20.

NOTE ON A PRINCIPLE IN THE THEORY OF NUMBERS AND THE RESOLUBILITY OF ANY NUMBER INTO THE SUM OF FOUR SQUARES.

[*Quarterly Journal of Mathematics*, I. (1857), pp. 196, 197.]

PROBABLY no one who has had any experience in the properties of numbers, could be found seriously doubting the truth of the proposition that any function of a variable integer, not algebraically decomposable into factors, must, among the infinite number of positive integers which it represents, be capable of affording prime as well as composite numbers, except in the case of its being of such a form as to admit of a constant divisor for all values of the variable. To prove this generally is probably a task reserved for remote generations, and for a more advanced development of the cerebral organization, but it is to my mind and conviction, and probably to that of most others, no less certain than the equally undemonstrable theorem which lies at the basis of the ordinary empirical geometry, that two parallels to the same line cannot be drawn through the same point. It would certainly be interesting to be able to deduce a connected body of doctrine as consequences flowing from the assumption of this principle, nor could the rigour of mathematical demonstration be in any degree prejudiced by its use, provided that every such consequence were stated only as a contingent truth, until either the principle itself had been as far as necessary apodictically established, or some other mode of demonstration substituted in its place. If this plan were followed out, it is not unlikely that the path would ultimately be discovered leading back to the demonstration of the fundamental principle, and, in the meanwhile, the *à priori* probability of its truth (if supposed to be inferior to moral certainty) would be confirmed by each additional experience of the correctness of the results to which it might be found to conduct.

Under this point of view it may not be uninteresting to show how the principle in question affords an almost instantaneous demonstration of the celebrated theorem of the resolubility of every integer into the sum of four squares.

Lemma. If M be any integer, and $3M = p^2 + q^2 + r^2 + s^2$, M may be expressed under the form $p'^2 + q'^2 + r'^2 + s'^2$.

For it may be observed, that of the four quantities p, q, r, s, either all are divisible by 3, or else one will be so divisible, and each of the others not; in either case, let p be divisible by 3, and give to the absolute values of $\sqrt{q^2}$, $\sqrt{r^2}$, $\sqrt{s^2}$ respectively such signs (if they do not all contain 3) as will make them congruent to one another *quâ* the modulus 3, then

$$M = \frac{p^2 + q^2 + r^2 + s^2}{3} = p'^2 + q'^2 + r'^2 + s'^2,$$

where
$$p' = \frac{\sqrt{q^2} + \sqrt{r^2} + \sqrt{s^2}}{3},$$

$$q' = \frac{\sqrt{r^2} - \sqrt{s^2} + p}{3},$$

$$r' = \frac{\sqrt{s^2} - \sqrt{q^2} + p}{3},$$

$$s' = \frac{\sqrt{q^2} - \sqrt{r^2} + p}{3};$$

consequently p', q', r', s' in either case, are all of them integers.

Suppose N to be odd, and of the form $4\mu + 1$; take the expression $3^{2x+1}N - 2$, and let T be one of the primes which, by virtue of our *principle* (since obviously in this case there is no constant factor), we assume it must contain. Then T is a prime number of the form $4\mu + 1$, that is, the sum of two squares, and consequently $T + 2$, that is, $3^{2x+1}N$ is the sum of four squares, whence, by the Lemma, it follows that N is the same.

In like manner if N is of the form $4\mu + 3$, we take T, one of the primes contained in the form $3^{2x}N - 2$, and as before $T + 2$, that is, $3^{2x}N$, and consequently N will be the sum of four squares.

If N be even, we may obviously consider it to be of the form $4\mu + 2$ (since the theorem, if true for N, will be so for $4N$), and then if T be a prime contained in the form $3^xN - 1$, $T + 1$ will be the sum of three squares, or which is the same thing of four squares, of which zero is one, and the reasoning is the same as before. Hence, in all cases, N is the sum of four squares; and the same result might be obtained with equal or greater facility by the application of the *principle* to various other forms.