International Journal of Security and Its Applications
Vol. 10, No. 3 (2016), pp.439-448
http://dx.doi.org/10.14257/ijsia.2016.10.3.38

A Novel Method of Searching Primitive Roots Modulo Fermat Prime Numbers

Dalei Zhang[1, 2] and Hong Zhong[1]

[1]School of Computer Science and Technology Anhui University
Hefei 230039, China
[2]Institute of Computer and Information Engineering
Huainan Normal University
Huainan 230001, Anhui, China
zhangdalei88@163.com

Abstract

Primitive root is a fundamental concept in modern cryptography as well as in modern number theory. Fermat prime numbers have practical uses in several branches of number theory. As of today, there is no simple general way to compute the primitive roots of a given prime, though there exists methods to find a primitive root that are faster than simply trying every possible number. We prove the equivalence between the primitive roots and the quadratic nonresidues modulo Fermat prime numbers. Therefore, the problem of searching primitive roots is transformed into solving the quadratic residues modulo Fermat primes, which is a much easier problem, having very simple solutions. Theoretical analysis and experimental results verify our conclusion.

***Keywords**: primitive root; Fermat prime; quadratic residue; modular power*

1. Introduction

Number theory is an ancient branch of mathematics, studying the properties of numbers. Primes have special importance in number theory, which are those natural numbers that are greater than 1, with no positive factors except for 1 and themselves. Though having a very long history, number theory was considered as useless in application. However, this opinion completely changed after the 1970s, when the public key cryptography was developed. Prime numbers are the basis for establishing several public key cryptography schemes, such as RSA. Nowadays, number theory has many important applications in the field of information security.

Pierre de Fermat, the famous French mathematician, first studied the Fermat numbers. Fermat found that the first 5 Fermat numbers are all primes. Then he conjectured that all Fermat numbers were prime numbers. The first five Fermat numbers are $F_0 = 3, F_1 = 5,$ $F_2 = 17, F_3 = 257, F_4 = 65537$, which are indeed primes. However, Leonhard Euler proved in 1732 that $F_5 = 4294967297 = 641 \times 6700417$, which was not a prime. In fact, as of 2015, the first five Fermat numbers are the only known primes in Fermat numbers [1-4]. It is widely believed that no more Fermat primes will be found. Fermat prime numbers have practical use in generating pseudo-random sequences of numbers. Research focuses mainly on the primality of Fermat numbers in recent years [5-9].

Primitive root plays an important role in modern cryptography, such as the Diffie-Hellman scheme. As of today, there is no simple general way to compute the primitive roots of a given prime, though there exists methods to find a primitive root that are faster than simply trying every possible number [10-11]. If m is a primitive root modulo p, then the multiplicative order of m is $\varphi(n)$, where $\varphi(n)$ is Euler's totient function. This theorem can be used to find primitive roots. At first, $\varphi(n)$ is computed. Then find the prime

ISSN: 1738-9976 IJSIA

divisors of $\varphi(n)$, say $p_1, p_2, \ldots, p_k$. Next compute $m^{\varphi(n)/p_i} \bmod n$ for $i = 1, 2, \ldots, k$. If the results are all not equal to 1, the number m is a primitive root. In fact, finding a quick algorithm to compute primitive roots is considered as one of the most important problem in the field of number theory.

The remainder of this paper is expanded as below. First we present preliminaries in section 2. In section 3, we present the main results. Section 4 provides our proposed scheme. The experimental results and analysis are presented in section 5. In section 6, we get some conclusions.

2. Preliminaries

Definition 1 A Fermat number is defined in the form where n is a nonnegative integer. If a Fermat number is a prime at the same time, it is called Fermat prime number.

$$F_n = 2^{2^n} + 1 \tag{1}$$

For example, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$are the only known five Fermat prime numbers, while $F_5 = 4294967297 = 641 \times 6700417$ is just a Fermat number.

According to Definition 1, $F_n = 2^{2^n} + 1$. Therefore, $F_n - 1 = 2^{2^n} = 2^k$, where $k = 2^n$. Thus, the divisors of $F_n - 1 = 2^k$ are all the power of 2.

For example, $F_0 - 1 = 2, F_1 - 1 = 2^2, F_2 - 1 = 2^4, F_3 - 1 = 2^8, F_4 - 1 = 2^{16}$.

Therefore, $F_0 - 1$ has divisors of 1 and 2. $F_1 - 1$ has divisors of 1, 2, 4 and so on.

Definition 2 The totient function $\varphi(n)$, which is also named Euler's totient function, is defined as the number of positive numbers $\leq n$ that are relatively prime to n.

For example, there are four totatives of 8, that is 1,3,5,7. So $\varphi(8) = 4$.

For a number $n = p^k$, which is a power of a prime, then

$$\varphi(p^k) = p^k(1 - \frac{1}{p}) \tag{2}$$

For a prime number p, $\varphi(p) = p - 1$, since each number $< p$ is relatively prime to p. For a number $n = p^k$, which is a power of a prime, the numbers that have common divisors with n are the multiples of p, that is $p, 2p, \ldots, p^{k-1}p$. Since there are p^{k-1} multiples, then

$$\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p}) \tag{3}$$

Definition 3 The smallest positive number x, satisfying

$$b^x \equiv 1 \pmod{p} \tag{4}$$

is called the multiplicative order of b modulo p, where b is an integer, and p a positive integer with $gcd(b, p) = 1$. The order of b modulo p is also written as $ord_p(b)$.

The multiplicative order of b modulo p must be one of the divisors of $p - 1$, where b is an integer, and p a positive integer with $gcd(b, p) = 1$. It can also be expressed as $ord_p(b)|(p-1)$. This is the consequence of Lagrange' theorem.

Obviously, if x is natural numbers, the number sequence $b^x \bmod p$ has a period. For example, $4^1 \bmod 5 = 4, 4^2 \bmod 5 = 1, 4^3 \bmod 5 = 4, 4^4 \bmod 5 = 1$.Thus, the number sequence $b^x \bmod p$ is $4, 1, 4, 1, \ldots$, the period of which is 2. When 1 appears in the number sequence, a period is formed. According to Fermat's Little Theorem, for each natural number b , where b is not divisible by p, then $b^{p-1} \equiv 1 \pmod{p}$. Therefore the number of the position $p - 1$in the number sequence must be 1. According to Definition 2, the multiplicative order of b modulo p is the smallest number, satisfying $b^x \equiv 1 \pmod{p}$. The multiplicative order of b modulo p is exactly the period of the number sequence

$b^x \bmod p$. Hence, the multiplicative order of b modulo p must be one of the divisors of $p-1$, where p is a prime.

Definition 4 Let b be an integer, and p be a positive prime with $gcd(b,p)=1$. If $ord_p(b)=p-1$, b is called a primitive root modulo p.

Each prime number has at least one primitive root [12]. If p is a prime, it has $\varphi(p-1)$ primitive roots, where $\varphi(n)$ is the Euler totient function.

Definition 5 If there is an integer $0<x<p$, such that then q is the quadratic residue modulo p.

$$x^2 \equiv q \pmod p \tag{5}$$

Lemma 1 (Euler's criterion) Let p be an odd prime integer, which is relatively prime to p. Then

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) = \begin{cases} 1 & \text{iff a is quardratic residue mod p} \\ -1 & \text{iff a is quardratic nonresidue mod p} \end{cases} \tag{6}$$

Lemma 2 Let $p>3$ be an Fermat prime and $0<a<p$ be an integer, which is relatively prime to p. If a is the quadratic residue modulo p, then $p-a$ is also the quadratic residue modulo p.

Proof. Since a is the quadratic residue modulo p, then according to Lemma 1, $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Let $\dfrac{p-1}{2}=t$, then

$$(p-a)^{\frac{p-1}{2}} = (p-a)^t = p^t + c_1p^{t-1}a + c_2p^{t-2}a^2 + \cdots + c_{t-1}pa^{t-1} + a^t$$

Therefore, $(p-a)^{\frac{p-1}{2}} \bmod p = a^t \bmod p = a^{\frac{p-1}{2}} = 1$, that is, $p-a$ is also the quadratic residue modulo p.

Let p be a prime, then

$$(p-1)^2 \equiv 1 \pmod p \tag{7}$$

Proof. Since $(p-1)^2 = p^2-2p+1$, $(p-1)^2 \bmod p = (p^2-2p+1) \bmod p = 1$. Therefore, $(p-1)^2 \equiv 1 \pmod p$.

3. Main Results

Lemma 3 For Fermat prime numbers $p=2^{2^n}+1$, they have primitive roots.

$$\varphi(p-1) = 2^{2^n-1} \tag{8}$$

Proof. Since Fermat prime numbers $2^{2^n}+1$have $\varphi(p-1)=\varphi(2^{2^n})$primitive roots. According to the definition of Euler totient function, $\varphi(2^{2^n}) = 2^{2^n}(1-\frac{1}{2}) = 2^{2^n-1}$.

Therefore, $F_0=3, F_1=5, F_2=17, F_3=257$ and $F_4=65537$ have 1, 2, 8, 128 and 32768 primitive roots respectively.

Lemma 4 (Fermat's Little Theorem) If p is a prime number, b is a natural number and b is not divisible by p, then

$$b^{p-1} \equiv 1 \pmod p \tag{9}$$

Theorem 1 b is the primitive root of Fermat prime number p, if and only if

$$b^{\frac{p-1}{2}} \equiv p-1 \pmod p \tag{10}$$

Proof. Sufficiency: assume by way of contradiction that b is not the primitive root of Fermat prime number p, then according to Lemma 1 and Lemma 3, the multiplicative order of b modulo $p \in \{1, 2, 2^2, 2^3, \ldots, (p-1)/2\}$. In any case, we have $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Therefore, if $b^{\frac{p-1}{2}} \equiv p-1 \pmod{p}$, then b is the primitive root of Fermat prime number p.

Necessity: assume that b is the primitive root of Fermat prime number p. Let $k = b^{\frac{p-1}{2}}$, then $k^2 = (b^{\frac{p-1}{2}})^2 = b^{p-1}$. According to Lemma 4, $b^{p-1} \equiv 1 \pmod{p}$, then $k^2 \equiv 1 \pmod{p}$. Obviously, k has two possible values, i.e. 1 and $p-1$.

Since b is the primitive root of Fermat prime number p, the multiplicative order of b modulo p is $p-1$, so $k = b^{\frac{p-1}{2}} \bmod p$ cannot be 1. Therefore, $b^{\frac{p-1}{2}} \equiv p-1 \pmod{p}$. The proof is completed.

Corollary 1 b is a primitive root of a Fermat prime number p, if and only if b is the quadratic non-residue modulo p.

Proof. According to Lemma 1 (Euler's criterion) and Theorem 1, clearly, If b is the primitive root of Fermat prime number p, then if and only b is the quadratic nonresidue modulo p.

Lemma 5 There are the same number of quadratic residues and nonresidues modulo an odd prime number p. And they are $1 \bmod p, 2^2 \bmod p, \ldots, (\frac{p-1}{2})^2 \bmod p$.

Theorem 2 If $N_k = 2^k + 1$ is prime, and $k > 0$, k must be a power of 2.

Proof. Assume by way of contradiction that if k has odd factor b, then

$$2^k + 1 = (2^a)^b + 1 = (2^a + 1)[2^{a(b-1)} - 2^{a(b-2)} + 2^{a(b-3)} - \cdots]$$

Therefore, for a prime N_k, k must be a power of 2.

4. The Proposed Scheme

Table 1 and Table 2 are are produced in such way: let r be the row number of the table, and c be the column number of the table. Each element in the Table 1 is equal to $r^c \bmod 5$. The elements of Table 2 are equal to $r^c \bmod 7$ respectively.

It can be seen that there are ten laws in these tables:

(1) The elements in the first row are all 1, since $1^k \bmod p = 1 \bmod p = 1$. Or it can be expressed that the period of the first row is 1.

(2) The elements in the last column are all 1, which is the result of Fermat's Little Theorem.

(3) The elements in the last row are $p-1, 1, p-1, 1, \ldots,$ which can also be expressed that the period of the last row is 2.

(4) In the middle column, the elements are divided into 2 equal sets, each set having $(p-1)/2$ numbers, containing 1 and $p-1$ respectively. For example, in Table 2, there are three 1 and three 6 in the middle column. This is the result of Euler's criterion.

(5) The elements appearing in the second column are all quadratic residues modulo p. For example, in Table 1, 1 and 4 appear in the second column, which are all quadratic residues modulo 5. This is the result of Lemma 5.

(6) For those rows, the numbers of which are quadratic residues modulo p, the middle elements are all 1. For example, in Table 1, the elements of the 1st and 4th row are all 1, which is also the result of Euler's criterion.

(7) When p is a Fermat prime number, the number of each row is either quadratic residues modulo p or primitive roots modulo p. For example, in Table 1, 1 and 4 are all quadratic residues modulo 5. 2 and 3 are all primitive roots modulo 5. This is the result of Corollary 1.

(8) When p is a Fermat prime number, if the elements in the middle column are 1, the row number of them are quadratic residues modulo p. And if the elements in the middle column are $p-1$, the row number of them are the primitive roots modulo p. This is the result of Theorem 1.

(9) The period of each row is one of the divisors of $p-1$.For example, in Table 2, there are 4 periods, that is 1, 2, 3 and 6, which are all divisors of 6.

(10) The row numbers are the primitive roots modulo p, if the period of these rows are $p-1$. This is the result of Definition 4.

Table 1. Modular Power Modulo p (p=5)

$r^c \bmod 5$	**1**	**2**	**3**	**4**
1	1	1	1	1
2	2	4	3	1
3	3	4	2	1
4	4	1	4	1

Table 2. Modular Power Modulo p(p=7)

$r^c \bmod 7$	**1**	**2**	**3**	**4**	**5**	**6**
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

When dealing with the problem of searching the primitive roots of a given Fermat prime number, we can first find out the quadratic residues of this prime, which is extremely simple.

For example, if we want to search the primitive roots of a given Fermat prime, say 17, we just need to find out the quadratic residues modulo 17 first. The result includes 8 numbers, i.e. 1, 2, 4, 8, 9, 13, 15, 16. Then the remaining numbers between 1 and 16 are all primitive roots modulo 17, i.e. 3, 5, 6, 7, 10, 11, 12, 14.

Furthermore, we can speed up the searching process, using Lemma 2. Once we find a quadratic residue modulo p, another number is determined at the same time.

For example, if we find that 1, 2, 4, 8 are all quadratic residues modulo 17. Then we know that $17-1=16, 17-2=15, 17-4=13, 17-8=9$ are also quadratic residues modulo 17. In this way, the searching time can be reduced by half.

For other Fermat prime numbers, the primitive roots can be found in similar way.

5. Experimental Results and Analysis

5.1. Experimental Results

5.1.1. Existing Method: Since there is no general method to compute the primitive roots of a given prime, the existing method to find the primitive roots is to try several times to test whether a number is a primitive root modulo a prime. It can be described as follows:

For a prime p, first compute $\varphi(p)$, where $\varphi(p)$ is Euler's totient function. Then find the prime divisors of $\varphi(p)$, say $p_1, p_2, \ldots, p_k$. Next compute $a^{\varphi(p)/p_i} \bmod p$ for $i = 1, 2, \cdots, k$. If the results are all not equal to 1, the number a is a primitive root.

For example, Let $p = 17$. If we want to find whether 2 is a primitive root modulo 17, we first compute $\varphi(17) = 16$. Then the set of prime factors of 16 is 2. Next compute $2^{\varphi(17)/2} \bmod 17 = 2^{16/2} \bmod 17 = 2^8 \bmod 17 = 1$, therefore 2 is not a primitive root of 17.

Similarly, let $p = 257$. To find whether 2 is a primitive root modulo 257, we need to compute $2^{\varphi(257)/2} \bmod 257 = 2^{256/2} \bmod 257 = 2^{128} \bmod 257 = 1$, therefore 2 is also not a primitive root of 257.

If $p = 65537$, we will need to compute $2^{\varphi(65537)/2} \bmod 65537 = 2^{32768} \bmod 65537 = 1$ to confirm that 2 is not a primitive root of 65537.

5.1.2. Proposed Scheme: To test the results we proved above, some experiments are conducted. We display the quadratic residues and primitive roots modulo Fermat prime numbers in one picture. In each picture, quadratic residues are framed with square boxes, and the rest are all primitive roots. Fermat number $F_0 = 3, F_1 = 5, F_2 = 17$ and $F_3 = 257$ are handled in Figure 1, Figure 2, Figure 3, and Figure 4 respectively. Figure 5 and Figure 6 show part of the quadratic residues and primitive roots of $F_4 = 65537$.

It can be seen that, in Figure 1, Figure 2, Figure 3, and Figure 4, there are exactly half of the numbers are framed with square boxes, since each Fermat prime number $F_n$has $(F_n - 1)/2$ quadratic residues and the same number primitive roots.

As Fermat prime F_4 has 32768 quadratic residues and the same number primitive roots, it is impossible to show them all in one picture. Therefore, part of the quadratic residues and primitive roots are displayed in Figure 5 and Figure 6.

Figure 5 shows the first 256 quadratic residues and primitive roots of $F_4 = 65537$. Figure 6 shows the last 100 quadratic residues and primitive roots of $F_4 = 65537$. From the Figure 2, it can be seen that 1 and 4 are the quadratic residues of $F_1 = 5$. So, 2 and 3 are the primitive roots of $F_1 = 5$. In the same way, the set of quadratic residues modulo 17 is {1, 2, 4, 8, 9, 13, 15, 16} and the set of primitive roots modulo 17 is {3, 5, 6, 7, 10, 11, 12, 14}.

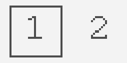


Figure 1. Quadratic Residues and Primitive Roots of 3

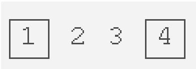
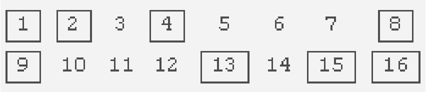
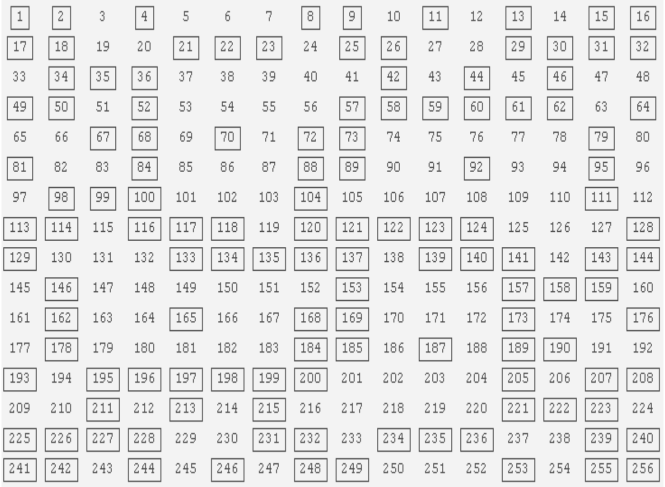


Figure 2. Quadratic Residues and Primitive Roots of 5



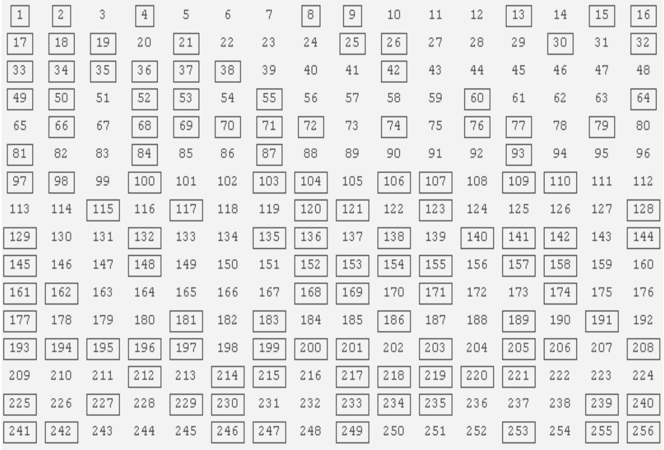
$\boxed{1}$	$\boxed{2}$	3	$\boxed{4}$	5	6	7	$\boxed{8}$
$\boxed{9}$	10	11	12	$\boxed{13}$	14	$\boxed{15}$	$\boxed{16}$

Figure 3. Quadratic Residues and Primitive Roots of 17



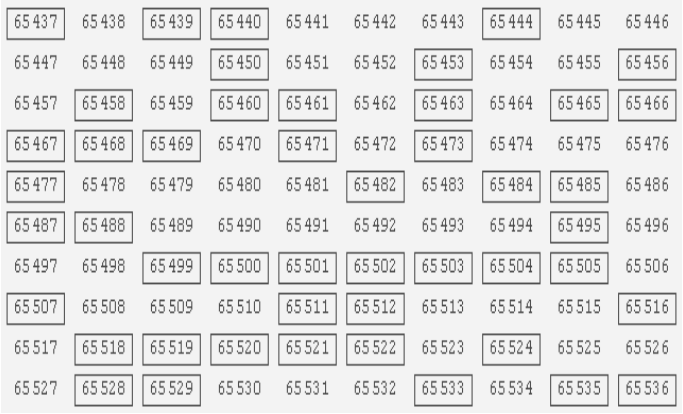
$\boxed{1}$	$\boxed{2}$	3	$\boxed{4}$	5	6	7	$\boxed{8}$	$\boxed{9}$	10	$\boxed{11}$	12	$\boxed{13}$	14	$\boxed{15}$	$\boxed{16}$
$\boxed{17}$	$\boxed{18}$	19	20	$\boxed{21}$	$\boxed{22}$	$\boxed{23}$	24	$\boxed{25}$	$\boxed{26}$	27	28	$\boxed{29}$	$\boxed{30}$	$\boxed{31}$	$\boxed{32}$
33	$\boxed{34}$	$\boxed{35}$	$\boxed{36}$	37	38	39	40	41	$\boxed{42}$	43	$\boxed{44}$	45	$\boxed{46}$	47	48
$\boxed{49}$	$\boxed{50}$	51	$\boxed{52}$	53	54	55	56	$\boxed{57}$	$\boxed{58}$	$\boxed{59}$	$\boxed{60}$	$\boxed{61}$	$\boxed{62}$	63	$\boxed{64}$
65	66	$\boxed{67}$	$\boxed{68}$	69	$\boxed{70}$	71	$\boxed{72}$	$\boxed{73}$	74	75	76	77	78	$\boxed{79}$	80
$\boxed{81}$	82	83	$\boxed{84}$	85	86	87	$\boxed{88}$	$\boxed{89}$	90	91	$\boxed{92}$	93	94	$\boxed{95}$	96
97	$\boxed{98}$	$\boxed{99}$	$\boxed{100}$	101	102	103	$\boxed{104}$	105	106	107	108	109	110	$\boxed{111}$	112
$\boxed{113}$	$\boxed{114}$	115	$\boxed{116}$	$\boxed{117}$	$\boxed{118}$	119	$\boxed{120}$	$\boxed{121}$	$\boxed{122}$	$\boxed{123}$	$\boxed{124}$	125	126	127	$\boxed{128}$
$\boxed{129}$	130	131	132	$\boxed{133}$	$\boxed{134}$	$\boxed{135}$	$\boxed{136}$	$\boxed{137}$	138	$\boxed{139}$	$\boxed{140}$	$\boxed{141}$	142	$\boxed{143}$	$\boxed{144}$
145	$\boxed{146}$	147	148	149	150	151	152	$\boxed{153}$	154	155	156	$\boxed{157}$	$\boxed{158}$	$\boxed{159}$	160
161	$\boxed{162}$	163	164	$\boxed{165}$	166	167	$\boxed{168}$	$\boxed{169}$	170	171	172	$\boxed{173}$	174	175	$\boxed{176}$
177	$\boxed{178}$	179	180	181	182	183	$\boxed{184}$	$\boxed{185}$	186	$\boxed{187}$	188	$\boxed{189}$	$\boxed{190}$	191	192
$\boxed{193}$	194	$\boxed{195}$	$\boxed{196}$	$\boxed{197}$	$\boxed{198}$	$\boxed{199}$	$\boxed{200}$	201	202	203	204	$\boxed{205}$	206	$\boxed{207}$	$\boxed{208}$
209	210	$\boxed{211}$	212	$\boxed{213}$	214	$\boxed{215}$	216	217	218	219	220	$\boxed{221}$	$\boxed{222}$	$\boxed{223}$	224
$\boxed{225}$	$\boxed{226}$	$\boxed{227}$	$\boxed{228}$	229	230	$\boxed{231}$	$\boxed{232}$	233	$\boxed{234}$	$\boxed{235}$	$\boxed{236}$	237	238	$\boxed{239}$	$\boxed{240}$
$\boxed{241}$	$\boxed{242}$	243	$\boxed{244}$	245	$\boxed{246}$	247	$\boxed{248}$	$\boxed{249}$	250	251	252	$\boxed{253}$	254	$\boxed{255}$	$\boxed{256}$

Figure 4. Quadratic Residues and Primitive Roots of 257



$\boxed{1}$	$\boxed{2}$	3	$\boxed{4}$	5	6	7	$\boxed{8}$	$\boxed{9}$	10	11	12	$\boxed{13}$	14	$\boxed{15}$	$\boxed{16}$
$\boxed{17}$	$\boxed{18}$	$\boxed{19}$	20	$\boxed{21}$	22	23	24	$\boxed{25}$	$\boxed{26}$	27	28	29	$\boxed{30}$	31	$\boxed{32}$
$\boxed{33}$	$\boxed{34}$	$\boxed{35}$	$\boxed{36}$	$\boxed{37}$	$\boxed{38}$	39	40	41	$\boxed{42}$	43	44	45	46	47	48
$\boxed{49}$	$\boxed{50}$	51	$\boxed{52}$	$\boxed{53}$	54	$\boxed{55}$	56	57	58	59	$\boxed{60}$	61	62	63	$\boxed{64}$
65	$\boxed{66}$	67	$\boxed{68}$	$\boxed{69}$	$\boxed{70}$	$\boxed{71}$	$\boxed{72}$	73	$\boxed{74}$	75	$\boxed{76}$	$\boxed{77}$	78	$\boxed{79}$	80
$\boxed{81}$	82	83	$\boxed{84}$	85	86	$\boxed{87}$	88	89	90	91	92	$\boxed{93}$	94	95	96
$\boxed{97}$	$\boxed{98}$	99	$\boxed{100}$	101	102	$\boxed{103}$	$\boxed{104}$	105	$\boxed{106}$	$\boxed{107}$	108	$\boxed{109}$	$\boxed{110}$	111	112
113	114	$\boxed{115}$	116	$\boxed{117}$	118	119	$\boxed{120}$	$\boxed{121}$	122	$\boxed{123}$	124	125	126	127	$\boxed{128}$
$\boxed{129}$	130	131	$\boxed{132}$	133	134	$\boxed{135}$	$\boxed{136}$	137	$\boxed{138}$	139	$\boxed{140}$	$\boxed{141}$	$\boxed{142}$	143	$\boxed{144}$
$\boxed{145}$	146	147	$\boxed{148}$	149	150	151	$\boxed{152}$	$\boxed{153}$	$\boxed{154}$	$\boxed{155}$	156	$\boxed{157}$	$\boxed{158}$	159	160
$\boxed{161}$	$\boxed{162}$	163	164	165	166	167	$\boxed{168}$	$\boxed{169}$	170	$\boxed{171}$	172	173	$\boxed{174}$	175	176
$\boxed{177}$	178	179	180	$\boxed{181}$	182	$\boxed{183}$	184	185	$\boxed{186}$	187	188	$\boxed{189}$	190	$\boxed{191}$	192
$\boxed{193}$	$\boxed{194}$	$\boxed{195}$	$\boxed{196}$	$\boxed{197}$	198	$\boxed{199}$	$\boxed{200}$	$\boxed{201}$	202	$\boxed{203}$	204	$\boxed{205}$	$\boxed{206}$	207	$\boxed{208}$
209	210	211	$\boxed{212}$	213	$\boxed{214}$	$\boxed{215}$	216	$\boxed{217}$	$\boxed{218}$	$\boxed{219}$	$\boxed{220}$	$\boxed{221}$	222	223	224
$\boxed{225}$	226	$\boxed{227}$	228	$\boxed{229}$	$\boxed{230}$	231	232	$\boxed{233}$	$\boxed{234}$	$\boxed{235}$	236	237	238	$\boxed{239}$	$\boxed{240}$
$\boxed{241}$	$\boxed{242}$	243	244	245	$\boxed{246}$	$\boxed{247}$	248	$\boxed{249}$	250	251	252	$\boxed{253}$	254	$\boxed{255}$	$\boxed{256}$

Figure 5. First 256 Quadratic Residues and Primitive Roots of 65537



$\boxed{65437}$	65438	$\boxed{65439}$	$\boxed{65440}$	65441	65442	65443	$\boxed{65444}$	65445	65446
65447	65448	65449	$\boxed{65450}$	65451	65452	$\boxed{65453}$	65454	65455	$\boxed{65456}$
65457	$\boxed{65458}$	65459	$\boxed{65460}$	$\boxed{65461}$	65462	$\boxed{65463}$	65464	$\boxed{65465}$	$\boxed{65466}$
$\boxed{65467}$	$\boxed{65468}$	$\boxed{65469}$	65470	$\boxed{65471}$	65472	$\boxed{65473}$	65474	65475	65476
$\boxed{65477}$	65478	65479	65480	65481	$\boxed{65482}$	65483	$\boxed{65484}$	$\boxed{65485}$	65486
$\boxed{65487}$	$\boxed{65488}$	65489	65490	65491	65492	65493	65494	$\boxed{65495}$	65496
65497	65498	$\boxed{65499}$	$\boxed{65500}$	$\boxed{65501}$	$\boxed{65502}$	$\boxed{65503}$	$\boxed{65504}$	$\boxed{65505}$	65506
$\boxed{65507}$	65508	65509	65510	$\boxed{65511}$	$\boxed{65512}$	65513	65514	65515	$\boxed{65516}$
65517	$\boxed{65518}$	$\boxed{65519}$	$\boxed{65520}$	$\boxed{65521}$	$\boxed{65522}$	65523	$\boxed{65524}$	65525	65526
65527	$\boxed{65528}$	$\boxed{65529}$	65530	65531	65532	$\boxed{65533}$	65534	$\boxed{65535}$	$\boxed{65536}$

Figure 6. Last 100 Quadratic Residues and Primitive Roots of 65537

5.2. Analysis of the Proposed Scheme

As is shown in the tables above, the proposed scheme just need to compute the quadratic residues to find out the primitive roots of a given prime. While the existing scheme needs to compute $a^{\varphi(p)/2} \bmod p$ to confirm whether a is a primitive root modulo Fermat prime p, where$\varphi(p) = p - 1$grows larger as p becomes larger. So the computation is fairly large when p is a big number.

6. Conclusions and Future Works

In this paper, a simple searching scheme for finding the primitive roots modulo Fermat prime numbers is proposed. We prove the equivalence between the primitive roots and the quadratic nonresidues modulo Fermat prime numbers. Thus, the problem of searching primitive roots is translated into solving the quadratic residues modulo Fermat primes, which is a much easier problem, having very simple solutions. Furthermore, we can speed up the process of computing the quadratic residues modulo Fermat primes, using a special property displayed in Lemma 6. Later, we conduct some experiments to test our scheme. In our experiment, we find out nearly all primitive roots modulo different Fermat primes.

In conclusion, the proposed scheme improves the searching speed of finding the primitive roots modulo a special kind of prime, the Fermat primes. However, whether there is other Fermat primes remain unsolved, besides the known 5 numbers. In addition, developing a general algorithm to compute primitive roots is still considered as one of the most difficult problem in the field of number theory, despite the great efforts devoted into it.

Acknowledgements

This work is supported by National Natural Science Foundation of China (No.61173188 , No. 61173187 and No. 61403157), Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20133401110004), the 211 Project Foundation of Anhui University(No. 02303402).

References

[1] B. Richard P., and M. John M Pollard. "Factorization of the eighth Fermat number", Mathematics of Computation, vol. 36, no. 154, **(1981)**, pp. 627-630.

[2] A. K Lenstra,., H W Lenstra, Manasse, M. S., and Pollard, J. M. "The factorization of the ninth Fermat number", Mathematics of Computation, vol. 61, no. 203, **(1993**,pp. 319-349.

[3] R Crandall, J Doenias, C Norrie , and J Young, "The twenty-second Fermat number is composite", mathematics of computation, vol. 64, no. 210, **(1995)**, pp. 863-868,

[4] C Richard, E Mayer, and J Papadopoulos. "The twenty-fourth Fermat number is composite", Mathematics of computation, vol. 72, no. 243, **(2003)**, pp.1555-1572.

[5] A. Abatzoglou, A. Silverberg, A. V. Sutherland, A. Wong. "Deterministic elliptic curve primality proving for a special sequence of numbers", in Algorithmic Number Theory (ANTS X), Mathematical Sciences Publishers, pp. 1-20, (**2013**).

[6] S Alice. "Some Remarks on Primality and Elliptic Curves", Advances in Mathematics of Communications vol.8, no. 4, **(2014)**, pp. 427-436.

[7] B. Iain, and M Goetz. "Extending the Generalized Fermat Prime Number Search Beyond One Million Digits Using GPUs", Parallel Processing and Applied Mathematics. Springer Berlin Heidelberg, pp. 106-113, (**2014**).

[8] K Steven G., and H R. Parks. "Primality Testing", A Mathematical Odyssey. Springer US, pp. 255-275, (**2014**).

[9] G Kristina Leonidovna, and S Sergeevich Titov. "The equivalent problem of testing Fermat primes", Prikladnaya Diskretnaya Matematika. Supplement 7, **(2014)**, pp. 13-14.

[10] K M., Luca, F., Somer, L."17 Lectures on Fermat Numbers. From Number Theory to Geometry", Springer, New York, **(2001).** pp. 33-40.

[11] P Pollack, "Bounded gaps between primes with a given primitive root." Algebra & Number Theory vol.8, no. 7, **(2014)**, pp. 1769-1786.

[12] I Kenneth, and M Rosen. "A classical introduction to modern number theory. " vol. 84. Springer Science & Business Media, **(2013).**

Authors

Dalei Zhang, He received the B.S. degree in Department of Computer communication from Nanjing University of Posts and Telecommunications, China in 2001, and the M.S. degree in Department of Computer Application Technology from Nanjing University of Posts and Telecommunications, China in 2008. He is currently pursuing the PhD degree with Department of Computer science and technology in Anhui University. His research interests include information hiding, computer cryptography.

Hong Zhong, She has an M.S., Ph. D (Computer science and technology, Computer science and technology), currently, Professor of Anhui University, China. Her research interests include Network security, Authentication, Secret Sharing, Security of Cloud Computing, etc. She has 25 Years of experience in Teaching & Research. She has published more than 50 Research papers in International & National Journals and Conferences.