Andrew Ardito

Wolstenholme's Theorem:

If $\frac{1}{1} + \frac{1}{2} + ... + \frac{1}{p-1}$ is written in the form $\frac{A_k}{B_k}$ with $\gcd(A_k, B_k) = 1$, then $A_k \equiv 0\ (mod\ p^2)$, for p a prime greater than 3.

Proof:

Grouping the terms like this:

$(\frac{1}{1} + \frac{1}{p-1}) + ... + (\frac{1}{k} + \frac{1}{p-k})$, we have:

$\frac{1}{1} + \frac{1}{2} + ... + \frac{1}{p-1} = \frac{p}{p-1} + \frac{p}{2(p-2)} + ... + \frac{p}{(\frac{p-1}{2})(\frac{p+1}{2})}$

Factoring out all the p's in the numerator, all we have to show is that:

$\frac{1}{p-1} + \frac{1}{2(p-2)} + ... + \frac{1}{(\frac{p-1}{2})(\frac{p+1}{2})}$ when written as a fraction in lowest terms has a numerator divisible by p.

$p - k \equiv -k\ (mod\ p)$, so we can rewrite the above as:

$-\left(\frac{1}{1^2} + \frac{1}{2^2} + ... + \frac{1}{(\frac{p-1}{2})^2}\right)$

We can see that this sum is the same as:

$-\left(1^2 + (2)^2 + ... + (\frac{p-1}{2})^2\right)$

Dropping the negative sign, we just need to show:

$(1)^2 + (2)^2 + ... + (\frac{p-1}{2})^2 \equiv 0\ (mod\ p)$

we know this sum is equivalent to $(\frac{p+1}{2})^2 + ... + (p-1)^2\ (mod\ p)$

So $2(1^2 + 2^2 + ... + (\frac{p-1}{2})^2) \equiv 1^2 + 2^2 + ... + (p-1)^2 \equiv 0\ (mod\ p)$ if $p > 3$.

Since $gcd(2, p) = 1$, Wolstenholme's Theorem is true.

□