48.

INSTANTANEOUS PROOF OF A THEOREM OF LAGRANGE ON THE DIVISORS OF THE FORM $Ax^2+By^2+Cz^2$, WITH A POSTSCRIPT ON THE DIVISORS OF THE FUNCTIONS WHICH MULTISECT THE PRIMITIVE ROOTS OF UNITY.

[*American Journal of Mathematics*, III. (1880), pp. 390—392.]

IF possible, let p be not a divisor of x^2+y^2+1, and consequently not of the form $4i+1$, since, if it were of that form, x^2+1 would contain it.

Let ρ be any primitive pth root of unity.

Call $R=\Sigma\rho^{x^2}$, where x^2 means any one of the quadratic residues of and inferiors to p, and let the period conjugate to R be called R'.

Let R^2 be expanded as a sum of powers of ρ. Then, because p is not of the form $4i+1$, we cannot have $x^2+y^2=p$, so that no pth power of ρ can occur in that expansion; again, because by hypothesis neither $2x^2$ nor x^2+y^2 can be congruous to -1 [mod. p], no such power as ρ^{p-1} which belongs to R', nor consequently any other term of R', can appear in R^2; and as each power of ρ in R^2 belonging to the same period must appear a like number of times, we must have

$$R^2=\frac{p-1}{2}R, \text{ that is, } R=0, \text{ or } R=\frac{p-1}{2},$$

each of which suppositions is in the highest degree absurd. Hence p is a divisor of x^2+y^2+1. Q.E.D.

Compare Legendre's *Théorie des Nombres*, Ed. 1830, Tom. I. pp. 211—213, and again Serret's *Cours d'Algèbre Supérieure*, Tom. II. pp. 94—99, for proofs of the more general similar theorem due to Lagrange, concerning u^2+Bt^2+C. These proofs are highly ingenious, but long and laboured in no slight degree; and as the sole apparent object of either author in proving the general theorem is to make use of the particular case of it to which this note refers as a foundation to the proof of Fermat's law of the four squares, I have

thought that an intuitive proof of so important a lemma might not be without interest to some of the junior readers of the *Journal**.

But in fact the general theorem may be proved with scarcely any greater trouble than the particular case disposed of.

For, supposing A, B, C to be all quadratic residues to p, we may write

$$A \equiv \alpha^2, \quad B \equiv \beta^2, \quad C \equiv \gamma^2 \text{ [mod. } p\text{]},$$
$$\alpha x = u, \quad \beta y = v, \quad \gamma z = w;$$

and the congruence $u^2 + v^2 + w^2 \equiv 0$, as previously shown, being soluble, evidently

$$Ax^2 + By^2 + Cz^2 \equiv 0$$

will be so too, since

$$\alpha x \equiv u, \quad \beta y \equiv v, \quad \gamma z \equiv w \text{ [mod. } p\text{]},$$

give integer values for x, y, z; and as obviously the case of A, B, C being all non-residues falls into the previous case by multiplying the congruence by any non-residue, we have only to consider the case of two of the three coefficients being residues and the third a non-residue, or the converse case, which, however, by multiplication as above, may be reduced to the former one.

Suppose, then, $A = \alpha^2$, $B = \beta^2$, C a non-residue, and that

$$Ax^2 + By^2 + Cz^2 \equiv 0 \text{ [mod. } p\text{]}$$

is insoluble. For simplicity, let $z = 1$. Then $u^2 + v^2 + C = 0$ must be insoluble; if p is of the form $4i + 3$, we shall obtain, precisely as before,

$$R^2 = \frac{p-1}{2} R,$$

and if p is of the form $4i + 1$,

$$R^2 = 2\frac{p-1}{4} + \left\{\left(\frac{p-1}{2}\right)^2 - \left(\frac{p-1}{2}\right)\right\} \div \frac{p-1}{2} \cdot R,$$

or $$R^2 - \frac{p-3}{2} R + \frac{p-1}{2} = 0, \text{ that is, } R = \frac{p-1}{2}, \text{ or } R = -1,$$

any of which conclusions are eminently absurd.

* From this lemma there is scarcely more than a step to the theorem in question. If P is contained as a factor in the sum of four squares, it is easy to see that we may write

$$PQ = f^2 + g^2 + h^2 + k^2,$$

where $Q < P$, and

$$QQ' = (f - \alpha Q')^2 + (g - \beta Q')^2 + (h - \gamma Q')^2 + (k - \delta Q')^2,$$

where $Q' < Q$, and consequently, applying the Quaternion law of multiplication,

$$PQ' = f'^2 + g'^2 + h'^2 + k'^2,$$

and so we may form a continually decreasing series of quantities Q, Q', Q'', ... any one of which multiplied by P is a sum of four squares. Hence any divisor of such sum is itself such a sum, but by the lemma any prime number is a divisor of the sum of three, which plays the same part for present purposes as a sum of four squares, and is therefore a sum of four squares; consequently any number whatever, by the rule of multiplication already alluded to in this note, will be a sum of four squares.

Hence $Ax^2 + By^2 + Cz^2 \equiv 0$ [mod. p] *cannot* be insoluble; that is, the left-hand side of the congruence must contain p as a divisor.

P.S. In a future communication I will prove very simply that if a prime number $p = ef + 1$, and e is itself a prime number such that $(e - 1)$ contains no odd square number, then every divisor, without exception (other than p), of the function whose roots are the e periods of the primitive pth roots of unity, must be an eth power residue of p. If $(e - 1)$ contains any square number, the proof still holds good, except as regards the factors of such square, and there is no reason at present for supposing that the theorem may not be extended to the case of these excepted factors*. The same kind of reasoning may be applied also to the theory of period-functions for which e (the number of the periods) is not a prime number, and I find for the case of $e = 4$, that, leaving out of account the number 2 (which is always a divisor of the four-period function to p when p is of the form $8i + 1$, but never when it is of the form $8i + 5$, and may be or not a biquadratic residue of p, according to a well-known law), the divisors of the four-period function (excepting p) which do not divide g (the even term in the equation $[f^2 + g^2 = p]$), are necessarily biquadratic residues of p; as is also true of the prime-number divisors of g which are of the form $4i + 1$; but the prime-number divisors of g (all of which are necessarily divisors of the four-period function), of the form $4i - 1$, are quadratic only, and not biquadratic residues of p when p is of the form $8i + 5$; whereas for the case of $p = 8i + 1$ *all* the odd divisors of the four-period function (not counting p) are biquadratic residues of p†. The same investigation leads to the remarkable conclusion that if $p = f^2 + 4\gamma^2$, where f and γ are both of them odd and p a prime number, every divisor of $\frac{f^2 + 3\gamma^2}{4}$ is a biquadratic residue of p,—a theorem which I imagine would be difficult to prove by any other method.

* Thus, for example, if e is a prime number of the form $2^{2^x} + 1$, I am able to prove that *every* divisor of the e-period function (not excepting 2, if 2 should happen to be such a divisor) is an eth-power residue of p. Thus for $e = 2, 3, 5, 7, 11, 17$ we may be certain that there are none but eth-power-residue divisors of the period-function.

† Of course in a certain sense p or zero is an any-power residue. But there is good reason for separating p from the residues proper, inasmuch as only the *first* power of p, but an *unlimited* power of any true eth-power residue is a divisor of the e-period function,—a most important fact, which I presume must have been known to Bachmann, but has not been stated by him (in his *Kreistheilung*, 1872). An exceedingly simple proof of this and of the corresponding theorem for any cyclotomic function was given by Mr Hathaway at a recent meeting of the Mathematical Seminarium, at the Johns Hopkins University.