XXVIII.—*On a Proposition in the Theory of Numbers.* By BALFOUR STEWART,
Esq., of the Kew Observatory.

(Read 21st April 1856.)

Problem. If p be one of the roots of the equation $x^m - 1 = 0$, (not 1,) then $(1-p)(1-p^2) \dots (1-p^{m-1}) = m$, provided m is a prime number.

If m be not a prime number, and if $p_1 = \cos \frac{2\pi}{m} + \sqrt{-1} \sin \frac{2\pi}{m}$, the same will hold for all roots $p = p_1^\alpha$, where α is a number $< m$ and prime to m . But for all roots $p = p_1^\alpha$, where α , or one of its prime factors, is also a prime factor of m , the product $(1-p)(1-p^2) \dots (1-p^{m-1})$ will be equal to 0.

Preliminary Propositions.

I. If m be a prime number, and α, β two numbers, each less than m ; and if $\alpha\beta = \gamma m + \delta$, where δ is less than m ; then δ is neither equal to α nor to β .

For if $\delta = \alpha$, we shall have $\alpha(\beta - 1) = \gamma m$, where α and $\beta - 1$ are both less than m , which clearly violates the well-known theorem that a number cannot be made up in two ways of prime factors.

II. Again, if $\alpha(\beta + \beta_1) = \gamma_1 m + \delta_1$ (where $\beta + \beta_1 < m$); then δ_1 is not equal to δ .

For if $\delta_1 = \delta$, then $\alpha(\beta + \beta_1) = \gamma_1 m + \delta$

$$= (\gamma_1 - \gamma) m + \gamma m + \delta$$

$$= (\gamma_1 - \gamma) m + \alpha \beta$$

$$\text{therefore} \quad \alpha \beta_1 = (\gamma_1 - \gamma) m,$$

or a number is made up in two ways of prime factors, which is impossible.

III. If, therefore, we arrange in a horizontal row all the numbers in order of magnitude from 1 to $\overline{m-1}$ inclusive, and the same in a vertical row downwards, so that the two columns shall form the adjacent sides of a square, and if we multiply each successive number in the top horizontal column by the number in the vertical (as in the multiplication table), divide the product by m , and write down the remainders: then none of these remainders will be the same, for they will not be the multiplier itself (Prop. I.), nor, 2°, will any two be alike (Prop. II.). The multiplier and remainders will contain all the numbers from

1	2	3	4	5	6
2					
3	6	2	5	1	4
4	1	5	2	6	3
5					
6					

1 to $\overline{m-1}$ inclusive, though not in order of magnitude. We have exhibited this in the margin for $m=7$, the multipliers being 3 and 4.

IV. If m be not a prime, but composed of the prime factors $a \times b \times c \times d \times e \times f \times \dots$, and if a or one of its prime factors (f) be also one of the prime factors of m , then in some case will $a\beta = \gamma m$, where β is one of the numbers 1, 2, 3, $\dots$, $\overline{m-1}$.

For $\frac{m}{f}$ and $\frac{\alpha}{f}$ are whole numbers $< m$; and $a \cdot \frac{m}{f} = \frac{\alpha}{f} \cdot m$, which satisfies the condition.

V. If neither a nor any of its prime factors is also a prime factor of m , then there will be a remainder $\delta < m$ whatever be β .

For if not, let $a\beta = \gamma m$; then since $m > \beta \therefore \gamma < a$. Therefore γ is either prime to a , or there is a factor in a which is not in γ : but this factor is, by hypothesis, not in m : it is, consequently, not in γm , which is absurd.

VI. The remainders will be different for every different value of β . For if possible, let

$$\begin{aligned} a\beta &= \gamma m + \delta \\ a(\beta + \beta_1) &= \gamma_1 m + \delta \\ &= (\gamma_1 - \gamma) m + a\beta \end{aligned}$$

therefore, $a\beta_1 = (\gamma_1 - \gamma)m$ which, as in the last Prop., is impossible.

VII. If, then, we arrange the numbers as in Prop. III., we shall have 0 amongst the remainders, for all values of a which either divide m , or have a prime factor in common with it; whilst, for all other values of a , we shall have the same results as in Prop. III. This is shown for $m=8$ in the margin, for the multipliers 3, 4, and 6.

1	2	3	4	5	6	7
2						
3	6	1	4	7	2	5
4	0	4	0	4	0	4
5						
6	4	2	0	6	4	2
7						

Problem 1. If m be a prime number, the roots of the equation $x^m - 1 = 0$ are $1, p_1, p_1^2, \dots, p_1^{m-1}$ where $p_1 = \cos \frac{2\pi}{m} + \sqrt{-1} \sin \frac{2\pi}{m}$.

For, from the theory of equations,

$$x^m - 1 = (x-1)(x-p_1)(x-p_1^2) \dots (x-p_1^{m-1})$$

or

$$x^{m-1} + x^{m-2} + \dots + 1 = (x-p_1)(x-p_1^2) \dots$$

putting 1 for x ,

$$m = (1-p_1)(1-p_1^2) \dots (1-p_1^{m-1}).$$

If $p = p_1^\alpha$,

since $p_1^m = 1$,

$$p_1^{\alpha m} = 1;$$

and if $a\beta = \gamma m = \delta$,

$$p_1^{\alpha\beta} = p_1^\delta$$

hence, $(1-p_1^\alpha)(1-p_1^{2^\alpha}) \dots (1-p_1^{(m-1)^\alpha})$ will be the same as

$$(1-p_1^{\delta_1})(1-p_1^{\delta_2}) \dots (1-p_1^{\delta_{m-1}}),$$

where $\delta_1, \delta_2, \&c.$ are the remainders. But, by Prop. III., $\delta_1, \delta_2, \&c.$, are all different, and are the numbers $1, 2, \dots, \overline{m-1}$: hence,

$$\begin{aligned} (1-p)(1-p^2) \dots (1-p^{m-1}) &= (1-p_1^\alpha)(1-p_1^{2^\alpha}) \dots \\ &= (1-p_1)(1-p_1^2) \dots (1-p_1^{m-1}) \\ &= m. \end{aligned}$$

Problem 2. If m be not a prime number, the same equation is true, by Prop. VII., for $p=p_1^\alpha$, where α is less than, and prime to m ; but if α or one of its prime factors is a prime factor of m , then one of the factors $(1-p_1^\alpha)(1-p_1^{2^\alpha}) \dots (1-p_1^{(m-1)^\alpha})$ will be of the form $1-p_1^{\gamma m}=0$; and, consequently, the product itself will be equal to 0.