54.

ON THE RESULTANT OF TWO CONGRUENCES.

[*Johns Hopkins University Circulars*, I. (1881), p. 131.]

LET an integer function of a variable be understood to mean an integral rational function thereof whose coefficients are all of them positive or negative integers.

Suppose p to be a fixed prime number; any integer function which is contained in $Fx + p\psi x$, where ψ is an arbitrary integer form, may be termed a modular factor of Fx and all modular factors which are equivalent (quâ the fixed modulus) may be regarded as identical.

An integer function containing no modular factor (except itself) may be regarded as modularly irreducible, and as a very advantageous *façon de parler* may be affirmed to have as many modular roots as there are units in its degree. If linear, there is one modular root which is *actual*, in other cases the modular roots may be termed *hypothetic*, (words which seem preferable to *real* and *imaginary* for the purpose in view). The theorem of Galois, that the number of modular roots of any integer function is the same as the number of units in its degree, is then tantamount to the affirmation that just as an integer number is capable of being resolved in only one way into a product of prime integer factors, so an integer function can be resolved in only one way into a product of modularly irreducible factors.

If one integer root of an irreducible integer function is also a root of a second function, it is well known that all the roots of the first are roots of the second: from that it follows that, *If the resultant of two integer functions vanishes, they must have an irreducible factor in common.* This is analogous to, or, rather is, so to say, an exaltation of, the fact that if the resultant of two real functions of a variable vanishes, they must have a real factor, linear or quadratic, in common*; indissoluble association of pairs of imaginary roots in the world of real quantity being the analogue of indissoluble association of groups of hypothetic roots in the world of integer numbers. In what immediately precedes, the factors spoken of are ordinary algebraical factors. If now we pass from ordinary to modular factors or roots, the theorem above stated, on the introduction of the word 'modular', becomes the theorem referred to by Professor Smith, in the *British Association Report*, 1860, p. 162, and by Mr Hathaway at the last meeting, which may be thus expressed: "*If the resultant of two integer functions is modularly zero* (that is, contains the modulus), *they must have a modular factor in common.*"

* So as a particular exemplification, if one of two integral rational functions with only real coefficients has no real root and their resultant vanishes, they must have two roots in common.