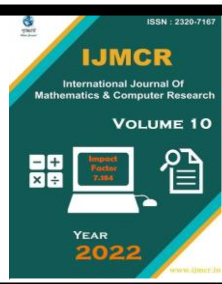
International Journal of Mathematics and Computer Research
ISSN: 2320-7167
Volume 10 Issue 02 February 2022, Page no. – 2579-2580
Index Copernicus ICV: 57.55, Impact Factor: 7.184
DOI: 10.47191/ijmcr/v10i2.05



Polynomial Factorization and Primality Criterion for Fermat Numbers

Oumar FALL[1], Chérif Bachir DEME[2]
[1]Mathematics department, Faculty of Sciences and Technology of Eucation and Training, Cheikh Anta Diop de Dakar University, Senegal
[2]Alioune Diop University of Bambey, Senegal

ARTICLE INFO	ABSTRACT
Published online 14 February 2022 Corresponding author: **Oumar FALL**	Let p be a prime integer and let $k \in \mathbb{N}$. We purpose a factorization of $X^{2k}+1 \pmod p$ allowing ti give a primality criterion for Fermat numbers. Mathematics Subject Classification 2010 11A07 11 A 51

KEYWORDS: Fermat numbers, Legendre's symbol, polynomials factorization, law of quadratic reciprocity

INTRODUCTION.

Fermat numbers were studied by many authors. We can cite J.C. Morehead, M. Mignotte, A.E. Western, G.A. Paxson, R.M. Robinson, etc...

Among them, some had to write about the criteria of primality. We have chosen here to give a primality criterion of Fermat numbers.

In section 1, we give some necessary background on Legendre's symbol used to prove our main results.

In section 2, we present the factorization of $X^{2k}+1 \pmod p$.

In section 3, we present a primality criterion of Fermat numbers.

1. Legendre's symbol.

Proposition 1.1. We have

$$\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8.$$

Proof

Let ζ be primitive root $8th$ of unity.

Then, ζ is a root of X^4+1. We consider $K = \mathbb{F}p$, $K0 = K(\zeta)$ and $\tau = \zeta + \zeta^{-1} \in K^0$. Then

$\tau^2 = \zeta^2 + \zeta^{-2} + 2 = \zeta^{-2}(1+\zeta^4)+2 = 2.$

- $p \equiv 1 \pmod 8$, $p = 8k+1$. We have $|K^?| = 8k$ and $K^?$ is cyclic, then $\zeta \in K$ and $\tau \in K$, then 2 is square. Example : $6^2 \equiv 2 \pmod{17}$.
- $p \equiv -1 \pmod 8$, $p = 8k-1$. Then $\zeta^p = \zeta^{8k-1} = \zeta^{-1}$; therefore $\tau^p = \zeta^p + \zeta^{-p} = \tau$; thus $\tau \in K$ and 2 is square. Example : $3^2 \equiv 2 \pmod 7$.
- $p \equiv 5 \pmod 8$, $p = 8k+5$. Then $\zeta^p = \zeta^{8k+5} = \zeta^4\zeta^{-1} = -\zeta$, therefore $\zeta \in 6\, K$ et 2 isn't square.
- $p \equiv -5 \pmod 8$, $p = 8k-5$. Thus $\zeta^p = \zeta^{-5} = -\zeta^{-1}$; we have $\tau^p = -\tau$ and 2 isn't square.

Proposition 1.2. We have

- $\left(\frac{-2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8.$
- $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod 4.$

2. Factorization of $X^{2k}+1 \pmod p$.

2.1. Factorization for $k = 1$ and $k = 2$

If $-1 \equiv a^2$, thus $X^2+1 = (X+a)(X-a)$.

If $2 = b^2$, $X^4+1 = (X^2+1)^2 - b^2X^2 = (X^2 - bX + 1)(X^2 + bX + 1)$.

If $-2 = c^2$, $X^4+1 = (X^2-1)^2 - c^2X^2 = (X^2 - cX - 1)(X^2 + cX - 1)$.

2.2. Factorization of $X^{2k}+1$

Suppose that $p \equiv 1 \pmod{2^{k+1}}$ and let g be a primitive root modulo p.

Thus $z = g^{\frac{(p-1)}{2^{k+1}}}$ is a 2^{k+1}th of unity.

This is valid for z^{2i+1}, where $i \in \{0,1,2,3,...,2^k-1\}$.

$$X^{2^k}+1 \equiv \prod_{i=0}^{2^k-1}(X - z^{2i+1}) \pmod p$$

Therefore.

Example : Let take $p = 17$; $p \equiv 1 \pmod{16}$.

If g is a primitive root modulo p, then $z = g^{\frac{(p-1)}{16}}$ is a 16th root of unity, as well as z^3, z5, z7, z9, z11, z13, z15.

And $X^8 + 1 \equiv \prod_{i=0}^{7}(X - z^{2i+1})$ is splitting completely.

Example, $3^4 \equiv 64 \equiv -4 \pmod{17}$, $3^8 \equiv 16 \equiv -1 \pmod{17}$.

Thus $X^8 + 1 = \prod_{i=0}^{7}(X - 3^{2i+1}) \pmod{17}$.

4. Primality criterion of Fermat numbers.

Let put $P_k(X) = X^{2k} + 1$. Then $P_k(2) = 2^{2k} + 1 = F_k$ allows to obtain all Fermat numbers.

We know that $F_k \equiv 1 \pmod{2^{k+1}}$; if F_k is prime, then it exists a 2^{k+1}th root of unity z such that $P_k(X)$ splits completely mod F_k.

REFERENCES

1. J.C. Morehead, Note on Fermat's numbers, Bull. Amer. Math. Soc.,v. 11, 1905, p. 543-545.
2. M. Mignotte, Mathematics for Computer Algebra, Springer-Verlag, New York, Inc, 1992.
3. J.C. Morehead and A.E. Western, Note on Fermat's numbers, Bull. Amer. Math. Soc. 16 (1909), *n*°1, 1-6.
4. G.A. Paxson, The compositeness of the thirteenth Fermat number, Math. Comp. 15 (1961), 420.
5. R.M. Robinson, Mersenne and Fermat numbers, Proc. Amer. Math. Soc. 5 (1954), 842-846.
6. S. Roman, Coding and Information theory; Irvine, Springer-Verlag, New York Berlin Heidelberg London Paris Tokyo Hong Kong Barcelona Budapest, 1991.