**THEOREM OF THE DAY**

**Wolstenholme’s Theorem**: If $p \geq 5$ is prime, then $\left(\frac{2p - 1}{p - 1}\right) \equiv 1 \mod p^3$.

The fact that $p$ divides $\left(\frac{2p - 1}{p - 1}\right) - 1$ for any prime $p$ can be deduced easily from the remarkable theorem of Lucas which says that $\left(\frac{n}{p}\right)$ is congruent, mod $p$, to the product $\prod \left(\frac{k}{p}\right)$, where the $n_i$ and $k_i$ are matching pairs of digits in the base-$p$ representations of $n$ and $k$. Indeed, $\left(\frac{n}{p}\right) \equiv \left(\frac{m}{p}\right) \mod p$, since multiplying by $p$ merely contributes an extra zero to a base-$p$ representation.

Now take $n = 2$ and $k = 1$, giving $\left(\frac{2}{p}\right) \equiv \left(\frac{p}{p}\right) \mod p$, or $2 \equiv 2\left(\frac{2p - 1}{p - 1}\right) \mod p$. Further investigation reveals that, for odd primes $p$, $\left(\frac{2}{p}\right) \equiv \left(\frac{3}{p}\right) \equiv \left(\frac{m}{p}\right) \mod p^3$, for primes $p \geq 5$. For example, taking $n = 4$, $k = 3$ and $p = 5$ we can confirm that $4 = \left(\frac{4}{5}\right) \equiv \left(\frac{3}{5}\right) = 15504 \mod 125$ (the single, boxed figures, left).

But here it stops. E.g. $3 = \left(\frac{3}{11}\right) \equiv \left(\frac{11}{11}\right) = 116280 \mod 7^4$ (the circled figures). In fact, the least values $p$ for which $\left(\frac{2p - 1}{p - 1}\right) \equiv 1 \mod p^4$ holds are 16843 and 2124679 (the first two so-called Wolstenholme primes).

Moving deeper into number theory, let $H_{n,m}$ denote the sum $1 + \frac{1}{2^m} + \frac{1}{3^m} + \ldots + \frac{1}{n^m}$. Then $\frac{1}{2}(H_{p-1,1}^2 - H_{p-1,2})$ is the coefficient of $p^2$ in the product

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

and so $\left(\frac{2p - 1}{p - 1}\right) = \prod_{k=1}^{p-1} \left(1 + \frac{p}{k}\right)$ is given mod $p^3$ by the sum

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

Now, it may be established that $H_{p-1,1} \equiv 0 \mod p^3$ (i.e. numerator of $H_{p-1,1}$ is divisible by $p^3$), and $H_{p-1,2} \equiv 0 \mod p$. Substituting into our mod $p^3$ sum, taking a little care that the fractions behave as they should, this is enough to confirm that $p^3$ divides $\left(\frac{2p - 1}{p - 1}\right) - 1$.

Charles Babbage proved in 1819 that $p^2$ divides $\left(\frac{2p - 1}{p - 1}\right) - 1$. Joseph Wolstenholme’s congruences, both the binomial and the more influential $H_{m,n}$ ‘harmonic series’ forms, date from 1862.


Created by Robin Whitty for www.theoremoftheday.org