In a similar manner it can be shewn that if $f(x, y, t)$ be a solution of the equation

$$\frac{\partial V}{\partial t} = a^2 \left(\frac{\partial^2 V}{\partial x^2} + \frac{\partial^2 V}{\partial y^2} \right),$$

then the expression

$$\frac{1}{t} e^{-\frac{x^2+y^2}{4a^2t}} f\left(\frac{x}{t},\ \frac{y}{t},\ -\frac{1}{t}\right)$$

is also a solution. In particular, we have the solution

$$\frac{1}{t} e^{-\frac{x^2+y^2}{4a^2t}} \left\{ F\left(\frac{x+iy}{t}\right) + f\left(\frac{x-iy}{t}\right) \right\},$$

given by Earnshaw in his *Theory of Germs*. It was in attempting to test the generality of the results given by Earnshaw that I discovered the above theorem.

ON SOME SQUARE ROOTS OF UNITY FOR A PRIME MODULUS.

By *H. W. Lloyd Tanner, M.A., F.R.A.S.*

1. An example of the square roots in question is the power $x^{\frac{1}{2}(p-1)}$, where p is the prime modulus and x is any of the numbers $1, 2, \ldots, p-1$; the value 0 being excluded. This power is ± 1 for all the values of x considered; viz., it is 1 when x is a quadratic residue, mod. p, and -1 when x is a non-residue. In the following paper it is proposed to determine all the expressions

$$A + Bx + Cx^2 + \ldots + Dx^{p-2}, = Fx,$$

which have a similar property, viz. $Fx \equiv \pm 1$ for every proper (*i.e.* non-vanishing) value of x. The distribution of the signs $\pm$ of Fx for the different values of x is however arbitrary, and every such distribution gives rise to a particular form of Fx. Since there is a choice of two values for $F1$, for $F2$, ..., and for $F(p-1)$, there are 2^{p-1} different forms of Fx.*

* Similarly, if δ is any factor of $p-1$ ($\delta\delta' - p - 1$ say), there are δ^{p-1} different δ^{th} roots of unity, mod. p. Also there are $2^{\delta'}$ different square roots of the form $F(x^2)$ and $\delta^{\delta'}$ different δ^{th} roots of the form $F(x^{\delta})$.

2. The $p-1$ coefficients of Fx are given by the $p-1$ linear congruences,

$$A+B.1+C.1^2+\ldots+D.1^{p-2}\equiv F1, \text{ mod. } p,$$
$$A+B.2+C.2^2+\ldots+D.2^{p-2}\equiv F2,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

where the values $F1$, $F2$, ..., are supposed to be known.

The system is consistent; for its determinant, being the product of the differences of 1, 2, ..., $p-1$, cannot be 0. (It is in fact ± 1, being a square root of the discriminant of $x^{p-1}-1$). It follows that a square root, Fx, actually exists for every one of the 2^{p-1} different arrangements of signs in $F1$, $F2$, ..., $F(p-1)$.

3. There is an interesting modification of this process. We can write Fx in the form

$$Fx = a+bx^2+\ldots+cx^{p-3}+x^q(\alpha+\beta x^2+\ldots+\gamma x^{p-3})$$
$$= f(x^2)+x^q.\phi(x^2),$$

where q is an odd number, namely the greatest odd factor of $p-1$; so that

$$p=2^\lambda.q+1.$$

The definition of Fx gives

$$(fx^2+x^q.\phi x^2)^2\equiv 1, \text{ mod. } p \quad \ldots\ldots\ldots\ldots(1),$$

and, since this congruence is true also for $-x$,

$$(fx^2-x^q.\phi x^2)^2\equiv 1.$$

By subtraction, we get

$$x^q.\phi x^2.fx^2\equiv 0 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2).$$

From (2) and (1) it follows that for every proper value of x either

$$\phi x^2\equiv 0, \text{ and } fx^2\equiv Fx,$$

or

$$fx^2\equiv 0, \text{ and } \phi x^2\equiv x^{-q}Fx.$$

It is obvious that the former case, $\phi x^2\equiv 0$, arises when

$$Fx\equiv F(-x),$$

and the latter, $fx^2\equiv 0$, when

$$Fx\equiv -F(-x).$$

Now suppose that $fx^2 \equiv 0$ when $x = \pm g, \pm h, \dots, \pm k$ ($2r$ values), and ϕx^2 when $x = \pm s, \pm t, \dots$, ($p - 1 - 2r$ values). Then fx^2 is divisible by $(x^2 - g^2)(x^2 - h^2) \dots (x^2 - k^2)$, that is to say

$$fx^2 = (x^2 - g^2)(x^2 - h^2) \dots (x^2 - k^2) f_1 x^2 \dots\dots\dots (3).$$

To calculate the $\frac{1}{2}(p-1) - r$ coefficients of $f_1 x^2$, we have the congruences

$$(x^2 - g^2)(x^2 - h^2) \dots (x^2 - k^2) f_1 x^2 \equiv Fx,$$

when $x^2 = \pm r, \pm s$, &c. When $f_1 x^2$ is found, fx^2 is given by (3). In the same way ϕx is obtained, and thus Fx. It will be observed that in this process only $\frac{1}{2}(p-1)$ coefficients have to be calculated from congruences instead of $p - 1$.

Although it is so easily explained, the property indicated by (2)—that for each value of x, the value of Fx is determined solely by the even powers of x or solely by the odd powers—strikes me as worthy of remark. In the particular case of $x = 1$ it gives the theorem that in any square root Fx, the sum of the coefficients of the even powers, *or* the sum of the coefficients of the odd powers is divisible by y. The sum which is not so divisible is $\equiv \pm 1$, mod. p.

4. A third method is based on the remark that Fx, $F_1 x$ being two square roots, then $F(ax)$ (where $a = 1, 2, \dots$, or $p - 1$), $F(x^n)$, and $Fx \times F_1 x$ are also square roots. Now we have

$$(\chi x =)\ (x^{p-1} - 1)/(x - 1) \equiv -1, \text{ when } x = 1$$
$$\equiv \quad 0, \text{ when } x = 2, 3, \dots, p - 1;$$

therefore
$$a\chi x + b \equiv -a + b, \text{ when } x = 1$$
$$\equiv \quad b, \text{ when } x = 2, 3, \dots, p - 1.$$

Thus, putting $a = 2$, $b = 1$, we find that

$$2\chi x + 1, = 3 + 2x + 2x^2 + \dots + 2x^{p-2}, = F_1 x \text{ say},$$

is a square root of 1, mod. p. The distribution of signs may be denoted by

$$F_1 x = - + \ + \dots +,$$

meaning that $F_1 x = -1$ when $x = 1$, and $= +1$ for other values.

Another square root of 1 is

$$F(a^{-1}x) = 3 + 2a^{-1}x + 2a^{-2}x^2 + \dots + 2ax^{p-2}.$$

Now $F_1(a^{-1}x) \equiv F_1(1) \equiv -1$, when $x = a$ and is + for all other values of x.

Hence $\qquad F_1(a^{-1}x) = + \; + \; + \ldots - \ldots +,$

the solitary – occurring in the a^{th} place.

To obtain a square root whose sign symbol contains – in the a^{th}, b^{th}, ..., and c^{th} places, and nowhere else, we form the product

$$F_1(a^{-1}x)\,F_1(b^{-1}x)\ldots F_1(c^{-1}x).$$

It is clear that in this way all the forms of Fx can be calculated.

5. It would be very laborious to perform the multiplications indicated; but an artifice gives the result without much trouble.

For all proper values of x,

$$(1 + x + \ldots + x^{p-2})(\alpha + \beta x + \ldots + \delta x^{p-2})$$
$$\equiv (1 + x + \ldots + x^{p-2})(\alpha + \beta + \ldots + \gamma), \text{ mod. } p.$$

For, when $x \equiv 1$ the two sides become identical in form, and when x is not $\equiv 1$ the first factor of each side vanishes, mod. p.

Now $\qquad F_1x = 1 + 2(1 + x + x^2 + \ldots + x^{p-2}).$

Hence $\qquad F_1x \times (\alpha + \beta x + \ldots + \gamma x^{p-2})$

$$\equiv \alpha + \beta x + \ldots \gamma x^{p-2} + 2\sigma(1 + x + \ldots + x^{p-2})$$
$$\equiv \alpha + 2\sigma + (\beta + 2\sigma)x + \ldots + (\gamma + 2\sigma)x^{p-2},$$

where σ is the sum of the coefficients α, β, ..., γ.

The sum of the coefficients of $F_1(ax)$ is F_1a, and this is $+1$ save in the useless case when $a = 1$. Hence, the product

$$F_1x \,.\, F_1(ax)$$

can be written down by adding 2 to each of the coefficients of $F_1(ax)$. In this change x into bx, where b may or may not be equal to a. The sum of the coefficients, $= F_1b \,.\, F_1(ab)$, is 1 (unless b or ab is 1). Therefore the product

$$F_1x \,.\, F_1(bx)\,F_1(abx)$$

is formed by adding 2 to each of the coefficients of the previously found product $F_1(bx) \,.\, F_1(abx)$. Thus, by alternately replacing x by a suitable multiple, and adding 2 to each of the coefficients, we can obtain any one of the products required in the preceding paragraph. There is a certain range of choice in the multipliers a, b, c, ..., and the derivation of $F(ax)$ from Fx is facilitated by processes on which it is not necessary to enlarge.

6. The function

$$F_1(x^\delta), = 1 + 2\delta\,(1 + x^\delta + x^{2\delta} + \ldots + x^{p-1-\delta}),$$

which will be indicated by $F_\delta(x)$, has properties similar to those of $F_1 x$. It may be used as a multiplier for functions of x^δ, the product being formed by adding $2\delta\sigma$ to each coefficient of the multiplicand, σ being, as before, the sum of these coefficients. Thus all the square roots, $F(x^\delta)$, can be independently found. These can now serve as multiplicands for $F_1 x$, and probably this would be the most rapid process for obtaining the complete set of roots.

In illustration, the square roots, Fx^2, for modulus 11 are here determined.

We have $\quad F_2 x = 5 + 4x^2 + 4x^4 + 4x^8 + 4x^6 \ldots (A)$;

therefore $\quad F_2(2x) = 5 + 5x^2 + 9x^4 + 1x^8 + 3x^6 \ldots (B)$;

therefore $\quad F_2 x \,.\, F_2(2x) = 9 + 9x^2 + 2x^4 + 5x^8 + 7x^6 \ldots (C)$;

therefore $\quad F_2(2x) \,.\, F_2(4x) = 9 + 3x^2 + 10x^4 + 4x^8 + 8x^6 \ldots (D)$,

and $\quad F_2(4x) \,.\, F_2(8x) = 9 + 1x^2 + 6x^4 + 1x^8 + 6x^6 \ldots (E)$.

The powers of x are here arranged with the indices in geometric progression, (mod. 10), to take advantage of the fact that $(p-1)/\delta$ is in this case a prime number. The substitution of $2x$ for x is effected by multiplying the last four coefficients by 4, 5, 3, 9 respectively. It so happens that this is the only substitution required. But if it were required to multiply x by any other number the multipliers would still be a cyclic substitution of 4, 5, 3, 9. For instance, to get (E) independently, we might proceed thus:

$$F_2(6x) = 5 + 1x^2 + 3x^4 + 5x^8 + 9x^6,$$

the multipliers being $3\ (\equiv 6^2)$, 9, 4, 5;

therefore $\quad F_2 x \,.\, F_2 6x = 9 + 5x^2 + 7x^4 + 9x^8 + 2x^6$;

therefore $\quad F_2 8x \,.\, F_2 4x = 9 + 1x^2 + 6x^4 + 1x^8 + 6x^6$,

the multipliers being $9\ (\equiv 8^2)$, 4, 5, 3.

To complete the determination, in each of the functions marked A, B, C, D, E, replace x by x^3, (2 being a primitive root of 1, mod. 5), and repeat the operation.

It is seen that this is equivalent to a cyclic transposition of the last four coefficients.

For example, (B) gives the functions whose coefficients are (5; 9, 1, 3, 5), (5; 1, 3, 5, 9), and (5; 3, 5, 9, 1). There are thus four distinct functions implied in (B), and as each may have either sign prefixed, B gives 8 square roots. So likewise (C), (D) give 8; E, 4; and A, 2.

There are also the trivial roots ± 1; and in all we have

$$3 \times 8 + 4 + 2 + 2 = 32$$

square roots. This is the full number, 2^5, of square roots, mod. 11, which are functions of x^2.

7. The square roots for $p = 3, 5, 7$ are given below. The numbers appended indicate the number of square roots implied by the formula on the same line. In explanation it may be added that an expression

$$f(x^2) + x^q . \phi(x^2)$$

may be affected with $\pm$; x may be replaced by $-x$, so that the sign of the second term may be changed independently of the first; and when $(p-1)/2 = q$, (= an odd number), fx^2 and ϕx^2 may be interchanged, this being equivalent to multiplying by $x^{\frac{1}{2}(p-1)}$ which is a square root of 1.* These are the only changes unexpressed in the following list, and they give either 2, 4 or 8 roots for each formula.

$$
\begin{array}{lll}
p = 3, & \pm 1, \ \pm x & 4,
\end{array}
$$

$$
\left.\begin{array}{lll}
p = 5, & \pm 1, \ \pm x^2 & 4, \\
 & x(3 + x^2), \ x(1 + 3x^2) & 4, \\
 & 3 + 2x^2 + x(2 + 2x^2) & 4, \\
 & 2 + 2x^2 + x(1 - x^2) & 4
\end{array}\right\} = 16.
$$

$$
\left.\begin{array}{lll}
p = 7, & \pm 1, \ \pm x^3 & 4, \\
 & 5 + 4x^2 + 4x^4 & 4, \\
 & 5 + 2x^2 + x^4 & 4, \\
 & 5 + x^2 + 2x^4 & 4, \\
 & (3 + 2x^2 + 2x^4) + x^3(2 + 2x^2 + 2x^4) & 8, \\
 & (3 + x^2 + 4x^4) + x^3(2 + x^2 + 4x^4) & 8, \\
 & (3 + 4x^2 + x^4) + x^3(2 + 4x^4 + x^4) & 8, \\
 & (2 + 2x^2 + 2x^4) + x^3(\ \ + 3x^2 - 3x^4) & 8, \\
 & (2 + x^2 + 4x^4) + x^3(\ \ 2x^2 - x^4) & 8, \\
 & (2 + 4x^2 + x^4) + x^3(\ \ x^2 - 2x^4) & 8,
\end{array}\right\} = 64.
$$

* It may be noted that, when $q = \frac{1}{2}(p-1)$, $\pm fx^2 \pm \phi x^2$ is a square root, a theorem which gives an easy check upon the calculations. The roots for $p = 7$ furnish examples.

Univ. Coll., Cardiff.