RATIONAL FUNCTIONS REPRESENTING ALL RESIDUES MOD $p$. II

L. J. MORDELL*

* Deceased 12 March 1972

Abstract. Two rational functions representing all residues mod $p$ are given.

In a recent paper, I have proposed the

**Problem.** To find two rational functions of $x$, say $f(x)$, $g(x)$ defined mod $p$ an odd prime for all $x$ except possibly $x \equiv 0 \pmod{p}$ such that for every integer $n$, either $f(x) \equiv n$ or $g(x) \equiv n$ is solvable.

A trivial instance is when $f(x) = x^2$, $g(x) = kx^2$, where $k$ is a nonquadratic residue mod $p$.

Another instance, with the usual meaning of $1/x$ is

\begin{equation}
\begin{aligned}
f(x) &= ax^4 + bx^2 + cx, \\
g(x) &= x - \frac{b^2}{4a} - \frac{bc^2}{8ax} - \frac{c^4}{64ax^2}.
\end{aligned}
\end{equation}

This was communicated to me by Schinzel after I had given him the special case when $b = 0$. We must impose the condition $c \not\equiv 0$ as the result is false when $c \equiv 0$.

My proof [1] depended upon the consideration of a double exponential sum and applying Salie’s result for the sum of the series $\sum_{x=1}^{p-1} e(Ax + B/x)(x/p)$ where $(x/p)$ is the Legendre symbol. Schinzel’s proof was an arithmetic one based on Skolem’s result [2] on quartic congruences.

I notice now a much simpler method which makes the result more obvious.

In (1), it suffices to take $a = 1$ as is obvious on dividing $f(x)$ by $a$ and replacing $x$ in $g(x)$ by $ax$.

Write $e(x)$ for $e(2\pi ix/p)$. Now consider the sum

\begin{equation}
S = \sum_{x=0}^{p-1} e(x^4 + bx^2 + cx).
\end{equation}

Received by the editors October 13, 1971.

*AMS 1970 subject classifications. Primary 10–02, 10G05.

© American Mathematical Society 1972

411
Then multiplying by \(e(-y^2)\) and replacing \(y^2\) by \((y+x^2)^2\) on the right-hand side, we have

\[
S \sum_{y=0}^{p-1} e(-y^2) = \sum_{x,y=0}^{p-1} e(x^4 + bx^2 + cx - (y + x^2)^2)
\]

\[= \sum_{x,y=0}^{p-1} e(x^2(b - 2y) + cx - y^2).\]

Since \(\sum_{x=0}^{p-1} e(Ax^2+Bx)=\sqrt{p}i((p-1)/2)^2(A/p)e(-B^2/4A)\) if \(A\not\equiv 0 \pmod{p}\), we have

\[
S\sqrt{p}i((p-1)/2)^2 \left(\frac{-1}{p}\right) = \sqrt{p}i((p-1)/2)^2 \sum_{y=0}^{p-1} e\left(\frac{-c^2}{4(b - 2y)} - y^2\right)\left(\frac{b - 2y}{p}\right)
\]

if \(b - 2y \equiv 0 \pmod{p}\). If \(b - 2y \equiv 0 \pmod{p}\), the sum for \(x\) in (3) is zero. Hence replacing \(y\) by \((4b - y)/8\), we obtain

\[
S\left(\frac{-1}{p}\right) = \sum_{y=1}^{p-1} e\left(\frac{-c^2}{y} - \left(\frac{4b - y^2}{8}\right)\right)\left(\frac{y}{p}\right).
\]

Since the cyclotomic equation \(x^{p-1} + \cdots + 1 = 0\) is irreducible, an identity \(\sum_{r=0}^{p-1} d_r e(r) = 0\) can hold only if it can be written as \(\sum_{r=0}^{p-1} d_r e(r) = 0\), unless all the \(d_r\) are zero. Not all the terms in (4) can cancel, since there are \(p\) terms on the left-hand side and only \(p-1\) on the right-hand side. Hence every residue \(\pmod{p}\) must occur in the left-hand side or the right-hand side. Schinzel's result follows on writing \(1/y\) for \(y\).

REFERENCES
