Simple proof of Fermat's last theorem for $n=11$

A.M.D.M. Shadini, R.A.D.Piyadasa
Department of mathematics, University of Kelaniya,Sri Lanka

Abstract

Proof of Fermat's last theorem for any odd prime is difficult. It may be extremely difficult to generalize any available Proof of Fermat's last theorem for small prime such as $n=3,5,7$ to $n=11$[1]. The prime $n=11$ is different from $n=13,17,19$ in the sense that $2n+1=23$ is also a prime and hence the corresponding Fermat equation may have only one type (Class.2) of solutions due to a theorem of Germaine Sophie[1],[2]. In this contribution, we will give a simple proof for the exponent $n=11$ based on elementary mathematics. The Darbrusow identity[1] that we will use in the proof can be obtained as Darbrusow did using the multinomial theorem on three components[1]. In our proof, it is assumed that the Fermat equation $z^{11}=y^{11}+x^{11}$,$(x,y)=1$ has non-trivial integer solutions for (x,y,z) and the parametric solution of the equation is obtained using elementary mathematics. The proof of the theorem is done by showing that the necessary condition that must be satisfied by the parameters is never satisfied.

Parametric Solution of the equation

We obtain the parametric solution of the equation

$$z^{11}=y^{11}+x^{11}, \qquad (x,y)=1 \tag{1}$$

using following simple lemmas.

Lemma 1

If $a^{11}\equiv b^{11}(\text{mod } 11^m)$ $(m\neq 0)$ and $(a,11)=(b,11)=1$ then $a\equiv b(\text{mod } 11^{m-1})$ and $m\geq 2$.

If we assume that $a^{11}-b^{11}=11^{11m}t^{11}$ and $(a,b)=1$ in addition to $(a,11)=(b,11)=1$,then $a-b=11^{11m-1}u^{11}$, where u is a factor of t.

Proof of this lemma can be done exactly as in the case of $n=3,5$.Therefore we assume this lemma without proof.

Lemma 2

If the equation (1) has non-trivial integer solutions for the triple (x,y,z), then one of x,y,z is divisible by 11. If one assumes that none of x,y,z is divisible by 11, taking

$y=11a\pm 1,11b\pm 2,11c\pm 3,11d\pm 4,11e\pm 5, x=11f\pm 1,11g\pm 2,11h\pm 3,11i\pm 4,11j\pm 5$

it can be easily shown that

$$x^5+y^5\equiv(0,\pm 2,\pm 4,\pm 6,\pm 8,\pm 10,\pm 12,\pm 13,\pm 18,\pm 24,\pm 26,\pm 28,\pm 30,\pm 31,\pm 36,\pm 37,\pm 39,\pm 41,\pm 43,\pm 49,\pm 54)(\text{mod}11^2)$$

But $z^5\equiv(\pm 1,\pm 3,\pm 9,\pm 27,\pm 40)(\text{mod } 11^2)$ and therefore $x^5+y^5=z^5$ is not satisfied.

Hence, our assumption that none of x,y,z divisible 11 is wrong, and we conclude that one of x,y,z is divisible by 11. Assume that $y\equiv 0(\text{mod}11)$.

This assumption is quite general since we can replace x,y,z in (1) by $-x,-y,-z$.

Now the equation (1) can be written as

$$z^{11}=11^{11n}t^{11}+x^{11}, \quad (x,z)=1 \tag{2}$$

Lemma 3

$$z - x = 11^{11m-1}u^{11}$$

We this lemma without proof since its proof is as in the case of $n = 3.5$.

The equation (2) can now be written as

$$z^{11} = 11^{11m}u^{11}e^{11} + x^{11} \tag{3}$$

where $(11,u) = (11,e)(=(u,e) = 1$.

It is clear that $(z - y)$ is a eleven power and let $z - y = h^{11}$, where h is a factor of x.

If $z = gr$, where $(g,r) = 1$, then $(x + y) = g^{11}$.

Now,

$$(x + y) - z = g^{11} - gr = g(g^{10} - r)$$

$$x + y - z = y - (z - x) = 11^m ue - 11^{11m}u^{11} = 11^m u\left(e - 11^{11m-1}u^{10}\right)$$

Hence, $x - h^{11} = x + y - z \equiv 0 (\text{mod } 11^m ugh)$ since $(g,r) = (e,u) = 1$.

Now, consider $x + y - z$ in the form

$$x + y - z = x - (z - y) = y - (z - x) = (x + y) - z$$

(4)

to deduce that factor common to $x + y - z$ and x, y, z are the factors of $(z - y), (z - x), (x + y)$ respectively. Using the identity

$$x^{11} + y^{11} = (x + y)^{11} + 11xy(x + y)^9 + 44x^2y^2(x + y)^7 + 77x^3y^3(x + y)^4 + 55x^4y^4(x + y)^2 + 11x^2y^2$$

and the binomial expansion of $((x + y) - z)^{11}$ or directly using the identity

$$(x + y - z)^{11} = 11(x + y)(z - y)(z - x)\left\{\begin{array}{l} x^8 + y^8 + z^8 + 4(x^7y - x^7z + xy^7 - xz^7 - yz^7 - y^7z) \\ +11(x^6y^2 + x^6z^2 + x^2y^6 + x^2z^6 + y^2z^6 + y^6z^2) \\ +19(x^5y^3 + x^5z^3 + x^3y^5 + x^3z^5 + y^3z^5 + y^5z^3) \\ +23(x^4y^4 + x^4z^4 + y^4z^4) - 21(x^6yz + xy^6z - xyz^6) \\ +54(x^5yz^2 - x^5y^2z - x^2y^5z + xy^5z^2 - x^2yz^5 - xy^2z^5) \\ -84(x^4y^3z + x^3y^4z + x^4yz^3 - x^3yz^4 + xy^4z^3 - xy^3z^4) \\ +123(x^4y^2z^2 + x^2y^4z^2 + x^2y^2z^4) + 159(x^3y^3z^2 - x^3y^2z^3 - x^2y^3z^3) \end{array}\right\}$$

due to Darbrusow[1] one deduce that $x + y - z$ contains a factor d co-prime to xyz, where d^{11} is equal to the term in the curly bracket. Therefore $x + y - z = 11^m ughd$ and since

$$x + y - z = z - h^{11} = 11^m ughd \tag{5}$$

we get

$$x = 11^m ughd + h^{11} \tag{a}$$

$$y = 11^m ughd + 11^{11m-1}u^{11} \tag{b}$$

$$z = 11^m ughd + 11^{11m-1}u^{11} + h^{11} \tag{c}$$

In addition to this, we have $x + y = g^{11}$ and therefore from (a) and (b), we get

$$11^m ugh + h^{11} + 11^m ughd + 11^{11m-1}u^{11} = g^{11}$$

$$g^{11} - h^{11} - 2.11^m ughd - 11^{11m-1}u^{11} = 0 \tag{6}$$

Proof of Fermat's Last theorem for $n = 11$

Our proof of the theorem is based in the equation (6) and the Lemma 1.The equation (6) can be written as

$$g^{11} - 2.11^m ughd - 11^{11m-1}u^{11} - h^{11} = 0 \tag{7}$$

This equation (7) is an eleven degree polynomial equation in g ,and $g, u, h, d, 11$ are co-prime to one another. We fix the parameters $m\ (\geq 2)$, u of y in the Fermat equation (6) and try to find g for

different h. It is clear that $g^{11} - h^{11} \equiv 0 \pmod{11^m u}$ But $g^{11} - h^{11}$ is co-prime to h, d since h, d are co-prime to $11, u$.

Now, from the Lemma 1, $g - h = 11^{m-1} j$ for some j unless $g = 0$. i.e $g = 11^{m-1} j + h \quad (m \geq 2)$, where j is an integer co-prime to $11, d, h$. Therefore (7) can be written as

$$h^{11} + 11^{11m-1} u^{11} = (h + 11^{m-1} j)\left[(h + 11^{m-1} j)^{10} - 2.11^m uhd\right] \tag{8}$$

It is clear that $h + 11^{m-1} j$ is a factor of $h^{11} + 11^{11m-1} u^{11}$ and hence we must have

$$-11^{11m-11} j^{11} + 11^{11m-1} u^{11} = 0 \tag{9}$$

This is never satisfied since $(11, j) = (11, u) = 1$. i.e, there is no non-zero g satisfying (7). This completes the proof.

References

(1)Paulo Ribenboim (1991) .Fermat's last theorem for amateurs, Springer-Verlag

(2)Harold M.Edwards, Fermat's last theorem (1977) A genetic introduction to algebraic number theory, Springer-Verlag