10-20-2002

Fixed Point and Two-cycles of the Discrete Logarithm

Joshua Holden
Rose-Hulman Institute of Technology, holden@rose-hulman.edu

Fixed Point and Two-cycles of the Discrete Logarithm

Joshua B. Holden

Mathematical Sciences Technical Report Series
MSTR 02-12

October 20, 2002

Department of Mathematics
Rose-Hulman Institute of Technology
http://www.rose-hulman.edu/math

Fax (812)-877-8333 **Phone (812)-877-8193**

Fixed Points and Two-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

Abstract. We explore some questions related to one of Brizolis: does every prime p have a pair (g, h) such that h is a fixed point for the discrete logarithm with base g? We extend this question to ask about not only fixed points but also two-cycles. Campbell and Pomerance have not only answered the fixed point question for sufficiently large p but have also rigorously estimated the number of such pairs given certain conditions on g and h. We attempt to give heuristics for similar estimates given other conditions on g and h and also in the case of two-cycles. These heuristics are well-supported by the data we have collected, and seem suitable for conversion into rigorous estimates in the future.

1 Introduction, Previous Work, and Data on Fixed Points

In [4], paragraph F9 includes the following problem, due to Brizolis: given a prime $p > 3$, is there always a pair (g, h) such that g is a primitive root of p, $1 \leq h \leq p-1$, 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? It has been proved that the number $N(p)$ of such pairs is greater than $\phi(p-1)^2/(p-1) + O(p^{1/2+\epsilon})$, thereby showing that the answer to Brizolis' question is yes at least for sufficiently large p. This result seems to have been first proved by Zhang in [7] and later, independently, by Cobeli and Zaharescu in [2]. Campbell and Pomerance ([6]) have again rediscovered the result and made the value of "sufficiently large" small enough that they expect to be able to use a direct search to finish the problem.

This paper attempts to start a similar project for 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

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

Using the work of Campbell and Pomerance as a starting point we give heuristics for estimating the number of such pairs with and without various side conditions, and provide computational evidence to support them. We expect that the methods used by Campbell and Pomerance would also be useful in turning these heuristics into asymptotic theorems.

The first observation that Campbell and Pomerance make is that if h is a primitive root modulo p which is also relatively prime to $p-1$, then there is a unique primitive root g satisfying (1), namely $g = h^{\overline{h}}$ reduced modulo p, where $\overline{h}$ denotes the inverse of h modulo $p-1$ throughout this paper. (Note that if h is relatively prime to $p-1$ then h is a primitive root if and only if g is. Likewise, g and h have the same order modulo p if and only if h is relatively prime to $p-1$.) Their technique for estimating $N(p)$ is thus to count the number of such h. One possible underlying heuristic for this is to observe that there are $\phi(p-1)$ possibilities for h which are relatively prime to $p-1$, and we would expect each of them to be a primitive root with probability $\phi(p-1)/(p-1)$. (There are $\phi(p-1)$ primitive roots for p among the numbers between 1 and $p-1$.) This by itself gives a very accurate estimate of the number of solutions to (1) with g a primitive root and h relatively prime to $p-1$, as is shown for some sample p in Table 1. (See Section 3 for details on how the tables were computed.)

Table 1. Solutions to (1) with g PR, h RPPR

p	predicted	observed
10007	2500.5	2539
10009	1096.1	1103
10037	2115.7	2111
10039	812.6	781
10061	1603.2	1605

Campbell and Pomerance also observe that the solutions to (1) with g a primitive root and h relatively prime to $p-1$ make up a positive proportion of the solutions with g a primitive root but no restrictions on h. To obtain a heuristic for this problem which may prove useful we look at a simpler version of Brizolis' problem where g is not necessarily a primitive root. To reduce the amount of excess verbiage, in the rest of this paper 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 $N(p) = N_{(1),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)$.

With this notation, we now look at $N_{(1),g\,\mathsf{ANY},h\,\mathsf{RP}}(p)$ and $N_{(1),g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$. In the first case, h has an inverse modulo $p-1$, so as before there is a unique g for each h such that (g,h) satisfies (1). Thus $N_{(1),g\,\mathsf{ANY},h\,\mathsf{RP}}(p) = \phi(p-1)$ with no error term.

On the other hand if h is ANY then there are two possibilities. Let $d = \gcd(h, p-1)$. If h is a d-th power residue modulo p then there are d solutions g to (1), since d divides $p-1$. If h is not a a d-th power residue then there are no

solutions to (1). The number of d-th power residues modulo p is $(p-1)/d$, so the chance that h is a residue is $1/d$. Thus we expect on the average 1 pair (g,h) for every h, or $p-1$ pairs in all, giving us $N_{(1),g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) \approx p-1$. Table 2 gives evidence that this is correct.

Table 2. Solutions to (1) with g ANY, h ANY

p	predicted	observed
10007	10006	10082
10009	10008	9820
10037	10036	10249
10039	10038	10058
10061	10060	9923

Now suppose g is PR, h is ANY. The analysis is the same as in the previous case, except that now each solution g has an estimated chance of $\phi(p-1)/(p-1)$ of being a primitive root modulo p. Thus $N_{(1),g\,\mathsf{PR},h\,\mathsf{ANY}}(p) \approx \phi(p-1)$, as suggested by Table 3.

Table 3. Solutions to (1) with g PR, h ANY

p	predicted	observed
10007	5002	5079
10009	3312	3295
10037	4608	4643
10039	2856	2812
10061	4016	3987

We have not yet mentioned all of the (sixteen) possible combinations of conditions on g and h. By observations made above,

$$N_{(1),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) = N_{(1),g\,\mathsf{PR},h\,\mathsf{RP}}(p) = N_{(1),g\,\mathsf{PR},h\,\mathsf{PR}}(p) = N_{(1),g\,\mathsf{ANY},h\,\mathsf{RPPR}}(p).$$

We have not yet collected data for $N_{(1),g\,\mathsf{ANY},h\,\mathsf{PR}}(p)$ but there is every reason to believe that it is approximately $\phi(p-1)/(p-1)N_{(1),g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) \approx \phi(p-1)$ since the extra condition on h is independent in our heuristics. Likewise in the cases where g is RP or RPPR we would expect the values to be approximately $\phi(p-1)/(p-1)$ times the corresponding values where g is ANY or PR. (The case where g is RPPR is also mentioned in [4].)

In summary, we have the following:

Theorem 1 (Zhang, independently by others).

$$N_{(1),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) \approx \phi(p-1)^2/(p-1)$$

Conjecture 1.

(a) $N_{(1),g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) \approx p-1$
(b) $N_{(1),g\,\mathsf{PR},h\,\mathsf{ANY}}(p) \approx \phi(p-1)$
(c) $N_{(1),g\,\mathsf{ANY},h\,\mathsf{PR}}(p) \approx \phi(p-1)$
(d) $N_{(1),g\,\mathsf{RP},h\bullet}(p) \approx \phi(p-1)/(p-1)N_{(1),g\,\mathsf{ANY},h\bullet}(p)$
(e) $N_{(1),g\,\mathsf{RPPR},h\bullet}(p) \approx \phi(p-1)/(p-1)N_{(1),g\,\mathsf{PR},h\bullet}(p)$

2 Two-cycles: Heuristics

Attacking (2) directly requires the simultaneous solution of two modular equations, presenting both computational and theoretical difficulties. In the fixed point case we started with the situations where h was RP and we could solve (1) immediately. Similarly, in the two-cycle case we will use similar conditions to reduce the solution of two equations to the solution of one equation.

(As an aside, it should be noted that (2) is already in some sense only one equation, as a is in fact explicitly defined. Thus we could write (2) in the form

$$g^{g^h \bmod p} \equiv h \mod p \ .$$

However, this has the serious drawback of an unnatural reduction modulo p in the exponent. There does not seems to be any added insight gained from writing the equation this way which would make up for this problem.)

Consider 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). We will start with the situations where the equivalence is relatively straightforward.

If h is RP and a is ANY in (3) then we can let $g \equiv a^{\overline{h}}$ modulo p; then it is straightforward to show that we have a two-cycle with h RP and no particular condition on g. (In fact given h there is a one-to-one correspondence between instances of g which are ANY and instances of a which are ANY.) Conversely, given a two-cycle with h RP and g ANY, we have (3) with h RP and a ANY. Thus $N_{(2),g\,\mathsf{ANY},h\,\mathsf{RP}}(p) = N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p)$. Computationally, the second of these is much easier to compute; instead of looping through both g and h we only need to loop through a and record the value of each a^a modulo p and whether a was RP.

For a heuristic estimate of $N_{(2),g\,\mathsf{ANY},h\,\mathsf{RP}}(p) = N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p)$, it turns to be useful to make a distinction between two-cycles which are fixed points and "proper" two-cycles. The former correspond to the trivial solutions $h = a$ of (3). (Indeed, we saw already in the case of fixed points that we should set $g \equiv h^{\overline{h}} = a^{\overline{h}}$.) We estimated that there are approximately $\phi(p-1)$ fixed points in this case. The proper two-cycles correspond to pairs (h, a) with $h \neq a$; the values of h^h and a^a modulo p are distributed according to no obvious pattern, so given h we suppose a chance of $1/(p-1)$ that $h^h \equiv a^a$. There are $\phi(p-1)$ values of h which are RP and $p-2$ values of $a \neq h$ for an expected number of nontrivial pairs equal to $(p-1)\phi(p-1)/(p-2) \approx \phi(p-1)$. (We will ignore the $o(1)$ terms coming from $a \neq h$ in the future.)

Conjecture 2. $N_{(2),g\,\mathsf{ANY},h\,\mathsf{RP}}(p) = N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$.

Table 4 in Section 3 gives values of $N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p)$ determined by experiment which agree quite well with the estimated ones.

Adding conditions to a does not significantly complicate the analysis. If h and a are both RP in a solution to (3) then it is easy to see that this is equivalent to a solution to (2) with h RP and $\mathrm{ord}_p(g) = \mathrm{ord}_p(h)$, but no other conditions on g. We will say that $N_{(3),h\,\mathsf{RP},a\,\mathsf{RP}}(p) = N_{(2),h\,\mathsf{RP},g\,\mathsf{ORD}\,h}(p)$. We estimate this by separating the trivial and nontrivial pairs (h, a) once again. There are approximately $\phi(p-1)$ of the former and approximately $\phi(p-1)^2/(p-1)$ of the latter, since there are only $\phi(p-1)$ values of a which are RP.

Conjecture 3. $N_{(3),h\,\mathsf{RP},a\,\mathsf{RP}}(p) = N_{(2),h\,\mathsf{RP},g\,\mathsf{ORD}\,h}(p) \approx \phi(p-1)+\phi(p-1)^2/(p-1)$.

If h is RP and a is PR in a solution to (3), then this is equivalent to a solution to (2) with g PR and h RP, so $N_{(2),g\,\mathsf{PR},h\,\mathsf{RP}}(p) = N_{(3),h\,\mathsf{RP},a\,\mathsf{PR}}(p)$. In separating the trivial and nontrivial pairs it is necessary to observe that if $h = a$ then h is RPPR, so the trivial pairs contribute $\approx \phi(p-1)^2/(p-1)$. The nontrivial pairs also contribute $\approx \phi(p-1)^2/(p-1)$.

Conjecture 4. $N_{(2),g\,\mathsf{PR},h\,\mathsf{RP}}(p) = N_{(3),h\,\mathsf{RP},a\,\mathsf{PR}}(p) \approx 2\phi(p-1)^2/(p-1)$.

If either h or a is required to be RPPR in a solution to (3), then both must be. This is equivalent to a solution of (2) with g PR and h RPPR; i.e., $N_{(2),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) = N_{(3),h\,\mathsf{RPPR},a\,\mathsf{RPPR}}(p)$. The trivial pairs (h, a) contribute $\approx \phi(p-1)^2/(p-1)$. The nontrivial pairs contribute $\approx \phi(p-1)^3/(p-1)^2$, since there are $\approx \phi(p-1)^2/(p-1)$ values each of a and h which are RPPR, but the values of h^h and a^a are now constrained to be PR so there are only $\phi(p-1)$ possibilities.

Conjecture 5. $N_{(2),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) = N_{(3),h\,\mathsf{RPPR},a\,\mathsf{RPPR}}(p) \approx \phi(p-1)^2/(p-1) + \phi(p-1)^3/(p-1)^2$.

If a is RP but h is not necessarily so, then we may proceed similarly, letting $g \equiv h^{\overline{a}}$ modulo p. If a is RP and h is ANY, this is equivalent to a solution to (2) with h ANY and $\mathrm{ord}_p(g) = \mathrm{ord}_p(h)$. Thus $N_{(2),h\,\mathsf{ANY},g\,\mathsf{ORD}\,h}(p) =$

$N_{(3),h\,\mathsf{ANY},a\,\mathsf{RP}}(p)$. This of course is the same as $N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$. Similarly, if a is RP and h is PR then this is equivalent to a solution to (2) with g and h both PR, so $N_{(2),h\,\mathsf{PR},g\,\mathsf{PR}}(p) = N_{(3),h\,\mathsf{PR},a\,\mathsf{RP}}(p)$. This is the same as $N_{(3),h\,\mathsf{RP},a\,\mathsf{PR}}(p) \approx 2\phi(p-1)^2/(p-1)$.

Conjecture 6.

(a) $N_{(2),h\,\mathsf{ANY},g\,\mathsf{ORD}\,h}(p) = N_{(3),h\,\mathsf{ANY},a\,\mathsf{RP}}(p) \approx 2\phi(p-1)$.
(b) $N_{(2),h\,\mathsf{PR},g\,\mathsf{PR}}(p) = N_{(3),h\,\mathsf{PR},a\,\mathsf{RP}}(p) \approx 2\phi(p-1)^2/(p-1)$.

The heuristics for (3) so far seem to be well supported by the data (see Section 3), are easy to convert to heuristics for (2), and seem to be suitable for a rigorous approach along the lines of [6]. The situation when neither h nor a is RP is less convenient.

We will first discuss the solutions to (3), and afterwards their relationship to (2). The expected chance that a number is PR is the same as the chance that a number is RP, so we would expect $N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$, and of course the same for $N_{(3),h\,\mathsf{ANY},a\,\mathsf{PR}}(p)$. This appears to be the case. Similarly we expect $N_{(3),h\,\mathsf{PR},a\,\mathsf{PR}}(p) \approx N_{(3),h\,\mathsf{RP},a\,\mathsf{RP}}(p) \approx \phi(p-1) + \phi(p-1)^2/(p-1)$. Finally, the same heuristics predict that $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx 2(p-1)$. This does not seem to fit well with the data, however. (See Section 3.)

A finer analysis in this case is in order. (The following argument was suggested by an anonymous referee.) Fix the prime p, and let S_m be the set of h which are ANY such that $\mathrm{ord}_p(h^h) = m$. Let T_m be the set of h which are ANY such that $\mathrm{ord}_p(h) = m$. Then the estimated chance that h^h modulo p is a particular number in T_m is $|S_m|/|T_m|$ and the estimated chance that h^h and a^a are the same number modulo p is $|S_m|^2/|T_m|^2$. The number of solutions to (3) with $\mathrm{ord}_p(h^h) = \mathrm{ord}_p(a^a) = m$ is thus $\approx |S_m|^2/|T_m|$, and the total number of nontrivial solutions to (3) is $\approx \sum_{m|p-1} |S_m|^2/|T_m|$.

Now it's not hard to see that h^h has order m if and only if h has order dm for some d dividing $(p-1)/m$ and also $\gcd(h, \mathrm{ord}_p(h)) = d$. So

$$S_m = \bigcup_{d|(p-1)/m} \left(\{\mathrm{ord}_p(a) = dm\} \cap \{\gcd(a, dm) = d\}\right).$$

Supposing as we have been that conditions on order are independent of conditions on greatest common divisors, we have

$$|S_m| \approx \sum_{d|(p-1)/m} \frac{\phi(dm)\phi(m)}{dm} = \frac{\phi(m)}{m} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d} \right)$$

and

$$\sum_{m|p-1} |S_m|^2/|T_m| \approx \sum_{m|p-1} \frac{\phi(m)}{m} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d} \right).$$

Thus we estimate

$$N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx (p-1) + \sum_{m|p-1} \frac{\phi(m)}{m} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d} \right)$$

which gives much better agreement with the data.

In the case where $p-1$ is squarefree, ϕ can be treated as completely multiplicative and this can be simplified to

$$\sum_{m|p-1} \frac{\phi(m)^2}{m} \left(\sum_{d|(p-1)/m} \frac{\phi(d)}{d} \right) = \sum_{m|p-1} \left(\prod_{q|m} \frac{\phi(q)^2}{q} \right) \left(\prod_{q|(p-1)/m} \left(1 + \frac{\phi(q)}{q} \right) \right)$$
$$= \prod_{q|p-1} \left(\frac{\phi(q)^2}{q} + 1 + \frac{\phi(q)}{q} \right) = \prod_{q|p-1} \left(q + 1 - \frac{1}{q} \right).$$

Thus

$$N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx (p-1) + \prod_{q|p-1} \left(q + 1 - \frac{1}{q} \right).$$

In all cases the product is taken over primes q.

A similar analysis can be done in the general case; let $p-1 = \prod q^\alpha$ and let $m = \prod q^\beta$, then

$$|S_m| \approx \sum_{d|(p-1)/m} \frac{\phi(dm)\phi(m)}{dm} = \prod_q \phi(q^\beta) \left(\sum_{0 \le \gamma \le \alpha - \beta} \frac{\phi(q^{\alpha+\beta})}{q^{\alpha+\beta}} \right)$$
$$= \prod_q \phi(q^\beta) \left(\left(1 - \frac{1}{q} \right) (\alpha - \beta) + \frac{\phi(q^\beta)}{q^\beta} \right)$$

and

$$\sum_{m|p-1} |S_m|^2/|T_m| \approx \prod_q \left(\sum_{\beta=0}^{\alpha} \phi(q^\beta) \left[\left(1 - \frac{1}{q} \right) (\alpha - \beta) + \frac{\phi(q^\beta)}{q^\beta} \right]^2 \right)$$
$$= \prod_q \left(\left[\left(1 - \frac{1}{q} \right) \alpha + 1 \right]^2 + \sum_{\beta=1}^{\alpha} q^\beta \left(1 - \frac{1}{q} \right) \left[\left(1 - \frac{1}{q} \right) (\alpha - \beta + 1) \right]^2 \right)$$
$$= \prod_q \left(\left[\left(1 - \frac{1}{q} \right) \alpha + 1 \right]^2 \right.$$
$$+ \left(1 - \frac{1}{q} \right)^3 \left[(\alpha+1)^2 \frac{q^{\alpha+1} - q}{q-1} - 2(\alpha+1) \frac{\alpha q^{\alpha+2} - (\alpha+1)q^{\alpha+1} + q}{(q-1)^2} \right.$$
$$\left. \left. + \frac{\alpha^2 q^{\alpha+3} - (2\alpha^2 + 2\alpha - 1)q^{\alpha+2} + (\alpha^2 + 2\alpha + 1)q^{\alpha+1} - q^2 - q}{(q-1)^3} \right] \right) \quad (4)$$

To summarize:

Conjecture 7.

(a) $N_{(3),h\ \mathsf{ANY},a\ \mathsf{ANY}}(p) \approx (p-1) + \sum_{m|p-1} \frac{\phi(m)}{m} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d} \right)$.

(b) If $p-1$ is squarefree then $N_{(3),h\ \mathsf{ANY},a\ \mathsf{ANY}}(p) \approx (p-1) + \prod_{q|p-1} \left(q + 1 - \frac{1}{q} \right)$, where the product is taken over primes q dividing $p-1$.

(c) In general, $N_{(3),h\ \mathsf{ANY},a\ \mathsf{ANY}}(p) \approx (p-1)$ plus the formula given in (4).

(This finer analysis can also be carried out for the other sets of conditions on h and a that we have investigated. The reader will find that the heuristic estimates produced in these cases are the same as those that result from the coarser analyses above.)

We now turn to the the implications for $N_{(2),g\ \mathsf{ANY},h\ \mathsf{ANY}}(p)$. A solution to (2) certainly gives us a solution to (3) by letting $a \equiv g^h$ modulo p. Thus, for instance, we expect $N_{(2),g\ \mathsf{ANY},h\ \mathsf{ANY}}(p) \lessapprox N_{(3),h\ \mathsf{ANY},a\ \mathsf{ANY}}(p)$. In the other direction, given a solution to (3) we can try to solve $g^{ha} \equiv h^h$ modulo p; this will succeed $1/d$ of the time where $d = \gcd(ha, p-1)$. If there is a solution, then there are d such solutions, which look like $g\xi$ where $\xi^d \equiv 1$ modulo p. Now $(g^a)^h \equiv h^h$, so $h \equiv g^a\zeta$ for some $\zeta^{h'} \equiv 1$, $h' = \gcd(h, p-1)$. Likewise $a \equiv g^h\zeta'$ for some $\zeta'^{a'} \equiv 1$, $a' = \gcd(h, p-1)$. We want to find ξ such that $(g\xi)^a \equiv h \equiv g^a\zeta$ and $(g\xi)^h \equiv a \equiv g^h\zeta'$, or $\xi^a \equiv \zeta$ and $\xi^h \equiv \zeta'$. We would expect that the chance of this happening for a particular ξ would be $a'h'/d^2$. There are d values of ξ such that $(g\xi)^{ha} \equiv h^h$ if there are any, but g only exists $1/d$ of the time. Thus given a pair (h, a) which is a solution to (3) we expect on the average $a'h'/d^2 = \gcd(a, p-1)\gcd(h, p-1)/\gcd(ha, p-1)^2$ pairs (g, h) which are solutions to (2). If h and a are both RP then this number is 1; in general it will be less. This seems to be born out by the data as far as it goes.

3 Two-cycles: Data

Tables 4 through 7 give the number of solutions to (3) for all of the conditions on h and a discussed above, keeping in mind that conditions on h and a are symmetric. Each table was calculated in a few minutes on a home computer using Maple. Almost all of the observed data points are within a few percent of their predicted values.

Tables 8 and 9 give the number of solutions to (2) for some representative conditions on g and h. Table 8 was computed on a SPARC-station in 7.2 hours, using Maple. (Tables 1 and 3 were computed at the same time.) Table 9 was computed on a Pentium III running Linux in 3.5 hours, using Maple. (Table 2 was computed at the same time.) No particular attempts were made to optimize the code. The numbers for h RP are identical with the corresponding numbers for (3) given above.

The predicted numbers for h ANY were not calculated using the heuristics for (3) discussed above. Instead, we observed that non-trivial solutions to (2) are also equivalent to non-trivial solutions of the equation

$$g^h \equiv \log_g h$$

Table 4. Solutions to (3) with h RP

p	$N_{a\,\mathsf{ANY}}$ predicted	$N_{a\,\mathsf{ANY}}$ observed	$N_{a\,\mathsf{PR}}$ predicted	$N_{a\,\mathsf{PR}}$ observed
10007	10004	9947	5001.0	5050
10009	6624	6569	2192.1	2186
10037	9216	9092	4231.5	4174
10039	5712	5724	1625.2	1611
10061	8032	8008	3206.4	3176

Table 5. More solutions to (3) with h RP

p	$N_{a\,\mathsf{RP}}$ predicted	$N_{a\,\mathsf{RP}}$ observed	$N_{a,h\,\mathsf{RPPR}}$ predicted	$N_{a,h\,\mathsf{RPPR}}$ observed
10007	7502.5	7516	3750.5	3853
10009	4408.1	4454	1458.8	1449
10037	6723.7	6578	3087.2	3019
10039	3668.6	3690	1043.8	999
10061	5619.2	5572	2243.2	2205

Table 6. Solutions to (3) with h PR

p	$N_{a\,\mathsf{ANY}}$ predicted	$N_{a\,\mathsf{ANY}}$ observed	$N_{a\,\mathsf{PR}}$ predicted	$N_{a\,\mathsf{PR}}$ observed
10007	10004	10001	7502.5	7520
10009	6624	6491	4408.1	4356
10037	9216	9207	6723.7	6668
10039	5712	5857	3668.6	3732
10061	8032	8046	5619.2	5634

Table 7. Solutions to (3) with h ANY, a ANY

p	N predicted	N observed
10007	22516.0	22428
10009	28790.4	28434
10037	24891.5	24638
10039	27323.4	27238
10061	26137.5	26328

where the left-hand side is taken to be reduced modulo p and the right-hand side is taken as a number between 0 and $p-2$ if it exists. We assume that the left-hand and right-hand sides are distributed independently. If g is PR, there are $\phi(p-1)$ choices for g. For each g there are $p-1$ choices for h and for each one a $1/(p-1)$ chance that the left-hand and right-hand sides will coincide, for

an expected total of $\phi(p-1)$ non-trivial choices. If g is ANY, then there are $p-1$ choices for g. The right-hand side only exists if h is a power of g, but the left-hand side can only take on as many values as there are powers of g, so these factors balance out for an expected total of $p-1$. Combining these with our predictions for fixed points gives:

Conjecture 8.

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

These results agree with the observed numbers within a few percentage points. (The drawback of these heuristics compared to those derived from (3) is that they do not seem as suitable for a rigorous approach.)

Table 8. Solutions to (2) with g PR

p	$N_{h\,\mathsf{ANY}}$ predicted	$N_{h\,\mathsf{ANY}}$ observed	$N_{h\,\mathsf{RP}}$ predicted	$N_{h\,\mathsf{RP}}$ observed
10007	10004	10061	5001.0	5050
10009	6624	6479	2192.1	2186
10037	9216	9125	4231.5	4174
10039	5712	5730	1625.2	1611
10061	8032	7923	3206.4	3176

Table 9. Solutions to (2) with g ANY

p	$N_{h\,\mathsf{ANY}}$ predicted	$N_{h\,\mathsf{ANY}}$ observed	$N_{h\,\mathsf{RP}}$ predicted	$N_{h\,\mathsf{RP}}$ observed
10007	20012	20006	10004	9947
10009	20018	19628	6624	6569
10037	20072	20107	9216	9092
10039	20076	20084	5712	5724
10061	20120	19853	8032	8008

4 Applications, Conclusion, and Future Work

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 [5] and [3], 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 all 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 $1/(p-1)$ except in the case where g is chosen PR and h is chosen RPPR, in which case the chance is $1/\phi(p-1)$ due to the redundancy of the conditions. This might perhaps be taken as an indication that the seed of one of these pseudorandom generators should be chosen not to be RPPR if this is feasible. (In these protocols g is often taken to be PR as a given.)

Most of the results of this paper are perhaps not surprising. We hope, however, that the heuristics introduced will lead to rigorous bounds on the error terms for our estimates. A likely consequence of these bounds would be proofs that every prime has a pair (g, h) which is a non-trivial two-cycle given various conditions on g and h. One area which we are not able to fully develop is the relationship between $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}$ and $N_{(2),g\,\mathsf{ANY},h\,\mathsf{ANY}}$. Also, it may be possible to clean up the general formula for $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}$. More work is definitely needed in these areas. Another obvious direction for further work would be to extend our analysis to three-cycles and more generally k-cycles for small values of k.

Acknowledgments

The author would like to thank the anonymous referees for their comments, for pointing out further references, and especially for suggesting the finer analysis for $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)$ carried out above, including the formula for the squarefree case. Thanks also go to John Rickert for his help with formulas, to Igor Shparlinski for his encouragement and for pointing out references, and to Mariana Campbell and Carl Pomerance for their interest in this project.

References

1. Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput.*, 13(4):850–864, 1984.
2. Cristian Cobeli and Alexandru Zaharescu. An exponential congruence with solutions in primitive roots. *Rev. Roumaine Math. Pures Appl.*, 44(1):15–22, 1999.
3. Rosario Gennaro. An improved pseudo-random generator based on discrete log. In M. Bellare, editor, *Advances in Cryptology — CRYPTO 2000*, pages 469–481. Springer, 2000.
4. Richard K. Guy. *Unsolved Problems in Number Theory.* Springer-Verlag, 1981.
5. Sarvar Patel and Ganapathy S. Sundaram. An efficient discrete log pseudo-random generator. In H. Krawczyk, editor, *Advances in Cryptology — CRYPTO '98*, pages 304–317. Springer, 1998.
6. Carl 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.
7. Wen Peng Zhang. On a problem of Brizolis. *Pure Appl. Math.*, 11(suppl.):1–3, 1995.

Notes added after publication

(a) Several typos and formatting errors have been corrected, notably two errors in (4).

(b) Conjecture 1(c) is incorrect. In (1) if $h\,\mathsf{PR}$ then $g\,\mathsf{PR}$ also, so $N_{(1),g\,\mathsf{ANY},h\,\mathsf{PR}}(p)$ is in fact equal to $N_{(1),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)$.

(c) The same observation for (2) gives $N_{(2),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) = N_{(2),g\,\mathsf{ANY},h\,\mathsf{RPPR}}(p)$ and $N_{(2),g\,\mathsf{PR},h\,\mathsf{PR}}(p) = N_{(2),g\,\mathsf{ANY},h\,\mathsf{PR}}(p)$.

(d) In Conjectures 2 and 6(a) it should be noted that the observed values in question must be exactly equal, by the symmetry of (3). Likewise in Conjectures 4 and 6(b).

(e) The analysis in the last paragraph of Section 2 is incomplete and should be modified to reflect the role of $\gcd(h, a)$ and the fact that more than one solution to (2) may give the same solution to (3).

Addenda/Corrigenda
Fixed Points and Two-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

Abstract. This report consists of additions and corrections to the author's paper [1], which appeared in the proceedings of the ANTS V conference. The work described here was presented at the conference itself, which took place after the original paper was published. The abstract of the original paper was as follows: We explore some questions related to one of Brizolis: does every prime p have a pair (g, h) such that h is a fixed point for the discrete logarithm with base g? We extend this question to ask about not only fixed points but also two-cycles. Campbell and Pomerance have not only answered the fixed point question for sufficiently large p but have also rigorously estimated the number of such pairs given certain conditions on g and h. We attempt to give heuristics for similar estimates given other conditions on g and h and also in the case of two-cycles. These heuristics are well-supported by the data we have collected, and seem suitable for conversion into rigorous estimates in the future.

The formulas leading up to Conjecture 7 have several typos. The corrected formulas should read:

$$\sum_{m|p-1} |S_m|^2/|T_m| \approx \sum_{m|p-1} \frac{\phi(m)}{m^2} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d} \right)^2$$

$$N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx (p-1) + \sum_{m|p-1} \frac{\phi(m)}{m^2} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d} \right)^2$$

(This is also the formula which should appear in Conjecture 7(a).)

$$\sum_{m|p-1} \frac{\phi(m)^3}{m^2} \left(\sum_{d|(p-1)/m} \frac{\phi(d)}{d} \right)^2 = \sum_{m|p-1} \left(\prod_{q|m} \frac{\phi(q)^3}{q^2} \right) \left(\prod_{q|(p-1)/m} \left(1 + \frac{\phi(q)}{q} \right)^2 \right)$$

$$= \prod_{q|p-1} \left(\frac{\phi(q)^3}{q^2} + \left(1 + \frac{\phi(q)}{q}\right)^2 \right) = \prod_{q|p-1} \left(q + 1 - \frac{1}{q}\right)$$

In addition, there are two errors in (4); the equation should read:

$$\begin{aligned}
&\sum_{m|p-1} |S_m|^2/|T_m| \approx \prod_q \left(\sum_{\beta=0}^{\alpha} \phi(q^\beta) \left[\left(1 - \frac{1}{q}\right)(\alpha - \beta) + \frac{\phi(q^\beta)}{q^\beta} \right]^2 \right) \\
&= \prod_q \left(\left[\left(1 - \frac{1}{q}\right)\alpha + 1 \right]^2 + \sum_{\beta=1}^{\alpha} q^\beta \left(1 - \frac{1}{q}\right) \left[\left(1 - \frac{1}{q}\right)(\alpha - \beta + 1) \right]^2 \right) \\
&= \prod_q \left(\left[\left(1 - \frac{1}{q}\right)\alpha + 1 \right]^2 \right. \\
&\quad + \left(1 - \frac{1}{q}\right)^3 \left[(\alpha+1)^2 \frac{q^{\alpha+1} - q}{q-1} - 2(\alpha+1) \frac{\alpha q^{\alpha+2} - (\alpha+1)q^{\alpha+1} + q}{(q-1)^2} \right. \\
&\qquad \left. \left. + \frac{\alpha^2 q^{\alpha+3} - (2\alpha^2 + 2\alpha - 1)q^{\alpha+2} + (\alpha^2 + 2\alpha + 1)q^{\alpha+1} - q^2 - q}{(q-1)^3} \right] \right) \qquad (4)
\end{aligned}$$

Conjecture 1(c) is incorrect. In (1) if $h\,\mathsf{PR}$ then $g\,\mathsf{PR}$ also, so $N_{(1),g\,\mathsf{ANY},h\,\mathsf{PR}}(p)$ is in fact equal to $N_{(1),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)$.

The same observation for (2) gives $N_{(2),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) = N_{(2),g\,\mathsf{ANY},h\,\mathsf{RPPR}}(p)$ in Conjecture 5 and $N_{(2),g\,\mathsf{PR},h\,\mathsf{PR}}(p) = N_{(2),g\,\mathsf{ANY},h\,\mathsf{PR}}(p)$ in Conjecture 6(b).

In Conjectures 2 and 6(a) it should be noted that the observed values in question must be exactly equal, by the symmetry of (3). Likewise in Conjectures 4 and 6(b).

A complete and corrected list of Theorems and Conjectures follows. The numbering from the original paper has been preserved as much as possible.

Proposition 1. $N_{(1),g\,\mathsf{ANY},h\,\mathsf{RP}}(p) = \phi(p-1)$.

Theorem 1 (Zhang, independently by others).

$$\begin{aligned}
N_{(1),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) &= N_{(1),g\,\mathsf{PR},h\,\mathsf{RP}}(p) \\
&= N_{(1),g\,\mathsf{PR},h\,\mathsf{PR}}(p) \\
&= N_{(1),g\,\mathsf{ANY},h\,\mathsf{RPPR}}(p) \\
&= N_{(1),g\,\mathsf{ANY},h\,\mathsf{PR}}(p) \\
&\approx \phi(p-1)^2/(p-1)
\end{aligned}$$

Conjecture 1.

(a) $N_{(1),g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) \approx p - 1$
(b) $N_{(1),g\,\mathsf{PR},h\,\mathsf{ANY}}(p) \approx \phi(p-1)$
(c) (See above.)
(d) $N_{(1),g\,\mathsf{RP},h\bullet}(p) \approx \phi(p-1)/(p-1) N_{(1),g\,\mathsf{ANY},h\bullet}(p)$

(e) $N_{(1),g\,\mathsf{RPPR},h\bullet}(p) \approx \phi(p-1)/(p-1)N_{(1),g\,\mathsf{PR},h\bullet}(p)$

Conjecture 2.

$$\begin{aligned} N_{(2),g\,\mathsf{ANY},h\,\mathsf{RP}}(p) &= N_{(3),h\,\mathsf{RP},a\,\mathsf{ANY}}(p) \\ &\approx 2\phi(p-1). \end{aligned}$$

Conjecture 3.

$$\begin{aligned} N_{(2),h\,\mathsf{RP},g\,\mathsf{ORD}\,h}(p) &= N_{(3),h\,\mathsf{RP},a\,\mathsf{RP}}(p) \\ &\approx \phi(p-1) + \phi(p-1)^2/(p-1). \end{aligned}$$

Conjecture 4.

$$\begin{aligned} N_{(2),g\,\mathsf{PR},h\,\mathsf{RP}}(p) &= N_{(3),h\,\mathsf{RP},a\,\mathsf{PR}}(p) \\ &\approx 2\phi(p-1)^2/(p-1). \end{aligned}$$

Conjecture 5.

$$\begin{aligned} N_{(2),g\,\mathsf{PR},h\,\mathsf{RPPR}}(p) &= N_{(2),g\,\mathsf{ANY},h\,\mathsf{RPPR}}(p) \\ &= N_{(3),h\,\mathsf{RPPR},a\bullet}(p) \\ &= N_{(3),h\bullet,a\,\mathsf{RPPR}}(p) \\ &= N_{(3),h\,\mathsf{RPPR},a\,\mathsf{RPPR}}(p) \\ &\approx \phi(p-1)^2/(p-1) + \phi(p-1)^3/(p-1)^2. \end{aligned}$$

Conjecture 6.

(a)

$$\begin{aligned} N_{(2),h\,\mathsf{ANY},g\,\mathsf{ORD}\,h}(p) &= N_{(3),h\,\mathsf{ANY},a\,\mathsf{RP}}(p) \\ &\approx 2\phi(p-1). \end{aligned}$$

(b)

$$\begin{aligned} N_{(2),g\,\mathsf{PR},h\,\mathsf{PR}}(p) &= N_{(2),g\,\mathsf{ANY},h\,\mathsf{PR}}(p) \\ &= N_{(3),h\,\mathsf{PR},a\,\mathsf{RP}}(p) \\ &\approx 2\phi(p-1)^2/(p-1). \end{aligned}$$

Conjecture 7.

(a) $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx (p-1) + \sum_{m|p-1} \frac{\phi(m)}{m^2} \left(\sum_{d|(p-1)/m} \frac{\phi(dm)}{d}\right)^2$.

(b) If $p-1$ is squarefree then $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx (p-1) + \prod_{q|p-1} \left(q+1-\frac{1}{q}\right)$, where the product is taken over primes q dividing $p-1$.

(c) In general, $N_{(3),h\,\mathsf{ANY},a\,\mathsf{ANY}}(p) \approx (p-1)$ plus the formula given in (4).

(d) $N_{(3),h\,\mathsf{PR},a\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$.

(e) $N_{(3),h\,\mathsf{ANY},a\,\mathsf{PR}}(p) \approx 2\phi(p-1)$.

(f) $N_{(3),h\,\mathsf{PR},a\,\mathsf{PR}}(p) \approx \phi(p-1) + \phi(p-1)^2/(p-1)$.

Conjecture 8.

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

Conjecture 9.

(a) $N_{(2),g\,\mathsf{RP},h\bullet}(p) \approx \phi(p-1)/(p-1)N_{(2),g\,\mathsf{ANY},h\bullet}(p)$.
(b) $N_{(2),g\,\mathsf{RPPR},h\bullet}(p) \approx \phi(p-1)/(p-1)N_{(2),g\,\mathsf{PR},h\bullet}(p)$.

These conjectures are summarized in Tables A-1, A-2, and A-3, which also contain new data presented at ANTS V. This data was collected on a Beowulf cluster, 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 $N_{(\bullet),\bullet,\bullet}(p)$, for five primes p starting at 100000. Table A-4 summarizes the relationships between solutions to (2) and solutions to (3).

Table A-1. Solutions to (1)

(a) Predicted formulas for $N_{(1)}(p)$

$g \setminus h$	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 $N_{(1)}(100057)$

$g \setminus h$	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 $N_{(1)}(100057)$

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

Finally, the analysis in the last paragraph of Section 2 is incomplete. If $\gcd(h, a, p-1) = 1$, then the correspondence between solutions of (2) and solutions of (3) is one-to-one. (E.g., if $h\,\mathsf{RP}$ or $a\,\mathsf{RP}$.) If $\gcd(h, a, p-1) > 1$, however,

Table A-2. Solutions to (3)

(a) Predicted formulas for the nontrivial part of $N_{(3)}(p)$

$a \setminus h$	ANY	PR	RP	RPPR
ANY	$\approx \sum \frac{\lvert S_m \rvert^2}{\lvert T_m \rvert}$	$\approx_{\phi(p-1)}$	$\approx_{\phi(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
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 $N_{(3)}(100057)$

$a \setminus h$	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 $N_{(3)}(100057)$

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

more than one solution to (2) may give the same solution to (3). This will be explored in more detail in a forthcoming paper.

References

1. Joshua 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. http://link.springer-ny.com/link/service/series/0558/bibs/2369/23690405.htm.

Table A-3. Solutions to (2)

(a) Predicted formulas for the nontrivial part of $N_{(2)}(p)$

$g \setminus h$	ANY	PR	RP	RPPR
ANY	$\approx_{(p-1)}$	$\approx_{\phi(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$
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	$\approx_{\phi(p-1)}$	$\approx \frac{\phi(p-1)^2}{(p-1)}$	$\approx \frac{\phi(p-1)^3}{(p-1)^2}$	$\approx \frac{\phi(p-1)^4}{(p-1)^3}$
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 $N_{(2)}(100057)$

$g \setminus h$	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 $N_{(2)}(100057)$

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

Table A-4. Relationship between solutions to (2) and solutions to (3)

$a \setminus h$	ANY	PR	RP	RPPR
ANY			g ANY h RP	g PR h RPPR
PR			g PR h RP	g PR h RPPR
RP	h ANY g ORD h	g PR h PR	h RP g ORD h	g PR h RPPR
RPPR	g PR h RPPR	g PR h RPPR	g PR h RPPR	g PR h RPPR