Corollaries 7.4 and 7.6 could also have been proved by squaring the results of Corollaries 6.2 and 6.4 respectively, and summing over all c.

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press

8. Conclusions and future work

Previous work on solutions to (1.1) and related equations has focused on finding how primitive roots modulo p, or specified powers of primitive roots, are distributed in arithmetic progressions contained in $\{1, \dots, p\}$ with differences dividing $p-1$. We hope that this paper shows that another course might also be fruitful: start with the solutions to an exponential equation in $\{1, \dots, p(p-1)\}$ or $\{1 \dots, p^e(p-1)\}$ and determine how they are distributed among the subintervals of length p or p^e. Furthermore, we think the use of p-adic numbers also suggests new lines of attack that may be useful in the future. For example, the ability to extend the p-adic exponential function to rings of integers in extension fields of $\mathbb{Q}_p$ might provide a useful way of looking at, or even posing, new problems in finite field extensions of $\mathbb{Z}/p\mathbb{Z}$.

In the future, we hope to consider solutions of other exponential equations, such as

$$h^{h/d} \equiv a^{a/d} \bmod p^e, \quad d = \gcd(h, a, p-1),$$

considered (with $e = 1$) in [15] as closely related to (1.3). Another problem that should be tractable using our methods is finding solutions of

$$g^{x-1+c} \equiv x \bmod p^e$$

for c fixed. This was raised in [7] (with $e = 1$) as related to 'Golomb rulers', which have applications in error correction and in controlling the effects of electromagnetic signals interference. One could also consider the 'discrete Lambert' map $x \mapsto xg^x$ for g fixed, which is related to the standard ElGamal signature scheme and the Digital Signature Algorithm much as the self-power function is related to its variants. Then one could ask for solutions of

$$xg^x \equiv c \bmod p^e$$

for fixed c, or collisions of the discrete Lambert map, namely solutions of

$$hg^h \equiv ag^a \bmod p^e.$$

Finally, for completeness one should investigate the case when $p = 2$. In this case, counting solutions modulo p is trivial, but the p-adic situation is more complicated.

Acknowledgement

The first-named author thanks the Department of Mathematics and Statistics at Mount Holyoke College for hospitality during a visit there in the spring of 2010.

References

[1] A. Balog, K. A. Broughan and I. E. Shparlinski, 'On the number of solutions of exponential congruences', *Acta Arith.* **148** (2011), 93–103.

[2] N. Bourbaki, *Commutative Algebra: Chapters 1–7*, 1st edn (Addison-Wesley, Reading, MA, 1972).

[3] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings, and fixed points of the discrete logarithm', *Int. Math. Res. Not. IMRN* **rnn090** (2008), 29.
[4] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Distribution of elements of cosets of small subgroups and applications', *Int. Math. Res. Not. IMRN* **rnr097** (2011), 42.
[5] M. Campbell, 'On fixed points for discrete logarithms' MA Thesis, University of California at Berkeley, 2003.
[6] C. Cobeli and A. Zaharescu, 'An exponential congruence with solutions in primitive roots', *Rev. Roumaine Math. Pures Appl.* **44** (1999), 15–22.
[7] K. Drakakis, 'Three challenges in Costas arrays', *Ars Combin.* **89** (2008), 167–182.
[8] R. Field, V. Gargeya, M. M. Robinson, F. Schoenberg and R. Scott, 'The Igusa local zeta function for $x^m + y^n$', Technical Report, Mount Holyoke College, 1994, available at http://arxiv.org/abs/1207.2474.
[9] L. Glebsky, 'Cycles in repeated exponentiation modulo p^n', Preprint, 2010, available at http://arxiv.org/abs/1006.2500.
[10] L. Glebsky and I. Shparlinski, 'Short cycles in repeated exponentiation modulo a prime', *Des. Codes Cryptogr.* **56** (2010), 35–42.
[11] F. Q. Gouvea, *p-adic Numbers: An Introduction*, 2nd edn (Springer, Berlin, 1997).
[12] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edn (Springer, New York, 2004).
[13] J. Holden, 'Addenda/corrigenda: fixed points and two-cycles of the discrete logarithm', Rose-Hulman Institute of Technology Mathmatical Sciences Technical Report Series 02-12, 2002, available at http://arxiv.org/abs/0208028.
[14] J. Holden, 'Fixed points and two-cycles of the discrete logarithm', in: *Algorithmic Number Theory (ANTS 2002)*, Lecture Notes in Computer Science, 2369 (eds. C. Fieker and D. R. Kohel) (Springer, Berlin, 2002), pp. 405–415.
[15] J. Holden and P. Moree, 'Some heuristics and results for small cycles of the discrete logarithm', *Math. Comp.* **75** (2006), 419–449.
[16] J. Igusa, *Lectures on Forms of Higher Degree*, 1st edn (Springer, Berlin, 1979).
[17] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd edn (Springer, New York, 1984).
[18] M. Levin, C. Pomerance and K. Soundarajan, 'Fixed points for discrete logarithms', in: *Algorithmic Number Theory (ANTS-IX)*, Lecture Notes in Computer Science, 6197 (eds. G. Hanrot, F. Morain and E. Thomé) (Springer, Berlin, 2010), pp. 6–15.
[19] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, Boca Raton, FL, 1996).
[20] L. Somer, 'The residues of n^n modulo p', *Fibonacci Quart.* **19** (1981), 110–117.
[21] W. P. Zhang, 'On a problem of Brizolis', *Pure Appl. Math. (Xi'an)* **11**(suppl.) (1995), 1–3.

JOSHUA HOLDEN, Department of Mathematics,
Rose-Hulman Institute of Technology, Terre Haute, IN 47803, USA
e-mail: holden@rose-hulman.edu

MARGARET M. ROBINSON, Department of Mathematics and Statistics,
Mount Holyoke College, 50 College Street, South Hadley, MA 01075, USA
e-mail: robinson@mtholyoke.edu

https://doi.org/10.1017/S1446788712000262 Published online by Cambridge University Press