A PROOF OF THE THEOREM OF RECIPROCITY FOR QUADRATIC RESIDUES.

By *F. Franklin*, Assistant Professor in the Johns Hopkins University.

1. It was shewn by Gauss that, p being an odd prime, $D^{\frac{1}{2}(p-1)} \equiv 1$ or -1 (mod. p) according as, in the series

$$D,\ 2D,\ 3D,\ \ldots,\ \tfrac{1}{2}(p-1)D,$$

the number of numbers whose least positive remainder (mod. p) exceeds $\frac{1}{2}p$ is even or odd. But to say that the least positive remainder of λD exceeds $\frac{1}{2}p$ is the same as to say that $E\frac{2\lambda D}{p}$ is an odd number. Hence we have the transformed criterion: *D is a quadratic residue or non-residue of p* according as the number of odd numbers in the series

$$E\frac{2D}{p},\ E\frac{4D}{p},\ \ldots,\ E\frac{(p-1)D}{p}$$

is even or odd: hence *according as*

$$E\frac{2D}{p} + E\frac{4D}{p} + \ldots + E\frac{(p-1)D}{p}$$

is even or odd.

2. *If a and b be any two relative primes,*

$$E\frac{a}{b} + E\frac{2a}{b} + E\frac{3a}{b} + \ldots + E\frac{(b-1)a}{b} = \tfrac{1}{2}(a-1)(b-1).$$

For, if we write under this series the same series reversed, the sum of the two complete fractions in any column is a; therefore, each being actually fractional, the sum of their integer parts is $a-1$; hence the sum of the proposed series is $\frac{1}{2}(a-1)(b-1)$.

3. Let us denote *the number of odd numbers* in a set by prefixing the symbol I (impar.); then, *if a and b are odd relative primes,*

$$I\left\{E\frac{2a}{b},\ E\frac{4a}{b},\ \ldots,\ E\frac{(b-1)a}{b}\right\}$$
$$= \tfrac{1}{2}I\left\{E\frac{a}{b},\ E\frac{2a}{b},\ E\frac{3a}{b},\ \ldots,\ E\frac{(b-1)a}{b}\right\}.$$

For, in the complete set, if any term is odd its symmetrical is odd (their sum being $a-1$, an even number); and if one of these terms belongs to the even set $\left(E\frac{2a}{b},\ E\frac{4a}{b},\ \ldots\right)$, the other does not. Hence the even set contains half as many odd numbers as the complete set. Q. E. D.

4. By 2,

$$E\frac{D}{p}+E\frac{2D}{p}+E\frac{3D}{p}+E\frac{4D}{p}+\ldots$$
$$+E\frac{(p-2)D}{p}+E\frac{(p-1)D}{p}=\tfrac{1}{2}(p-1)(D-1).$$

And if $D<p$, it is plain that

$$-E\frac{D}{p}+E\frac{2D}{p}-E\frac{3D}{p}+E\frac{4D}{p}-\ldots-E\frac{(p-2)D}{p}+E\frac{(p-1)D}{p}$$
$$=I\left\{E\frac{p}{D},\ E\frac{2p}{D},\ E\frac{3p}{D},\ \ldots,\ E\frac{(D-1)p}{D}\right\};$$

for $E\frac{2\lambda D}{p}-E\frac{(2\lambda-1)D}{p}$ is 1 or 0 according as there is or is not a multiple of p between $(2\lambda-1)D$ and $2\lambda D$; in other words, it is 1 as many times as there are multiples of p, not exceeding $(p-1)D$, whose quotient by D is an odd number; whence the above equation.

Adding the equations above written, we have

$$E\frac{2D}{p}+E\frac{4D}{p}+\ldots+E\frac{(p-1)D}{p}$$
$$=\frac{p-1}{2}\,\frac{D-1}{2}+\tfrac{1}{2}I\left\{E\frac{p}{D},\ E\frac{2p}{D},\ \ldots,\ E\frac{(D-1)p}{D}\right\}.$$

If D is odd, this becomes, by 3,

$$E\frac{2D}{p}+E\frac{4D}{p}+\ldots+E\frac{(p-1)D}{p}$$
$$=\frac{p-1}{2}\,\frac{D-1}{2}+I\left\{E\frac{2p}{D},\ E\frac{4p}{D},\ \ldots,\ E\frac{(D-1)p}{D}\right\}$$
$$\equiv\frac{p-1}{2}\,\frac{D-1}{2}+E\frac{2p}{D}+E\frac{4p}{D}+\ldots+E\frac{(D-1)p}{D}\ (\text{mod. }2).$$

Hence, if D is an odd prime, the quadratic characters of D with respect to p and of p with respect to D are the same, unless $\frac{1}{2}(p-1)$ and $\frac{1}{2}(D-1)$ are both odd, in which case the characters are opposite.