MATHEMATICS OF COMPUTATION
Volume 75, Number 253, Pages 419–449
S 0025-5718(05)01768-0
Article electronically published on June 28, 2005

SOME HEURISTICS AND RESULTS FOR SMALL CYCLES OF THE DISCRETE LOGARITHM

JOSHUA HOLDEN AND PIETER MOREE

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 extend these heuristics and prove results for some of them, 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 [5] 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, $1 \leq h \leq p-1$, 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? As we shall see, Zhang ([18]) 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 as a primitive root, and also have h as a primitive root which thus must be relatively prime to $p-1$. This result seems to have been discovered and proved by Zhang in [18] and later, independently, by Cobeli and Zaharescu in [2]. Campbell ([1]) and Pomerance 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 [6], we will also consider a number of variations involving side conditions on g and h.

In [6], 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

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

Received by the editor January 4, 2004 and, in revised form, August 30, 2004.
2000 *Mathematics Subject Classification.* Primary 11A07; Secondary 11N37, 94A60, 11-04.
The first author would like to thank the Rose-Hulman Institute of Technology for the special stipend which supported this project during the summer of 2002.
The research of the second author was carried out while he was a visiting assistant professor at the University of Amsterdam and supported by Prof. E. M. Opdam's Pioneer Grant of the Netherlands Organization for Scientific Research (NWO).

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) that 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 [6], we will refer to an integer that is a primitive root modulo p as PR and an integer that is relatively prime to $p-1$ as RP. An integer that is both will be referred to as RPPR and one that has no restrictions will be referred to as ANY. In some instances, $\bullet$ will be used to stand for any one of these four conditions.

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 relatively prime to $p-1$, then we will say $N(p) = F_{g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)$ (F for "fixed points") and similarly for other equations and conditions. Likewise the number of solutions to (2) will be denoted by T (for "two-cycles") and the number of solutions to (3) will be denoted by C (for "collisions"). If $\operatorname{ord}_p(g) = \operatorname{ord}_p(h)$, we say that $g\,\mathsf{ORD}\,h$.

The first part of this paper focuses on solutions to (1), with Section 2 covering the basic heuristics used and the lemmas that can be proved about them. Section 3 presents the conjectures about those solutions to (1) that follow from the heuristics, and Section 4 proves some new theorems which give support to the conjectures.

The middle of the paper deals with solutions to (2) and (3). Section 5 examines the relationship between solutions of the two equations, while Section 6 presents the heuristics used to estimate the number of solutions to these two equations and the conjectures that follow from these heuristics.

The later sections of the paper deal with average versions of the conjectures and results presented in previous sections. Section 7 sets out the lemmas we need and gives average versions of the conjectures. Section 8 gives average versions of the results we have proved, where possible, and makes conjectures on the others. Section 9 discusses further work to be done along the lines of this paper.

2. The "independence" of order and GCD

The fundamental observation at the heart of the estimation of $F_{g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)$ is that if h is a primitive root modulo p that 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. Thus to estimate $N(p)$, we only need to count the number of such h; g no longer has to be considered. We observe that there are $\phi(p-1)$ possibilities for h that are relatively prime to $p-1$, and we would expect each of them to be a primitive root with probability $\phi(p-1)/(p-1)$. This heuristic uses the assumption that the condition of being a primitive root is in some sense "independent" of the condition of being relatively prime.

Heuristic 2.1. *The condition of $x\,\mathsf{RP}$ is independent of the condition that $x\,\mathsf{PR}$, in the sense that for all p,*

$$\frac{\#\{x \in \{1,\dots,p-1\}\colon x\,\mathsf{RPPR}\}}{p-1} \approx \frac{\#\{x \in \{1,\dots,p-1\}\colon x\,\mathsf{RP}\}}{p-1} \cdot \frac{\#\{x \in \{1,\dots,p-1\}\colon x\,\mathsf{PR}\}}{p-1}.$$

That this is essentially the case was proved in [18] and in [2]. We start with the key lemmas of [2]. Fix a prime p. Let

$$\mathcal{P} = \mathcal{P}(a,r,N) = \{a, a+r, \dots, a+(N-1)r\}$$

be an arithmetic progression, where a, r, and N are positive integers such that $\mathcal{P} \subseteq \{1,\dots,p\}$. Let

$$\mathcal{P}^{\mathsf{PR}} = \{x \in \mathcal{P}\colon x\,\mathsf{PR}\}$$

(this is called $\mathcal{P}'$ in [2]),

$$\mathcal{P}^{\mathsf{RP}} = \{x \in \mathcal{P}\colon x\,\mathsf{RP}\},$$

and

$$\mathcal{P}^{\mathsf{RPPR}} = \{x \in \mathcal{P}\colon x\,\mathsf{RPPR}\}.$$

Finally, for any set of integers $\mathcal{S}$, let

$$\mathcal{S}^{(k)} = \big\{x \in \mathcal{S}\colon x \equiv y^k \mod p \text{ for some } y\big\}$$

(k-th powers of x modulo p) and

$$\mathcal{S}_d = \{x \in \mathcal{S}\colon x \equiv 0 \mod d\}.$$

Then:

Lemma 2.2. *Let $\mathcal{S}$ be a set of integers and e a divisor of $p-1$. Then*

$$\#\{x \in \mathcal{S}\colon \gcd(x,p-1) = e\} = \sum_{k \mid \frac{p-1}{e}} \mu(k) \#\mathcal{S}_{ek},$$

where $\mu(k)$ is the Möbius function.

Lemma 2.3 (Lemma 4 of [2])**.** *Let $\mathcal{S}$ be a set of integers. Then*

$$\#\mathcal{S}^{\mathsf{PR}} = \sum_{k \mid p-1} \mu(k) \#\mathcal{S}^{(k)}.$$

Lemma 2.4 (Lemma 5 of [2])**.** *Let $p > 3$ be a prime number, $\mathcal{P} = \mathcal{P}(a,r,N)$, and let k and d be integers between 1 and $p-1$ such that k divides $p-1$. Then*

$$\left| \#\mathcal{P}_d^{(k)} - \frac{\#\mathcal{P}_d}{k} \right| \le \sqrt{p}(1+\ln p).$$

It should be noted that [2] only proves Lemma 2.4 for $\gcd(r,d) = 1$, but the proof goes through more generally.

Now the "independence" of RP and PR:

Lemma 2.5 (Lemma 6 of [2])**.** *Let $\mathcal{P} = \mathcal{P}(a,r,N)$ with $\gcd(r,p-1) = 1$. Then*

$$\left| \#\mathcal{P}^{\mathsf{RPPR}} - N\left(\frac{\phi(p-1)}{p-1}\right)^2 \right| \le d(p-1) + d(p-1)^2\sqrt{p}(1+\ln p).$$

As the second author observed in [13], the factors of $d(p-1)$ that occur here can in fact be improved to $\sum_{d|p-1}|\mu(d)| = 2^{\omega(p-1)}$ using the same proof; this is also done in [18]. In addition, if $p-1 \mid N$, then the first $d(p-1)$ term may be omitted.

In fact, several times in [6] the following more general heuristic was used:

Heuristic 2.6. *The order of x modulo p is independent of the greatest common divisor of x and $p-1$, in the sense that for all p,*

$$\begin{aligned}\frac{1}{p-1}\#\left\{x \in \{1,\dots,p-1\}\colon \gcd(x,p-1)=e, \quad \operatorname{ord}_p(x)=\frac{p-1}{f}\right\} \\ \approx \frac{1}{p-1}\#\{x \in \{1,\dots,p-1\}\colon \gcd(x,p-1)=e\} \\ \times \frac{1}{p-1}\#\left\{x \in \{1,\dots,p-1\}\colon \operatorname{ord}_p(x)=\frac{p-1}{f}\right\}.\end{aligned}$$

To prove a rigorous form of this we need slightly less generality in the sequence than in Lemma 2.5. (The observations on Lemma 2.5 likewise hold here.)

Lemma 2.7. *Let e and f be divisors of $p-1$, and N a multiple of $p-1$. Let $\mathcal{P}=\mathcal{P}(1,1,N)$ and*

$$\mathcal{P}'=\left\{x \in \mathcal{P}\colon \gcd(x,p-1)=e, \quad \operatorname{ord}_p(x)=\frac{p-1}{f}\right\}.$$

Then

$$\begin{aligned}\left|\#\mathcal{P}'-\frac{N}{(p-1)^2}\phi\left(\frac{p-1}{f}\right)\phi\left(\frac{p-1}{e}\right)\right| &\le d\left(\frac{p-1}{f}\right)d\left(\frac{p-1}{e}\right)\sqrt{p}(1+\ln p) \\ &\le d\,(p-1)^2\sqrt{p}(1+\ln p).\end{aligned}$$

With the use of the more general version of Lemma 2.4, the proof of Lemma 2.7 is essentially the same as that of Lemma 2.5.

An equivalent way of thinking about Heuristic 2.6 is to fix a primitive root b modulo p and say that the discrete logarithm log with base b is a "random map" considered in terms of divisibility; that is, that $\gcd(\log x, p-1)$ (which equals $(p-1)/\operatorname{ord}_p(x)$) is distributed independently of $\gcd(x,p-1)$. If we apply this discrete logarithm to (1), we get a new equation:

$$h\log g \equiv \log h \mod p-1. \tag{4}$$

Looking at (4) with the "random map" idea in mind, we see that $\gcd(g,p-1)$ seems to be independent of this equation. This is the idea underlying the following heuristic:

Heuristic 2.8. *Among solutions to* (1)*, the greatest common divisor of g and $p-1$ is independent of all other conditions on the order and the greatest common divisor*

of g and h, in the sense that for all p,

$$\begin{aligned}\frac{1}{p-1}\#\Big\{&g\colon (1)\ \textit{holds},\ \gcd(h,p-1)=e,\\ &\qquad \operatorname{ord}_p(h)=\frac{p-1}{f},\ \operatorname{ord}_p(g)=\frac{p-1}{d},\ \gcd(g,p-1)=n\Big\}\\ \approx\frac{1}{p-1}\#\Big\{&g\colon (1)\ \textit{holds},\ \gcd(h,p-1)=e,\\ &\qquad \operatorname{ord}_p(h)=\frac{p-1}{f},\ \operatorname{ord}_p(g)=\frac{p-1}{d}\Big\}\\ \times\frac{1}{p-1}\#\{&g\colon (1)\ \textit{holds},\ \gcd(g,p-1)=n\}.\end{aligned}$$

Heuristic 2.8, unlike Heuristics 2.1 and 2.6, cannot yet be made rigorous.

3. Conjectures for fixed points

The following conjectures and theorems on fixed points were listed in [6] and corrected in the unpublished notes [7].

Proposition 3.1. $F_{g\,\mathsf{ANY},h\,\mathsf{RP}}(p)=\phi(p-1)$.

Theorem 3.2 (Zhang, independently by Cobeli and Zaharescu)**.**

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

Conjecture 3.3.

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

Remark 3.4. Note that Conjecture 1(c) of [6] is incorrect. In (1), if $h\,\mathsf{PR}$, then $g\,\mathsf{PR}$ also, so $F_{g\,\mathsf{ANY},h\,\mathsf{PR}}(p)$ is equal to $F_{g\,\mathsf{PR},h\,\mathsf{RPPR}}(p)$ and not different as was originally conjectured.

Proposition 3.1 follows directly from the fact that $g=h^{\overline{h}}$. Theorem 3.2 also follows, with the application of Lemma 2.5 (that is, Heuristic 2.1). Conjecture 3.3(a) is essentially the same but we need to consider whether h is an e-th power, where $e=\gcd(h,p-1)$. Thus the conjecture uses Heuristic 2.6. More specifically, we see that (1) can be solved exactly when $\gcd(h,p-1)=e$ and h is an e-th power modulo p, and in fact there are exactly e such solutions. Thus

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)=\sum_{e\mid p-1}e\,T(e,p), \tag{5}$$

where

$$T(e,p)=\#\left\{h\in\mathcal{P}\,(1,1,p-1)^{(e)}:\ \gcd(h,p-1)=e\right\}.$$

According to Heuristic 2.6, we can model this sum using a set of independent random variables $X_1, \dots, X_{p-1}$ such that

$$X_h = \begin{cases} \gcd(h, p-1) & \text{with probability } \frac{1}{\gcd(h,p-1)}; \\ 0 & \text{otherwise.} \end{cases}$$

Then the heuristic suggests that $F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$ is approximately equal to the expected value of $X_1 + \cdots + X_{p-1}$, which is clearly $p-1$.

Conjecture 3.3(b) was justified in [6] using the argument that $g\,\mathsf{PR}$ should be independent of $\gcd(h, p-1)$ and $\operatorname{ord}_p h$. This is somewhat dubious on the face of it, since if (1) holds, then the order of g is certainly constrained by both $\gcd(h, p-1)$ and $\operatorname{ord}_p h$. The assumption is not necessary, however.

Observe first that if (4) holds with $g\,\mathsf{PR}$, then $\gcd(h, p-1) = \gcd(\log h, p-1)$. Then we apply the following elementary lemma:

Lemma 3.5. *Let* $\gcd(a, q) = \gcd(b, q) = d$. *Then the number of solutions of*

$$ax \equiv b \mod q$$

with $\gcd(x, q) = 1$ *is given by* $\phi(q)/\phi(q/d)$. *In particular, there are always between* 1 *and* d *solutions.*

Thus the number of solutions to (1) with $g\,\mathsf{PR}$ and $h\,\mathsf{ANY}$ is

$$\sum_{d|p-1} \#\left\{x \in \{1, \dots, p-1\}\colon \gcd(x, p-1) = d, \quad \operatorname{ord}_p(x) = \frac{p-1}{d}\right\} \frac{\phi(p-1)}{\phi\left((p-1)/d\right)},$$

which by Heuristic 2.6 is approximately equal to

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

This argument justifies Conjecture 3.3(b).

Conjectures 3.3(c) and 3.3(d) were justified in [6] with Heuristic 2.8; in fact the conjectures are merely special cases of the heuristic.

In Section 4, we will try to approximate the error term in Conjectures 3.3(a) and 3.3(b) using Lemma 2.7. The results, however, will not be entirely satisfactory. With this in mind, we will also use Heuristic 2.6 to model the distribution of the values of $F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$. Let $X_1, \dots, X_{p-1}$ be as above. Then we wish to find σ^2, the expected value of

$$\left(\sum_{h=1}^{p-1} X_h - (p-1)\right)^2.$$

Note that the expected value of $X_h X_j$ is $\gcd(h, p-1)$ if $h = j$ and 1 otherwise. Using this, an easy computation shows that

$$\sigma^2 = \sum_{h=1}^{p-1} \gcd(h, p-1) - (p-1) = \sum_{d|p-1} d\ \phi\left(\frac{p-1}{d}\right) - (p-1).$$

In particular, $\sigma < p^{1/2+\epsilon}$ for every $\epsilon > 0$. Thus we have the following:

Conjecture 3.6. *There are* $o(x/\ln x)$ *primes* $p \le x$ *for which*

$$|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-1)| > p^{1/2+\epsilon}$$

for every $\epsilon > 0$.

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

Some progress toward proving this conjecture is described in Section 4.

Proposition 3.1, Theorem 3.2, and Conjecture 3.3 are summarized in Table 1, which appeared in [7]. The table also contains new data collected since [6].

4. Theorems on fixed points

The first rigorous result on this subject was Theorem 3.2. Both [18] and [2] provided bounds on the error involved; we will use notation closer to [2].

Theorem 4.1 (Theorem 1 of [2])**.**

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

Proof. Apply Lemma 2.5 with $\mathcal{P} = \mathcal{P}(1,1,p-1)$. (The observations on $d(p-1)$ apply.) □

We next turn our attention to $F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$. Recall from Section 3 that its value can be expressed by (5). The quantity $T(e,p)$ that occurs there can be straightforwardly evaluated using Lemmas 2.2 and 2.4. We can also use the following characterization:

Lemma 4.2. *Let $k \mid p-1$. Then*

$$T\left(\frac{p-1}{k}, p\right) = \#\big\{j\colon 1 \le j \le k, \quad (j,k) = 1, \quad (-j)^k \equiv k^k \mod p\big\}.$$

Proof. For each integer h with $\gcd(h, p-1) = (p-1)/k$, $h = j(p-1)/k$ for some $1 \le j \le k$ with $\gcd(j,k) = 1$, such that, moreover,

$$j\,\frac{p-1}{k} \equiv x^{(p-1)/k} \mod p$$

for some integer x. It follows that

$$\left(j\,\frac{p-1}{k}\right)^k \equiv 1 \mod p$$

and hence

$$(-j)^k \equiv k^k \mod p.$$

(Note that $p \nmid k$.) On observing that if

$$z^k \equiv 1 \mod p,$$

then

$$z \equiv x^{(p-1)/k} \mod p$$

for some integer x, the proof of the reverse implication easily follows. □

We now have the following results:

Proposition 4.3. *Let $e \mid p-1$. Then*

(a) $\left|T(e,p) - \frac{1}{e}\phi\left(\frac{p-1}{e}\right)\right| \le d\left(\frac{p-1}{e}\right)\sqrt{p}(1+\ln p)$.

(b) $T(1,p) = \phi(p-1)$.

(c) *If k is a divisor of $p-1$ such that $2k^k \le p$, then* $T\left(\frac{p-1}{k}, p\right) = 0$.

(d) $0 \le T(e,p) \le \phi\left(\frac{p-1}{e}\right)$.

(e) $|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-3)| \le d(p-1)\left(\sigma(p-1) - \frac{3}{2}(p-1)\right)\sqrt{p}(1+\ln p)$.

(f) *For any E, $1 \le E \le p-1$,*

$$|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-1)| \le E\ d(p-1)^2\sqrt{p}(1+\ln p) + (p-1)d_{\frac{p-1}{E}}(p-1),$$

where

$$d_k(n) = \#\{d \mid (p-1) \colon d < k\}.$$

Proof. The cardinality of $T(e,p)$ equals

$$\begin{aligned}&\#\Big\{h \in \mathcal{P}\,(1,1,p-1)^{(e)} :\ \gcd(h,p-1) = e\Big\}\\ &= \sum_{k\mid\frac{p-1}{e}} \mu(k)\#\mathcal{P}\,(1,1,p-1)^{(e)}_{ek}\end{aligned}$$

by Lemma 2.2

$$= \sum_{k\mid\frac{p-1}{e}} \mu(k)\left[\frac{1}{e}\#\mathcal{P}\,(1,1,p-1)_{ek} + \eta_{e,k}\sqrt{p}(1+\ln p)\right]$$

for some $-1 \le \eta_{e,k} \le 1$, by Lemma 2.4

$$= \sum_{k|\frac{p-1}{e}} \mu(k) \left[\frac{1}{e} \frac{p-1}{ek} + \eta_{e,k} \sqrt{p}(1+\ln p) \right]$$

$$= \left[\left(\sum_{k|\frac{p-1}{e}} \frac{\mu(k)}{k} \right) \frac{p-1}{e^2} + \eta_e \sqrt{p}(1+\ln p) d\left(\frac{p-1}{e}\right) \right]$$

for some $-1 \le \eta_e \le 1$

$$= \frac{1}{e} \left[\phi\left(\frac{p-1}{e}\right) + \eta_e \sqrt{p}(1+\ln p) d\left(\frac{p-1}{e}\right) \right]$$

from whence part (a) follows.

Parts (b) and (d) are clear from the definition.

Part (c) follows from Lemma (4.2), since for such values of k one has

$$0 < k^k - (-j)^k < p$$

for any j between 1 and k, relatively prime to k. (This was observed by an anonymous referee.)

Part (e) follows upon noting that

$$\sum_{e|p-1} e\ T(e,p) = \sum_{e|p-1} \left[\phi\left(\frac{p-1}{e}\right) + e\ \eta_e \sqrt{p}(1+\ln p) d\left(\frac{p-1}{e}\right) \right]$$
$$= (p-1) + \eta \sqrt{p}(1+\ln p) d\,(p-1)\,\sigma(p-1)$$

for some $-1 \le \eta \le 1$ and then applying part (c).

Part (f) is similar; observe that

$$\sum_{e|p-1} e\ T(e,p)$$
$$= \sum_{\substack{e|p-1 \\ e \le E}} \left[\phi\left(\frac{p-1}{e}\right) + e\ \eta_e \sqrt{p}(1+\ln p) d\left(\frac{p-1}{e}\right) \right] + \sum_{\substack{e|p-1 \\ e > E}} e\ T(e,p)$$
$$= \sum_{\substack{e|p-1 \\ e \le E}} \left[\phi\left(\frac{p-1}{e}\right) + e\ \eta_e \sqrt{p}(1+\ln p) d\left(\frac{p-1}{e}\right) \right] + \eta' \sum_{\substack{e|p-1 \\ e > E}} e\ \phi\left(\frac{p-1}{e}\right)$$
$$= (p-1) + \sum_{\substack{e|p-1 \\ e \le E}} e\ \eta_e \sqrt{p}(1+\ln p) d\left(\frac{p-1}{e}\right) + \eta' \sum_{\substack{e|p-1 \\ e > E}} (e-1)\phi\left(\frac{p-1}{e}\right)$$
$$= (p-1) + E\ \eta\ d(p-1)^2 \sqrt{p}(1+\ln p) + \eta' \sum_{\substack{e|p-1 \\ e > E}} (p-1)$$
$$= (p-1) + E\ \eta\ d(p-1)^2 \sqrt{p}(1+\ln p) + \eta'(p-1) d_{\frac{p-1}{E}}(p-1),$$

where $-1 \le \eta \le 1$, $-1 \le \eta_e \le 1$, $-1 \le \eta' \le 1$. □

Unfortunately for part (e), $\sigma(p-1)-3(p-1)/2 = O(p\ln\ln p)$ in the worst case, although if p is a Sophie Germain prime, $\sigma(p-1)-3(p-1)/2 = 3$, and the "average case", averaging over a range of p, is $\sigma(p-1)-3(p-1)/2 \approx 0.70386(p-1)$. (See later in this section for more on Sophie Germain primes, and Sections 7 and 8 for further details of the "average case".) Thus the "error" term for $F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$ will be larger than the main term for infinitely many p. In fact, this estimate is even weaker than the rather trivial bound

$$\phi(p-1) \le F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) \le \sum_{e|p-1} e\ \phi\left(\frac{p-1}{e}\right) \le (p-1)d(p-1)$$

obtained from parts (b) and (d) of the proposition. (On the basis of a heuristic argument we conjecture that the average order of

$$\sum_{e|p-1} e\ \phi\left(\frac{p-1}{e}\right)$$

is $c_1 p\ln p$ with c_1 a positive constant.) A little thought reveals the problem: since $\#\{h \in \mathcal{P}(1,1,p-1)^{(e)}\colon \gcd(h,p-1)=e\}$ is multiplied by each divisor e of $p-1$, an error of even 1 in calculating the number of elements in the set for a large value of e will result in an error of $O(p-1)$.

Part (f) gives us something of an improvement; but it does not solve the problem in general. In order to make the term $E\ d(p-1)^2\sqrt{p}(1+\ln p)$ be even $O(p-1)$, we must pick $E < \sqrt{p-1}$, which makes $d_{\frac{p-1}{E}}(p-1) \le d(p-1)/2$ by an elementary counting of divisors. Thus the "error" term will still be of larger order than the main term.

On the other hand, the line of argument from part (e) works if we restrict to primes p for which

$$E(p) = \max\{e\colon e \mid p-1, \quad T(e,p) > 0\}$$

is not too large. (Thus, the error in $T(e,p)$ will not be multiplied by too large an e.)

Proposition 4.4. *Suppose that* $1/4 \le \beta \le 1$, $E(p) \le p^\beta$, *and* $\delta > 0$. *Then*

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = (p-1) + O_\delta\left(p^{1/2+\beta+\delta}\right).$$

More specifically,

$$|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-1)| \le p^{1/2+\beta} d(p-1)^2(2+\ln p).$$

Proof. By the assumption on $E(p)$, (5), and Proposition 4.3(a), we have

$$\begin{aligned} F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) &= \sum_{\substack{e|p-1\\ e\le p^\beta}} e\ T(e,p) \\ &= \sum_{\substack{e|p-1\\ e\le p^\beta}} \phi\left(\frac{p-1}{e}\right) + \eta_1 p^\beta d(p-1)^2\sqrt{p}(1+\ln p) \end{aligned}$$

for some $-1 \le \eta_1 \le 1$

$$= p - 1 - \left(\sum_{\substack{e \mid p-1 \\ e > p^\beta}} \phi\left(\frac{p-1}{e}\right) \right) + \eta_1 p^{1/2+\beta} d(p-1)^2 (1 + \ln p)$$

$$= p - 1 + \eta_2 d(p-1) p^{1-\beta} + \eta_1 p^{1/2+\beta} d(p-1)^2 (1 + \ln p)$$

for some $-1 \le \eta_2 \le 0$

$$= p - 1 + \eta_3 p^{1/2+\beta} d(p-1)^2 (2 + \ln p)$$

for some $-1 \le \eta_3 \le 1$

$$= p - 1 + O\left(p^{1/2+\beta+\delta}\right),$$

where we used the facts that $d(n) = O_\delta\left(n^\delta\right)$ for every $\delta > 0$ and $\phi(n) \le n$. □

Remark 4.5. One reason to consider the more specific version of this proposition is to aid in computer searches such as the one described in [1].

Proposition 4.4 is, of course, only useful if there exist sufficiently many primes satisfying $E(p) \le p^\beta$ for some appropriate β. For instance, β needs to be less than $1/2$ before the error term is less than the main term:

Corollary 4.6. *Suppose $E(p) \le p^{1/2-\delta}$ and $\delta > 0$. Then*

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = (p-1) + o(p).$$

In fact, we will prove that there are $\gg x/\ln x$ primes $p \le x$ for which $E(p) \le p^{0.3313}$ and thus that there are $\gg x/\ln x$ primes $p \le x$ such that

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = (p-1) + O\left(p^{5/6}\right).$$

The proof of this starts with the following application of Lemma 4.2:

Proposition 4.7. *Let $\delta > 0$, $\alpha \ge 2/3$. Except for $O\left(x^{3-3\alpha}/\ln^{3\alpha-1+3\delta} x\right)$ primes $p \le x$ we have*

$$E(p) < p^\alpha \ln^{\alpha+\delta} p.$$

In particular, letting $\alpha = 2/3$, except for $O\left(x/\ln^{1+3\delta} x\right)$ primes $p \le x$ we have

$$E(p) < p^{2/3} \ln^{2/3+\delta} p.$$

Proof. Let $f_\delta(x) = x^{1-\alpha}/\ln^{\alpha+\delta} x$. If $p \le x$ is a prime not dividing

$$P = \prod_{1 \le k \le f_\delta(x)} \prod_{\substack{j=1 \\ (j,k)=1}}^{k} \left((-j)^k - k^k\right),$$

then, by Lemma 4.2,

$$T\left(\frac{p-1}{k_1}, p\right) > 0$$

for some k_1 implies

$$k_1 > f_\delta(x) > \frac{p-1}{p^\alpha \ln^{\alpha+\delta} p}$$

and hence

$$E(p) < p^{\alpha} \ln^{\alpha+\delta} p.$$

The nonzero integer P has

$$O\left(\sum_{k \le f_\delta(x)} k^2 \ln k\right) = O\left(f_\delta(x)^3 \ln f_\delta(x)\right) = O\left(\frac{x^{3-3\alpha}}{\ln^{3\alpha-1+3\delta} x}\right)$$

distinct prime divisors. These are the possible exceptions to the inequality

$$E(p) < p^{\alpha} \ln^{\alpha+\delta} p.$$

□

We can now prove:

Proposition 4.8. *There are $\gg x/\ln x$ primes $p \le x$ for which $E(p) \le p^{0.3313}$.*

Proof. It is a deep result of Fouvry (see, e.g., [4]), that $\gg x/\ln x$ primes $p \le x$ are such that $p-1$ has a prime factor larger than $p^{0.6687}$. In combination with Proposition 4.7 it follows that there are $\gg x/\ln x$ primes $p \le x$ for which $E(p) < p^{0.668}$ and $p-1$ has a prime factor larger than $p^{0.6687}$. Since $E(p)$ is a divisor of $p-1$ it must divide the factors of $p-1$ besides the largest, and thus $E(p) < p^{0.3313}$ for any such primes. □

Letting $\beta = 0.3313$ and $\delta = 0.002$ in Proposition 4.4 and invoking Proposition 4.8, we now have:

Theorem 4.9. *There are $\gg x/\ln x$ primes $p \le x$ such that*

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = (p-1) + O\left(p^{5/6}\right).$$

More specifically, there are $\gg x/\ln x$ primes $p \le x$ such that

$$|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-1)| \le p^{0.8313} d(p-1)^2 (2 + \ln p).$$

Remark 4.10. If one can establish that in Fouvry's assertion, 0.6687 can be replaced by some larger θ (up to $\theta = 3/4$), then in Theorem 4.9 the exponents 5/6 and 0.8313 can be replaced by $3/2 - \theta + \delta$ and $3/2 - \theta$ for any $\delta > 0$.

The most well-known primes p with $p-1$ having a large prime factor are the Sophie Germain primes. These are the primes p such that $p - 1 = 2q$ with q a prime. For these primes it is easily shown (using Proposition 4.3(c) with $k = 1$ and $k = 2$) that

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = T(1,p) + 2T(2,p).$$

Proceeding as in the proof of Proposition 4.3(e), the following result is then obtained:

Proposition 4.11. *If p is a Sophie Germain prime, then*

$$|F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) - (p-3)| \le 2\sqrt{p}(1 + \ln p).$$

By sieving methods it can be shown that there are $\ll x/\log^2 x$ Sophie Germain primes $p \le x$. On the other hand, it is not known whether or not there are infinitely many Sophie Germain primes.

In fact, we can state a similar result for primes p of the form $p-1 = mq$ as long as q is prime and m is sufficiently small. (This was observed by an anonymous referee.)

Let W be the Lambert W function, which has the property that $W(x)e^{W(x)} = x$ for any x. Then as long as $m \le \ln(p/2)/W(\ln(p/2))$, any divisor k of m will have the property that $2k^k \le p$. Thus Proposition 4.3(c) gives us

$$F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = \sum_{e|m} e\ T(e,p)$$

and thus:

Proposition 4.12. *If p is a prime as described above, then*

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

(The factor $2d(m)\sigma(m)$ can sometimes be improved, as was the case for Sophie Germain primes.)

It is also worth asking how large $E(p)$ can be with respect to p. We put forward the following conjecture:

Conjecture 4.13. *Let $\alpha < 1$. There exist infinitely many primes p with $E(p) > p^\alpha$.*

The idea is that amongst the numbers of the form

$$k^k - (-j)^k, \quad 1 \le j \le k, \quad \gcd(j,k) = 1,$$

there will be many that are close to being a prime and that if q is a large prime divisor of such a number, then $E(q)$ will be large. Taking $k = 29$ and $j = 5$ we infer, for example, that the prime

$$q = \frac{29^{29} + 5^{29}}{34}$$

satisfies $E(q) > q^{0.964}$. If k is odd and

$$q = k^k - (-j)^k$$

is a prime for some $1 \le j \le k$, then $E(q) > (q-1)^{1-1/k}$.

Turning back to the general case, the situation where g is PR and h is ANY follows the argument explained in the justification of Conjecture 3.3(b), and uses Lemma 2.7 to estimate the error term. It is very similar to the previous case, and unfortunately has the same problem in the general case:

Proposition 4.14.

(a)

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

(b) *For any E, $1 \le E \le p-1$,*

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

We can proceed in the same fashion as Theorem 4.9, however, to prove:

Theorem 4.15. *There are $\gg x/\ln x$ primes $p \le x$ such that*

$$F_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p) = \phi(p-1) + O\left(p^{5/6}\right).$$

More specifically, there are $\gg x/\ln x$ primes $p \le x$ such that

$$|F_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p) - \phi(p-1)| \le p^{0.8313}d(p-1)^3(2+\ln p).$$

Finally, we should mention that the second author (in [13]) 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 $h\,\mathsf{ANY}$. From

$$G_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = \sum_{e|p-1} \#\Big\{h\colon \operatorname{ord}_p h = \frac{p-1}{e},\ \gcd(h,p-1)=e\Big\},$$

it was shown:

Theorem 4.16.

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

Similarly, we can estimate

$$G_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p) = \sum_{e|p-1} \#\Big\{h\in\mathcal{P}(1,1,p-1)^{(e)}\colon\ \gcd(h,p-1)=e\Big\},$$

giving:

Theorem 4.17.

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

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

(For completeness, we should note that if h is RP and/or PR, then

$$G_{g\bullet,h\bullet}(p) = F_{(1),g\bullet,h\bullet}(p).$$

Heuristic 2.8 would also predict that

$$G_{g\,\mathsf{RP},h\bullet}(p) \approx \phi(p-1)/(p-1)G_{g\,\mathsf{ANY},h\bullet}(p)$$

and

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

5. Equivalence of the equations for two-cycles

As observed in [6], conditions on (2) can sometimes be translated into conditions on (3) in a relatively straightforward manner. Table 2, reproduced from [7], summarizes these straightforward relationships.

We can go slightly further, however. Taking the logarithm of the two equations of (2) with respect to the same primitive root b gives us new equations:

$$\begin{aligned} h\log g &\equiv \log a \mod p-1;\\ a\log g &\equiv \log h \mod p-1. \end{aligned} \tag{6}$$

Let $d=\gcd(h,a,p-1)$, and let u_0 and v_0 be such that

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

TABLE 2. 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

By using the Smith Normal Form, we can show that (6) is equivalent to the equations:

$$\begin{aligned} 0 &\equiv \frac{h}{d}\log h - \frac{a}{d}\log a \mod p-1; \\ d\log g &\equiv v_0 \log h + u_0 \log a \mod p-1, \end{aligned} \tag{7}$$

or:

$$\begin{aligned} h^{h/d} &\equiv a^{a/d} \mod p; \\ g^d &\equiv h^{v_0} a^{u_0} \mod p. \end{aligned} \tag{8}$$

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

$$\begin{aligned} h^h &\equiv a^a \mod p; \\ g &\equiv h^{v_0} a^{u_0} \mod p. \end{aligned} \tag{9}$$

Thus:

Proposition 5.1. *If* $\gcd(h, a, p-1) = 1$*, then there is a one-to-one correspondence between triples* (g, h, a) *that satisfy* (2) *and pairs* (h, a) *that 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*.*

It was observed in [6] that when neither h nor a is RP the relationship between (2) and (3) is less clear. It was claimed there that given a pair (h, a) that is a solution to (3) we expect on average $\gcd(a, p-1)\gcd(h, p-1)/\gcd(ha, p-1)^2$ pairs (g, h) that are solutions to (2).

It is clear from (8), however, that when $d = \gcd(h, a, p-1) \neq 1$ this is not the correct way to think about things. The proper equation to look at in this case is not (3), but

$$h^{h/d} \equiv a^{a/d} \mod p. \tag{10}$$

We will use C' to denote the number of solutions to (10).

Now (8) shows that a nontrivial solution to (10) produces d pairs (g, h) which are nontrivial solutions to (2) if $h^{v_0} a^{u_0}$ is a d-th power modulo p, and otherwise no solutions. (As in [6], we consider the "trivial" solutions to (2) to be the ones that are also solutions to (1).) Thus the following heuristic implies that every nontrivial solution to (10) produces on average one pair (g, h) that is a nontrivial solution to (2).

TABLE 3. Relationship between solutions to (2) and solutions to (10)

$g \setminus h$	ANY	PR	RP	RPPR
ANY	h ANY, a ANY $\mathbb{E}(T/C') \approx 1$	h PR a RP	h RP a ANY	h RPPR a RPPR
PR	h ANY, a ANY $\mathbb{E}(T/C') \approx \frac{\phi(p-1)}{p-1}$	h PR a RP	h RP a PR	h RPPR a RPPR

Heuristic 5.2. *For any pair (h,a), let $d = \gcd(h,a,p-1)$, and let u_0 and v_0 be such that*

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

Then $(h,a) \mapsto h^{v_0}a^{u_0}$ is a random map, even when restricted to $\gcd(h,a,p-1) = d$, in the sense that

$$\frac{\#\{(h,a)\colon h^{v_0}a^{u_0} \equiv y \mod p,\ \gcd(h,a,p-1)=d\}}{\#\{(h,a)\colon \gcd(h,a,p-1)=d\}} \approx \frac{1}{\#\{y \in \{1,\dots,p-1\}\}}.$$

On the other hand, there is a solution to (8) with g PR if and only if $h^{v_0}a^{u_0}$ is exactly a d-th power modulo p; that is, $\operatorname{ord}_p(h^{v_0}a^{u_0}) = (p-1)/d$. Then Lemma 3.5 says that the number of such solutions is $\phi(p-1)/\phi((p-1)/d)$. Thus Heuristic 5.2 implies that every solution to (10) produces on average $\phi(p-1)/(p-1)$ pairs (g,h) that are solutions to (2) with g PR. These relationships between conditions on (2) and conditions on (10) are summarized in Table 3, where $\mathbb{E}(T/C')$ is the expected number of solutions to (2) given a solution to (10).

6. Heuristics and conjectures for two-cycles

We mentioned in Section 2 that we could view $x \mapsto \log x$ as a "random map" in some sense. We will also suppose that the map $x \mapsto x^x \mod p$ is "random", in a slightly different sense.

Heuristic 6.1. *The map $x \mapsto x^x \mod p$ is a random map given the obvious restrictions on order in the sense that for all p, given $y \in \{1,\dots,p-1\}$, then*

$$\#\{x \in \{1,\dots,p-1\}\colon x^x \equiv y \mod p\} \approx \frac{\#\{z \in \{1,\dots,p-1\}\colon (\operatorname{ord}_p z)/\gcd(z,\operatorname{ord}_p z) = \operatorname{ord}_p y\}}{\#\{w \in \{1,\dots,p-1\}\colon \operatorname{ord}_p w = \operatorname{ord}_p y\}}.$$

(The fraction on the right-hand side was referred to in [6] as $\#S_m/\#T_m$, where $m = \operatorname{ord}_p y$. The arguments there used this heuristic implicitly.)

In fact, we would like a slightly stronger version of this:

Heuristic 6.2. *The map $x \mapsto x^x \mod p$ is a random map, even when restricted to a specific order and greatest common divisor, in the sense that for all p, given $y \in \{1,\dots,p-1\}$ such that $\operatorname{ord}_p y = f/\gcd(e,f)$, then*

$$\#\{x \in \{1,\dots,p-1\}\colon x^x \equiv y \mod p,\ \gcd(x,p-1)=e,\ \operatorname{ord}_p x = f\} \approx \frac{\#\{z \in \{1,\dots,p-1\}\colon \gcd(z,p-1)=e,\ \operatorname{ord}_p z = f\}}{\#\{w \in \{1,\dots,p-1\}\colon \operatorname{ord}_p w = \operatorname{ord}_p y\}}.$$

Heuristic 6.2, like Heuristic 2.8, cannot yet be made rigorous.

Using Proposition 5.1 and Heuristic 6.2, we have the following conjectures from [6], as corrected in [7].

Conjecture 6.3.

(a) $T_{g\,\mathsf{ANY},h\,\mathsf{RP}}(p) = C_{h\,\mathsf{RP},a\,\mathsf{ANY}}(p) \approx 2\phi(p-1)$.
(b) $T_{h\,\mathsf{RP},g\,\mathsf{ORD}\,h}(p) = C_{h\,\mathsf{RP},a\,\mathsf{RP}}(p) \approx \phi(p-1) + \phi(p-1)^2/(p-1)$.
(c) $T_{g\,\mathsf{PR},h\,\mathsf{RP}}(p) = C_{h\,\mathsf{RP},a\,\mathsf{PR}}(p) \approx 2\phi(p-1)^2/(p-1)$.
(d)

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

(e) $T_{h\,\mathsf{ANY},g\,\mathsf{ORD}\,h}(p) = C_{h\,\mathsf{ANY},a\,\mathsf{RP}}(p) \approx 2\phi(p-1)$.
(f) $T_{g\,\mathsf{PR},h\,\mathsf{PR}}(p) = T_{g\,\mathsf{ANY},h\,\mathsf{PR}}(p) = C_{h\,\mathsf{PR},a\,\mathsf{RP}}(p) \approx 2\phi(p-1)^2/(p-1)$.

In Conjectures 6.3(a) and 6.3(e) it should be noted that the observed values in question must be exactly (not just approximately) equal, by the symmetry of (3). The same applies in Conjectures 6.3(c) and 6.3(f).

We also made in [6] the following conjectures about solutions to (3).

Conjecture 6.4.

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

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

(c) *In general,*

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

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 6.4(a) and Conjecture 6.4(c) appear in [6] with typos. They appear correctly here and in [7].)

TABLE 4. Solutions to (3)

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

$a \setminus h$	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 $C(100057)$

$a \setminus h$	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

These conjectures rely on Heuristics 2.6 and 6.2 and a standard birthday paradox argument. Thanks to Lemma 2.7 we are now closer to making them into rigorous theorems. All of the conjectures on (3) are summarized in Table 4, which appeared in [7]. The table also contains new data collected since [6]. As in [6], we distinguish between the "trivial" solutions to (3), where $h = a$, and the "nontrivial" solutions.

As observed in Section 5, to estimate the number of solutions to (2) in the remaining cases we need to look at (10). We start by estimating the number of nontrivial solutions. This requires a finer version of Heuristic 6.2 which takes $d = \gcd(h, a, p-1)$ into account.

Heuristic 6.5. *Fix d, e such that e divides $p-1$ and d divides e. Then the map $x \mapsto x^{x/d} \mod p$ is a random map, even when restricted to a specific order and greatest common divisor, in the sense that for all p, given $y \in \{1, \dots, p-1\}$ such that $\operatorname{ord}_p y = f/\gcd(e, f)$, then*

$$\#\Big\{x \in \{1,\dots,p-1\}\colon x^{x/d} \equiv y \mod p,\ \gcd(x, p-1) = e,\ \operatorname{ord}_p x = f\Big\} \approx \frac{\#\{z \in \{1,\dots,p-1\}\colon \gcd(z,p-1) = e,\ \operatorname{ord}_p z = f\}}{\#\{w \in \{1,\dots,p-1\}\colon \operatorname{ord}_p w = \operatorname{ord}_p y\}}.$$

Now we can approximate the number of nontrivial solutions of (10) using a similar birthday paradox argument to that used in [6] for Conjecture 6.4.

By Heuristic 6.5, we see that the nontrivial part of $C'_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)$ is equal to:

$$\begin{aligned}
&\sum_{d|p-1} \#\{(h,a)\colon h\neq a,\ (10)\text{ holds},\ \gcd(h,a,p-1)=d\}\\
&=\sum_{d|p-1}\sum_{\substack{e,f|p-1\\ \gcd(e,f)=d}} \#\{(h,a)\colon h\neq a,\ (10)\text{ holds},\ \gcd(h,p-1)=e,\\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \gcd(a,p-1)=f\}\\
&\approx \sum_{d|p-1}\sum_{\substack{e,f|p-1\\ \gcd(e,f)=d}}\sum_{m|p-1}\frac{\#S_{m,e}\cdot\#S_{m,f}}{\#T_m},
\end{aligned}$$

where

$$\begin{aligned}
S_{m,r}&=\left\{x\colon \operatorname{ord}_p(x^{x/d})=m,\ \gcd(x,p-1)=r\right\}\\
&=\bigcup_{n|(p-1)/m}\left\{x\colon \operatorname{ord}_p(x)=nm,\ \gcd\left(\frac{x}{d},nm\right)=n,\ \gcd(x,p-1)=r\right\}\\
&=\bigcup_{\substack{n|(p-1)/m\\ \gcd\left(\frac{r}{d},nm\right)=n}}\{x\colon \operatorname{ord}_p(x)=nm,\ \gcd(x,p-1)=r\}
\end{aligned}$$

and $T_m=\{x\colon \operatorname{ord}_p x=m\}$. Then, by Heuristic 2.6, we have:

$$\begin{aligned}
\#S_{m,r}&\approx\sum_{\substack{n|(p-1)/m\\ \gcd\left(\frac{r}{d},nm\right)=n}}\frac{1}{p-1}\#\{x\colon \operatorname{ord}_p(x)=nm\}\cdot\#\{x\colon \gcd(x,p-1)=r\}\\
&=\sum_{\substack{n|(p-1)/m\\ \gcd\left(\frac{r}{d},nm\right)=n}}\frac{1}{p-1}\phi(nm)\phi\left(\frac{p-1}{r}\right).
\end{aligned}$$

Thus

$$\begin{aligned}
&\sum_{d|p-1} \#\{(h,a)\colon h\neq a,\ (10)\text{ holds},\ \gcd(h,a,p-1)=d\}\\
&\approx\sum_{d|p-1}\sum_{\substack{e,f|p-1\\ \gcd(e,f)=d}}\sum_{m|p-1}\frac{1}{\phi(m)}\left(\sum_{\substack{n|(p-1)/m\\ \gcd\left(\frac{e}{d},nm\right)=n}}\frac{1}{p-1}\phi(nm)\phi\left(\frac{p-1}{e}\right)\right)\\
&\qquad\qquad\times\left(\sum_{\substack{t|(p-1)/m\\ \gcd\left(\frac{f}{d},tm\right)=t}}\frac{1}{p-1}\phi(tm)\phi\left(\frac{p-1}{f}\right)\right)\\
&=\sum_{d|p-1}\sum_{\substack{e,f|p-1\\ \gcd(e,f)=d}}\sum_{m|p-1}\sum_{\substack{n|(p-1)/m\\ \gcd\left(\frac{e}{d},nm\right)=n}}\sum_{\substack{t|(p-1)/m\\ \gcd\left(\frac{f}{d},tm\right)=t}}\frac{\phi(nm)\phi(tm)\phi\left(\frac{p-1}{e}\right)\phi\left(\frac{p-1}{f}\right)}{(p-1)^2\phi(m)}.
\end{aligned}$$

Proposition 6.6. *For any d dividing q,*

$$\sum_{\substack{e,f|q\\ \gcd(e,f)=d}} \sum_{m|q} \sum_{\substack{n|q/m\\ \gcd\left(\frac{e}{d},nm\right)=n}} \sum_{\substack{t|q/m\\ \gcd\left(\frac{f}{d},tm\right)=t}} \frac{\phi(nm)\phi(tm)\phi\left(\frac{q}{e}\right)\phi\left(\frac{q}{f}\right)}{\phi(m)} = q\ J_2\left(\frac{q}{d}\right),$$

where $J_2(r)$ is the Jordan function $J_2(r)=\sum_{s|r} s^2\mu\left(\frac{r}{s}\right)$.

Proof. This can be verified directly when q is a prime power; then use multiplicativity for the general case. □

It seems likely that a more combinatorial proof of this proposition can be found.

Finally, we see that the nontrivial part of $C'_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)$ is approximately

$$\begin{aligned}\sum_{d|p-1} \sum_{\substack{e,f|p-1\\ \gcd(e,f)=d}} \sum_{m|p-1} \sum_{\substack{n|(p-1)/m\\ \gcd\left(\frac{e}{d},nm\right)=n}} \sum_{\substack{t|(p-1)/m\\ \gcd\left(\frac{f}{d},tm\right)=t}} \frac{\phi(nm)\phi(tm)\phi\left(\frac{p-1}{e}\right)\phi\left(\frac{p-1}{f}\right)}{(p-1)^2\phi(m)}&\\ = \sum_{d|p-1} \frac{1}{p-1}\ J_2\left(\frac{p-1}{d}\right)&\\ = p-1.&\end{aligned}$$

As we saw in Section 5, Heuristic 5.2 implies that every nontrivial solution to (10) with $h\,\mathsf{ANY}$ and $a\,\mathsf{ANY}$ produces on average one pair (g,h) that is a nontrivial solution to (2). Thus the nontrivial part of $T_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)$ and also the nontrivial part of $C'_{h\,\mathsf{ANY},a\,\mathsf{ANY}}(p)$ are both approximately equal to $p-1$.

Similarly, we saw that Heuristic 5.2 implies that every solution to (10) with $h\,\mathsf{ANY}$ and $a\,\mathsf{ANY}$ produces on average $\phi(p-1)/(p-1)$ pairs (g,h) that are solutions to (2) with $g\,\mathsf{PR}$. Combining this with the previous argument, we see that the nontrivial part of $T_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p)$ is approximately

$$\sum_{d|p-1} \frac{J_2\left(\frac{p-1}{d}\right)}{p-1} \frac{\phi(p-1)}{p-1} = \phi(p-1).$$

These calculations justify the following conjectures:

Conjecture 6.7.

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

These conjectures were made in [6] on the basis of an extension of the "random map" idea for $x \mapsto \log x$. As was explained there, however, it was not clear how to formulate the idea as a heuristic that could be proved in a rigorous form. The new analysis explains the complications in the relationship between $C_{h\,\mathsf{ANY},a\,\mathsf{ANY}}$ and $T_{g\,\mathsf{ANY},h\,\mathsf{ANY}}$ encountered in [6].

Finally, Heuristic 5.2 can be used to justify the last set of conjectures from [7]:

Conjecture 6.8.

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

TABLE 5. 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

The conjectures on (2) are summarized in Table 5, which appeared in [7]. The table also contains new data collected since [6]. The data sets from Tables 1, 4, and 5 were 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 $F(p)$, $T(p)$, and $C(p)$, for five primes p starting at 100000.

7. Averages of the main terms

Thus far we have considered variants of the Brizolis conjecture for a fixed finite field with p elements. In the next two sections 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 only result from analytic number theory we need in order to prove these lemmas is the so-called Siegel-Walfisz theorem. As usual $\pi(x; d, a)$ denotes the number of primes $p \le x$ such that $p \equiv a$ modulo d, and $\mathrm{Li}(x) = \int_2^x dt/\ln t$ denotes the logarithmic integral.

Lemma 7.1 ([15, Satz 4.8.3])**.** *Let $C > 0$ be arbitrary. Then*

$$\pi(x; d, a) = \frac{\mathrm{Li}(x)}{\phi(d)} + O(xe^{-c_1\sqrt{\ln x}}),$$

uniformly for $1 \le d \le \ln^C x$, $(a, d) = 1$, where the constants depend at most on C.

The following result for $k = 1$ is well known; see, e.g., [12, 16]. For arbitrary k it was claimed by Esseen [3] (but only proved for $k = 3$). We present a proof based on an idea of Carl Pomerance [14]. An analogue of this result for natural numbers was proved by Issai Schur in his Winter Semester lectures of 1923–24. He proved, for any complex number s, that

$$\lim_{m\to\infty}\frac{1}{m}\sum_{n=1}^{m}\left(\frac{\phi(n)}{n}\right)^s=\prod_p\left(1+\frac{(1-1/p)^s-1}{p}\right).$$

For an instructive discussion of this result see [8, Chapter 4.2].

Lemma 7.2. *Let k and C be arbitrary real numbers with $C > 0$. Then*

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

where

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

Proof. (The implicit constants in this proof depend at most on C and k.) Let g_k be the Dirichlet convolution of the Möbius function and $(\phi(n)/n)^k$. Notice that g_k is a multiplicative function and that $(\phi(n)/n)^k=\sum_{d|n}g_k(d)$. Using the latter identity we infer that

$$\sum_{p\le x}\left(\frac{\phi(p-1)}{p-1}\right)^k=\sum_{p\le x}\sum_{d|p-1}g_k(d)=\sum_{d\le x}g_k(d)\pi(x;d,1).$$

If p is a prime, then clearly $g_k(p)=(1-1/p)^k-1$ and $g_k(p^r)=0$ for $r\ge 2$. For every k there exists a constant c_k such that $|g_k(p)|\le c_k/p$ for every prime p. Note that

$$|g_k(n)|\le\frac{c_k^{\omega(n)}|\mu(n)|}{n}\ll n^{-1+\epsilon}, \tag{11}$$

where $\omega(n)$ denotes the number of distinct prime divisors of n. Now write

$$\begin{aligned}\sum_{d\le x}g_k(d)\pi(x;d,1) &= \sum_{d\le\ln^B x}g_k(d)\pi(x;d,1)+\sum_{\ln^B x<d\le x}g_k(d)\pi(x;d,1)\\ &= S_1+S_2,\end{aligned}$$

say, where $B > 0$ is arbitrary for the moment. In order to estimate S_1, we invoke Lemma 7.1. This gives

$$S_1=\mathrm{Li}(x)\sum_{d\le\ln^B x}\frac{g_k(d)}{\phi(d)}+O_C\left(\frac{x}{\ln^C x}\right).$$

Now

$$\sum_{d\le\ln^B x}\frac{g_k(d)}{\phi(d)}=\sum_{d=1}^{\infty}\frac{g_k(d)}{\phi(d)}+O\left(\sum_{d>\ln^B x}\frac{|g_k(d)|}{\phi(d)}\right).$$

We have $d/\phi(d)=\prod_{p|d}(1-p^{-1})^{-1}\le\prod_{p\le d}(1-p^{-1})^{-1}\ll\ln d$, using Mertens' formula. This together with the estimate (11) shows that the sum $\sum_{d=1}^{\infty}g_k(d)/\phi(d)$

TABLE 6. The constants A_k

k	A_k
1	0.37395 58136 19202 28805$\cdots$
2	0.14734 94000 02001 45807$\cdots$
3	0.06082 16551 20305 08600$\cdots$
4	0.02610 74463 14917 70808$\cdots$
5	0.01156 58420 47143 35542$\cdots$
6	0.00525 17580 26977 39754$\cdots$
7	0.00243 02267 63032 72703$\cdots$

is absolutely convergent. Since, moreover, $g_k(d)/\phi(d)$ is multiplicative, we find using the Euler product identity that $\sum_{d=1}^{\infty} g_k(d)/\phi(d) = A_k$. Using (11) we infer that

$$\sum_{d>\ln^B x} \frac{|g_k(d)|}{\phi(d)} \ll \sum_{d>\ln^B x} \frac{\ln d}{d^{2-\epsilon}} \ll \frac{B \ln\ln x}{\ln^{B(1-\epsilon)} x}.$$

Invoking the estimates $\pi(x;d,1) < x/d$ and (11) leads to $S_2 = O(x \ln^{-B(1-\epsilon)} x)$. On putting everything together and taking B sufficiently large, the result follows. □

Remark 7.3. Using, e.g., Maple it turns out that in the range $0 \le k \le 27$ the constant A_k is quite well approximated by $e^{-1.011k+0.0278k^2}$. The constant A_1 equals the Artin constant. Let

$$A_{k,n} = \prod_{p>n} \left(1 + \frac{(1-1/p)^k - 1}{p-1}\right) \text{ and } \zeta_n(k) = \zeta(k) \prod_{p\le n} (1-p^{-k}).$$

If k is a natural number and n is sufficiently large, then $A_{k,n} = \prod_{k\ge 2} \zeta_n(r)^{e_{k,r}}$, where the exponents $e_{k,r}$ are integers that can be explicitly computed [11]. In this way A_k and indeed any other Euler product appearing in this paper can be evaluated with arbitrary precision; cf. Theorem 2 of [11]. In Table 6 we present a few examples.

If a and b are natural numbers, then by (a,b) we denote the greatest common divisor of a and b and by $[a,b]$ the lowest common multiple.

Lemma 7.4. *Let a and b be natural numbers and $C > 0$. We have*

$$\sum_{\substack{p\le x \\ p\equiv 1 \mod a \\ p\equiv 1 \mod b}} \frac{\phi(\frac{p-1}{a})\phi(\frac{p-1}{b})}{(p-1)^2} = r(a,b) A_2 \mathrm{Li}(x) + O_{a,b,C}\left(\frac{x}{\ln^C x}\right), \tag{12}$$

where

$$r(a,b) = \frac{\phi(\frac{[a,b]}{(a,b)})\phi([a,b])}{[a,b]^4} \prod_{p\mid ab} \frac{p(p^2+p-1)}{p^3-p^2-2p+1} \prod_{p\mid \frac{ab}{(a,b)^2}} \frac{p(p^2-1)}{p^3-2p+1}. \tag{13}$$

We have

$$\frac{\phi(\frac{[a,b]}{(a,b)})}{\phi([a,b])[a,b]^2} \le r(a,b) \le 4.13 \frac{\phi(\frac{[a,b]}{(a,b)})}{\phi([a,b])[a,b]^2}. \tag{14}$$

Proof. The proof can be carried out similarly to that of Lemma 7.2. We introduce an arithmetic function $h_{a,b}$ that satisfies

$$\frac{\phi(m\frac{a}{(a,b)})\phi(m\frac{b}{(a,b)})}{m\phi(\frac{a}{(a,b)})m\phi(\frac{b}{(a,b)})} = \sum_{d|m} h_{a,b}(d). \tag{15}$$

On noting that the left-hand side of (15) is a multiplicative function of m, it follows that $h_{a,b}$ is multiplicative. Then $h_{a,b}$ is easily evaluated. Taking $m = (p-1)/[a,b]$ we find that (12) holds with constant

$$\frac{\phi(\frac{[a,b]}{(a,b)})}{\phi([a,b])[a,b]^2} \sum_{d=1}^{\infty} \frac{h_{a,b}(d)\phi([a,b])}{\phi(d[a,b])}.$$

After some manipulations the latter expression, in which the sum has as argument a multiplicative function, is seen to equal

$$A_2 \frac{\phi(\frac{[a,b]}{(a,b)})}{\phi([a,b])[a,b]^2} \prod_{p|ab} \frac{(p-1)(p^3-2p+1)}{p(p^3-p^2-2p+1)} \prod_{p|\frac{ab}{(a,b)^2}} \frac{p(p^2-1)}{p^3-2p+1}. \tag{16}$$

On further simplification this is seen to equal $r(a,b)A_2$. It can be shown that

$$\prod_p \frac{(p-1)(p^2-1)}{p^3-p^2-2p+1} \leq 4.13.$$

This inequality and the fact that the local factors in the two products appearing in (16) are all > 1 then establishes the truth of (14). □

Lemma 7.5. *Let $C > 0$ be arbitrary. We have*

$$\sum_{p\leq x} \frac{1}{p-1} \sum_{e|p-1} \frac{1}{e}\phi\left(\frac{p-1}{e}\right) = S\ \mathrm{Li}(x) + O_C\left(\frac{x}{\ln^C x}\right),$$

where

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

is the Stephens constant (see [17]*).*

Proof. Using the fact that $\phi(n)/n = \sum_{d|n} \mu(d)/d$ with $n = (p-1)/e$, we find on making the substitution $de = v$ and swapping the order of summation that

$$\sum_{p\leq x} \frac{1}{p-1} \sum_{e|p-1} \frac{1}{e}\phi\left(\frac{p-1}{e}\right) = \sum_{v\leq x-1} \frac{\sum_{d|v}\mu(d)d}{v^2} \sum_{\substack{p\leq x \\ p\equiv 1 \bmod v}} 1.$$

On splitting the summation range in the range $v \leq \ln^B x$ and $v > \ln^B x$ for an appropriate B, the result is then deduced as in Lemma 7.2. □

Remark 7.6. Let $V = \{V_n\}_{n=0}^{\infty}$ be a sequence of integers. We say that m divides the sequence V if m divides at least one term of the sequence. Denote by $\delta(V)$ the natural density of primes p dividing V, if it exists. Stephens [17] proved, subject to the Generalized Riemann Hypothesis (GRH), that $\delta(V)$ exists for a large class of second-order linear recurrences. Moreover he showed, subject to GRH, that for these sequences $\delta(V)$ equals a rational number times the Stephens constant.

His work is extended and corrected in [9, 10]. For more details on the numerical approximation to S given in the lemma see [11, p. 397].

Lemma 7.7. *Let $C > 0$ be arbitrary. We have*

$$\sum_{p\le x}\frac{1}{(p-1)^2}\sum_{e|p-1}\phi\left(\frac{p-1}{e}\right)^2 = A_1\frac{\zeta(3)}{\zeta(2)}\mathrm{Li}(x) + O_C\left(\frac{x}{\ln^C x}\right),$$

where

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

Proof. Using the fact that $(\phi(n)/n)^2 = \sum_{d|n} g_2(d)$ with $n = (p-1)/e$ (for the definition of $g_2(d)$ see the proof of Lemma 7.2), we find on making the substitution $de = v$ and swapping the order of summation that

$$\sum_{p\le x}\frac{1}{p-1}\sum_{e|p-1}\phi\left(\frac{p-1}{e}\right)^2 = \sum_{v\le x-1}\frac{\sum_{d|v} d^2 g_2(d)}{v^2}\sum_{\substack{p\le x\\ p\equiv 1 \bmod v}} 1.$$

On splitting the summation range in the range $v \le \ln^B x$ and $v > \ln^B x$ for an appropriate B, the result is then deduced as in Lemma 7.2. □

Remark 7.8. Lemma 7.4 suggests that the sum in the previous lemma is asymptotically equal to $A_2\sum_{e=1}^{\infty} r(e,e)$. Some computation shows that, in agreement with Lemma 7.7, we have

$$A_2\sum_{e=1}^{\infty} r(e,e) = A_2\sum_{e=1}^{\infty}\frac{1}{e^3}\prod_{p|e}\frac{p^3-2p+1}{p^3-p^2-2p+1} = A_1\frac{\zeta(3)}{\zeta(2)}.$$

Lemma 7.9. *Let $C > 0$ be arbitrary. We have*

$$\sum_{p\le x}\frac{1}{p-1}\sum_{m|p-1}\phi(m)\left(\sum_{d|\frac{p-1}{m}}\frac{\phi(d)}{d}\right)^2 = U\ \mathrm{Li}(x) + O_C\left(\frac{x}{\ln^C x}\right), \tag{17}$$

where

$$U = \prod_p\left(1+\frac{3p^2+2p+1}{p(p+1)(p^2-1)}\right) \approx 3.4210\cdots.$$

Proof. Let us define $h_1(n) = (\sum_{d|n}\phi(d)/d)^2$. Note that h_1 is multiplicative. Let us denote the left-hand side of (17) by I_1. We have

$$\begin{aligned} I_1 &= \sum_{p\le x}\sum_{m|p-1}\frac{\phi(\frac{p-1}{m})}{m\frac{p-1}{m}}h_1(m)\\ &= \sum_{p\le x}\sum_{m|p-1}\frac{h_1(m)}{m}\sum_{\delta|\frac{p-1}{m}}\frac{\mu(\delta)}{\delta}\\ &= \sum_{v\le x}\frac{\sum_{\delta|v}\mu(\delta)h_1(\frac{v}{\delta})}{v}\sum_{\substack{p\le x\\ p\equiv 1 \bmod v}} 1. \end{aligned}$$

Proceeding as in most of the earlier lemmas, we then deduce that (17) holds true with constant

$$\sum_{v=1}^{\infty}\frac{\sum_{\delta|v}\mu(\delta)g(\frac{v}{\delta})}{v\phi(v)}=\prod_p\left(1+\sum_{k=1}^{\infty}\frac{2+(2k-1)(1-1/p)}{p^{2k}}\right),$$

which, after some tedious calculation, is seen to equal U. □

Lemma 7.10. *Let $C>0$ be arbitrary. We have*

$$\sum_{p\le x}\frac{1}{p-1}\sum_{m|p-1}\frac{\phi(m)^3}{m^2}\left(\sum_{d|\frac{p-1}{m}}\frac{\phi(d)}{d}\right)^2=L\ \mathrm{Li}(x)+O_C\left(\frac{x}{\ln^C x}\right), \tag{18}$$

where

$$L=\prod_p\left(1+\frac{p^5+2p^4-3p^3+p^2+1}{p^3(p+1)^3(p-1)}\right)\approx 1.4446\cdots.$$

Proof. Let us denote the left-hand side of (18) by I_2. We have

$$\begin{aligned}I_2&=\sum_{p\le x}\sum_{m|p-1}\frac{h_1(m)}{m}\left(\frac{\phi(\frac{p-1}{m})}{\frac{p-1}{m}}\right)^3\\&=\sum_{p\le x}\sum_{m|p-1}\frac{h_1(m)}{m}\sum_{\delta|\frac{p-1}{m}}g_3(\delta)\\&=\sum_{v\le x-1}\frac{\sum_{\delta|v}\delta h_1(\delta)g_3(\frac{v}{\delta})}{v}\sum_{\substack{p\le x\\ p\equiv 1 \bmod v}}1.\end{aligned}$$

Proceeding as in most of the earlier lemmas, we then deduce that (18) holds true with constant

$$\sum_{v=1}^{\infty}\frac{\sum_{\delta|v}\delta h_1(\delta)g_3(\frac{v}{\delta})}{v\phi(v)}$$
$$=\prod_p\left(1+\sum_{k=1}^{\infty}\frac{(1+k(1-\frac{1}{p}))^2+((1-\frac{1}{p})^3-1)p(1+(k-1)(1-\frac{1}{p}))^2}{p^{2k}}\right),$$

which, after some tedious calculation, is seen to equal L. □

The final lemma we will present is actually used in our error terms and not our main terms, but it is of the same character as the others in this section.

Lemma 7.11. *Let k and C be arbitrary real numbers with $C>0$, $k>0$. Then*

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

where

$$\sigma_k(n)=\sum_{d|n}d^k$$

and

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

TABLE 7. The constants T_k

k	T_k
1	$2.20386\cdots$
2	$1.38098\cdots$
3	$1.15762\cdots$
4	$1.07163\cdots$
5	$1.03397\cdots$
6	$1.01646\cdots$
7	$1.00808\cdots$

Proof. Using the fact that $\sigma_k(n)/n^k = \sum_{d|n} d^k/n^k = \sum_{d|n} 1/d^k$, we see that

$$\sum_{p\le x} \frac{\sigma_k(p-1)}{(p-1)^k} = \sum_{p\le x} \sum_{d|p-1} \frac{1}{d^k} = \sum_{d\le x} \frac{1}{d^k}\pi(x;d,1).$$

On splitting the summation range in the range $v \le \ln^B x$ and $v > \ln^B x$ for an appropriate B, the result is then deduced as in Lemma 7.2. □

We have not yet computed the constants T_k using the techniques described in Remark 7.3, but a rough approximation using Maple gives the results shown in Table 7.

8. Averages of the conjectures and results

Given the lemmas from the previous section it is trivial to establish average versions of some of our results. For example, we have:

Theorem 8.1. *Let $C > 0$ be arbitrary. We have*

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

Proof. This follows at once from Theorem 4.1, Lemma 7.2, and the observation that, for every $\epsilon > 0$, $\sum_{p\le x} d(p-1)\sqrt{p}(1+\ln p)/(p-1) = O(x^{1/2+\epsilon})$. □

Similarly, we have:

Theorem 8.2. *Let $C > 0$ be arbitrary. We have*

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

and

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

Proof. This likewise follows from Theorems 4.16 and 4.17 and Lemmas 7.5 and 7.7. □

Propositions 4.3 and 4.14 are unfortunately more problematic, due to the presence of the exceptionally large error term. As remarked there, the factor of $\sigma(p-1)-3(p-1)/2$ in the error term can be averaged as

$$\sum_{p\le x}\frac{\sigma(p-1)-3(p-1)/2}{p-1}=(T_2-3/2)\mathrm{Li}(x)+O_C\left(\frac{x}{\ln^C x}\right)$$
$$\approx 0.70386\mathrm{Li}(x)+O_C\left(\frac{x}{\ln^C x}\right).$$

(Apply Lemma 7.11.) The factor of $\sqrt{p}$, however, will still result in an error term with an order of magnitude larger than the main term.

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. For instance, we have:

Conjecture 8.3.

(a) $\displaystyle\sum_{p\le x}\frac{F_{g\,\mathsf{ANY},h\,\mathsf{ANY}}(p)}{p-1}\approx \mathrm{Li}(x).$

(b) $\displaystyle\sum_{p\le x}\frac{F_{g\,\mathsf{PR},h\,\mathsf{ANY}}(p)}{p-1}\approx A_1\mathrm{Li}(x).$

These conjectures and the average versions of our other conjectures are summarized in Tables 8, 9, and 10. The data sets in these tables were collected on the same Beowulf cluster 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 6.4(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 8.4. *Let $C>0$ be arbitrary. We have*

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

Although we cannot prove (or even completely justify) this at present, we can establish the following result.

Lemma 8.5. *For every x sufficiently large we have*

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

TABLE 8. Average solutions to (1)

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

$g \setminus h$	ANY	PR	RP	RPPR
ANY	1	A_2	A_1	A_2
PR	A_1	A_2	A_2	A_2
RP	A_1	A_3	A_2	A_3
RPPR	A_2	A_3	A_3	A_3

(b) Predicted approximate numeric values for $\frac{1}{\pi(x)} \sum_{p \le x} F(p)$

$g \setminus h$	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

(c) 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 9. Average solutions to (3)

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

$a \setminus h$	ANY	PR	RP	RPPR
ANY	$1.644\cdots$	A_1	A_1	A_3
PR	A_1	A_2	A_2	A_3
RP	A_1	A_2	A_2	A_3
RPPR	A_3	A_3	A_3	A_3

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

$a \setminus h$	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

(c) 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

TABLE 10. 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	A_2	A_1	A_3
PR	A_1	A_2	A_2	A_3
RP	A_1	A_3	A_2	A_4
RPPR	A_2	A_3	A_3	A_4

(b) Predicted approximate numeric 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

(c) 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

Proof. Note that

$$\sum_{m|p-1} \frac{\phi(m)^3}{m^2}\left(\sum_{d|\frac{p-1}{m}} \frac{\phi(d)}{d}\right)^2 \le w(p) \le \sum_{m|p-1} \phi(m)\left(\sum_{d|\frac{p-1}{m}} \frac{\phi(d)}{d}\right)^2,$$

where the first inequality, by the way, is exact if $p-1$ is squarefree. The result now follows on invoking Lemma 7.10 and Lemma 7.9. □

9. Conclusion and future work

Most of the theorems of Section 4 suffer from an error term that is larger than the main term. This seems to be a direct consequence of the use of Lemma 2.7 and may be unavoidable. However, we have shown that we can put some limits on how often the error actually approaches the worst case, and we have conjectured that even better limits exist. The best next step may be further data collection in order to empirically count the number of primes with the potential for large errors.

We have begun to put our conjectures on a firm footing, deriving them from as few heuristics as possible. We hope to be able to prove these heuristics in the future. Then we should be able to convert the conjectures into theorems by merely estimating the error term.

The project of extending our analysis to three-cycles and more generally k-cycles for small values of k, mentioned in [6], still remains to be done. Along similar lines, Igor Shparlinski has suggested attempting to analyze the average length of a cycle,

which could have many practical applications in the analysis of cryptographically secure pseudorandom bit generators, as mentioned in [6].

Acknowledgments

Once again, the first author would like to thank the people mentioned in [6]: 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. Both authors would like to thank the anonymous referees for many helpful comments.

References

1. Campbell, Mariana, *On fixed points for discrete logarithms*, Master's Thesis, 2003.
2. Cristian Cobeli and Alexandru Zaharescu, *An exponential congruence with solutions in primitive roots*, Rev. Roumaine Math. Pures Appl. **44** (1999), 15–22. MR1841958 (2002d:11005)
3. Carl-Gustav Esseen, *A stochastic model for primitive roots*, Rev. Roumaine Math. Pures Appl. **38** (1993), 481–501. MR1258051 (94m:11110)
4. Étienne Fouvry, *Théorème de Brun-Titchmarsh: Application au théorème de Fermat*, Invent. Math. **79** (1985), 383–407. MR0778134 (86g:11052)
5. Richard K. Guy, *Unsolved problems in number theory*, Springer-Verlag, 1981. MR0656313 (83k:10002)
6. Joshua Holden, *Fixed points and two-cycles of the discrete logarithm*, Algorithmic number theory (ANTS 2002) (C. Fieker and D. Kohel, eds.) LNCS, Springer, 2002, pp. 405–415. MR2041100
7. ———, *Addenda/corrigenda: Fixed points and two-cycles of the discrete logarithm*, 2002, unpublished
8. Mark Kac, *Statistical independence in probability, analysis and number theory*, The Carus Mathematical Monographs, vol. 12, Mathematical Association of America, 1959. MR0110114 (22:996)
9. Pieter Moree and Peter Stevenhagen, *A two-variable Artin conjecture*, J. Number Theory **85** (2000), 291–304. MR1802718 (2001k:11188)
10. ———, *Prime divisors of the Lagarias sequence*, J. Théor. Nombres Bordeaux **13** (2001), 241–251. MR1838084 (2002c:11016)
11. Pieter Moree, *Approximation of singular series and automata*, Manuscripta Math. **101** (2000), 385–399. MR1751040 (2001f:11204)
12. ———, *Asymptotically exact heuristics for (near) primitive roots*, J. Number Theory **83** (2000), 155–181. MR1767657 (2001m:11161)
13. Pieter Moree, *An exponential congruence with solutions in primitive roots (review)*, Mathematical Reviews (2002). MR1841958 (2002d:11005)
14. Carl Pomerance, Personal communication.
15. Karl Prachar, *Primzahlverteilung*, Springer, 1957. MR0087685 (19:393b)
16. P.J. Stephens, *An average result for Artin's conjecture*, Mathematika **16** (1969), 178–188. MR0498449 (58:16565)
17. ———, *Prime divisors of second order linear recurrences I, II*, J. Number Theory **8** (1976), 313–332, 333–345. MR0417081 (54:5142); MR0417082 (54:5143)
18. Wen Peng Zhang, *On a problem of Brizolis*, Pure Appl. Math. **11** (1995), 1–3. MR1454053 (98d:11099)

Department of Mathematics, Rose-Hulman Institute of Technology, Terre Haute, Indiana, 47803-3999
E-mail address: holden@rose-hulman.edu

Max-Planck-Institut für Mathematik, Vivatsgasse 7, D-53111 Bonn, Germany
E-mail address: moree@mpim-bonn.mpg.de
URL: http://xxx.lanl.gov/abs/math.NT/0208028