July, 2001.

Sophie's Primes.

For positive integers p and q, the factorization $x^p + y^p = (x+y)f(x,y)$ entails

$$x + y \equiv 0 \pmod{q} \quad \Longrightarrow \quad f(x,y) \equiv p \cdot x^{p-1} \pmod{q}\,, \tag{1}$$

because $f(x,y) = x^{p-1} - x^{p-2}y + \cdots + y^{p-1}$, whence $f(x,-x) = p \cdot x^{p-1}$. If x and y are relatively prime (hence non-zero) integers, then x and $x+y$ are relatively prime as well, and we can draw the following conclusion.

Lemma: *If p is prime, and x, y are relatively prime, the greatest common divisor of $(x+y)$ and $f(x,y)$ is either 1 or p.*

Theorem: *Let p and $q = 2p+1$ be odd primes, and suppose that $x^p + y^p + z^p = 0$, for relatively prime integers x, y, and z. Then p divides xyz.*

Proof. Without reference to q, note that p can divide at most one of x, y, z, and does so whenever it divides the sum of the other two.

By the Lemma, the proof would now be finished, unless $(x+y)$, $(x+z)$, and $(y+z)$ are all relatively prime to their complements $f(x,y)$, $f(x,z)$, and $f(y,z)$. Since $(x+y)f(x,y) = x^p + y^p$ is a p-th power, we would then have $x+y = a^p$ and $f(x,y) = d^p$ individually, and likewise $x+z = b^p$, $y+z = c^p$, etc. We must show that this cannot happen.

The argument takes place in the field F_q of q elements. Recall that $u^{q-1} = 1$ for any $0 \neq u \in F_q$, and hence *the only possible values for any p-th power are* $0, \pm 1$. Up to permutation of the variables, the only way the equation $x^p + y^p + z^p = 0$ can hold in F_q is in the form $1 - 1 + 0 = 0$.

Suppose, then, that z is zero in F_q. Then $x = b^p = \pm 1$ and $y = c^p = \pm 1$, forcing $x+y = a^p$ to be zero. Since, as an integer, $f(x,y) = c^p$ is relatively prime to $x+y$, it must be ± 1 in F_q. On the other hand, $f(x,y) = p \cdot x^{p-1} = p \cdot (\pm 1)^{p-1} = p$. This cannot be.