# The self-power map and its image modulo a prime

by

Catalina V. Anghel

Thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

# Abstract

The self-power map and its image modulo a prime

Catalina V. Anghel

Doctor of Philosophy

Graduate Department of Mathematics

University of Toronto

2013

The self-power map is the function from the set of natural numbers to itself which sends the number $n$ to $n^n$. Motivated by applications to cryptography, we consider the image of this map modulo a prime $p$. We study the question of how large $x$ must be so that $n^n \equiv a \bmod p$ has a solution with $1 \leq n \leq x$, for every residue class $a$ modulo $p$. While $n^n \bmod p$ is not uniformly distributed, it does appear to behave in certain ways as a random function. We give a heuristic argument to show that the expected $x$ is approximately $p^2 \log \phi(p-1)/\phi(p-1)$, using the coupon collector problem as a model. Rigorously, we prove the bound $x < p^{2-\alpha}$ for sufficiently large $p$ and a fixed constant $\alpha > 0$ independent of $p$, using a counting argument and exponential sum bounds. Additionally, we prove nontrivial bounds on the number of solutions of $n^n \equiv a \bmod p$ for a fixed residue class $a$ when $1 \leq n \leq x$, extending the known bounds when $1 \leq n \leq p-1$.

# Dedication

For my parents, Mirela and Vinicius Anghel.

# Acknowledgements

**Academic Acknowledgments.** First and foremost, I would like to thank my supervisor, *Prof. Kumar Murty*, who first suggested the study of the self-power map. His help, encouragement, and optimism have been invaluable over the past five years. I thank him for creating a wonderful sense of community (including a viewing of the Kung Fu Panda movie!). Most of all, I am grateful to him for taking me seriously as a researcher.

I am grateful to *Prof. Balasubramanian (Prof. Balu)* for two very useful discussions at the start of my study. *Dr. Venkatesan (Venkie)* introduced me to an algorithmic approach to thinking about the self-power map, and always was cheerfully ready to talk with me about my work, even from Seattle and India. I thank *Prof. Repka* for his advice and reassurance. It was wonderful to have a faculty member I felt completely comfortable approaching when I was struggling.

*Prof. Ram Murty* forwarded me his article and suggestions at a key moment in my research. His ideas were different from the path I ultimately took, but he was correct in thinking that my problem was similar. His article helped me get "unstuck" when finding the deterministic bound.

I was amazed that my external examiner, *Prof. Igor Shparlinski*, came from halfway around the world to visit the department on the occasion of my defense. I am very grateful for his interest in my work, from suggestions for improving a proposition in the second chapter to forwarded articles for further reading.

I thank the members of my supervisory committee, *Prof. Murnaghan* and *Prof. Kamnitzer*, for being a kind audience during our meetings. They also accepted receiving my many email updates or helped with (very, very) last-minute reference letters.

As every mathematics graduate student before me, I am incredibly grateful to *Ida Bulat* for her warmth, kindness and dedication. From reminders about forgotten deadlines to meeting for coffee to catch up, I am so glad that she is always there to ensure that everything goes smoothly.

A huge thank you goes out to my Ganita lab-mates: *Robby Burko*, *Aaron Chow*, *Payman Eskandari*, *William George*, *Nataliya Laptyeva*, *Mariam Mourtada*, *Meng Fai Lim*, and *Ying Zong* as well as visitors *Brendon Hanson* and *Anastasia Zaytseva*. Thank you for your questions, advice, and support, and for providing such a welcoming environment for me to share my ideas. I am so glad to also call you friends. Thank you for the musical shows, cozy potlucks, French movies, dinners, wedding, introductions to new babies, and ceilidh dances over the past years.

I would also like to thank *Aude Plateaux*, for her warm welcome at ENSICAEN this summer. In her expert care, I had a quiet place to start writing my thesis, as well as a wonderful travel experience.

**Personal Acknowledgments.** While I would have never finished my thesis without the mathematical support of my professors and colleagues, I also would have never finished without the encouragement of my friends and family.

Thank you to *Charlotte Ochanine*, the kindest person I know. You were my biggest cheerleader during my first year and your encouragement and practical advice helped me survive the comprehensive exams. Your visit to Deep River over the winter holidays is one of my fondest memories of my time as a PhD. Thank you for being so patient with me even during my most stressful times.

Thank you to *Peter Lee* for making me more conscious about trying new things and getting out in nature, both of which restore me when things get tough.

*Hanae Hanzawa*, you are my role model for being a kind and confident woman. You are so much fun to be around, and so open about everything (including trying strange Romanian food).

Thank you to *Caroline Schmeing*, who is always ready for new adventures, whether it is attending a baseball game, or cooking exotic dishes, or saving me from a mouse two days before my supervisory committee meeting. *Terry (Theresa) Lim* is not only one of my closest friends, but has also been my roommate. We definitely bonded over shared experiences, like the plumbing mishap at 1 am! Thank you for your practical, tell-it-like-it-is advice to my fanciful musings, and for all the shared activities, from spin class to kayaking.

Thank you so much to *Tom Kuwahara*, my best friend and confidant in these past five and a half years. Thank you for your wisdom, your sense of humour and your understanding during the many times when I have been stressed and irritable. So many of my best memories during the past years are with you: the early, long study stretches for analysis and topology, breaks for tea and Greg's ice cream, hikes through the Toronto ravines and the Newfoundland coast, and all the laughter in our weekly chats. It's with you that I feel most 'me'.

There are two people whom I cannot even begin to thank, my parents *Mira* and *Vinicius Anghel*. My father has been the sounding board for my ideas and the first reader of my work. My mother patiently listened to all my worries and struggles (and I am not one to suffer in silence!). I am so grateful that their confidence in me never wavered. Their love and support got me through the painful years when nothing worked. It's been a gift to finally be able to do mathematics, to find a pattern when at first there is none. I could have never gotten there without them.

# Contents

# Chapter 1

# Introduction

**Definition 1.1.** *The self-power map is the function $f$ from the set of natural numbers to itself, such that*

$$f(n) = n^n.$$

Our definition differs from Holden's definition in [Hol02b, HR11], where $n \in \mathbb{N}$ is mapped to $n^n \bmod p$ (or $p^e$). Since some authors also consider $n^n \bmod b$ for composite $b$ [GOM12], we give this more general definition. However, from now on we will consider the image of the self-power map modulo a prime $p$.

## 1.1 The self-power map and the discrete logarithm problem

We begin by describing two applications to cryptography that motivate the study of the self-power map. The self-power map and its image modulo a prime $p$ is related to the discrete logarithm problem in $(\mathbb{Z}/p\mathbb{Z})^\times$.

**Definition 1.2.** *The discrete logarithm problem in $(\mathbb{Z}/p\mathbb{Z})^\times$ is the following: Given $g \in (\mathbb{Z}/p\mathbb{Z})^\times$, and $h$ an element in the subgroup generated by $g$, find an integer $a$ such that $g^a \equiv h \bmod p$.*

While it is computationally easy to raise an element to a power, the discrete logarithm problem, which is the inverse operation, is assumed to be difficult in general. Thus, the security of many cryptographic applications is based on this one-way property, and the discrete logarithm has been widely studied.

### 1.1.1 ElGamal signature scheme

One of the applications of the discrete logarithm is the ElGamal signature scheme. However, the security of two variations of the ElGamal signature scheme also rely on the difficulty of inverting the self-power map.

Algorithms 1 and 2 describe the ElGamal signature algorithm, taken from [MvOV96], section 11.5.2, and [FLM10]. We assume that Alice is sending a message $m$ to Bob, and she would like to sign it so that Bob can verify her identity.

**Algorithm 1** Generation of Alice's public and secret key

1: Choose a large random prime $p$ and a generator $g$ of $(\mathbb{Z}/p\mathbb{Z})^\times$.

2: Select a random integer $a$ such that $1 \leq a \leq p-1$ and compute $y = g^a$.

3: Alice's public key is $(p, g, y)$ and her private key is $a$.

**Algorithm 2** ElGamal signature generation and verification

1: Alice's signature generation:

**(a)** Select a random integer $k$ such that $1 \leq k \leq p-2$ and $\gcd(k, p-1) = 1$.

**(b)** Compute $r = g^k \mod p$.

**(c)** Compute $s = k^{-1}(h(m) - ar)$ where the inverse of $k$ is calculated modulo $(p-1)$ and $h(m)$ is the hash of the message $m$.

**(d)** Alice's signature for the message of $m$ is the pair $(r, s)$.

**Algorithm 2** ElGamal signature generation and verification (continued)

2: Verification of the signature by Bob:

**(a)** Verify that $1 \leq r \leq p-1$, else reject.

**(b)** Compute $v_1 = y^r r^s \mod p$.

**(c)** Compute $v_2 = g^{h(m)} \mod p$, after calculating $h(m)$.

**(d)** Accept the signature if $v_1 = v_2$.

The signature verification in Algorithm 2 works because

$$\begin{aligned} v_1 &= y^r r^s \mod p \\ &\equiv (g^a)^r \left(g^k\right)^{k^{-1}(h(m)-ar)} \mod p \\ &\equiv g^{ar} g^{h(m)-ar} \mod p \\ &\equiv g^{h(m)} \mod p \\ &= v_2. \end{aligned}$$

Variations of the ElGamal signature scheme may be obtained by changing the value of $s$ in step 1(c) of the signing algorithm, Algorithm 2. Notice that the signing equation in terms of the exponents can be also expressed as

$$u = av + kw \mod (p-1)$$

where

$$u = h(m), \quad v = r, \quad w = s.$$

Assigning to $u$, $v$ and $w$ the values $s$, $r$, and $h(m)$ in different orders defines a new signing equation, which produces a different expression for $s$ in terms of $a$, $k$, $r$, and $h(m)$. Table 1.1 from [MvOV96, Table 11.5] summarizes the possibilities.

The verification equations for variations 2 and 4 involve the expression $r^r$. Thus, an adversary who can solve the self-power problem may forge Alice's signature by choosing

| | $u$ | $v$ | $w$ | Signing equation | Verification |
|---|---|---|---|---|---|
| 1 | $h(m)$ | $r$ | $s$ | $h(m) = ar + ks$ | $g^{h(m)} = (g^a)^r r^s$ |
| 2 | $h(m)$ | $s$ | $r$ | $h(m) = as + kr$ | $g^{h(m)} = (g^a)^s r^r$ |
| 3 | $s$ | $r$ | $h(m)$ | $s = ar + kh(m)$ | $g^s = (g^a)^r r^{h(m)}$ |
| 4 | $s$ | $h(m)$ | $r$ | $s = ah(m) + kr$ | $g^s = (g^a)^{h(m)} r^r$ |
| 5 | $r$ | $s$ | $h(m)$ | $r = as + kh(m)$ | $g^r = (g^a)^s r^{h(m)}$ |
| 6 | $r$ | $h(m)$ | $s$ | $r = ah(m) + ks$ | $g^r = (g^a)^{h(m)} r^s$ |

Table 1.1: Variations of the ElGamal signing equation. Signing equations are computed modulo $(p-1)$; verification is done modulo $p$.

$s$, then solving

$$g^{h(m)} \left[(g^a)^s\right]^{-1} = r^r \quad \text{or} \quad g^s \left[(g^a)^{h(m)}\right]^{-1} = r^r,$$

for $r$.

### 1.1.2 Two-cycles of the discrete logarithm

Another application of the discrete logarithm related to the self-power map is a pseudo-random bit generator of Blum and Micali [BM84].

Let $g_0$ be a fixed generator of $(\mathbb{Z}/p\mathbb{Z})^\times$. Associating the residue classes modulo $p-1$ with integers between 1 and $p$, we can define the following function

$$f(x) = g_0^x \bmod p$$

from the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$ to itself. Blum and Micali [BM84] describe a pseudo-random bit generator which depends on an iteration $\left\{x, f(x), f^2(x), \ldots, f^N(x)\right\}$. The pseudo-randomness of the sequence is compromised if the iteration falls into a fixed point or a short cycle.

Cycles of length two of the discrete logarithm, of the form

$$g^h = a \bmod p \quad \text{and} \quad g^a = h \bmod p, \tag{1.1}$$

are related to collisions of the self-power map

$$h^h \equiv a^a \pmod{p}. \tag{1.2}$$

Given a solution $(g, h, a)$ to equation (1.1), the values $h$ and $a$ also satisfy equation (1.2). In certain cases, solutions to (1.2) also produce solutions to (1.1). Holden and his co-authors study the relationship between two-cycles of the discrete logarithm and collisions of the self-power map modulo $p$ in [Hol02b, Hol02a, HM06]. We reproduce the following proposition from [HM06].

**Proposition 1.3.** *If* $\gcd(h, a, p-1) = 1$*, then there is a one-to-one correspondence between triples* $(g, h, a)$ *which satisfy (1.1) and pairs* $(h, a)$ *which satisfy (1.2), and the value of* $g$ *is unique given* $h$ *and* $a$*. In particular, this is true when* $h$ *or* $a$ *is relatively prime to* $p - 1$*.*

*Proof.* Fix an arbitrary primitive root $b \pmod{p}$, and denote by $\operatorname{ind} x$ the discrete logarithm modulo $p$ of $x$ with respect to the base $b$. That is,

$$\operatorname{ind} x = y \quad \Leftrightarrow \quad b^y \equiv x \pmod{p}.$$

The system of equations (1.1) is then equivalent to the following system

$$\begin{cases} h \operatorname{ind} g \equiv \operatorname{ind} a & \bmod (p-1) \\ a \operatorname{ind} g \equiv \operatorname{ind} h & \bmod (p-1). \end{cases} \tag{1.3}$$

If $\gcd(h, a, p-1) = d$, there exist $u$ and $v$ such that $uh + va \equiv d \bmod p - 1$. Using elementary operations on systems of equations, we can show with a bit of work that (1.3) is equivalent to the following system:

$$\begin{cases} 0 \equiv \frac{a}{d} \operatorname{ind} a - \frac{h}{d} \operatorname{ind} h & \bmod p - 1 \\ g^d \equiv h^v a^u & \bmod p. \end{cases} \tag{1.4}$$

In our case $\gcd(h, a, p-1) = 1$, and we obtain the equivalent system:

$$\begin{cases} a^a & \equiv & h^h & \mod p \\ g & \equiv & h^v a^u & \mod p. \end{cases} \tag{1.5}$$

□

Many heuristics for the number of solutions of two-cycles of the discrete logarithm and collisions of the self-power map modulo a prime are given in Holden's work.

## 1.2 Past work on the self-power map

While we have described the cryptographic applications related to the self power map and its image modulo a prime, the behaviour of the self-power map is an interesting problem in its own right.

Past work on the self power map was limited to the case $1 \leq n \leq p-1$. We begin our study with the simple question:

**Question 1.4.** *Given any residue class $a$ modulo $p$, does there exist $n$ such that $n^n \equiv a \mod p$ and $1 \leq n \leq p-1$?*

The answer is no, not necessarily. When restricted to $1 \leq n \leq p-1$ the self power map is not injective, and thus not surjective, since the residue 1 appears at least twice:

$$1^1 \equiv (p-1)^{(p-1)} \equiv 1 \mod p.$$

The earliest results on the self-power map are due to Crocker [Cro69], who gives the lower bound on the number of distinct residue classes that are represented by $\{n^n : 1 \leq n \leq p-1\}$.

**Theorem 1.5.** *Let $p$ be an odd prime. The number of distinct residues modulo $p$ of $n^n$, where $1 \leq n \leq p-1$, is at least $\left\lfloor \sqrt{(p-1)/2} \right\rfloor$.*

Somer [Som81] gives an upper bound.

**Theorem 1.6.** *Let $p$ be an odd prime. The number of distinct residues modulo $p$ of $n^n$, where $1 \leq n \leq p-1$, is at most $\frac{3}{4}p + O_\epsilon\left(p^{\frac{1}{2}+\epsilon}\right)$, where $\epsilon$ is any positive real number and the impicit constant depends only on $\epsilon$.*

The upper bound is proved by bounding the number quadratic non-residues which do not appear among the residues of $n^n \bmod p$ when $1 \leq n \leq p-1$. The constant is related to the class number of $\mathbb{Q}(\sqrt{-p})$.

Somer finds lower bounds for the number of primitive roots modulo $p$ which do not appear as residues of $n^n \bmod p$. Given any $M \in \mathbb{N}$, he shows that the residue 1 (or $-1$) appears at least $M$ times as $n^n \bmod p$ for some large prime $p$. Thus a related question is the following:

**Question 1.7.** *What is the number of times that a residue class may be represented in the form $n^n \bmod p$ with $1 \leq n \leq p-1$?*

More recently, Balog, Broughan, and Shparlinski [BBS11] have given bounds on the number of times a residue class appears, depending on its multiplicative order in $(\mathbb{Z}/p\mathbb{Z})^\times$. Let us introduce the following notation.

**Definition 1.8.** *Denote by*

$$N(x;a) = \left|\{n \leq x : \ n^n \equiv a \pmod{p}\}\right|,$$

*the number of solutions to $n^n = a \bmod p$ with $1 \leq n \leq x$.*

Balog et al. [BBS11] give the following bounds.

**Theorem 1.9.** *Uniformly over $t|(p-1)$ and all integers $a$ with $\gcd(a,p) = 1$ of multiplicative order $t$, the following bounds hold as $p \to \infty$:*

$$N(p;a) \ \leq \ \max\left\{t, p^{\frac{1}{2}}t^{\frac{1}{4}}\right\} p^{o(1)},$$

$$\begin{aligned} N(p;a) &\leq p^{\frac{1}{3}+o(1)}t^{2/3}, \\ N(p;a) &\leq p^{1+o(1)}t^{-1/12}. \end{aligned}$$

The first two bounds are most useful when the order of $t$ is small, while the last is useful when $a$ has large order. In Chapter 2 our proofs will follow those of Balog et al. very closely to extend these estimates to $N(x;a)$, for $p < x \leq p(p-1)$.

## 1.3 Extension to larger values of $n$

As a variation of the Question 1.4, we may ask:

**Question 1.10.** *If we do not restrict $n$ to $1 \leq n \leq p-1$ can we find a solution to $n^n \equiv a \bmod p$, for any $a$?*

The answer is yes, if we allow $1 \leq n \leq p(p-1)$. Given any $a$ such that $1 \leq a \leq p-1$, then $a$ may be expressed as $n^n$ by taking

$$n = a + p(p-a) = 1 + (p-1)(p+1-a)$$

because

$$n^n = (a + p(p-a))^{1+(p-1)(p+1-a)} \equiv a \bmod p.$$

The sequence $\{n^n\}$ is periodic with period $p(p-1)$.

Given $n^n \bmod p$, the base is determined modulo $p$ and the exponent is determined modulo $p-1$. Thus, we may organize the values of $n^n \bmod p$ where $\gcd(n,p) = 1$ as in Table 1.2, by multiples of $p$. Reducing the base modulo $p$ and the exponent modulo $p-1$ gives us Table 1.3. An example for $p = 11$ is given in Table 1.4.

The number of times a residue $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order $t$ appears in Table 1.3 is

$$\sum_{k \mid \frac{p-1}{t}} \phi(kt) \cdot \frac{p-1}{kt}, \tag{1.6}$$

from Theorem 1 of [Som81]. If $p-1$ is square free, it can also be estimated in the following way, independently found by R. Balasubramanian, [Bal11].

| | Values of $n^n$, where $n = kp + b$ | | | |
|---|---|---|---|---|
| $b$ | 1 | 2 | ... | $(p-1)$ |
| $k = 0$ | $1^1$ | $2^2$ | ... | $(p-1)^{(p-1)}$ |
| $k = 1$ | $(p+1)^{(p+1)}$ | $(p+2)^{(p+2)}$ | ... | $(2p-1)^{(2p-1)}$ |
| $k = 2$ | $(2p+1)^{(2p+1)}$ | $(2p+2)^{(2p+2)}$ | ... | $(3p-1)^{(3p-1)}$ |
| $k = 3$ | $(3p+1)^{(3p+1)}$ | $(3p+2)^{(3p+2)}$ | ... | $(4p-1)^{(4p-1)}$ |
| $\vdots$ | $\vdots$ | | | |
| $k = (p-2)$ | $((p-2)p+1)^{((p-2)p+1)}$ | $((p-2)p+2)^{((p-2)p+2)}$ | ... | $((p-1)p-1)^{((p-1)p-1)}$ |

Table 1.2: The table of values of $n^n$, arranged by groups of $p$, omitting multiples of $p$.

| | Values of $n^n \bmod p$, where $n = kp + b$ | | | | | |
|---|---|---|---|---|---|---|
| $b$ | 1 | 2 | 3 | ... | $(p-2)$ | $(p-1)$ |
| $k = 0$ | $1^1$ | $2^2$ | $3^3$ | ... | $(p-2)^{p-2}$ | $(p-1)^{p-1}$ |
| $k = 1$ | $1^2$ | $2^3$ | $3^4$ | ... | $(p-2)^{p-1}$ | $(p-1)^1$ |
| $k = 2$ | $1^3$ | $2^4$ | $3^5$ | ... | $(p-2)^1$ | $(p-1)^2$ |
| $\vdots$ | $\vdots$ | | | | | |
| $k = (p-2)$ | $1^{p-1}$ | $2^1$ | $3^2$ | ... | $(p-2)^{p-3}$ | $(p-1)^{p-2}$ |

Table 1.3: The values of $n^n$ from Table 1.2 considered modulo $p$, where the base is reduced modulo $p$, and the exponent modulo $p-1$.

| | Values of $n^n$ mod $p$, for $p = 11$ | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $b$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Order of $b$ | 1 | 10 | 5 | 5 | 5 | 10 | 10 | 10 | 5 | 2 |
| | 1 | 4 | 5 | 3 | 1 | 5 | 6 | 5 | 5 | 1 |
| | 1 | 8 | 4 | 1 | 5 | 8 | 9 | 7 | 1 | 10 |
| | 1 | 5 | 1 | 4 | 3 | 4 | 8 | 1 | 9 | 1 |
| | 1 | 10 | 3 | 5 | 4 | 2 | 1 | 8 | 4 | 10 |
| | 1 | 9 | 9 | 9 | 9 | 1 | 7 | 9 | 3 | 1 |
| | 1 | 7 | 5 | 3 | 1 | 6 | 5 | 6 | 5 | 10 |
| | 1 | 3 | 4 | 1 | 5 | 3 | 2 | 4 | 1 | 1 |
| | 1 | 6 | 1 | 4 | 3 | 7 | 3 | 10 | 9 | 10 |
| | 1 | 1 | 3 | 5 | 4 | 9 | 10 | 3 | 4 | 1 |
| | 1 | 2 | 9 | 9 | 9 | 10 | 4 | 2 | 3 | 10 |

Table 1.4: An example of the $n^n$ mod $p$ table reduced modulo $p$, for $p = 11$.

**Proposition 1.11.** *Let $a$ be an element of order $t$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Define a multiplicative function on square-free numbers by setting*

$$g(q) = 2q - 1$$

*where $q$ is prime. Assuming $p - 1$ is squarefree,*

$$N(p(p-1); a) = \phi(t) g\left(\frac{p-1}{t}\right).$$

*Proof.* In Table 1.3, for $b \in (\mathbb{Z}/p\mathbb{Z})^\times$, each column consists of the elements

$$b^b, b^{b+1}, b^{b+2}, \ldots, b^{p-1}, b^p, \ldots, b^{b-1}.$$

Each column is a permutation of

$$1, b, b^2, \ldots, b^{p-1}.$$

The residue class $a$ will appear in any column where the order of $b$ is a multiple of the order of $a$. Letting $\operatorname{ord} a = t$ and $\operatorname{ord} b = kt$, then $a$ will occur $(p-1)/kt$ times in this column. Hence, the total number of times $a$ appears in the table is

$$\begin{aligned}\sum_{k|\frac{p-1}{t}} \phi(kt) \cdot \frac{p-1}{kt} &= (p-1)\frac{\phi(t)}{t} \sum_{k|\frac{p-1}{t}} \frac{\phi(k)}{k} \\ &= (p-1)\frac{\phi(t)}{t} \cdot \frac{g\left(\frac{p-1}{t}\right)}{\left(\frac{p-1}{t}\right)} = \phi(t) g\left(\frac{p-1}{t}\right)\end{aligned}$$

□

The residues $n^n \bmod p$ in Table 1.3 are not equidistributed, but depend on the order of $n$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. In particular, elements of lower order appear more frequently than those of higher order. Holden [HR11] conjectured that

$$N(p;a) \sim \sum_{k|\frac{p-1}{t}} \frac{\phi(kt)}{kt}$$

which is $1/(p-1)$-th the number of times the element $a$ appears in the entire table, over one period of the sequence $\{n^n\}$.

The question we study in the second part of the thesis is the following:

**Question 1.12.** *How large should $x$ be so that $n^n \equiv a \bmod p$ has a solution with $1 \leq n \leq x$, for any given residue class $a$ modulo $p$?*

The trivial bounds for $x$ are $p < x \leq p(p-1)$. A probabilistic model, described in Chapters 3 and 4 provides a heuristic argument to show that the value of $x$ is approximately $p^2 \log \phi(p-1)/\phi(p-1)$. In Chapter 5, we rigorously prove that $x < p^{2-\alpha}$ for large enough $p$, for an explicit value $\alpha > 0$, which is independent of $p$.

# Chapter 2

# Bounds on $N(x;a)$

## 2.1 Introduction

Recall that $N(x;a)$ denotes the number of solutions to the congruence $n^n = a \mod p$ with $1 \leq n \leq x$ for a fixed residue class $a$ modulo $p$. Balog et al. [BBS11] give estimates for $N(p;a)$ and we extend those estimates to $N(x;a)$ for $x > p$. The sequence $n^n$ has period $p(p-1)$. Thus, we may consider only $p < x < p(p-1)$ since if $x$ is larger than $p(p-1)$ we can add an appropriate factor of $N(p(p-1);a)$, evaluated using equation (1.6) or Prop. 1.11.

The method of proof is completely analogous to that of Balog et al. [BBS11]. The value $N(p;a)$ is the number of occurrences of the residue class $a \bmod p$ in the first row of Table 1.3. We obtain bounds for $N(x;a)$ which are approximately $(x/p)$ times the bounds for $N(p;a)$, as expected; the residue class $a \bmod p$ should appear about equally often in each row. Thus, if $a = 1$, for instance,

$$N(x;1) \leq x^{1+\epsilon}p^{-2/3}$$

from Proposition 2.3, with $t = 1$. If $a$ is a primitive root, the estimate for $a$ of large order gives

$$N(x;a) \ll xp^{-1/12+\epsilon}$$

using Prop. 2.5. This bound is nontrivial for $x \leq p^{13/12-\epsilon}$.

## 2.2 Estimates for $N(x;a)$ for $a$ of small order

This section describes two estimates for $N(x;a)$ that are non-trivial when $a$ has relatively small multiplicative order. For any element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, and given a fixed primitive root $g$, let $\operatorname{ind} a$ denote the discrete logarithm modulo $p$ of $a$ with respect to the base $g$. That is,

$$\operatorname{ind} a = b \quad \Leftrightarrow \quad g^b \equiv a \bmod p.$$

The sum representing the number of divisors, denoted $\mathbf{d}(T) = \sum_{d|T} 1$ will occur several times in the proofs. We will use the bound

$$\sum_{d|T} 1 \ll T^\epsilon. \tag{2.1}$$

Aside from elementary number arguments, Proposition 2.2 also requires the following sum-product result of Garaev ([Gar08], Theorem 1). Let $\mathcal{A}$ be a subset of $(\mathbb{Z}/p\mathbb{Z})^\times$. Define the sets

$$\begin{aligned} \mathcal{A}+\mathcal{A} &= \{a_1+a_2 : a_1, a_2 \in \mathcal{A}\} \\ \mathcal{A}\cdot\mathcal{A} &= \{a_1 a_2 : a_1, a_2 \in \mathcal{A}\}. \end{aligned}$$

**Lemma 2.1.** *For any set $\mathcal{A} \subset (\mathbb{Z}/p\mathbb{Z})^\times$*

$$|\mathcal{A}+\mathcal{A}| \cdot |\mathcal{A}\cdot\mathcal{A}| \gg \min\left\{ p|\mathcal{A}|, \frac{|\mathcal{A}|^4}{p} \right\}.$$

A suggestion from I. Shparlinski for the definition of the set $W_d$ greatly simplified the following proposition. [Shp13]

**Proposition 2.2.** *Uniformly in $t|(p-1)$, we have for $p \leq x \leq p(p-1)$*

$$\sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \operatorname{ord} a | t}} N(x;a) \ll x^{1+\epsilon} p^{-1} \max\left\{ t, p^{1/2} t^{1/4} \right\}. \tag{2.2}$$

*Proof.* Consider the $(k+1)$st row of the Table 1.3. We denote the number of times a fixed residue class $a \pmod p$ appears in the $(k+1)$st row by

$$N_k(p;a) = \left|\left\{n \in \mathbb{Z} : n^{n+k} \equiv a \pmod p, \quad \gcd(a,p) = 1, \quad 1 \le n \le p-1\right\}\right|.$$

We will show that we can bound $N_k(p;a)$ in the same way as $N(p;a)$ is bounded in Balog et al.

Fix a primitive root $g \bmod p$. We use $g$ as the base of the discrete logarithm, so that we can express $n = g^{\operatorname{ind} n}$. Let $t$ denote the multiplicative order of $a$ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Then starting from the equivalence $n^{n+k} \equiv a \pmod p$, we obtain:

$$\begin{aligned} n^{t(n+k)} &\equiv 1 \pmod p \\ \Leftrightarrow g^{(\operatorname{ind} n)t(n+k)} &\equiv 1 \pmod p \\ \Leftrightarrow (n+k)t(\operatorname{ind} n) &\equiv 0 \pmod{p-1}. \end{aligned}$$

Set $T = \frac{p-1}{t}$. The last condition is equivalent to

$$(n+k)(\operatorname{ind} n) \equiv 0 \pmod T.$$

Suppose that $\gcd(n+k,T) = d$ so that $n+k = dy$. We have $\gcd(y,T) = 1$ and $1 \le y \le \frac{(p-1+k)}{d}$. Let $D = \frac{(p-1+k)}{d}$ and note that $D < \frac{2p}{d}$. Then,

$$dy \operatorname{ind}(dy-k) \equiv 0 \pmod T.$$

Setting $T_d = \frac{T}{d}$,

$$\begin{aligned} y \operatorname{ind}(dy-k) &\equiv 0 \pmod{T_d}, \\ \operatorname{ind}(dy-k) &\equiv 0 \pmod{T_d}. \end{aligned}$$

Set

$$\begin{aligned} X_d &= \{y \in \mathbb{Z} : \operatorname{ind}(dy-k) \equiv 0 \pmod{T_d}, \quad 1 \le y \le D, \quad \gcd(y,T_d) = 1\} \\ W_d &= \left\{\bar{y} : \quad \bar{y} \equiv y - kd^{-1} \pmod p,\ y \in X_d\right\}. \end{aligned}$$

Then

$$\sum_{\substack{a\in(\mathbb{Z}/p\mathbb{Z})^\times \\ \operatorname{ord} a|t}} N_k(a,p) = \sum_{d|T} |X_d| \leq 2\sum_{d|T} |W_d|,$$

since $y \in X_d$ is bounded from above by $2p$. To bound this sum, we will apply the sum-product theorem to estimate $|W_d|$.

We have

$$|W_d + W_d| \leq |X_d + X_d| \leq 2D < \frac{4p}{d}.$$

To estimate $|W_d \cdot W_d|$ consider two elements $\bar{y}_1$ and $\bar{y}_2$ in $W_d$. These correspond to some elements $y_1$ and $y_2$ in $X_d$, such that $dy_1 - k \equiv g^{T_d\alpha_1} \pmod p$ and $dy_2 - k \equiv g^{T_d\alpha_2} \pmod p$. Thus,

$$\begin{aligned} d^2\bar{y}_1\bar{y}_2 &\equiv d(y_1 - kd^{-1})d(y_2 - kd^{-1}) \pmod p \\ &\equiv (dy_1 - k)(dy_2 - k) \pmod p \\ &\equiv g^{T_d\alpha_1}g^{T_d\alpha_2} \pmod p \\ &\equiv g^{T_d(\alpha_1+\alpha_2)} \pmod p. \end{aligned}$$

We conclude that

$$\bar{y}_1\bar{y}_2 \equiv d^{-2}g^{T_d(\alpha_1+\alpha_2)} \pmod p.$$

There are $(p-1)/T_d = dt$ choices for the sum $(\alpha_1 + \alpha_2)$, thus we obtain

$$|W_d \cdot W_d| \leq dt.$$

By the Lemma 2.1, we have that

$$\min\left\{p\,|W_d|\,, \frac{|W_d|^4}{p}\right\} \ll |W_d + W_d| \cdot |W_d \cdot W_d| \ll pt,$$

and we note that

$$p\,|W_d| \leq \frac{|W_d|^4}{p} \quad \Leftrightarrow \quad |W_d| \geq p^{2/3}.$$

We obtain as in Balog et al.

$$|W_d| \ll \max\left\{t, p^{\frac{1}{2}}t^{\frac{1}{4}}\right\}. \ll \begin{cases} t & \text{if } t \geq p^{\frac{2}{3}} \\ p^{\frac{1}{2}}t^{\frac{1}{4}} & \text{if } t < p^{\frac{2}{3}}. \end{cases}$$

Applying the bound from (2.1), and noting that $T < p$ we obtain

$$\sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a | t}} N_k(p;a) \ll \sum_{d|T} |W_d| \ll \max\left\{t, p^{\frac{1}{2}}t^{\frac{1}{4}}\right\} p^\epsilon$$

and

$$\begin{aligned} \sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a | t}} N(x;a) &= \sum_{k=0}^{\left\lfloor \frac{x}{p} \right\rfloor} \sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a | t}} N_k(p;a) \\ &\ll \left(\frac{x}{p} + 1\right) \max\left\{t, p^{1/2}t^{1/4}\right\} p^\epsilon \\ &\ll \begin{cases} x^{1+\epsilon}p^{-1}t & \text{if } t \geq p^{\frac{2}{3}} \\ x^{1+\epsilon}p^{-\frac{1}{2}}t^{\frac{1}{4}} & \text{if } t < p^{\frac{2}{3}}. \end{cases} \end{aligned}$$

□

Another estimate obtained for $a$ of small order follows exactly as in Balog et al.

**Proposition 2.3.** *Uniformly over $t|(p-1)$, for $p \leq x \leq p(p-1)$, we have as $p \to \infty$,*

$$\sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a | t}} N(x;a) \ll x^{1+\epsilon}p^{-\frac{2}{3}}t^{\frac{2}{3}}.$$

*Proof.* The first part of the proof is similar to Proposition 2.2, up until the definition of the sets $X_d$ and $W_d$. This time, however, we only restrict $n$ to be between 1 and $x$. Fix a primitive root $g$ mod $p$. We have

$$\sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a | t}} N(x;a) = \sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a | t}} \sum_{\substack{n \leq x \\ n^n \equiv a \bmod p}} 1 = \sum_{\substack{n \leq x \\ n^{tn} \equiv 1 \bmod p}} 1.$$

We use $g$ as the base of the discrete logarithm. Starting from the equivalence $n^{tn} \equiv 1 \bmod p$ we obtain:

$$\begin{aligned} n^{tn} &\equiv 1 \pmod{p}, \\ \Leftrightarrow \quad g^{(\operatorname{ind} n)tn} &\equiv 1 \pmod{p} \\ \Leftrightarrow \quad (\operatorname{ind} n)tn &\equiv 0 \pmod{p-1} \end{aligned}$$

Set $T = \frac{p-1}{t}$. Then the last condition implies

$$n(\operatorname{ind} n) \equiv 0 \pmod{T}.$$

Fix $d|T$ and set $T_d = \frac{T}{d}$. If $\gcd(n,T) = d$, then write $n = dy$ and

$$y(\operatorname{ind} dy) \equiv 0 \pmod{T_d} \Leftrightarrow \operatorname{ind} dy \equiv 0 \pmod{T_d}$$

since

$$\gcd(y, T_d) = 1, \quad 1 \le y \le D = \frac{x}{d}.$$

Set

$$\begin{aligned} X_d &= \{y \in \mathbb{Z}, 1 \le y \le D : \operatorname{ind} dy \equiv 0 \pmod{T_d}, \gcd(y, T_d) = 1\} \\ W_d &= \{y \pmod{p} : y \in X_d\}. \end{aligned}$$

We now denote both elements of $X_d$ and $W_d$ by $y$, since the elements of $W_d$ are simply residue classes of elements in $X_d$.

Our goal is to estimate the sum

$$\sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \operatorname{ord} a | t}} N(x;a) = \sum_{d|T} |X_d|.$$

We also have

$$|X_d| \le \left(\frac{D}{p} + 1\right) |W_d| = \left(\frac{x}{dp} + 1\right) |W_d|.$$

Let

$$s(b) = \#\{(y_1, y_2) : y_1, y_2 \in X_d, y_1 y_2 \equiv b \pmod{p}\}.$$

Thus $s(b) > 0$ implies that $b \in W_d \cdot W_d$. Hence

$$|X_d|^2 = \sum_{b \in \mathbb{Z}/p\mathbb{Z}} s(b) \leq |W_d \cdot W_d| \cdot \max s(b).$$

For a given $b$, since $y_1 y_2 \leq D^2 = x^2/d^2$ and $y_1 y_2 = b + kp$, the product $y_1 y_2$ can take at most

$$\left(\frac{x^2}{pd^2} + 1\right)$$

values. Once $z$ such that $y_1 y_2 = z$ is fixed, there are

$$\mathbf{d}(z) = z^{o(1)} \leq \left(\frac{x}{d}\right)^{2o(1)} \leq \left(\frac{x}{d}\right)^{\epsilon}$$

possibilities for the pair $(y_1, y_2)$. Hence

$$s(b) \leq \left(\frac{x^2}{pd^2} + 1\right)\left(\frac{x}{p}\right)^{\epsilon}$$

By a similar argument as in the proof of Proposition 2.2, if $y_1$ and $y_2 \in W_d$, then $d^2 y_1 y_2 \equiv g^{T_d(\alpha_1+\alpha_2)} \pmod{p}$ and we have $|W_d \cdot W_d| \leq dt$.

Therefore

$$\begin{aligned} |X_d|^2 &\leq dt\left(\frac{x^2}{pd^2} + 1\right)\left(\frac{x}{p}\right)^{\epsilon} \\ |X_d| &\ll \left(\frac{x}{p}\right)^{\epsilon}\left(\frac{x\sqrt{t}}{\sqrt{pd}} + \sqrt{td}\right). \end{aligned}$$

On the other hand, from the condition $\operatorname{ind}(dy) \equiv 0 \pmod{T_d}$ we have

$$|X_d| \leq \left(\frac{x}{dp} + 1\right) dt \leq \left(\frac{x}{p} + 1\right) dt$$

From the condition $y \leq D$, we have also

$$|X_d| \leq D = \frac{x}{d}.$$

We choose the intervals $d \leq p^{\frac{1}{3}} t^{-\frac{1}{3}}$, $p^{\frac{1}{3}} t^{-\frac{1}{3}} \leq d \leq p^{\frac{2}{3}} t^{-\frac{1}{3}}$, and $d \geq p^{\frac{2}{3}} t^{-\frac{1}{3}}$ as in the proof of Balog et al. These intervals are chosen such that the bounds all have similar

(though not equal) orders of magnitude. We conclude that

$$|X_d| \ll \begin{cases} \left(\frac{x}{p}+1\right) dt & \text{if } d \le p^{\frac{1}{3}}t^{-\frac{1}{3}} \\ \left(\frac{x}{p}\right)^{\epsilon} dt \left(\frac{x\sqrt{t}}{\sqrt{pd}} + \sqrt{td}\right) & \text{if } p^{\frac{1}{3}}t^{-\frac{1}{3}} \le d \le p^{\frac{2}{3}}t^{-\frac{1}{3}} \\ \frac{x}{d} & \text{if } d \ge p^{\frac{2}{3}}t^{-\frac{1}{3}} \end{cases}$$

which simplifies to

$$|X_d| \ll \begin{cases} xp^{-\frac{2}{3}}t^{\frac{2}{3}} & \text{if } d \le p^{\frac{1}{3}}t^{-\frac{1}{3}} \\ x^{1+\epsilon}p^{-\frac{2}{3}}t^{\frac{2}{3}} & \text{if } p^{\frac{1}{3}}t^{-\frac{1}{3}} \le d \le p^{\frac{2}{3}}t^{-\frac{1}{3}} \\ xp^{-\frac{2}{3}}t^{\frac{1}{3}} & \text{if } d \ge p^{\frac{2}{3}}t^{-\frac{1}{3}}. \end{cases}$$

We will use the largest bound above, $|X_d| \ll x^{1+\epsilon}p^{-\frac{2}{3}}t^{\frac{2}{3}}$ in the sum. Again, we apply the number of divisors bound (2.1). Thus, for $x \ge p$,

$$\sum_{\substack{a\in(\mathbb{Z}/p\mathbb{Z})^\times \\ \text{ord}\, a|t}} N(x;a) = \sum_{d|T} |X_d| \le T^{\epsilon}x^{1+\epsilon}p^{-\frac{2}{3}}t^{\frac{2}{3}} \ll x^{1+\epsilon}p^{-\frac{2}{3}}t^{\frac{2}{3}}.$$

□

## 2.3 Estimates for $N(x;a)$ for $a$ of large order

Next we consider a method of bounding $N(x;a)$ that is good when $a$ has large order. We require the following lemma from Balog et al.[BBS11], from [CFK+00, Lemma 7].

**Lemma 2.4.** *For $n \ge 2$, given elements $a_1, \dots, a_n \in \mathbb{F}_q^\times$, and integers $k_1, \dots, k_n \in \mathbb{Z}$, let us denote by $Q$ the number of solutions of the equation*

$$\sum_{i=1}^{n} a_i X^{k_i} = 0, \qquad X \in \mathbb{F}_q^\times.$$

*Then*

$$Q \le 2q^{1-1(n-1)}\Delta^{1/(n-1)} + O(q^{1-2/(n-1)}\Delta^{2/(n-1)}),$$

*where*

$$\Delta = \min_{1\le i\le n} \max_{j\neq i} \gcd\left(k_j - k_i, q-1\right).$$

**Proposition 2.5.** *Uniformly over $t|(p-1)$ and all integers $a$ with $\gcd(a,p)=1$ of multiplicative order $\operatorname{ord} a = t$, we have as $p\to\infty$*

$$N(x;a) \ll xp^{\epsilon}t^{-\frac{1}{12}}.$$

*for $p \le x \le p(p-1)$.*

*Proof.* We consider Table 1.3 of $n^n \bmod p$. We divide each row of the table into two sets. For $a$ with $\gcd(a,p)=1$, let

$$\begin{aligned} N_{k,1}(p;a) &= \#\left\{n\in\mathbb{Z} : n^{n+k} \equiv a \pmod p, \quad 1\le n\le p-1-k\right\} \\ N_{k,2}(p;a) &= \#\left\{n\in\mathbb{Z} : n^{n+k-p+1} \equiv a \pmod p, \quad p-k\le n\le p-1\right\}. \end{aligned}$$

We will then have

$$N(x;a) = \sum_{k=0}^{\lfloor x/p\rfloor} \left(N_{k,1}(p;a) + N_{k,2}(p;a)\right).$$

The purpose of splitting each row into two sets is that the proof of Balog et al. is easily modified for each of the two sets, since the exponents are small. Below we will show that the bound for $N(p;a)$ from Balog et al. also holds for $N_{k,1}(p;a)$. The proof for $N_{k,2}(p;a)$ is analogous.

As before, let $\operatorname{ord} a = t$ and set $T = \frac{p-1}{t}$. There exists a primitive root $g$ such that $a \equiv g^T \pmod p$. For the rest of this argument, the index (e.g. $\operatorname{ind} n$) will be the discrete logarithm modulo $p$ with respect to the base $g$. We have

$$\begin{aligned} & n^{n+k} \equiv a \pmod p \\ \Leftrightarrow \quad & n^{n+k} \equiv g^T \pmod p \\ \Leftrightarrow \quad & (n+k)\operatorname{ind} n \equiv T \pmod{p-1}. \end{aligned}$$

Thus, $\gcd(n+k,p-1)|T$ and we may let $\gcd(n+k,p-1)=d$, so that $n+k=dy$. Setting $T_d=\frac{T}{d}$, and $D=\frac{p-1}{d}$,

$$\begin{aligned} dy \operatorname{ind}(dy-k) &\equiv T \pmod{p-1} \\ \Leftrightarrow \quad y \operatorname{ind}(dy-k) &\equiv T_d \pmod{D}. \end{aligned}$$

In fact, we have $y=\frac{n+k}{d}$, so that $\frac{k}{d}\leq y\leq \frac{p-1}{d}$, where the second inequality is deliberately obtained from the construction of $N_{k,1}(p;a)$. Secondly, taking the lower bound to be 1 instead of $\frac{k}{d}$ only increases the number of solutions. These two modifications allow us to use Balog et al.'s proof with few adjustments.

Since $1\leq y\leq D, \gcd(y,D)=1$, the congruence $yz\equiv 1 \pmod{D}$ induces a 1-1 correspondence

$$\{1\leq y\leq D, \gcd(y,D)=1\} \leftrightarrow z\in(\mathbb{Z}/D\mathbb{Z})^{\times}$$

and a 1-to-$M_d$ correspondence

$$\{1\leq y\leq D, \gcd(y,D)=1\} \leftrightarrow z\in(\mathbb{Z}/(p-1)\mathbb{Z})^{\times},$$

where $M_d$ is the number of residue classes in $(\mathbb{Z}/(p-1)\mathbb{Z})^{\times}$ of the form $z+lD$. Residue classes are automatically coprime to $D$, but must be also coprime to $d$ in order to be coprime to $p-1$ and in $(\mathbb{Z}/(p-1)\mathbb{Z})^{\times}$. Using the Möbius function [NZM91, p.193], we have that

$$\begin{aligned} M_d &= \sum_{k=1}^{d} \sum_{f|\gcd(z+kD,d)} \mu(f) = \sum_{f|d}\mu(f) \sum_{\substack{k=1 \\ z+kD\equiv 0 \pmod f}}^{d} 1 \\ &= \sum_{\substack{f|d \\ \gcd(f,D)=1}} \mu(f)\frac{d}{f} = d\frac{\phi(m)}{m}, \end{aligned}$$

where

$$m=\prod_{\substack{q|d \\ q\nmid D}} q.$$

Using the estimate $\phi(m)=m^{1-o(1)}$ for the Euler totient function, and the inequality $m\leq d\leq p$, we have $M_d=dp^{o(1)}$. From now on $1\leq y\leq D$ and $z\in(\mathbb{Z}/(p-1)\mathbb{Z})^{\times}$ will always be related by $yz\equiv 1 \pmod{D}$, even if not explicitly stated.

Let us set

$$\mathcal{Z}_d = \left\{ z \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times : \operatorname{ind}(dy-k) \equiv \frac{Dz}{t} \pmod{D}, 1 \le y \le D, yz \equiv 1 \pmod{D} \right\}.$$

We have

$$N_{k,1}(p;a) = \sum_{d|T} \frac{1}{M_d} |\mathcal{Z}_d| \le p^{o(1)} \sum_{d|T} \frac{1}{d} |\mathcal{Z}_d|.$$

Thus, we must find a bound for $|\mathcal{Z}_d|$.

We have

$$\begin{aligned} \operatorname{ind}(dy-k) &\equiv \tfrac{Dz}{t} \pmod{D} \\ \Leftrightarrow \qquad dy-k &\equiv \rho g^{\frac{Dz}{t}} \pmod{p} \end{aligned}$$

for some $\rho \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$, $\rho^d \equiv 1 \pmod{p}$.

Split $\mathcal{Z}_d$ into subsets

$$\mathcal{Z}_{d,\rho} = \left\{ z \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times : dy-k \equiv \rho g^{\frac{Dz}{t}} \pmod{p}, 1 \le y \le D \right\},$$

so that

$$|\mathcal{Z}_d| = \sum_{\substack{\rho \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times \\ \rho^d \equiv 1 \pmod{p}}} |\mathcal{Z}_{d,\rho}|.$$

We have that

$$|\mathcal{Z}_{d,\rho}|^2 = \left| \left\{ z_1, z_2 \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times : dy_j \equiv \rho g^{\frac{Dz_j}{t}} + k \pmod{p}, j = 1,2 \right\} \right|$$

and adding the two congruences,

$$\begin{aligned} |\mathcal{Z}_{d,\rho}|^2 &\le \left| \left\{ z_1, z_2 \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times : d(y_1+y_2) \equiv \rho \left( g^{\frac{Dz_1}{t}} + g^{\frac{Dz_2}{t}} \right) + 2k \pmod{p} \right\} \right| \\ &= \sum_{v \in \mathbb{Z}} \left| \left\{ z_1, z_2 \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times : d(y_1+y_2) = v, \rho \left( g^{\frac{Dz_1}{t}} + g^{\frac{Dz_2}{t}} \right) \equiv v - 2k \pmod{p} \right\} \right|. \end{aligned}$$

The sum over $v \in \mathbb{Z}$ is empty unless $v = dw$, where $2 \le w \le 2D$ by the bounds on $y_1$ and $y_2$. By Cauchy-Schwartz,

$$|\mathcal{Z}_{d,\rho}|^4 \le \left( \sum_{v \in \mathbb{Z}} 1^2 \right) \left( \sum_{v \in \mathbb{Z}} \left| \left\{ z_1, z_2 \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times : d(y_1+y_2) = v, \right. \right. \right.$$

$$\rho\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)\equiv v-2k \pmod p\Big\}\Big|^2\Big)$$
$$\leq\ 2D\left|\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : d(y_1+y_2)=d(y_3+y_4)\right.$$
$$\left.\equiv\rho\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)+2k\equiv\rho\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right)+2k \pmod p\Big\}\right|.$$

For any fixed $\rho$, the set

$$\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : d(y_1+y_2)=d(y_3+y_4)$$
$$\equiv\rho\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)+2k\equiv\rho\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right)+2k \pmod p\Big\}$$

is contained in the set

$$\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : y_1+y_2=y_3+y_4,$$
$$\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)\equiv\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right) \pmod p\Big\}.$$

Since there are $d$ values for $\rho$ such that $\rho^d\equiv 1 \bmod p$, we have

$$\sum_{\rho^d\equiv 1 \bmod p}|\mathcal{Z}_{d,\rho}|^4 \leq \sum_{\rho^d\equiv 1 \bmod p} 2D\left|\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : d(y_1+y_2)=d(y_3+y_4)\right.$$
$$\left.\equiv\rho\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)+2k\equiv\rho\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right)+2k \pmod p\Big\}\right|$$
$$\leq\ 2D\sum_{\rho^d\equiv 1 \bmod p}\left|\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : y_1+y_2=y_3+y_4,\right.$$
$$\left.\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)\equiv\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right) \pmod p\Big\}\right|$$
$$=\ 2(p-1)\left|\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : y_1+y_2=y_3+y_4,\right.$$
$$\left.\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)\equiv\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right) \pmod p\Big\}\right|.$$

There is no longer any dependence on $k$ in the set above. The argument for bounding its number of elements is identical to the one in Balog et al. It is included here for the sake of completeness.

Relaxing the condition $y_1+y_2=y_3+y_4$ to $y_1+y_2\equiv y_3+y_4 \pmod D$ only increases the number of solutions. It also allows us to consider $y_j$ as a residue class modulo $D$, defined by $y_jz_j\equiv 1 \pmod D$, for $j=1,2,3,4$. Thus

$$\sum_{\rho^d\equiv 1 \bmod p}|\mathcal{Z}_{d,\rho}|^4 \leq 2p\left|\Big\{z_1,z_2,z_3,z_4\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : y_1+y_2\equiv y_3+y_4 \pmod D\right),$$

$$\left(g^{\frac{Dz_1}{t}}+g^{\frac{Dz_2}{t}}\right)\equiv\left(g^{\frac{Dz_3}{t}}+g^{\frac{Dz_4}{t}}\right)\pmod p\Big\}\Big|.$$

For $j=1,2,3,4$, the substitution

$$\begin{aligned} z_j &\to wz_j \\ y_j &\to w^{-1}y_j \end{aligned}$$

where $w\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times$ and $w^{-1}$ is defined modulo $D$ permutes the set $\{z_1,z_2,z_3,z_4\}$. Hence,

$$\begin{aligned}\sum_{\rho^d\equiv 1 \bmod p}|\mathcal{Z}_{d,\rho}|^4 \;\le\; \frac{2p}{\phi(p-1)}\Big|\big\{z_1,z_2,z_3,z_4,w\in(\mathbb{Z}/(p-1)\mathbb{Z})^\times : y_1+y_2\equiv y_3+y_4 \pmod D,\\ (g^w)^{\frac{Dz_1}{t}}+(g^w)^{\frac{Dz_2}{t}}\equiv(g^w)^{\frac{Dz_3}{t}}+(g^w)^{\frac{Dz_4}{t}}\pmod p\Big\}\Big|.\end{aligned}$$

Let $X=g^w$, and

$$k_j=\frac{Dz_j}{t}=\frac{(p-1)z_j}{dt}=T_dz_j,\quad\text{for}\quad j=1,2,3,4.$$

After fixing $z_1,z_2,z_3$, and $z_4$, the number of $w$ satisfying the condition

$$(g^w)^{\frac{Dz_1}{t}}+(g^w)^{\frac{Dz_2}{t}}\equiv(g^w)^{\frac{Dz_3}{t}}+(g^w)^{\frac{Dz_4}{t}}\pmod p$$

is bounded by the number of solutions to $X^{k_1}+X^{k_2}\equiv X^{k_3}+X^{k_4}\pmod p$, for $X\in\mathbb{F}_p^\times$. Applying Lemma 2.4 with $n=4$, we obtain the bound $O\left(p^{2/3}\Delta^{1/3}\right)$, where

$$\Delta=\min_{1\le i\le 4}\max_{j\ne i}\gcd\left(T_d(z_i-z_j),p-1\right)=T_d\min_{1\le i\le 4}\max_{j\ne i}\gcd(z_i-z_j,dt).$$

For every fixed $i,j$, such that $1\le i<j\le 4$ and $\delta|dt$ there are at most $(p-1)^2/\delta$ choices of $(z_i,z_j)$ with $\gcd(z_i-z_j,dt)=\delta$.

When $z_i$ and $z_j$ are fixed, the congruence $y_1+y_2\equiv y_3+y_4\pmod D$ implies that there are at most $dp^{1+o(1)}$ choices for the remaining two variables. (Recall that each $y$ determines $M_d=dp^{o(1)}$ different choices of $z$. If $z_i$ and $z_j$ are fixed, there are $p$ choices for $y_k$, and $dp^{1+o(1)}$ for $z_k$. The remaining $y_l$ is determined mod $D$ and gives $dp^{o(1)}$ choices for $z_l$.)

Putting it all together, we have

$$\begin{aligned}\sum_{\rho^d\equiv 1 \bmod p} |\mathcal{Z}_{d,\rho}|^4 &\ll \frac{p}{\phi(p-1)}p^{2/3}\left(T_d^{1/3}\sum_{\delta|dt}\left(\delta^{1/3}\frac{p^2}{\delta}dp^{1+o(1)}\right)\right)\\ &\ll p^{11/3+o(1)}dT_d^{1/3}\sum_{\delta|dt}\delta^{-2/3}\\ &\ll p^{4+o(1)}d^{\frac{2}{3}+\epsilon}t^{-\frac{1}{3}+\epsilon}.\end{aligned}$$

Therefore,

$$\begin{aligned}|\mathcal{Z}_d| &= \sum_{\rho^d\equiv 1 \pmod p} |\mathcal{Z}_{d,\rho}|\\ &\le \left(\sum_{\rho^d\equiv 1 \pmod p} 1^{4/3}\right)^{3/4}\left(\sum_{\rho^d\equiv 1 \pmod p} |\mathcal{Z}_{d,\rho}|^4\right)^{1/4}\\ &\ll p^{1+o(1)}d^{\frac{11}{12}+\epsilon}t^{-\frac{1}{12}+\epsilon}\end{aligned}$$

and

$$N_{k,1}(p;a) \le p^{o(1)}\sum_{d|T}\frac{1}{d}|\mathcal{Z}_d| \le p^{1+o(1)}t^{-\frac{1}{12}+\epsilon}\sum_{d\left|\frac{p-1}{t}\right.} d^{-\frac{1}{12}+\epsilon} \le p^{1+o(1)}t^{-\frac{1}{12}+\epsilon}$$

The proof for $N_{k,2}(p;a)$ is analogous. Thus, absorbing $t^\epsilon$ into $p^\epsilon$,

$$N_{k,1}(p;a) + N_{k,2}(p;a) \ll\le p^{1+\epsilon}t^{-\frac{1}{12}}$$

as well, and

$$N(x;a) = \sum_{k=0}^{\left\lfloor\frac{x}{p}\right\rfloor}(N_{k,1}(p;a)+N_{k,2}(p;a)) \ll \left(\frac{x}{p}+1\right)p^{1+\epsilon}t^{-\frac{1}{12}} \ll xp^\epsilon t^{-\frac{1}{12}}.$$

□

## 2.4 Number of collisions of the form $x^x \equiv y^y \pmod p$

Let $M$ be the number of solutions to the symmetric congruence

$$n^n \equiv m^m \pmod p, \quad 1 \le n, m \le x, \quad \gcd(n,p) = \gcd(m,p) = 1.$$

**Proposition 2.6.** *With notation as above, if $p \leq x \leq p(p-1)$, we have*

$$M \ll x^2 p^{-\frac{2}{27}+\epsilon}.$$

*Proof.* The proof here is similar to the proof for the weaker of the two bounds obtained in Balog et al. The bound is an immediate consequence of Proposition 2.3 and Proposition 2.5. We have that

$$M = \sum_{a=1}^{p-1} N(x;a)^2 = \sum_{t|(p-1)} \sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \operatorname{ord} a = t}} N(x;a)^2.$$

The estimates $xp^\epsilon t^{-\frac{1}{12}+\epsilon}$ and $x^{1+\epsilon}p^{-\frac{2}{3}}t^{\frac{2}{3}}$ are equal when $t = p^{\frac{8}{9}\pm\epsilon}$. (Here $\epsilon$ is loosely used to denote any small positive quantity.) Thus, we can use the common estimate $xp^{-\frac{2}{27}+\epsilon}$.

$$\begin{aligned}
\sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \operatorname{ord} a = t}} N(x;a)^2 &\ll \left(xp^{-\frac{2}{27}+\epsilon}\right) \sum_{t|(p-1)} \sum_{\substack{a \in (\mathbb{Z}/p\mathbb{Z})^\times \\ \operatorname{ord} a = t}} N(x;a) \\
&\ll xp^{-\frac{2}{27}+\epsilon}\left(\frac{\phi(p)}{p}x + O(1)\right) \\
&\ll x^2 p^{-\frac{2}{27}+\epsilon}.
\end{aligned}$$

□

# Chapter 3

# A preliminary probability model

The remainder of the thesis will focus on Question 1.12:

**Question.** *How large should $x$ be so that $n^n \equiv a \bmod p$ has a solution with $1 \leq n \leq x$, for any given residue class $a$ modulo $p$?*

The two main tools in our study are exponential sums from number theory and the coupon collector problem from probability. The first two sections of this chapter cover the background needed. A simple application results in a first estimate for $x$ as approximately $p^2 \log p/\phi(p-1)$. The more refined heuristic argument in the next chapter gives an expected $x$ of $(p-1)^2 \log \phi(p-1)/\phi(p-1)$. These expectations are essentially the same, but finer estimate allows us to compute the cumulative distribution function. The preliminary model described in this chapter is useful in illustrating the development of the final heuristic.

## 3.1 Equidistribution and exponential sums

One of the necessary criteria for randomness is uniform distribution, or equidistribution. We will use the terms uniform distribution and equidistribution interchangeably. As explained in Chapter 1, values $n^n \bmod p$ do not form an equidistributed sequence.

However, the sequence is 'scattered enough' to allow us to give a non-trivial answer of how large $x$ has to be so that $n^n \equiv a \bmod p$ has a solution $n \leq x$, for any given residue class $a$ modulo $p$.

A concise, clear introduction to equidistribution can be found in [Fri07] or [Mur08, Chapter 11]. The fundamental reference books are [KN06] and [DT97].

Consider a sequence of points

$$\{\mathbf{x}_n\}_{n=1}^N = \{(x_{1n}, x_{2n}, \ldots, x_{kn})\}_{n=1}^N$$

in the $k$-dimensional unit cube $[0,1)^k$. Let $B$ be a box

$$B = [\alpha_1, \beta_1) \times [\alpha_2, \beta_2) \times \cdots \times [\alpha_k, \beta_k) \subset [0,1)^k$$

of volume

$$|B| = \prod_{i=1}^{k} (\beta_i - \alpha_i).$$

Denote by $\mathcal{N}(B)$ the number of points $\mathbf{x}_n$, where $1 \leq n \leq N$, for which $\mathbf{x}_n \in B$.

**Definition 3.1.** *The sequence of points $\{\mathbf{x}_n\}$ that fall inside $[0,1)^k$ is said to be equidistributed if for every box $B \subseteq [0,1)^k$,*

$$\lim_{N \to \infty} \frac{\mathcal{N}(B)}{N} = |B|.$$

In other words, the ratio of the number of elements from the sequence that fall inside the box $B$ is proportional to the volume of $B$ as $N$ tends to infinity.

A key theorem in the theory of equidistribution is the Weyl criterion, which transforms the problem of determining equidistribution into the estimation of certain exponential sums. First we introduce the notations

$$\begin{aligned} e(x) &= \exp(2\pi i x) \\ e_t(x) &= \exp(2\pi i x/t) \end{aligned}$$

for the sake of brevity.

**Theorem 3.2** (Weyl's Criterion)**.** *The $k$-dimensional sequence $\{\mathbf{x}_n\}_{n=1}^N$ in $[0,1)^k$ is uniformly distributed if and only if for every nonzero vector $\mathbf{h}$ we have*

$$\sum_{n=1}^{N} e(\mathbf{h}\cdot\mathbf{x}_n) = o(N).$$

The discrepancy of a sequence gives a quantitative and more general measure of uniform distribution.

**Definition 3.3.** *With notation as above, the discrepancy of the sequence $\{\mathbf{x}_n\}_{n=1}^N$ in $[0,1)^k$ is defined as*

$$\Delta = \sup_{B\subseteq[0,1)^k} \left|\frac{\mathcal{N}(B)}{N} - |B|\right|$$

*where the supremum runs over all boxes $B$ inside the $k$-dimensional unit cube.*

Thus, the discrepancy measures the largest deviation of $\mathcal{N}(B)$ from its expected value. The trivial bound for discrepancy is 1. We may rescale a sequence so that its terms fall in the unit cube, and a uniformly distributed sequence will have discrepancy tending to zero as the number of terms $N$ tends to infinity. However, the bound of discrepancy for finite sequences is also a useful, quantitative indicator of how scattered the sequence is within a region.

Again exponential sums are key, since a bound on $\sum_{n=1}^N e(\mathbf{h}\cdot\mathbf{x}_n)$ gives a bound for the discrepancy of a sequence, from the following important theorem.

**Theorem 3.4** (Erdős-Turán Inequality)**.** *Let $\{\mathbf{x}_n\}_{n=1}^N$ be points in the $k$-dimensional unit cube and $M$ an arbitrary positive integer. Then*

$$\Delta \le \left(\frac{3}{2}\right)^k \left(\frac{2}{M+1} + \sum_{0<\|\mathbf{h}\|\le M} \frac{1}{r(\mathbf{h})}\left|\frac{1}{N}\sum_{n=1}^{N} e(\mathbf{h}\cdot\mathbf{x}_n)\right|\right)$$

*where $\|\mathbf{h}\| = \max_{1\le j\le k}|a_j|$ and $r(\mathbf{h}) = \prod_{j=1}^k \max(1,|a_j|)$ for $\mathbf{h} = (a_1,\ldots,a_k) \in \mathbb{Z}^k$.* [DT97].

In the next section, we move to probability theory and the coupon collector problem.

## 3.2 The classical coupon collector problem

The coupon collector problem asks the following question: if $m$ coupons are collected with replacement, how many trials are needed in order to collect all $m$ coupons? For example, if cereal boxes randomly contain one of $m$ coupons, how many boxes must be bought in order to collect at least one of every coupon?

The motivation for considering the coupon collector problem is simply the ideal scenario. If elements were randomly distributed in Table 1.3, then the expected $x$ in Question 1.12 would be the same as the expected number of random draws required to obtain all residue classes. In our case the cereal boxes correspond to the $n$'s (or a subsequence thereof) and the coupons to the residue classes $a \bmod p$.

In Table 1.3 the residue classes occur with different frequencies, depending on their order. However, we begin by describing the classical coupon collector model which assumes that every coupon occurs with equal probability. The following calculation gives the expected time, or number of draws to obtain a full collection. [Isa95, p. 80-82].

**Proposition 3.5.** *Consider $m$ different objects that are drawn with replacement. Suppose each object occurs with equal probability $1/m$. The expected number of draws required to collect all $m$ objects is*

$$E(T) = m \log m + \gamma m + \frac{1}{2} + o(1).$$

*Proof.* Let $T$ be the time (or number of trials) required to collect all $m$ coupons, and let $t_i$ be the time to collect the $i$-th new coupon given that $i-1$ coupons have been collected. The $T$ and $t_i$ are random variables. The probability of collecting a new coupon given $i-1$ collected coupons is

$$p_i = \frac{m-i+1}{m}.$$

The $t_i$ has geometric distribution with expectation

$$E(t_i) = \frac{1}{p_i}.$$

(For instance if the probability of an event is $\frac{1}{3}$, then the expected number of trials to obtain a success is 3.) We have

$$\begin{aligned} E(T) &= E(t_1) + E(t_2) + \ldots + E(t_m) \\ &= \frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_m} \\ &= \frac{m}{m} + \frac{m}{m-1} + \ldots + \frac{1}{m} \\ &= m\left(1 + \frac{1}{2} + \ldots + \frac{1}{m}\right) \\ &= mH_m \\ &= m\log m + \gamma m + \frac{1}{2} + o(1) \end{aligned}$$

In the last two lines we used the notation $H_m$ for the $m$-th Harmonic number, the sum of the reciprocals of the first $m$ natural numbers, and the bound

$$\frac{1}{2m} - \frac{1}{8m^2} < H_m - \log m - \gamma < \frac{1}{2m} \tag{3.1}$$

where $\gamma$ is the Euler-Mascheroni constant [PS72, Ex. 18]. □

The following limit theorem for the probability distribution of time $T$ until a complete collection is due to Erdős and Rényi. [ER61]

**Theorem 3.6.** *For any $t \in \mathbb{R}$ , we have that:*

$$P(T \leq m\log m + tm) \to e^{-e^{-t}} \quad \text{as} \quad m \to \infty.$$

## 3.3 Powers of primitive roots and a first estimate of $x$

The first, simple model considers a subsequence of $\{n^n \pmod p\}_n$ that is equidistributed as $p$ tends to infinity. [1] The congruence $n^n \equiv a \pmod p$ seems most difficult to solve if

[1] We view the terms of the sequence as numbers from 1 to $p-1$. Consider the fractional parts after division by $p$, so that the terms fall in the unit interval. We say that the sequence is equidistributed as $p$ tends to infinity if Definition 3.1 and the Weyl Criterion 3.2 are satisfied when we replace $N$ by $p$.

$a$ is a primitive root, as $n$ must be primitive as well. Thus, starting from Table 1.3, we consider only the columns which correspond to primitive elements, and only the first $R$ rows corresponding to $k = 0, \ldots, R-1$.

Let $g_1, g_2, \ldots, g_{\phi(p-1)}$ be all the primitive roots modulo $p$. We will show that the elements $\left\{g_i^{g_i+k}\right\}_{k,i}$, listed in Table 3.1 are equidistributed modulo $p$ as $p$ tends to infinity, when $R$ is greater than $p^\delta$.

| | Columns corresponding to primitive roots | | | | |
|---|---|---|---|---|---|
| Primitive roots | $g_1$ | $g_2$ | $g_3$ | $\cdots$ | $g_{\phi(p-1)}$ |
| $k=0$ | $g_1^{g_1}$ | $g_2^{g_2}$ | $g_3^{g_3}$ | $\cdots$ | $g_{\phi(p-1)}^{g_{\phi(p-1)}}$ |
| $k=1$ | $g_1^{g_1+1}$ | $g_2^{g_2+1}$ | $g_3^{g_3+1}$ | $\cdots$ | $g_{\phi(p-1)}^{g_{\phi(p-1)}+1}$ |
| $k=2$ | $g_1^{g_1+2}$ | $g_2^{g_2+2}$ | $g_3^{g_3+2}$ | $\cdots$ | $g_{\phi(p-1)}^{g_{\phi(p-1)}+2}$ |
| $k=3$ | $g_1^{g_1+3}$ | $g_2^{g_2+3}$ | $g_3^{g_3+3}$ | $\cdots$ | $g_{\phi(p-1)}^{g_{\phi(p-1)}+3}$ |
| $\vdots$ | | | | | |
| $k=R-1$ | $g_1^{g_1+R-1}$ | $g_2^{g_2+R-1}$ | $g_3^{g_3+R-1}$ | $\cdots$ | $g_{\phi(p-1)}^{g_{\phi(p-1)}+R-1}$ |

Table 3.1: The residues modulo $p$ of the self-power map $n^n$ from Table 1.3, where we consider only the columns corresponding to primitive roots, and only the first $R$ rows.

The following is Corollary 1 in [BGK06].

**Theorem 3.7.** *There exist positive constants $C_1$ and $C_2$ such that for any $\delta > 0$, and positive integer $t \geq p^\delta$, and any element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ such that the multiplicative order of $g$ is greater than $t$, we have*

$$\max_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} \left| \sum_{k=0}^{t-1} \exp\left(\frac{2\pi i a g^k}{p}\right) \right| \leq t p^{-\gamma}, \qquad \gamma = \exp\left(-C_1/\delta^{C_2}\right).$$

**Proposition 3.8.** *Given $\delta > 0$ and $R = p^\delta$, then elements $\Gamma = \left\{g_i^{g_i+k}\right\}_{k,i}$ in Table 3.1, form an equidistributed sequence as $p$ tends to infinity and the discrepancy of the sequence*

*is bounded by*

$$\Delta \leq Cp^{-\gamma} \log p$$

*Proof.* According to Weyl's criterion 3.2, we bound the following exponential sum where $h$ is nonzero modulo $p$.

$$\begin{aligned} & \sum_{i=1}^{\phi(p-1)} \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h g_i^{g_i+k}}{p}\right) \\ = & \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h g_1^{g_1} g_1^k}{p}\right) + \ldots + \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h g_{\phi(p-1)}^{g_{\phi}(p-1)} g_{\phi(p-1)}^k}{p}\right) \\ = & \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h_1 g_1^k}{p}\right) + \ldots + \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h_{\phi(p-1)} g_{\phi(p-1)}^k}{p}\right) \end{aligned}$$

In the third line, we have set $hg_i^{g_i} = h_i$, as they are independent of $k$. Each $g_i$ has order $\phi(p-1) \gg p^{1-\epsilon}$, thus the order of $g_i$ is clearly greater than $R$. The conditions of Theorem 3.7 are satisfied and we have

$$\sum_{i=1}^{\phi(p-1)} \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h g_i^{g_i+k}}{p}\right) \leq Rp^{-\gamma} + \ldots + Rp^{-\gamma} = \phi(p-1)Rp^{-\gamma}$$

This sum is of the order $o(\phi(p-1)R)$, where $\phi(p-1)R$ is the total number of terms, thus the sequence $\left\{g_i^{g_i+k}\right\}_{k,i}$ is equidistributed by Weyl's criterion, Theorem 3.2.

We may use the Erdős Turàn Inequality, Theorem 3.4, with $M = p-1$ to estimate the discrepancy. Since we have taken $h$ positive, the constant factor from the Erdős Turàn inequality is multiplied by two: $C = 2(3/2)$. The constant $\gamma > 0$ comes from Theorem 3.7 (note that it is not related to the Euler-Mascheroni constant).

$$\begin{aligned} \Delta & \leq C\left(\frac{2}{p} + \sum_{0<h\leq p-1} \frac{1}{h}\left|\frac{1}{\phi(p-1)R} \sum_{i=1}^{\phi(p-1)} \sum_{k=0}^{R-1} \exp\left(\frac{2\pi i h g_i^{g_i+k}}{p}\right)\right|\right) \\ & \leq \frac{2C}{p} + C \sum_{0<h\leq p-1} \frac{1}{h}\left|\frac{1}{\phi(p-1)R}\phi(p-1)Rp^{-\gamma}\right| \\ & \leq Cp^{-\gamma}\log p + O\left(p^{-\gamma}\right). \end{aligned}$$

□

If we could assume that the sequence $\Gamma = \left\{g_i^{g_i+k}\right\}_{k,i}$ were random, then we would like to find the number of rows $R$ required so that every residue class $a \bmod p$ would appear as some element of the sequence. We are taking $\phi(p-1)R$ terms of the sequence, and using Theorem 3.6, we obtain

$$\begin{aligned} P\left(\phi(p-1)R < (p-1)\log(p-1) + t(p-1)\right) &\to e^{-e^{-t}} \\ P\left(R < \frac{(p-1)}{\phi(p-1)}\log(p-1) + t\frac{(p-1)}{\phi(p-1)}\right) &\to e^{-e^{-t}}. \end{aligned}$$

Again consider Table 1.3 with all $p-1$ columns, but assume that columns of non-primitive elements do not contribute to obtaining new residue classes. Since we are taking $R$ rows of the table, we need to take $x = pR$:

$$P\left(x < \frac{p(p-1)\log(p-1)}{\phi(p-1)} + t\frac{p(p-1)}{\phi(p-1)}\right) \to e^{-e^{-t}}. \tag{3.2}$$

Figure 3.1 shows the graph of the actual value of $x$ such that all the residues $a \pmod p$ appear as $n^n \pmod p$ for some $1 \le n \le x$, versus the estimated value of $x$ found using the classical coupon collector model. We consider all odd primes less than 72500. The ratio is close to, but less than 1.

We may rewrite equation (3.2) as

$$P\left(\left(x - \frac{p(p-1)\log(p-1)}{\phi(p-1)}\right)\left(\frac{\phi(p-1)}{p(p-1)}\right) < t\right) \to e^{-e^{-t}}.$$

Let

$$X_p = \left(x - \frac{p(p-1)\log(p-1)}{\phi(p-1)}\right)\left(\frac{\phi(p-1)}{p(p-1)}\right),$$

where $x$ depends on $p$ in each case, and is the smallest natural number so that $n^n \equiv a \pmod p$ and $n \le x$ has a solution for every residue class $a$ modulo $p$. Assume that the $X_p$'s are independent variables.

Given the simple coupon collector model, the cumulative distribution function from which the $X_p$'s are sampled should approach

$$F(t) = e^{-e^{-t}}.$$

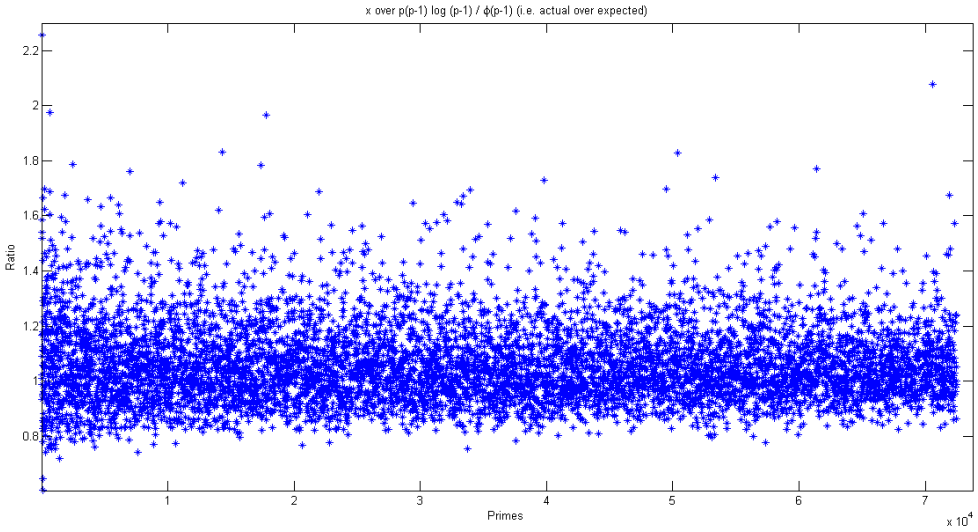


Figure 3.1: The ratio of the smallest $x$ so that all residues $a$ can be expressed as $n^n \pmod p$ for some $n \leq x$, versus the expected value of $x$ calculated using the coupon-collector model.

The empirical distribution function is defined as follows [Pre98, p. 257-259]

$$\hat{F}(t) := \frac{|p : X_p \leq t|}{N}$$

where $N$ is the number of primes considered.

Figure 3.2 illustrates the comparison between the empirical and the theoretical distribution function and shows more clearly that the simple coupon collector model overestimates $x$, since there is a left shift for the empirical data. The closeness of the fit seems to depend on $\phi(p-1)$, since the best fit occurs when considering only primes of the form $p = 2q + 1$, where $q$ is also prime, and the worst when $\phi(p-1)$ is small.

To correct the overestimation, one possibility would have been to consider sampling without replacement. The classical coupon collector is a model of sampling with replacement (darts thrown at random at the $n^n$ table) whereas taking the first $x$ terms of the sequence $n^n \pmod p$ is a sampling without replacement (where two darts cannot hit the same spot on the $n^n$ table). However, this difference is negligible when $p$ is large. More

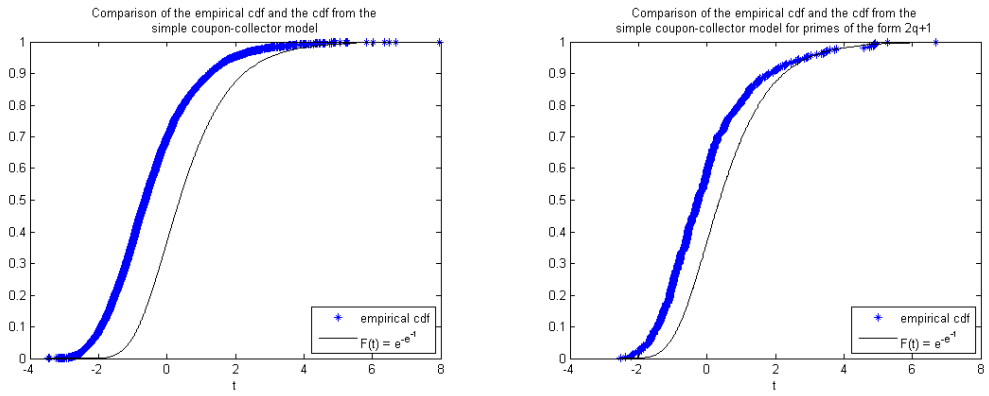


Figure 3.2: Comparison between the cumulative distribution function derived from the coupon collector problem and the empirical distribution function for the variables $X_p$ from equation (3.3). On the right is the graph considering only primes of the from $p = 2q + 1$, for some prime $q$; in this case, there is a translation of approximately 0.6 units between the curves.

importantly, each column corresponding to a primitive root contains distinct elements. This case is more difficult to model probabilistically.

In Chapter 4, we will instead refine the model to incorporate the non-uniform distribution of elements in the entire Table 1.3. The new model will correct the left-shift in the cumulative distribution function.

Before continuing, it is worthwhile to give a final motivation for the preliminary model. The elements in columns corresponding to primitive roots follow a simple pattern. If $g$ is a primitive root, the elements in the column corresponding to $g$ are

$$\left\{g^g, g^{g+1}, g^{g+2}, \ldots g^{g-1}\right\}.$$

Given another primitive root, $g_1 = g^r$, the elements in the column corresponding to $g^r$ are

$$\begin{aligned} & \left\{g^{rg^r}, g^{r(g^r+1)}, g^{r(g^r+2)}, \ldots, g^{r(g^r-1)}\right\} \\ = & \left\{g^{rg^r}, g^{rg^r+r}, g^{rg^r+2r}, \ldots, g^{r(g^r-1)}\right\} \\ = & \left\{g^s, g^{s+r}, g^{s+2r}, \ldots, g^{s+(p-1)r}\right\}, \end{aligned}$$

where in the last line we let $s \equiv rg^r \pmod{p-1}$. Thus, the elements in the column corresponding to $g^r$ are every $r$th element from the column for $g$, starting from $g^s$.

We have an isomorphism between $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\mu_{p-1}$, the group of $(p-1)$st roots of unity, where we map generator $g$ to $e^{\frac{2\pi i}{p-1}}$. The problem of obtaining all the residue classes transforms into one of covering all the elements of $\mu_{p-1}$ on the unit circle. The numbers in each column corresponding a primitive root $g^r$ where $\gcd(r, p-1) = 1$ are mapped to roots of unity in 'hops' of length $r$ about the unit circle $\mu_{p-1}$.

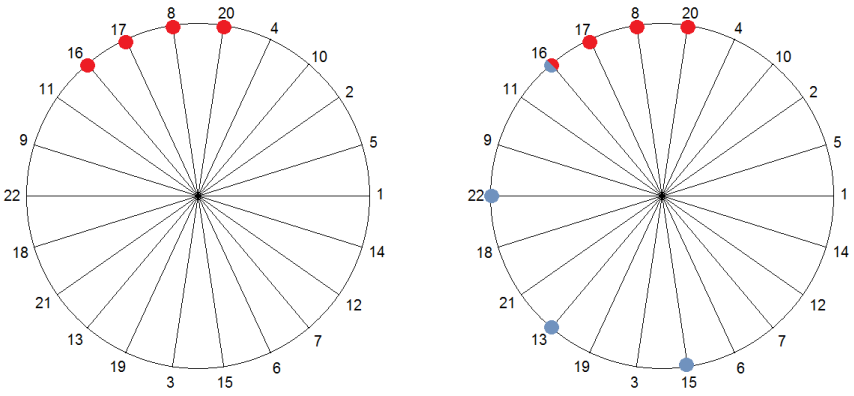


Figure 3.3: An illustration of the isomorphism between $(\mathbb{Z}/23\mathbb{Z})^\times$ and $\mu_{22}$ where 5 (mod 23) is mapped to $e^{\frac{2\pi i}{22}}$. The first elements $5^5, 5^6, 5^7$, and $5^8 \pmod{23}$ of the column corresponding to 5 are indicated. The diagram on the left also includes the first elements $10^{10}, 10^{11}, 10^{12}, 10^{13} \pmod{23}$, of the column corresponding to $10 \equiv 5^3 \pmod{23}$ and which appear in 'hops' of length 3 on the circle.

This is reminiscent of the equidistribution of the fractional part of $n\theta$ in the unit interval when $\theta$ is an irrational number. While the sequence $\Gamma = \left\{g_i^{g_i+k}\right\}_{k,i}$ is equidistributed only as $p$ tends to infinity, in both cases the initial elements of the sequence follow a pattern, yet the sequence fills or appears to fill the interval of interest.

# Chapter 4

# Expectation of $x$ and its cumulative distribution

In this chapter we give a detailed heuristic argument to find the expected $x$ such that $n^n \equiv a \mod p$ has a solution $1 \leq n \leq x$ for any given residue class $a \bmod p$. This expected value of $x$ has main term $(p-1)^2 \log \phi(p-1)/\phi(p-1)$. The expression is in terms of $(p-1)$ because it is derived from a probabilistic argument involving the frequencies of the $(p-1)$ residue classes in a period of the self power map. The order of the expectation is the same as obtained in the previous chapter, but the $\log \phi(p-1)$ factor is important in the calculation of the cumulative distribution function.

The argument consists of two parts. First, we give a variation of the coupon collector problem, including blank coupons which need not be collected. This model provides a better estimate for the expected $x$. Secondly, using this value for the expectation, we calculate the probability distribution for the number of draws until a complete collection. After a suitable normalization, we obtain the double exponential distribution $e^{-e^{-t}}$, as in the classical coupon collector case. The saddle point method is used in the calculation of the probability distribution.

These heuristics are well-supported by the computational results.

## 4.1 Coupon collector problem with blank coupons

In order to calculate the expected $x$ in Question 1.12, we will use a variant of the coupon collector problem. As before, we assume that the elements of Table 1.3 are randomly distributed. Thus, our expected $x$ should be equal to the number of draws required to obtain a full collection of residue classes from a random sampling of entries in Table 1.3. The different residue classes $a$ congruent to $1, 2, \ldots, (p-1) \bmod p$ correspond to the 'coupons' to be collected.

A part of Theorem 4.1 of [FGT92] gives the expectation of the time necessary to obtain a full collection from a random, but non-uniform probability distribution.

**Proposition 4.1.** *The expectation $E(T)$ of the time necessary to gather a complete collection of $m$ objects from a general probability distribution $\{p_i\}_{i=1}^m$, sampling with replacement, is given by*

$$E(T) = \int_0^\infty \left(1 - \prod_{i=1}^{m} \left(1 - e^{-p_i t}\right)\right) dt.$$

Since higher order elements occur least often in Table 1.3, we set the residue classes $a \bmod p$ which are primitive roots modulo $p$ to be the coupons of value. All other coupons will be blank coupons.

In this section, we will calculate the expected number of trials to obtain a full collection of useful coupons. We will use the terms *useful* and *non-blank* interchangeably. This problem is a variation on the coupon collector problem under non-uniform distribution.

Consider a collection of $m$ coupons and let $m_B$ coupons, which appear with probabilities $p_1, p_2, \ldots, p_{m_B}$, be blank. We do not keep track of how many of these coupons are collected, if any. They are omitted from the coupon collector problem in the sense that we want to collect the $m - m_B$ useful coupons, not all $m$ coupons. Let

$$p_1 + p_2 + \ldots + p_{m_B} = \beta.$$

Our goal in this section is to prove the following proposition.

**Proposition 4.2.** *With notation as above, the expectation $E(T_j)$ of the time necessary to gather a collection of $j$ useful (non-blank) coupons under a general probability distribution with $m_B$ blank coupons is*

$$E(T_j) = \sum_{q=0}^{j-1} \int_0^\infty [u^q] \left( \prod_{i=m_B+1}^{m} \left(1 + u\left(e^{p_i t} - 1\right)\right) \right) e^{(\beta-1)t} dt, \tag{4.1}$$

*where $[u^q]f(u)$ denotes the $q$-th coefficient in the Taylor expansion of $f(u)$. For the full collection of the $m - m_B$ useful coupons the expectation is*

$$E(T) = \int_0^\infty \left( 1 - \prod_{i=m_B+1}^{m} (1 - e^{-p_i t}) \right) dt. \tag{4.2}$$

The proof of Proposition 4.2 follows the proofs of Theorems 3.1 and 4.1 in [FGT92] very closely. Using regular languages extended by the 'shuffle product', Flajolet et al. produce generating functions to derive integral representations for expectations and probability distributions. Appendix A gives a summary of the background required. We begin by rewriting Theorem 3.1 of [FGT92] to obtain Proposition 4.4 below, of which Proposition 4.2 is a corollary.

The alphabet $\mathcal{A}$ consists of $m$ different coupons, and $p_i$ is the probability of choosing coupon $\alpha_i$ from $\mathcal{A}$. Consider the following generalization of the coupon-collector problem:

**Question 4.3.** *Determine the expectation of the number $B_j$ of elements that need to be drawn from $\mathcal{A}$ (with replacement) until we first obtain $j$ distinct coupons that are each repeated at least $k$ times.*

The case $k = 2$ and $j = 1$ is the classical birthday problem of determining the expected number of random people needed such that two will share a birthday. The case $k = 1$ and $j = m$ is the coupon collector problem where a full collection is desired. Below we determine $E(B_j)$ for the case when the alphabet $\mathcal{A}$ contains blank coupons.

**Proposition 4.4.** *Consider a set of $m$ coupons under a general probability distribution $\{p_i\}_{i=1}^m$, which are drawn with replacement. Let $m_B$ coupons, which appear with probabilities $p_1, p_2, \ldots, p_{m_B}$, be blanks. The expectation $E(B_j)$ of the time for obtaining $j \leq m - m_B$ distinct useful coupons, each appearing $k$ times, is given by*

$$E(B_j) = \sum_{q=0}^{j-1} \int_0^\infty [u^q] \left( \prod_{i=m_B+1}^{m} \left( \tilde{e}_{k-1}(p_i t) + u \left( e^{p_i t} - \tilde{e}_{k-1}(p_i t) \right) \right) \right) e^{(\beta-1)t} dt \tag{4.3}$$

*where $\tilde{e}_{k-1}(t)$ represents the truncated exponential*

$$\tilde{e}_{k-1}(t) = 1 + \frac{t}{1!} + \frac{t^2}{2!} + \ldots + \frac{t^k}{k!}.$$

*Proof.* Let the random variable $B_j$ be the number of draws for first obtaining at least $k$ copies of $j$ useful coupons in an infinite sequence of trials.

Let $Y_n$ be the random variable defined on $\mathcal{A}^n$ representing the number of $k$-occurrences of different useful coupons in a sequence of $n$ trials. The two probability distributions are related by

$$\Pr\{Y_n \geq j\} = \Pr\{B_j \leq n\}.$$

From this, the expectation of $B_j$ is found as follows:

$$\begin{aligned} E(B_j) &= \sum_{n \geq 1} n \Pr\{B_j = n\} \\ &= \sum_{n \geq 0} \Pr\{B_j > n\} \\ &= \sum_{n \geq 0} \Pr\{Y_n < j\} \\ &= \sum_{q=0}^{j-1} \left( \sum_{n \geq 0} \Pr\{Y_n = q\} \right). \end{aligned}$$

It remains to estimate the sum $\sum_{n \geq 0} \Pr\{Y_n = q\}$.

Let $H_q$ be the language consisting of words with exactly $q$ useful letters that occur at least $k$ times. Label the letters corresponding to the blank coupons as $\alpha_1, \alpha_2, \ldots, \alpha_{m_B}$,

and these may occur any number of times. All other letters occur at most $k-1$ times. Let us set

$$\alpha^{<k} = \varepsilon + \alpha + \alpha^2 + \ldots + \alpha^{k-1}$$

and

$$\alpha^{\geq k} = \alpha^k \cdot \alpha^*.$$

The language $H_q$ can be expressed as

$$H_q = \left(\alpha_1^* \sqcup\!\sqcup \alpha_2^* \sqcup\!\sqcup \ldots \sqcup\!\sqcup \alpha_{m_B}^*\right) \sqcup\!\sqcup \bigcup_{I,J} \left(\alpha_{i_1}^{\geq k} \sqcup\!\sqcup \alpha_{i_2}^{\geq k} \sqcup\!\sqcup \ldots \sqcup\!\sqcup \alpha_{i_q}^{\geq k}\right) \sqcup\!\sqcup \left(\alpha_{j_1}^{<k} \sqcup\!\sqcup \alpha_{j_2}^{<k} \sqcup\!\sqcup \ldots \sqcup\!\sqcup \alpha_{j_r}^{<k}\right)$$

where the union is over all sets $I$ and $J$ of cardinality $q$ and $r = m - m_B - q$ such that

$$\begin{aligned} I &= \{i_1, i_2, \ldots, i_q\} \\ J &= \{j_1, j_2, \ldots, j_r\} \\ I \cap J &= \emptyset \\ I \cup J &= \{m_B + 1, m_B + 2, \ldots, m\}. \end{aligned}$$

If $\alpha$ is a letter with probability $\sigma$, the exponential generating functions of $\alpha^*$, $\alpha^{<k}$ and $\alpha^{\geq k}$ are $e^{\sigma z}$, $\tilde{e}_{k-1}(\sigma z)$ and $e^{\sigma z} - \tilde{e}_{k-1}(\sigma z)$, respectively. Thus, the exponential generating function of $H_q$ is

$$\begin{aligned} \hat{h}(z) &= e^{p_1 z} \cdots e^{p_{m_B} z} \sum_{I,J} \left( (e^{p_{i_1} z} - \tilde{e}_{k-1}(p_{i_1} z)) \cdots \left(e^{p_{i_q} z} - \tilde{e}_{k-1}(p_{i_q} z)\right)\right) \cdot (\tilde{e}_{k-1}(p_{j_1} z) \cdots \tilde{e}_{k-1}(p_{j_r} z)) \\ \hat{h}(z) &= e^{\beta z} \sum_{I,J} \left( (e^{p_{i_1} z} - \tilde{e}_{k-1}(p_{i_1} z)) \cdots \left(e^{p_{i_q} z} - \tilde{e}_{k-1}(p_{i_q} z)\right)\right) \cdot (\tilde{e}_{k-1}(p_{j_1} z) \cdots \tilde{e}_{k-1}(p_{j_r} z)) \end{aligned}$$

Therefore,

$$\hat{h}(z) = e^{\beta z} [u^q] \Phi(z, u)$$

where $[u^q]$ denotes the coefficient of the $q$th power of $u$ of

$$\Phi(z, u) = \prod_{i=m_B+1}^{m} \left( \tilde{e}_{k-1}(p_i t) + u \left(e^{p_i t} - \tilde{e}_{k-1}(p_i t)\right)\right). \tag{4.4}$$

The ordinary generating function of $H_q$ is given by the Laplace-Borel transform,

$$h_q(z) = \int_0^\infty e^{\beta z t}[u^q]\Phi(zt, u)e^{-t}dt.$$

Therefore,

$$\sum_{n\geq 0} \Pr\{Y_n = q\} = h_q(1) = \int_0^\infty [u^q]\Phi(t, u)e^{(\beta-1)t}dt,$$

and summing over $q$ ranging from 0 to $j-1$, we have the statement of the theorem. □

We can now prove Proposition 4.2.

*Proof.* The equation (4.1) is a specialization of equation (4.3) of Proposition 4.4 to the case $k = 1$.

To obtain equation (4.2) from (4.1), we introduce the function

$$\Phi(t, u) = \prod_{i=m_B+1}^{m} \left(1 + u\left(e^{p_i t} - 1\right)\right) \tag{4.5}$$

which is the function $\Phi$ in equation (4.4) in the case $k = 1$. Expand $\Phi(t, u)$ as follows:

$$\Phi(t, u) = \sum_{q=0}^{m-m_B} \phi_q(t)u^q.$$

We have:

$$\begin{aligned}
E(T) = E(T_{m-m_B}) &= \sum_{q=0}^{m-m_B-1} \int_0^\infty [u^q]\Phi(t, u)|_{u=1}\, e^{(\beta-1)t}dt \\
&= \int_0^\infty \sum_{q=0}^{m-m_B-1} [u^q]\Phi(t, u)|_{u=1}\, e^{(\beta-1)t}dt \\
&= \int_0^\infty (\phi_0(t) + \phi_1(t) + \ldots + \phi_{m-m_B-1}(t))\, e^{(\beta-1)t}dt \\
&= \int_0^\infty (\Phi(t, 1) - \phi_{m-m_B}(t))\, e^{(\beta-1)t}dt.
\end{aligned}$$

We have that $\phi_{m-m_B}(t) = \prod_{i=m_B+1}^{m} (e^{p_i t} - 1)$ and, using (4.5),

$$\begin{aligned}
\Phi(t, 1) &= \prod_{i=m_B+1}^{m} e^{p_i t} = \prod_{i=1}^{m} e^{p_i t} \prod_{i=1}^{m_B} e^{-p_i t} \\
&= e^{(p_1+p_2+\ldots+p_m)t} e^{-(p_1+p_2+\ldots+p_{m_B})t} = e^{(1-\beta)t}.
\end{aligned}$$

Therefore, we obtain:

$$\begin{aligned} E(T) &= \int_0^\infty \left(\Phi(t,1) - \phi_{m-m_B}(t)\right) e^{(\beta-1)t} dt \\ &= \int_0^\infty \left( e^{(1-\beta)t} - \prod_{i=m_B+1}^{m} \left(e^{p_i t} - 1\right) \right) e^{(\beta-1)t} dt \\ &= \int_0^\infty \left( 1 - e^{(\beta-1)t} \prod_{i=m_B+1}^{m} e^{p_i t} \prod_{i=m_B+1}^{m} \left(1 - e^{-p_i t}\right) \right) dt \\ &= \int_0^\infty \left( 1 - \prod_{i=m_B+1}^{m} \left(1 - e^{-p_i t}\right) \right) dt \end{aligned}$$

□

## 4.2 Upper and lower bounds for expectation

Assume that the elements in Table 1.3 are randomly selected with replacement. In this section we give upper and lower bounds for the expectation of the number of draws required to obtain a full collection of all residue classes $1, 2, \ldots, (p-1) \bmod p$. The lower bound of the expectation is the same as the expectation for the coupon collector with blank coupons, where all coupons except those corresponding to primitive roots are blank.

This lower bound is the one we will use in the calculation of the cumulative distribution in the following section. It is more accurate in the case of primes of the form $p = 2q + 1$ where $q$ is also prime.

**Proposition 4.5.** *Assume that the elements in Table 1.3 are randomly selected with replacement. Then the expected time required to obtain a full collection is bounded as follows:*

$$\frac{(p-1)^2}{\phi(p-1)} \left(\log \phi(p-1) + \gamma + o(1)\right) < E(T) < \frac{(p-1)^2}{\phi(p-1)} \left(\log(p-1) + \gamma + o(1)\right).$$

*The lower bound for $E(T)$ is the expectation for the coupon collector problem with blank coupons, where all elements other than the primitive roots are blank.*

*Proof.* In Table 1.3, the elements that occur least frequently are the $\phi(p-1)$ primitive roots modulo $p$. Each one will occur exactly $\phi(p-1)$ times, once in each column corresponding to a primitive root. If the elements in Table 1.3 are randomly selected with replacement, using Proposition 4.1 the expected time required to collect elements from all $p-1$ nonzero residue classes is:

$$\begin{aligned} E(T) &= \int_0^\infty \left(1 - \prod_{\substack{\text{primitive}\\ \text{roots}}} \left(1-e^{-p_i t}\right) \prod_{\substack{\text{non-primitive}\\ \text{roots}}} \left(1-e^{-p_i t}\right)\right) dt \\ &= \int_0^\infty \left(1 - \left(1-e^{-\frac{\phi(p-1)}{(p-1)^2}t}\right)^{\phi(p-1)} \prod_{\substack{\text{non-primitive}\\ \text{roots}}} \left(1-e^{-p_i t}\right)\right) dt. \end{aligned}$$

We have used that $\frac{\phi(p-1)}{(p-1)^2}$ is the probability of choosing a primitive root. Replacing all the $(1-e^{-p_i t})$ terms corresponding to non-primitive residue classes by $\left(1-e^{-\frac{\phi(p-1)}{(p-1)^2}t}\right)$ in the product makes the integral larger. Thus:

$$\begin{aligned} E(T) &< \int_0^\infty \left(1 - \left(1-e^{-\frac{\phi(p-1)}{(p-1)^2}t}\right)^{p-1}\right) dt \\ &= -\frac{(p-1)^2}{\phi(p-1)} \int_1^0 \frac{\left(1-(1-u)^{p-1}\right)}{u} du, \qquad \text{where } u = e^{-\frac{\phi(p-1)}{(p-1)^2}t} \\ &= \frac{(p-1)^2}{\phi(p-1)} \int_0^1 \frac{(1-x^{p-1})}{1-x} dx, \qquad \text{where } x = 1-u \\ &= \frac{(p-1)^2}{\phi(p-1)} \int_0^1 \left(1+x+x^2+\cdots+x^{p-2}\right) dx \\ &= \frac{(p-1)^2}{\phi(p-1)} \left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}\right) \\ &= \frac{(p-1)^2}{\phi(p-1)} H_{p-1} \\ &< \frac{(p-1)^2}{\phi(p-1)} \left(\log(p-1)+\gamma+\frac{1}{2(p-1)}\right). \end{aligned}$$

In the last step we used inequality (3.1) for estimating $H_{p-1}$.

Similarly, dropping all the $(1-e^{-p_i t})$ terms gives us a lower bound:

$$E(T) > \int_0^\infty \left(1 - \left(1-e^{-\frac{\phi(p-1)}{(p-1)^2}t}\right)^{\phi(p-1)}\right) dt$$

$$\begin{aligned} &= \frac{(p-1)^2}{\phi(p-1)} H_{\phi(p-1)} \\ &> \frac{(p-1)^2}{\phi(p-1)} \left( \log \phi(p-1) + \gamma + \frac{1}{2\phi(p-1)} - \frac{1}{8\phi(p-1)^2} \right), \end{aligned}$$

again using inequality (3.1). Note that by Proposition 4.2,

$$\int_0^\infty \left( 1 - \left( 1 - e^{-\frac{\phi(p-1)}{(p-1)^2} t} \right)^{\phi(p-1)} \right) dt$$

is equal to the expected time if we assume the elements in Table 1.3 are randomly distributed but all elements other than the primitive roots are blank. □

### 4.2.1 Expectation estimate for the case $p = 2q + 1$

Let $p = 2q+1$, where $q$ is also a prime. We let the residue classes 1 and $p-1 \equiv -1 \bmod p$ correspond to the blank coupons since they are easy to collect; they will appear in the first two rows of Table 1.3. We need only consider the number of draws required to collect all other residue classes, which have large order. There are $q-1$ elements of order $q$ in $(\mathbb{Z}/p\mathbb{Z})^\times$, each of which appear $3(q-1)$ times in Table 1.3, and $q-1$ elements of order $2q$, each of which appear $(q-1)$ times in Table 1.3.

**Proposition 4.6.** *Given $2q$ different coupons of which two are blank, $q-1$ each appear with probability $\frac{(q-1)}{4q^2}$, and $q-1$ each appear with probability $\frac{3(q-1)}{4q^2}$, then the expected number of draws to obtain all $2q-2$ useful coupons is bounded by*

$$\begin{aligned} E(T) &= \int_0^\infty \left( 1 - \left( 1 - e^{-\frac{(q-1)t}{4q^2}} \right)^{(q-1)} \left( 1 - e^{-\frac{3(q-1)t}{4q^2}} \right)^{(q-1)} \right) dt \\ &\leq \frac{(p-1)^2}{\phi(p-1)} \left( \log(p-1) + \log\frac{1}{2} + \gamma + O\left( \frac{1}{q^{1/4}} \right) + \frac{1}{4(p-1)} \right). \end{aligned}$$

*Proof.* By Proposition 4.2, the expected time to collect the $2q-2$ useful coupons is given by

$$E(T) = \int_0^\infty \left( 1 - \left( 1 - e^{-\frac{(q-1)t}{4q^2}} \right)^{(q-1)} \left( 1 - e^{-\frac{3(q-1)t}{4q^2}} \right)^{(q-1)} \right) dt.$$

Let $u = e^{-\frac{(q-1)t}{4q^2}}$. Then $dt = -\frac{4q^2}{(q-1)}\frac{du}{u}$ and

$$\begin{aligned}
E(T) &= -\frac{4q^2}{(q-1)}\int_1^0 \frac{1}{u}\left(1-(1-u)^{(q-1)}(1-u^3)^{(q-1)}\right)du \\
&= \frac{4q^2}{(q-1)}\int_0^1 \frac{1}{u}\left(1-(1-u)^{(q-1)}(1-u)^{(q-1)}(1+u+u^2)^{(q-1)}\right)du \\
&= \frac{4q^2}{(q-1)}\int_0^1 \frac{1}{u}\left(1-(1-u)^{2(q-1)}\left((1-u)^2+3u\right)^{(q-1)}\right)du \\
&= \frac{4q^2}{(q-1)}\int_0^1 \frac{1}{u}\left(1-(1-u)^{2(q-1)}\left((1-u)^{2(q-1)}+\binom{q-1}{1}(1-u)^{2(q-2)}3u+\right.\right. \\
&\qquad \left.\left.\ldots+3^{(q-1)}u^{(q-1)}\right)\right)du \\
&= \frac{4q^2}{(q-1)}\int_0^1 \frac{1}{u}\left(1-(1-u)^{4(q-1)}-\ldots-\binom{q-1}{k}(1-u)^{2(q-1)+2(q-k)}3^k u^k-\right. \\
&\qquad \left.\ldots-3^{(q-1)}u^{(q-1)}(1-u)^{2(q-1)}\right)du.
\end{aligned}$$

The first term is evaluated as in Proposition 4.5:

$$\begin{aligned}
\frac{4q^2}{(q-1)}\int_0^1 \frac{1}{u}\left(1-(1-u)^{4(q-1)}\right)du &= \frac{4q^2}{(q-1)}H_{4(q-1)} \\
&= \frac{4q^2}{(q-1)}\left(\log 4(q-1)+\gamma+\frac{1}{2(p-1)}\right) \\
&= \frac{(p-1)^2}{\phi(p-1)}\left(\log(p-1)+\log 2+\gamma+\frac{1}{4(p-1)}\right).
\end{aligned}$$

The other terms in the binomial expansion can be approximated as follows. We recall the definition of the Euler Beta function:

$$\int_0^1 (1-t)^{a-1}t^{b-1} = B(a,b) = \frac{(a-1)!(b-1)!}{(a+b-1)!}.$$

Then

$$\begin{aligned}
& 3^k\int_0^1 \binom{q-1}{k}(1-u)^{2(q-1)+2(q-k)}u^{k-1}du \\
= \; & 3^k\binom{q-1}{k}B\left(2(q-1)+2(q-k)+1,k\right) \\
= \; & 3^k\left(\frac{(q-1)!}{k!(q-1-k)!}\right)\frac{(2(q-1)+2(q-k))!(k-1)!}{(2(q-1)+2(q-k)+k)!} \\
= \; & \frac{3^k}{k}\frac{(q-1)}{(4q-k-2)}\frac{(q-2)}{(4q-k-2-1)}\cdots\frac{(q-1-l)}{(4q-k-2-l)}\cdots\frac{(q-1-k+1)}{(4q-k-2-k+1)}.
\end{aligned}$$

In general:

$$\frac{(q-1-l)}{(4q-k-2-l)} = \frac{1}{4} + \frac{-2-3l+k}{4(4q-k-2-l)}.$$

Since $0 \leq l < k$ and $k$ ranges from 1 to $q-1$, we can bound the left hand side from above:

$$\begin{aligned} \frac{1}{4} + \frac{-2-3l+k}{4(4q-k-2-l)} &\leq \frac{1}{4} + \frac{-2+k}{4(4q-k-2-l)} \\ &\leq \frac{1}{4} + \frac{-2+q}{16q} \\ &\leq \frac{1}{4} + \frac{1}{16} = \frac{5}{16}. \end{aligned}$$

Let $K$ be a number much less than $q-1$. We will take $K = q^{1/4}$ for simplicity, although any $K = o(q^{1/2})$ is sufficient. Summing over $k$ we have

$$\begin{aligned} & \sum_{k=1}^{q-1} \frac{3^k}{k} \prod_{l=0}^{k-1} \frac{(q-1-l)}{(4q-k-2-l)} \\ = & \sum_{k=1}^{q-1} \frac{3^k}{k} \prod_{l=0}^{k-1} \left( \frac{1}{4} + \frac{-2-3l+k}{4(4q-k-2-l)} \right) \\ \leq & \sum_{k=1}^{K} \frac{3^k}{k} \prod_{l=0}^{k-1} \left( \frac{1}{4} + \frac{-2+k}{4(4q-k-2-l)} \right) + \sum_{k=K}^{q-1} \frac{3^k}{k} \prod_{l=1}^{k-1} \frac{5}{16}. \end{aligned}$$

The second term can be approximated by a geometric sum:

$$\begin{aligned} \sum_{k=K}^{q-1} \frac{3^k}{k} \prod_{l=1}^{k-1} \frac{5}{16} &= \sum_{k=K}^{q-1} \frac{3^k}{k} \left( \frac{5}{16} \right)^{k-1} \\ &\leq \frac{16}{5} \sum_{k=K}^{\infty} \frac{1}{k} \left( \frac{15}{16} \right)^k \\ &= \frac{16}{5} \frac{1}{K} \left( \frac{15}{16} \right)^K \left( 1 - \frac{15}{16} \right)^{-1} \\ &= \frac{(16)^2}{5} \frac{1}{K} \left( \frac{15}{16} \right)^K. \end{aligned}$$

The first term will be approximated with the aid of several inequalities obtained from Taylor series. Since $e^x > 1 + x$ for all real $x$, we have,

$$\sum_{k=1}^{K} \frac{3^k}{k} \prod_{l=0}^{k-1} \left( \frac{1}{4} + \frac{-2+k}{4(4q-k-2-l)} \right)$$

$$\begin{aligned} &= \sum_{k=1}^{K} \frac{1}{k} \left(\frac{3}{4}\right)^k \prod_{l=0}^{k-1} \left(1 + \frac{-\frac{2}{q} + \frac{k}{q}}{4\left(1 - \frac{k}{16q} - \frac{1}{8q} - \frac{l}{16q}\right)}\right) \\ &\leq \sum_{k=1}^{K} \frac{1}{k} \left(\frac{3}{4}\right)^k e^{\frac{1}{q}\sum_{l=0}^{k-1} \frac{-2+k}{4\left(1 - \frac{k}{16q} - \frac{1}{8q} - \frac{l}{16q}\right)}}. \end{aligned}$$

Using

$$\frac{1}{q}\sum_{l=0}^{k-1} \frac{-2+k}{4\left(1 - \frac{k}{16q} - \frac{1}{8q} - \frac{l}{16q}\right)} \leq \frac{1}{q}\sum_{l=0}^{k-1} \frac{-2+k}{3} \leq \frac{1}{q}\left(-\frac{2}{3}k + \frac{k}{6}(k-1)\right) \leq \frac{k^2}{q}$$

and the inequality $e^x < 1/(1-x)$ for $x > 0$, we have

$$\begin{aligned} \sum_{k=1}^{K} \frac{3^k}{k} \prod_{l=0}^{k-1} \left(\frac{1}{4} + \frac{-2+k}{4(4q-k-2-l)}\right) &\leq \sum_{k=1}^{K} \frac{1}{k}\left(\frac{3}{4}\right)^k e^{\frac{k^2}{q}} \\ &\leq \sum_{k=1}^{K} \frac{1}{k}\left(\frac{3}{4}\right)^k \frac{1}{1-\frac{k^2}{q}} \\ &\leq \sum_{k=1}^{K} \frac{1}{k}\left(\frac{3}{4}\right)^k \frac{q}{q-k^2} \\ &= \sum_{k=1}^{K} \frac{1}{k}\left(\frac{3}{4}\right)^k \left(1 + \frac{k^2}{q-k^2}\right) \\ &= \sum_{k=1}^{K} \frac{1}{k}\left(\frac{3}{4}\right)^k + \sum_{k=1}^{K} \frac{1}{k}\left(\frac{3}{4}\right)^k \left(\frac{k^2}{q-k^2}\right). \end{aligned}$$

Finally, we use the Taylor expansion for $\log(1-x)$ to obtain

$$\begin{aligned} \sum_{k=1}^{K} \frac{3^k}{k} \prod_{l=0}^{k-1} \left(\frac{1}{4} + \frac{-2+k}{4(4q-k-2-l)}\right) &\leq -\log\left(\frac{1}{4}\right) + O\left(\frac{K^2}{q}\right)\ln\left(\frac{3}{4}\right) \\ &= \log 4 - O\left(\frac{K^2}{q}\right). \end{aligned}$$

Putting it all together, we conclude

$$\begin{aligned} E(T) &\leq \frac{(p-1)^2}{\phi(p-1)}\left(\log(p-1) + \log 2 - \log 4 + \gamma + O\left(\frac{1}{q^{1/4}}\right) + \frac{1}{4(p-1)}\right) \\ &= \frac{(p-1)^2}{\phi(p-1)}\left(\log(p-1) + \log\frac{1}{2} + \gamma + O\left(\frac{1}{q^{1/4}}\right) + \frac{1}{4(p-1)}\right). \end{aligned}$$

□

Thus the expected number of draws required to collect all residue classes differs from the classical coupon collector model by $\log(1/2) \approx -0.693$. It may be reasonable to assume that the entire probability distribution function has shifted by this amount, since in Figure 3.2, the empirical distribution function differs from the theoretical one by a shift to the left of approximately 0.6 units, for primes of the form $p = 2q + 1$.

We note that $\log p + \log(1/2)$ is approximately $\log \phi(p-1)$. Although only -1 and 1 were considered as blank coupons, the upper bound of the expectation approaches the lower bound in Proposition 4.5, where all non-primitive residue classes were considered blanks. In the next section, we will use the lower bound in Proposition 4.5 in determining the cumulative distribution function.

## 4.3 Cumulative distribution function

Recall that for the classical coupon collector problem with $m$ types of coupons which are uniformly distributed, we have

$$E(T) = m \log m + \gamma m + \frac{1}{2} + o(1)$$

and

$$\lim_{m \to \infty} P\left(T \leq m \log m + tm\right) = e^{-e^{-t}}.$$

Similarly, given a coupon collector problem with probability distribution matching the frequencies of the residue classes in Table 1.3, if all but the primitive element residue classes are considered to be blank we have

$$E(x) = \frac{(p-1)^2}{\phi(p-1)} \log \phi(p-1) + \gamma \frac{(p-1)^2}{\phi(p-1)} + \frac{1}{2}\left(\frac{p-1}{\phi(p-1)}\right)^2 + o(1)$$

from the proof of Proposition 4.5. Using this estimate for the expectation, we show that

$$\lim_{p \to \infty} P\left(x \leq \frac{(p-1)^2}{\phi(p-1)} \log \phi(p-1) + t\frac{(p-1)^2}{\phi(p-1)}\right) = e^{-e^{-t}}$$

in the coupon collector problem considering the entire table with no blank coupons, if $p-1$ is square-free.

To calculate the cumulative distribution function, we return to generating functions. In [FS09, p. 192], we have the following result.

**Proposition 4.7.** *Consider a set of $m$ coupons under a general probability distribution $\{p_i\}_{i=1}^m$, which are drawn with replacement. Then the probability of obtaining a full collection by time $T$ less than or equal $n$ is given by*

$$P(T \leq n) = n![z^n] \prod_{i=1}^{m} \left(e^{p_i z} - 1\right).$$

*Proof.* Associate to the $m$ coupons the letters $\alpha_1, \alpha_2, \ldots, \alpha_m$. Let $L$ be the language consisting of words containing each letter at least once. Then

$$L = \alpha_1^{\geq 1} \sqcup \alpha_2^{\geq 1} \sqcup \cdots \sqcup \alpha_m^{\geq 1}$$

where

$$\alpha^{\geq 1} = \alpha \cdot \alpha^*.$$

If $\alpha_i$ is a letter occuring with probability $p_i$, then the exponential generating function associated to $\alpha_i^{\geq 1}$ is $(e^{p_i z} - 1)$. Thus, the exponential generating function of $L$ is

$$\hat{l}(z) = \prod_{i=1}^{m} \left(e^{p_i z} - 1\right).$$

Thus, the probability that a random word of $n$ letters is in the language $L$ is

$$n![z^n] \prod_{i=1}^{m} \left(e^{p_i z} - 1\right).$$

□

From now on, we assume that $p$ is a prime such that $p-1$ is square-free. By Proposition 1.11 each residue class of order $d$ in appears in Table 1.3 a total of $\phi(d)g\left((p-1)/d\right)$ times,

where $g$ is a multiplicative function and $g(q) = 2q - 1$. Since there are $\phi(d)$ elements of order $d$, we would like to estimate

$$n![z^n] \prod_{d|(p-1)} \left( e^{\frac{\phi(d) g\left(\frac{p-1}{d}\right)}{(p-1)^2} z} - 1 \right)^{\phi(d)} = \frac{n!}{(p-1)^{2n}} [z^n] \prod_{d|(p-1)} \left( e^{\phi(d) g\left(\frac{p-1}{d}\right) z} - 1 \right)^{\phi(d)}.$$

Thus, we set

$$G(z) = \prod_{d|(p-1)} \left( e^{\phi(d) g\left(\frac{p-1}{d}\right) z} - 1 \right)^{\phi(d)}.$$

Since $G(z)$ is an analytical function, let

$$G(z) = \sum_{n=0}^{\infty} g_n z^n,$$

so that $g_n = [z^n]G(z)$. By the Cauchy integral formula,

$$g_n = \frac{1}{2\pi i} \int_{\mathcal{C}} \frac{G(z)}{z^{n+1}} dz$$

where $\mathcal{C}$ is a contour that encircles the origin. For certain functions $G(z)$, the integral can be evaluated using the saddle point method. Roughly speaking, we can choose a contour $\mathcal{C}$ such that the function is large only on a small part of the contour and small everywhere else; the integral may be approximated by a Gaussian integral which captures the area under the peak. The path of integration passes near to the saddle point of the function, hence the name.

We can use the saddle point method if $G(z)$ is Hayman-admissible. The following definition is from [Hay56, p. 68], with notation from [FS09, Definition VIII.1., p. 565]. Letting $z = re^{i\theta}$, we have

$$\log G\left(re^{i\theta}\right) = \log G(r) + \sum_{\nu=1}^{\infty} \alpha_\nu(r) \frac{(i\theta)^\nu}{\nu!}$$

and define

$$h(z) = \log G(z)$$

and

$$\begin{aligned} a(r) &= \alpha_1(r) = rh'(r) \\ b(r) &= \alpha_2(r) = r^2 h''(r) + rh'(r). \end{aligned}$$

**Definition 4.8** (Hayman-admissibility)**.** *Let $G(z)$ have a radius of convergence $R$ with $0 < R \leq \infty$ and be always positive on some subinterval $(R_0, R)$ of $(0, R)$. The function $G(z)$ is said to be H-admissible (or Hayman-admissible) if, with $a(r)$ and $b(r)$ defined as above, it satisfies the following three conditions:*

1. *(Capture condition)* $\lim_{r\to R} a(r) = \infty$ *and* $\lim_{r\to R} b(r) = \infty$.

2. *(Locality condition) For some function $\theta_0(r)$, defined over $(R_0, R)$ and satisfying $0 < \theta_0 < \pi$, one has*

$$G\left(re^{i\theta}\right) \sim G(r)e^{i\theta a(r)-\theta^2 b(r)/2}$$

   *as $r \to R$, uniformly in $|\theta| \leq \theta_0(r)$.*

3. *(Decay condition) Uniformly in $\theta_0(r) \leq |\theta| \leq \pi$,*

$$G\left(re^{i\theta}\right) = o\left(\frac{G(r)}{\sqrt{b(r)}}\right).$$

One of the convenient closure properties of Hayman-admissibility functions is the following, [Hay56, Theorem VII.].

**Proposition 4.9.** *If $G_1(z)$ and $G_2(z)$ are H-admissible functions with the same radius of convergence $R$, then $G_1(z)G_2(z)$ is also H-admissible.*

Thus for $G(z)$ to be H-admissible it is sufficient to check that a function of the form $H(z) = (e^{\alpha z} - 1)$, where $\alpha > 0$, is H-admissible.

**Proposition 4.10.** *$H(z) = (e^{\alpha z} - 1)$ where $\alpha > 0$ is H-admissible.*

*Proof.* $H(z)$ is analytic and positive on $(0, \infty)$, as required. We have

$$\begin{aligned} a(z) &= \alpha z\left(\frac{e^{\alpha z}}{e^{\alpha z}-1}\right) \\ b(z) &= \alpha z\left(\frac{e^{\alpha z}}{e^{\alpha z}-1}\right) - \frac{\alpha^2 z^2 e^{\alpha z}}{(e^{\alpha z}-1)^2} \end{aligned}$$

and

$$\lim_{r\to\infty} a(r) = \infty, \quad \lim_{r\to\infty} b(r) = \infty,$$

satisfying the first condition.

The value of $\theta_0$ is found using the coefficients in the expansion of $\log G(re^{i\theta})$, by requiring

$$\begin{aligned}\alpha_2(r)\theta_0^2 &\to \infty \\ \alpha_3(r)\theta_0^3 &\to 0.\end{aligned}$$

Since the coefficients $\alpha_j(r)$ tend to $\alpha r$, we can take $\theta_0 = (\alpha r)^{-\frac{2}{5}}$.

Thus,

$$\begin{aligned}\log G(r)e^{i\theta a(r)-\theta^2 b(r)/2} &= \log\left(e^{\alpha r}-1\right) + i\theta a(r) - \theta^2\frac{b(r)}{2} \\ &\sim \alpha r + i\theta\alpha r - \theta^2\alpha\frac{r}{2} \\ &= \alpha r\left(1 + i\theta - \frac{1}{2}\theta^2\right)\end{aligned}$$

as $r$ tends to infinity. On the other hand,

$$\begin{aligned}\log G\left(re^{i\theta}\right) &= \log\left(e^{\alpha r e^{i\theta}}-1\right) \\ &= \log e^{\alpha r e^{i\theta}}\left(1-e^{-\alpha r e^{i\theta}}\right) \\ &= \alpha r e^{i\theta} + \log\left(1-e^{-\alpha r e^{i\theta}}\right) \\ &\sim \alpha r e^{i\theta} \\ &= \alpha r\left(1 + \frac{i\theta}{1!} + \frac{(i\theta)^2}{2!} + \ldots\right).\end{aligned}$$

For $n \geq 3$, the terms

$$\left|\alpha r\frac{(i\theta)^n}{n!}\right| = \frac{1}{n!}\alpha^{1-2n/5}r^{1-2n/5}$$

tend to zero as $r$ tends to infinity. Thus $G\left(re^{i\theta}\right) \sim G(r)e^{i\theta a(r)-\theta^2 b(r)/2}$, satisfying the locality condition.

Finally,

$$\begin{aligned}\left|G\left(re^{i\theta}\right)\right| = \left|e^{\alpha r e^{i\theta}}-1\right| \sim \left|e^{\alpha r\cos\theta}\right| &\leq \left|e^{\alpha r\left(1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}\right)}\right| \\ &\leq \left|e^{\alpha r-\frac{1}{2}(\alpha r)^{1/5}+\frac{1}{24}(\alpha r)^{-3/5}}\right|\end{aligned}$$

$$\begin{aligned} &\leq \frac{e^{\alpha r}}{e^{\frac{1}{2}(\alpha r)^{1/5}}} \\ &= o\left(\frac{e^{\alpha r}}{\sqrt{\alpha r}}\right) = o\left(\frac{G(r)}{\sqrt{b(r)}}\right) \end{aligned}$$

as $r$ tends to infinity. We have used the bound $\theta < (\alpha r)^{-2/5}$ above.

□

The theorem below allows us to estimate the Taylor coefficients of an H-admissible function, from [Hay56, Theorem I.] with notation from [FS09, Theorem VIII.4., p. 565].

**Theorem 4.11.** *Let $G(z)$ be an H-admissible function and $\xi = \xi(n)$ be the unique solution in the interval $(R_0, R)$ of the equation*

$$\xi \frac{G'(\xi)}{G(\xi)} = n.$$

*The Taylor coefficients of $G(z)$ satisfy, as $n \to \infty$:*

$$g_n = [z^n]G(z) \sim \frac{G(\xi)}{\xi^n \sqrt{2\pi b(\xi)}}, \quad \textit{where}, \quad b(z) = z^2 h''(z) + z h'(z),$$

*where $h(z) = \log G(z)$.*

**Theorem 4.12.** *Let $p$ be a prime such that $p-1$ is squarefree. If the elements of Table 1.3 are sampled at random, with replacement, and $x$ is the time (or the number of draws) until obtaining a complete collection of residue classes modulo $p$, we have*

$$\lim_{p\to\infty} P\left(x < \frac{(p-1)^2}{\phi(p-1)} \log \phi(p-1) + t\frac{(p-1)^2}{\phi(p-1)}\right) = e^{-e^{-t}}.$$

*Proof.* Recall that our goal is to estimate

$$g_n = [z^n]G(z) = [z^n] \prod_{d|(p-1)} \left(e^{\phi(d) g\left(\frac{p-1}{d}\right) z} - 1\right)^{\phi(d)}.$$

We have

$$h(z) = \sum_{d|(p-1)} \phi(d) \log\left(e^{\phi(d) g\left(\frac{p-1}{d}\right) z} - 1\right)$$

$$\begin{aligned} h'(z) = \frac{G'(z)}{G(z)} &= \sum_{d|(p-1)} \frac{\phi(d)^2 g\left(\frac{p-1}{d}\right) e^{\phi(d)g\left(\frac{p-1}{d}\right)z}}{\left(e^{\phi(d)g\left(\frac{p-1}{d}\right)z} - 1\right)} \\ h''(z) &= -\sum_{d|(p-1)} \frac{\phi(d)^3 g\left(\frac{p-1}{d}\right)^2 e^{\phi(d)g\left(\frac{p-1}{d}\right)z}}{\left(e^{\phi(d)g\left(\frac{p-1}{d}\right)z} - 1\right)^2}. \end{aligned}$$

Using the equality

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

from Theorem 1.11, we have

$$\begin{aligned} \lim_{r\to\infty} h'(r) &= \sum_{d|(p-1)} \phi(d)^2 g\left(\frac{p-1}{d}\right) = (p-1)^2 \\ \lim_{r\to\infty} h''(r) &= 0. \end{aligned}$$

In addition,

$$\begin{aligned} a(z) &= zh'(z) \to \sum_{d|(p-1)} \phi(d)^2 g\left(\frac{p-1}{d}\right) z = (p-1)^2 z \\ b(z) &= z^2 h''(z) + zh'(z) \to \sum_{d|(p-1)} \phi(d)^2 g\left(\frac{p-1}{d}\right) z = (p-1)^2 z. \end{aligned}$$

The radius of integration should be a good approximation for the solution to the equation $\xi \frac{G'(\xi)}{G(\xi)} = n$, thus

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

We use an estimate of the expectation of $x$ in our expression for $n$,

$$n = \frac{(p-1)^2 \log \phi(p-1) + t(p-1)^2}{\phi(p-1)},$$

and we will find how the cumulative distribution function varies with $t$.

Our goal is to evaluate

$$\frac{n!}{p^{2n}} \left(\frac{1}{\xi^n \sqrt{2\pi b(\xi)}}\right) G(\xi).$$

Using the Stirling approximation for $n!$, the factor $\frac{n!}{p^{2n}} \left(\frac{1}{\xi^n \sqrt{2\pi b(\xi)}}\right)$ tends to $\frac{1}{e^n}$. We have,

$$\frac{1}{e^n} G(\xi) = \frac{1}{e^n} \prod_{d|(p-1)} \left(e^{\phi(d)g\left(\frac{p-1}{d}\right)\frac{n}{(p-1)^2}} - 1\right)^{\phi(d)}$$

$$
\begin{aligned}
&= e^{-n} \prod_{d|(p-1)} e^{\frac{n\phi(d)^2 g\left(\frac{p-1}{d}\right)}{(p-1)^2}} \left(1 - e^{-\frac{n\phi(d) g\left(\frac{p-1}{d}\right)}{(p-1)^2}}\right)^{\phi(d)} \\
&= e^{-n+n\left(\frac{\sum_{d|p-1} \phi(d)^2 g\left(\frac{p-1}{d}\right)}{(p-1)^2}\right)} \prod_{d|(p-1)} \left(1 - e^{-\frac{n\phi(d) g\left(\frac{p-1}{d}\right)}{(p-1)^2}}\right)^{\phi(d)} \\
&= \prod_{d|(p-1)} \left(1 - e^{-n \cdot \frac{\phi(d) g\left(\frac{p-1}{d}\right)}{(p-1)^2}}\right)^{\phi(d)} \\
&= \prod_{d|(p-1)} \left(1 - e^{-\frac{(p-1)^2(\log\phi(p-1)+t)}{\phi(p-1)} \cdot \frac{\phi(d) g\left(\frac{p-1}{d}\right)}{(p-1)^2}}\right)^{\phi(d)} \\
&= \prod_{d|(p-1)} \left(1 - e^{-(\log\phi(p-1)+t)\frac{\phi(d) g\left(\frac{p-1}{d}\right)}{\phi(p-1)}}\right)^{\phi(d)} \\
&= \left(1 - e^{-(\log\phi(p-1)+t)}\right)^{\phi(p-1)} \prod_{d|\frac{(p-1)}{2}} \left(1 - e^{-(\log\phi(p-1)+t)\frac{\phi(d) g\left(\frac{p-1}{d}\right)}{\phi(p-1)}}\right)^{\phi(d)} \\
&= \left(1 - \frac{1}{\phi(p-1)} e^{-t}\right)^{\phi(p-1)} \prod_{d|\frac{(p-1)}{2}} \left(1 - e^{-(\log\phi(p-1)+t)\frac{\phi(d) g\left(\frac{p-1}{d}\right)}{\phi(p-1)}}\right)^{\phi(d)}
\end{aligned}
$$

Since

$$\lim_{p\to\infty} \left(1 - \frac{1}{\phi(p-1)} e^{-t}\right)^{\phi(p-1)} = e^{-e^{-t}},$$

it remains to show that the product over divisors of $(p-1)/2$ tends to 1. Let

$$
\begin{aligned}
\alpha &= \prod_{d|\frac{(p-1)}{2}} \left(1 - e^{-(\log\phi(p-1)+t)\frac{\phi(d) g\left(\frac{p-1}{d}\right)}{\phi(p-1)}}\right)^{\phi(d)} \\
\log\alpha &= \sum_{d|\frac{(p-1)}{2}} \phi(d) \log\left(1 - \left(\frac{e^{-t}}{\phi(p-1)}\right)^{\frac{g\left(\frac{p-1}{d}\right)}{\phi\left(\frac{p-1}{d}\right)}}\right).
\end{aligned}
$$

We must have $t \gg -\phi(p-1)$, since we expect $n \gg p^2/\phi(p-1)$ by Theorem 4.5 on the lower bound on expectation. Thus, $\left(\frac{e^{-t}}{\phi(p-1)}\right) \ll 1$. Using the Taylor expansion for $\log(1-x)$ for small $x$, we have

$$\log\alpha = \sum_{d|\frac{(p-1)}{2}} \phi(d)\left(-\left(\frac{e^{-t}}{\phi(p-1)}\right)^{\frac{g\left(\frac{p-1}{d}\right)}{\phi\left(\frac{p-1}{d}\right)}} + O\left(\frac{e^{-t}}{\phi(p-1)}\right)^{2\frac{g\left(\frac{p-1}{d}\right)}{\phi\left(\frac{p-1}{d}\right)}}\right)$$

If $(p-1)/d = q_1 q_2 \dots q_r$ then

$$\begin{aligned} g\left(\frac{p-1}{d}\right) &= (2q_1-1)(2q_1-1)\cdots(2q_r-1) \\ \phi\left(\frac{p-1}{d}\right) &= (q_1-1)(q_1-1)\cdots(q_r-1) \end{aligned}$$

so that

$$\inf \frac{g\left(\frac{p-1}{d}\right)}{\phi\left(\frac{p-1}{d}\right)} = 2.$$

Notice that $(p-1)/d = q$ and as $q$ gets very large, then $(2q-1)/(q-1)$ approaches 2. We will use the notation $\mathbf{d}(x)$ for the number of divisors of $x$. We have

$$\begin{aligned} |\log\alpha| &< \left|\sum_{d|\frac{(p-1)}{2}} \phi(d)\left(-\left(\frac{e^{-t}}{\phi(p-1)}\right)^2 + O\left(\frac{e^{-t}}{\phi(p-1)}\right)^4\right)\right| \\ &< \left|-\left(\frac{e^{-t}}{\phi(p-1)}\right)^2 \phi(p-1)\mathbf{d}\left(\frac{p-1}{2}\right) + \phi(p-1)\mathbf{d}\left(\frac{p-1}{2}\right) O\left(\frac{e^{-t}}{\phi(p-1)}\right)^4\right| \\ &< \left|-\left(\frac{e^{-2t}}{\phi(p-1)}\right) p^{\epsilon} + O\left(\frac{e^{-4t}p^{\epsilon}}{\phi(p-1)^3}\right)\right|. \end{aligned}$$

Thus:

$$\begin{aligned} \lim_{p\to\infty} \log\alpha &= 0. \\ \lim_{p\to\infty} \alpha &= 1, \end{aligned}$$

as required. □

## 4.4 Computational results

The theoretical cumulative distribution function now agrees well with empirical results, correcting the shift seen in the simple model. We change

$$X_p = \left(x - \frac{p(p-1)\log(p-1)}{\phi(p-1)}\right)\left(\frac{\phi(p-1)}{p(p-1)}\right),$$

to

$$X_p = \left(x - \frac{p(p-1)\log\phi(p-1)}{\phi(p-1)}\right)\left(\frac{\phi(p-1)}{p(p-1)}\right). \tag{4.6}$$

We have modified the expression from Theorem 4.12 by a multiple of $p/(p-1)$, to correct for the omission of multiples of $p$ when we are drawing elements from Table 1.3. However, this is not a significant change.

The empirical distribution function for the $X_p$'s matches the function $e^{-e^{-t}}$ quite well, as shown in Figure 4.1. We will use the Kolmogorov-Smirnov test, which is based on a stronger version of the Glivenko-Cantelli theorem, to compare the empirical and theoretical distributions.

**Theorem 4.13** (Glivenko-Cantelli)**.** *Let $X_1, X_2, \ldots, X_n$ independent, identically distributed random variables with cumulative distribution function $F(x)$. Then the empirical cumulative distribution $\hat{F}_n(x)$ converges uniformly to $F(x)$. That is,*

$$\sup_{x\in\mathbb{R}} |\hat{F}_n(x) - F(x)| \to 0$$

*almost surely (i.e. with probability 1).*

Kolmogorov proved the following stronger result.

**Theorem 4.14** (Kolmogorov)**.** *If $F(x)$ is continuous then the distribution of $\sup_{x\in\mathbb{R}} |\hat{F}_n(x) - F(x)|$ does not depend on $F$.*

Furthermore $D_n = \sqrt{n}\sup_{x\in\mathbb{R}} |\hat{F}_n(x) - F(x)|$ converges to the Kolmogorov-Smirnov distribution.

**Theorem 4.15.** *With notation as above, we have,*

$$P\left(D_n \leq t\right) \to H(t) = 1 - 2\sum_{k=1}^{\infty}(-1)^{k-1}e^{-2k^2t^2}$$

*where $H(t)$ is the cumulative distribution function of the Kolmogorov-Smirnov distribution.*

Thus, if the empirical sample has cumulative probability distribution $F(x)$, then the distribution of $D_n$ (which depends only on $n$) is approximated by the Kolmogorov-Smirnov distribution. Otherwise, $\sup_{x\in\mathbb{R}} |\hat{F}_n(x) - F(x)| > \delta$, and $D_n > \sqrt{n}\delta \to \infty$ as $n \to \infty$. The Kolmogorov-Smirnov test rejects or accepts the null hypothesis based on a threshold value of $D_n$, which depends on the level of significance.

For primes less than 72500, the graphs comparing the empirical and theoretical distributions shows a great improvement from the graphs in Section 3.3. For squarefree primes, the Kolmogorov-Smirnov test accepts the null hypothesis of the double exponential distribution $e^{-e^{-t}}$, at a significance value 0.05, with $p$-value of 0.05301. For all odd primes less than 72500, the test accepts the null hypothesis at a significance value 0.05, with $p$-value of 0.7318.

The $p$-value is the probability of getting a result at least as extreme as the empirical value, assuming that the null hypothesis is true. A $p$-value of 0.7318 means that there is little or no evidence against the null hypothesis.

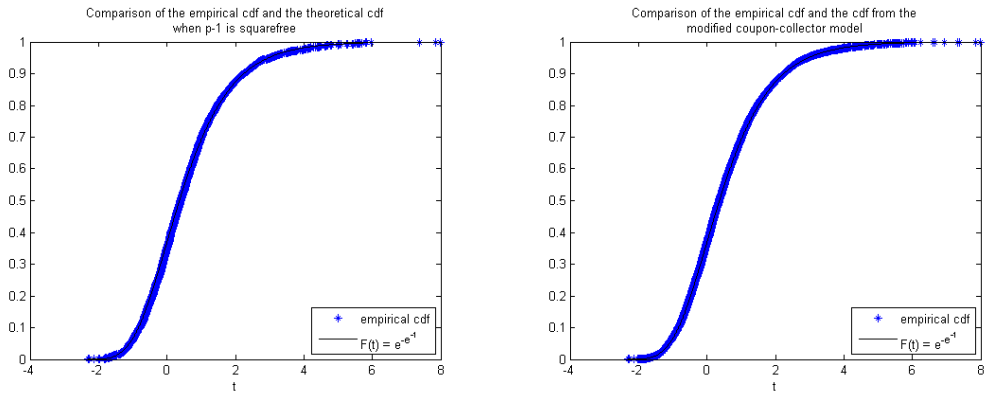


Figure 4.1: Comparison between the cumulative distribution function derived from the coupon collector problem and the empirical distribution function for the variables $X_p$ from equation (4.6). The graphs represent the empirical distributions obtained from squarefree primes less than 72500 and all odd primes less than 72500, respectively.

# Chapter 5

# A deterministic bound

In this chapter we will prove the following theorem.

**Theorem 5.1.** *For a sufficiently large prime $p$, and any fixed residue class $a \pmod p$, there exists an $n$ such that*

$$n^n \equiv a \pmod p$$

*and $n < p^{2-\alpha}$, for some $\alpha > 0$ independent of $p$.*

For instance, for any large $p$, the value $\alpha \leq 1 \times 10^{-3}$ is sufficient, as shown in Section § 5.4.

## 5.1 Elements $a$ of small order

If $a \equiv 0 \pmod p$, we have $p^p \equiv 0 \pmod p$, and so we may consider only nonzero elements $a$ in $\mathbb{Z}/p\mathbb{Z}$. Table 1.3, reproduced below for convenience, will again be useful.

Given $a$, finding a solution $n < p^{2-\alpha}$ to the equation $n^n \equiv a \pmod p$ is equivalent to the element $a$ appearing in the first $p^{1-\alpha}$ rows of the table. Using the notation from the table, this means that we have $n^n \equiv a \pmod p$ with $n = kp + b$ where $k < p^{1-\alpha}$ and $1 \leq b \leq p-1$.

| | Values of $n^n \pmod p$, where $n = kp + b$ | | | | | |
|---|---|---|---|---|---|---|
| $b$ | 1 | 2 | 3 | ... | $(p-2)$ | $(p-1)$ |
| $k = 0$ | $1^1$ | $2^2$ | $3^3$ | ... | $(p-2)^{p-2}$ | $(p-1)^{p-1}$ |
| $k = 1$ | $1^2$ | $2^3$ | $3^4$ | ... | $(p-2)^{p-1}$ | $(p-1)^1$ |
| $k = 2$ | $1^3$ | $2^4$ | $3^5$ | ... | $(p-2)^1$ | $(p-1)^2$ |
| $\vdots$ | $\vdots$ | | | | | |
| $k = (p-2)$ | $1^{p-1}$ | $2^1$ | $3^2$ | ... | $(p-2)^{p-3}$ | $(p-1)^{p-2}$ |

Recall that if $b \pmod p$ has low multiplicative order, $\operatorname{ord} b = m$, then all the elements of order dividing $m$ will appear in the first $m$ rows of the $b$th column in Table 1.3. Thus if a column is 'generated' by an element $b$ of low order, then $b$ itself will appear as

$$n^n = (kp + b)^{kp+b} \equiv b \pmod p$$

for some $k < m$.

Therefore if

$$n^n \equiv a \pmod p$$

where $a$ has small order, say $p^\eta$, we may find solutions with $n \leq p^{1+\eta}$ simply by considering the elements in the column generated by $a$. Therefore, we separate the elements of $(\mathbb{Z}/p\mathbb{Z})^\times$ into those of small multiplicative order (less than or equal to $p^\eta$) and those of large order (greater than $p^\eta$). It remains to prove the theorem for $a$ of large order.

To obtain an numerical value for $\alpha$ in Theorem 5.1 using a deterministic bound from Shparlinski [Shp11], we must take $\eta > 1/2$.

## 5.2 Elements $a$ of large order

The idea for the proof for elements of large order is as follows: we would like the position of an element $a$ to be scattered enough in Table 1.3, so that $a$ will appear at least once

in the top rows. We will consider the appearance of $a$ only in the columns of elements of the same order. To simplify further, it is sufficient for $a$ to be scattered in the columns of Table 5.1.

| | Values of $n^j \pmod p$ | | | | | |
|---|---|---|---|---|---|---|
| $n$ | 1 | 2 | 3 | ... | $(p-2)$ | $(p-1)$ |
| $j=1$ | $1^1$ | $2^1$ | $3^1$ | ... | $(p-2)^1$ | $(p-1)^1$ |
| $j=2$ | $1^2$ | $2^2$ | $3^2$ | ... | $(p-2)^2$ | $(p-1)^2$ |
| $j=3$ | $1^3$ | $2^3$ | $3^3$ | ... | $(p-2)^3$ | $(p-1)^3$ |
| $\vdots$ | $\vdots$ | | | | | |
| $j=(p-1)$ | $1^{p-1}$ | $2^{p-1}$ | $3^{p-1}$ | ... | $(p-2)^{p-1}$ | $(p-1)^{p-1}$ |

Table 5.1: We consider the table $n^j \pmod p$, from which we may obtain the table for $n^n \pmod p$ by a shift along the diagonal. Thus if elements in this table are scattered, so are those in the $n^n$ table.

The proof follows the strategy for Theorem 8 in [Mur10]. We relabel $a$ as $g$, and we consider it to be a fixed element in $(\mathbb{Z}/p\mathbb{Z})^\times$ of multiplicative order $t > p^\eta$. On a first reading of the proof, it may be useful to think of the simplest case, when $g$ is a primitive root; hence the change in notation.

Denote the representatives mod $p$ of all the elements of order $t$ as

$$1 < g_1 < g_2 < \ldots < g_N < p$$

where $N = \phi(t)$. Note that $g$ is equal to one of the $g_i$'s. Let $1 \leq a_i < t$ be the numbers relatively prime to $t$ such that

$$g_i^{a_i} \equiv g \mod p.$$

Then,

$$g_i \equiv g^{a_i^{-1}} \mod p,$$

where the inverse of $a_i$ is taken modulo $t$.

To show that $n^n \equiv g \mod p$ has a solution in $n$ with $n < p^{2-\alpha}$, it will be enough to show that the sequence $\{(a_i, g_i)\}_{i=1}^N$ is sufficiently scattered in the $t \times p$ rectangle. This is equivalent to the element $g$ being scattered in Table 5.1. First normalize to the unit square $[0,1)^2$ and recall that $g_i \equiv g^{a_i^{-1}} \mod p$, to obtain the sequence

$$\left\{\left(\frac{a_i}{t}, \frac{g_i}{p}\right)\right\}_{i=1}^N = \left\{\left(\frac{a_i}{t}, \frac{g^{a_i^{-1}}}{p}\right)\right\}_{i=1}^N.$$

We begin by showing that the discrepancy of this sequence is small.

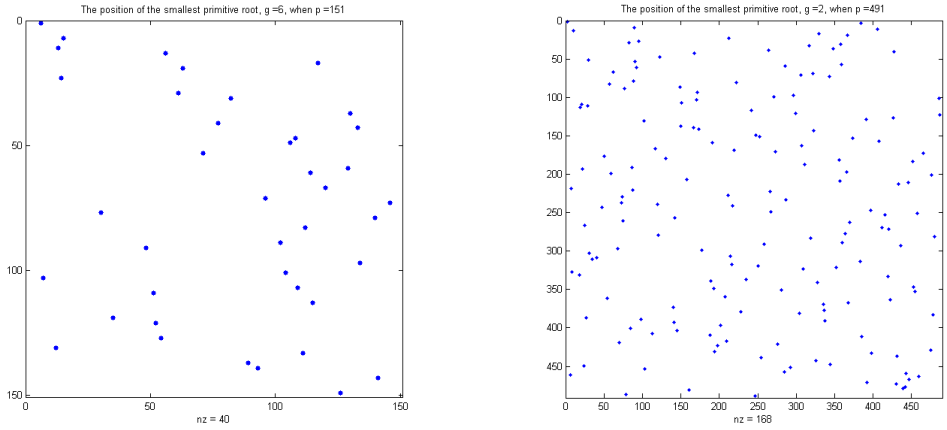


Figure 5.1: If $g$ is primitive, the rectangle of interest has dimensions $(p-1) \times p$. The figure shows the positions of $\{(a_i, g_i)\}_{i=1}^N$ corresponding to the smallest primitive roots $g = 6$ and $g = 2$ for the primes 151 and 491, respectively.

**Proposition 5.2.** *Let $p$ be a prime. The discrepancy of the sequence*

$$\left\{\left(\frac{a_i}{t}, \frac{g_i}{p}\right)\right\}_{i=1}^N$$

*is bounded by $O\left((\log^2 t) N^{-1} t^{1-\delta}\right)$, for some $\delta > 0$, where $N = \phi(t)$.*

*Proof.* Consider the sum

$$S_{m,n} = \sum_{i=1}^N e\left(m\frac{g^{a_i^{-1}}}{p} + n\frac{a_i}{t}\right)$$

$$\begin{aligned} &= \sum_{i=1}^{N} e_p\left(mg^{a_i^{-1}}\right) e_t(na_i) \\ &= \sum_{(x,t)=1} e_p\left(mg^{x^{-1}}\right) e_t(nx). \end{aligned}$$

We will restrict $m, n$ to be integers less than $t$ in magnitude. Theorem 4 in [BS08] gives the following bound, which applies for the case $m \neq 0$ and $-t < m, n < t$.

**Theorem 5.3.** *For any $\eta > 0$ there exists $\delta > 0$ such that for $t \geq p^{\eta}$, uniformly over $m \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ and $n \in \mathbb{Z}/t\mathbb{Z}$, we have the bound*

$$S_{m,n} \ll t^{1-\delta}.$$

If $n \neq 0$ and $m = 0$ the sum reduces to the Ramanujan sum:

$$S_{0,n} = \sum_{(x,t)=1} e_t(nx).$$

We have

$$S_{0,n} = \overline{S_{0,-n}},$$

so that $|S_{0,n}| = |S_{0,-n}|$. Therefore, we need only consider the cases when $m, n$ are non-negative. The Ramanujan sum can be evaluated using von Sterneck's formula, where $k = \gcd(n, t)$:

$$S_{0,n} = \mu\left(\frac{t}{k}\right) \frac{\phi(t)}{\phi\left(\frac{t}{k}\right)}.$$

By the Erdős-Turán inequality, Theorem 3.4 for two dimensions, we have

$$\Delta \leq C \left( \frac{2}{M+1} + \frac{1}{N} \sum_{\substack{(m,n)\neq(0,0) \\ 0\leq m,n\leq M}} \left(\frac{1}{1+m}\right)\left(\frac{1}{1+n}\right) |S_{m,n}| \right). \tag{5.1}$$

Taking $m$ and $n$ non-negative above only changes the constant in Erdös-Turán inequality by a multiple of 4, so that

$$C = 4 \cdot \left(\frac{3}{2}\right)^2.$$

We can separate the sum above into two parts, depending on whether $|S_{m,n}| < t^{1-\delta}$ or $|S_{m,n}| > t^{1-\delta}$. By the result of [BS08] quoted above, we only have to consider sums of the form $|S_{0,n}|$. Let $A$ be the set

$$A = \left\{1 \leq n < t \text{ such that } |S_{0,n}| > t^{1-\delta}\right\}.$$

Taking $M = t - 1$ in equation (5.1), we have

$$\begin{aligned} \Delta &\leq C\left(\frac{2}{t} + \frac{1}{N}\sum_{\substack{(m,n)\neq(0,0),n\notin A\\ 0\leq m,n<t}}\left(\frac{1}{1+m}\right)\left(\frac{1}{1+n}\right)t^{1-\delta} + \frac{1}{N}\sum_{\substack{n\in A\\ 1\leq n<t}}\left(\frac{1}{1+n}\right)|S_{0,n}|\right) \\ &\leq C\left(\frac{2}{t} + (\log^2 t)\frac{t^{1-\delta}}{N} + \frac{1}{N}\sum_{\substack{n\in A\\ 1\leq n<t}}\left(\frac{1}{1+n}\right)|S_{0,n}|\right) \end{aligned} \tag{5.2}$$

In order to show that the discrepancy is small, it remains to show that

$$\frac{1}{N}\sum_{\substack{n\in A\\ 1\leq n<t}}\left(\frac{1}{1+n}\right)|S_{0,n}|$$

is small. We obtain the needed bound from the following two lemmas.

**Lemma 5.4.** *If $n \in A$, then $n > t^{1-2\delta}$.*

*Proof.* In general, $S_{0,n} = 0$, or

$$|S_{0,n}| = \frac{\phi(t)}{\phi\left(\frac{t}{k}\right)}.$$

For $n \in A$, it follows that

$$\frac{\phi(t)}{\phi\left(\frac{t}{k}\right)} > t^{1-\delta}.$$

Thus $\phi\left(\frac{t}{k}\right) < t^{\delta}$.

Since for all $x > 2$,

$$\phi(x) > \frac{x}{e^{\gamma}\log\log x + \frac{3}{\log\log x}}$$

[BS66, p. 320] and $\log\log(t/k) > 1$ for $(t/k) > e^e$, we have

$$t^{\delta} > \phi\left(\frac{t}{k}\right) > \frac{\frac{t}{k}}{e^{\gamma}\log\log\frac{t}{k} + 3}$$

provided $(t/k) > e^e$. Thus

$$\begin{aligned} t^\delta &> \frac{\frac{t}{k}}{e^\gamma \log\log t + 3} \\ k &> \frac{t^{1-\delta}}{e^\gamma \log\log t + 3}. \end{aligned} \tag{5.3}$$

We remark that in the case $\log\log(t/k) < 1$, we have $k > (t/e^e)$. Thus in either case, $n > k > t^{1-2\delta}$ for $t$ large enough. □

**Lemma 5.5.** *For $p$ large enough, $|A| \leq t^{2\delta}$.*

*Proof.* We have from [Bac97] the identity

$$\sum_{n=1}^{t} |S_{0,n}| = \phi(t) 2^{\omega(t)}$$

where $\omega(t)$ is the number of distinct prime divisors of $t$. From the inequality [NZM91, p. 394]

$$2^{\omega(t)} < t^{\frac{(1+\epsilon)\log 2}{\log\log t}}$$

we obtain $2^{\omega(t)} < t^\delta$ if $t$ is large enough.

Thus, there are at most

$$\frac{2^{\omega(t)} N}{t^{1-\delta}} \leq 2^{\omega(t)} t^\delta \leq t^{2\delta}$$

elements of $A$, where we have $N = \phi(t)$. □

We can now return to the proof of Theorem 5.1. Using the trivial estimate $|S_{0,n}| < N$, we have

$$\frac{1}{N} \sum_{\substack{n \in A \\ 1 \leq n < t}} \left( \frac{1}{1+n} \right) |S_{0,n}| \leq t^{2\delta} t^{-1+2\delta} = \frac{1}{t^{1-4\delta}}.$$

Substituting this into the expression for the discrepancy in (5.2), we have

$$\Delta < C'(\log^2 t) \frac{t^{1-\delta}}{N} < C'(\log^2 t) \frac{t^{1-\delta}}{N}.$$

□

**Proposition 5.6.** *Every element $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order $t > p^{1/2}$ can be represented as $n^n \equiv g \mod p$ for some natural number $n \leq p^{2-\alpha}$ for some $\alpha > 0$.*

*Proof.* For the equivalence $n^n \equiv g \mod p$ to have a solution with $n < p^{2-\alpha}$, we must show that

$$g_i^{g_i+k_i} \equiv g \mod p$$

for $k_i < p^{1-\alpha}$, for at least one value $i = i_0$. Then the required $n$ is equal to $pk_{i_0} + g_{i_0}$. We find such a solution as follows.

Recall that the discrepancy is defined by

$$\Delta = \sup_{B \subset [0,1)^2} \left| \frac{\mathcal{N}(B)}{N} - |B| \right|$$

where $\mathcal{N}(B)$ is the number of elements in the sequence that fall into the box $B$. Recall that $N = \phi(t)$ and using the bound for discrepancy as in [Mur10], we obtain

$$\begin{aligned} \mathcal{N}(B) &> N(|B| - \Delta) \\ &> \phi(t)|B| - C'(\log^2 t)t^{1-\delta}. \end{aligned}$$

Therefore, if

$$|B| = \phi(t)^{-\delta'}, \text{ where } \delta' < \delta$$

we have $\mathcal{N}(B) > 0$ for $p$ large enough; this is because $t^{1-\delta} = o\left(\phi(t)^{1-\delta'}\right)$. In other words $B$ contains at least one point,

$$\left\{ \left( \frac{a_i}{t}, \frac{g_i}{p} \right) \right\}_{i=1}^{N}$$

from the sequence.

When we re-normalize, we note that the length and width of the box were stretched by different factors, so that we must multiply the area by $pt$. Thus, in the $t \times p$ rectangle every box of area

$$|B_{\text{re-normalized}}| = pt\phi(t)^{-\delta'} = pt^{1-\delta''}, \text{ where } \delta'' < \delta' < \delta. \tag{5.4}$$

contains a point of the sequence $\{(a_i, g_i)\}_{i=1}^{N}$.

The rectangles of size $t \times p$ will repeat within the larger $(p-1) \times p$ rectangle. Consider a box of height $t^{1-\delta''/2}$ and length $pt^{-\delta''/2}$. Position it as in Figure 5.2, so that its upper right corner is along the diagonal $(c, c), 1 \leq c \leq p-1$ and so that it falls within one of the $t \times p$ rectangles. Then we have

$$g_{i_0}^{a_{i_0}} \equiv g_{i_0}^{g_{i_0}+k_{i_0}} \equiv g \pmod{p}$$

where

$$k_{i_0} < pt^{-\delta''/2} + t^{1-\delta''/2}.$$

If we take $t > p^{1/2+o(1)}$, then

$$k_{i_0} < p^{1-\delta''/4} + t^{1-\delta''/2} \leq 2p^{1-\delta''/4} < p^{1-\alpha}$$

as required.

□

## 5.3 Proof of Theorem 5.1

To summarize, to prove Theorem 5.1 we divided the elements $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ into two sets according to their multiplicative order. From §5.1, if $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ has multiplicative order less than or equal $p^\eta$, there exits $n$ so that

$$n^n \equiv a \pmod{p}$$

and $n \leq p^{1+\eta}$.

From §5.2, if $a$ has multiplicative order greater than $p^\eta$, there exits $n$ so that

$$n^n \equiv a \pmod{p}$$

and $n < p^{2-\alpha}$ for some $\alpha > 0$.

Choosing $\eta < 1 - \alpha$ we obtain Theorem 5.1 for all $a \in (\mathbb{Z}/p\mathbb{Z})^\times$.

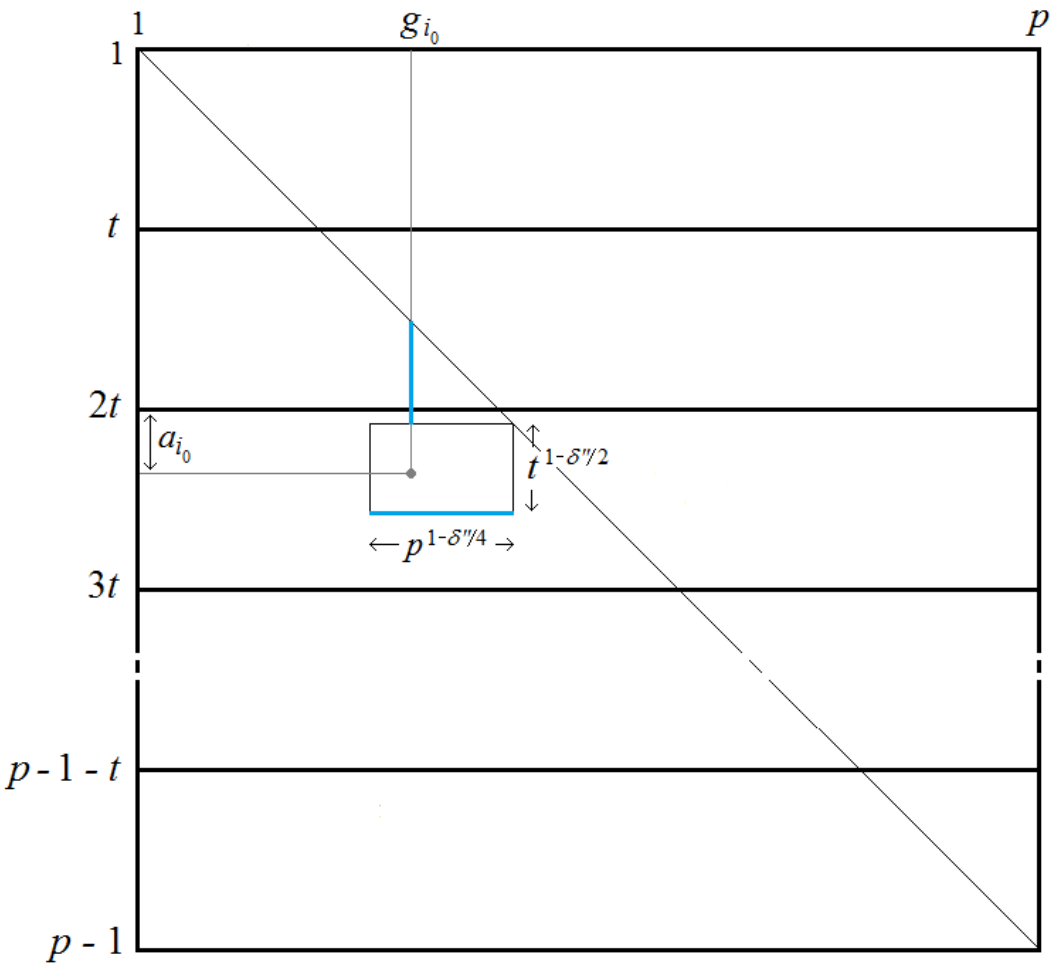


Figure 5.2: Every box of height $t^{1-\delta''/2}$ and length $p^{1-\delta''/4}$ contains one element of the sequence $\{(a_i, g_i)\}_{j=1}^{N}$. Considering a box positioned under the diagonal will give an element $(a_{i_0}, g_{i_0})$ with the required properties.

## 5.4 A numerical value of $\alpha$

To find a finite value of $\alpha$ in Theorem 5.1 that is large enough, it is sufficient to maximize $\delta''$, hence $\delta$ (see equation (5.4)). Let $t = p^\eta$ where $\frac{1}{2} < \eta \leq 1$. We will find a value of $\delta$ in terms of $\eta$ that is maximal according to the following explicit bound for $S_{m,n}$ given by Shparlinski in [Shp11].

**Theorem 5.7.** *Let $g$ be of multiplicative order $t$. Then for any fixed integers $u, v \geq 2$ uniformly over $m \in (\mathbb{Z}/p\mathbb{Z})^\times$ and $n \in \mathbb{Z}/t\mathbb{Z}$, we have the bound*

$$S_{m,n} \leq t^{1-r_{u,v}} p^{s_{u,v}+o(1)}$$

*as $p \to \infty$ where*

$$r_{u,v} = \frac{1}{2(2u+v)} - \frac{1}{4uv} \quad \text{and} \quad s_{u,v} = \frac{1}{4(2u+v)}.$$

Since $r_{u,v} < s_{u,v}/2$, we may assume that

$$t \geq p^{1/2}(\log p)^2$$

as otherwise the bound is trivial. Let $t = p^\eta$, where $\eta > 1/2$. Substituting $p = t^{1/\eta}$ into the inequality for $S_{m,n}$,

$$S_{m,n} \leq t^{1+\frac{1}{\eta}\frac{1}{4(2u+v)} - \frac{1}{2(2u+v)} + \frac{1}{4uv} + \frac{o(1)}{\eta}} = t^{1-\delta}$$

where

$$\delta = \delta_{u,v} = \frac{1}{2(2u+v)} - \frac{1}{4uv} - \frac{1}{\eta}\frac{1}{4(2u+v)} - \frac{o(1)}{\eta}. \tag{5.5}$$

We will find the appropriate values of $u, v > 2$ that maximize $\delta$ for a given $\eta$ according to the formula above. This is a small calculus exercise.

**Claim.** *The value $\delta$ is maximized in the equation (5.5) when*

$$u = \frac{4\eta}{(2\eta - 1)}$$

$$v = \frac{8\eta}{(2\eta - 1)}$$

*and*

$$\delta = \frac{1}{2^7}\frac{(2\eta-1)^2}{\eta^2} - \frac{o(1)}{\eta}.$$

*Proof.* Let $z = 2u + v$. Then $v = z - 2u$ and

$$\delta = \left(\frac{1}{2} - \frac{1}{4\eta}\right) z^{-1} - \frac{1}{4}u^{-1}(z-2u)^{-1}.$$

$$\begin{aligned}
\delta_u &= -\frac{1}{4}(-1)u^{-2}(z-2z)^{-1} - \frac{1}{4}u^{-1}(-1)(z-2u)^{-2}(-2) \\
\delta_z &= \left(\frac{1}{2} - \frac{1}{4\eta}\right)(-1)z^{-2} - \frac{1}{4}u^{-1}(-1)(z-2u)^{-2}.
\end{aligned}$$

For $\delta_u$ to be zero,

$$\begin{aligned}
\frac{1}{u^2}\frac{1}{(z-2u)} - \frac{2}{u}\frac{1}{(z-2u)^2} &= 0 \\
\frac{1}{u^2}\frac{1}{(z-2u)} &= \frac{2}{u}\frac{1}{(z-2u)^2} \\
(z-2u) &= 2u \\
z &= 4u \\
\therefore v &= 2u.
\end{aligned}$$

For $\delta_v$ to be zero as well,

$$\left(\frac{1}{2} - \frac{1}{4\eta}\right)\frac{1}{z^2} = \frac{1}{4}\cdot\frac{1}{u}\cdot\frac{1}{(z-2u)^2}.$$

Substituting $z = 4u$,

$$\begin{aligned}
\left(\frac{1}{2} - \frac{1}{4a}\right)\cdot\frac{1}{16u^2} &= \frac{1}{4}\cdot\frac{1}{u}\cdot\frac{1}{(2u)^2} \\
u &= \frac{1}{\left(\frac{1}{2} - \frac{1}{4\eta}\right)} \\
\therefore u &= = \frac{4\eta}{(2\eta-1)}.
\end{aligned}$$

Substituting the above expression of $u$ in terms of $\eta$ into $z = 4u$ and then into $\delta_{u,z}$, yields the required values. It remains now to show by the second-derivative test that these values are maximums. Since

$$\begin{aligned}
\delta_{uu}|_{u=\frac{4\eta}{(2\eta-1)}} &= -\frac{1}{4}\left(\frac{1}{2}-\frac{1}{4\eta}\right)^4 < 0 \\
\delta_{zz}|_{u=\frac{4\eta}{(2\eta-1)}} &= -\frac{1}{32}\left(\frac{1}{2}-\frac{1}{4\eta}\right)^4 < 0 \\
\delta_{uz}|_{u=\frac{4\eta}{(2\eta-1)}} &= \frac{1}{16}\left(\frac{1}{2}-\frac{1}{4\eta}\right)^4
\end{aligned}$$

and

$$\delta_{uu}\delta_{zz} - \delta_{uz}^2 = \frac{1}{256}\left(\frac{1}{2}-\frac{1}{4\eta}\right)^4 > 0,$$

by the second derivative test, we have a local maximum.

The maximum found is absolute. The function $\delta_{u,v}$ has continuous derivatives in $u$ and $v$, so that it is sufficient to check the values on the boundaries of $u, v \in [2, \infty)$. As $u$ or $v$ tend to infinity, $\delta_{u,v}$ tends to $-\frac{o(1)}{\eta}$. If $v = 2$,

$$\delta_{u,2} = \frac{1}{(u+1)}\left(\frac{1}{4}-\frac{1}{8\eta}\right) - \frac{1}{8u} - \frac{o(1)}{\eta} < 0.$$

If $u = 2$, $\delta_{2,v}$ has a maximum at

$$v = \frac{4}{-1+\sqrt{4-\frac{2}{\eta}}}$$

provided that $\eta > \frac{2}{3}$, but this maximum is smaller than the one found inside the region $u, v > 2$.

□

We have $\delta'' < \delta' < \delta$ and $\alpha < \delta''/4$. Therefore if $\eta = 5/6$, for instance, we ensure that $u = 5$ and $v = 10$ are integers and by equation (5.5)

$$\delta = 0.005 - \frac{5}{6}\cdot o(1).$$

We may take

$$\alpha < 0.004/4 = 0.001.$$

# Chapter 6

# Conclusion and future work

We expect that $n^n \equiv a \bmod p$ has a solution with $n \leq x$, for any given residue class $a$, if $x$ is approximately $p^2 \log \phi(p-1)/\phi(p-1)$. We have proved the deterministic bound $x < p^{2-\alpha}$ where $\alpha > 0$ is small. The first natural question to ask is whether it may be possible to obtain a deterministic bound that is closer to the heuristic bound.

To obtain the heuristic estimate, we used a model based on the coupon collector problem. To our knowledge, the coupon collector problem has not previously appeared in a number theory context. We anticipate modifying the problem to improve and obtain other estimates. A first improvement would be to calculate the cumulative distribution function for all primes $p$, not only for the case when $p-1$ is square free.

Furthermore, it would be interesting to check under what conditions the least frequent coupons are the bottleneck for determining the expectation. Thus, the coupon collector problem with blank coupons may be used to obtain estimates for a full collection of residue classes with a desired property, such as $k$th powers. All residue classes not possessing the property would be 'blank' coupons.

Finally, we may be able to give a heuristic argument for the number of different residue classes that appear as $n^n \bmod p$ where $1 \leq n \leq p-1$, to determine the sharpness of the bounds given by Crocker [Cro69] and Somer [Som81].

We established the existence of small solutions for $n^n \equiv a \bmod p$, although $n^n \bmod p$ is not uniformly distributed. The method of proof was first applied in [Mur10] to find small solutions for $x^q \equiv a \bmod p$, where the order of $a$ is a multiple of $(p-1)/q$ and the magnitude of $q$ depends on $p$. Thus, the same method may be used to find small solutions of other functions.

In the first part of the thesis, we extended bounds for the number of solutions to $n^n \equiv a \bmod p$ for a fixed residue class $a$. Previous bounds from Balog et al. [BBS11] considered $1 \leq n \leq p-1$, and we extended those bounds for the case when $n > p$. The bounds obtained are quite far from the conjectured values [Hol02b]. Using further tools from additive combinatorics and exponential sums, we may perhaps obtain stronger results.

# Appendix A

# Formal Languages and Probabilities

The following background on formal languages, generating functions, and probabilities is taken from Section 2 of [FGT92], which summarizes the methods used to relate formal descriptions of regular languages to generating functions and probability estimates.

**Definition A.1.** *Let $\mathcal{A} = \{a_1, a_2, \ldots, a_m\}$ be a fixed set called the alphabet whose elements are the letters. Then $\mathcal{A}^*$ denotes the set of all finite sequences, called the* words *or strings of $\mathcal{A}$. A* language *is any subset of $\mathcal{A}^*$.*

Given languages $L_1$, $L_2$, and $L$, we define the following operations:

- *union* of $L_1$ and $L_2$: $L_1 + L_2 = \{w | w \in L_1 \text{ or } w \in L_2\}$
- *product* of $L_1$ and $L_2$: $L_1 L_2 = \{w_1 w_2 | w_1 \in L_1 \text{ and } w_2 \in L_2\}$
- *star* $L^*$: the language formed from all possible sequences from elements of $L$,

$$L^* = \{\varepsilon\} + L + (L \cdot L) + (L \cdot L \cdot L) + \ldots$$

  where $\varepsilon$ denotes the empty word.

**Definition A.2.** *The class of* regular languages *is the smallest class of languages containing the finite sets and closed under the three operations of union, product and star.*

We extend the class of regular languages by the addition of another operation:

- *shuffle product*: Given two words $w_1$ and $w_2$, their shuffle, $(w_1 \sqcup\!\sqcup w_2)$ is the set of all words obtained by interlacing the letters of $w_1$ and $w_2$ in all possible ways, while preserving their order inside $w_1$ and $w_2$. For example, if $w_1 = ab$ and $w_2 = xy$, then

$$(ab \sqcup\!\sqcup xy) = \{abxy, axby, axyb, xaby, xayb, xyab\}.$$

  The shuffle of two languages $L_1$ and $L_2$ is

$$L_1 \sqcup\!\sqcup L_2 = \bigcup_{\substack{w_1 \in L_1 \\ w_2 \in L_2}} (w_1 \sqcup\!\sqcup w_2)\,.$$

These operations translate into generating functions which are used to estimate probabilities. Given a language $L$, let $l_{n_1,\ldots,n_m}$ be the number of words in $L$ that have $n_1$ occurrences of letter $a_1$, ..., $n_m$ occurrences of $a_m$. The *multivariate function* of $L$ is

$$l(z_1, \ldots, z_m) = \sum_{n_1,\ldots,n_m \geq 0} l_{n_1,\ldots,n_m} z_1^{n_1} z_2^{n_2} \cdots z_m^{n_m}.$$

We use the notation $[x^m y^n z^k] f(x, y, z)$ to denote the coefficient of the term $x^m y^n z^k$ in the polynomial $f(x, y, z)$.

Associate to the alphabet $\mathcal{A} = \{a_1, a_2, \ldots, a_m\}$ a weight distribution where letter $a_i$ has weight $p_i$. The weight extends multiplicatively to words so that $w = a_{j_1} a_{j_2} \ldots a_{j_n}$ has weight

$$\pi[w] = p_{j_1} p_{j_2} \cdots p_{j_n}.$$

In our case, the weight distribution is a probability distribution and $\sum_{i=1}^{m} p_i = 1$. Furthermore $\pi[w]$ is the probability of a word $w$ being in $\mathcal{A}^n$, the set of words with $n$ letters.

**Definition A.3.** *The function*

$$l(z) = l(p_1 z, p_2 z, \ldots, p_m z) = \sum_{n_1,\ldots,n_m} l_{n_1,\ldots n_m} p_1^{n_1} \cdots p_m^{n_m} z^{n_1+\ldots+n_m} = \sum_{w \in \mathcal{A}^*} \pi[w] z^{|w|}$$

*is called the* ordinary generating function *(OGF) of the language $L$ with respect to the weight distribution $\vec{p} = (p_1, \ldots, p_m)$ and is denoted by $l(z)$. The* exponential generating function *(EGF) is defined with $z^n/n!$ replacing $z^n$,*

$$\hat{l}(z) = \sum_{n_1,\ldots,n_m} l_{n_1,\ldots n_m} p_1^{n_1} \cdots p_m^{n_m} \frac{z^{n_1+\ldots+n_m}}{(n_1+\ldots+n_m)!} = \sum_{w\in\mathcal{A}^*} \pi[w] \frac{z^{|w|}}{|w|!}.$$

The value $[z^n]l(z)$ is the probability that a random word in $\mathcal{A}^n$ is in $L$.

The ordinary and exponential generating functions are related by the Laplace-Borel transform

$$l(z) = \int_0^\infty \hat{l}(zt)e^{-t}dt$$

following from the classical relation

$$\int_0^\infty t^n e^{-t} dt = n!$$

An operation on languages is unambiguous if every word of the resulting language is obtained only once. The following is Theorem 2.1 in [FGT92]. Along with the Laplace transform integral, it is the key to determining the generating function of a language defined by a combination of the four basic operations.

**Theorem A.4.** *When they operate unambiguously on their arguments, the operations of union, product, star, and shuffle product translate into generating functions:*

$$\begin{aligned}
&(a) \quad L = L_1 + L_2 \quad \Rightarrow \quad l(z) = l_1(z) + l_2(z).\\
&(b) \quad L = L_1 \cdot L_2 \quad \Rightarrow \quad l(z) = l_1(z) l_2(z).\\
&(c) \quad L = L_1^* \quad \Rightarrow \quad l(z) = (1 - l_1(z))^{-1}.\\
&(d) \quad L = L_1 \sqcup\!\sqcup L_2 \quad \Rightarrow \quad \hat{l}(z) = \hat{l}_1(z)\hat{l}_2(z).
\end{aligned}$$

# Bibliography


[Bac97] Gennady Bachman. On an optimality property of Ramanujan sums. *Proc. Amer. Math. Soc.*, 125:1001–1003, 1997.

[Bal11] R. Balasubramanian. Private communication, 2011.

[BBS11] Antal Balog, Kevin Broughan, and Igor Shparlinski. On the number of solutions of exponential congruences. *Acta Arith.*, 148(1):93–103, 2011.

[BGK06] Jean Bourgain, Alexey A. Glibichuck, and Sergei V. Konyagin. Estimates for the number of sums and products and for exponential sums in fields of prime order. *J. London Math. Soc.*, 73(2):380–398, 2006.

[BM84] Manuel Blum and Silvio Micali. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput.*, 13(4):850–864, 1984.

[BS66] Eric Bach and Jeffrey Shallit. *Algorithmic Number Theory, Vol I: Efficient Algorithms*. The MIT Press, Cambridge, 1966.

[BS08] Jean Bourgain and Igor E. Shparlinski. Distribution of consecutive modular roots of an integer. *Acta Arith.*, 134(1):83–91, 2008.

[CFK+00] R. Canetti, J.B. Friedlander, S.V. Konyagin, M. Larsen, D. Lieman, and I.E. Shparlinski. On the statistical properties of Diffie-Hellman distributions. *Israel J. Math*, 120:23–46, 2000.

[Cro69] Roger Crocker. On residues of $n^n$. *Amer. Math. Monthly*, 76(4):1028–1029, 1969.

[DT97] Michael Drmota and Robert F. Tichy. *Sequences, discrepancies and applications*. Lecture Notes in Mathematics, volume 1651. Springer, 1997.

[ER61] Paul Erdős and Alfréd Rényi. On a classical problem of probability theory. *Magyar Tudományos Akadémia Matematikai Kutató Intézetének Kőzleményei*, 6:215220, 1961.

[FGT92] Philippe Flajolet, Danièle Gardy, and Loys Thimonier. Birthday paradox, coupon collectors, caching algorithms and self-organizing search. *Discr. Appl. Math.*, 39:207–229, 1992.

[FLM10] Matthew Friedrichsen, Brian Larson, and Emily McDowell. Structure and statistics of the self-power map. *RHIT Undergrad. Math. J.*, 11(2):107–139, 2010.

[Fri07] John Friedlander. Uniform distribution, exponential sums and cryptography. In Andrew Granville and Zeév Rudnick, editors, *Equidistribution in Number Theory, An Introduction*, pages 29–57. Springer, 2007.

[FS09] Philippe Flajolet and Robert Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009.

[Gar08] M. Z. Garaev. The sum-product estimate for large subsets of prime fields. *Proc. Amer. Math. Soc.*, 136(8):2735–2739, 2008.

[GOM12] José María Grau and Antonio M. Oller-Marcén. On the last digit and the last non-zero digit of $n^n$ in base $b$. Unpublished, available at arXiv:1203.4066v1, 2012.

[Hay56] W.K. Hayman. A generalisation of stirling's formula. *J. Reine Angew. Math.*, 196:65–95, 1956.

[HM06] Joshua Holden and Pierre Moree. Some heuristics and results for small cycles of the discrete logarithm. *Mathematics of Computation*, 75(253):419–449, 2006.

[Hol02a] Joshua Holden. Addenda/corrigenda: Fixed points and two-cycles of the discrete logarithm. Unpublished, available at http://xxx.lanl.gov/abs/math.NT/0208028, 2002.

[Hol02b] Joshua Holden. Fixed points and two-cycles of the discrete logarithm. *Algorithmic number theory (ANTS 2002)*, pages 405–415, 2002.

[HR11] Joshua Holden and Margaret M. Robinson. Counting fixed points, two-cycles, and collisions of the discrete exponential function using $p$-adic methods. Unpublished, available at arxiv.org/pdf/1105.5346, 2011.

[Isa95] Richard Isaac. *The Pleasures of Probability, University Texts in Mathematics.* Springer-Verlag, 1995.

[KN06] L. Kuipers and H. Niederreiter. *Uniform Distribution of Sequences.* Dover Publications, Inc, 2006.

[Mur08] M. Ram Murty. *Problems in Analytic Number Theory, 2nd edition.* Springer-Velag, 2008.

[Mur10] M. Ram Murty. Small solutions of polynomial congruences. *Ind. J. Pure Appl. Math.*, 41(1):15–23, 2010.

[MvOV96] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montogomery. *An Introduction to the Theory of Numbers, 5th edition.* John Wiley & Sons, Inc., 1991.

[Pre98] Wiebe R. Prestman. *Mathematical Statistics.* Walter de Gruyter, 1998.

[PS72] George Pólya and Gabor Szegő. *Problems and Theorems in Analysis, Vol. I.* Springer-Verlag, 1972.

[Shp11] Igor E. Shparlinski. Exponential sums with consecutive modular roots of an integer. *Quart. J. Math.*, 62:207–213, 2011.

[Shp13] Igor E. Shparlinski. Private communication, 2013.

[Som81] Lawrence Somer. The residues of $n^n$ modulo $p$. *The Fibonacci Quarterly*, 19(2):110–117, 1981.