Fields Institute Communications
Volume **00**, 0000

New Conjectures and Results for Small Cycles of the Discrete Logarithm

Joshua Holden
Department of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, IN, 47803-3999, USA
holden@rose-hulman.edu

Pieter Moree
Korteweg-de Vries Institute, Plantage Muidergracht 24, 1018 TV Amsterdam, The Netherlands
moree@science.uva.nl

Abstract. Brizolis asked the question: does every prime p have a pair (g, h) such that h is a fixed point for the discrete logarithm with base g? The first author previously extended this question to ask about not only fixed points but also two-cycles, and gave heuristics (building on work of Zhang, Cobeli, Zaharescu, Campbell, and Pomerance) for estimating the number of such pairs given certain conditions on g and h. In this paper we give a summary of conjectures and results which follow from these heuristics, building again on the aforementioned work. We also make some new conjectures and prove some average versions of the results.

1 Introduction and Statement of the Basic Equations

Paragraph F9 of [6] includes the following problem, attributed to Brizolis: given a prime $p > 3$, is there always a pair (g, h) such that g is a primitive root of p, $1 \le h \le p-1$, and

$$g^h \equiv h \mod p \ ? \tag{1}$$

In other words, is there always a primitive root g such that the discrete logarithm $\log_g$ has a fixed point? As we shall see, Zhang ([17]) not only answered the question for sufficiently large p, but also estimated the number $N(p)$ of pairs (g, h) which satisfy the equation, have g is primitive root, and also have h a primitive root which thus must be relatively prime to $p-1$. This result seems to have been discovered and proved by Zhang in [17] and later, independently, by Cobeli and Zaharescu in [3]. Campbell and Pomerance ([2], [14]) made the value of "sufficiently large" small enough that they were able to use a direct search to affirmatively answer Brizolis' original question. As in [7], we will also consider a number of variations involving side conditions on g and h.

The first author would like to thank the Rose-Hulman Institute of Technology for the special stipend which supported this project.

In [7], the first author also investigated the two-cycles of $\log_g$, that is the pairs (g, h) such that there is some a between 1 and $p-1$ such that

$$g^h \equiv a \mod p \quad \text{and} \quad g^a \equiv h \mod p. \tag{2}$$

As we observed, attacking (2) directly requires the simultaneous solution of two modular equations, presenting both computational and theoretical difficulties. Whenever possible, therefore, we instead work with the modular equation

$$h^h \equiv a^a \mod p. \tag{3}$$

Given g, h, and a as in (2), then (3) is clearly satisfied and the common value is g^{ah} modulo p. Conditions on g and h in (2) can (sometimes) be translated into conditions on h and a in (3). On the other hand, given a pair (h, a) which satisfies (3), we can attempt to solve for g such that (g, h) satisfies (2) and translate conditions on (h, a) into conditions on (g, h). Again, we will investigate using various side conditions.

Using the same notation as in [7], we will refer to an integer which is a primitive root modulo p as PR and an integer which is relatively prime to $p-1$ as RP. An integer which is both will be referred to as RPPR and one which has no restrictions will be referred to as ANY. All integers will be taken to be between 1 and $p-1$, inclusive, unless stated otherwise. If $N(p)$ is, as above, the number of solutions to (1) such that g is a primitive root and h is a primitive root which is relatively prime to $p-1$, then we will say $N(p) = F_{g\,\mathsf{PR}, h\,\mathsf{RPPR}}(p)$, and similarly for other conditions. Likewise the number of solutions to (2) will be denoted by T and the number of solutions to (3) will be denoted by C. If $\mathrm{ord}_p(g) = \mathrm{ord}_p(h)$, we say that $g\,\mathsf{ORD}\,h$.

The idea of repeatedly applying the function $x \mapsto g^x \bmod p$ is used in the famous cryptographically secure pseudorandom bit generator of Blum and Micali. ([1]; see also [12] and [5], among others, for further developments.) If one could predict that a pseudorandom generator was going to fall into a fixed point or cycle of small length, this would obviously be detrimental to cryptographic security. Our data suggests, however, that the chance that a pair (g, h) is a non-trivial two-cycle is $1/(p-1)$ for most of the conditions on choosing g and h that we have investigated. Likewise the chance that a pair (g, h) is a fixed point is generally $1/(p-1)$. This might perhaps be taken as an indication that the seed of one of these pseudorandom generators should be chosen to avoid redundant conditions which would increase the chances of a small cycle.

This paper is meant to serve as a summary of the authors' recent work. For detailed proofs and explanation we refer the reader to our forthcoming paper ([9]), in preparation. Numerical examples are provided here to illustrate the conjectures and results.

2 Conjectures and Theorems for Fixed Points

A list of conjectures and theorems on fixed points appeared in [7] and was corrected in the unpublished notes [8]. These conjectures and theorems are summarized in Table 1, which appeared in [8]. The table also contains new data collected since [7].

The first rigorous result on this subject was for $F_{g\,\mathsf{PR}, h\,\mathsf{RPPR}}(p)$. Both [17] and [3] provided bounds on the error involved; we will use notation closer to [3].

Table 1 Solutions to (1)

(a) Predicted formulas for $F(p)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	$\approx (p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$= \phi(p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$
PR	$\approx \phi(p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$
RP	$\approx \phi(p-1)$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
RPPR	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$

(b) Predicted values for $F(100057)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	100056	9139.46	30240	9139.46
PR	30240	9139.46	9139.46	9139.46
RP	30240	2762.23	9139.46	2762.23
RPPR	9139.46	2762.23	2762.23	2762.23

(c) Observed values for $F(100057)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	98506	9192	30240	9192
PR	29630	9192	9192	9192
RP	29774	2784	9037	2784
RPPR	9085	2784	2784	2784

Theorem 1 (Theorem 1 of [3]**)**

$$\left| F_{g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) - \frac{\phi(p-1)^2}{p-1} \right| \leq d(p-1)^2 \sqrt{p}(1+\ln p).$$

We next turn our attention to $F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$, for which we can prove the following result:

Theorem 2

$$|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-1)| \leq d(p-1)\sigma(p-1)\sqrt{p}(1+\ln p).$$

Unfortunately, $\sigma(n) = O(n \ln\ln n)$ in the worst case and in any case $\sigma(p-1) \geq p-1+(p-1)/2+2+1 > 3p/2$. Thus the error term overwhelms the main term. The problem occurs because we use the fact that (1) can be solved exactly when $\gcd(h, p-1) = e$ and h is a e-th power modulo p, and in fact there are exactly e such solutions. When h is RPPR then e is always 1 so counting the number of h is sufficient. When h is ANY, however, we need to count the number of h such that $\gcd(h, p-1) = e$ and h is a e-th power modulo p and then multiply by e, and do this for each divisor e of $p-1$. Thus an error of even 1 in calculating the number of h above for a large value of e will result in an error of $O(p-1)$. (We can improve the situation somewhat by separating out the elements where e is $p-1$ or $(p-1)/2$, but the results are still not what one would wish for. More details will appear in [9].)

The case where g is PR and h is ANY is very similar to the previous case, and unfortunately has the same problem:

Theorem 3

$$|F_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p)-\phi(p-1)|\le d(p-1)^2\sigma(p-1)\sqrt{p}(1+\ln p).$$

Finally, we should mention that the second author (in [11]) pointed out that we could also estimate the number $G_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p)$ of values h such that there exists *some* g satisfying (1), with $g\,\mathsf{PR}$ and $h\,\mathsf{ANY}$:

Theorem 4

$$\left|G_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p)-\frac{1}{p-1}\sum_{e|p-1}\phi\left(\frac{p-1}{e}\right)^2\right|\le d(p-1)^3\sqrt{p}(1+\ln p).$$

Similarly, we have:

Theorem 5

$$\left|G_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)-\sum_{e|p-1}\frac{1}{e}\phi\left(\frac{p-1}{e}\right)\right|\le d(p-1)^2\sqrt{p}(1+\ln p).$$

Since we are no longer counting multiple solutions for each value of h the problem mentioned above disappears; the error terms are $O(p^{1/2+\epsilon})$ while the main terms look on average like a constant times p.

3 Conjectures for Two-Cycles

Conjectures relating to equations (3) and (2) also appeared in [7] and were corrected in the unpublished notes [8]. These are summarized in Tables 2 and 3, which appeared in [8]. The table also contains new data collected since [7]. As in [7], we distinguish between the "trivial" solutions to (3), where $h=a$, and the "nontrivial" solutions.

It was observed in [7] that when neither h nor a is RP the relationship between (2) and (3) is more complicated than in the other cases. (Summaries of the conjectures in these cases are given in Tables 2 and 3.) We were able, however, to make the following conjectures about solutions to (3).

Conjecture 1

(a) $C_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)\approx(p-1)+\sum_{m|p-1}\phi(m)\left(\sum_{d|(p-1)/m}\frac{\phi(dm)}{dm}\right)^2$.

(b) *If $p-1$ is squarefree then* $C_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)\approx(p-1)+\prod_{q|p-1}\left(q+1-\frac{1}{q}\right)$, *where the product is taken over primes q dividing $p-1$.*

(c) *In general,*

$$\begin{aligned}&C_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)\\&\approx(p-1)+\prod_{q^\alpha\|p-1}\left(\left[\left(1-\frac{1}{q}\right)\alpha+1\right]^2\right.\\&\quad+\left(1-\frac{1}{q}\right)^3\left[(\alpha+1)^2\frac{q^{\alpha+1}-q}{q-1}-2(\alpha+1)\frac{\alpha q^{\alpha+2}-(\alpha+1)q^{\alpha+1}+q}{(q-1)^2}\right.\\&\qquad\left.\left.+\frac{\alpha^2q^{\alpha+3}-(2\alpha^2+2\alpha-1)q^{\alpha+2}+(\alpha^2+2\alpha+1)q^{\alpha+1}-q^2-q}{(q-1)^3}\right]\right),\end{aligned}$$

where the product is taken over primes q dividing $p-1$ and α is the exact power of q dividing $p-1$.

(d) $C_{h\,\mathsf{PR},a\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$.
(e) $C_{h\,\mathsf{ANY},a\,\mathsf{PR}}(p) \approx 2\phi(p-1)$.
(f) $C_{h\,\mathsf{PR},a\,\mathsf{PR}}(p) \approx \phi(p-1) + \phi(p-1)^2/(p-1)$.

(The formulas in Conjecture 1(a) and Conjecture 1(c) appear in [7] with typos. They appear correctly here and in [8].)

Table 2 Solutions to (3)

(a) Predicted formulas for the nontrivial part of $C(p)$

$a \setminus h$	ANY	PR	RP	RPPR
ANY	$\approx \sum \phi(m) \left(\sum \frac{\phi(dm)}{dm}\right)^2$	$\approx \phi(p-1)$	$\approx \phi(p-1)$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
PR	$\approx \phi(p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
RP	$\approx \phi(p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
RPPR	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$

(b) Predicted values for the nontrivial part of $C(100057)$

$a \setminus h$	ANY	PR	RP	RPPR
ANY	190822.0	30240	30240	2762.225
PR	30240	9139.458	9139.458	2762.225
RP	30240	9139.458	9139.458	2762.225
RPPR	2762.225	2762.225	2762.225	2762.225

(c) Observed values for the nontrivial part of $C(100057)$

$a \setminus h$	ANY	PR	RP	RPPR
ANY	190526	30226	30291	2820
PR	30226	9250	9231	2820
RP	30291	9231	9086	2820
RPPR	2820	2820	2820	2820

As observed in [7], conditions on (2) can sometimes be translated into conditions on (3) in a relatively straightforward manner. In other cases, however, things are more complicated. Let $d = \gcd(h, a, p-1)$, and let u_0 and v_0 be such that

$$u_0 h + v_0 a \equiv d \mod p-1.$$

Taking the logarithm of the two equations of (2) with respect to the same primitive root b and using Smith Normal Form, we can show that (2) is equivalent to the equations:

$$h^{h/d} \equiv a^{a/d} \mod p \quad \text{and} \quad g^d \equiv h^{v_0} a^{u_0} \mod p. \tag{4}$$

In the case where $d = \gcd(h, a, p-1) = 1$ then this becomes just

$$h^h \equiv a^a \mod p \quad \text{and} \quad g \equiv h^{v_0} a^{u_0} \mod p. \tag{5}$$

Thus:

Proposition 1 *If* $\gcd(h, a, p-1) = 1$*, then there is a one-to-one correspondence between triples* (g, h, a) *which satisfy* (2) *and pairs* (h, a) *which satisfy* (3)*, and the value of* g *is unique given* h *and* a*. In particular, this is true if* h *is* RP *or* a *is* RP*.*

In [7] it was claimed that given a pair (h, a) which is a solution to (3) we expect on the average $\gcd(a, p-1)\gcd(h, p-1)/\gcd(ha, p-1)^2$ pairs (g, h) which are solutions to (2). It is clear from (4), however, that the proper equation to look at in this case is not (3), but

$$h^{h/d} \equiv a^{a/d} \mod p. \tag{6}$$

Now we can approximate the number of nontrivial solutions of (6) using a similar birthday paradox argument to that used in [7] for Conjecture 1. The end result (see our forthcoming paper for details) is the following conjectures:

Conjecture 2

(a) $T_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$.
(b) $T_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) \approx 2(p-1)$.

and:

Conjecture 3

(a) $T_{g\,\mathsf{RP},h\bullet}(p) \approx [\phi(p-1)/(p-1)]\, T_{g\,\mathsf{ANY},h\bullet}(p)$.
(b) $T_{g\,\mathsf{RPPR},h\bullet}(p) \approx [\phi(p-1)/(p-1)]\, T_{g\,\mathsf{PR},h\bullet}(p)$.

(where $\bullet$ *stands for any one of the four conditions which we have used on* h*)*

The data from Tables 1, 2, and 3 was collected on a Beowulf cluster[1], with 19 nodes, each consisting of 2 Pentium III processors running at 1 Ghz. The programming was done in C, using MPI, OpenMP, and OpenSSL libraries. The collection took 68 hours for all values of $F(p)$, $T(p)$, and $C(p)$, for five primes p starting at 100000.

4 Averages of the Results and Conjectures

Thus far we have considered variants of Brizolis conjecture for a fixed finite field with p elements. In this section we consider average versions of these results and conjectures. The conjectures predict a main term; the results give a main term and an error term. The following sequence of lemmas gives the behavior of the main terms, on average.

The following result for $k = 1$ is well-known, see e.g. [10, 15]. For arbitrary k it was claimed by Esseen [4] (but only proved for $k = 3$). A proof can be given based on an idea of Carl Pomerance [13]. (Proofs of all of the results in this section will appear in a forthcoming paper.)

Lemma 1 *Let* k *and* C *be arbitrary real numbers with* $C > 0$*. Then*

$$\sum_{p \le x} \left(\frac{\phi(p-1)}{p-1}\right)^k = A_k \ \mathrm{Li}(x) + O_{C,k}\left(\frac{x}{\log^C x}\right),$$

where

$$A_k = \prod_p \left(1 + \frac{(1-1/p)^k - 1}{p-1}\right).$$

Given this lemma it is trivial to establish:

[1] A type of high-speed parallel computing system built out of standard PC parts.

Table 3 Solutions to (2)

(a) Predicted formulas for the nontrivial part of $T(p)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	$\approx(p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx\phi(p-1)$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
PR	$\approx\phi(p-1)$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
RP	$\approx\phi(p-1)$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^4}{(p-1)^3}$
RPPR	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^4}{(p-1)^3}$

(b) Predicted values for the nontrivial part of $T(100057)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	100056	9139.5	30240	2762.2
PR	30240	9139.5	9139.5	2762.2
RP	30240	2762.2	9139.5	834.8
RPPR	9139.5	2762.2	2762.2	834.8

(c) Observed values for the nontrivial part of $T(100057)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	100860	9231	30291	2820
PR	30850	9231	9231	2820
RP	30368	2882	9240	916
RPPR	9376	2882	2882	916

Theorem 6 *Let $C > 0$ be arbitrary. We have*

$$\sum_{p\le x} \frac{F_{g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)}{p-1} = A_2 \mathrm{Li}(x) + O_C\left(\frac{x}{\log^C x}\right).$$

Using similar lemmas, one can prove:

Theorem 7 *Let $C > 0$ be arbitrary. We have*

$$\sum_{p\le x} \frac{G_{g\mathrm{PR},h\mathrm{ANY}}(p)}{p-1} = A_1 \frac{\zeta(3)}{\zeta(2)} \mathrm{Li}(x) + O_C\left(\frac{x}{\log^C x}\right),$$

where

$$A_1 \frac{\zeta(3)}{\zeta(2)} = \prod_p \left(1 - \frac{2p}{p^3-1}\right) \approx 0.27327\ 30607\ 85299\ 15983\cdots$$

and

$$\sum_{p\le x} \frac{G_{g\mathrm{ANY},h\mathrm{ANY}}(p)}{p-1} = S\mathrm{Li}(x) + O_C\left(\frac{x}{\log^C x}\right),$$

where

$$S = \prod_p \left(1 - \frac{p}{p^3-1}\right) \approx 0.57595\ 99688\ 92945\ 43964\cdots$$

is the Stephens constant (see [16]*).*

Theorems 2 and 3 are unfortunately more problematic, due to the presence of the exceptionally large error term. The error term can probably be reduced to no larger order than the main term by separating out the most problematic cases and considering the sort of averaging we are doing in this section but the results are still conjectural at present, and the error term is still not satisfactory in any case.

On the other hand, almost all of the conjectures on (1), (3), and (2) lend themselves easily to average versions of the sort treated above. These average versions are summarized in Tables 4, 5, and 6. The data in these tables was collected on the same Beowulf cluster mentioned above, with similar software. The collection took 17 hours for all values of $\sum_{p\le x}\frac{F(p)}{p-1}$, $\sum_{p\le x}\frac{T(p)}{p-1}$, and $\sum_{p\le x}\frac{C(p)}{p-1}$, for $x = 6143$.

The results of the preceding section unfortunately do not allow us to evaluate the average value of the right hand side of Conjecture 1(a). Let us put

$$w(p) = \sum_{m|p-1}\phi(m)\left(\sum_{d|m}\frac{\phi(dm)}{dm}\right)^2.$$

Numerically it seems that

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}\frac{w(p)}{p-1} = 1.644\cdots,$$

with rather fast convergence. We are thus tempted to propose the following conjecture.

Conjecture 4 *Let $C > 0$ be arbitrary. We have*

$$\sum_{p\le x}\frac{C_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)}{p-1} = 2.644\cdots\mathrm{Li}(x) + O_C\left(\frac{x}{\log^C x}\right).$$

Although we cannot prove this at present, we can establish the following result.

Lemma 2 *For every x sufficiently large we have*

$$1.444 \le \frac{1}{\pi(x)}\sum_{p\le x}\frac{w(p)}{p-1} \le 3.422$$

Acknowledgments

Once again, the first author would like to thank the people mentioned in [7]: John Rickert, Igor Shparlinski, Mariana Campbell, and Carl Pomerance. He would also like to thank Victor Miller for the suggestion to use the Smith Normal Form.

The authors would like to thank the anonymous referees for several helpful suggestions.

References

[1] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput.*, 13(4):850–864, 1984.

[2] M. Campbell. On fixed points for discrete logarithms. Talk given at the Central Section meeting of the AMS, Bloomington, IN, April 4, 2003. Joint work with Carl Pomerance.

[3] C. Cobeli and A. Zaharescu. An exponential congruence with solutions in primitive roots. *Rev. Roumaine Math. Pures Appl.*, 44(1):15–22, 1999.

Table 4 Average Solutions to (1)

(a) Predicted approximate values for $\frac{1}{\pi(x)} \sum_{p \leq x} F(p)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	1	0.1473494000	0.3739558136	0.1473494000
PR	0.3739558136	0.1473494000	0.1473494000	0.1473494000
RP	0.3739558136	0.0608216551	0.1473494000	0.0608216551
RPPR	0.1473494000	0.0608216551	0.0608216551	0.0608216551

(b) Observed values for $x = 6143$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	0.9904034375	0.14851987375	0.37592474125	0.14851987375
PR	0.3749536975	0.14851987375	0.14851987375	0.14851987375
RP	0.3739629175	0.0612404775	0.15122619375	0.0612404775
RPPR	0.14792889125	0.0612404775	0.0612404775	0.0612404775

Table 5 Average Solutions to (3)

(a) Predicted approximate values for the nontrivial part of $\frac{1}{\pi(x)} \sum_{p \leq x} C(p)$

$a \setminus h$	ANY	PR	RP	RPPR
ANY	$1.644\cdots$	0.3739558136	0.3739558136	0.0608216551
PR	0.3739558136	0.1473494000	0.1473494000	0.0608216551
RP	0.3739558136	0.1473494000	0.1473494000	0.0608216551
RPPR	0.0608216551	0.0608216551	0.0608216551	0.0608216551

(b) Observed values for the nontrivial part for $x = 6143$

$a \setminus h$	ANY	PR	RP	RPPR
ANY	1.6113896337	0.3655877485	0.3765792535	0.060552674
PR	0.3655877485	0.14608992975	0.1478925015	0.060552674
RP	0.3765792535	0.1478925015	0.146740421	0.060552674
RPPR	0.060552674	0.060552674	0.060552674	0.060552674

[4] C.-G. Esseen. A stochastic model for primitive roots. *Rev. Roumaine Math. Pures Appl.*, 38:481–501, 1993.

[5] R. Gennaro. An improved pseudo-random generator based on discrete log. In M. Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 469–481. Springer, 2000.

[6] R. Guy. *Unsolved Problems in Number Theory.* Springer-Verlag, 1981.

[7] J. Holden. Fixed points and two-cycles of the discrete logarithm. In C. Fieker and D. R. Kohel, editors, *Algorithmic Number Theory (ANTS 2002)*, number 2369 in LNCS, pages 405–415. Springer, 2002.

[8] J. Holden. Addenda/corrigenda: Fixed points and two-cycles of the discrete logarithm, 2002. Unpublished, http://xxx.lanl.gov/abs/math.NT/0208028.

[9] J. Holden and P. Moree. Some heuristics and results for small cycles of the discrete logarithm. In preparation.

[10] P. Moree. Asymptotically exact heuristics for (near) primitive roots. *J. Number Theory*, 83:155–181, 2000.

Table 6 Average Solutions to (2)

(a) Predicted approximate values for the nontrivial part of $\frac{1}{\pi(x)}\sum_{p\le x} T(p)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	1	0.1473494000	0.3739558136	0.0608216551
PR	0.3739558136	0.1473494000	0.1473494000	0.0608216551
RP	0.3739558136	0.0608216551	0.1473494000	0.0261074463
RPPR	0.1473494000	0.0608216551	0.0608216551	0.0261074463

(b) Observed values for the nontrivial part for $x = 6143$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	0.9933146575	0.14884923375	0.3772284725	0.06150940625
PR	0.37381320625	0.14884923375	0.14884923375	0.06150940625
RP	0.36701980375	0.06089004625	0.146029115	0.02640389625
RPPR	0.14697618875	0.06089004625	0.06089004625	0.02640389625

[11] P. Moree. An exponential congruence with solutions in primitive roots (review). *Mathematical Reviews*, 2002d:11005.

[12] S. Patel and G. Sundaram. An efficient discrete log pseudo-random generator. In H. Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, pages 304–317. Springer, 1998.

[13] C. Pomerance. Personal communication.

[14] C. Pomerance. On fixed points for discrete logarithms. Talk given at the Central Section meeting of the AMS, Columbus, OH, September 22, 2001. Joint work with Mariana Campbell.

[15] P. J. Stephens. An average result for Artin's conjecture. *Mathematika*, 16:178–188, 1969.

[16] P. J. Stephens. Prime divisors of second-order linear recurrences. I. *J. Number Theory*, 8:313–332, 1976.

[17] W. P. Zhang. On a problem of Brizolis. *Pure Appl. Math.*, 11(suppl.):1–3, 1995.