Similarly, from $x^n = z^n - y^n$, x has at least $r+1$ distinct prime factors, except when $z = y+1$ and n is odd, in which case, it can only be said that x has at least r distinct prime factors. □

And now, more explicitly.

(5C) *Let $n > 2$, let $0 < x < y < z$ be relatively prime integers satisfying* (5.1). *Then*

1. *z, y are not prime powers.*
2. *If x is a prime power, then $z = y+1$ and n is an odd prime.*

PROOF.

(1) If z is a prime power, so is $z^n = x^n + y^n$. By the preceding result, n is a power of 2, $n \geq 4$, and this contradicts Fermat's theorem, which is true for such exponents. The same argument is enough to show that y is not a prime power.

(2) If x is a prime power, by (5B), $n = p^e$, $e \geq 1$, p an odd prime and $z = y+1$. It remains to show that $e = 1$.

Assume $e > 1$ so $z^{p^{e-1}} - y^{p^{e-1}} > 1$ and

$$\begin{aligned} x^{p^e} &= z^{p^e} - y^{p^e} \\ &= (z^{p^{e-1}} - y^{p^{e-1}})(z^{(p-1)p^{e-1}} + z^{(p-2)p^{e-1}}y^{p^{e-1}} + \cdots + y^{(p-1)p^{e-1}}). \end{aligned} \tag{5.2}$$

Hence p does not divide

$$z^{p^e} - y^{p^e} = (y+1)^{p^e} - y^{p^e} = \sum_{j=1}^{p^e} \binom{p^e}{j} y^{p^e - 1}$$

because p divides all but the last summand. So x^{p^e} is the power of a prime $q \neq p$. Hence q divides both factors of (5.2), that is,

$$y^{p^{e-1}} \equiv z^{p^{e-1}} \pmod{q} \quad \text{and} \tag{5.3}$$

$$z^{(p-1)p^{e-1}} + z^{(p-2)p^{e-1}}y^{p^{e-1}} + \cdots + y^{(p-1)p^{e-1}} \equiv py^{(p-1)p^{e-1}} \equiv 0 \pmod{q}.$$

Thus q divides y and therefore by (5.3), q divides $z = y+1$, a contradiction. □

With more refined, but still elementary methods, Inkeri proved in 1946 that if $0 < x < y < z$, $x^p + y^p = z^p$, and $p \nmid xyz$, then $z - y > 1$ and so x is not a prime-power. I'll return to this question in my lecture on estimates.

6. Fermat's Equation with Even Exponent

As I shall indicate, it is possible to prove the first case of Fermat's theorem for even exponents. Clearly, it suffices to consider the exponents $2p$, where p is an odd prime.

The first result in this connection was obtained by Kummer, in 1837. It is his first paper on Fermat's equation and it is written in Latin. Later, this result was rediscovered many times (Niedermeier, 1943; Griselle, 1953; Oeconomu, 1956).

The best theorem concerning the exponent $2p$ was published by Terjanian, in December 1977. It is indeed quite surprising that his proof, which requires only very elementary considerations, was not found beforehand. I'll not jump to the conclusion that perhaps there is also a simple proof of Fermat's theorem awaiting to be discovered. I would rather say that Terjanian's result shows that the first case of Fermat's theorem for an even exponent is far easier than for a prime exponent.

I begin with Kummer's theorem:

(6A) *Let $n > 1$ be an odd integer. If there exist nonzero integers x, y, z such that $x^{2n} + y^{2n} = z^{2n}$ and $\gcd(n,xyz) = 1$, then $n \equiv 1 \pmod 8$.*

PROOF. It is possible to take x, y, z positive and relatively prime. A simple observation tells that x may be assumed even, while y, z are odd. Write

$$x^{2n} = z^{2n} - y^{2n} = (z^2 - y^2) \times \frac{z^{2n} - y^{2n}}{z^2 - y^2} \tag{6.1}$$

and observe that if the two factors on the right are relatively prime, then they are $2n$th powers.

$z^2 - y^2$ is even, and

$$\frac{z^{2n} - y^{2n}}{z^2 - y^2} = z^{2(n-1)} + z^{2(n-2)}y^2 + \cdots + y^{2(n-1)} \tag{6.2}$$

is a sum of n odd summands, hence it is odd, therefore of the form k^{2n}, with k odd.

Each summand on the right is of the form $(2a + 1)^2 = 4a(a + 1) + 1 \equiv 1 \pmod 8$.

Thus (6.2) becomes an equality of the form

$$8b + 1 = (8a_1 + 1) + \cdots + (8a_n + 1).$$

Therefore $n \equiv 1 \pmod 8$. □

For example, the first case of Fermat's theorem holds for $2n = 14$.

Kummer's theorem was extended by Grey in 1954 and by Long in 1960. Just for the record, I quote one of Long's results:

(6B) *If n is an integer whose last digit (in decimal notation) is 4 or 6, and if x, y, z are nonzero integers such that $x^n + y^n = z^n$, then $\gcd(n,xyz) > 2$.*

Now I shall give the proof of Terjanian's theorem, which contains all the above results as corollaries. Once more, as in §1, it is question of the quotient

$$Q_n(z,y) = \frac{z^n - y^n}{z - y},$$

If m, n are nonzero relatively prime integers, n odd, $n \geq 3$, let $\left(\frac{m}{n}\right)$ denote the Jacobi symbol defined by $\left(\frac{m}{n}\right) = 1$ when m is a square modulo n and $\left(\frac{m}{n}\right) = -1$ otherwise.

Lemma 6.1. *Let y, z be distinct nonzero integers.*

1. *If $m = nq + r$, $0 \leq r < n < m$, then*

$$Q_m(z,-y) = z^r Q_q(z^n,-y^n)Q_n(z,-y) + y^{m-r}Q_r(z,-y).$$

2. *If $m = nq - r$, $0 \leq r < n < m$, then*

$$Q_m(z,-y) = [z^{n-r}Q_{q-1}(z^n,-y^n) + y^{m-n}]Q_n(z,-y) - y^{m-n}z^{n-r}Q_r(z,-y).$$

3. *If z, y are odd, relatively prime, $z \equiv y \pmod 4$ and m is odd, then $Q_m(z,-y) \equiv m \pmod 4$, so $Q_m(z,-y)$ is odd.*
4. *If z, y are odd, relatively prime, $z \equiv y \pmod 4$ and m and n are odd natural numbers, then*

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{m}{n}\right).$$

Proof. The assertions (1) and (2) follow at once from the definitions.

(3) Let $z = y + 4t$. Then

$$Q_m(z,-y) = \frac{(y+4t)^m - y^m}{4t} = \binom{m}{1}y^{m-1} + \binom{m}{2}y^{m-2}4t + \cdots$$

$$= my^{m-1} \equiv m \pmod 4,$$

because $m - 1$ is even, y is odd, so $y^{m-1} \equiv 1 \pmod 4$.

(4) The assertion is proved by induction on $m + n$. It is trivial when $m = n = 1$. Let $m + n > 2$.

If $m > n$, then there exist an integer r, odd, $0 < r < n$, and q such that $m = qn + r$ or $m = qn - r$.

If $m = qn + r$, then $m - r$ is even, so by (1) and induction

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{y^{m-r}Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{r}{n}\right) = \left(\frac{m}{n}\right).$$

If $m = qn - r$, then $m - n$ and $n - r$ are even, so by (2) and induction

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{\cdots y^{m-n}z^{n-r}Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-Q_r(z,-y)}{Q_n(z,-y)}\right)$$

$$= \left(\frac{-1}{Q_n(z,-y)}\right)\left(\frac{Q_r(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-1}{Q_n(z,-y)}\right)\left(\frac{r}{n}\right).$$

By (3), $Q_n(z,y) \equiv n \pmod 4$. If $n = \prod_{i=1}^{s} p_i^{e_i}$, then it is easy to check that $n - 1 \equiv \sum_{i=1}^{s}(p_i - 1)e_i \pmod 4$, so

$$\left(\frac{-1}{n}\right) = \prod_{i=1}^{s}\left(\frac{-1}{p_i}\right)^{e_i} = (-1)^{\sum_{i=1}^{s}((p_i-1)/2)e_i} = (-1)^{(n-1)/2}.$$

Since $Q_n(z,y) \equiv n \pmod 4$,

$$\frac{Q_n(z,-y)-1}{2} \equiv \frac{n-1}{2} \pmod 2$$

hence

$$\left(\frac{-1}{Q_n(z,-y)}\right) = \left(\frac{-1}{n}\right).$$

Thus

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = \left(\frac{-1}{n}\right)\left(\frac{r}{n}\right) = \left(\frac{m}{n}\right).$$

Now, if $m < n$, by Jacobi's reciprocity law and the above proof

$$\left(\frac{Q_m(z,-y)}{Q_n(z,-y)}\right) = (-1)^{\frac{1}{2}(Q_m(z,-y)-1)\frac{1}{2}(Q_n(z,-y)-1)}\left(\frac{Q_n(z,-y)}{Q_m(z,-y)}\right)$$

$$= (-1)^{\frac{1}{2}(m-1)\frac{1}{2}(n-1)}\left(\frac{n}{m}\right)$$

$$= \left(\frac{m}{n}\right). \qquad \square$$

After this lemma, Terjanian's result follows almost at once:

(6C) *Let p be an odd prime. If x, y, z are nonzero integers such that $x^{2p} + y^{2p} = z^{2p}$, then $2p$ divides x or y.*

PROOF. There is no loss of generality in assuming that x, y, z are pairwise relatively prime. Also x, y cannot be both odd, since this would imply that $x^{2p} \equiv y^{2p} \equiv 1 \pmod 4$ and hence that $z^{2p} \equiv 2 \pmod 4$, which is impossible. Let x be even, so y, z are odd. Then

$$x^{2p} = z^{2p} - y^{2p} = (z^2 - y^2)\frac{z^{2p} - y^{2p}}{z^2 - y^2}.$$

By Lemma 1.2

$$\gcd\left(z^2 - y^2, \frac{z^{2p} - y^{2p}}{z^2 - y^2}\right) = p \text{ or } 1.$$

If the greatest common divisor is p, then p divides x^{2p}, so $2p$ divides x.

I show now that it is not possible that $z^2 - y^2$ and $(z^{2p} - y^{2p})/(z^2 - y^2)$ are relatively prime. If they are, both must be squares. But $z^2 \equiv y^2 \pmod 4$. Since p is not a square, there exists a prime q such that p is not a square modulo q. It follows from Lemma 6.1 that

$$-1 = \left(\frac{p}{q}\right) = \left(\frac{Q_p(z^2,-y^2)}{Q_q(z^2,-y^2)}\right),$$

which is absurd, because $Q_p(z^2,-y^2)$ is a square.

This concludes the proof. $\square$