Proof that for a binomial expansion of $(x+y)^p$ $\{\mathbb{N}\}$ with prime exponent $p \geqq 5$, the parity of $m : pxy(x+y)m = \sum_{i=1}^{p-1}\binom{p}{i}x^{p-i}y^i$ is even, if and only if x and y are also even.

David L. Roper

Abstract

Although the binomial theorem $z^p = (x+y)^p$ p prime is rarely, if at all, reduced to its internally factored form of $x^p + pxyzm + y^p$; this expression does, nevertheless, include an important feature that is of special interest in number theory and the History of Mathematics. It contains the key to rediscovering Fermat's original proof by infinite descent of $a^p + b^p \gtrless c^p$ for all positive integers.

Thus, after dividing $\sum_{i=1}^{p-1}\binom{p}{i}x^{p-i}y^i$ by $pxyz$, the parity of the factor, $m \in \{2n\}$, if and only if $(x, y, z) \subset \{2n\}$.

Proof: Consider the binomial equation in $\{\mathbb{N}\}$ raised to the power of prime $p \geqq 5$.

$$z^p = x^p + \sum_{i=1}^{p-1}\binom{p}{i}x^{p-i}y^i + y^p \text{ and } z^p - x^p - y^p = \sum_{i=1}^{\frac{1}{2}(p-1)}\binom{p}{i}(xy)^i(x^{p-2i} + y^{p-2i}).$$

Therefore, $p \,\Big|\, \binom{p}{i}$, $xy \,\big|\, (xy)^i$, $(x+y) \,\big|\, (x^{p-2i} + y^{p-2i})$ $\therefore$ $pxy(x+y)m = \sum_{i=1}^{p-1}\binom{p}{i}x^{p-i}y^i$.

Division by pxy reduces the equation to $zm = \frac{1}{p}\sum_{i=1}^{p-1}\binom{p}{i}x^{(p-i)-1}\,y^{i-1}$

$$zm = \frac{1}{p}\left\{\binom{p}{1}x^{p-2} + \binom{p}{2} + x^{p-3}y + \binom{p}{3}x^{p-4}y^2 + \cdots + \binom{p}{p-2}xy^{p-3} + \binom{p}{p-1}y^{p-2}\right\}$$

Definition: It is now necessary to divide this equation by $z = (x+y)$. But, because the coefficients of the quotient are required for this proof, the notation, $\sum\binom{p}{i\mp}$ is introduced.

$\sum\binom{p}{i\mp}$: $\sum\binom{p}{1\mp} = \binom{p}{1}$; $\sum\binom{p}{2\mp} = \binom{p}{2} - \binom{p}{1}$; $\sum\binom{p}{3\mp} = \binom{p}{3} - \binom{p}{2} + \binom{p}{1}$ $\cdots$

In general, $\sum\binom{p}{n\mp} = \binom{p}{n} - \binom{p}{n-1} + \binom{p}{n-2} - \cdots \pm \binom{p}{n-(n-1)}$.

[The sum of each $\sum\binom{p}{i\mp}$ therefore represents a coefficient in the expression for m, after the dividend zm is divided by $(x+y)$, as can be ascertained by performing the long division.]

$$\therefore \ m = \frac{1}{p}\sum_{i=1}^{p-2}\binom{p}{i\mp}x^{(p-i)-2}y^{i-1}$$

Hence, $m = \frac{1}{p}\left\{\sum\binom{p}{1\mp}x^{p-3} + \sum\binom{p}{2\mp}x^{p-4}y + \sum\binom{p}{3\mp}x^{p-5}y^2 + \cdots \sum\binom{p}{(p-2\mp)}y^{p-3}\right\}$.

$$m = \frac{1}{p}\left[\binom{p}{1}x^{p-3} + \left\{\binom{p}{2} - \binom{p}{1}\right\}x^{p-4}y + \left\{\binom{p}{3} - \binom{p}{2} + \binom{p}{1}\right\}x^{p-5}y^2 + \cdots + \left\{\binom{p}{p-2} - \cdots - \binom{p}{2} + \binom{p}{1}\right\}y^{p-3}\right].$$

By inspecting the first and final term in m, if x and y have opposite parity, then $m \in \{2n-1\}$. But, if x and y both have even parity, then $m \in \{2n\}$. It therefore remains to prove the parity of m when x and y both have odd parity.

The middle term in m is $c = \frac{1}{p}\sum\binom{p}{\frac{1}{2}(p-1)\mp}(xy)^{\frac{1}{2}(p-3)}$

Each side of c, the coefficients are quotients of their respective binomial dividend, after division by $(x+y)$. They therefore form pairs of equal value placed symmetrically either side of c.

That is: $\frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p-3)\mp}=\frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p+1)\mp}$; $\frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p-5)\mp}=\frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p+3)\mp}$

In general, $\frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p-(2n+3))\mp}=\frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p+(2n+1))\mp}$ $\quad n \in \{0,1,2,3, \dots \tfrac{1}{2}(p-5)\}$.

Hence, the sum of each symmetrically equal pair, together with their terms in x and y, is therefore even; whence, the sum total, S, of these paired coefficients, is also even. Therefore, $m = S + c$.

That is,
$$m = S + \frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p-1)\mp}(xy)^{\frac{1}{2}(p-3)}$$

It is seen from this equation that with the parity of S, p and xy known, the parity of m is decided by $\Sigma\binom{p}{\frac{1}{2}(p-1)\mp}$.

It is known that for any binomial expansion in $\{\mathbb{N}\}$, $(a+b)^p$: $\sum_{i=0}^{p+1}\binom{p}{i}=2^p$. $\therefore$ $\sum_{i=0}^{p+1}\binom{p}{i}-\binom{p}{0}-\binom{p}{p}=2^p-2$.

$$\therefore \sum_{i=0}^{p+1}\binom{p}{i}-\binom{p}{0}-\binom{p}{p}=2^p-2 \quad \Rightarrow \quad \sum_{i=1}^{\frac{1}{2}(p-1)}\binom{p}{i}=2^{p-1}-1.$$

But, $\sum_{i=1}^{\frac{1}{2}(p-1)}\binom{p}{i}$ has the same number of terms as $\Sigma\binom{p}{\frac{1}{2}(p-1)\mp}$. Therefore, when each of these negative values are replaced by an equivalent positive value, they add twice their sum to the original total; thereby leaving the parity of $\Sigma\binom{p}{\frac{1}{2}(p-1)\mp}$ unchanged, but now equal to $2^{p-1}-1$.

Therefore, the parity of $\Sigma\binom{p}{\frac{1}{2}(p-1)\mp} \in \{2n-1\}$. Hence, $m = S + \frac{1}{p}\Sigma\binom{p}{\frac{1}{2}(p-1)\mp}(xy)^{\frac{1}{2}(p-3)}$ and $m \in \{2n-1\}$.

$\therefore \quad m = 2r \ : \ r \in \{\mathbb{N}\}$ and $2r = \frac{z^p-x^p-y^p}{pxyz}$ if and only if $(x,y,z) \subset \{2n\}$ with $p \geqq 5$. [If $p = 3$, $r = \tfrac{1}{2}$.]

Ever since Professor Sir Andrew Wiles proved the Taniyama-Shimura conjecture in 1995, with its corollary that an equation of the form $a^p + b^p = c^p$, in positive integers with prime p > 2, can have no solutions, mathematicians have become convinced that Fermat was in error to have claimed that he possessed a 'wonderful' proof, when using only the 17th century mathematics at his disposal. Instead, what it does prove is that neither mathematicians nor the universities know everything.

The demonstration given above, which proves $2r = \frac{z^p-x^p-y^p}{pxyz}$ if and only if $(x,y,z) \subset \{2n\}$ with $p \geqq 5$, and a special case for $p = 3$, would have been well within Fermat's capability.

Added to this, with a little ingenuity, it becomes an easy matter to demonstrate that if $a^p + b^p = c^p$ it would imply the existence of $2r = \frac{z^p-x^p-y^p}{pxyz}$. Therefore, since x, y and z are, themselves, always even: and in the present case factors of a, b and c, it must follow that these three terms are divisible by 2. In which case, $a^p + b^p = c^p$ becomes reducible to terms of lower value. Thereafter, the same argument can be applied to this new equation to reduce these terms to even lower values—and so on, again and again; hence, infinite descent.

Therefore, Fermat's claim has been vindicated. Whereupon, it must be admitted that Professor Wiles did not actually rediscover Fermat's proof. Instead, his proof of the Taniyama-Shimura conjecture, while being a brilliant success, is actually a circumbendibus of Fermat's far simpler, elegant and direct proof of having earlier achieved the same result.