Hiroshima Math. J.
**41** (2011), 409–414

# A family of entire functions which determines the splitting behavior of polynomials at primes

Hajime Kuroiwa

(Received July 30, 2010)
(Revised March 28, 2011)

**Abstract.** In this paper, we prove that there exist entire functions which determines the splitting behavior of polynomials at prime. First, to any monic irreducible polynomial and any prime $p$, we associate a function defined on the set of primes which determines whether the polynomial splits completely at $p$ or not. Then we extend them to entire functions.

## 1. Introduction

In an introductory article by Professor Ihara, a problem is introduced. To describe it, let us employ the following notation.

Notation 1. Let $P$ be the set of prime numbers. Let $f(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial. We define $P_f$ to be the set of prime numbers $p$ such that $f(x)$ splits completely on $\mathbf{F}_p$.

Definition 2. A sequence of prime numbers $\{p_i\}$ is said to be of **completely splitting type** if for any monic irreducible $f(x)$, there exists $N_f$ such that $n \geq N_f$ implies $p_n \in P_f$.

Problem 1 [1, Problem 3.1]. *Can we construct a family $\mathscr{F}$ of countably many complex valued functions which satisfies the following condition: For any sequence $\{p_i\}$ of prime numbers,*
*$\{p_i\}$ is of completely splitting type $\Leftrightarrow$*
*For any $F \in \mathscr{F}$, there exists a number $M_F$ such that $n \geq M_F$ implies*

$$F(p_n) = 0.$$

To solve the above problem affirmatively, we prove the following theorem.

Theorem 2. *Let $u(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree $d$. Then there exist holomorphic functions $F_{u,0}, F_{u,1}, \dots, F_{u,d-1}$ on $\mathbf{C}^{\times}$ such that for*

2010 *Mathematics Subject Classification.* 11A41, 11A51.
*Key words and phrases.* entire function, completely splitting, non-abelian class field theory.

*any prime $p$, $u(x)$ splits completely on $\mathbf{F}_p$ if and only if $F_{u,0}(p) = 0$, $F_{u,1}(p) = 0, \dots, F_{u,d-1}(p) = 0$.*

The functions $F_{u,1}, \dots, F_{u,d-1}$ are entire functions on $\mathbf{C}$. We may replace $F_{u,0}$ in Theorem 2 by two other entire functions $G_u$ and $G_{u^{(1)}}$, and may use only entire functions. Theorem 3 gives an affirmative answer to Problem 1 as follows. Indeed, we put

$$\mathscr{F} = \bigcup_{d \geq 1} \mathscr{F}_d$$

$$\mathscr{F}_d = \{G_u, G_{u^{(1)}}, F_{u,1}, \dots, F_{u,d-1} \mid u \in \mathbf{Z}[x] : \text{monic irreducible, } \deg u = d\}.$$

Then we see that $\mathscr{F}$ satisfies the required condition. Indeed, we notice that $\mathscr{F}$ is denumerable. Then we use the relation

$$p \in P_u \Leftrightarrow G_u(p) = 0, \qquad G_{u^{(1)}}(p) = 0, \qquad F_{u,1}(p) = 0, \dots, F_{u,d-1}(p) = 0$$

in Theorem 3. Professor Ihara raised this problem to be solved by some non-abelian class field theory. Thus, the proof here must not be what he wanted to mean. Anyway, it would be not too bad to give an elementary proof.

## 2. The function $r_u$ associated by a polynomial $u$

DEFINITION 3. Let $u(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree $d$. Let

$$u(x) = \prod_{j=1}^{d} (x - \alpha_j)$$

be the factorization of $u(x)$ over $\mathbf{C}$. Let $r_u^{(p)}(x)$ be the remainder of $x^p$ divided by $u(x)$.

$$x^p \equiv r_u^{(p)}(x) \bmod u(x), \qquad \deg r_u^{(p)}(x) < d$$

It is worth while to note that the computation above may be done over $\mathbf{Z}$ (instead of the field $\mathbf{F}_p$). Now, we extend the polynomial $r_u^{(p)}(x)$. We compute $r_u^{(p)}(x)$ in terms of the roots of $u(x)$:

PROPOSITION 1 (Lagrangian interpolation). *Let $u(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree $d$ and let $\alpha_1, \dots, \alpha_d$ be the roots of $u(x)$. Then*

$$(1) \quad r_u^{(p)}(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)}.$$

Proof. Let us put

$$h(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)} - r_u^{(p)}(x).$$

Then we have $\deg h(x) \leq d - 1$, $h(\alpha_j) = 0$. We thus conclude that $h(x) = 0$. $\square$

Proposition 2. *Let $u(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree $d$. Then:*

(i) *For $u(x) \in \mathbf{Z}[x]$, there exists an entire function $r_u^{(z)}(x)$ in $z$ whose special values at primes are equal to the value of $r_u^{(p)}(x)$.*

(ii) *$u(x)$ splits completely on $\mathbf{F}_p \Leftrightarrow r_u^{(p)}(x) = x$ on $\mathbf{F}_p$.*

By using equation (1) and by choosing a logarithm $\log(\alpha_j)$ of $\alpha_j$ for each $j$, we may extend the function $r_u^{(p)}(x)$ to an entire function in complex variable $p$.

Definition 4. Under the same assumption as in Proposition 2, We define $g_{u,i}^{(p)}$ to be the coefficients of the polynomial $r_u^{(p)}(x)$ in $x$. In other words, we put

$$(2) \quad r_u^{(p)}(x) = \sum_{i=0}^{d-1} g_{u,i}^{(p)} x^i.$$

## 3. Proof of Theorem 2

Proof. Let us define

$$F_{u,i}(p) = \exp\left(\frac{2\pi\sqrt{-1}}{p}(g_{u,i}^{(p)} - \delta_{i,1})\right) - 1$$

where $g_{u,i}^{(p)}$ is the entire function in $p$-variable defined by the equation (2) in Definition 4. So, $F_{u,i}(p) = 0$ if and only if $g_{u,i}^{(p)} - \delta_{i,1}$ is divisible by $p$. Thus, $F_{u,i}(p) = 0$ for all $0 \leq i \leq d - 1$ if and only if $r_u^{(p)}(x) - x$ is divisible by $p$, namely $x^p - x \bmod p$ is divisible by $u(x) \bmod p$, which is equivalent to the completely splitting property at $p$. $\square$

## 4. Use of entire functions

The functions $F_{u,i}(p)$ in Theorem 2 are surely holomorphic functions on $\mathbf{C}^\times$. But they may have singularities at the origin. We may modify our functions so that we only make use of entire functions.

DEFINITION 5. Let $u(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree $d$. Then we define

$$u^{(1)}(x) := u(x+1)$$

$$G_u(p) := (F_{u,0}(p)+1)(F_{u,1}(p)+1) - 1.$$

THEOREM 3. *Let $u(x) \in \mathbf{Z}[x]$ be a monic irreducible polynomial of degree $d$. Then*

(i) *$F_{u,2}(p), \dots, F_{u,d-1}(p)$, $G_u(p)$ are entire functions.*

(ii) *$u(x)$ splits completely on $\mathbf{F}_p \Leftrightarrow F_{u,2}(p) = 0, \dots, F_{u,d-1}(p) = 0$, $G_u(p) = 0$, $G_{u^{(1)}}(p) = 0$.*

PROOF. (i) We may compute so that

$$r_u^{(0)}(x) = \sum_{j=1}^{d} \frac{u(x)}{u'(\alpha_j)(x-\alpha_j)} = 1$$

holds. Thus,

$$g_{u,0}^{(0)} = 1, g_{u,1}^{(0)} = 0, \dots, g_{u,d-1}^{(0)} = 0.$$

Therefore,

$$F_{u,2}(p), \dots, F_{u,d-1}(p), \qquad G_u(p) = \exp\left(\frac{2\pi\sqrt{-1}}{p}(g_{u,0}^{(p)} + g_{u,1}^{(p)} - 1)\right) - 1$$

are entire functions.

(ii) ($\Leftarrow$) obvious from Theorem 2.

($\Rightarrow$) From the definition of $F_{u,i}(p)$ and $G_u(p)$, we see that

$$x^p = ax + (1-a) \mod u(x), \ \ p$$

holds. We have furthermore

$$(x+1)^p = ax + 1 \mod u^{(1)}(x), \ \ p.$$

Namely, we have

$$x^p = ax \mod u^{(1)}(x), \ \ p.$$

Therefore, we conclude that $r_u^{(p)}(x) = x$ on $\mathbf{F}_p$. □

## 5. Example

(1) The case of $u(x) = x^2 - l$ ($l \in \mathbf{Z}$). We may easily compute by using equation (1) so that

$$r_u^{(p)}(x) = l^{(p-1)/2}x, \qquad g_{u,0}^{(p)} = 0, \qquad g_{u,1}^{(p)} = l^{(p-1)/2}$$

holds. Then we see that $F_{u,i}(p)$ and $G_u(p)$ are given as follows:

$$F_{u,0}(p) = 0, \qquad F_{u,1}(p) = G_u(p) = \exp\left(\frac{2\pi\sqrt{-1}}{p}(l^{(p-1)/2} - 1)\right) - 1.$$

The reader may easily verify that

$$u(x) \text{ splits completely on } \mathbf{F}_p \Leftrightarrow \left(\frac{l}{p}\right) = 1 \Leftrightarrow F_{u,1}(p) = 0.$$

($\left(\frac{l}{p}\right)$ is the quadratic residue symbol.)

NOTE 4. *In general, if* $\mathbf{Q}[x]/u(x)$ *is abelian extension, then by the class field theory, it is known already that* Theorem 2 *is solved by periodic functions like*

$$F_m(p) = \exp\left(\frac{2\pi\sqrt{-1}}{m}(p-1)\right) - 1$$

*instead of our complicated function* $F_{u,i}$. *See* [1, §3], [3, I §10, VI].

(2) The case of $u(x) = x^2 - x - 1$. We may compute similarly

$$r_u^{(p)}(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)} = F_p x + F_{p-1}$$

when $F_n$ is the $n$-th Fibonacci numbers. $r_u^{(p)}$ in this case somehow inherits the properties of the Fibonacci numbers. We may thus expect that even for a general $u$, our function $F_{u,i}$ has rich contents as the Fibonacci numbers have.

(3) The case of $u(x) = x^3 - l$.

$$\begin{aligned} r_u^{(p)}(x) &= \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)} = \sum_{j=1}^{3} \frac{1}{3}\alpha_j^{p-2} \frac{u(x)}{(x - \alpha_j)} \\ &= \frac{1}{3} l^{(p-2)/3}(1 + \omega^{p-2} + \omega^{2(p-2)})x^2 + \frac{1}{3} l^{(p-1)/3}(1 + \omega^{p-1} + \omega^{2(p-1)})x \end{aligned}$$

(4) The case of $u(x) = x^n - l$.

$$r_u^{(p)}(x) = \sum_{j=1}^{d} \frac{\alpha_j^p u(x)}{u'(\alpha_j)(x - \alpha_j)} = \sum_{j=1}^{n} \frac{1}{n}\alpha_j^{p-n+1} \frac{u(x)}{(x - \alpha_j)}$$

## References

[1] Y. Ihara, "Koremoaremo...imadatoketeimasen (Neither this nor that is yet solved)" (in Japanese), Suurikagaku (Mathematical science), saiensu-sya, Tokyo, August 1994.

[2] D. E. Knuth, The Art of Computer Programming volume 2 SEMINUMERICAL ALGORITHMS Arithmetic, Addison-Wesley, 1969.
[3] J. Neukirch, Algebraische Zahlentheorie, Springer-Verlag, 1992.

*Hajime Kuroiwa*
*Department of Mathematics*
*Faculty of Science*
*Kochi University*
*Kochi,* 780-8520*, Japan*
*E-mail: b10d6a05@s.kochi-u.ac.jp*