Legendre polynomials and Jacobsthal sums

Zhi-Hong Sun(孙智宏)
Huaiyin Normal University(淮阴师范学院)
http://www.hytc.edu.cn/xsjl/szh

Notation: $\mathbb{Z}$—the set of integers, $\mathbb{N}$—the set of positive integers, $[x]$— the greatest integer not exceeding x, $(\frac{a}{p})$—the Legendre symbol, R_p—the set of rational numbers whose denominator is coprime to p.

Keywords: congruence, Legendre polynomial, Jacobsthal sum, elliptic curve

Main references:

[S1] Z.H. Sun, Congruences concerning Legendre polynomials, Proc. Amer. Math. Soc. 139(2011), 1915-1929.

[S2] Z.H. Sun, Congruences concerning Legendre polynomials II, J. Number Theory 133(2013), 1950-1976.

[S3] Z.H. Sun, Congruences involving $\binom{2k}{k}^2\binom{3k}{k}$, J. Number Theory 133(2013), 1572-1595.

[S4] Z.H. Sun, Congruences concerning Legendre polynomials III, Int. J. Number Theory 9(2013), 965-999.

[S5] Z.H. Sun, Legendre polynomials and supercongruences, Acta Arith. 159(2013), 169-200.

§1. Cubic Jacobsthal sums

Let p be an odd prime and $m, n \in \mathbb{Z}$. The sums

$$\sum_{x=0}^{p-1} \left(\frac{x^3+mx}{p}\right) \quad \text{and} \quad \sum_{x=0}^{p-1} \left(\frac{x^3+n}{p}\right)$$

are called cubic Jacobsthal sums.

Let $A, B, C \in \mathbb{Z}$. The sum

$$\sum_{x=0}^{p-1} \left(\frac{x^3+Ax^2+Bx+C}{p}\right)$$

is called general cubic Jacobsthal sum.

Hasse's theorem: Let $p > 3$ be a prime, $A, B, C \in R_p$, and let D be the discriminant of x^3+Ax^2+Bx+C. If $D \not\equiv 0 \pmod{p}$, then

$$\left| \sum_{x=0}^{p-1} \left(\frac{x^3+Ax^2+Bx+C}{p}\right) \right| \leq 2\sqrt{p}.$$

For a prime $p > 3$ and $A, B, C \in R_p$ let $\#E_p(y^2 = x^3 + Ax^2 + Bx + C)$ be the number of points on the curve $E_p: \ y^2 = x^3 + Ax^2 + Bx + C$ over the field $\mathbb{F}_p$ of p elements. For $A, B, C \in R_p$, it is easily seen that

$$\begin{aligned}
&\#E_p(y^2 = x^3 + Ax^2 + Bx + C) \\
&= 1 + \sum_{\substack{x=0 \\ (\frac{x^3+Ax^2+Bx+c}{p})=0}}^{p-1} 1 + 2 \sum_{\substack{x=0 \\ (\frac{x^3+Ax^2+Bx+c}{p})=1}}^{p-1} 1 \\
&= p + 1 + \sum_{\substack{x=0 \\ (\frac{x^3+Ax^2+Bx+c}{p})=1}}^{p-1} 1 \\
&\quad - \sum_{\substack{x=0 \\ (\frac{x^3+Ax^2+Bx+c}{p})=-1}}^{p-1} 1 \\
&= p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + Ax^2 + Bx + C}{p} \right).
\end{aligned}$$

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field and the curve $y^2 = x^3 + mx + n$ has complex multiplication by an order in K. By Deuring's theorem, we have

$$\begin{aligned} &\#E_p(x^3 + mx + n) \\ &= \begin{cases} p + 1 & \text{if } p \text{ is inert in } K, \\ p + 1 - \pi - \bar{\pi} & \text{if } p = \pi\bar{\pi} \text{ in } K, \end{cases} \end{aligned}$$

where π is in an order in K and $\bar{\pi}$ is the conjugate number of π. If $4p = u^2 + dv^2$ with $u, v \in \mathbb{Z}$, we may take $\pi = \frac{1}{2}(u + v\sqrt{-d})$. Thus, (1.0)

$$\begin{aligned} &\sum_{x=0}^{p-1} \left(\frac{x^3 + mx + n}{p}\right) \\ &= \begin{cases} \pm u & \text{if } 4p = u^2 + dv^2 \text{ with } u, v \in \mathbb{Z}, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

In [Gr, Gross(1982)], [JM, Joux and Morain(1995)] and [PV, Padma and Venkataraman(1996)] the sign of u was determined for those imaginary quadratic fields K with class number 1. In [LM, Leprévost and Morain (1997)] and [I, Ishii(2004)] the sign of u was determined for imaginary quadratic fields K with class number 2.

From (1.0) and some known results we derive that

(1.1)
$$\sum_{x=0}^{p-1}\left(\frac{x^3-11x+14}{p}\right)$$
$$=\begin{cases}(-1)^{\frac{p+3}{4}}2a & \text{if } 4\mid p-1,\ p=a^2+b^2,\ 4\mid a-1,\\ 0 & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

(1.2)
$$\sum_{x=0}^{p-1}\left(\frac{x^3-15x+22}{p}\right)$$
$$=\begin{cases}-2A & \text{if } 3\mid p-1,\ p=A^2+3B^2 \text{ and } 3\mid A-1,\\ 0 & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

(1.3)

$$\sum_{x=0}^{p-1}\left(\frac{x^3-30x+56}{p}\right)$$

$$=\begin{cases}(-1)^{\frac{p+7}{8}}(\frac{3}{p})2c & \text{if } 8|p-1,\ p=c^2+2d^2,\ 4|c-1\\ (-1)^{\frac{p-3}{8}}(\frac{3}{p})2c & \text{if } 8|p-3,\ p=c^2+2d^2,\ 4|c-1\\ 0 & \text{if } p\equiv 5,7 \pmod 8.\end{cases}$$

(1.4)

$$\sum_{x=0}^{p-1}\left(\frac{x^3-35x+98}{p}\right)$$

$$=\begin{cases}(-1)^{\frac{p+1}{2}}2(\frac{C}{7})C & \\ \quad \text{if } p=C^2+7D^2\equiv 1,2,4 \pmod 7, & \\ 0 \quad \text{if } p\equiv 3,5,6 \pmod 7. & \end{cases}$$

(1.5)

$$\sum_{x=0}^{p-1}\left(\frac{x^3-595x+5586}{p}\right)$$
$$=\begin{cases}(-1)^{\frac{p+1}{2}}2C(\frac{C}{7})\\ \quad \text{if } p=C^2+7D^2\equiv 1,2,4 \pmod 7,\\ 0 \quad \text{if } p\equiv 3,5,6 \pmod 7.\end{cases}$$

(1.6)

$$\sum_{x=0}^{p-1}\left(\frac{x^3-120x+506}{p}\right)$$
$$=\begin{cases}(\frac{2}{p})L & \text{if } 3\mid p-1,\ 4p=L^2+27M^2,\ 3\mid L-1,\\ 0 & \text{if } p\equiv 2 \pmod 3.\end{cases}$$

I conjectured (1.6) in 2010 and proved it in 2011 by using Legendre polynomials and Jacobsthal sums.

It is also known that (J.C. Parnami and A.R. Rajwade, 1982)

(1.7)

$$\sum_{x=0}^{p-1}\left(\frac{x^3-96\cdot 11x+112\cdot 11^2}{p}\right)$$
$$=\begin{cases}(\frac{2}{p})(\frac{u}{11})u & \text{if } (\frac{p}{11})=1 \text{ and } 4p=u^2+11v^2,\\ 0 & \text{if } (\frac{p}{11})=-1\end{cases}$$

and that ([RPR,1984],[JM,1995],[PV,1996])

(1.8)

$$\sum_{x=0}^{p-1}\Big(\frac{x^3-8\cdot 19x+2\cdot 19^2}{p}\Big)$$
$$=\begin{cases}(\frac{2}{p})(\frac{u}{19})u & \text{if } (\frac{p}{19})=1 \text{ and } 4p=u^2+19v^2,\\ 0 & \text{if } (\frac{p}{19})=-1,\end{cases}$$

$$\sum_{x=0}^{p-1}\Big(\frac{x^3-80\cdot 43x+42\cdot 43^2}{p}\Big)$$
$$=\begin{cases}(\frac{2}{p})(\frac{u}{43})u & \text{if } (\frac{p}{43})=1 \text{ and } 4p=u^2+43v^2,\\ 0 & \text{if } (\frac{p}{43})=-1,\end{cases}$$

$$\sum_{x=0}^{p-1}\Big(\frac{x^3-440\cdot 67x+434\cdot 67^2}{p}\Big)$$
$$=\begin{cases}(\frac{2}{p})(\frac{u}{67})u & \text{if } (\frac{p}{67})=1 \text{ and } 4p=u^2+67v^2,\\ 0 & \text{if } (\frac{p}{67})=-1,\end{cases}$$

$$\sum_{x=0}^{p-1}\Big(\frac{x^3-80\cdot 23\cdot 29\cdot 163x+14\cdot 209\cdot 127\cdot 163^2}{p}\Big)$$
$$=\begin{cases}(\frac{2}{p})(\frac{u}{163})u & \text{if } (\frac{p}{163})=1 \text{ and } 4p=u^2+163v^2,\\ 0 & \text{if } (\frac{p}{163})=-1.\end{cases}$$

§2. **Congruences for** $\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p})$ (mod p)

Main problem: For a given odd prime p find a simple expression for $\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p})$ (mod p) without Legendre symbols.

Many mathematicians attacked this problem, but their formulas are complicated.

In 2006, using the theory of elliptic curves and differential equations P. Morton (JNT 120(2006), 234-271) obtained a general and explicit formula for $\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p})$ (mod p) in terms of certain Jacobi polynomials.

Morton (2006): Let $p > 3$ be a prime , $m, n \in R_p$ and $4m^3 + 27n^2 \not\equiv 0 \pmod{p}$. Then

$$\begin{aligned}
&\sum_{x=0}^{p-1} \left(\frac{x^3 + mx + n}{p}\right) \\
&\equiv -(-48m)^{\frac{1-(\frac{p}{3})}{2}} (864n)^{\frac{1-(\frac{-1}{p})}{2}} \\
&\quad \times (-16(4m^3 + 27n^2))^{[\frac{p}{12}]} \\
&\quad \times 1728^{[\frac{p}{12}]} P_{[\frac{p}{12}]}^{(-\frac{1}{3}(\frac{p}{3}), -\frac{1}{2}(\frac{-1}{p}))} \left(\frac{-4m^3 + 27n^2}{4m^3 + 27n^2}\right) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \pmod{p},
\end{aligned}$$

where $P_k^{(\alpha,\beta)}(x)$ is the Jacobi polynomial given by

$$P_k^{(\alpha,\beta)}(x) = \frac{1}{2^k} \sum_{r=0}^{k} \binom{k+\alpha}{r} \binom{k+\beta}{k-r} (x-1)^{k-r} (x+1)^r.$$

The Legendre polynomials $\{P_n(x)\}$ are given by

$$P_n(x) = P_n^{(0,0)}(x) = \frac{1}{2^n \cdot n!} \cdot \frac{d^n}{dx^n}(x^2-1)^n$$
$$= \frac{1}{2^n} \sum_{k=0}^{[n/2]} \binom{n}{k} (-1)^k \binom{2n-2k}{n} x^{n-2k}.$$

A famous formula due to Murphy states that

$$P_n(x) = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k} \left(\frac{x-1}{2}\right)^k.$$

We have $P_n(-x) = (-1)^n P_n(x)$ and

$$P_n(0) = \begin{cases} 0 & \text{if } 2 \nmid n, \\ \dfrac{1}{(-4)^m} \binom{2m}{m} & \text{if } n = 2m. \end{cases}$$

Theorem 2.1 ([S5 (Z.H. Sun, Acta Arith. 159(2013), 169-200), Theorem 2.1]). *Let $p > 3$ be a prime and $m, n \in R_p$ with $m \not\equiv 0 \pmod p$. Then*

$$\sum_{x=0}^{p-1}\left(\frac{x^3+mx+n}{p}\right)$$
$$\equiv\begin{cases} -(-3m)^{\frac{p-1}{4}}P_{[\frac{p}{6}]}(\frac{3n\sqrt{-3m}}{2m^2}) \pmod p & \text{if } 4\mid p-1,\\ -\dfrac{(-3m)^{\frac{p+1}{4}}}{\sqrt{-3m}}P_{[\frac{p}{6}]}(\frac{3n\sqrt{-3m}}{2m^2}) \pmod p & \text{if } 4\mid p-3.\end{cases}$$

I first deduced Theorem 2.1 by using Morton's work, and later found an elementary and straightforward (?) proof.

One can easily prove the following lemma.

Lemma 2.1. *Let p be an odd prime. Then*

(i) $\binom{\frac{p-1}{2}}{k} \equiv \frac{1}{(-4)^k}\binom{2k}{k} \pmod{p}$ *for* $k \le \frac{p-1}{2}$,

(ii) $\binom{\frac{p-1}{2}-k}{2k} \equiv \frac{\binom{6k}{3k}\binom{3k}{k}}{4^{2k}\binom{2k}{k}} \pmod{p}$ *for* $k \le \left[\frac{p}{6}\right]$,

(iii) $\binom{[\frac{p}{3}]+k}{2k} \equiv \frac{1}{(-27)^k}\binom{3k}{k} \pmod{p}$ *for* $k \le \left[\frac{p}{3}\right]$ $(p \ne 3)$.

Using Lemma 2.1 one can easily prove:

Lemma 2.2. *Let $p > 3$ be a prime and $k \in \{0, 1, \ldots, [\frac{p}{12}]\}$. Then*

$$\binom{[\frac{p}{6}]}{k}\binom{2[\frac{p}{6}]-2k}{[\frac{p}{6}]}$$

$$\equiv (-1)^{[\frac{p}{6}]}3^{3k+\frac{1-(\frac{p}{3})}{2}}4^{[\frac{p}{6}]-k}\binom{\frac{p-1}{2}}{[\frac{p}{3}]-k}\binom{\frac{p-(\frac{p}{3})}{6}+k}{3k+\frac{1-(\frac{p}{3})}{2}} \pmod{p}.$$

Proof of Theorem 2.1. For any positive integer k it is well known (see [IR, Lemma 2, p.235]) that

$$\sum_{x=0}^{p-1} x^k \equiv pB_k \equiv \begin{cases} p-1 \pmod{p} & \text{if } p-1 \mid k, \\ 0 \pmod{p} & \text{if } p-1 \nmid k. \end{cases}$$

For $k, r \in \mathbb{Z}$ with $0 \le r \le k \le \frac{p-1}{2}$ we have $0 \le k+2r \le \frac{3(p-1)}{2}$. Thus,

$$\sum_{x=0}^{p-1} x^{k+2r} \equiv \begin{cases} p-1 \pmod{p} & \text{if } k = p-1-2r, \\ 0 \pmod{p} & \text{if } k \neq p-1-2r \end{cases}$$

and therefore

(2.1)

$$\sum_{x=0}^{p-1}(x^3+mx+n)^{\frac{p-1}{2}}$$

$$=\sum_{x=0}^{p-1}\sum_{k=0}^{(p-1)/2}\binom{(p-1)/2}{k}(x^3+mx)^k n^{\frac{p-1}{2}-k}$$

$$=\sum_{x=0}^{p-1}\sum_{k=0}^{(p-1)/2}\binom{(p-1)/2}{k}\sum_{r=0}^{k}\binom{k}{r}x^{3r}(mx)^{k-r}n^{\frac{p-1}{2}-k}$$

$$=\sum_{r=0}^{\frac{p-1}{2}}\sum_{k=r}^{\frac{p-1}{2}}\binom{(p-1)/2}{k}\binom{k}{r}m^{k-r}n^{\frac{p-1}{2}-k}\sum_{x=0}^{p-1}x^{k+2r}$$

$$\equiv-\sum_{r=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{p-1-2r}\binom{p-1-2r}{r}m^{p-1-3r}n^{2r-\frac{p-1}{2}}$$

$$=-\sum_{\frac{p-1}{4}\le r\le\frac{p-1}{3}}\binom{\frac{p-1}{2}}{p-1-2r}\binom{p-1-2r}{r}$$

$$\times m^{p-1-3r}n^{2r-\frac{p-1}{2}}\pmod p.$$

If $n \equiv 0 \pmod p$, from the above we deduce that

$$\sum_{x=0}^{p-1}\Big(\frac{x^3+mx+n}{p}\Big) \equiv \sum_{x=0}^{p-1}(x^3+mx+n)^{\frac{p-1}{2}}$$
$$\equiv \begin{cases} -\binom{\frac{p-1}{2}}{\frac{p-1}{4}} m^{\frac{p-1}{4}} \pmod p & \text{if } 4 \mid p-1, \\ 0 \pmod p & \text{if } 4 \mid p-3. \end{cases}$$

Thus applying Lemma 2.2 (with $k = [\frac{p}{12}]$) we get

$$P_{[\frac{p}{6}]}(0) = \begin{cases} \dfrac{1}{(-4)^{[\frac{p}{12}]}}\binom{[\frac{p}{6}]}{[\frac{p}{12}]} \equiv (-1)^{[\frac{p}{12}]} 3^{\frac{p-1}{4}} \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \\ \equiv (-3)^{-\frac{p-1}{4}}\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod p \text{ if } 4 \mid p-1, \\ 0 \qquad \text{if } 4 \mid p-3. \end{cases}$$

Hence the result is true for $n \equiv 0 \pmod p$.

Now we assume $n \not\equiv 0 \pmod p$. From (2.1) we see that

$$
\begin{aligned}
&\sum_{x=0}^{p-1}\left(\frac{x^3+mx+n}{p}\right)\\
&\equiv\sum_{x=0}^{p-1}(x^3+mx+n)^{\frac{p-1}{2}}\\
&\equiv(p-1)\frac{m^{p-1}}{n^{\frac{p-1}{2}}}\sum_{\frac{p-1}{4}\le r\le\frac{p-1}{3}}\binom{\frac{p-1}{2}}{p-1-2r}\binom{p-1-2r}{r}\frac{n^{2r}}{m^{3r}}\\
&\equiv-\left(\frac{n}{p}\right)\sum_{\frac{p-1}{4}\le r\le\frac{p-1}{3}}\binom{(p-1)/2}{r}\binom{\frac{p-1}{2}-r}{p-1-3r}\left(\frac{n^2}{m^3}\right)^r\\
&=-\left(\frac{n}{p}\right)\sum_{k=0}^{[\frac{p}{12}]}\binom{\frac{p-1}{2}}{[\frac{p}{3}]-k}\binom{\frac{p-(\frac{p}{3})}{6}+k}{3k+\frac{1-(\frac{p}{3})}{2}}\left(\frac{n^2}{m^3}\right)^{[\frac{p}{3}]-k}\pmod p.
\end{aligned}
$$

On the other hand,

$$
\begin{aligned}
&P_{[\frac{p}{6}]}\Big(\frac{3n\sqrt{-3m}}{2m^2}\Big)\\
&= 2^{-[\frac{p}{6}]}\sum_{k=0}^{[\frac{p}{12}]}\binom{[\frac{p}{6}]}{k}(-1)^k\binom{2[\frac{p}{6}]-2k}{[\frac{p}{6}]}\Big(\frac{3n\sqrt{-3m}}{2m^2}\Big)^{[\frac{p}{6}]-2k}\\
&= 2^{-[\frac{p}{6}]}\sum_{k=0}^{[\frac{p}{12}]}\binom{[\frac{p}{6}]}{k}(-1)^k\binom{2[\frac{p}{6}]-2k}{[\frac{p}{6}]}\\
&\quad\times\Big(\frac{3n\sqrt{-3m}}{2m^2}\Big)^{\frac{1-(\frac{-1}{p})}{2}}\Big(-\frac{27n^2}{4m^3}\Big)^{[\frac{p}{12}]-k}\\
&= (-1)^{[\frac{p}{12}]}2^{-[\frac{p}{6}]}\sum_{k=0}^{[\frac{p}{12}]}\binom{[\frac{p}{6}]}{k}\binom{2[\frac{p}{6}]-2k}{[\frac{p}{6}]}\\
&\quad\times\Big(\frac{3n\sqrt{-3m}}{2m^2}\Big)^{\frac{1-(\frac{-1}{p})}{2}}\Big(\frac{27n^2}{4m^3}\Big)^{[\frac{p}{3}]-k-\frac{p-(\frac{-1}{p})}{4}}\\
&\equiv \delta(m,p)^{-1}\Big(\frac{n}{p}\Big)\Big(\frac{3}{p}\Big)(-1)^{[\frac{p}{12}]}2^{-[\frac{p}{6}]}\\
&\quad\times\sum_{k=0}^{[\frac{p}{12}]}\binom{[\frac{p}{6}]}{k}\binom{2[\frac{p}{6}]-2k}{[\frac{p}{6}]}\Big(\frac{27n^2}{4m^3}\Big)^{[\frac{p}{3}]-k}\pmod p,
\end{aligned}
$$

where

$$\delta(m,p)=\begin{cases}(-3m)^{\frac{p-1}{4}} & \text{if } p\equiv 1 \pmod 4,\\ \dfrac{(-3m)^{\frac{p+1}{4}}}{\sqrt{-3m}} & \text{if } p\equiv 3 \pmod 4.\end{cases}$$

Hence, by the above and Lemma 2.2 we get

$$\begin{aligned}&\delta(m,p)P_{[\frac{p}{6}]}\Big(\frac{3n\sqrt{-3m}}{2m^2}\Big)\\ &\equiv\Bigg(\sum_{k=0}^{[\frac{p}{12}]}(-1)^{[\frac{p}{6}]}3^{3k+\frac{1-(\frac{p}{3})}{2}}4^{[\frac{p}{6}]-k}\\ &\quad\times\binom{\frac{p-1}{2}}{[\frac{p}{3}]-k}\binom{\frac{p-(\frac{p}{3})}{6}+k}{3k+\frac{1-(\frac{p}{3})}{2}}\Big(\frac{27n^2}{4m^3}\Big)^{[\frac{p}{3}]-k}\Bigg)\\ &\quad\times\Big(\frac{n}{p}\Big)\Big(\frac{3}{p}\Big)(-1)^{[\frac{p}{12}]}2^{-[\frac{p}{6}]}\pmod p.\end{aligned}$$

Since

$$\left(\frac{3}{p}\right)(-1)^{[\frac{p}{12}]}2^{-[\frac{p}{6}]}(-1)^{[\frac{p}{6}]}3^{3k+\frac{1-(\frac{p}{3})}{2}}4^{[\frac{p}{6}]-k}\left(\frac{27}{4}\right)^{[\frac{p}{3}]-k}$$
$$= (-1)^{[\frac{p}{12}]+[\frac{p}{6}]}\left(\frac{3}{p}\right)2^{[\frac{p}{6}]-2[\frac{p}{3}]}3^{3[\frac{p}{3}]+(1-(\frac{p}{3}))/2}$$
$$= (-1)^{[\frac{p}{12}]+[\frac{p}{6}]}\left(\frac{3}{p}\right)2^{-\frac{p-1}{2}}3^{p-1}$$
$$\equiv (-1)^{[\frac{p}{12}]+[\frac{p}{6}]}\cdot(-1)^{\frac{p-(\frac{p}{3})}{6}}\cdot(-1)^{-[\frac{p+1}{4}]}$$
$$= (-1)^{2[\frac{p}{12}]} = 1 \pmod{p},$$

from the above we deduce that

$$\delta(m,p)P_{[\frac{p}{6}]}\left(\frac{3n\sqrt{-3m}}{2m^2}\right)$$
$$\equiv \left(\frac{n}{p}\right)\sum_{k=0}^{[\frac{p}{12}]}\binom{\frac{p-1}{2}}{[\frac{p}{3}]-k}\binom{\frac{p-(\frac{p}{3})}{6}+k}{3k+\frac{1-(\frac{p}{3})}{2}}\left(\frac{n^2}{m^3}\right)^{[\frac{p}{3}]-k}$$
$$\equiv -\sum_{x=0}^{p-1}\left(\frac{x^3+mx+n}{p}\right) \pmod{p}.$$

This completes the proof.

For a prime $p > 3$ and $k \in \{0, 1, \ldots, p-1\}$ it is easily seen that

$$\binom{[\frac{p}{6}]}{k}\binom{[\frac{p}{6}]+k}{k} = \binom{[\frac{p}{6}]+k}{2k}\binom{2k}{k} \equiv \frac{\binom{6k}{3k}\binom{3k}{k}}{(-432)^k} \pmod{p}.$$

Therefore $p \mid \binom{6k}{3k}\binom{3k}{k}$ for $\frac{p}{6} < k < p$, and

$$(2.2)\quad P_{[\frac{p}{6}]}(t) \equiv \sum_{k=0}^{[p/6]} \binom{6k}{3k}\binom{3k}{k}\left(\frac{1-t}{864}\right)^k \pmod{p}.$$

Corollary 2.1. *Let $p > 3$ be a prime and $m, n \in R_p$ with $m \not\equiv 0 \pmod{p}$. Then*

$$\begin{aligned} P_{[\frac{p}{6}]}\left(\frac{n}{2m^3}\right) &\equiv \sum_{k=0}^{[p/6]} \binom{6k}{3k}\binom{3k}{k}\left(\frac{2m^3-n}{12^3m^3}\right)^k \\ &\equiv -\left(\frac{3m}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-3m^2x+n}{p}\right) \pmod{p}. \end{aligned}$$

Corollary 2.2. *Let $p > 3$ be a prime, and let $c(n)$ be given by*

$$q\prod_{k=1}^{\infty}(1-q^k)^2(1-q^{11k})^2=\sum_{n=1}^{\infty}c(n)q^n \quad (|q|<1).$$

Then

$$c(p)\equiv P_{[\frac{p}{6}]}\left(\frac{19}{8}\right)\equiv(-1)^{\frac{p-1}{2}}\sum_{k=0}^{[p/6]}\frac{\binom{6k}{3k}\binom{3k}{k}}{256^k}\ (\mathrm{mod}\ p).$$

Proof. It is easy to see that the result holds for $p = 11$. Now assume $p \neq 11$. By the well known result of Eichler (see [KKS, Theorem 12.2]), we have

$$|\{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\ y^2+y=x^3-x^2\}|=p-c(p).$$

Since

$$
\begin{aligned}
&|\{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\ y^2+y=x^3-x^2\}|\\
&=\left|\left\{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\ \left(y+\frac{1}{2}\right)^2=x^3-x^2+\frac{1}{4}\right\}\right|\\
&=\left|\left\{(x,y)\in\mathbb{F}_p\times\mathbb{F}_p:\ y^2=x^3-x^2+\frac{1}{4}\right\}\right|\\
&=p+\sum_{x=0}^{p-1}\left(\frac{x^3-x^2+\frac{1}{4}}{p}\right)\\
&=p+\sum_{x=0}^{p-1}\left(\frac{(x+\frac{1}{3})^3-(x+\frac{1}{3})^2+\frac{1}{4}}{p}\right)\\
&=p+\sum_{x=0}^{p-1}\left(\frac{x^3-\frac{1}{3}x+\frac{19}{108}}{p}\right)\\
&=p+\sum_{x=0}^{p-1}\left(\frac{(\frac{x}{6})^3-\frac{1}{3}\cdot\frac{x}{6}+\frac{19}{108}}{p}\right)\\
&=p+\left(\frac{6}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-12x+38}{p}\right),
\end{aligned}
$$

we obtain

$$
c(p)=-\left(\frac{6}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-12x+38}{p}\right). \tag{2.3}
$$

Using Corollary 2.1 we see that

$$c(p) = -\left(\frac{6}{p}\right)\sum_{x=0}^{p-1}\left(\frac{x^3-12x+38}{p}\right)$$
$$\equiv P_{[\frac{p}{6}]}\left(\frac{19}{8}\right) \pmod{p}.$$

Therefore,

$$P_{[\frac{p}{6}]}\left(\frac{19}{8}\right) = (-1)^{[\frac{p}{6}]}P_{[\frac{p}{6}]}\left(-\frac{19}{8}\right)$$
$$\equiv (-1)^{\frac{p-1}{2}}\sum_{k=0}^{[p/6]}\binom{6k}{3k}\binom{3k}{k}\left(\frac{1+19/8}{864}\right)^k$$
$$= (-1)^{\frac{p-1}{2}}\sum_{k=0}^{[p/6]}\frac{\binom{6k}{3k}\binom{3k}{k}}{256^k} \pmod{p}.$$

Thus the result follows.

Remark 2.1 Set $q = \mathrm{e}^{2\pi iz}$ and $f(z) = q\prod_{k=1}^{\infty}(1-q^k)^2(1-q^{11k})^2$. It is known that $f(z)$ is the unique weight 2 modular form of level 11.

For positive integers a_1, a_2, a_3, a_4 let

$$q\prod_{k=1}^{\infty}(1-q^{a_1k})(1-q^{a_2k})(1-q^{a_3k})(1-q^{a_4k})$$
$$=\sum_{n=1}^{\infty}c(a_1,a_2,a_3,a_4;n)q^n \quad (|q|<1).$$

For $(a_1,a_2,a_3,a_4)=(1,1,11,11),(2,2,10,10)$, $(1,3,5,15),(1,2,7,14)$ and $(4,4,8,8)$ it is known that (see [MO, Theorem 1])

$$f(z)=\sum_{n=1}^{\infty}c(a_1,a_2,a_3,a_4;n)q^n \quad (q=\mathrm{e}^{2\pi iz})$$

are weight 2 newforms.

Conjecture 2.1 Let $p>3$ be a prime. Then

$$c(2,2,10,10;p)=-\Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-12x-11}{p}\Big),$$

$$c(2,4,6,12;p)=-\Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-39x-70}{p}\Big),$$

$$c(1,3,5,15;p)=-\Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-3x-322}{p}\Big)$$

and

$$c(1,2,7,14;p) = -\Big(\frac{p}{3}\Big)\sum_{x=0}^{p-1}\Big(\frac{x^3-75x-506}{p}\Big).$$

Is Conjecture 2.1 known according to Wiles' work on Fermat's last theorem? Wiles revealed the connection between elliptic curves and modular forms.

Theorem 2.2 ([S5, Theorem 2.6]). *Let $p > 3$ be a prime and $m, n \in R_p$ with $m \not\equiv 0 \pmod p$. Then*

$$\sum_{x=0}^{p-1}\Big(\frac{x^3+mx+n}{p}\Big)$$

$$\equiv \begin{cases} -(-3m)^{\frac{p-1}{4}}\displaystyle\sum_{k=0}^{[\frac{p}{12}]}\binom{[\frac{p}{12}]}{k}\binom{[\frac{5p}{12}]}{k}(\frac{4m^3+27n^2}{4m^3})^k \\ \qquad\qquad (\mathrm{mod}\ p) \quad \textit{if } 4 \mid p-1, \\ -\dfrac{3n}{2m^2}(-3m)^{\frac{p+1}{4}}\displaystyle\sum_{k=0}^{[\frac{p}{12}]}\binom{[\frac{p}{12}]}{k}\binom{[\frac{5p}{12}]}{k}(\frac{4m^3+27n^2}{4m^3})^k \\ \qquad\qquad (\mathrm{mod}\ p) \quad \textit{if } 4 \mid p-3. \end{cases}$$

Proof. It is known (see [AAR, p.315]) that

$$P_{2n}(x) = P_n^{(0,-\frac{1}{2})}(2x^2-1),$$
$$P_{2n+1}(x) = xP_n^{(0,\frac{1}{2})}(2x^2-1).$$

From [H. Bateman, Higher Transcendental Functions (vol II), 1953), p.170] we know that

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

If $p \equiv 1 \pmod 4$, then $[\frac{p}{6}] = 2[\frac{p}{12}]$ and so

$$P_{[\frac{p}{6}]}\left(\frac{3n\sqrt{-3m}}{2m^2}\right) = P_{[\frac{p}{12}]}^{(0,-\frac{1}{2})}\left(2\cdot\frac{-27n^2}{4m^3}-1\right)$$
$$= \sum_{k=0}^{[\frac{p}{12}]} \binom{[\frac{p}{12}]}{k}\binom{-\frac{1}{2}-[\frac{p}{12}]}{k}\left(1+\frac{27n^2}{4m^3}\right)^k$$
$$\equiv \sum_{k=0}^{[\frac{p}{12}]} \binom{[\frac{p}{12}]}{k}\binom{\frac{p-1}{2}-[\frac{p}{12}]}{k}\left(\frac{4m^3+27n^2}{4m^3}\right)^k$$
$$= \sum_{k=0}^{[\frac{p}{12}]} \binom{[\frac{p}{12}]}{k}\binom{[\frac{5p}{12}]}{k}\left(\frac{4m^3+27n^2}{4m^3}\right)^k \pmod p;$$

if $p \equiv 3 \pmod 4$, then $[\frac{p}{6}] = 2[\frac{p}{12}] + 1$ and so

$$
\begin{aligned}
&P_{[\frac{p}{6}]}\Big(\frac{3n\sqrt{-3m}}{2m^2}\Big) \\
&= \frac{3n\sqrt{-3m}}{2m^2} P_{[\frac{p}{12}]}^{(0,\frac{1}{2})}\Big(2 \cdot \frac{-27n^2}{4m^3} - 1\Big) \\
&= \frac{3n\sqrt{-3m}}{2m^2} \sum_{k=0}^{[\frac{p}{12}]} \binom{[\frac{p}{12}]}{k} \binom{-\frac{3}{2} - [\frac{p}{12}]}{k} \Big(1 + \frac{27n^2}{4m^3}\Big)^k \\
&\equiv \frac{3n\sqrt{-3m}}{2m^2} \sum_{k=0}^{[\frac{p}{12}]} \binom{[\frac{p}{12}]}{k} \binom{\frac{p-3}{2} - [\frac{p}{12}]}{k} \Big(\frac{4m^3 + 27n^2}{4m^3}\Big)^k \\
&= \frac{3n\sqrt{-3m}}{2m^2} \sum_{k=0}^{[\frac{p}{12}]} \binom{[\frac{p}{12}]}{k} \binom{[\frac{5p}{12}]}{k} \Big(\frac{4m^3 + 27n^2}{4m^3}\Big)^k \pmod p.
\end{aligned}
$$

Now combining the above with Theorem 2.1 we deduce the result.

Theorem 2.3 (Z.H. Sun [S1-S5]) For any prime $p > 3$ and $t \in R_p$,

$$P_{\frac{p-1}{2}}(t)$$

$$\equiv -(\frac{-6}{p}) \sum_{x=0}^{p-1} (\frac{x^3 - 3(t^2+3)x + 2t(t^2-9)}{p}) \pmod p$$

$$(\sqrt{t})^{\frac{p-1}{2}} P_{\frac{p-1}{2}}(\sqrt{t}) \equiv -\sum_{x=0}^{p-1} \left(\frac{x^3 - 2tx^2 + tx}{p}\right) \pmod p,$$

$$P_{[\frac{p}{4}]}(t) \equiv -(\frac{6}{p}) \sum_{x=0}^{p-1} (\frac{x^3 - \frac{3(3t+5)}{2}x + 9t + 7}{p}) \pmod p,$$

$$P_{[\frac{p}{3}]}(t) \equiv -(\frac{p}{3})$$

$$\sum_{x=0}^{p-1} (\frac{x^3 + 3(4t-5)x + 2(2t^2 - 14t + 11)}{p}) \pmod p,$$

$$P_{[\frac{p}{6}]}(t) \equiv -(\frac{3}{p}) \sum_{x=0}^{p-1} (\frac{x^3 - 3x + 2t}{p}) \pmod p.$$

§3. A congruence for $(\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p}))^2 \pmod p$

Lemma 3.1. *For any nonnegative integer n we have*

$$\sum_{k=0}^{n}\binom{2k}{k}\binom{3k}{k}\binom{6k}{3k}\binom{k}{n-k}(-432)^{n-k}$$
$$=\sum_{k=0}^{n}\binom{3k}{k}\binom{6k}{3k}\binom{3(n-k)}{n-k}\binom{6(n-k)}{3(n-k)}.$$

Lemma 3.1 can be proved by using WZ method. Using Lemma 3.1 we deduce:

Theorem 3.1 ([S5, Theorem 3.1]). *Let p be an odd prime and let x be a variable. Then*

$$\sum_{k=0}^{p-1}\binom{2k}{k}\binom{3k}{k}\binom{6k}{3k}(x(1-432x))^k$$
$$\equiv\Big(\sum_{k=0}^{p-1}\binom{3k}{k}\binom{6k}{3k}x^k\Big)^2 \pmod{p^2}.$$

Theorem 3.1 can be viewed as a $p-$analogue of Clausen's identity.

Theorem 3.2 ([S5, Theorem 4.2]) . *Let $p > 3$ be a prime and $m, n \in R_p$ with $m \not\equiv 0 \pmod{p}$. Then*

$$\Big(\sum_{x=0}^{p-1}\Big(\frac{x^3+mx+n}{p}\Big)\Big)^2$$

$$\equiv \Big(\frac{-3m}{p}\Big)\sum_{k=0}^{\frac{p-1}{2}}\binom{2k}{k}\binom{3k}{k}\binom{6k}{3k}\Big(\frac{4m^3+27n^2}{12^3\cdot 4m^3}\Big)^k \pmod{p}.$$

Moreover, if $\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p}) = 0$, then

$$\sum_{k=0}^{\frac{p-1}{2}}\binom{2k}{k}\binom{3k}{k}\binom{6k}{3k}\Big(\frac{4m^3+27n^2}{12^3\cdot 4m^3}\Big)^k \equiv 0 \pmod{p^2}.$$

Proof. We first assume that $4m^3 + 27n^2 \equiv 0 \pmod{p}$. Clearly $-3m \equiv (\frac{9n}{2m})^2 \pmod{p}$ and so $(\frac{-3m}{p}) = 1$. As $x^3 + mx + n \equiv (x - \frac{3n}{m})(x +$

$\frac{3n}{2m})^2 \pmod p$ we see that

$$\begin{aligned}
&\sum_{x=0}^{p-1}\left(\frac{x^3+mx+n}{p}\right)\\
&=\sum_{x=0}^{p-1}\left(\frac{(x-\frac{3n}{m})(x+\frac{3n}{2m})^2}{p}\right)\\
&=\sum_{\substack{x=0\\ x\not\equiv -\frac{3n}{2m} \pmod p}}^{p-1}\left(\frac{x-\frac{3n}{m}}{p}\right)\\
&=\sum_{t=0}^{p-1}\left(\frac{t}{p}\right)-\left(\frac{-\frac{3n}{2m}-\frac{3n}{m}}{p}\right)=-\left(\frac{-2mn}{p}\right).
\end{aligned}$$

Since $m \not\equiv 0 \pmod{p}$ we have $n \not\equiv 0 \pmod{p}$ and so $\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p}) = -(\frac{-2mn}{p}) = \pm 1$. Thus the result holds in this case.

Now we assume that $4m^3+27n^2 \not\equiv 0 \pmod{p}$. Set $t = \frac{3n\sqrt{-3m}}{2m^2}$ and $m_1 = \frac{1728 \cdot 4m^3}{4m^3+27n^2}$. Then $t = \sqrt{1-1728/m_1}$. From Theorems 2.1 and 3.1 we have

$$\begin{aligned}
&\Big(\sum_{x=0}^{p-1}\Big(\frac{x^3+mx+n}{p}\Big)\Big)^2 \\
&\equiv (-3m)^{\frac{p-1}{2}} P_{[\frac{p}{6}]}(t)^2 \\
&\equiv \Big(\frac{-3m}{p}\Big) \sum_{k=0}^{(p-1)/2} \frac{\binom{2k}{k}\binom{3k}{k}\binom{6k}{3k}}{m_1^k} \pmod{p}.
\end{aligned}$$

Recall that $p \mid \binom{3k}{k}\binom{6k}{3k}$ for $\frac{p}{6} < k < p$. If $\sum_{x=0}^{p-1}(\frac{x^3+mx+n}{p}) = 0$, we must have $P_{[\frac{p}{6}]}(t) \equiv 0 \pmod{p}$. Thus, applying Theorem 3.1 we see that

$$\sum_{k=0}^{(p-1)/2} \frac{\binom{2k}{k}\binom{3k}{k}\binom{6k}{3k}}{m_1^k} \equiv 0 \pmod{p^2}.$$

§4. A theorem concerning eta products and binary quadratic forms

Theorem 4.1 (Z.H. Sun, Adv. in Appl. Math. 48(2012), 106-120.) For $a,b,n\in\mathbb{N}$ let $\lambda(a,b;n)\in\mathbb{Z}$ be given by

$$q\prod_{k=1}^{\infty}(1-q^{ak})^3(1-q^{bk})^3=\sum_{n=1}^{\infty}\lambda(a,b;n)q^n\ (|q|<1).$$

(1) Suppose $2\nmid ab$ and p is an odd prime such that $p\neq a,b$, $p\nmid ab+1$ and $p=ax^2+by^2$ with $x,y\in\mathbb{Z}$. Let $n=((ab+1)p-a-b)/8$. Then

$$(-1)^{\frac{a+b}{2}x+\frac{b+1}{2}}(4ax^2-2p)=\lambda(a,b;n+1).$$

(2) Let $a,b\in\mathbb{N}$ with $(a,b)=1$. Let p be an odd prime such that $p\neq ab,ab+1$ and $p=x^2+aby^2$ with $x,y\in\mathbb{Z}$. Let $n=(a+b)(p-1)/8$. If $2\nmid a$, $2\mid b$, $8\nmid b$ and $8\mid p-1$, then

$$(-1)^{\frac{y}{2}}(4x^2-2p)=\lambda(a,b;n+1).$$