Notes on Wolstenholme's Theorem

Timothy H. Choi

October 12, 2008

Let $p > 3$ be prime throughout the sequel. However, in the first claim p can be 3. Let

$$H(n) = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

be the sum of the reciprocals of the positive integers from 1 to n.

Wolstenholme's Theorem: p^2 divides the numerator of the reduced form of $H(p-1)$.

Proof. We prove the assertion using a sequence of claims.

Claim 1: p divides the numerator of the reduced form of $H(p-1)$.

Proof of Claim 1. Note that

$$\begin{aligned}
H(p-1) &= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \\
&= \left(\frac{1}{1} + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) \\
&\quad + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{p - \frac{p-1}{2}}\right) \\
&= \left(\frac{(1)(p-1)}{(1)(p-1)} + \frac{(1)(1)}{(1)(p-1)}\right) \\
&\quad + \left(\frac{(1)(p-2)}{(2)(p-2)} + \frac{(1)(2)}{(2)(p-2)}\right) \\
&\quad + \cdots \\
&\quad + \left(\frac{(1)(p - \frac{p-1}{2})}{(\frac{p-1}{2})(p - \frac{p-1}{2})} + \frac{(1)(\frac{p-1}{2})}{(\frac{p-1}{2})(p - \frac{p-1}{2})}\right) \\
&= \frac{p}{(1)(p-1)} + \frac{p}{(2)(p-2)} + \cdots \\
&\quad + \frac{p}{(\frac{p-1}{2})(p - \frac{p-1}{2})} \\
&= p\left(\frac{1}{p-1} + \frac{1}{2(p-2)} + \cdots \right. \\
&\quad \left. + \frac{1}{(\frac{p-1}{2})(p - \frac{p-1}{2})}\right) \\
&= p\frac{A}{(p-1)!} \\
&= \frac{pA}{(p-1)!}
\end{aligned}$$

where A is the whatever integer should be. Since none of the factors of the denominator, i.e. $(p-1)!$, divides p, even in the reduced form of the fraction $\frac{pA}{(p-1)!}$, the factor p will not be canceled in the numerator of the reduced form. Thus, the numerator is divisible by p. □

Note that the integer A in the derivations mentioned in the proof of the claim above is

$$\frac{(p-1)!}{(1)(p-1)} + \frac{(p-1)!}{(2)(p-2)} + \cdots + \frac{(p-1)!}{(\frac{p-1}{2})(p - \frac{p-1}{2})}$$

Claim 2: For $a \in \{1, 2, \ldots, (p-1)\}$, we have

$$\frac{(p-1)!}{(a)(p-a)} \equiv (a^2)^{-1} \pmod{p}.$$

Proof of Claim 2. Let $x = \frac{(p-1)!}{(a)(p-a)} \in \mathbb{Z}$. Then

$$(a)(p-a)x = (p-1)!.$$

By Wilson's Theorem, we have

$$(a)(p-a)x = (p-1)! \equiv -1 \pmod{p}.$$

In particular,

$$-a^2 x \equiv -1 \pmod{p}.$$

Thus, $a^2 x \equiv 1 \pmod{p}$, so $x \equiv (a^2)^{-1} \pmod{p}$. Therefore,

$$\frac{(p-1)!}{(a)(p-a)} \equiv (a^2)^{-1} \pmod{p}.$$

□

Since, for all $a \not\equiv 0 \pmod{p}$, we know that $(a^2)^{-1} \equiv (a^{-1})^2 \pmod{p}$, we have by Claim 2

$$\begin{aligned}
A &\equiv (1^2)^{-1} + (2^2)^{-1} + \cdots + \left(\left(\frac{p-1}{2}\right)^2\right)^{-1} \\
&\equiv (1^{-1})^2 + (2^{-1})^2 + \cdots + \left(\left(\frac{p-1}{2}\right)^{-1}\right)^2
\end{aligned}$$

Claim 3:

$$1^2+2^2+\cdots+(p-1)^2 \equiv 0 \pmod{p}.$$

Proof of Claim 3. One can easily prove that, for all natural number n, the sum of the squares is

$$1^2+2^2+\cdots+n^2 = \frac{(n)(n+1)(2n+1)}{6}.$$

In particular, $\frac{(n-1)(n)(2n+1)}{6} \in \mathbb{Z}$. If $n = p-1$, then since $6 \nmid p$, we know that $6 \mid (p-1)(2(p-1)+1)$. Thus, $p \mid \frac{(p-1)(p)(2(p-1)+1)}{6}$. Therefore,

$$\begin{aligned} 1^2+2^2+\cdots+(p-1)^2 &\equiv \frac{(p-1)(p)(2(p-1)+1)}{6} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

□

As there is a bijection between the set $\{1, 2, \ldots, (p-1)\}$ and $\{1^{-1}, 2^{-1}, \ldots, (p-1)^{-1}\}$, we have $1^2+2^2+\cdots+(p-1)^2 \equiv (1^{-1})^2+(2^{-1})^2+\cdots+((p-1)^{-1})^2 \pmod{p}$.

Claim 4: $A \equiv 0 \pmod{p}$.

Proof of Claim 4. We will first show that $2A \equiv 0 \pmod{p}$. As $-(a^{-1}) \equiv (-a)^{-1} \pmod{p}$, we have

$$\begin{aligned} 2A &= A + A \\ &= (1^{-1})^2+(2^{-1})^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2 \\ &\quad +(1^{-1})^2+(2^{-1})^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2 \\ &= (1^{-1})^2+(2^{-1})^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2 + \\ &\quad (-(1^{-1}))^2+(-(2^{-1}))^2+\cdots+\left(-\left(\left(\frac{p-1}{2}\right)^{-1}\right)\right)^2 \\ &\equiv (1^{-1})^2+(2^{-1})^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2 + \\ &\quad ((-1)^{-1})^2+((-2)^{-1})^2+\cdots+\left(\left(-\left(\frac{p-1}{2}\right)\right)^{-1}\right)^2 \\ &\equiv (1^{-1})^2+(2^{-1})^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2 + \\ &\quad \left(\left(-\left(\frac{p-1}{2}\right)\right)^{-1}\right)^2+\cdots+((-2)^{-1})^2+((-1)^{-1})^2 \\ &\equiv (1^{-1})^2+(2^{-1})^2+\cdots+\left(\left(\frac{p-1}{2}\right)^{-1}\right)^2 + \\ &\quad \left(\left(\frac{p+1}{2}\right)^{-1}\right)^2+\cdots+((p-2)^{-1})^2+((p-1)^{-1})^2 \\ &\equiv (1^{-1})^2+(2^{-1})^2+\cdots+((p-1)^{-1})^2 \\ &\equiv 1^2+2^2+\cdots+(p-1)^2 \\ &\equiv 0 \pmod{p} \end{aligned}$$

by Claim 3. Thus, $2A \equiv 0 \pmod{p}$. As $2 \nmid p$, we have $A \equiv 0 \pmod{p}$. □

By Claim 1 and Claim 4, we have $H(p-1) = \frac{pA}{(p-1)!} = \frac{p^2B}{(p-1)!}$ where B is whatever integer should be. By the same token, p^2 will still survive as a factor of the numerator even in the reduced form of $H(p-1)$ as none of the factors of $(p-1)!$ can divide p. Therefore, p^2 divides the numerator of the reduced form of $H(p-1)$. □

Some calculations (up to 38-th prime number p) suggest the following conjecture.

Conjecture: If s is the numerator of the reduced form of $H(p-1)$, then $\frac{s}{p^2}$ is square-free.