THE USE OF FERMAT QUOTIENTS IN CRYPTOGRAPHY

by

Titilayo Agboola

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

at

Dalhousie University
Halifax, Nova Scotia
April 2023

To all lights of the world, shine for Jesus!

Table of Contents

List of Tables

Abstract

Fermat quotients are based on Fermat's little theorem. Fermat quotients are of the form $q_p(u) \equiv \frac{u^{p-1}-1}{p} \pmod{p}$, for a prime p and an integer u with $\gcd(u, p) = 1$. They possess properties that make them suitable for generating pseudo-random numbers. They can also be used to generate Boolean functions. This thesis presents an overview of major milestones in the study of Fermat quotients and related concepts. In particular, applications of Fermat quotients in cryptography are discussed.

List of Abbreviations and Symbols Used

In what follows, and throughout this thesis, n and r are positive integers, p a prime, and q a power of p.

Notation	Description
$f(x) \ll g(x)$	$\lvert f(x)\rvert \leq Cg(x)$ for all $x \geq a$ holds for some constant $C > 0$. This is equivalent to $f(x) = O(g(x))$.
$f(x) \gg g(x)$	$\lvert f(x)\rvert \geq Cg(x)$ for all $x \geq a$ holds for some constant $C > 0$.
$f(x) = o(g(x))$	$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$
$u \equiv v \pmod{n}$	$v - u = kn$ for some integer k.
$u \not\equiv v \pmod{n}$	$v - u \neq kn$ for any integer k.
$\gcd(u, v)$	the greatest common divisor of u and v.
$\operatorname{lcm}(u, v)$	the least common multiple of u and v.
$q_p(u)$	the Fermat quotient of p with base u defined by $\frac{u^{p-1}-1}{p} \pmod{p}$.
$\mathbb{N}$	the set of natural numbers.
$\mathbb{Z}$	the ring of integers.
$(\mathbb{Z}_p, +, \cdot)$	the ring of p-adic integers with p-adic topology.
$\mathbb{Z}_p$	the additive group of the ring $(\mathbb{Z}_p, +, \cdot)$.
$\mathbb{Z}_p^*$	the multiplicative group of units in the ring $(\mathbb{Z}_p, +, \cdot)$.
$\mathbb{F}_q$	a finite field with q elements.
$B(u_1, \ldots, u_r)$	Boolean function of $r = \lfloor 2 \log_2 p \rfloor$ variables.
l_p	the smallest u for which $q_p(u) \not\equiv 0 \pmod{p}$.
$\varphi(m)$	the Euler's totient function of m.
$q(u, m)$	the Euler quotient of m with base u defined by $\frac{u^{\varphi(m)}-1}{m} \pmod{m}$.
$\lambda(m)$	the Carmichael function of m.
$C_m(u)$	the Carmichael quotient of m with base u.
w_p	the Wilson quotient defined by $\frac{(p-1)!+1}{p} \pmod{p}$.
$\left(\frac{u}{p}\right)$	the Legendre symbol of u modulo p.
$u \mid v$	u divides v; that is, $v = uk$ for some integer k.
$u \nmid v$	u does not divide v, that is, $v \neq uk$ for any integer k.

Acknowledgements

I am grateful to Jesus for life and the enablement to complete my master's thesis. I also appreciate my family for their constant love and support.

Prof. Karl Dilcher, thank you for your proficient supervision, for specifically helping me get comfortable with Latex, and for being ever ready to provide guidance. Anna, you are loved.

I recognize and appreciate the Nova Scotia Government for establishing the NSGS (Nova Scotia Graduate Scholarship). I also appreciate the array of arduous teachers and lecturers that I have passed through up to this stage in my life, thanks to each one of you.

To all the professors that have taught me so far at the department of Mathematics and Statistics, thanks to each one of you for sharing your wealth of knowledge. The non-academic staff at the department were indispensable and ever-ready to help; thank you. I also acknowledge and appreciate other graduate students.

Chapter 1

Introduction

1.1 Overview of cryptography

The information in this section has been taken from [20], [24], [27], [63].

Cryptography is almost as old as mankind. This is because human beings have always communicated and had the need to keep messages private and readable only by the intended recipients.

Cryptography is the study of techniques used to keep information secret. *Cryptanalysis* is the science of studying attacks against cryptographic schemes. Cryptanalysis seeks methods through which information, kept secret using cryptographic schemes, can be uncovered without knowing the key. Cryptography and cryptanalysis are both classified under cryptology. *Cryptology*, therefore, is the science of secret communications.

The commonly used analogy is to assume a sender, *Alice*, wants to send a message to a receiver, *Bob*. If she sends a confidential message using an insecure communication channel, such as a telephone line, an eavesdropper could easily intercept and read the message. In a worse case, an adversary, *Eve*, might be able to modify the message imperceptibly during transmission. Cryptography seeks to forestall such attacks.

A closely related concept is steganography. Steganography is another way of securing communication. While cryptography attempts to change a message to a format unintelligible to an interceptor, steganography seeks to obscure the very existence of such a message. *Steganography* is the study of methods used to keep information hidden. Steganography provides security through obscurity. Altering the least significant bit in a file is the most common way of hiding data; this file could be an audio

file, an image file, or a video file. What cryptanalysis is to cryptography, steganalysis is to steganography. *Steganalysis* is the study of methods used to detect messages hidden through steganography.

There are records of cryptography being in use as far back as 3000 years ago when Egyptians communicated with each other by sending their messages written in hieroglyphs. Some other records in the historical evolution of cryptography include:

- ca. 100 BC: The Caesar Cipher was developed.
- 1466: The first cipher disk was developed by Leon Battista Alberti.
- 1553: The Vigenère cipher was described by Giovan Battista Bellaso.
- 1854: The Playfair cipher was invented by Sir Charles Wheatstone, named after Baron Lyon Playfair, who popularised it.
- 1918: The Enigma machine was invented by Arthur Scherbius and was used in military communication.
- Both world wars: Playfair cipher, ADFGVX, the Enigma machine.
- 1948: Claude E. Shannon published an article entitled "A mathematical theory of communication" which introduced information theory.
- 1977: The Rivest-Shamir-Adleman (RSA) algorithm was publicly described.
- 1977: Data Encryption Standard (DES) was published as an official Federal Information Processing Standard (FIPS) for the United States.
- 1985: Elliptic Curve Cryptography (ECC) was described.
- 1991: Phil Zimmermann released the public key encryption program Pretty Good Privacy (PGP).
- 1994: Peter Shor described an algorithm for a theoretical quantum computer that will allow prime factorization of a composite number in polynomial time.
- 2001: DES was replaced by the Rijndael algorithm, called the Advanced Encryption Standard (AES).

1.2 Important terms in cryptography

The information in this section has been taken from [20], [24], [27], [66].

Some of the basic terms encountered in the study and practice of cryptography include:

- *Plaintext*: the message (text, numerical data, an executable program, or any kind of information) that is to be transmitted.
- *Ciphertext*: the output of an encryption process on the plaintext.
- *Cipher*: an algorithm for performing encryption or decryption.
- *Encryption*: the process that converts the plaintext into a ciphertext.
- *Decryption*: the process that converts the ciphertext back into plaintext.
- *Key*: a piece of information that can encrypt and/or decrypt a message.
- *Cryptosystem*: a system that consists of the plaintext, the ciphertext, the keys, the encryption algorithm, and the decryption algorithm.
- *One-way function*: a function f that is easy to compute on every input x, but infeasible to invert, that is, to compute x from $f(x)$.
- *One-time pad*: a system in which a randomly generated key is used only once to encrypt a message.
- *Nonce*: an arbitrary number that can be used just once in a cryptographic communication.
- *Seed*: a number (or vector) used as input to initialize a pseudo-random number generator.
- *Hash function*: a function that takes a variable length string of bits (called a *message*) as input and outputs a bit string of a fixed length (called a *hash value* or a *message digest*).

- *Exhaustive search* (also known as *Brute force attack*): a cryptographic attack that tries all the possible passwords.

1.3 Classifying cryptography

Encryption and decryption can be done either using the same key or using a pair of keys – one for encryption, the other for decryption. If the same key, or a key easily computable from it, encrypts and decrypts messages, this is called *Symmetric Cryptography*. If different keys, which are not easily computable from one another, encrypt and decrypt messages, this is called *Asymmetric Cryptography*.

Symmetric cryptography was the only kind of cryptography publicly known until 1976 when Diffie and Hellman introduced the concept of asymmetric cryptography. In symmetric encryption, the key to be used must be shared between the parties that intend to communicate. Secure key exchange is a major challenge for implementing symmetric-key encryption [24, p. 187].

Symmetric encryption can use either *block ciphers* or *stream ciphers* [27]. *Block ciphers* encrypt blocks of plaintext of fixed length. The length of the blocks of plaintext is called the *block length* [20, p. 15]. The length of the resulting blocks of ciphertext is the same as the block length. DES is an example of a block cipher.

Stream ciphers encrypt data as a stream, one bit of plaintext at a time. Most stream ciphers make use of the binary exclusive-or operator, XOR. Vernam's one-time pad is a classic example of a stream cipher [20, p. 13].

In asymmetric cryptography, two keys are used; a public key (which may be known to others) and a private key (which must not be known by anyone except the owner). The public key is used for encryption while the private key is used for decryption [27, p. 226]. Asymmetric cryptography is also known as *public-key cryptography* [27]. Asymmetric algorithms are fundamental to modern-day internet security, particularly in e-commerce. For instance, secure websites often make use of SSL/TLS (Secure Sockets Layer/Transport Layer Security) which uses public-key encryption.

More details on its implementation can be found in [24].

Asymmetric cryptography is also used in digital signatures. Digital signatures primarily help in ensuring the authenticity of messages sent; this is done by verifying the identity of the sender. For instance, they are used to protect the authenticity of electronic ID cards [10, p. 91]. The Rivest-Shamir-Adleman (RSA) algorithm, the Diffie–Hellman key exchange protocol, and ECC (Elliptic-Curve Cryptography) are a few examples of asymmetric techniques.

It is worthwhile to note that *Kerckhoffs' principle* [20, p. 4], named after Auguste Kerckhoffs, is one of the basic principles of modern cryptography. The principle holds that the adversary knows all the details of a cryptosystem, in particular, the algorithm used and its implementation. According to this principle, the security of a cryptosystem must be based entirely on the secret key.

Encryption and decryption can be achieved using a key and an algorithm (cipher). Classical ciphers can be divided into two general classes [24, p. 8]: substitution ciphers and transposition ciphers. A *substitution cipher* is a method of encrypting by which units of plaintext are replaced with the ciphertext in a defined manner, with the help of a key. Substitution ciphers are recorded as the first ciphers used in history [27, p. 5]. Substitution ciphers have variations [24, pp. 8–9]. They are described below:

A substitution cipher is called *mono-alphabetic* if a given letter of plaintext is substituted for the corresponding letter of the ciphertext, and *poly-alphabetic or multi-alphabetic* if more than one ciphertext is used to replace each plaintext. If two letters of plaintext are substituted at a time, the cipher is called *digraphic* and it is called *polygraphic* if more than two letters of plaintext are substituted at a time. A *homophonic* cipher provides multiple substitutions for some letters but not others. Some examples of substitution ciphers are: the Caesar cipher, Vigenère cipher, and Playfair cipher.

A *transposition cipher* is a method of encryption that rearranges the letters of the plaintext according to a specific rule and key. The simplest transposition cipher is the columnar transposition [24, p. 10]. It is possible to combine both substitution and transposition in a cipher. This provides *diffusion* and is implemented in modern block ciphers. The concept of diffusion in information security was explained in Shannon's 1948 paper, for instance, [27, p. 59]. Diffusion means changes to one character in the plaintext affect multiple characters in the ciphertext.

Quantum computing will render most of the current asymmetric cryptographic protocols obsolete [27, p. 385] while symmetric algorithms such as the Advanced Encryption Standard (AES) will still be usable, but may need longer keys. Designing alternative public-key cryptosystems that resist quantum computer attacks is the basis for studying post-quantum cryptography [10, p.88]. *Quantum key distribution* (more commonly known as *quantum cryptography*) enables the sender *Alice* and the receiver *Bob* to establish an unconditionally secure shared secret key. Delfs and Knebl wrote more on this in [20].

1.4 Objectives of cryptography

To realize the objectives of cryptography, there are basic building blocks called *cryptographic primitives* or *cryptographic protocols* used to solve problems involving secrecy, authentication, or data integrity [20, p. 5]. Some of them are encryption and decryption algorithms, cryptographic hash functions, and pseudo-random generators.

Attacks on the secrecy of an encryption scheme depend on the resources available to the adversary. Studying techniques to break a cipher without knowledge of the key is the work of a cryptanalyst. Some of these techniques are mentioned in [20, pp. 4–5]; they include: *Ciphertext-only attack, Known-plaintext attack*, *Chosen-plaintext attack*.

Wherever there is communication, there is a need for security. Thus, a primary application of cryptography is in ensuring secure electronic communication, including encrypting internet communications. Cryptography also finds applications in digital

signatures and disk encryption [27].

The following are some of the objectives of cryptography [20, pp. 2–3]:

- *Confidentiality*: this ensures that there is limited access to encrypted information.
- *Data integrity*: this takes care of the consistency and accuracy of information as it is transmitted from the sender to the receiver.
- *Authentication*: this verifies the origin as well as the sending and receiving parties in a communication.
- *Non-repudiation*: this makes a sender of a message unable to deny its authorship.

Chapter 2

Pseudo-randomness

Many algorithms and processes require the concept of randomness, and cryptographic systems are no exception. Randomness has to do with unpredictability, while pseudo-randomness is a simulated type of randomness that is based on an algorithm, so the process is repeatable.

The concept of randomness has different areas of applications such as in statistics, science, Monte Carlo methods, operations research, games, and computer programming. For example, random numbers are used to test the effectiveness of computer algorithms. More on random numbers can be seen in [37], [48].

2.1 Generating random numbers

Randomness is of particular importance in cryptography because the security of cryptographic operations depends on a random choice of keys and sequences [20]. Randomness is used, for instance, to generate stream ciphers. It is therefore useful to know how to generate random numbers, or at least pseudo-random numbers.

Before modern computing, throwing dice and flipping coins were common methods used to generate random data. With the advent of computers, making computers produce random data using algorithms became imperative. Generally, numbers are classified as truly random or pseudo-random [70, p. 1].

A *true random number generator* (TRNG) uses a non-deterministic source to produce randomness. True random numbers can be generated from naturally occurring (physical) phenomena like atmospheric noise or radioactive decay [27], [70]. True Random Number Generators (TRNGs) usually depend on hardware.

A *pseudo-random number generator* (PRNG) uses a deterministic algorithm to produce an apparently random sequence of length l, given a random sequence of length k, with l larger than k [52, p. 170]. In other words, PRNGs create numbers with good random properties but are predetermined based on an algorithm [27].

Cryptographically secure pseudo-random number generators (CSPRNGs) are more appropriate for cryptographic operations than general pseudo-random number generators. Two distinguishing features of a CSPRNG are *computational indistinguishability* and *unpredictability*. That is, pseudo-random numbers are said to be *cryptographically secure* if they satisfy the aforementioned features.

Unpredictability means that it should not be feasible to predict the next bit in the pseudo-random sequence from the preceding bits. Computational indistinguishability means that any subset of numbers taken from a given pseudo-random sequence should not be distinguishable from any other subset of numbers in polynomial time by an efficient algorithm. More technical details on computational indistinguishability and cryptographically secure pseudo-random number generators can be seen in [27], [44].

The Dual Elliptic Curve Deterministic Random Bit Generator [27, p. 273] is a PRNG that was promoted as a CSPRNG by the National Institute of Standards and Technology (NIST).

2.2 Pseudo-random number generators (PRNGs)

Bhattacharjee, Maity, and Das [8, pp. 2–3] gave a mathematical definition of a pseudo-random number generator as follows:

Definition 1. A *pseudo-random number generator* (PRNG) is defined as a structure $G = (\mathscr{S}, \mu, f, \mathscr{U}, g)$, where $\mathscr{S}$ is a finite set of states, μ is the probability distribution on $\mathscr{S}$ for the initial state called seed, $f : \mathscr{S} \to \mathscr{S}$ is a transition function, $\mathscr{U}$ is the output space and $g : \mathscr{S} \to \mathscr{U}$ is the output function. The generator G generates the numbers in the following way:

1. Select a seed $s_0 \in \mathscr{S}$ based on μ. The first number is $u_0 = g(s_0)$.

2. At each step $i \geq 1$, the state of the PRNG is $s_i = f(s_{i-1})$ and output is $u_i = g(s_i)$. The outputs of the PRNG are pseudo-random numbers.

A PRNG works using an algorithm and is initialized with a random seed. Since the same seed will yield the same sequence every time, it is important that the seed be properly chosen and kept hidden for security [8]. A pseudo-random number generator is so important because it is often difficult to obtain a truly random seed and it is desirable to be able to stretch random seeds to much longer sequences that appear random [52, p. 170].

2.2.1 Properties of a good PRNG

Bhattacharjee, Maity, and Das [8] put forward a number of properties a good PRNG is expected to have:

- *Uniformity*:
  This property ensures that the generated numbers are equally probable in every part of the number space. That is, for every i,
  $$e_i = \frac{N}{K},$$
  where N is the range of the numbers divided into K equal subintervals and e_i is the expected number of samples.

- *Independence*:
  This means there should not be any serial correlation between numbers generated in succession. This property ensures that any subsequence of numbers has no correlation with any other subsequences.

- *Large period*:
  The period of a PRNG is the smallest positive integer ρ such that, for every $n \geq k$, we have
  $$s_{p+n} = s_n, \text{ where } k \geq 0 \text{ is an integer.}$$

A small period makes the sequence of numbers completely predictable, so a PRNG is not considered good unless it has a large period.

- *Reproducibility*:
  Since PRNGs are deterministic algorithms, reproducibility is a prominent reason for constructing them. This is the property that ensures the same sequence of numbers is generated from the same seed. It is useful in simulations and debugging.

- *Consistency*:
  This is to ensure that the traits of the PRNG are to be independent of the seed.

- *Disjoint subsequences*:
  There should be little or no correlation between subsequences generated by different seeds.

- *Portability*:
  It is desirable that for a PRNG, the same algorithm can work on every system.

- *Efficiency*:
  Generating a random number using a PRNG should not take significant time. A PRNG should also not use much storage so as not to hinder its efficiency.

- *Coverage*:
  This means the PRNG covers the output space for any seed. That is, for any seed, every element of the output space eventually appears in the sequence.

- *Spectral characteristics*:
  The expected frequency of generation of each number should be the same.

- *Cryptographic security*:
  The requirements of an ordinary PRNG are also satisfied by a cryptographically secure PRNG, but the converse is not true. To be used in cryptographic applications, the generated numbers should be cryptographically secure.

Ideally, all the above properties are satisfied for a good PRNG but practically, most of the PRNGs do not possess all these properties. The first four properties are

particularly important in determining a good PRNG [27]. However, many PRNGs are considered good enough for usage in the applications for which they are intended.

Some examples of PRNGs [27] are the inversive generator, Linear Congruential Generator (LCG), Lagged Fibonacci Generator (LFG), and Blum-Blum-Shub. Easttom [27] wrote on improving PRNGs by shuffling the output or using a hash function. This is one of the numerous reasons for studying hash functions. Bhattacharjee, Maity, and Das [8] also wrote on the method of combining more than one LCG to improve the randomness of an LCG.

2.3 Pseudo-random sequences

Definition 2. A *pseudo-random sequence* is the output of a pseudo-random number generator [52, p. 170]. A pseudo-random sequence is a sequence that appears to be random but has been produced by a deterministic algorithm.

Pseudo-random sequences are widely used in cryptography. For example, they are used to generate the key stream which is used in some stream ciphers. The Legendre sequence (see below) is an example of a pseudo-random sequence [52].

Following Mauduit and Sárközy in their paper [45], the concept of a pseudo-random sequence can be viewed in three ways:

- pseudo-random sequences in $[0, 1)$;
- pseudo-random sequences of integers selected from $\{1, \ldots, N\}$;
- pseudo-random binary sequences.

Although these three concepts of a pseudo-random sequence are related, their differences lie in their approach to studying various concepts of pseudo-randomness. Mauduit and Sárközy [45] focused on pseudo-random binary sequences with uniform distribution in their paper. One of the applications of pseudo-random binary sequences is in generating the key stream in the Vernam cipher, see [33].

2.3.1 Pseudo-random binary sequences

The information from this subsection has been taken from [34], [49], [60], [66], [68].

Definition 3. Let $(e_n), n \geq 0$, be a *bit sequence* (that is, a sequence over $\{0,1\}$). (e_n) is said to be *t-periodic* if $e_{n+t} = e_t$ for any integer $n \geq 0$.

Definition 4. A sequence (e_n) is called a *linear recurrence sequence* of order k over $\{0,1\}$ if it satisfies the relation

$$e_{n+k} \equiv a_{k-1} \cdot e_{n+k-1} + a_{k-2} \cdot e_{n+k-2} + \cdots + a_0 \cdot e_n \pmod 2, \quad n = 0, 1, \ldots \tag{2.1}$$

for some $a_0, a_1, \ldots, a_{k-1}$ in $\{0,1\}$, $a_0 \neq 0$.

Definition 5. Take $\mathbb{F}_2 = \{0,1\}$ to be the finite field of order 2. The polynomial $c(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0 \in \mathbb{F}_2[x]$ corresponding to the linear recursion (2.1) is the *characteristic polynomial* of the sequence (e_n). We can assume $c(x)$ is *monic* (that is, its leading coefficient is 1).

Definition 6. The characteristic polynomial of (e_n) with minimal degree is called the *minimal polynomial* of (e_n) and is denoted by $c_{\min}(x)$.

The minimal polynomial of a t-periodic sequence (e_n) is given by

$$\frac{x^t - 1}{\gcd(x^t - 1, ((e_n), t)(x))} \tag{2.2}$$

where $((e_n), t)(x) \equiv e_0 + e_1 x + \cdots + e_{t-1}x^{t-1} \pmod 2$.

Definition 7. Let N be a positive integer. The *Nth linear complexity*, $L_N((e_n))$, of the sequence (e_n) is the smallest k such that the first N terms of e_n can be generated by a linear recurrence relation over $\{0,1\}$ of order k.

$$L_N((e_n)) = \begin{cases} 0 & \text{if the first } N \text{ elements of } (e_n) \text{ are all zero,} \\ N & \text{if the first } N-1 \text{ elements of } (e_n) \text{ are zero, and } e_N \neq 0. \end{cases}$$

Definition 8. Let $L_N((e_n))$ denote again the Nth linear complexity. Then the non-decreasing sequence of non-negative integers $L_1((e_n)), L_2((e_n)), \ldots$ is called the *linear complexity profile* of (e_n).

Definition 9. The *linear complexity* of the sequence (e_n) is the value

$$L((e_n)) = \sup_{N \geq 1} L_N((e_n)).$$

The linear complexity of a linear recurring sequence corresponds to the degree of its minimal polynomial, that is, the least order among all linear recursions for (e_n). For a t-periodic sequence $(e_n) = (e_0 e_1 \cdots e_{t-1} \cdots)$,

$$L((e_n)) = L((e_n), 2t) \leq t.$$

Thus the linear complexity of a periodic sequence is finite. The linear complexity of a t-periodic sequence (e_n) can also be calculated thus:

$$t - deg(\gcd(x^t - 1, ((e_n), t)(x)))$$

where $((e_n), t)(x) \equiv e_0 + e_1 x + \cdots + e_{t-1} x^{t-1} \pmod 2$.

The linear complexity of a sequence is a measure of its unpredictability. Sequences with low linear complexity should be avoided for cryptographic applications, and sequences with high linear complexity should be used with care. For instance, a pseudo-random number generator can become easily predictable in polynomial time if sufficiently many bits of its consecutive terms are known.

Examples:

1. $e_{n+3} \equiv e_{n+2} + e_n \pmod 2$, with initial values $(e_0 e_1 e_2) = (101)$.
   So the sequence is $(e_n) = (1010011 \ldots)$, and it is 7-periodic.
   We also have

$$\begin{aligned} ((e_n), t)(x)) &\equiv 1 + 0 \cdot x + 1 \cdot x^2 + 0 \cdot x^3 + 0 \cdot x^4 + 1 \cdot x^5 + 1 \cdot x^6 \\ &\equiv x^6 + x^5 + x^2 + 1 \pmod 2. \end{aligned}$$

   The corresponding characteristic polynomial, $c(x)$, is $x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.
   The minimal polynomial of this sequence is

$$c_{\min}(x) = \frac{x^7 - 1}{\gcd(x^7 - 1, x^6 + x^5 + x^2 + 1)} = \frac{x^7 - 1}{x^4 + x^2 + x + 1} = x^3 + x + 1 \in \mathbb{F}_2[x].$$

   Since the minimal polynomial of (e_n) has degree 3, it follows that the linear complexity of (e_n), $L((e_n))$, is 3.

2. $e_{n+4} \equiv e_{n+3} + e_{n+2} + e_n \pmod 2$, with initial values $(e_0e_1e_2e_3) = (1011)$.
   So the sequence $(e_n) = (1011100\ldots)$, and it is 7-periodic.
   We also have

$$\begin{aligned}((e_n), t)(x)) &\equiv 1 + 0 \cdot x + 1 \cdot x^2 + 1 \cdot x^3 + 1 \cdot x^4 + 0 \cdot x^5 + 0 \cdot x^6 \\ &\equiv x^4 + x^3 + x^2 + 1 \pmod 2.\end{aligned}$$

   The corresponding characteristic polynomial, $c(x)$, is $x^4 + x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.
   The minimal polynomial of this sequence is

$$c_{\min}(x) = \frac{x^7 - 1}{\gcd(x^7 - 1, x^4 + x^3 + x^2 + 1)} = \frac{x^7 - 1}{x^4 + x^3 + x^2 + 1} = x^3 + x^2 + 1 \in \mathbb{F}_2[x].$$

   Since the minimal polynomial of (e_n) has degree 3, it follows that the linear complexity of (e_n), $L((e_n))$, is 3.

2.3.2 Measures of pseudo-randomness of binary sequences

In addition to the linear complexity and the linear complexity profile, Mauduit and Sárközy [45], [46] described certain measures of pseudo-randomness of binary sequences $(e_N) \in \{-1, 1\}^N$. Chen, Ostafe, and Winterhof [15] gave corresponding definitions of some of these measures for a finite binary sequence $(e_n)_{n=1}^N = (e_1, \ldots, e_N)$ from $\{0, 1\}^N$. These measures include:

- *Correlation measure*

  The correlation measure of order k of the sequence $(e_n)_{n=1}^N$ from $\{-1, 1\}^N$ is defined by

$$C_k((e_n)_{n=1}^N) = \max_{M,D} \left| \sum_{a=1}^{M} e_{a+d_1} \ldots e_{a+d_k} \right|$$

  where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and $M > 0$ such that $0 \le d_1 < \ldots < d_k \le N - M$.
  For ease of notation,

$$\text{denote } \left| \sum_{a=1}^{M} e_{a+d_1} \ldots e_{a+d_k} \right| \text{ as } C_{\{-1,1\}}(M, D).$$

  The correlation measure of order k of the sequence $(e_n)_{n=1}^N$ from $\{0, 1\}^N$ is defined by

$$C_k((e_n)_{n=1}^N) = \max_{M,D} \left| \sum_{a=1}^{M} (-1)^{e_{a+d_1} \cdots e_{a+d_k}} \right|$$

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and $M > 0$ such that $0 \leq d_1 < \ldots < d_k \leq N - M$.

For ease of notation,

$$\text{denote } \left|\sum_{a=1}^{M}(-1)^{e_{a+d_1}\cdots e_{a+d_k}}\right| \text{ as } C_{\{0,1\}}(M, D).$$

- *Well-distribution measure*

  The well-distribution measure of the sequence $(e_n)_{n=1}^N$ from $\{-1, 1\}^N$ is defined by

  $$W((e_n)_{n=1}^N) = \max_{a,b,t}\left|\sum_{j=0}^{t-1} e_{a+bj}\right|,$$

  where the maximum is taken over all $a, b, t \in \mathbb{N}$ such that $1 \leq a + b \leq a + (t - 1)b \leq N$.

  For ease of notation,

  $$\text{denote } \left|\sum_{j=0}^{t-1}(-1)^{e_{a+bj}}\right| \text{ as } W_{\{-1,1\}}(a, b, t).$$

  The well-distribution measure of the sequence $(e_n)_{n=1}^N$ from $\{0, 1\}^N$ is defined by

  $$W((e_n)_{n=1}^N) = \max_{a,b,t}\left|\sum_{j=0}^{t-1}(-1)^{e_{a+bj}}\right|,$$

  where the maximum is taken over all $a, b, t \in \mathbb{N}$ such that $1 \leq a + b \leq a + (t - 1)b \leq N$.

  For ease of notation,

  $$\text{denote } \left|\sum_{j=0}^{t-1}(-1)^{e_{a+bj}}\right| \text{ as } W_{\{0,1\}}(a, b, t).$$

  Observe that the well-distribution is taken relative to arithmetic progressions: we can think of a as the first term, b as the common difference, and t as the number of terms in the progression.

Examples:

1. Denote the sequence $(e_n)_{n=1}^{6} = (010011)$ as S_1. From Table 2.1 and Table 2.2, we find that $C_2(S_1) = 4$ and $W(S_1) = 2$.

2. Denote the sequence $(e_n)_{n=1}^{6} = (011100)$ as S_2. From Table 2.1 and Table 2.2, we find that $C_2(S_2) = 3$ and $W(S_2) = 3$.

The computations for the correlation measure of order 2 and the well-distribution measure of the sequences S_1 and S_2 are shown in Table 2.1 and Table 2.2 respectively. Note that the cell entries correspond to $C_{\{0,1\}}(M, D)$ and $W_{\{0,1\}}(a, b, t)$ respectively.

		M				
$D = (d_1, d_2)$	Sequence	1	2	3	4	5
$(0,1)$	S_1	1	2	3	4	3
$(0,1)$	S_2	1	0	1	0	1
$(0,2)$	S_1	1	2	3	4	
$(0,2)$	S_2	1	0	1	2	
$(0,3)$	S_1	1	0	1		
$(0,3)$	S_2	1	2	3		
$(0,4)$	S_1	1	0			
$(0,4)$	S_2	1	2			
$(0,5)$	S_1	1				
$(0,5)$	S_2	1				
$(1,2)$	S_1	1	2	3	2	
$(1,2)$	S_2	1	2	1	0	
$(1,3)$	S_1	1	2			
$(1,3)$	S_2	1	0			
$(1,4)$	S_1	1	0			
$(1,4)$	S_2	1	2			
$(1,5)$	S_1	1				
$(1,5)$	S_2	1				
$(2,3)$	S_1	1	2	1		
$(2,3)$	S_2	1	0	1		
$(2,4)$	S_1	1	2			
$(2,4)$	S_2	1	2			
$(2,5)$	S_1	1				
$(2,5)$	S_2	1				
$(3,4)$	S_1	1	0			
$(3,4)$	S_2	1	2			
$(3,5)$	S_1	1				
$(3,5)$	S_2	1				
$(4,5)$	S_1	1				
$(4,5)$	S_2	1				

Table 2.1: Computing the correlation measure of sequences S_1 and S_2.

		t					
(a,b)	Sequence	1	2	3	4	5	6
$(1,1)$	S_1	1	0	1	2	1	0
$(1,1)$	S_2	1	0	1	2	1	0
$(1,2)$	S_1	1	2	1			
$(1,2)$	S_2	1	0	1			
$(1,3)$	S_1	1	2				
$(1,3)$	S_2	1	0				
$(1,4)$	S_1	1	0				
$(1,4)$	S_2	1	2				
$(1,5)$	S_1	1	0				
$(1,5)$	S_2	1	2				
$(2,1)$	S_1	1	0	1	0	1	
$(2,1)$	S_2	1	2	3	2	1	
$(2,2)$	S_1	1	0	1			
$(2,2)$	S_2	1	2	1			
$(2,3)$	S_1	1	2				
$(2,3)$	S_2	1	0				
$(2,4)$	S_1	1	2				
$(2,4)$	S_2	1	0				
$(3,1)$	S_1	1	2	1	0		
$(3,1)$	S_2	1	2	1	0		
$(3,2)$	S_1	1	0				
$(3,2)$	S_2	1	0				
$(3,3)$	S_1	1	0				
$(3,3)$	S_2	1	0				
$(4,1)$	S_1	1	0	1			
$(4,1)$	S_2	1	0	1			
$(4,2)$	S_1	1	0				
$(4,2)$	S_2	1	0				
$(5,1)$	S_1	1	2				
$(5,1)$	S_2	1	2				
$(6,1)$	S_1	1					
$(6,1)$	S_2	1					

Table 2.2: Computing the well-distribution measure of sequences S_1 and S_2.

2.3.3 The Legendre sequence: an example of a pseudo-random binary sequence

Definition 10. An integer u co-prime with p is a *quadratic residue* modulo p if it is congruent to a perfect square modulo p; that is, if there exists an integer x such that

$$x^2 \equiv u \pmod{p}.$$

Otherwise u is called a *quadratic non-residue* modulo p [7, p. 178].

Definition 11. Let p be an odd prime. The *Legendre symbol* of an integer u modulo p [7, p. 179] is defined as follows:

$$\left(\frac{u}{p}\right) = \begin{cases} 1 & \text{if } u \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } u \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } u \equiv 0 \pmod{p}. \end{cases}$$

Definition 12. For an odd prime p, the *Legendre sequence* (ℓ_n) [6, p. 370] is defined by

$$(\ell_n) = \begin{cases} 1, & \text{if } \left(\frac{n}{p}\right) = -1, \\ 0, & \text{otherwise,} \end{cases} \qquad n \geq 0,$$

where $\left(\frac{n}{p}\right)$ is the Legendre symbol of the integer n modulo p.

The linear complexity of the Legendre sequence is:

$$L((\ell_n)) = \begin{cases} (p-1)/2, & p \equiv 1 \pmod{8}, \\ p, & p \equiv 3 \pmod{8}, \\ p-1, & p \equiv 5 \pmod{8}, \\ (p+1)/2, & p \equiv 7 \pmod{8}. \end{cases}$$

Examples:

1. For $p = 5$, the Legendre symbols are:

$$\left(\left(\frac{1}{5}\right), \left(\frac{2}{5}\right), \left(\frac{3}{5}\right), \left(\frac{4}{5}\right), \left(\frac{5}{5}\right), \left(\frac{6}{5}\right), \left(\frac{7}{5}\right), \left(\frac{8}{5}\right), \ldots\right),$$

   and the corresponding Legendre sequence is: (0, 1, 1, 0, 0, 0, 1, 1 ...).
   Since $p \equiv 5 \pmod{8}$, its linear complexity, $L((\ell_n)) = 4$.

2. For $p = 7$, the Legendre symbols are:

$$\left(\left(\frac{1}{7}\right), \left(\frac{2}{7}\right), \left(\frac{3}{7}\right), \left(\frac{4}{7}\right), \left(\frac{5}{7}\right), \left(\frac{6}{7}\right), \left(\frac{7}{7}\right), \left(\frac{8}{7}\right), \left(\frac{9}{7}\right), \left(\frac{10}{7}\right), \ldots\right),$$

and the corresponding Legendre sequence is: (0, 0, 1, 0, 1, 1, 0, 0, 0, 1, ...). Since $p \equiv 7 \pmod 8$, its linear complexity $L((\ell_n)) = 4$.

The Legendre sequence has period p. It has a high linear complexity, a small well-distribution measure, and a small correlation measure. These properties make it very suitable for cryptographic use when p is sufficiently large.

In 1988, Damgård [19] considered the possibility of constructing a CSPRNG using a sequence of Legendre symbols modulo a prime. Gyarmati, Mauduit, and Sárközy [19], [32] looked at Legendre symbols in the context of pseudo-random binary sequences. Particularly, Mauduit and Sárközy [45] investigated the pseudo-randomness of the Legendre sequence by showing it has some desirable properties.

In particular, Mauduit and Sárközy [45] showed that for the sequence $(e_n) = (e_1, \ldots, e_n)$ where $n = p - 1, e_i = \left(\frac{i}{p}\right)$, there exist positive numbers c_1 and c_2 such that

$$C_k((e_n)) < c_1 p^{1/2} \log_2 p$$

and

$$W((e_n)) < c_2 p^{1/2} \log_2 p.$$

For more on the Legendre sequence, see [17], [66], [67].

Examples:

1. For $p = 5, \quad n = p - 1 = 4$,

$$(e_4) = \left(\left(\frac{1}{5}\right), \left(\frac{2}{5}\right), \left(\frac{3}{5}\right), \left(\frac{4}{5}\right)\right) = (1, -1, -1, 1).$$

Denote this sequence by E_1. Then the computations in Table 2.3 and Table 2.4 show that

$$C_2(E_1) = 2 \text{ and } W(E_1) = 2.$$

2. For $p = 7, \quad n = p - 1 = 6$,

$$(e_6) = \left(\left(\frac{1}{7}\right), \left(\frac{2}{7}\right), \left(\frac{3}{7}\right), \left(\frac{4}{7}\right), \left(\frac{5}{7}\right), \left(\frac{6}{7}\right)\right) = (1, 1, -1, 1, -1, -1).$$

Denote this sequence by E_2. Then (see again Table 2.3 and Table 2.4) we have

$$C_2(E_2) = 3 \text{ and } W(E_2) = 2.$$

The computations for the correlation measure of order 2 and the well-distribution measure of the sequences E_1 and E_2 are shown in Table 2.3 and Table 2.4 respectively. Note that the cell entries correspond to $C_{\{-1,1\}}(M, D)$ and $W_{\{-1,1\}}(a, b, t)$ respectively.

		M				
$D = (d_1, d_2)$	Sequence	1	2	3	4	5
$(0, 1)$	E_1	1	0	1		
$(0, 1)$	E_2	1	0	1	2	3
$(0, 2)$	E_1	1	2			
$(0, 2)$	E_2	1	0	1	0	
$(0, 3)$	E_1	1				
$(0, 3)$	E_2	1	0	1		
$(0, 4)$	E_2	1	2			
$(0, 5)$	E_2	1				
$(1, 2)$	E_1	1	0			
$(1, 2)$	E_2	1	2	3	2	
$(1, 3)$	E_1	1				
$(1, 3)$	E_2	1	2			
$(1, 4)$	E_2	1	2			
$(1, 5)$	E_2	1				
$(2, 3)$	E_1	1				
$(2, 3)$	E_2	1	2	1		
$(2, 4)$	E_2	1	0			
$(2, 5)$	E_2	1				
$(3, 4)$	E_2	1	0			
$(3, 5)$	E_2	1				
$(4, 5)$	E_2	1				

Table 2.3: Computing the correlation measure of Legendre sequences E_1 and E_2.

		t					
(a,b)	Sequence	1	2	3	4	5	6
$(1,1)$	E_1	1	0	1	0		
$(1,1)$	E_2	1	2	1	2	1	0
$(1,2)$	E_1	1	0				
$(1,2)$	E_2	1	0	1			
$(1,3)$	E_1	1	2				
$(1,3)$	E_2	1	2				
$(1,4)$	E_1	1					
$(1,4)$	E_2	1	0				
$(1,5)$	E_1	1					
$(1,5)$	E_2	1	0				
$(2,1)$	E_1	1	2	1			
$(2,1)$	E_2	1	0	1	0	1	
$(2,2)$	E_1	1	0				
$(2,2)$	E_2	1	2	1			
$(2,3)$	E_1	1					
$(2,3)$	E_2	1	0				
$(2,4)$	E_1	1					
$(2,4)$	E_2	1	0				
$(3,1)$	E_1	1	0				
$(3,1)$	E_2	1	0	1	2		
$(3,2)$	E_1	1					
$(3,2)$	E_2	1	2				
$(3,3)$	E_1	1					
$(3,3)$	E_2	1	2				
$(4,1)$	E_1	1					
$(4,1)$	E_2	1	0	1			
$(4,2)$	E_1	1					
$(4,2)$	E_2	1	0				
$(5,1)$	E_2	1	2				
$(6,1)$	E_2	1					

Table 2.4: Computing the well-distribution measure of Legendre sequences E_1 and E_2.

Chapter 3

Fermat quotients

3.1 Definition and basics of Fermat quotients

The Fermat quotient is based on Fermat's little theorem [7, p. 113]:

Theorem 1. *If p is a prime and u an integer with* $\gcd(u,p) = 1$*, then* $u^{p-1} \equiv 1 \pmod{p}$.

This theorem is named after Pierre de Fermat. By Fermat's little theorem, $u^{p-1}-1$ is divisible by p, and the quotient obtained is called the *Fermat quotient* of p with base u [2, p. 30]. Equivalently, this quotient can also be called the *Fermat quotient* of u with respect to p [53].

Definition 13. For a prime p and an integer u with $\gcd(u,p) = 1$, the unique integer that satisfies

$$q_p(u) \equiv \frac{u^{p-1}-1}{p} \pmod{p}, \;\; 0 \leq q_p(u) \leq p-1,$$

is called the *Fermat quotient* of p with base u; and we set $q_p(kp) = 0$, $k \in \mathbb{Z}$. Note also that $q_p(0)$ is taken to be 0.

The Fermat quotient with base 2 is of particular interest. It was used by Wieferich in his theorem concerning the first case of Fermat's last theorem [2]:

Theorem 2. *(Wieferich) If p is an odd prime, and x, y, z are integers, not divisible by p, satisfying the equation $x^p + y^p + z^p = 0$, then*

$$q_p(2) \equiv 0 \pmod{p}.$$

By the definition of the Fermat quotient, we have

$$q_p(2) \equiv \frac{2^{p-1}-1}{p} \pmod{p}.$$

Thus, $q_p(2) \equiv 0 \pmod{p}$ is equivalent to $2^{p-1} \equiv 1 \pmod{p^2}$. (As we will later see, Fermat quotients are p^2-periodic).

Definition 14. Odd primes that satisfy the congruence

$$q_p(2) \equiv 0 \pmod{p}$$

are called *Wieferich primes*.

Wieferich primes occur very rarely; in fact, only two of such primes are presently known: 1093, discovered by Meissner (1913), and 3511, discovered by Beeger (1922) [2]. More on Wieferich primes can be read in [23], and the latest published search results can be found in [25].

3.2 Properties of Fermat quotients

The following properties of Fermat quotients were discovered by Eisenstein [1, p. 159], [31, p. 1049], [64, pp. 167–168]:

Proposition 1. *For an odd prime p and any integers u and v with $gcd(uv, p) = 1$,*

(a) $q_p(1) \equiv 0 \pmod{p}$.

(b) $q_p(-u) \equiv q_p(u) \pmod{p}$.
This means Fermat quotients behave like an "even function".

(c) $q_p(uv) = q_p(u) + q_p(v) \pmod{p}$.
This is called the "logarithmic property" [35]. This property implies there exists a group homomorphism $q_p : \mathbb{Z}_{p^2}^* \to \mathbb{Z}_p$ [16], [64].

(d) $q_p(u + pv) \equiv q_p(u) - v \cdot \frac{1}{u} \pmod{p}$.

(e) $2q_p(2) \equiv 1 - \frac{1}{2} + \cdots - \frac{1}{(p-1)/2} \pmod{p}$.
Equivalently,

$$2q_p(2) \equiv \sum_{r=1}^{p-1} \frac{(-1)^{r-1}}{r} \equiv -\sum_{r=1}^{\frac{p-1}{2}} \frac{1}{r} \pmod{p}.$$

Proof. (a) Using the definition of the Fermat quotient,

$$\begin{aligned} q_p(1) &\equiv \frac{1^{p-1}-1}{p} \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

(b) By the definition of the Fermat quotient,

$$\begin{aligned} q_p(-u) &\equiv \frac{(-u)^{p-1}-1}{p} \pmod{p} \\ &\equiv \frac{(-1)^{p-1}u^{p-1}-1}{p} \pmod{p} \\ &\equiv \frac{1\cdot u^{p-1}-1}{p} \pmod{p} \\ &\equiv \frac{u^{p-1}-1}{p} \pmod{p} \\ &\equiv q_p(u). \end{aligned}$$

(c) By the definition of the Fermat quotient,

$$\begin{aligned} q_p(uv) &\equiv \frac{(uv)^{p-1}-1}{p} \pmod{p} \\ &\equiv \frac{(uv)^{p-1}-v^{p-1}+v^{p-1}-1}{p} \pmod{p} \\ &\equiv \frac{(uv)^{p-1}-v^{p-1}}{p} + \frac{v^{p-1}-1}{p} \pmod{p} \\ &\equiv \frac{u^{p-1}-1}{p}\cdot v^{p-1} + \frac{v^{p-1}-1}{p} \pmod{p} \\ &\equiv q_p(u)v^{p-1} + q_p(v) \pmod{p}. \end{aligned}$$

The result follows using Fermat's little theorem.

(d) Using the definition of the Fermat quotient and then the binomial theorem,

$$\begin{aligned}
q_p(u+pv) &\equiv \frac{(u+pv)^{p-1}-1}{p} \pmod p \\
&\equiv \frac{u^{p-1}+(p-1)(pv)(u)^{p-2}+\cdots+(pv)^{p-1}-1}{p} \pmod p \\
&\equiv \frac{u^{p-1}-1}{p} - \frac{v}{u}\Big((1-p)(u^{p-1}) - \cdots - up^{p-2}v^{p-2}\Big) \pmod p \\
&\equiv \frac{u^{p-1}-1}{p} - v\cdot\frac{1}{u} \pmod p \text{ (using Fermat's little theorem)} \\
&\equiv q_p(u) - v\cdot\frac{1}{u} \pmod p.
\end{aligned}$$

(e) Observe that $\frac{1}{p}\binom{p}{r} \equiv \frac{(-1)^{r-1}}{r} \pmod p$, $1 \le r \le p-1$:

By expanding the binomial coefficient:

$$\begin{aligned}
\frac{1}{p}\binom{p}{r} &= \frac{p(p-1)\cdots(p-r+1)}{r!} \pmod p \\
&\equiv \frac{(-1)(-2)\cdots(-(r-1))}{1\cdot 2\cdot(r-1)\cdot r} \pmod p \\
&\equiv \frac{(-1)^r}{r} \pmod p.
\end{aligned}$$

$$\text{Thus, } -\sum_{r=1}^{\frac{p-1}{2}}\frac{1}{r} \pmod p \equiv \sum_{r=1}^{p-1}\frac{(-1)^{r-1}}{r} \pmod p \equiv \sum_{r=1}^{p-1}\frac{1}{p}\binom{p}{r} \pmod p$$

$$\begin{aligned}
&\equiv \frac{1}{p}\left(\sum_{r=0}^{p}\binom{p}{r} - \binom{p}{0} - \binom{p}{p}\right) \pmod p \\
&\equiv \frac{1}{p}(2^p - 1 - 1) \pmod p \\
&\equiv \frac{2^p-2}{p} \pmod p \\
&\equiv 2\frac{2^{p-1}-1}{p} \pmod p \equiv 2q_p(2).
\end{aligned}$$

This completes the proof. □

Corollary 1. *For an odd prime p and any integers $r \ge 0$, and u with $gcd(u,p) = 1$,*

$$q_p(u^r) \equiv rq_p(u) \pmod p.$$

Proof. Note that this result is a direct consequence of "the logarithmic property" of Fermat quotients. We can also prove it directly from the definition of the Fermat quotient as follows;

$$\begin{aligned}
q_p(u^r) &\equiv \frac{(u^r)^{p-1}-1}{p} \pmod p \\
&\equiv \frac{(u^{p-1})^r-1}{p} \pmod p \\
&\equiv \frac{(u^{p-1}-1)(1+u^{p-1}+\cdots(u^{p-1})^{r-1})}{p} \pmod p \\
&\equiv \frac{(u^{p-1}-1)(1+1+\cdots+1)}{p} \pmod p \text{ (using Fermat's little theorem)} \\
&\equiv \frac{(u^{p-1}-1)\cdot r}{p} \pmod p \\
&\equiv r q_p(u) \pmod p.
\end{aligned}$$

□

Corollary 2. *For an odd prime p and an integer u with $gcd(u,p)=1$,*

$$q_p(u+p^2) \equiv q_p(u) \pmod p.$$

Proof. Take $v=p$ in Proposition 1(d) so that

$$q_p(u+p^2) \equiv q_p(u) - p\cdot\frac{1}{u} \pmod p \equiv q_p(u) \pmod p.$$

Therefore the Fermat quotient is p^2-periodic. □

3.2.1 Dynamic properties of Fermat quotients

The information in this section has been taken from [50].

Ostafe and Shparlinski [50] investigated the dynamical system generated by Fermat quotients. They studied the sequence

$$u_n = q_p(u_{n-1}),\ n=1,2,\ldots$$

for an initial value $u_0 \in \{0,1,\ldots,p-1\}$, where p is a sufficiently large prime that is fixed.

The authors obtained the following results:

- Fixed points of Fermat quotients:
  Let $F(p)$ be the number of fixed points of the map $u \mapsto q_p(u)$. Then we have

$$F(p) \ll p^{\frac{11}{12}+o(1)}, \text{ as } p \to \infty.$$

- Concentration of values:
  Let $U(p;k,h)$ be the number of $u \in \{0,1,\ldots,p-1\}$ for which there exists some $z \in [k+1, k+h]$ such that $q_p(u) \equiv z \pmod p$. Then for any integers k and $h \geq 1$,

$$U(p;k,h) \leq h^{0.5}p^{0.5+o(1)}, \text{ as } p \to \infty.$$

- Image size: Let $M(p)$ be the image size of $q_p(u)$ for $\{0,1,\ldots,p-1\}$. Then

$$M(p) \geq (1+o(1))\frac{p}{(\log_2 p)^2}, \text{ as } p \to \infty.$$

Example: Fix $p = 101, k = 9, h = 11$, we find from Table 3.1 that $U(101;9,11) = 14$. Table 3.1 shows the computation to obtain the concentration of u for $q_p(u)$ in the range $[10,20]$.

$z \in [10,20]$	$u \vert q_p(u) \equiv z \pmod p$	**card**$\{u \vert q_p(u) \equiv z \pmod p\}$
10	50	1
11	93	1
12	none	0
13	92	1
14	70	1
15	34,69,76	3
16	none	0
17	57	1
18	62,67,98	3
19	25,87,90	3
20	none	0
		$U(101;9,11) = 14$

Table 3.1: Concentration of u for $q_p(u)$ in the range $[10,20]$; $p = 101$.

A list of fixed points can be found in Table 3.2, and image sizes for the first 72 odd primes are listed in Table 3.3.

Prime	Fixed points	Prime	Fixed points	Prime	Fixed points
3	none	101	none	229	218
5	none	103	none	233	225
7	$2, 4$	107	86	239	53
11	none	109	none	241	126
13	none	113	none	251	123
17	6	127	none	257	109, 185
19	none	131	none	263	103
23	none	137	none	269	20
29	none	139	$20, 52, 80, 84$	271	187, 197
31	none	149	none	277	none
37	none	151	$38, 67, 121$	281	none
41	none	157	none	283	none
43	none	163	40	293	100
47	$21, 32$	167	142	307	none
53	6	173	106,170	311	189, 246
59	none	179	103, 173	313	232
61	57	181	none	317	41, 150
67	$7, 39, 50$	191	84	331	none
71	$2, 4, 25$	193	40	337	none
73	none	197	6	347	none
79	26	199	none	349	99
83	60	211	none	353	183, 206, 319, 324
89	$28, 48$	223	168	359	289
97	none	227	84, 145	367	268

Table 3.2: Fixed points of the map u $\mapsto q_p(u)$ for $3 \leq p \leq 370$.

Prime	Image size	Prime	Image size	Prime	Image size
3	2	101	62	229	146
5	3	103	71	233	147
7	5	107	70	239	147
11	7	109	67	241	146
13	9	113	70	251	166
17	12	127	89	257	167
19	14	131	82	263	157
23	13	137	86	269	168
29	19	139	89	271	174
31	21	149	100	277	186
37	25	151	98	281	177
41	26	157	98	283	184
43	29	163	107	293	192
47	31	167	110	307	203
53	38	173	112	311	182
59	42	179	110	313	207
61	38	181	117	317	214
67	39	191	121	331	206
71	44	193	122	337	218
73	50	197	132	347	230
79	51	199	126	349	228
83	58	211	139	353	204
89	54	223	168	359	226
97	61	227	147	367	231

Table 3.3: Image size of $q_p(u)$ for $3 \leq p \leq 370$.

3.2.2 Divisibility of Fermat quotients

The divisibility condition of $q_p(u)$ by p has been studied by various authors. The smallest u for which $q_p(u) \not\equiv 0 \pmod{p}$ is commonly denoted by l_p. Studying the divisibility of Fermat quotients is related to other number-theoretic problems, especially to the first case of Fermat's last theorem (see Theorem 10 in section 5.3).

Lenstra [42] showed that

$$l_p \leq \begin{cases} 4(\log_2 p)^2, & \text{if } p \geq 3, \\ (4e^{-2} + o(1))(\log_2 p)^2, & \text{if } p \to \infty. \end{cases}$$

Bourgain, Ford, Konyagin, and Shparlinski [9] improved Lenstra's bound:

$$l_p \leq (\log_2 p)^{\frac{463}{252}+o(1)}.$$

Shteinikov [62] further improved this bound: For each $\varepsilon > 0$, there exists a $\delta > 0$ such that for sufficiently large Q, the inequality

$$l_p \leq (\log_2 p)^{\frac{3}{2}+\varepsilon}$$

holds for all primes $p < Q$, with the exception of $O(Q^{1-\delta})$ primes.

3.2.3 Pseudo-randomness of Fermat quotients

Ostafe and Shparlinski [50] also wrote on the pseudo-randomness of Fermat quotients by studying the distribution of the points

$$\left(\frac{q_p(u+d_0)}{p}, \ldots, \frac{q_p(u+d_{s-1})}{p}\right), \quad u = 1, \ldots, N,$$

for $D = (d_0, \ldots, d_{s-1})$ with $0 \leq d_0 < d_{s-1} < p^2$.

The authors obtained the following results:

- Linear complexity of a sequence of Fermat quotients:
  For a sufficiently long sequence of Fermat quotients:

  For $p^2 > N \geq 1$, the linear complexity $L_p(N)$ of the sequence $q_p(u), u = 0, \ldots, N-1$, satisfies

$$L_p(N) \geq \frac{1}{2}\min\{p-1, N-p-1\}.$$

For arbitrary segments of a sequence of Fermat quotients:

For M and $p^2 > N \geq 1$, the linear complexity $L_p(N)$ of the sequence $q_p(u), u = M+1, \ldots, M+N$, satisfies

$$L_p(M,N) \geq \min\left\{\frac{p-1}{2}, \frac{N-p-1}{3}\right\}.$$

- Joint distribution:

  For integers $M, N \geq 1, s \geq 1$ and an integer vector $\mathbf{b} = (b_0, \ldots, b_{s-1})$, consider the exponential sums

$$S_{s,p}(M,N;\mathbf{b}) = \sum_{u=M+1}^{M+N} e\left(\frac{\sum_{j=0}^{s-1} b_j q_p(u+j)}{p}\right).$$

  Then for any integer $s \geq 1$,

$$\max_{\gcd(b_0,\ldots,b_{s-1},p)=1} |S_{s,p}(M,N;\mathbf{b})| \ll sp\log_2 p$$

  uniformly over M and $p^2 > N \geq 1$.

3.3 Character sums and exponential sums

3.3.1 Character sums of Fermat quotients

To better grasp the concept of character sums, it is helpful to review the following definitions [7]:

Definition 15. A *character* of an arbitrary group G is a complex-valued function f defined on G with the multiplicative property:

$$f(uv) = f(u)f(v)$$

for all $u, v \in G$, and if $f(w) \neq 0$ for some $w \in G$.

Definition 16. Let G be the group of reduced residue classes modulo k. A *Dirichlet character* modulo k is an arithmetical function χ corresponding to each character f of G, defined as follows:

$$\chi(n) = \begin{cases} f(\hat{n}), & \text{if } \gcd(n,k) = 1, \\ 0, & \text{if } \gcd(n,k) > 1. \end{cases}$$

where the residue class $\hat{n}$ is the set of all integers congruent to n modulo k.

A character χ_1 is *principal* if

$$\chi_1(n) = \begin{cases} 1, & \text{if } \gcd(n,k) = 1, \\ 0, & \text{if } \gcd(n,k) > 1. \end{cases}$$

Definition 17. The Dirichlet L-functions,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where χ is a Dirichlet character and $s > 1$, $s = \sigma + it$, $\sigma, t \in \mathbb{R}$.

Basic properties of Dirichlet characters modulo k

1. $\chi(uv) = \chi(u)\chi(v)$ for all $u, v \in G$.
   This means χ is completely multiplicative.

2. $\chi(u+k) = \chi(u)$ for all $u \in G$.
   That is, χ is periodic with period k.

3. The group of reduced residue classes modulo k, G, is a finite abelian group of order $\varphi(k)$.

4. Let $\chi_1, \chi_2, \ldots, \chi_{\varphi(k)}$ denote the $\varphi(k)$ Dirichlet characters modulo k. Let u and v be two integers, with $\gcd(k,v) = 1$. Then we have

$$\sum_{r=1}^{\varphi(k)} \chi_r(u)\bar{\chi}_r(v) = \begin{cases} \varphi(k), & \text{if } u \equiv v \pmod{k}, \\ 0, & \text{if } u \not\equiv v \pmod{k}. \end{cases}$$

Trivially, $\varphi(k)$ is a sum bound for non-principal Dirichlet characters. Different authors have worked on non-trivial sum bounds for non-principal Dirichlet characters. For instance, Shparlinski [61] proved a non-trivial bound for a non-principal Dirichlet character χ modulo p:

For every fixed integer $v \geq 1$, for any integers H and $N \geq 1$:

$$\sum_{u=H+1}^{H+N} \chi(q_p(ku)) \leq N^{1-\frac{1}{v}} p^{\frac{5v+1}{4v^2+o(1)}},\ 1 \leq N \leq p^2,$$

as $p \to \infty$, uniformly over all integers k with $\gcd(k,p) = 1$.

Gomez and Winterhof [30] extended Shparlinski's result:

$$\sum_{u=0}^{N-1} \chi(q_p(au+b)) \ll N^{1-\frac{1}{v}} p^{\frac{5v+1}{4v^2}} (\log_2 p)^{\frac{1}{v}},\ 1 \le N \le p^2,$$

for any integers a, b with $\gcd(a, p^2) \neq p^2$.

Also, the authors obtained the following result for a set of non-principal Dirichlet characters $\chi_1, \ldots, \chi_l$ modulo p:

$$\sum_{u=0}^{N-1} \chi_1(q_p(u+d_1)) \cdots \chi_l(q_p(u+d_l)) \ll \max\left\{ \frac{lN}{p^{\frac{1}{3}}}, lp^{\frac{3}{2}\log_2 p} \right\}$$

for any integers $0 \le d_1 < d_2 < \cdots < d_l \le p^2 - 1$ and $1 \le N \le p^2$.

3.3.2 Exponential sums of Fermat quotients

Let p be a prime, and set $e(x) = e^{2\pi i x}$.

Definition 18. *Heilbronn's exponential sum* [35] is defined by

$$S(a) = \sum_{u=1}^{p} e\Big(\frac{au^p}{p^2}\Big),$$

for any integer a with $\gcd(a, p) = 1$.

Heath-Brown [35] showed that $S(a) = o(p)$ as $p \to \infty$ but he was also able to deduce the following result:

If p is a prime and $\gcd(a, p) = 1$ *then*

$$\sum_{\substack{M < u \le M+N \\ \gcd(u,p)=1}} e\Big(\frac{au^p}{p^2}\Big) \ll p^{\frac{11}{12}} \log p,$$

uniformly in a, for all M, and for all $N \le p$.

By studying exponential sums involving u^{p-1} instead of u^p, the author showed that $q_p(u)$ is uniformly distributed modulo p^2 for all $N \le p$. The result is presented in the following theorem:

Theorem 3. *For any integer a with* $\gcd(a, p) = 1$,

$$\sum_{\substack{M < u \le M+N \\ \gcd(u,p)=1}} e\Big(\frac{aq_p(u)}{p}\Big) \ll N^{\frac{1}{2}} p^{\frac{3}{8}},$$

uniformly for $M, N \geq 1$. *In particular,*

$$\sum_{n=1}^{p-1} e\Big(\frac{aq_p(u)}{p}\Big) \ll p^{\frac{7}{8}},$$

uniformly for $\gcd(a, p) = 1$.

For the proof, we require an estimate from the following theorem by Burgess [12, p. 525]:

Theorem 4. *If* χ *is a non-principal character modulo* k, *and if* $L(s, \chi)$ *denotes the* L*-function corresponding to* χ, *where* $s = \sigma + it$, σ *and* t *are fixed real numbers satisfying* $0 < \sigma < 1$, *then for any fixed* $\varepsilon > 0$,

$$|L(s,\chi)| \ll \begin{cases} k^{\frac{4-5\sigma+\varepsilon}{8}}, & \text{for } 0 < \sigma \leq \frac{1}{2}, \\ k^{\frac{3-3\sigma+\varepsilon}{8}}, & \text{for } \frac{1}{2} \leq \sigma < 1, \end{cases} \tag{3.1}$$

and in particular,

$$\left| L\left(\frac{1}{2} + it, \chi\right)\right| \ll k^{\frac{3}{16}+\varepsilon}.$$

Proof of Theorem 3. From Proposition 1, $q_p(uv) = q_p(u)+q_p(v) \pmod p$, with $\gcd(uv, p) = 1$. Thus,

$$\chi(u) = \begin{cases} e\Big(\frac{aq_p(u)}{p}\Big), & \gcd(u, p) = 1, \\ 0, & \gcd(u, p) > 1, \end{cases}$$

is a non-principal character modulo p^2, of order p. Thus the sum above can be written as $\sum_{M<u\leq M+N} \chi(u)$, and the proof is concluded by using Burgess's estimate, taking k to be p^2. □

Character and exponential sums help in describing the pseudo-randomness of sequences derived from Fermat quotients [15].

3.4 Fermat quotient over function fields

Sauerberg and Shu [53] examined the generalization of Fermat quotients to the field of rational functions over a finite field.

3.4.1 Fermat quotient for the field of rational functions over a finite field

Let P be an irreducible polynomial of degree d in $\mathbb{F}_q[x]$, where q is a power of a prime p, and let U be any polynomial in $\mathbb{F}_q[x]$. Sauerberg and Shu [53] defined the Fermat quotient for the field of rational functions over a finite field as follows:

Definition 19. The function Q_P on $\mathbb{F}_q[x]$ defined by

$$Q_P(U) = \frac{U^{q^d} - U}{P} = \frac{U^{q^{deg(P)}} - U}{P}$$

is called the *Fermat quotient for the field of rational functions over a finite field*.

Examples:

1. Let $P = x^3 + x^2 + 2x + 1$, $U = x^2 + x + 1$, $P, Q \in \mathbb{F}_3[x]$; $q = 3, d = 3$. Then

$$\begin{aligned}
Q_{[x^3+x^2+2x+1]}(x^2+x+1) &= \frac{(x^2+x+1)^{3^3} - (x^2+x+1)}{x^3+x^2+2x+1} \\
&\equiv \frac{x^{54} + x^{27} + 1 - (x^2+x+1)}{x^3+x^2+2x+1} \in \mathbb{F}_3[x] \\
&\equiv \frac{x^{54} + x^{27} + 2x^2 + 2x}{x^3+x^2+2x+1} \in \mathbb{F}_3[x] \\
&\equiv x^{51} + 2x^{50} + 2x^{49} + 2x^{48} + x^{47} + 2x^{46} + x^{44} + x^{42} \\
&+ x^{41} + 2x^{38} + x^{37} + x^{36} + x^{35} + 2x^{34} + x^{33} + 2x^{31} \\
&+ 2x^{29} + 2x^{28} + x^{25} + x^{23} + x^{22} + 2x^{19} + x^{18} + x^{17} \\
&+ x^{16} + 2x^{15} + x^{14} + 2x^{12} + 2x^{10} + 2x^9 + x^6 + 2x^5 \\
&+ 2x^4 + 2x^3 + x^2 + 2x \in \mathbb{F}_3[x].
\end{aligned}$$

2. Let $P = x^2 + x + 1$, $U = x^2 + 1$, $P, Q \in \mathbb{F}_4[x]$ so that $q = 4, d = 2$. Then

$$\begin{aligned}
Q_{[x^2+x+1]}(x^2+1) &= \frac{(x^2+1)^{4^2} - (x^2+1)}{x^2+x+1} \\
&\equiv \frac{x^{32} + 2x^{16} + 1 - (x^2+1)}{x^2+x+1} \in \mathbb{F}_4[x] \\
&\equiv \frac{x^{32} + 2x^{16} + 3x^2}{x^2+x+1} \in \mathbb{F}_4[x] \\
&\equiv x^{30} + 3x^{29} + x^{27} + 3x^{26} + x^{24} + 3x^{23} + x^{21} + 3x^{20} \\
&+ x^{18} + 3x^{17} + x^{15} + x^{14} + 2x^{13} + x^{12} + x^{11} + 2x^{10} \\
&+ x^9 + x^8 + 2x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + 2x \in \mathbb{F}_4[x].
\end{aligned}$$

3. Let $P = x^2 + 2$, $U = 4x^3$, $P, Q \in \mathbb{F}_5[x]$ so that $q = 5, d = 2$. Then

$$\begin{aligned}
Q_{[x^2+2]}(4x^3) &= \frac{(4x^3)^{5^2} - 4x^3}{x^2+2} \\
&\equiv \frac{4x^{75} + x^3}{x^2+2} \in \mathbb{F}_5[x] \\
&\equiv 4x^{73} + 2x^{71} + x^{69} + 3x^{67} + 4x^{65} + 2x^{63} + x^{61} + 3x^{59} \\
&+ 4x^{57} + 2x^{55} + x^{53} + 3x^{51} + 4x^{49} + 2x^{47} + x^{45} + 3x^{43} \\
&+ 4x^{41} + 2x^{39} + x^{37} + 3x^{35} + 4x^{33} + 2x^{31} + x^{29} + 3x^{27} \\
&+ 4x^{25} + 2x^{23} + x^{21} + 3x^{19} + 4x^{17} + 2x^{15} + x^{13} + 3x^{11} \\
&+ 4x^9 + 2x^7 + x^5 + 3x^3 \in \mathbb{F}_5[x].
\end{aligned}$$

4. Let $P = x^2 + 2$, $U = 2x^3$, $P, Q \in \mathbb{F}_5[x]$ so that $q = 5, d = 2$. Then

$$\begin{aligned}
Q_{[x^2+2]}(2x^3) &= \frac{(2x^3)^{5^2} - 2x^3}{x^2+2} \\
&\equiv \frac{2x^{75} + 3x^3}{x^2+2} \in \mathbb{F}_5[x] \\
&\equiv 2x^{73} + x^{71} + 3x^{69} + 4x^{67} + 2x^{65} + x^{63} + 3x^{61} + 4x^{59} \\
&+ 2x^{57} + x^{55} + 3x^{53} + 4x^{51} + 2x^{49} + x^{47} + 3x^{45} + 4x^{43} \\
&+ 2x^{41} + x^{39} + 3x^{37} + 4x^{35} + 2x^{33} + x^{31} + 3x^{29} + 4x^{27} \\
&+ 2x^{25} + x^{23} + 3x^{21} + 4x^{19} + 2x^{17} + x^{15} + 3x^{13} + 4x^{11} \\
&+ 2x^9 + x^7 + 3x^5 + 4x^3 \in \mathbb{F}_5[x].
\end{aligned}$$

From examples 3 and 4 above,

$$Q_{[x^2+2]}(4x^3) = 2 \cdot Q_{[x^2+2]}(2x^3).$$

This seems to indicate that Fermat quotients for the field of rational functions over a finite field are closed under scalar multiplication (shown below). Some of the properties satisfied by Fermat quotients for the field of rational functions over a finite field include:

Proposition 2. *For all polynomials U and V in $\mathbb{F}_q[x]$ and constant c in $\mathbb{F}_q$, the following hold:*

(a) $Q_P(U+V) = Q_P(U) + Q_P(V)$.
This means Fermat quotients for the field of rational functions over a finite field satisfy the additive property [53].

(b) $Q_P(cU) = cQ_P(U)$.
This means Fermat quotients for the field of rational functions over a finite field are closed under scalar multiplication.

(c) $Q_P(UV) = PQ_P(U)Q_P(V) + VQ_P(U) + UQ_P(V)$.

(d) $Q_P(UV) = VQ_P(U) + \sigma(U)Q_P(V)$, *for* $\sigma(U) = U^{q^{deg(P)}}$.

(e) $Q_P(U+VP) \equiv Q_P(U) - V \pmod{P^{q^d-1}}$.

Proof of Proposition 2. (a) By the definition of Fermat quotient for rational function field,

$$\begin{aligned} Q_P(U+V) &= \frac{(U+V)^{q^d} - (U+V)}{P} \\ &= \frac{U^{q^d} + V^{q^d} - U - V}{P} \text{ using the Frobenius endomorphism} \\ &= \frac{U^{q^d} - U}{P} + \frac{V^{q^d} - V}{P} \\ &= Q_P(U) + Q_P(V). \end{aligned}$$

(b) From the definition of Fermat quotient for rational function field,

$$\begin{aligned} Q_P(cU) &= \frac{(cU)^{q^d} - (cU)}{P} \\ &= c \cdot \frac{U^{q^d} - U}{P} \\ &= cQ_P(U). \end{aligned}$$

(c) Using the definition of Fermat quotient for rational function field,

$$\begin{aligned} PQ_P(U)Q_P(V) &= P \cdot \frac{U^{q^d} - U}{P} \cdot \frac{V^{q^d} - V}{P} \\ &= \frac{U^{q^d}V^{q^d} - U^{q^d}V - UV^{q^d} + UV}{P}; \\ VQ_P(U) &= V \cdot \frac{U^{q^d} - U}{P}; \\ UQ_P(V) &= U \cdot \frac{V^{q^d} - V}{P}. \end{aligned}$$

Therefore,

$$\begin{aligned} PQ_P(U)Q_P(V) + VQ_P(U) &= \frac{U^{q^d}V^{q^d} - U^{q^d}V - UV^{q^d} + UV}{P} + V \cdot \frac{U^{q^d} - U}{P} \\ &= \frac{U^{q^d}V^{q^d} - UV^{q^d}}{P}. \end{aligned}$$

Adding the last piece, $UQ_P(V)$, we have

$$\begin{aligned} PQ_P(U)Q_P(V) + VQ_P(U) + UQ_P(V) &= \frac{U^{q^d}V^{q^d} - UV^{q^d}}{P} + U \cdot \frac{V^{q^d} - V}{P} \\ &= \frac{U^{q^d}V^{q^d} - UV^{q^d} + UV^{q^d} - UV}{P} \\ &= \frac{U^{q^d}V^{q^d} - UV}{P} \\ &= Q_P(UV). \end{aligned}$$

(d) Using the definition of Fermat quotient for rational function field,

$$\begin{aligned} Q_P(UV) &= \frac{(UV)^{q^d} - (UV)}{P} \\ &= \frac{UV^{q^d} + U^{q^d}V^{q^d} - UV - U^{q^d}V}{P} \text{ using the Frobenius endomorphism} \\ \\ &= \frac{U^{q^d}V^{q^d} - UV}{P} + \frac{U^{q^d}V^{q^d} - U^{q^d}V}{P} \\ &= V \cdot \frac{U^{q^d} - U}{P} + U^{q^d} \cdot \frac{V^{q^d} - V}{P} \\ &= VQ_P(U) + \sigma(U)Q_P(V) \quad \text{where } \sigma(U) = U^{q^d}. \end{aligned}$$

(e) By the definition of Fermat quotient for rational function field,

$$\begin{aligned} Q_P(U+VP) &= \frac{(U+VP)^{q^d} - (U+VP)}{P} \\ &= \frac{U^{q^d} + (VP)^{q^d} - U - VP}{P} \text{ using the Frobenius endomorphism} \\ &= \frac{U^{q^d} - U}{P} + \frac{(VP)^{q^d} - VP}{P} \\ &= \frac{U^{q^d} - U}{P} + V^{q^d} P^{q^d - 1} - V \\ &= Q_P(U) - V \pmod{P^{q^d-1}}. \end{aligned}$$

□

The following theorem presented by Sauerberg and Shu [53] is a precursor to some results about Fermat quotients over rational function fields.

Theorem 5. *Let P be an irreducible polynomial of degree d, let $U = \sum_{i=0}^{m} u_i x^i$ be a polynomial in $\mathbb{F}_q[x]$ of degree $m < d$, and let $\varepsilon = \varepsilon(U) = ord_p(\gcd\{i | u_i \neq 0\})$. Then P^{p^ε} divides $U^{q^d} - U$ in $\mathbb{F}_q[x]$ and*

$$\frac{U^{q^d} - U}{P^{p^\varepsilon}} \equiv V^{p^\varepsilon} \left(\sum_{p^\varepsilon | i} u_i \binom{i}{p^\varepsilon} x^{i - p^\varepsilon} \right) \pmod{P^{p^\varepsilon}},$$

or equivalently,

$$U^{q^d} - U \equiv (VP)^{p^\varepsilon} \left(\sum_{p^\varepsilon | i} u_i \binom{i}{p^\varepsilon} x^{i - p^\varepsilon} \right) \pmod{P^{p^\varepsilon}},$$

where $VP = x^{q^d} - x$, $ord_p(m)$ is the largest power of p dividing m. Further, the polynomial on the right-hand side of the first equivalence is relatively prime to P. In particular, p^ε is the exact power of P dividing $U^{q^d} - U$.

The results are presented in the corollary below:

Corollary 3. *Let P be an irreducible polynomial.*

(a) There are infinitely many pairs U, P in $\mathbb{F}_q[x]$ with P irreducible and $1 \leq deg(U) \leq deg(P)$ such that $Q_P(U) \equiv 0 \pmod{P}$.

(b) There are no irreducible polynomials U with $deg(U) < deg(P)$ and $Q_P(U) \equiv 0 \pmod{P}$.

(c) For a given $U \in \mathbb{F}_q[x]$ and $r \geq 1$, $Q_P(U)$ is divisible by P^r for infinitely many irreducible polynomials P if and only if U is a p^{∂_r}-th power in $\mathbb{F}_q[x]$ for $p^{\partial_r - 1} \leq r < p^{\partial_r}$.

Chapter 4

Applying Fermat quotients in cryptography

4.1 Constructing pseudo-random binary sequences

As earlier noted, pseudo-random sequences are produced from pseudo-random number generators. Fermat quotients can function as pseudo-random number generators because of their pseudo-random properties (see Section 3.2).

For instance, Heath-Brown [35] showed that the Fermat quotients are asymptotically uniformly distributed for $M, N \geq 1$ (see Theorem 3 in Section 3.3). This satisfies the need for uniformity which a good pseudo-random number generator is expected to have.

From Fermat quotients, pseudo-random sequences can be obtained. In particular, Chen, Ostafe, and Winterhof [15] considered the following *binary (threshold) sequence* derived from Fermat quotients modulo p defined by

$$(e_{p^2}) = \begin{cases} 0, & \text{if } 0 \leq \frac{q_p(u)}{p} < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leq \frac{q_p(u)}{p} < 1, \end{cases} \quad 1 \leq u \leq p^2. \tag{4.1}$$

Denote the sequence $(\frac{q_p(u)}{p})_{1 \leq u \leq p^2}$ by (Q_{p^2}).

Examples:

1. For $p = 3$, $p^2 = 9$:

$$\begin{aligned}(Q_9) &= \left(\frac{q_3(1)}{3}, \frac{q_3(2)}{3}, \frac{q_3(3)}{3}, \frac{q_3(4)}{3}, \frac{q_3(5)}{3}, \frac{q_3(6)}{3}, \frac{q_3(7)}{3}, \frac{q_3(8)}{3}, \frac{q_3(9)}{3}\right) \\ &= \left(\frac{0}{3}, \frac{1}{3}, \frac{0}{3}, \frac{2}{3}, \frac{2}{3}, \frac{0}{3}, \frac{1}{3}, \frac{0}{3}, \frac{0}{3}\right).\end{aligned}$$

Therefore, by (4.1),

$$(e_9) = (0, 0, 0, 1, 1, 0, 0, 0, 0)\,.$$

2. For $p = 5$, $p^2 = 25$:

$$(Q_{25}) = \left(\frac{q_5(1)}{5}, \frac{q_5(2)}{5}, \frac{q_5(3)}{5}, \frac{q_5(4)}{5}, \frac{q_5(5)}{5}, \frac{q_5(6)}{5}, \frac{q_5(7)}{3}, \frac{q_5(8)}{5}, \frac{q_5(9)}{5}, \frac{q_5(10)}{5}, \right.$$
$$\frac{q_5(11)}{5}, \frac{q_5(12)}{5}, \frac{q_5(13)}{5}, \frac{q_5(14)}{5}, \frac{q_5(15)}{5}, \frac{q_5(16)}{5}, \frac{q_5(17)}{5}, \frac{q_5(18)}{5}, \frac{q_5(19)}{5},$$
$$\left. \frac{q_5(20)}{5}, \frac{q_5(21)}{5}, \frac{q_5(22)}{5}, \frac{q_5(23)}{5}, \frac{q_5(24)}{5}, \frac{q_5(25)}{5} \right)$$
$$= \left(\frac{0}{5}, \frac{3}{5}, \frac{1}{5}, \frac{1}{5}, \frac{0}{5}, \frac{4}{5}, \frac{0}{5}, \frac{4}{5}, \frac{2}{5}, \frac{0}{5}, \frac{3}{5}, \frac{2}{5}, \frac{2}{5}, \frac{3}{5}, \frac{0}{5}, \frac{2}{5}, \frac{4}{5}, \frac{0}{5}, \frac{4}{5}, \frac{0}{5}, \frac{1}{5}, \frac{1}{5}, \frac{3}{5}, \frac{0}{5}, \frac{0}{5} \right).$$

Again, by (4.1),

$$(e_{25}) = (0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0).$$

Another binary sequence derived from Fermat quotients is the *Legendre-Fermat quotient sequence* [16] defined by

$$(f_u) = \begin{cases} 0, & \text{if } \left(\frac{q_p(u)}{p}\right) = 1 \quad \text{or} \quad q_p(u) = 0, \\ 1, & \text{otherwise,} \end{cases} \qquad u \geq 0; \tag{4.2}$$

where $\left(\frac{\div}{p}\right)$ is the Legendre symbol. The *Legendre-Fermat quotient sequence* is derived from a combination of the Legendre symbol and Fermat quotients.
Denote the sequence $\left(\left(\frac{q_p(u)}{p}\right)\right)_{u \geq 0}$ by (Q_p).

Note: The Legendre-Fermat quotient sequence is the case $m = 2$ of the *m-ary sequence, h_u, of discrete logarithms* modulo a divisor $m \geq 2$ of $p-1$ of Fermat quotients modulo p defined in [16], [30].

Examples:

1. For $p = 3$:

$$(Q_3) = \left(\left(\frac{q_3(1)}{3}\right), \left(\frac{q_3(2)}{3}\right), \left(\frac{q_3(3)}{3}\right), \left(\frac{q_3(4)}{3}\right), \left(\frac{q_3(5)}{3}\right), \left(\frac{q_3(6)}{3}\right), \left(\frac{q_5(7)}{3}\right), \right.$$
$$\left. \left(\frac{q_3(8)}{3}\right), \left(\frac{q_3(9)}{3}\right), \cdots \right)$$
$$= \left(\left(\frac{0}{3}\right), \left(\frac{1}{3}\right), \left(\frac{0}{3}\right), \left(\frac{2}{3}\right), \left(\frac{2}{3}\right), \left(\frac{0}{3}\right), \left(\frac{1}{3}\right), \left(\frac{0}{3}\right), \left(\frac{0}{3}\right), \cdots \right)$$
$$= (0, 1, 0, -1, -1, 0, 1, 0, 0, \ldots).$$

Therefore, by (4.2),

$$(f_u) = (0, 0, 0, 1, 1, 0, 0, 0, 0, \ldots)\,.$$

2. For $p = 5$:

$$\begin{aligned}(Q_5) =& \left(\left(\frac{q_5(1)}{5}\right), \left(\frac{q_5(2)}{5}\right), \left(\frac{q_5(3)}{5}\right), \left(\frac{q_5(4)}{5}\right), \left(\frac{q_5(5)}{5}\right), \left(\frac{q_5(6)}{5}\right), \right. \\ & \left(\frac{q_5(7)}{5}\right), \left(\frac{q_5(8)}{5}\right), \left(\frac{q_5(9)}{5}\right), \left(\frac{q_5(10)}{5}\right), \left(\frac{q_5(11)}{5}\right), \left(\frac{q_5(12)}{5}\right), \\ & \left(\frac{q_5(13)}{5}\right), \left(\frac{q_5(14)}{5}\right), \left(\frac{q_5(15)}{5}\right), \left(\frac{q_5(16)}{5}\right), \left(\frac{q_5(17)}{5}\right), \left(\frac{q_5(18)}{5}\right), \\ & \left(\frac{q_5(19)}{5}\right), \left(\frac{q_5(20)}{5}\right), \left(\frac{q_5(21)}{5}\right), \left(\frac{q_5(22)}{5}\right), \left(\frac{q_5(23)}{5}\right), \left(\frac{q_5(24)}{5}\right), \\ & \left.\left(\frac{q_5(25)}{5}\right), \cdots \right) \\ =& \left(\left(\frac{0}{5}\right), \left(\frac{3}{5}\right), \left(\frac{1}{5}\right), \left(\frac{1}{5}\right), \left(\frac{0}{5}\right), \left(\frac{4}{5}\right), \left(\frac{0}{5}\right), \left(\frac{4}{5}\right), \left(\frac{2}{5}\right), \left(\frac{0}{5}\right), \right. \\ & \left(\frac{3}{5}\right), \left(\frac{2}{5}\right), \left(\frac{2}{5}\right), \left(\frac{3}{5}\right), \left(\frac{0}{5}\right), \left(\frac{2}{5}\right), \left(\frac{4}{5}\right), \left(\frac{0}{5}\right), \left(\frac{4}{5}\right), \left(\frac{0}{5}\right), \left(\frac{1}{5}\right), \\ & \left.\left(\frac{1}{5}\right), \left(\frac{3}{5}\right), \left(\frac{0}{5}\right), \left(\frac{0}{5}\right), \cdots \right) \\ =& (0, -1, 1, 1, 0, 1, 0, 1, -1, 0, -1, -1, -1, -1, 0, -1, 1, 0, 1, 0, 1, 1, -1, 0, 0, \\ & \ldots).\end{aligned}$$

Therefore, by (4.2),

$$(f_u) = (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, \ldots).$$

Note that both the binary threshold and the Legendre-Fermat sequences are p^2-periodic.

4.1.1 Pseudo-randomness of binary sequences derived from Fermat quotients

Chen, Ostafe, and Winterhof [15] obtained the following results on the binary threshold sequence:

- A bound on the well-distribution measure:

$$W((e_{p^2})) \ll p(\log_2 p)^2.$$

- A bound on the correlation measure of order 2:
  For the binary threshold sequence (e_{p^2}), and $D = (d_1, d_2)$ with $0 \leq d_1 < d_2 < p^2$,

$$C_2((e_{p^2})) \ll p(\log_2 p)^3.$$

- A bound on the linear complexity profile:

$$L((e_{p^2}, N) \gg \frac{\log_2 \frac{N}{p}}{\log_2 \log_2 p} \text{ for } 2 \leq N \leq p^2.$$

Chen [16] obtained the following result on the linear complexities of the binary threshold sequence and the Legendre-Fermat sequence:

- If $2^{p-1} \not\equiv 1 \pmod{p^2}$ (that is, $p \neq 1093, 3511$), then the linear complexities of (e_{p^2}) and (f_u) both satisfy

$$L((e_{p^2})) = L((f_u)) = \begin{cases} p^2 - p, & \text{if } p \equiv 1 \pmod 4, \\ p^2 - 1, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Examples: Note that for $p = 3, 5,\ 2^{p-1} \not\equiv 1 \pmod{p^2}$ so

1. For $p = 3, L((e_9)) = L((f_u)) = 8$ since $3 \equiv 3 \pmod 4$.

2. For $p = 5, L((e_{25})) = L((f_u)) = 20$ since $5 \equiv 1 \pmod 4$.

4.2 Boolean functions derived from Fermat quotients

A Boolean function [69, p. 2] in n variables is a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ where $\mathbb{F}_2^n$ is the n-dimensional vector space and $\mathbb{F}_2$ is the binary field. A Boolean variable can assume one of two values, 0 (FALSE) or 1 (TRUE) [69]. Boolean functions are essential in cryptography [69]. For instance, they are used in the design of stream ciphers, digital signature schemes, and public-key cryptosystems.

4.2.1 Boolean functions and the Legendre symbol

Using the Legendre symbol, Aly and Winterhof [5] studied Boolean functions derived from Fermat quotients modulo p. They put forward the following definition for the Boolean function $B(U_1, \ldots, U_r)$ of $r = \lfloor 2 \log_2 p \rfloor$ variables:

$$B(u_1, \ldots, u_r) = \begin{cases} 0, & \text{if } \left(\frac{q_p(x)}{p}\right) = 1, \\ 1, & \text{if } \left(\frac{q_p(x)}{p}\right) \neq 1, \end{cases} \tag{4.3}$$

for any $0 \leq x \leq 2^r - 1$, where $(u_1, \ldots, u_r)$ is the binary representation of x, and $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol. Following [5], we use capital letters for variables and small letters for integers and their binary representations.

4.2.2 Some of the parameters for the Boolean function $B(u_1, \ldots, u_r)$

- *Hamming weight*:
  The Hamming weight $\|a\|$ of a vector $a \in \mathscr{B}_r$ is the number of its nonzero components, where $\mathscr{B}_r = \{0, 1\}^r$.

- *Fourier coefficients (or Walsh-Hadamard coefficients)*:

  $$\hat{B}(a) = \sum_{u \in \mathscr{B}_r} (-1)^{B(u_1, \ldots, u_r) + \langle a, u \rangle}$$

  where $a = (a_1, \ldots, a_r)$, $\langle a, u \rangle = a_1 u_1 + a_2 u_2 + \cdots + a_r u_r$ denotes the standard inner product.
  As a bound for the maximum Fourier coefficients, we have that:

  $$\max_{a \in \mathscr{B}_r} |\hat{B}(a)| \ll p^{\frac{15}{8}} \log_2^{\frac{1}{4}} p.$$

  Example:
  For the Boolean function $B(u_1, u_2, u_3, u_4)$ (see Table 4.2),

  $$\max_{a \in \mathscr{B}_4} |\hat{B}(a)| = 8.$$

- *Nonlinearity*:

  $$N(B) = 2^{r-1} - \frac{1}{2} \max_{a \in \mathscr{B}_r} |\hat{B}(a)|.$$

Example:

For the Boolean function $B(u_1, u_2, u_3, u_4)$ (see Table 4.2),

$$N(B) = 2^{4-1} - \frac{1}{2} \cdot 8 = 4.$$

x	(u_1, u_2, u_3, u_4)	$q_p(x)$	$\left(\frac{q_p(x)}{p}\right)$	$B(u_1, u_2, u_3, u_4)$
0	$(0,0,0,0)$	$q_5(0) \equiv 0$	$\left(\frac{0}{5}\right) = 0$	$B(0,0,0,0) = 1$
1	$(0,0,0,1)$	$q_5(1) \equiv \frac{1^4-1}{5} \pmod 5 \equiv 0$	$\left(\frac{0}{5}\right) = 0$	$B(0,0,0,1) = 1$
2	$(0,0,1,0)$	$q_5(2) \equiv \frac{2^4-1}{5} \pmod 5 \equiv 3$	$\left(\frac{3}{5}\right) = -1$	$B(0,0,1,0) = 1$
3	$(0,0,1,1)$	$q_5(3) \equiv \frac{3^4-1}{5} \pmod 5 \equiv 1$	$\left(\frac{1}{5}\right) = 1$	$B(0,0,1,1) = 0$
4	$(0,1,0,0)$	$q_5(4) \equiv \frac{4^4-1}{5} \pmod 5 \equiv 1$	$\left(\frac{1}{5}\right) = 1$	$B(0,1,0,0) = 0$
5	$(0,1,0,1)$	$q_5(5) \equiv \frac{5^4-1}{5} \pmod 5 \equiv 0$	$\left(\frac{0}{5}\right) = 0$	$B(0,1,0,1) = 1$
6	$(0,1,1,0)$	$q_5(6) \equiv \frac{6^4-1}{5} \pmod 5 \equiv 4$	$\left(\frac{4}{5}\right) = 1$	$B(0,1,1,0) = 0$
7	$(0,1,1,1)$	$q_5(7) \equiv \frac{7^4-1}{5} \pmod 5 \equiv 0$	$\left(\frac{0}{5}\right) = 0$	$B(0,1,1,1) = 1$
8	$(1,0,0,0)$	$q_5(8) = \frac{8^4-1}{5} \pmod 5 \equiv 4$	$\left(\frac{4}{5}\right) = 1$	$B(1,0,0,0) = 0$
9	$(1,0,0,1)$	$q_5(9) \equiv \frac{9^4-1}{5} \pmod 5 \equiv 2$	$\left(\frac{2}{5}\right) = -1$	$B(1,0,0,1) = 1$
10	$(1,0,1,0)$	$q_5(10) \equiv \frac{10^4-1}{5} \pmod 5 \equiv 0$	$\left(\frac{0}{5}\right) = 0$	$B(1,0,1,0) = 1$
11	$(1,0,1,1)$	$q_5(11) \equiv \frac{11^4-1}{5} \pmod 5 \equiv 3$	$\left(\frac{3}{5}\right) = -1$	$B(1,0,1,1) = 1$
12	$(1,1,0,0)$	$q_5(12) \equiv \frac{12^4-1}{5} \pmod 5 \equiv 2$	$\left(\frac{2}{5}\right) = -1$	$B(1,0,0,0) = 1$
13	$(1,1,0,1)$	$q_5(13) \equiv \frac{13^4-1}{5} \pmod 5 \equiv 2$	$\left(\frac{2}{5}\right) = -1$	$B(1,1,0,1) = 1$
14	$(1,1,1,0)$	$q_5(14) \equiv \frac{14^4-1}{5} \pmod 5 \equiv 3$	$\left(\frac{3}{5}\right) = -1$	$B(1,1,1,0) = 1$
15	$(1,1,1,1)$	$q_5(15) \equiv \frac{15^4-1}{5} \pmod 5 \equiv 0$	$\left(\frac{0}{5}\right) = 0$	$B(1,1,1,1) = 1$

Table 4.1: Boolean function of 4 variables, $B(u_1, \ldots, u_r)$, derived from Fermat quotients.

One can also define a Boolean function as follows [60]:

$$B(u_1, \ldots, u_r) = \begin{cases} 1, & \text{if } 2x+1 \text{ is square-free,} \\ 0, & \text{if } 2x+1 \text{ is not square-free,} \end{cases}$$

where $0 \leq x \leq 2^r - 1$, and $(u_1, \ldots, u_r)$ is the binary representation of x.

x	u_1	u_2	u_3	u_4	$\|u\|$	$\hat{B}(u)$
0	0	0	0	0	0	-8
1	0	0	0	1	1	4
2	0	0	1	0	1	0
3	0	0	1	1	2	4
4	0	1	0	0	1	0
5	0	1	0	1	2	-4
6	0	1	1	0	2	0
7	0	1	1	1	3	2
8	1	0	0	0	1	4
9	1	0	0	1	2	0
10	1	0	1	0	2	-2
11	1	0	1	1	3	0
12	1	1	0	0	2	-4
13	1	1	0	1	3	-8
14	1	1	1	0	3	-4
15	1	1	1	1	4	0

Table 4.2: Truth table, Hamming weight, and Fourier coefficients of $B(u_1, \ldots, u_r)$.

x	$(u_1, \ldots, u_r)$	$2x+1$	$B(u_1, \ldots, u_r)$
0	$(0,0,0,0)$	1	$B(0,0,0,0) = 1$
1	$(0,0,0,1)$	3	$B(0,0,0,1) = 1$
2	$(0,0,1,0)$	5	$B(0,0,1,0) = 1$
3	$(0,0,1,1)$	7	$B(0,0,1,1) = 1$
4	$(0,1,0,0)$	9	$B(0,1,0,0) = 0$
5	$(0,1,0,1)$	11	$B(0,1,0,1) = 1$
6	$(0,1,1,0)$	13	$B(0,1,1,0) = 1$
7	$(0,1,1,1)$	15	$B(0,1,1,1) = 1$
8	$(1,0,0,0)$	17	$B(0,1,1,1) = 1$
9	$(1,0,0,1)$	19	$B(1,0,0,1) = 1$
10	$(1,0,1,0)$	21	$B(1,0,1,0) = 1$
11	$(1,0,1,1)$	23	$B(1,0,1,1) = 1$
12	$(1,1,0,0)$	25	$B(1,1,0,0) = 0$
13	$(1,1,0,1)$	27	$B(1,1,0,1) = 0$
14	$(1,1,1,0)$	29	$B(1,1,1,0) = 1$
15	$(1,1,1,1)$	31	$B(1,1,1,1) = 1$

Table 4.3: Boolean function representation of 4 variables for square-free integers.

Chapter 5

Some further topics

5.1 Generalized Fermat quotients

5.1.1 Euler quotients

It is useful to recall the following definition [7, p. 25]:

Definition 20. *Euler's totient function* of m, $\varphi(m)$, is the number of positive integers not exceeding m which are relatively prime to m, where $m \geq 1$.

Examples: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(8) = 4$ because 1, 3, 5, and 7 are relatively prime to 8.

Recall an important property of Euler's totient function [7, p. 28]: For p a prime and $u \geq 1$ an integer, we have

$$\varphi(p^u) = p^{u-1}(p-1).$$

Example:

$$\varphi(32) = 2^{5-1}(2-1) = 16.$$

Fermat's little theorem, from which the Fermat quotient is derived, is a special case of Euler's theorem [7, p. 113]:

Theorem 6. *(Euler's theorem): Let u and m be two integers with* $\gcd(u, m) = 1, m \geq 2$. *Then*

$$u^{\varphi(m)} \equiv 1 \pmod{m}.$$

It seems natural to ask whether any quotient can be derived from Euler's theorem. Lerch [41] introduced a generalization of the Fermat quotient for composite moduli m (m odd, $m > 1$, subsequently extended to all $m \geq 2$) based on Euler's theorem.

Apart from Lerch's work, Agoh, Dilcher, and Skula [2] investigated these generalized Fermat quotients for composite moduli and called them *Euler quotients*.

Definition 21. Let u and $m \geq 2$ be two relatively prime integers. The quotient

$$q(u,m) \equiv \frac{u^{\varphi(m)}-1}{m} \pmod{m}$$

is called the *Euler quotient* of m with base u.

By Euler's theorem, the Euler quotient is an integer.

Properties of Fermat quotients can be generalized to Euler quotients. For instance:

Proposition 3. *Fix $m \geq 2$.*

(a) If u and v are integers with $\gcd(u,m) = \gcd(v,m) = 1$, then

$$q(uv,m) \equiv q(u,m) + q(v,m) \pmod{m}.$$

(b) If c, k are integers, c, m are relatively prime, and β is a positive integer, then

$$q(c+km^{\beta},m) \equiv q(c,m) + \frac{\varphi(m)k}{c}m^{\beta-1} \pmod{m^{\beta}}.$$

This corresponds to Proposition 1 in Section 3.2 and (a) is again referred to as the logarithmic property for Euler quotients.

Proof of Proposition 3. (a) By the definition of the Euler quotient,

$$\begin{aligned}
q_p(uv) &\equiv \frac{(uv)^{\varphi(m)}-1}{m} \pmod{m} \\
&\equiv \frac{(uv)^{\varphi(m)} - v^{\varphi(m)} + v^{\varphi(m)} - 1}{m} \pmod{m} \\
&\equiv \frac{u^{\varphi(m)-1}-1}{m} \cdot v^{\varphi(m)} + \frac{v^{\varphi(m)}-1}{m} \pmod{m} \\
&\equiv q(u,m)v^{\varphi(m)} + q(v,m) \pmod{m} \\
&\equiv q(u,m) + q(v,m) \pmod{m} \text{ using Euler's theorem.}
\end{aligned}$$

(b) Using the definition of the Euler quotient and then the binomial theorem,

$$\begin{aligned} q(c+km^\beta, m) &\equiv \frac{(c+km^\beta)^{\varphi(m)}-1}{m} \pmod{m} \\ &\equiv \frac{c^{\varphi(m)}+\varphi(m)(km^\beta)c^{\varphi(m)-1}+\cdots+(km^\beta)^{\varphi(m)}-1}{m} \pmod{m} \\ &\equiv \frac{c^{\varphi(m)}-1}{m}+\frac{\varphi(m)k}{c}m^{\beta-1} \pmod{m^\beta} \text{ using Euler's theorem} \\ &\equiv q(c,m)+\frac{\varphi(m)k}{c}m^{\beta-1} \pmod{m^\beta}. \end{aligned}$$

This completes the proof. □

Generalized Fermat quotients are related to the Bernoulli numbers and polynomials, and further congruences can be obtained from them (see [2]). Also analogous to the concept of a Wieferich prime (for Fermat quotients) is the concept of a *Wieferich number*:

Definition 22. Let $m \geq 2$ and u be relatively prime integers. m is a *Wieferich number* with base u if

$$q(u,m) \equiv 0 \pmod{m}.$$

The paper [2] has interesting results on Wieferich numbers.

5.1.2 Carmichael quotients

A different generalization of the Fermat quotient can be obtained using the Carmichael function [55], [56]:

Definition 23. The *Carmichael function* of m, $\lambda(m)$, is defined as follows for a prime power p^k:

$$\lambda(p^k) = \begin{cases} p^{k-1}(p-1) & \text{if } p \geq 3 \text{ or } k \leq 2, \\ 2^{k-2} & \text{if } p = 2 \text{ and } k \geq 3; \end{cases}$$

and

$$\lambda(m) = \operatorname{lcm}(\lambda(p_1^{k_1}), \lambda(p_2^{k_2}), \ldots, \lambda(p_s^{k_s})),$$

where "lcm" means the least common multiple, and $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$ is the prime factorization of m.

Note that $\lambda(1) = 1$, and if $m|n$, then $\lambda(m)|\lambda(n)$.

Examples:

$$\lambda(8) = 2^{3-2} = 2;$$
$$\lambda(32) = 2^{5-2} = 8;$$
$$\lambda(5) = 5^{1-1}(5-1) = 4;$$
$$\lambda(25) = 5^{2-1}(5-1) = 20.$$

Observe also that for every positive integer m, we have $\lambda(m)|\varphi(m)$, and $\lambda(m) = \varphi(m)$ if and only if $m \in \{1, 2, 4, p^k, 2p^k\}$, where p is an odd prime and $k \geq 1$.

As an analog of Euler's theorem, Carmichael [13, p. 233] showed that:

Theorem 7. *Let u and m be two integers with* $\gcd(u, m) = 1, m \geq 2$. *Then*

$$u^{\lambda(m)} \equiv 1 \pmod{m}.$$

Definition 24. Let $m \geq 2$ and u be relatively prime integers. The quotient

$$C_m(u) = \frac{u^{\lambda(m)} - 1}{m}$$

is called the *Carmichael quotient* of m with base u.

By Theorem 10, the Carmichael quotient is an integer.

Example:

$$\begin{aligned} C_5(3) &= \frac{3^{\lambda(5)} - 1}{5} \\ &= \frac{3^4 - 1}{5} \\ &= 16. \end{aligned}$$

Like Fermat quotients, Carmichael quotients also satisfy the "logarithmic property": If u and v are integers with $\gcd(uv, m) = 1$, then

$$C_m(uv) \equiv C_m(u) + C_m(v) \pmod{m}.$$

Carmichael quotients can also be used to construct sequences similar to the binary sequences derived from Fermat quotients which we considered in Section 4.1 and they have the potential for further study in the future. For instance, refer to [55], [56].

5.2 Related matters

5.2.1 Carmichael numbers

In this subsection, the term *pseudoprime* refers to a Fermat pseudoprime.

While investigating the converse of Fermat's little theorem, Robert Daniel Carmichael discovered *Carmichael numbers* in 1910 [13]. Leading to the definition of a Carmichael number, the following definitions are useful [65]:

Definition 25. If N is an odd composite number with $\gcd(u, N) = 1$ and if

$$u^{N-1} \equiv 1 \pmod{N},$$

then N is called a pseudoprime to base u.

Definition 26. If N is an odd composite number with $\gcd(u, N) = 1$ and if

$$u^{2^r d} \equiv -1 \pmod{N},$$

for some integer r with $0 \leq r < s$, where $N - 1 = d \cdot 2^s$ with d odd, then N is called a strong pseudoprime to base u.

Definition 27. If for every integer u with $\gcd(u, N) = 1$,

$$u^{N-1} \equiv 1 \pmod{N},$$

then N is called a Carmichael number.

A Carmichael number is also called an *absolute pseudoprime* [28, p. 201], or a *universal pseudoprime* [38, p. 508]. Some of the properties satisfied by Carmichael numbers include (see [51]):

1. If the prime p divides the Carmichael number N, then $N \equiv 1 \pmod{p-1}$, and hence $N \equiv 1 \pmod{p(p-1)}$.

2. Every Carmichael number is square-free.

   The two properties above are implied by *Korselt's criterion* [4, p. 703]: N *divides* $u^N - u$ *for all integers* u *if and only if* u *is square-free and* $p-1$ *divides* $N-1$ *for all primes* p *dividing* N.

Carmichael number	Factorization
561	$3 \cdot 11 \cdot 17$
1105	$5 \cdot 13 \cdot 17$
1729	$7 \cdot 13 \cdot 19$
2465	$5 \cdot 17 \cdot 29$
2821	$7 \cdot 13 \cdot 21$
6601	$7 \cdot 23 \cdot 41$
8911	$7 \cdot 19 \cdot 67$
10585	$5 \cdot 29 \cdot 73$
15841	$7 \cdot 31 \cdot 73$
29341	$13 \cdot 37 \cdot 61$
41041	$7 \cdot 11 \cdot 13 \cdot 41$
46657	$13 \cdot 37 \cdot 97$
52633	$7 \cdot 73 \cdot 103$
62745	$3 \cdot 5 \cdot 47 \cdot 89$
63973	$7 \cdot 13 \cdot 19 \cdot 37$
75361	$11 \cdot 13 \cdot 17 \cdot 31$
101101	$7 \cdot 11 \cdot 13 \cdot 2101$
115921	$13 \cdot 37 \cdot 241$
126217	$7 \cdot 13 \cdot 19 \cdot 73$
162401	$17 \cdot 41 \cdot 233$
172081	$7 \cdot 13 \cdot 31 \cdot 61$
188461	$7 \cdot 13 \cdot 19 \cdot 109$
252601	$41 \cdot 61 \cdot 101$

Table 5.1: The first 23 Carmichael numbers [38, p. 508].

The infinitude of Carmichael numbers remained a conjecture until 1994 when it was proved [4]. Carmichael numbers have been studied in more detail, for instance, in [4], [38], and [51].

5.2.2 Wilson quotients

Wilson quotients are closely related to Fermat quotients. Before proceeding with the definition of a Wilson quotient [3], it is helpful to state the following theorem:

Theorem 8. *(Wilson's theorem): If p is a prime, then* $(p-1)! \equiv -1 \pmod{p}$.

We are now ready to review the definition of the Wilson quotient.

Definition 28. Let p be a prime. The Wilson quotient is defined as:

$$w_p \equiv \frac{(p-1)!+1}{p} \pmod{p}.$$

Definition 29. The prime p is called a Wilson prime if $w_p \equiv 0 \pmod{p}$.

The first two Wilson primes are 5 and 13. This statement can be readily verified:

$$w_5 \equiv \frac{(5-1)!+1}{5} = \frac{25}{5} \equiv 0 \pmod{5}.$$
$$w_{13} \equiv \frac{(13-1)!+1}{5} = \frac{479001601}{13} \equiv 0 \pmod{13}.$$

The third Wilson prime is 563, and there are no other such primes below 2×10^{13} [18].

As we shall see below, Wilson quotients are related to Fermat quotients of prime moduli, and Fermat quotients of composite moduli (referred to as Euler quotients) in a number of ways. As with Fermat quotients, Wilson quotients can also be extended to composite moduli. The following theorem gives a basis for the definition of the Wilson quotient for composite moduli:

Theorem 9. *(Wilson's theorem for composite moduli): Let $m \geq 2$ be an integer, and set $\epsilon_m = -1$ when $m = 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime and α a positive integer, and $\epsilon_m = 1$ otherwise. Then*

$$\prod_{\substack{j=1 \\ \gcd(j,m)=1}}^{m} j \equiv \epsilon_m \pmod{m}.$$

Definition 30. Let $m \geq 2$ be an integer, and ϵ_m be defined as in Theorem 12. Denote

$$P(m) = \prod_{\substack{j=1 \\ \gcd(j,m)=1}}^{m} j.$$

Then the integer

$$W(m) \equiv \frac{P(m) - \epsilon_m}{m} \pmod{m}$$

is called the *generalized Wilson quotient* of m.

Analogous to the concept of Wieferich numbers for Euler quotients is the concept of *Wilson numbers* for Wilson quotients.

Definition 31. For $m \geq 4$, composite numbers that satisfy the congruence

$$W(m) \equiv 0 \pmod{m}$$

are called *Wilson numbers*.

Fermat quotients and Wilson quotients are related directly in a number of ways. For instance,

1. Let p be an odd prime and $m > 2$ an integer not divisible by p. Then

$$-mW(pm) \equiv W(p)\varphi(m) + \sum_{r|m} q_p(r)\frac{\varphi(m)}{r-1} \pmod{p},$$

   where the sum is taken over all primes r that divide m.

2. For any prime p, we have

$$\sum_{u=1}^{p-1} q_p(u) \equiv w_p \pmod{p}.$$

More on the relationship between Fermat quotients and Wilson quotients can be seen in [3], [39]. Table 5.2 shows Wilson numbers $\leq 5 \times 10^8$:

Wilson number	Factorization
5	prime
13	prime
563	prime
5971	$7 \cdot 853$
558771	$3 \cdot 19 \cdot 9803$
1964215	$5 \cdot 11 \cdot 71 \cdot 503$
8121909	$3 \cdot 139 \cdot 19477$
12326713	$7 \cdot 1760959$
23025711	$3 \cdot 1867 \cdot 4111$
26921605	$5 \cdot 67 \cdot 80363$
341569806	$2 \cdot 3 \cdot 181 \cdot 409 \cdot 769$
399292158	$2 \cdot 3 \cdot 17 \cdot 97 \cdot 40357$

Table 5.2: Wilson numbers $\leq 5 \times 10^8$ in [3, p. 848].

5.2.3 Fermat numbers

Like the Fermat quotients, Fermat numbers are also named after Pierre de Fermat. Numbers of the form

$$F_n = 2^{2^n} + 1, \;\; n \in \mathbb{Z}, \;\; n \geq 0$$

are called *Fermat numbers*.

Fermat noted that the first five such numbers are prime:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Fermat conjectured that all Fermat numbers are prime, but Euler refuted this conjecture when he showed that

$$F_5 = 4\,294\,967\,297$$

is composite. Precisely,

$$F_5 = 641 \cdot 6700417.$$

Fermat numbers and sieving

Many algorithms exist for factoring integers. An old method for factoring integers uses the method of difference of two squares introduced by Fermat and Legendre [11]. Many other factoring algorithms are based on the strategy used in this method. Some of them include the random squares method, the quadratic sieve, and the number field sieve.

The number field sieve [43] is an algorithm with which integers of the form $a^e \pm b$ can be factored where a and b are small positive integers, and e is a large integer. Although there are more efficient methods for factorizing Fermat numbers like the elliptic curve method, Fermat numbers have been factored by sieving. More on sieving and factoring Fermat numbers can be seen in [23], [43].

Although the following section is not related to cryptography, it is worth mentioning this historically important application of Fermat quotients.

5.3 The first case of Fermat's last theorem

Theorem 10. *(Fermat's last theorem): No three positive integers x, y, and z satisfy the equation $x^n + y^n = z^n$ for any integer value of n greater than 2.*

Dilcher and Skula [22] studied the first case of Fermat's last theorem in great detail. Their study was aided with special sums which they defined as follows:

$$s(k,N) = \sum_{j=\lfloor \frac{kp}{N} \rfloor + 1}^{\lfloor \frac{(k+1)p}{N} \rfloor} j^{p-2}$$

for p prime, integers N and k with $1 \leq N \leq p-1$ and $0 \leq k \leq N-1$. Fermat quotients are linked with these sums via the following formula:

$$Nq_p(N) \equiv \sum_{k=0}^{N-1} ks(k,N) \pmod{p}.$$

Dilcher and Skula [22] showed that:

Theorem 11. *If the first case of Fermat's last theorem is false, that is, if p is an odd prime and x, y, z are integers, not divisible by p, satisfying the equation $x^p+y^p+z^p = 0$, then $s(k, N) \equiv 0 \pmod{p}$ for all $1 \leq N \leq 46$ and $0 \leq k \leq N-1$.*

Dilcher and Skula [22] also showed the relationship between the first case of Fermat's last theorem, Bernoulli polynomials, and arithmetical functions.

Mirimanoff and Vandiver extended Wieferich's theorem (see Theorem 2 in Section 3.1):

Theorem 12. *(Mirimanoff) If the first case of Fermat's last theorem is false, that is, if p is an odd prime and x, y, z are integers, not divisible by p, satisfying the equation $x^p + y^p + z^p = 0$, then $q_p(3) \equiv 0 \pmod{p}$.*

Theorem 13. *(Vandiver) If the first case of Fermat's last theorem is false, that is, if p is an odd prime and x, y, z are integers, not divisible by p, satisfying the equation $x^p + y^p + z^p = 0$, then $q_p(5) \equiv 0 \pmod{p}$.*

These results were further extended by other authors; see [23], Section 4.2 for references.

Chapter 6

Conclusion

Although more could be discussed about Fermat quotients and their properties, their pseudo-randomness seems to be most suited to their applications in cryptography. Therefore, this final chapter summarizes the properties that make Fermat quotients function as pseudo-random number generators. An overview of fields is also presented as a refresher for the content in Chapter 2 and Chapter 3 pertaining to fields. Finally, some prospects for further work are mentioned.

6.1 Fermat quotient-based pseudo-random number generators (FQBPRNGs)

We now adopt the term *Fermat quotient-based pseudo-random number generators* (FQBPRNGs) for pseudo-random number generators based on Fermat quotients. Note also that Fermat quotients refer to Fermat quotients modulo a prime p, unless otherwise stated.

Let $M, N \geq 1$, p a fixed prime and u an integer with $\gcd(u, p) = 1$. The following is a summary of the properties of Fermat quotients and sequences produced by FQBPRNGs with respect to the properties described in Section 2.2:

- *Uniformity*:
  Fermat quotients $q_p(u), u = M+1, \ldots, M+N$, are uniformly distributed modulo p^2 for all $N \leq p$.

- *Independence*:
  Binary threshold sequences, (e_{p^2}), derived from Fermat quotients have a small well-distribution measure and a small correlation measure.

$$W((e_{p^2})) \ll p(\log_2 p)^2; \;\; C_2((e_{p^2})) \ll p(\log_2 p)^3.$$

- *Large period*:

  Fermat quotients $q_p(u), u \geq 0$, are p^2-periodic. That is,

  $$q_p(u + p^2) \equiv q_p(u) \pmod{p}.$$

  Both the binary threshold sequence, (e_{p^2}), and the Legendre-Fermat sequence, (f_u) are p^2-periodic.

- *Coverage*:

  The image size of Fermat quotients $q_p(u), u = 0, 1, \ldots, p-1$, $M(p)$, is at least $\frac{p}{(\log_2 p)^2}$ for p sufficiently large. That is,

  $$M(p) \geq (1 + o(1))\frac{p}{(\log_2 p)^2}, \text{ as } p \to \infty.$$

- *Cryptographic security (Unpredictability)*:

  For a sufficiently long sequence of Fermat quotients, the linear complexity, $L_p(N)$, of the sequence $q_p(u)$, $u = 0, \ldots, N-1$, $p^2 > N \geq 1$, is at least half the value of the minimum of $p-1$ and $N-p-1$. That is,

  $$L_p(N) \geq \frac{1}{2}\min\{p-1, N-p-1\}.$$

  Also, for arbitrary segments of a sequence of Fermat quotients, the linear complexity of the sequence, $L_p(M, N)$, $q_p(u)$, $u = M+1, \ldots, M+N$, M and $p^2 > N \geq 1$, is at least the value of the minimum of $\frac{p-1}{2}$ and $\frac{N-p-1}{3}$. That is,

  $$L_p(M, N) \geq \min\left\{\frac{p-1}{2}, \frac{N-p-1}{3}\right\}.$$

  If $2^{p-1} \not\equiv 1 \pmod{p^2}$ (that is, $p \neq 1093, 3511$), then the linear complexities of the binary threshold sequence (e_{p^2}) and the Legendre-Fermat sequence (f_u) both satisfy

  $$L((e_{p^2})) = L((f_u)) = \begin{cases} p^2 - p, & \text{if } p \equiv 1 \pmod{4}, \\ p^2 - 1, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

6.2 Glossary: An overview of fields

The information in this section has been taken from [26].

- *Group*: An ordered pair $(G, *)$ where G is a set and $*$ is a binary operation on G satisfying the following axioms:

  (i) $*$ is associative: $(u * v) * w = u * (v * w)$ for all $u, v, w \in G$,

  (ii) there exists an element e in G, called the *identity* of G, such that

  $$u * e = e * u = u, \text{ for all } u \in G,$$

  (iii) there is an element u^{-1} of G, called an *inverse* of u, such that

  $$u * u^{-1} = u^{-1} * u = e, \text{ for each } u \in G.$$

  The group $(G, *)$ is called *abelian* (or *commutative*) if $u \cdot v = v \cdot u$ for all $u, v \in G$.

- *Ring*: A *ring* is a set R together with two binary operations $+$ and $\cdot$ satisfying the following axioms:

  (i) $(R, +)$ is an abelian group,

  (ii) $\cdot$ is associative: $(u \cdot v) \cdot w = u \cdot (v \cdot w)$ for all $u, v, w \in R$,

  (iii) the distributive laws hold in R: for all $u, v, w \in R$,

  $$(u + v) \cdot w = (u \cdot w) + (v \cdot w) \text{ and } u \cdot (v + w) = (u \cdot v) + (u \cdot w).$$

  The ring R is *commutative* if multiplication is commutative for all elements of the ring, that is, $u \cdot v = v \cdot u$ for all $u, v \in R$. The ring R is said to have an *identity* (or *contain a* 1) if there is an element $1 \in R$ with $1 \cdot u = u \cdot 1$ for all $u \in R$.

- *Polynomial*: Let R be a commutative ring with identity. The formal sum $c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$ with $n \geq 0$ and each $c_i \in R$ is called a *polynomial* in x.

- *Degree of polynomial*: If $c_n \neq 0$, then n is said to be the degree of the polynomial.

- *Monic polynomial*: A polynomial is said to be *monic* if $c_n = 1$.

- *Irreducible polynomial*: A non-constant polynomial is *irreducible* if and only if it cannot be factored as a product of two monic polynomials of smaller degree.

- *Zero divisor*: A non-zero element u of R is called a *zero divisor* if there is a non-zero element v in R such that either $u \cdot v = 0$ or $v \cdot u = 0$.

- *Integral domain*: A commutative ring with identity $1 \neq 0$ is called an *integral domain* if it has no zero divisors.

- *Field*: A set $\mathbb{F}$ together with two binary operations $+$ and $\cdot$ on $\mathbb{F}$ such that $(\mathbb{F}, +)$ is an abelian group (with 0 as its identity), and $(\mathbb{F} - \{0\}, \cdot)$ (with 1 as its identity, $1 \neq 0$) is also an abelian group and the following distributive law holds:

$$u \cdot (v + w) = (u \cdot v) + (u \cdot w), \text{ for all } u, v, w \in \mathbb{F}.$$

- *Characteristic of a field*: The smallest positive integer r such that $1 + 1 + \cdots 1$ (r times) $= 0$ if such an r exists, and is defined to be 0 otherwise, where 1 is the identity of the field.

- *Finite field*: A field with a finite number of elements. A finite field has characteristic p for some prime p. For example, $\mathbb{F}_q[x]$ is a finite field with q elements, where $q = p^n$ for some prime p.

- *Rational function field (The field of rational functions)*: This contains elements of the form $\frac{u(x)}{v(x)}$, where $u(x)$ and $v(x)$ are polynomials with coefficients in an integral domain D with $v(x)$ not the zero polynomial.

- *Order of a field*: The number of elements in a field.

- *Field homomorphism*: a map of a field to another field that respects the field structures.

- *Frobenius endomorphism of a finite field*: a one-to-one field homomorphism, Fr, from $\mathbb{F}$ to $\mathbb{F}$ defined by $Fr(u) = u^p$, where $\mathbb{F}$ is a finite field of characteristic p.

6.3 Future work

One immediate potential for future work is to extend the results obtained (by various authors) for Fermat quotients to generalized Fermat quotients like Euler quotients.

Another prospect is the investigation of other areas of applying Fermat quotients in cryptography. For instance, using Fermat quotients as initialization vectors and comparing results obtained across classical pseudo-random number generators (PRNGs) like Linear Congruential Generators (LCGs).

Since pseudo-randomness is a ubiquitous concept, Fermat quotients, possessing good pseudo-random properties, can also find applications in other subject areas outside cryptography.

Bibliography

[1] T. Agoh. Fermat and Euler type quotients. *C. R. Math. Acad. Sci. Soc. R. Can.*, 17(4): 159–164, 1995.

[2] T. Agoh, K. Dilcher, and L. Skula. Fermat quotients for composite moduli. *Journal of Number Theory*, 66(1): 29–50, 1997.

[3] T. Agoh, K. Dilcher, and L. Skula. Wilson quotients for composite moduli. *Mathematics of Computation*, 67(222): 843–861, 1998.

[4] W. R. Alford, A. Granville, and C. Pomerance. There are infinitely many Carmichael numbers. *Annals of Mathematics, Second Series*, 139(3): 703–722, 1994.

[5] H. Aly and A. Winterhof. Boolean functions derived from Fermat quotients. *Cryptogr. Commun.*, 3(3): 165–174, 2011.

[6] H. Aly and A. Winterhof. On the k-error linear complexity over $\mathbb{F}_p$ of Legendre and Sidelnikov sequences. *Des. Codes Cryptogr.*, 40(3): 369–374, 2006.

[7] T. M. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York-Heidelberg, 1976.

[8] K. Bhattacharjee and S. Das. A search for good pseudo-random number generators: survey and empirical studies. *Computer Science Review*, 45, 100471, 2022.

[9] J. Bourgain, K. Ford, S. V. Konyagin, and I. E. Shparlinski. On the divisibility of Fermat quotients. *Michigan Mathematical Journal*, 59(2): 313–328, 2010.

[10] J. A. Buchmann, D. Butin, F. Göpfert, and A. Petzoldt. Post-quantum cryptography: state of the art. *The New Codebreakers*: 88–108, 2016.

[11] J. P. Buhler, H. W. Lenstra Jr., and C. Pomerance. Factoring integers with the number field sieve. *The development of the number field sieve*: 50–94, Lecture Notes in Math., 1554, Springer, Berlin, Heidelberg, 1993.

[12] D. A. Burgess. On character sums and L-series. II. *Proc. Lond. Math. Soc. (3)*, 13: 524–536, 1963.

[13] R. D. Carmichael. Note on a new number theory function. *Bulletin of the American Mathematical Society*, 16(5): 232–238, 1910.

[14] M. C. Chang. Short character sums with Fermat quotients. *Acta Arith.*, 152(1): 23–38, 2012.

[15] Z. Chen, A. Ostafe, and A. Winterhof. Structure of pseudorandom numbers derived from Fermat quotients, in *Arithmetic of Finite Fields*, *Lecture Notes in Computer Science*, vol 6087: 73–85, Springer, Berlin, 2010.

[16] Z. Chen. Trace representation and linear complexity of binary sequences derived from Fermat quotients. *Sci. China Inf. Sci.*, 57(11): 1–10, 2014.

[17] Z. Chen. Elliptic curve analogue of Legendre sequences. *Monatsh. Math.*, 154(1): 1–10, 2008.

[18] E. Costa, R. Gerbicz, and D. Harvey. A search for Wilson primes. *Mathematics of Computation*, 83(290): 3071–3091, 2014.

[19] I. B. Damgård. On the randomness of Legendre and Jacobi sequences, in S. Goldwasser (ed.), CRYPTO 1988. *Lecture Notes in Comput. Sci.*, 403: 163–172, Springer, Berlin, 1990.

[20] H. Delfs and H. Knebl. *Introduction to Cryptography Principles and Applications. Information Security and Cryptography*, Springer, Heidelberg, 2015.

[21] S. Dib. Distribution of Boolean functions according to the second-order nonlinearity. in *Arithmetic of Finite Fields*, *Lecture Notes in Computer Science*, vol 6087: 86–96, Springer, Berlin, 2010.

[22] K. Dilcher and L. Skula. A new criterion for the first case of Fermat's last theorem, *Mathematics of Computation*, 64(209): 363–392, 1995.

[23] K. Dilcher. Fermat numbers, Wieferich and Wilson primes: computations and generalizations, in *Proceedings of the Conference on Public Key Cryptography and computational number theory (Warsaw, 2000)*: 29–48, de Gruyter, Berlin, 2001.

[24] J. F. Dooley. *History of cryptography and cryptanalysis: Codes, ciphers, and their algorithms*. Springer, Cham, 2018.

[25] F. G. Dorais and D. Klyve. A Wieferich prime search up to 6.7×10^{15}. *J. Integer Seq.*, 14(9), Article 11.9.2: 1–14, 2011.

[26] D. S. Dummit and R. M. Foote. *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[27] W. Easttom. *Modern cryptography- applied mathematics for encryption and information security*. Springer, Cham, 2021.

[28] P. Erdös. On pseudoprimes and Carmichael numbers. *Publ. Math. Debrecen*, 4: 201–206, 1956.

[29] R. Ernvall and T. Metsänkylä. On the p-divisibility of Fermat quotients. *Mathematics of Computation*, 66(219): 1353–1365, 1997.

[30] D. Gomez and A. Winterhof. Multiplicative character sums of Fermat quotients and pseudorandom sequences. *Period. Math. Hungar.*, 64(2): 161–168, 2012.

[31] V. J. W. Guo. Some congruences related to the q-Fermat quotients. *International Journal of Number Theory* 11: 1049–1060, 2015.

[32] K. Gyarmati, C. Mauduit, and A. Sárközy. Pseudorandom binary sequences and lattices. *Acta Arith.*, 135(2): 181–197, 2008.

[33] K. Gyarmati, A. Sárközy, and C. L. Stewart. On Legendre symbol lattices. *Uniform Distribution Theory*, 4(1): 81–95, 2009.

[34] Y. K. Han, J. Chung, K. Yang. On the k-error linear complexity of p^m-periodic binary sequences. *IEEE Trans. Inf. Theory*, 53(6): 2297–2304, 2007.

[35] D. R. Heath-Brown. An estimate for Heilbronn's exponential sum, in *Analytic Number theory, Vol. 2, Progress in Mathematics*, 139: 451–463, Birkhäuser Boston, Boston, MA, 1996.

[36] W. Johnson. On the p-divisibility of the Fermat quotients. *Mathematics of Computation*, 32(141): 297–301, 1978.

[37] D. E. Knuth. *The Art of Computer Programming*, Vol. 2, 2nd ed., Addison-Wesley, Reading, Mass., 1981.

[38] D. H. Lehmer. Strong Carmichael numbers. *J. Austral. Math. Soc. Ser. A*, 21(4): 508–510, 1976.

[39] E. Lehmer. On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson. *Annals of Mathematics, Second Series*, 39(2): 350–360, 1938.

[40] M. Lerch. Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$. *Math. Ann.* 60: 471–490, 1905.

[41] M. Lerch. Sur les théorèmes de Sylvester concernant le quotient de Fermat. *C. R. Acad. Sci. Paris*, 142: 35–38, 1906.

[42] H. W. Lenstra. Miller's primality test. *Information Processing Letters*, 8(2): 86–88, 1979.

[43] A. K. Lenstra, H. W. Lenstra Jr, M. S. Manasse, and J. M. Pollard. The number field sieve, in *The development of the number field sieve*: 11–42. *Lecture Notes in Math.*, 1554, Springer, Berlin, 1993.

[44] M. Luby. *Pseudorandomness and Cryptographic Applications*. Princeton Computer Science Notes: Princeton University Press, Princeton, NJ, 1996.

[45] C. Mauduit and A. Sárközy. On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol. *Acta Arith.*, 82(4): 365–377, 1997.

[46] C. Mauduit, J. Rivat, and A. Sárközy. Construction of pseudorandom binary sequences using additive characters. *Monatsh. Math.*, 141(3): 197–208, 2004.

[47] R. Mestrovic. Congruences involving the Fermat quotient. *Czechoslovak Mathematical Journal*, 63(4): 949–968, 2013.

[48] H. Niederreiter. *Random Number Generation and Quasi-Monte Carlo Methods*. CBMS-NSF Regional Conference Series in Applied Mathematics, 63, SIAM, Philadelphia, PA, 1992.

[49] H. Niederreiter. Linear complexity and related complexity measures for sequences. Progress in cryptology—INDOCRYPT 2003, *Lecture Notes in Computer Science*2904: 1–17, Springer, Berlin, 2003.

[50] A. Ostafe and I. E. Shparlinski. Pseudorandomness and dynamics of Fermat quotients. *SIAM Journal on Discrete Mathematics*. 25(1): 50–71, 2011.

[51] C. Pomerance, J. L. Selfridge, S. S. Wagstaff. The pseudoprimes to $25 \cdot 10^9$. *Mathematics of Computation*, 35(151): 1003–1026, 1980.

[52] A. Sárközy, C. L. Stewart. On pseudorandomness in families of sequences derived from the Legendre symbol. *Period. Math. Hungar.* 54(2): 163–173, 2007.

[53] J. Sauerberg and L. Shu. Fermat quotients over function fields. *Finite fields and their applications*, 3(4): 275–286, 1997.

[54] B. Schneier. *Applied Cryptography – Protocols, Algorithms, and Source Code in C*, 2nd edition, 20th anniversary edition, Wiley, Indianapolis, IN, Wiley, 2015.

[55] M. Sha. The arithmetic of Carmichael quotients. *Period. Math. Hungar.* 71(1): 11–23, 2015.

[56] M. Sha. Correction to: The arithmetic of Carmichael quotients, *Period. Math. Hungar.*, 76(2): 271–273, 2018.

[57] I. D. Shkredov. On Heilbronn's exponential sum. *The Quarterly Journal of Mathematics*, 64(4): 1221–1230, 2013.

[58] I. E. Shparlinski. Fermat quotients: exponential sums, value set and primitive roots. *Bulletin of the London Mathematical Society*, 43(6): 1228–1238, 2011.

[59] I. E. Shparlinski. On the value set of Fermat quotients. *Proceedings of the American Mathematical Society*, 140(4): 1199–1206, 2012.

[60] I. E. Shparlinski. *Cryptographic Applications of Analytic Number Theory: Complexity Lower Bounds and Pseudorandomness. Progress in Computer Science and Applied Logic*, 22, Birkhäuser, Basel, 2003.

[61] I. E. Shparlinski. Character sums with Fermat quotients. *The Quarterly Journal of Mathematics*, 62(4): 1031–1043, 2011.

[62] Y. N. Shteinikov. Divisibility of Fermat quotients.Translation of Mat. Zametki 92(1): 116–122, 2012. *Mathematical Notes*, 92(1-2): 108–114, 2012.

[63] A. Stanoyevitch. *Introduction to Cryptography with Mathematical Foundations and Computer Implementations*. Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 2011.

[64] L. Skula. Fermat and Wilson quotients for p-adic integers. *Acta Math. Inform. Univ. Ostraviensis*, 6(1): 167–181, 1998.

[65] J. Sorenson and J. Webster. Strong pseudoprimes to twelve prime bases. *Mathematics of Computation*, 86(304): 985–1003, 2017.

[66] A. Topuzoğlu and A. Winterhof. Pseudorandom sequences, in *Topics in geometry, coding theory and cryptography*, *Algebr. Appl., volume 6*: 135–166. Springer, Dordrecht, 2007.

[67] R. J. Turyn. The linear generation of Legendre sequence. *J. Soc. Indust. Appl. Math.*, 12(1): 115–116, 1964.

[68] Q. Wang and X. Du. The linear complexity of binary sequences with optimal autocorrelation. *IEEE Trans. Inf. Theory*, 56(12): 6388–6397, 2010.

[69] C. K. Wu and D. Feng. *Boolean Functions and Their Applications in Cryptography. Advances in Computer Science and Technology*. Springer, Berlin, 2016.

[70] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu. A survey on true random number generators based on chaos. *Discrete Dyn. Nat. Soc.*, 2019.