[1]

ON THE MANNER OF RESOLVING THE EQUATION $t^2 - pu^2$ BY MEANS OF CIRCULAR FUNCTIONS

LEJEUNE DIRICHLET , TRANSLATED BY M. BEESON

In a memoir which I gave at the Academy of Sciences in Berlin, and of which one can find an extract in the Compte Rendu of last July, I set myself the task to prove rigorously that each infinite arithmetic progression, of which the first term and the interval are integers with no common divisor, necessarily contains an infinity of prime numbers. The methods which I have used to arrive at a complete demonstration of that proposition can be employed with success on different questions relative to numbers, and they have given me a chance to remark on a singular connection between two theories that up to now had no point of contact.

One knows that the equation $t^2 - pu^2 = 1$, in which p denotes a positive non-square integer, is always solvable in integers, and that that fundamental theorem in the theory of equations of the second degree has been deduced by LaGrange by consideration of the periodic continued fraction expansion of $\sqrt{p}$. It is remarkable that the solution of the preceding equation can also be carried out by means of the theory of binomial equations, which goes back to M. Gauss. It results not only that the equation is always solvable, but one may also deduce general formulas that express the unknowns t and u in terms of circular functions.

Although that manner of treating the equation is applicable to all cases, I shall limit myself here to the case when p is a prime number, which suffices to illustrate the spirit of the method. It is without doubt useless to add that the method of solution that we are going to indicate is very much less appropriate to numerical calculation than that which derives from the use of continued fractions.[2] The new method of solving the equation $t^2 - pu^2 = 1$ should be envisaged only as a theoretical connection between two branches of number theory.[3]

---

[1]This article originally appeared in Crelle, Journal für die Reine und angewandte Mathematik, Band 17, 8.286–290 (1837). It was reprinted in Band 1 of G. Lejeune Dirichlet's Werke, Herausgegeben auf Veranlassung der Preussischen Akademie der Wissenschaften, von L. Kronecker, in Zwei Banden, pp. 343-350.

[2]Translator's note: In Dirichlet's day, one could not compute trig functions to many decimal places of accuracy, and it would have been very laborious to multiply several values of the sine function even to six decimals. Today we can do that, although some difficulties still arise when we need thousands of decimal places. Even so, Dirichlet's remark remains true, because in his method, we have to multiply p numbers, so the method takes $O(p)$ steps, while the continued-fraction algorithm takes as many steps as the period of the continued fraction, which is conjectured to be $O(\sqrt{p})$, both in maximum and average. See `https://web.math.princeton.edu/mathlab/jr02fall/Periodicity/mariusjp.pdf`

[3]Translator's note: Today we would not look on the solution of Pell's equation and the study of the L-function (which is what that product of sines is) as two different branches of number theory; they both are tools for studying quadratic fields. Dirichlet's work in this paper is not often (if ever) cited, but it is in the unattributed core of number theory textbooks, e.g., Theorem 2, p. 344 of Borevic-Shafaravic. In this paper Dirichlet finds *some* solution of Pell's equation, but he never asserts that it is the fundamental solution, and in fact it is the fundamental solution raised to the power h, where h is the class number, as the cited theorem makes clear, at least after the minor correction in the next translator's note.

Let p be an odd prime number and consider the equation

$$\frac{x^p-1}{x-1} = X = 0 \tag{1}$$

The roots of this equation are given by the expression $e^{2m\pi i/p}$, where m is an integer in the sequence

$$1, 2, \ldots, (p-1).$$

Among these numbers there are $(p-1)/2$ quadratic residues mod p, and equally many non-residues, which we designate by

$$a_1, \ldots, a_{(p-1)/2} \text{ and } b_1, \ldots, b_{(p-1)/2},$$

respectively (in any order). With this notation, by the theory of M. Gauss[4] we have the two equations

$$\begin{aligned} Y + Z\sqrt{\pm p} &= 2(x - e^{a_1 2\pi i/p})(x - e^{a_2 2\pi i/p}) \ldots (x - e^{a_{(p-1)/2} 2\pi i/p}) \\ Y - Z\sqrt{\pm p} &= 2(x - e^{b_1 2\pi i/p})(x - e^{b_2 2\pi i/p}) \ldots (x - e^{b_{(p-1)/2} 2\pi i/p}) \end{aligned} \tag{2}$$

using the signs above or below according as p is congruent to 1 or 3 mod 4, and Y and Z are polynomials in x with integer coefficients. Multiplying the two preceding equations, we have

$$4X = Y^2 \mp pZ^2 \tag{3}$$

Because the numbers

$$a_1, \ldots, a_{(p-1)/2},$$

after re-ordering, are the remainders of the numbers

$$1^2, 2^2, \ldots, (\tfrac{1}{2}(p-1))^2$$

on division by p, the first of the equations (2) can evidently be replaced by

$$Y + Z\sqrt{\pm p} = 2(x - e^{1^2 2\pi i/p})(x - e^{2^2 2\pi i/p}) \ldots (x - e^{((p-1)/2)^2 2\pi i/p}) \tag{4}$$

Now we distinguish the two possible forms of p, and suppose for the first case that p is congruent to 1 mod 4. Taking $x = 1$ in equations (3) and (4), and designating by g and h the integer values of Y and Z corresponding to that substitution, there will come

$$g^2 - ph^2 = 4p, \tag{5}$$

$$g + h\sqrt{p} = 2(1 - e^{1^2 2\pi i/p})(1 - e^{2^2 2\pi i/p}) \ldots (1 - e^{((p-1)/2)^2 2\pi i/p})$$

Because one may write

$$1 - e^{s^2 2\pi i/p} = -2i \sin(s^2 \tfrac{\pi}{p}) e^{s^2 \pi i/p},$$

the last equation takes the form:

$$\begin{aligned} g + h\sqrt{p} = {} & 2^{\frac{1}{2}(p+1)} i^{\frac{1}{2}(p+1)} \sin(1^2 \tfrac{\pi}{p}) \sin(2^2 \tfrac{\pi}{p}) \ldots \\ & \sin((\tfrac{1}{2}(p-1))^2 \tfrac{\pi}{p}) e^{1^2 + 2^2 + \ldots + (\frac{1}{2}(p-1))^2 \pi i/p} \end{aligned}$$

On the other hand:

$$1^2 + 2^2 + \ldots + (\tfrac{1}{2}(p-1))^2 = p\frac{p^2-1}{24}$$

[4] *Disquisitiones Arithmeticae. Art. 357.*

where $\frac{p^2-1}{24}$ is evidently an even or odd integer, according as p is congruent to 1 or 5 mod 8. The exponential factor is therefore following the two cases $+1$ or -1, and can consequently be expressed as $(-1)^{\frac{1}{4}(p-1)}$. Substituting that expression into the previous equation, and recalling that $\frac{1}{2}(p-1)$ is odd, we have

$$g + h\sqrt{p} \quad = \quad 2^{\frac{1}{2}(p+1)} \sin(1^2\tfrac{\pi}{p}) \sin(2^2\tfrac{\pi}{p}) \ldots \sin((\tfrac{1}{2}(p-1))^2\tfrac{\pi}{p})$$

It results from equation (5) that the integer g is divisible by p; putting pk in place of g, we have

$$h^2 - pk^2 \quad = \quad -4 \tag{6}$$

$$h + k\sqrt{p} \quad = \quad \frac{2^{\frac{1}{2}(p+1)}}{\sqrt{p}} \sin(1^2\tfrac{\pi}{p}) \sin(2^2\tfrac{\pi}{p}) \ldots \sin((\tfrac{1}{2}(p-1))^2\tfrac{\pi}{p}) = \alpha$$

One sees thus that there are integers h and k such that

$$h^2 - pk^2 = -4$$

and that such integers may be expressed by the circular functions, because one easily concludes from the preceding equations that

$$\begin{aligned} h &= \frac{\alpha}{2} - \frac{2}{\alpha} \\ k &= \frac{1}{\sqrt{p}} \left(\frac{\alpha}{2} + \frac{2}{\alpha} \right) \end{aligned}$$

To pass to the equation

$$t^2 - pu^2 = 1,$$

it is necessary to distinguish the cases where p has the form $8\mu + 1$ or $8\mu + 5$. In the former case, h and k must both be even, and we will have

$$\left(\frac{h}{2}\right)^2 - \left(\frac{k}{2}\right)^2 = -1,$$

from which one concludes

$$\left(\frac{h}{2} + \frac{k}{2}\sqrt{p}\right)^2 = t + u\sqrt{p},$$

the rational parts and the coefficients of $\sqrt{p}$ being separately equal.

When p has the form $8\mu + 5$, h and k will both be odd.[5]

We put

$$(h + k\sqrt{p})^3 \quad = \quad h' + k'\sqrt{p}$$

[5]Translator's note: This is not true. For example, when $p = 37$, we have $h = -12$ and $k = 2$. To fix this, instead of dividing in cases according as p is congruent to 1 or 5 mod 8, we should divide in cases according as h and k are both even or not. In modern terms, we are checking whether the fundamental unit of $\mathbb{Q}(\sqrt{p})$ belongs to $\mathbb{Z}[\sqrt{p}]$ or not. Having p congruent to 5 mod 8 is necessary but not sufficient for it not to belong. In that case, we must cube $u = h - \sqrt{k}$. Of course, if we cube it when h and k are both even, we still get the solution u^3 of Pell's equation, but it will not be the one Dirichlet presumably intended, i.e. the fundamental solution of Pell raised to the power of the class number.

Consequently

$$\begin{aligned} h' &= h^3 + 3phk^2 \\ k' &= 3h^2k + pk^3 \end{aligned}$$

We have [multiplying $\left(h + k\sqrt{p}\right)^3 = h' + k'\sqrt{p}$ by its conjugate and using (6)]

$$(h')^2 - p(k')^2 = -4^3.$$

It is easy to see that the numbers h' and k' are both divisible by 8. Using (6) we have

$$\begin{aligned} h' &= 4h(pk^2 - 1) \\ k' &= 4k(h^2 + 1) \end{aligned}$$

The preceding equation then gives

$$\left(\frac{h'}{8}\right)^2 - p\left(\frac{k'}{8}\right)^2 = -1$$

from which one can deduce the solution of the equation $t^2 - pu^2 = 1$, on putting as above

$$\left(\frac{h'}{8} + \frac{k'}{8}\sqrt{p}\right)^2 = t + u\sqrt{p}$$

Now we take up the second case, in which p has the form $4\mu + 3$. In that case, the coefficients of the terms at equal distances from the extremes $2x^{\frac{1}{2}(p-1)}$ and -2 have the same numerical values with opposite signs, which one can put in the form

$$Y = 2(x^m - 1) + a(x^{m-2} - 1) + b(x^{m-4} - 1) + \ldots,$$

where for abbreviation $m = \frac{1}{2}(p-1)$. Then, on attributing to the indeterminant x the particular value i, one has

$$\begin{aligned} x^m - 1 &= -1 + i, & x(x^{m-2} - 1) &= -1 + i \\ x^2(x^{m-4} - 1) &= 1 + i, & x^3(x^{m-6} - 1) &= 1 + i \end{aligned}$$

or

$$\begin{aligned} x^m - 1 &= -1 - i, & x(x^{m-2} - 1) &= 1 - i \\ x^2(x^{m-4} - 1) &= 1 - i, & x^3(x^{m-6} - 1) &= -(1 - i) \end{aligned}$$

according as m has the form $4\mu + 3$ or $4\mu + 1$, that is to say, according as p has the form $8\mu + 7$ or $8\mu + 3$. One sees that the polynomial Y will become, according to the two cases,

$$g(1 + i) \text{ or } g(1 - i),$$

g designating an integer. As to the other polynomial Z whose coefficients equally distant from the beginning and the end are equal, one finds in a similar manner that it reduces, for $x = i$, to the form $h(1 + i)$ or $h(1 - i)$, according as $p = 8\mu + 7$ or $p = 8\mu + 5$, h designating similarly an integer.

The result of that, and of the fact that evidently $X = i$ when $x = i$, is that the equation

$$4X = Y^2 + pZ^2$$

will become

$$g^2(1 \pm i)^2 + ph^2(1 \mp i)^2 = 4i,$$

the signs above or below being taken according as p has the form $8\mu + 7$ or $8\mu + 3$.

The preceding equation is equivalent to this one:

$$g^2 - ph^2 = \pm 2, \tag{7}$$

which is therefore always solvable, and from which one passes easily to the equation $t - pu^2 = 1$ on putting

$$(g + h\sqrt{p})^2 = 2t + 2u\sqrt{p},$$

where t and u will be integers, g and h being evidently odd. To express afterwards g and h by circular functions, one puts $x = i$ in equation (4) and combines the result of that substitution with equation (7).

One sees that the solution just indicated is actually a simple corollary of a theorem due to M. Gauss, according to which the polynomial $4X$ may always be put in the form $Y^2 \mp pZ^2$, p being a prime number. To extend the same solution to the general case in which p is a composite number, one has to make a very great extension of the cited theorem. That generalization does not present any difficulty, and may be deduced from the principles on which rests the analysis of M. Gauss. That is why I will content myself with indicating the result for a number composed of two prime factors.

Let p and q be two different prime numbers. One finds that the entire function

$$4\,\frac{(x^{pq}-1)(x-1)}{(x^p-1)(x^q-1)} \tag{8}$$

can still be put in the form

$$Y^2 \mp pqZ^2$$

Y and Z always designate polynomials with integer coefficients; the sign above or below is used according as pq has the form $4\mu + 1$ or $4\mu + 3$. That decomposition results, as in the case of a single prime number, from the distribution in two groups of the roots of the equation obtained by setting expression (8) to zero.

Here is an example of this decomposition. Setting $p = 3$, $q = 11$, one will have

$$4\,\frac{(x^{33}-1)(x-1)}{(x^3-1)(x^{11}-1)} = Y^2 - 33Z^2,$$

$$\begin{aligned} Y &= 2x^{10} - x^9 + 8x^8 + 5x^7 + 2x^6 + 14x^5 + 2x^4 + 5x^3 + 8x^2 - x + 2, \\ Z &= x^9 + x^7 + 2x^6 + 2x^4 + x^3 + x \end{aligned}$$

1. Appendix by translator

Here I compare Dirichlet's solution to the formulas in Borevich-Shafarevich. Theorem 2, p.344, and equation (4.4) there say that

$$\epsilon^h = \frac{\prod_b \sin\frac{\pi b}{D}}{\prod_a \sin\frac{\pi a}{D}}$$

where a and b run through all natural numbers in $(0, D/2)$ which are relatively prime to D and satisfy $\chi(a) = +1, \chi(b) = -1$. Specializing to $D = p$, a runs through the quadratic residues and b runs through the non-residues, so the denominator is $\sqrt{p}/2^{\frac{1}{2}(p+1)}$ times Dirichlet's number α.