Some arithmetic properties of the Legendre polynomials

by

L. Carlitz (Durham, North Carolina)

1. The writer ([2], [3]) has indicated a connection between divisibility properties of the Legendre polynomial $P_m(a)$ for special values of a and the complex multiplication of elliptic functions. If $p = 2m+1$ is an odd prime, put

$$W_m(x) = \sum_{r=0}^{m} \binom{m}{r}^2 x^r. \tag{1.1}$$

Then we have

$$W_m(x) \equiv P_m(1-2x) \pmod{p} \tag{1.2}$$

and

$$W_m(x) = (1-x)^m P_m\left(\frac{1+x}{1-x}\right) = (x-1)^m P_m\left(\frac{x+1}{x-1}\right). \tag{1.3}$$

Assume that the elliptic function $\operatorname{sn} x$ admits of complex multiplication and let the period quotient belong to the imaginary quadratic field of discriminant d. If k^2 denotes the corresponding singular modulus, it is proved in [2] that

$$W_m(k^2) \equiv 0 \pmod{p}. \tag{1.4}$$

It is proved in [3] that, for example, when $p \equiv 3 \pmod{4}$, then $W_m(x)$ has the three linear factors $x+1$, $x-1$, $x+\frac{1}{2} \pmod{p}$; if the Legendre symbol $(-2/p) = -1$, then the quadratic x^2-6x+1 is a factor $(\operatorname{mod} p)$ of $W_m(x)$; if $(-3/p) = -1$, then $x^2-x+\frac{1}{16}$ is a factor $(\operatorname{mod} p)$ of $W_m(x)$.

It is not difficult to show that for $p \equiv 1 \pmod{4}$

$$P_m(3) \equiv W_m(-1) \equiv 2a \pmod{p}, \tag{1.5}$$

where a is the unique odd integer determined by

$$p = a^2+b^2, \quad a \equiv b+1 \pmod{p}. \tag{1.6}$$

In [4] the writer showed that for $p \equiv 1 \pmod{12}$ we have

$$P_m((-3)^{1/2}) \equiv W_m(-\omega) = -2u(c/p) \pmod{p} \tag{1.7}$$

where

$$c^2 \equiv 3, \quad \omega^2+\omega+1 \equiv 0 \pmod{p} \tag{1.8}$$

and u is determined by means of

$$p = u^2+3v^2, \quad u \equiv -1 \pmod{3}. \tag{1.9}$$

2. The proof of (1.7) depends upon Good's formula [6]

$$P_m(x) = \frac{1}{t}\sum_{r=0}^{t-1}\left\{x+(x^2-1)^{1/2}\cos\frac{2\pi r}{t}\right\}^m \qquad (t>m). \tag{2.1}$$

Mr. W. A. Al.-Salam has called the writer's attention to the following formula of Catalan [5]

$$P_m(x) = \frac{1}{2\pi}\int_0^{2\pi}\{(1+\cos\vartheta)x+i\sin\vartheta\}^m\,d\vartheta,$$

which has the finite analog

$$P_m(x) = \frac{1}{t}\sum_{r=0}^{t-1}\left\{\left(1+\cos\frac{2\pi r}{t}\right)x+i\sin\frac{2\pi r}{t}\right\}^m \qquad (t>m). \tag{2.2}$$

Comparing (2.2) with (2.1), the former has the advantage of not containing $(x^2-1)^{1/2}$. We now take $t=p-1$ in (2.2) and apply the method used in [4]. Put $\zeta = e^{2\pi i/(p-1)}$ and let Z denote the cyclotomic field $R(\zeta)$, where R is the rational field. Then if $\mathfrak{P}$ is a prime ideal divisor of (p) in Z, we have for some primitive root $g \pmod{p}$

$$\zeta = g \pmod{\mathfrak{P}}. \tag{2.3}$$

Thus

$$2\cos\frac{2\pi r}{p-1} = \zeta^r+\zeta^{-r}, \qquad 2i\sin\frac{2\pi r}{p-1} = \zeta^r-\zeta^{-r},$$

and (2.2) becomes in view of (2.3)

$$\begin{aligned}-P_m(a) &\equiv 2^{-m}\sum_{r=0}^{p-2}\{a(2+g^r+g^{-r})+(g^r-g^{-r})\}^m \\ &\equiv 2^{-m}\sum_{k=1}^{p-1}\{a(2+k+k^{-1})+(k-k^{-1})\}^m \pmod{p}.\end{aligned}$$

For brevity we put

$$\psi(a) = (a/p) \equiv a^m \pmod{p}. \tag{2.4}$$

Then

$$\begin{aligned}-P_m(a) &\equiv \psi(2)\sum_{k=1}^{p-1}\psi(k)\psi\{a(k^2+2k+1)+(k^2-1)\} \\ &\equiv \psi(2)\sum_{k=1}^{p-1}\psi(k(k+1))\psi(a(k+1)+(k-1)) \\ &\equiv \psi(2)\sum_{k\neq -1}\psi(k)\psi\left(a+\frac{k-1}{k+1}\right).\end{aligned}$$

Put

$$(k-1)/(k+1) = as \qquad (a \not\equiv 0 \pmod{p})$$

and the above congruence becomes

$$-P_m(a) \equiv \psi(-2)\sum_{s=0}^{p-1}\psi(s^2-1)\psi(a+s) \pmod{p}. \tag{2.5}$$

Alternatively this may be written as

$$-P_m(a) \equiv \psi(-2a)\sum_{s=0}^{p-1}\psi(a^2s^2-1)\psi(s+1) \pmod{p}. \tag{2.6}$$

Note that we have assumed $a \not\equiv 0 \pmod{p}$.

3. Suppose now that $p \equiv 1 \pmod{3}$ so that $\psi(-3) = 1$. Put

$$-3 \equiv c^2 \pmod{p} \tag{3.1}$$

and apply (2.6) with $a = c$. If we $s = 2/r-1$, we get

$$\begin{aligned}-P_m(c) &\equiv \psi(-2c)\sum_{r=1}^{p-1}\psi(2/r)\psi\{-3(2-r)^2-r^2\} \\ &\equiv \psi(2c)\sum_{r=0}^{p-1}\psi(2r)\psi(r^2-3r+3) \\ &\equiv \psi(c)\sum_{r=0}^{p-1}\psi((r+1)(r^2-r+1)) \\ &\equiv \psi(c)\sum_{r=0}^{p-1}\psi(r^3-1) \\ &\equiv \psi(c)\,2u,\end{aligned}$$

where u is defined by means of (1.9). Thus we have proved the congruence

$$P_m(c) \equiv -2u\psi(c) \pmod{p}, \tag{3.2}$$

where c satisfies (3.1) and u is defined by (1.9).

The formula (3.2) includes (1.7). This is a consequence of the evident fact that

$$2 = i(1-i)^2, \quad \psi(2) = \psi(i),$$

where $i^2 \equiv -1 \pmod{p}$ and $p \equiv 1 \pmod{4}$.

By employing Gauss's formula ([1], p.97)

$$F(2\alpha, 2\beta; \alpha+\beta+\tfrac{1}{2}; x) = F\big(\alpha, \beta; \alpha+\beta+\tfrac{1}{2}; 4x(1-x)\big), \tag{3.3}$$

we can obtain a number of results related to (3.2) in the case $p = 2m+1 = 4n+1 \equiv 1 \pmod{12}$. Indeed (3.3) implies

$$F(-m, -m; 1; x) \equiv F\big(-n, -n; 1; 4x(1-x)\big) \pmod{p};$$

by (1.1) this may be written in the form

$$W_m(x) \equiv W_n\big(4x(1-x)\big) \pmod{p}. \tag{3.4}$$

Now if $\omega^2+\omega+1 \equiv 0 \pmod{p}$, we have

$$P_m(c) \equiv W_m(-\omega).$$

Using (3.4) this becomes

$$P_m(c) \equiv W_n(4) \equiv \psi(2)\, W_n(\tfrac{1}{4}) \pmod{p}, \tag{3.5}$$

the second statement follows on reversing the series. But if we again use (3.4) we get

$$P_m(c) \equiv \psi(2)\, W_m\left(\frac{2-3^{1/2}}{4}\right) \equiv \psi(2)\, P_m\left(\frac{3^{1/2}}{2}\right) \pmod{p}. \tag{3.6}$$

Using (1.3), this becomes

$$P_m(c) \equiv \psi\left(\frac{2-3^{1/2}}{2}\right) W_m\big(-(2+3^{1/2})^2\big) \pmod{p}. \tag{3.7}$$

This process can be continued; for example we find

$$W_m\big(-(2+3^{1/2})^2\big) \equiv P_m(15+8\cdot 3^{1/2}).$$

Similarly when $p = 2m+1 = 4n+1$, we find that

$$W_m(-1) \equiv W_n(-8) \equiv (-2)^{-n} W_n(-\tfrac{1}{8}) \pmod{p}. \tag{3.8}$$

If n is even so that $2Rp$ then also

$$W_m(-1) \equiv (-2)^{-n} P_m\left(\frac{3}{2\cdot 2^{1/2}}\right) \equiv (-2)^n W_m\left(\frac{2\cdot 2^{1/2}-3}{4\cdot 2^{1/2}}\right) \pmod{p}. \tag{3.9}$$

The value of $W_m(-1)$ is furnished by (1.5) and (1.6).

We remark also that Clausen's formula ([1], p. 86)

$$\{F(\alpha, \beta; \alpha+\beta+\tfrac{1}{2}; x)\}^2 = F_2(2\alpha, 2\beta, \alpha+\beta; 2\alpha+2\beta, \alpha+\beta+\tfrac{1}{2}; x)$$

implies (for $p = 2m+1 = 4n+1$)

$$W_n^2(x) \equiv \sum_{r=0}^{m} (-1)^r \binom{m}{r}^3 x^r \pmod{p}. \tag{3.10}$$

Thus in particular by means of (3.5) and (3.8) we can determine the residues of

$$\sum_{r=0}^{m} (-1)^r \binom{m}{r}^3 2^{2r}, \qquad \sum_{r=0}^{m} \binom{m}{r}^3 2^{3r}$$

for $p \equiv 1 \pmod{12}$, $p \equiv 1 \pmod{4}$, respectively.

4. The congruence (2.6) can be verified in the following way. Using (2.4) we get

$$\sum_{s=0}^{p-1} \psi(a^2s^2-1)\,\psi(s+1) \equiv \sum_{s=0}^{p-1} (a^2s^2-1)^m (s+1)^m$$

$$\equiv \sum_{r=0}^{m} (-1)^{m-r} \binom{m}{r} a^{2r} \sum_{k=0}^{m} \binom{m}{k} \sum_{s=0}^{p-1} s^{2r+k}.$$

Since

$$\sum_{s=0}^{p-1} s^k \equiv \begin{cases} 0 & (p-1 \nmid k \text{ or } k = 0), \\ -1 & (p-1 \mid k,\quad k > 0), \end{cases}$$

the triple sum reduces to

$$\equiv -\sum_{r=0}^{m} (-1)^{m-r} \binom{m}{r} \binom{m}{2m-2r} a^{2r} \equiv -\sum_{r=0}^{m} (-1)^r \binom{m}{r} \binom{m}{2r} a^{-2r}$$

for any integer a not divisible by p. Since $p = 2m+1$, $m \equiv -\frac{1}{2} \pmod{p}$, so that

$$(-1)^r \binom{m}{r} \equiv (-1)^r \binom{-\frac{1}{2}}{\pi} \equiv 2^{-2r} \binom{2r}{r}, \qquad \binom{m}{2r} \equiv 2^{2r} \frac{\left(-\frac{m}{2}\right)\pi \left(-\frac{m-1}{2}\right)\pi}{(2r)!};$$

hence

$$(4.1)\qquad \sum_{s=0}^{p-1}\psi(a^2s^2-1)\psi(s+1) \equiv -F\left(-\frac{m}{2}, -\frac{m-1}{2}; 1; a^{-2}\right)$$

in the usual notation for hypergeometric functions. But ([7], p. 370, ex. 15)

$$P_m(x) = (2x)^m \binom{m-\frac{1}{2}}{m} F\left(-\frac{m}{2}, -\frac{m-1}{2}; -m+\frac{1}{2}; x^{-2}\right),$$

so that

$$(4.2)\qquad P_m(a) \equiv \psi(-2a)F\left(-\frac{m}{2}, -\frac{m-1}{2}; 1; a^{-2}\right).$$

Comparing (4.2) with (4.1) we get (2.6).

More generally it is clear that we have proved the identical congruence

$$(4.3)\qquad x^mP_m(x) \equiv -\psi(-2)\sum_{s=0}^{p-1}(s^2x^2-1)^m\psi(s+1) \pmod{p},$$

where x is an indeterminate. Indeed we have

$$(4.4)\qquad x^{m+k}P_{m-k}^{(1/2-k)}(x) \equiv -(-1)^m\binom{k+m}{m}\sum_{s=0}^{p-1}(s^2x^2-1)^m(s+1)^{m-k} \pmod{p},$$

where $P_m^{(\lambda)}$ is the ultraspherical polynomial ([7], p. 80) and k is an integer, $0 \leqslant k \leqslant m$.

We note also that the Jacobi polynomial ([7], p. 67)

$$P_n^{(\alpha,\beta)}(x) = \sum_{r=0}^{n}\binom{n+\alpha}{n-r}\binom{n+\beta}{r}\left(\frac{x-1}{2}\right)^r\left(\frac{x+1}{2}\right)^{n-r}$$

satisfies

$$(4.5)\qquad P_m^{(h-m,\,k-m)}(x) \equiv -\sum_{s=0}^{p-1}\left(1+\frac{x+1}{2}s^2\right)^h\left(1+\frac{x-1}{2}s^2\right)^k \pmod{p},$$

where h, k are non-negative integers such that $h+k < 2m$. More generally

$$(4.6)\qquad -\sum_{s=0}^{p-1}\left(1+\frac{x+1}{2}s^2\right)^h\left(1+\frac{x-1}{2}s^2\right)^k \equiv \sum_{0<tm\leqslant h+k} P_{tm}^{(h-tm,\,k-tm)}(x) \pmod{p},$$

for arbitrary non-negative integers h, k.

5. It is shown in [3], § 7 how irreducible factors $\pmod{p}$ of $W_m(x)$ can be obtained by making use of certain singular moduli; indeed the complete factorization is obtained for $p \leqslant 23$. We shall now carry out the factorization for $p = 29$ and 31. The following table, which holds for all $p \geqslant 3$, is useful.

condition	$-1Np$	factors	$x+1,\ x-2,\ x-\frac{1}{2}$,
,,	$-1Np$	,,	$x^2-34x+1$,
,,	$-2Np$	,,	x^2-6x+1,
,,	$-3Np$	,,	x^2-x+1,
,,	$-3Np$	,,	$x^2-x+\frac{1}{16}$,

It follows from (1.1), (1.2) and (1.3) that

$$(5.1)\qquad W_m(u) = u^mW_m\left(\frac{1}{u}\right),\quad W_m(u) \equiv (-1)^mW_m(1-u) \pmod{p}.$$

Thus each of the quadratic factors in the table (except x^2-x+1) gives rise to certain additional factors. For example when $p = 29$ we get the six (irreducible) quadratics

$$x^2-x+1,\quad x^2-6x+1,\quad x^2+4x-4,\quad x^2-x+7,\quad x^2-x-9,\quad x^2-16x+16.$$

Since $W_{14}(x)$ is of degree 14, only one additional quadratic remains to be found. To do this we compute a few additional singular moduli; the results will be used for $p = 31$ and can be applied to larger values of p.

We use the notation of Weber [8]:

$$(5.2)\qquad k^2k'^2 = \frac{16}{f^{24}((-m)^{1/2})},$$

$$(5.3)\qquad \frac{k'^4}{k^2}\cdot\frac{f_1^{24}((-n)^{1/2})}{16},$$

where of course $k^2+k'^2 = 1$. For example when $n = 2$, we have ([8], p. 721),

$$f_1((-2)^{1/2}) = 2^{1/4}.$$

Thus (5.3) yields $(k^2-1)^2 = 4k^2$, k^4-6k^2+1 in agreement with a previous result. Similarly for $n = 3$, we have $f((-3)^{1/2}) = 2^{1/3}$; using (5.2) we get $k^4-k^2+\frac{1}{16}$, which is again a known result.

For $n = 7$, we have $f((-7)^{1/2}) = 2^{1/2}$, so that

$$k^2k'^2 = 2^4/2^{12} = 1/256;$$

this leads to the quadratic factor

$$(5.4)\qquad x^2-x+1/256\qquad (-7Np).$$

For $n = 6$, we have

$$f_1^6((-6)^{1/2}) = 2(2+2^{1/2})$$

from which we get

$$(k^2-1)^2-(2+2^{1/2})^4k^2 = 0\,. \tag{5.5}$$

For $n = 5$, we have $f((-5)^{1/2}) = 1+5^{1/2}$, so that

$$k^4-k^2+\tfrac{1}{4}(9-4\cdot 5^{1/2})\,. \tag{5.6}$$

For $n = 10$, we have $2^{1/2}f_1^2((-10)^{1/2}) = 1+5^{1/2}$, which yields

$$(k^2-1)^2-\frac{(1+5^{1/2})^{12}}{2^{10}}k^2 = 0\,. \tag{5.7}$$

Now for $p = 29$ we have $-10N29$. Since $5 \equiv 11^2 \pmod{29}$, we find that (5.7) yields the quadratic factor $x^2+14x+1$, which is irreducible $(\bmod 29)$. We have therefore the following complete factorization

$$\begin{aligned} W_{14} \equiv{}& (x^2-x+1)(x^2-6x+1)(x^2+4x-4)(x^2-x+7)\times \\ &\times(x^2-x-9)(x^2-16x+16)(x^2+14x+1) \pmod{29}\,. \end{aligned} \tag{5.8}$$

For $p = 31$, we have from the first three lines of the table the factors

$$x+1\,,\quad x-2\,,\quad x-\tfrac{1}{2}\,,\quad x^2-3x+1\,,\quad x^2-6x+1\,; \tag{5.9}$$

note that

$$x^2-3x+1 \equiv (x+11)(x-14)\,,\qquad x^2-6x+1 \equiv (x+13)(x+12)\,. \tag{5.10}$$

In view of the second of (5.1) we get the additional linear factors

$$x-12\,,\quad x-13\,. \tag{5.11}$$

Again since $5 \equiv 6^2 \pmod{31}$ it is easily verified that (5.7) reduces to $2k^4-2k^2+1$, which yields the quadratic factor

$$x^2-x+\tfrac{1}{2}\,. \tag{5.12}$$

Employing (5.1) we get also

$$x^2-2x+2\,,\quad x^2+1\,. \tag{5.13}$$

Combining (5.9), (5.10), (5.11), (5.12), (5.13) we have finally the factorization

$$\begin{aligned} W_{15}(x) \equiv{}& (x+1)(x-2)(x-\tfrac{1}{2})(x+11)(x-14)(x+12)(x-12)\times \\ &\times(x+13)(x-13)(x^2-x+\tfrac{1}{2})(x^2-2x+2)(x^2+1) \pmod{31}\,. \end{aligned} \tag{5.14}$$

The factorizations (5.8) and (5.14) have been checked directly.

We remark that for $p \leqslant 31$, the irreducible factors of $W_m(x)$ are either linear or quadratic; indeed for $p \equiv 1 \pmod 4$, they are all quadratic. We note also that for $p = 47$, the first three lines of the table together with (5.1) give the 15 linear factors $x+1$, $x-2$, $x-\frac{1}{2}$, $x-7$, $x+20$, $x+6$, $x-21$, $x+8$, $x-9$, $x-17$, $x+11$, $x-12$, $x+16$, $x-4$, $x+3$, while the fourth line gives x^2-x+1. Now $-7N47$, but (5.4) yields nothing new; also $-6N47$ but (5.5) yields nothing.

References

[1] W. N. Bailey, *Generalized hypergeometric series*, Cambridge 1935.

[2] L. Carlitz, *The coefficients of singular elliptic functions*, Mathematische Annalen 127(1954), p. 162-169.

[3] — *Congruence properties of special elliptic functions*, Monatshefte für Mathematik 58(1954), p. 77-90.

[4] — *Some arithmetic properties of the Legendre polynomials*, Proceedings of the Cambridge Philosophical Society 53 (1957), p. 265-268.

[5] E. Catalan, *Nouvelles proprietés des fonctions X_n*, Mémoires de l'Academie Royale des Sciences, des lettres, et des beaux-arts de Belgique 47(1889), p. 3-24.

[6] I. J. Good, *A new finite series for Legendre polynomials*, Proceedings of the Cambridge Philosophical Society 51(1955), p. 385-388.

[7] G. Szegö, *Orthogonal polynomials*, New York 1939.

[8] H. Weber, *Lehrbuch der Algebra*, vol. 3, Braunschweig 1908.

DUKE UNIVERSITY

Reçu par la Rédaction le 20.5.1957