A NECESSARY AND SUFFICIENT CONDITION FOR TWIN PRIMES

Joseph B. Dence

University of Missouri-St. Louis

Thomas P. Dence

Ashland University

Wilson's Theorem, and its converse, give a necessary and sufficient condition for an integer p to be a prime [1]. In this note, we give an analogous condition for $(p, p+2)$ to be twin primes. This result, similar in nature to that of Clement [2], is not commonly encountered in introductory number theory texts [3,4,5], and would make an interesting topical addition to the first course.

We start with the well-known result that $(p-1)! \equiv -1 \pmod p$ if and only if p is a prime. Since $(p-1)!$ is equal to $(p-1)(p-2)!$, and $(p-1) \equiv -1 \pmod p$, it follows that $(-1)(p-2)! \equiv -1 \pmod p$ if and only if p is a prime. Repeating this reduction, next with $p-2$, $n-2$ more times gives the result

$$(1) \qquad (n-1)!(-1)^{n-1}(p-n)! \equiv -1 \pmod p, \quad 1 \le n < p.$$

Choosing $n = (p+1)/2$ and substituting into (1), we obtain a key identity,

$$(2) \qquad \left(\frac{p-1}{2}\right)!^2 \equiv \begin{cases} -1 \pmod p, & \text{if } p \text{ is a } (4k+1)\text{-prime} \\ +1 \pmod p, & \text{if } p \text{ is a } (4k+3)\text{-prime.} \end{cases}$$

In the case of twin primes, two cases arise.

<u>Case 1</u>. $p = 4k+1$ and $p+2 = 4k+3$.

Then (2) gives $((p-1)/2)!^2 \equiv -1 \pmod p$ and $((p+1)/2)!^2 \equiv 1 \pmod{p+2}$. The latter is equivalent to $(p^2+2p+1)\,((p-1)/2)!^2 \equiv 4 \pmod{p+2}$, and the reduction of $(p^2+2p+1) \equiv 1 \pmod{p+2}$ gives $((p-1)/2)!^2 \equiv 4 \pmod{p+2}$, or

$$(3) \qquad ((p-1)/2)!^2 = 4 + r(p+2)$$