Tohoku Math. J.
51 (1999), 75–79

HYPERGEOMETRIC POLYNOMIALS OVER FINITE FIELDS

MASAO KOIKE*

(Received August 25, 1997, revised June 12, 1998)

Abstract. Honda found certain hypergeometric polynomials over the prime field which can be expressed as a product of linear factors. In this paper we give a different proof of his result by using elementary functions described by hypergeometric series of Gauss. We can find another hypergeometric polynomials which Honda missed.

Introduction. Let p be any odd prime and let $\boldsymbol{F}_p$ denote the prime field of characteristic p. For any a in $\boldsymbol{F}_p$ and $0 \leq n \in \boldsymbol{Z}$, we put $(a)_0 = 1$ and $(a)_n = a(a+1)\cdots(a+n-1)$ if $n \geq 1$. For any a, b, c in $\boldsymbol{F}_p$, we define the hypergeometric polynomials over the finite field $\boldsymbol{F}_p$ by

$$\boldsymbol{F}(a, b, c; x) = \sum_{n=0} \frac{(a)_n (b)_n}{(1)_n (c)_n} x^n ,$$

where we stop the sum as soon as the numerator vanishes and assume that the denominator does not vanish before the numerator does.

These polynomials have already appeared in Deuring [1], Igusa [4], Ihara [5], Honda [3] and others.

Honda [3] proved the following result: Let $p \geq 5$ and let ϕ denote the Legendre character of $\boldsymbol{F}_p$. For any $\varepsilon, \varepsilon' \in \{1, -1\}$, we define

$$S_{\varepsilon,\varepsilon'} = \{a \in \boldsymbol{F}_p^{\times} \mid \phi(a) = \varepsilon, \phi(1-a) = \varepsilon'\} ,$$

$$F_{\varepsilon,\varepsilon'}(x) = \prod_{a \in S_{\varepsilon,\varepsilon'}} (x - a) .$$

Then Honda proved:

THEOREM 0.1 (Honda).

$$F_{-1,-1}(x) = a^{(p)}_{-1,-1} \cdot \boldsymbol{F}\left(-\frac{1}{4}, \frac{1}{4}, \frac{1}{2}; x\right),$$

$$F_{-1,1}(x) = a^{(p)}_{-1,1} \cdot \boldsymbol{F}\left(\frac{1}{4}, \frac{3}{4}, \frac{3}{2}; x\right),$$

where $a^{(p)}_{\varepsilon,\varepsilon'}$ *is a constant which takes value* 1, 2 *or* 1/2.

* This research was partially supported by the Grant-in-Aid for Scientific Research, The Ministry of Education, Science, Sports and Culture, Japan.

1991 *Mathematics Subject Classification.* Primary 11T06.

Honda proved these identities by showing that these polynomials satisfy the same differential equation of degree 2. Thus his proof does not clarify the meaning of these identities. He also mentioned that the remaining two polynomials should not have these descriptions by hypergeometric polynomials.

Contrary to his remark, we prove:

THEOREM 0.2.

$$F_{1,-1}(x)=a_{1,-1}^{(p)}\cdot F\left(\frac{1}{4},\frac{3}{4},\frac{1}{2};x\right),$$

$$F_{1,1}(x)=a_{1,1}^{(p)}\cdot F\left(\frac{3}{4},\frac{5}{4},\frac{3}{2};x\right),$$

where $a_{1,-1}^{(p)}$ *is equal to* 1 *if* $p\equiv 1 \pmod 4$ *and* -2 *if* $p\equiv 3 \pmod 4$ *and* $a_{1,1}^{(p)}$ *is equal to* 1 *if* $p\equiv 1 \pmod 4$ *and* $-1/2$ *if* $p\equiv 3 \pmod 4$.

Our method of proof is to use elementary functions described by hypergeometric series of Gauss [2];

$$(1)\qquad (t+u)^n+(t-u)^n=2t^n\,{}_2F_1\left(-\frac{1}{2}n,\ -\frac{1}{2}n+\frac{1}{2},\ \frac{1}{2};\ \frac{u^2}{t^2}\right),$$

$$(2)\qquad (t+u)^n-(t-u)^n=2nt^{n-1}u\,{}_2F_1\left(-\frac{1}{2}n+\frac{1}{2},\ -\frac{1}{2}n+1,\ \frac{3}{2};\ \frac{u^2}{t^2}\right).$$

The polynomials on the left hand side are cyclotomic polynomials, so the above results seem to be connected with the theory of cyclotomic fields.

1. Proof of Theorem 0.2. Let $f=(p-1)/2$. We quote the following identity from [3, p. 183]:

$$F_{-1,-1}(x)^2=\text{const}\cdot\frac{(x^f+1)((1-x)^f+1)}{x^f+(1-x)^f}.$$

Hence we know the degree of $F_{-1,-1}(x)$. Since $\deg F_{-1,-1}(x)+\deg F_{1,-1}=\deg F_{1,-1}(x)+\deg F_{1,1}(x)=p-2$, we get

PROPOSITION 1.1.

$$\deg F_{1,1}(x)=\begin{cases} f/2-1, & \text{if } p\equiv 1 \pmod 4,\\ (f-1)/2, & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

$$\deg F_{1,-1}(x)=\begin{cases} f/2, & \text{if } p\equiv 1 \pmod 4,\\ (f-1)/2, & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

First we prove Theorem 0.2 for $F_{1,-1}(x)$. Take the identity (1) for $n=f$ and $t=1$.

Then, taking reduction mod p, we obtain a new identity in $\boldsymbol{F}_p[u]$:

$$(1+u)^f+(1-u)^f=2\boldsymbol{F}\left(\frac{1}{4},\frac{3}{4},\frac{1}{2};u^2\right). \tag{3}$$

Assume that $p\equiv 1 \pmod 4$. Let $g(u)$ denote the left hand side of (3). It is clear that $g(\alpha)=0$ implies that $g(-\alpha)=0$. Also, 0, 1 and -1 are not roots of $g(u)=0$.

LEMMA 1.2.

$$S_{1,-1}=\{\alpha^2 \mid g(\alpha)=0\}.$$

PROOF. Let α be a root of $g(u)=0$ and put $\beta=(1+\alpha)/(1-\alpha)$. Then $g(\alpha)=0$ is equivalent to $\beta^f+1=0$, which implies that β belongs to the prime field and $\phi(\beta)=-1$. Since $\alpha=(\beta-1)/(1+\beta)$, α belongs to $\boldsymbol{F}_p$ and $1-\alpha^2=(4\beta)/(1+\beta)^2$. Therefore $\phi(1-\alpha^2)=\phi(\beta)=-1$, and α^2 belongs to $S_{1,-1}$. Since $-\alpha=(1/\beta-1)/(1+1/\beta)$, both β and $1/\beta$ correspond to α^2. Hence the number of different α^2 is $f/2$, which is equal to the cardinality of $S_{1,-1}$ by Proposition 1.1.

Since f is even, we get

$$(1+u)^f+(1-u)^f=2F_{1,-1}(u^2). \tag{4}$$

From (3), it follows that

$$F_{1,-1}(x)=\boldsymbol{F}\left(\frac{1}{4},\frac{3}{4},\frac{1}{2};x\right). \tag{5}$$

This completes the proof in this case.

Assume that $p\equiv 3 \pmod 4$. Then f is odd, hence the degree of $g(u)$ is $f-1$, which is even. Then an argument similar to the proof of Lemma 1.2 shows that the statement in Lemma 1.2 is also true in this case. Since the coefficient of u^{f-1} in $g(u)$ is $p-1$, we get

$$(1+u)^f+(1-u)^f=-F_{1,-1}(u^2). \tag{6}$$

From (3), we get

$$F_{1,-1}(x)=-2\boldsymbol{F}\left(\frac{1}{4},\frac{3}{4},\frac{1}{2};x\right). \tag{7}$$

Now we prove Theorem 0.2 for $F_{1,1}(x)$.

Take the identity (2) for $n=f$ and $t=1$. Taking reduction modulo p, we obtain a new identity in $\boldsymbol{F}_p[u]$:

$$(1+u)^f-(1-u)^f=-u\boldsymbol{F}\left(\frac{3}{4},\frac{5}{4},\frac{3}{2};u^2\right). \tag{8}$$

Put

$$g(u)=\frac{(1-u)^f-(1+u)^f}{u}.$$

Then, by the same argument as above, we can prove

$$S_{1,1}=\{\alpha^2 \mid g(\alpha)=0\}.$$

If $p\equiv 1 \pmod 4$, the degree of $g(u)$ is $f-2$ and the coefficient of u^{f-2} is 1, so

$$g(u)=F_{1,1}(u^2). \tag{9}$$

From (8), it follows that

$$F_{1,1}(x)=\boldsymbol{F}\left(\frac{3}{4},\frac{5}{4},\frac{3}{2};x\right). \tag{10}$$

If $p\equiv 3 \pmod 4$, the degree of $g(u)$ is $f-1$, and the coefficient of u^{f-1} is -2, so

$$g(u)=-2F_{1,1}(u^2). \tag{11}$$

Hence, we get

$$F_{1,1}(x)=-\frac{1}{2}\boldsymbol{F}\left(\frac{3}{4},\frac{5}{4},\frac{3}{2};x\right). \tag{12}$$

This completes the proof of Theorem 0.2.

REMARK. Honda's theorem can also be proved by our method. The identities in $\boldsymbol{F}_p[u]$ which are used to prove his theorem are the following:

$$(1+u)^{(p+1)/2}+(1-u)^{(p+1)/2}=2\boldsymbol{F}\left(-\frac{1}{4},\frac{1}{4},\frac{1}{2};u^2\right),$$

$$(1+u)^{(p+1)/2}-(1-u)^{(p+1)/2}=u\boldsymbol{F}\left(\frac{1}{4},\frac{3}{4},\frac{3}{2};u^2\right).$$

REMARK. There is another method to prove Honda's theorem, which uses Tschebysheff polynomials whose roots generate the maximal real subfields of cyclotomic fields. The fact that the decomposition of primes are completely known in these fields enables us to know the factorization of the reduction modulo p of Tschebysheff polynomials.

2. Generalization and comment. We understand that our theorem shows that all roots of certain hypergeometric polynomials belong to the prime field. We should remark that this resembles the fact that all roots of $\boldsymbol{F}(1/2, 1/2, 1; x)=0$ belong to the quadratic extension of the prime field, which are super-singular λ-invariants of elliptic curves ([1], [4]).

By our method of proof of Theorem 0.2, we can find a series of hypergeometric

polynomials whose roots belong to the prime field. For example, we can prove the following theorem.

THEOREM 2.1. *Let $p \geq 5$ be a prime. Let d be a positive even integer such that $d \mid (p-1)$. Then the roots of $\boldsymbol{F}(1/2d, 1/2d+1/2, 1/2; x)=0$ belong to the prime field.*

REFERENCES

[1] M. DEURING, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Hamb. 14 (1941), 197–272.
[2] C. GAUSS, Disquisitiones generales circa seriem infinitam $1+\alpha\cdot\beta/1\cdot\gamma x+\cdots$, Werke III, 125–162.
[3] T. HONDA, Algebraic differential equations, Symposia Math. 24 (1981), 169–203.
[4] J.-I. IGUSA, Class number of a definite quaternion with prime discriminant, Proc. Nat. Acad. Sci. U.S.A. 44 (1958), 312–314.
[5] Y. IHARA, Schwarzian equations, J. Fac. Sci. Univ. Tokyo, Sec. 1A 21-1 (1974), 97–118.

GRADUATE SCHOOL OF MATHEMATICS
KYUSHU UNIVERSITY
FUKUOKA, 812–8581
JAPAN

E-mail address: koike@math.kyushu-u.ac.jp