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

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

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

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

for some $r \in \mathbb{N}$. Hence, $4 + r(p+2) \equiv -1 \pmod{p}$, or $2r = -5 + mp$ for some $m \in \mathbb{Z}$. Solving this for r and substituting into (3), we obtain

$$2\left((p-1)/2\right)!^2 + 5p = -2 + mp(p+2),$$

or as the equivalent congruence

$$2\left(((p-1)/2)!^2 + 1\right) + 5p \equiv 0 \pmod{p(p+2)}, \tag{4}$$

if and only if $(p, p+2)$ are twin primes and p has the form $4k+1$.

Case 2. $p = 4k-1$, and $p+2 = 4k+1$.

Then (2) gives $((p-1)/2) \equiv 1 \pmod{p}$ and $((p+1)/2)^2 \equiv -1 \pmod{p+2}$, and duplication of the above steps gives as the companion to (4)

$$2\left(((p-1)/2)!^2 - 1\right) - 5p \equiv 0 \pmod{p(p+2)}, \tag{5}$$

if and only if $(p, p+2)$ are twin primes and p has the form $4k-1$.

Numerical checks are always assuring. When $p = 17$, then (4) demands $323|(2(8!)^2 + 85 + 2)$; in fact, $323 \cdot 10066269 = 3251404887$. In contrast, when $p = 13$ we find that $195 \nmid (2(720)^2 + 65 + 2)$. When $p = 11$, then (5) demands $143|(2(5!)^2 - 55 - 2)$; in fact, $143 \cdot 201 = 28743$. In contrast, when $p = 19$, we find that $399 \nmid (2(9!)^2 - 95 - 2)$. Of course, just like Wilson's Theorem, equations (4), (5) are grossly impractical as a test (for twin primes).

Extensions of the above equations (4), (5) are possible. We can show similarly that $(p, p+4)$ are a twin $(4k+1)$-prime pair if and only if

$$36\left(((p-1)/2)!^2 + 1\right) - 7p \equiv 0 \pmod{p(p+4)}, \tag{6}$$

and that $(p, p+4)$ are a twin $(4k+3)$-prime pair if and only if

$$36\left(((p-1)/2)!^2 - 1\right) + 7p \equiv 0 \pmod{p(p+4)}. \tag{7}$$

References

1. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, 1979, 68, 88.

2. P. A. Clement, "Congruences for Sets of Primes," *American Mathematical Monthly*, 56 (1949), 23–25.

3. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

4. C. Vanden Eynden, *Elementary Number Theory*, Random House, New York, 1987.

5. K. H. Rosen, *Elementary Number Theory and its Applications*, 3rd ed., Addison-Wesley, Reading, PA, 1993.