DEMONSTRATION

OF A

THEOREM OF ARITHMETIC.

(*New Memoirs of the royal Academy of Sciences and Belles-Lettres of Berlin*, year 1770[1].)

It is a Theorem known for a long time that *every whole number not a square can be always decomposed into two, or three, or four whole squares;* yet no-one, that I know of, has ever produced a demonstration. Mr. Bachet de Méziriac is the first who has mentioned this Theorem; it seems he was guided by the 31st question of the IVth book of Diophantus, where the Theorem we are discussing is to some extent tacitly supposed; yet Mr. Bachet was contented to assure himself the truth of this Theorem by induction, checking successively all whole numbers from 1 to 325; and as for the general demonstration, he confessed he had not yet been able to find one. "*The ability* (he says in his Commentary regarding the cited question) *to produce a complete proof has not yet been granted to me, so I will have high esteem for anyone who will produce more about it, especially but by no means only about this question but also and likewise about some in the fifth book of Diophantus where it is seen to be put down.*" I know of no two Authors, up till now, who have applied themselves to this research, as Mr. Fermat and Mr. Euler. In the Notes that the first has added to the Commentary of Bachet about Diophantus, he announces a great Work he has decided to compose about the theory of numbers, and he promises to prove in it this general proposition : that any number is, either triangular, or composed of two or of three triangular numbers; that it is, either square, or composed of two, or of three, or of four squares, and so on; yet this Work never showed up, and in all that is left of the works of this great Geometer, one finds absolutely nothing that can shed the weakest light on the demonstration in question. Regarding Mr. Euler, while his work on this subject has not met the success one should desire, one must be obliged to him for having opened the way that is followed in this sort of research. We must look in volume V of the *New Commentaries of St. Petersburg* at the result of the tentative ingenuities that the great Geometer has produced in order to reach the proof of Mr. Bachet's Theorem.

Mr. Euler has shown that the product of two, or of more numbers, each of them composed of four whole squares, are too always composed of four, or of a lesser number of whole squares; he also notes there that if the proposed Theorem could be proven for all prime numbers, it will be also true for all other numbers. Mr. Euler proved, in addition, that given any prime number, one can always find two or three square numbers whose sum is divisible by that number without any of the squares in particular being divisible by it, and that these square numbers can always be supposed to be such that the quotient of the division of their sum by the given prime number is less than that same number. From this Mr. Euler concludes, reasonably, that the Theorem in question will be proven for all prime numbers if one could only prove this other proposition, that is, that whenever the product of two numbers is the sum of four or less squares, and one of the multiplied numbers is similarly the some of four or less squares, the other multiplier is also the same sum. "*If a sum of four squares* (he says, page 55 of the cited volume) $a^2 + b^2 + c^2 + d^2$ *is divisible by a sum of four squares* $p^2 + q^2 + r^2 + s^2$*, then the quotient which is not only in fraction but also now integral is a sum of four squares; this is a most elegant Theorem of Fermat, whose demonstration has been hidden from me; I have not thus far been able to shed light upon this demonstration which captured me,* etc."

It is therefore only this last proposition that we need to prove. But for this we need not suppose that the divisor is also represented by a sum of four squares, and we prove, generally, that each prime number that is a divisor of some number composed of four or less squares, but not of any of them in particular, is necessarily also composed of four or less squares; after which nothing more is left to be desired for the complete demonstration of Bachet's general Theorem, that we have proposed to give in this Memoir.

Lemma.

The numbers which are the sum of two relatively prime squares do not admit other divisors than those that are similarly the sum of two squares.

This proposition, belonging to Mr. Fermat, has been proved by Mr. Euler in a Memoir printed in volume IV of the *New Commentaries of St. Petersburg.*

Corollary I. — *If two numbers equaling each a sum of two squares, like* $p^2 + q^2$ *and* $r^2 + s^2$*, are divisible by the same number* ρ*, such that the four squares* p^2*,* q^2*,* r^2*,* s^2 *have no common divisor, I claim that the two quotients* $\frac{p^2+q^2}{\rho}$ *and* $\frac{r^2+s^2}{\rho}$ *also equal each a sum of two squares.*

[1] *Works of Lagrange,* v. III, p. 189.

For let m be the greatest common divisor of p and q, and n the greatest common divisor of r and s, such that they are written

$$p = mp', \quad q = mq', \quad r = nr', \quad s = ns'$$

the numbers p' and q' are relatively prime, as are also the numbers r' and s'; we have therefore the two numbers $m^2(p'^2 + q'^2)$ and $n^2(r'^2 + s'^2)$ that are at once divisible by ρ. Yet I remark firstly that m and n are relatively prime; otherwise the four numbers p, q, r and s have a common divisor, which is contrary to the hypothesis. Now let μ be the greatest common divisor of m^2 and ρ, such that we have $\rho = \mu\rho'$, and that ρ' is relatively prime to $\frac{m^2}{\mu}$; hence m^2 is divisible by μ, and $p'^2 + q'^2$ must divide ρ', such that we have

$$\frac{p^2 + q^2}{\rho} = \frac{m^2}{\mu}\frac{p'^2 + q'^2}{\rho'};$$

yet p' and q' are relatively prime, and it follows from the preceding Lemma that the divisor ρ' is such that the quotient is the some of two squares; thus we have

$$\frac{p'^2 + q'^2}{\rho'} = \alpha^2 + \beta^2.$$

Moreover, let ν^2 be the greatest square factor of the number μ, such that $\mu = \nu^2\mu'$, μ' is a number which is divisible by no square, and it is clear that m^2 cannot be divisible by μ unless m divides $\nu\mu'$; let therefore $m = \mathrm{K}\nu\mu'$, and we have

$$\frac{m^2}{\mu} = \mathrm{K}^2\mu'.$$

But $n^2(r'^2 + s'^2)$ must also be divisible by $\rho = \mu\rho'$; hence μ divides $n^2(r'^2 + s'^2)$; yet μ already divides m^2; hence, since m^2 and n^2 are relatively prime, it follows that μ is also prime relative to n^2; consequentially, μ must divide $r'^2 + s'^2$; and as $\mu = \nu^2\mu'$, μ' must also be a divisor of $r'^2 + s'^2$; thus, since r' and s' are relatively prime, the divisor μ' must equal a sum of two squares by the Lemma. Hence writing $\mu' = \gamma^2 + \delta^2$, we get

$$\frac{m^2}{\mu} = \mathrm{K}^2(\gamma^2 + \delta^2);$$

and so

$$\frac{p^2 + q^2}{\rho} = \mathrm{K}^2(\gamma^2 + \delta^2)(\alpha^2 + \beta^2) = \mathrm{K}^2(\gamma\alpha + \delta\beta)^2 + \mathrm{K}^2(\gamma\beta - \delta\alpha)^2,$$

that is equal to a sum of two squares. One proves the same way that the quotient $\frac{r^2+s^2}{\rho}$ also equals a sum of two squares.

Corollary II. — *If a sum of two squares is divisible by another sum of two squares, the quotient always equals a sum of two squares.*

For let $a^2 + b^2$ be divisible by $c^2 + d^2$, and if the numbers a, b, c, d have a common divisor, let us denote it by l, such that we have

$$a = lp, \quad b = lq, \quad c = lr, \quad d = ls,$$

and that p, q, r, s have no common divisor; thus we have

$$\frac{a^2 + b^2}{c^2 + d^2} = \frac{p^2 + q^2}{r^2 + s^2},$$

such that $p^2 + q^2$ is divisible by $r^2 + s^2$; yet, writing $r^2 + s^2 = \rho$, we get by the preceding Corollary that $\frac{p^2+q^2}{\rho}$ equals a sum of two squares; hence, etc.

Theorem I.

If a sum of four squares is divisible by a prime number greater that the square root of the same sum, that number necessarily equals a sum of four squares.

For let $p^2 + q^2 + r^2 + s^2$ be divisible by A, A a prime number, such that we have

$$\mathrm{A}a = p^2 + q^2 + r^2 + s^2,$$

and as we suppose that the divisor A is greater than

$$\sqrt{p^2+q^2+r^2+s^2},$$

it is clear that the quotient a is smaller than the same root, such that we have $a < \mathrm{A}$.

This assumed, if the numbers p, q, r and s have a common divisor d, it is clear that the sum of their squares is divisible by d^2, and so it must be that $\mathrm{A}a$ also is; but d^2 being smaller than $\mathrm{A}a$, d is smaller than $\sqrt{\mathrm{A}a} < A$, because $\mathrm{A} < a$; thus, since A is prime (hypothesis), it is clear that A and d are relatively prime; from which it follows that $\mathrm{A}a$ cannot be divisible by d^2 unless a is; so, dividing the number a as well as each of the squares p^2, q^2,... by d^2, we get an equation of the same form as the preceding one, where the coefficient a is always smaller than A and where the four squares p^2, q^2, r^2, s^2 have no common divisor.

Let us consider therefore the equation

$$\mathrm{A}a = p^2+q^2+r^2+s^2$$

as if already reduced to that state, and if the number p^2+q^2 is not relatively prime to a, let ρ be their greatest common divisor, such that we have

$$a = b\rho \quad \text{and} \quad p^2+q^2 = t\rho,$$

b and t being relatively prime; we have therefore

$$\mathrm{A}b\rho = t\rho + r^2 + s^2,$$

from which we see that r^2+s^2 must also be divisible by ρ, such that, naming the quotient u, the equation becomes

$$\mathrm{A}b = t+u;$$

but, since ρ divides p^2+q^2 as well as r^2+s^2, and since p, q, r and s have no common divisor, it follows by Corollary I of the preceding Lemma that the quotients $\frac{p^2+q^2}{\rho} = t$ and $\frac{r^2+s^2}{\rho} = u$ are one and another the sum of two squares; so we have

$$t = m^2+n^2 \quad \text{and} \quad u = h^2+l^2;$$

therefore, multiplying all the equation by t, we get

$$\mathrm{A}bt = t^2+tu,$$

or better, writing $x = mh+nl$ and $y = ml-nh$, such that $tu = x^2+y^2$, we get the following equation

$$\mathrm{A}bt = t^2+x^2+y^2.$$

Now, as b and t are relatively prime, one can always find two multiples of b and t such that their some or their difference is equal to any given number, and moreover one can suppose that one of these multiples is smaller than $\frac{bt}{2}$ [*see* Lemma I of the Memoir on the indeterminate problems, that is printed in volume XXIV of the *Memoirs of the royal academy of Sciences and Belles-Lettres of Berlin*, of the year 1768[2]]; so we can put

$$x = \alpha t + \gamma b \quad \text{et} \quad y = \beta t + \delta b,$$

α, β, γ and δ are positive or negative whole numbers, and one can suppose the same time that α and β, taken positively, are one and another smaller than $\frac{b}{2}$. Performing this substitution in the preceding equation, it becomes

$$\mathrm{A}bt = t^2(1+\alpha^2+\beta^2) + 2\alpha\gamma tb + 2\beta\delta tb + \gamma^2b^2 + \delta^2b^2,$$

where we see that all the terms are multiplied by b, except the following

$$t^2(1+\alpha^2+\beta^2);$$

so, to make it possible to substitute in this equation whole numbers as is the case, it is necessary that $t^2(1+\alpha^2+\beta^2)$ be also divisible by b; yet b and t are relatively prime, hence b must divide $1+\alpha^2+\beta^2$, such that naming the quotient a' we get

$$a'b = 1+\alpha^2+\beta^2;$$

and as α and β are each smaller than $\frac{b}{2}$, $1+\alpha^2+\beta^2$ is smaller than $\frac{b^2}{2}+1$; consequentially a' is smaller than $\frac{b}{2}+\frac{1}{b}$.

But, putting in the equation above $a'b$ in place of $1+\alpha^2+\beta^2$, and dividing afterwards by b, we get

$$\mathrm{A}t = a't^2 + 2\alpha\gamma t + 2\beta\delta t + (\gamma^2+\delta^2)b,$$

[2] *Works of Lagrange,* v. II, p. 659.

where I remark again that all the terms are multiplied by t, except the following

$$(\gamma^2+\delta^2)b,$$

the number $(\gamma^2+\delta^2)b$ must be divisible by t, and as b and t are relatively prime, $\gamma^2+\delta^2$ must be divisible by t.

If one multiplies the equation we have found by a', it can be brought under this form

$$\mathrm{A}a't=(a't+\alpha\gamma+\beta\delta)^2+(\gamma^2+\delta^2)a'b-(\alpha\gamma+\beta\delta)^2,$$

or better under the following

$$\mathrm{A}a't=(a't+\alpha\gamma+\beta\delta)^2+\gamma^2(a'b-\alpha^2)+\delta^2(a'b-\beta^2)-2\alpha\beta\gamma\delta;$$

but we have

$$a'b=1+\alpha^2+\beta^2,$$

hence the previous equation becomes

$$\mathrm{A}a't=(a't+\alpha\gamma+\beta\delta)^2+\gamma^2(1+\beta^2)+\delta^2(1+\alpha^2)-2\alpha\beta\gamma\delta,$$

that is

$$\mathrm{A}a't=(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2+\gamma^2+\delta^2.$$

Yet we have said above that $\gamma^2+\delta^2$ must be divisible by t, hence the number

$$(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2$$

must also be; but we have

$$t=m^2+n^2,$$

thus, by Corollary II of the Lemma, each of the two quotients must be a sum of two squares; such that we have

$$\gamma^2+\delta^2=t(p'^2+q'^2)\quad\text{and}\quad(a't+\alpha\gamma+\beta\delta)^2+(\beta\gamma-\alpha\delta)^2=t(r'^2+s'^2).$$

Hence we get, after having divided all the equation by t,

$$\mathrm{A}a'=p'^2+q'^2+r'^2+s'^2.$$

It follows from this that if Aa is a sum of four squares, Aa' is also a sum of four squares, a' being smaller than $\frac{b}{2}+\frac{1}{b}$ and $a=b\rho$; so if a is greater than 1, a' is necessarily smaller than a; and, if a' is also greater than 1, one proves the same way that Aa'' is also a sum of four squares, a'' being smaller than a'; and so on; hence as the numbers a, a', a'',... are whole numbers, none of them equal to zero (because these numbers are divisors of the numbers $1+\alpha^2+\beta^2$, $1+\alpha'^2+\beta'^2$,... that, as one sees, can never become null), and as these numbers are diminishing, it is clear that we reach necessarily one of these numbers which is equal to unity, and therefore we have that A equals to a sum of four whole squares.

Corollary. — *If some prime number is a divisor of a sum of four squares having no common divisor, that number is also the sum of four squares.*

For naming, as above, A the given prime number and $p^2+q^2+r^2+s^2$ the number composed of four squares which is divisible by A, it is clear that, if each of the roots p, q, r, s is smaller than $\frac{\mathrm{A}}{2}$, we have

$$p^2+q^2+r^2+s^2<4\left(\frac{\mathrm{A}}{2}\right)^2<\mathrm{A}^2;$$

such that A is greater than $\sqrt{p^2+q^2+r^2+s^2}$ as is supposed in the preceding Theorem; hence, etc.

Yet I claim that whatever are the numbers p, q,..., one can always reduce them to be smaller than $\frac{\mathrm{A}}{2}$; since let, for example, $p>\frac{\mathrm{A}}{2}$, it is visible that if $p^2+q^2+r^2+s^2$ is divisible by A, $(p-m\mathrm{A})^2+q^2+r^2+s^2$ is also, the same for $(mA-p)^2+q^2+r^2+s^2$, whatever is the number m; but one can always take m such that $p-m\mathrm{A}$ or $m\mathrm{A}-p$ is smaller than $\frac{\mathrm{A}}{2}$; hence one need only put in place of p the number $p-m\mathrm{A}$ or $m\mathrm{A}-p$; and one can do the same with respect to any other number found to be greater than $\frac{\mathrm{A}}{2}$.

If p is divisible by A we have

$$p-m\mathrm{A}=0;$$

such that in that case one must put 0 in place of p; one must do the same regarding q if it also is divisible by A, and so for the others; yet as we suppose that p, q, r and s have no common divisor, it cannot happen that all are

divisible at the same time by A, and the same cannot happen for more than two; otherwise all the four must divide it; such that we should not fear that, during these reductions, the dividend $p^2+q^2+r^2+s^2$ will become null.

Remark — In the rest it is clear that the demonstration of the preceding Theorem is no less true if one supposes that one or two of the four squares that compose the dividend are null; whereas conversely it can also happen that one or two of the four squares that one finds for the divisor A are null; thus, in general, *any prime number that divides a sum of four or less whole squares, provided they have no common divisor, necessarily equals a sum of four or less whole squares.*

Theorem II.

If A *is a prime number and if* B *and* C *are some positive or negative numbers not divisible by* A*, I claim that one can always find two numbers* p *and* q *such that the number* $p^2-\mathrm{B}q^2-\mathrm{C}$ *is divisible by* A*.*

For : 1° If we can find a number q such that $\mathrm{B}q^2+\mathrm{C}$ is divisible by A, we need then only take a p divisible by A, or better $p=0$;

2° If no number chosen for q renders $\mathrm{B}q^2+\mathrm{C}$ divisible by A, write, for brevity, $\mathrm{B}q^2+\mathrm{C}=b$, and supposing

$$\mathrm{P}=p^{\mathrm{A}-3}+bp^{\mathrm{A}-5}+b^2p^{\mathrm{A}-7}+\ldots+b^{\frac{\mathrm{A}-3}{2}},$$

we get

$$(p^2-\mathrm{B}q^2-\mathrm{C})\mathrm{P}=p^{\mathrm{A}-1}-b^{\frac{\mathrm{A}-1}{2}}=p^{\mathrm{A}-1}-1-\left(b^{\frac{\mathrm{A}-1}{2}}-1\right);$$

multiplying this equation by $b^{\frac{\mathrm{A}-1}{2}}+1$ that we suppose equals Q, we get

$$(p^2-\mathrm{B}q^2-C)\mathrm{PQ}=\mathrm{Q}(p^{\mathrm{A}-1}-1)-(b^{\mathrm{A}-1}-1).$$

But, by a well-known Theorem of Fermat, that Mr. Euler proved in the *Commentaries of St. Petersburg,* we know that if A is some prime number and a some other number not divisible by A, $a^{\mathrm{A}-1}-1$ is always divisible by A. Hence, if we suppose that p is not divisible by A, we get that the two numbers $p^{\mathrm{A}-1}-1$ and $b^{\mathrm{A}-1}-1$ are simultaneously divisible by A, because b is never divisible by A, whatever is q (hypothesis). Thus the number $(p^2-\mathrm{B}q^2-\mathrm{C})\mathrm{PQ}$ is divisible by A, such that, if neither P nor Q is divisible by A, $p^2-\mathrm{B}q^2-\mathrm{C}$ must divide it, because A is a prime number by the hypothesis. So the difficulty is reduced to showing that one can always take a p and a q such that neither P nor Q is divisible by A, p not being so also.

For this I remark firstly that, whatever is the value of q, one can always find a value of p smaller than A and consequentially not divisible by A, such that P is not divisible by A. For if one substitutes successively in the expression of P the numbers 1, 2, 3,... up to $\mathrm{A}-2$ inclusively in place of p, and names P', P'', P''',..., $P^{(\mathrm{A}-2)}$ the resulting values of P, one gets, by the well-known theory of differences,

$$\mathrm{P}'-(\mathrm{A}-3)P''+\frac{(\mathrm{A}-3)(\mathrm{A}-4)}{2}P'''-\ldots+\mathrm{P}^{(\mathrm{A}-2)}=1.2.3.4\ldots(\mathrm{A}-3).$$

But, if all the numbers P', P'', P''',... up to $\mathrm{P}^{(A-2)}$ were divisible by A, the number $1.2.3\ldots(\mathrm{A}-3)$ would also have to be; that cannot happen because A is prime, and it follows that among the numbers P', P'',..., $P^{(\mathrm{A}-2)}$ one can necessarily find some number that is not divisible by A; hence, etc.

So it remains only to show that one can always take a q such that Q or $(\mathrm{B}q^2+\mathrm{C})^{\frac{\mathrm{A}-1}{2}}+1$ is not divisible by A.

Let, for simplicity, $\frac{\mathrm{A}-1}{2}=m$, and we get

$$\mathrm{Q}=\mathrm{B}^mq^{\mathrm{A}-1}+m\mathrm{B}^{m-1}q^{\mathrm{A}-3}\mathrm{C}+\frac{m(m-1)}{2}\mathrm{B}^{m-2}q^{\mathrm{A}-5}\mathrm{C}^2+\ldots+m\mathrm{B}q^2\mathrm{C}^{m-1}+\mathrm{C}^m+1.$$

But if C^m+1 is not divisible by A, it is clear that one need only take a q divisible by A, or better $q=0$; for then Q is not divisible by A.

Yet if C^m+1 is divisible by A, then for Q not to divide it, q must not too, and the quantity

$$\mathrm{B}^mq^{\mathrm{A}-3}+m\mathrm{B}^{m-1}q^{\mathrm{A}-5}\mathrm{C}+\frac{m(m-1)}{2}\mathrm{B}^{m-2}q^{A-7}\mathrm{C}^2+\ldots+m\mathrm{BC}^{m-1}$$

must also not; but we can show, as before, that there must exist a value of q smaller than A and consequentially not divisible by A, such that the quantity in question does not divide it. For naming R this quantity, and designating by R', R'', R''',..., $\mathrm{R}^{(\mathrm{A}-2)}$ the values of R that result from substituting the numbers 1, 2, 3,..., $\mathrm{A}-2$ in place of q, we get

$$\mathrm{R}'-(\mathrm{A}-3)\mathrm{R}''+\frac{(\mathrm{A}-3)(\mathrm{A}-4)}{2}R'''-\ldots+\mathrm{R}^{(\mathrm{A}-2)}=1.2.3\ldots(\mathrm{A}-3)\mathrm{B}^m.$$

But as A is prime and as B is not divisible by A, it is clear that the number $1.2.3\ldots(\mathrm{A}-3)\mathrm{B}^m$ is not also; hence, etc.

Corollary I. — If one puts $\mathrm{B}=-1$ and $\mathrm{C}=-1$, one gets a number p^2+q^2+1 that is divisible by A; from which it follows that *given any prime number one can always find a number equal to a sum of three squares one of which is the same as unity, that is divisible by the given prime number.*

This Theorem has already been proved by Mr. Euler in a different manner, in volume V of the *New Commentaries of St. Petersburg;* yet in order to leave nothing to be desired for our lecturers we believed we must prove it anew, and moreover our demonstration has the advantage of having a very great generality.

Corollary II. — Combining thus the preceding Theorem with the remark following Theorem I, we deduce : that *each prime number necessarily equals a sum of four or less whole squares.* From which it is straightforward to conclude that *each whole number is also equal to a sum of four or less squares;* for one knows that the product of two, or of more numbers equaling each a sum of four or less squares, also necessarily equals a sum of four or less squares; actually, one has

$$\begin{aligned}&(p^2+q^2+r^2+s^2)(p'^2+q'^2+r'^2+s'^2)\\&\quad=(pp'-qq'-rr'+ss')^2+(pq'+qp'-rs'-sr')^2\\&\quad+(pr'+qs'+rp'+sq')^2+(qr'-ps'+sp'-rq')^2,\end{aligned}$$

and also more generally

$$\begin{aligned}&(p^2-\mathrm{B}q^2-\mathrm{C}r^2+\mathrm{BC}s^2)(p'^2-\mathrm{B}q'^2-\mathrm{C}r'^2+\mathrm{BC}s'^2)\\&=[pp'+\mathrm{B}qq'\pm\mathrm{C}(rr'+\mathrm{B}ss')]^2-\mathrm{B}[pq'+qp'\pm\mathrm{C}(rs'+sr')]^2\\&\quad-\mathrm{C}[pr'-\mathrm{B}qs'\pm(rp'-\mathrm{B}sq')]^2+\mathrm{BC}[qr'-ps'\pm(sp'-rq')]^2.\end{aligned}$$