An Infinite Product of Euler.

In a letter to Stirling, dated July 27, 1738, Euler mentions having happened on the infinite product, "satis notatu dignam," $\frac{3.5.7.11.13.17.19\ldots}{4.4.8.12.12.16.20\ldots}$, the numerators being the odd primes in their natural order, the denominators the multiples of 4 nearest to those primes. He says he can prove that the limit of this product is $\frac{\pi}{4}$. His proof was probably as follows:

$$\frac{3.5.7.11.13.17.19\ldots}{4.4.8.12.12.16.20\ldots} = \left(1+\frac{1}{3}\right)^{-1}\left(1-\frac{1}{5}\right)^{-1}\left(1+\frac{1}{7}\right)^{-1}\left(1+\frac{1}{11}\right)^{-1}\left(1-\frac{1}{13}\right)^{-1}\cdots$$

$$= \left(1-\frac{1}{3}+\frac{1}{3^2}-\frac{1}{3^3}+\ldots\right)\left(1+\frac{1}{5}+\frac{1}{5^2}+\ldots\right)\left(1-\frac{1}{7}+\frac{1}{7^2}-\ldots\right)\left(1-\frac{1}{11}+\frac{1}{11^2}-\ldots\right)(\ldots)$$

$$= \sum_{n=0}^{\infty}(-)^n\frac{1}{2n+1} = \arctan 1 = \frac{\pi}{4}.$$

A. C. AITKEN.

An Elementary Proof of Girard's Theorem.

Girard enunciated in 1625 the following celebrated theorem, which is associated with the name of Fermat:

Every prime of the form $4m+1$ is the sum of two squares in one way only, and no prime of the form $4m-1$ is a factor of the sum of two squares that are not both multiples of that prime.

The theorem will be deduced here from an immediate corollary of the H.C.F. theorem, namely that if a is prime to b, we may find c and d such that $ad-bc=k$, where k is any assigned integer.

§ 1. If k is less than and prime to n, and q is given, only one number h less than n exists such that $kh \equiv q \pmod{n}$.

At least one exists, for, since k is prime to n, we may find c and d such that $kc - nd = q$, and c may be set as $pn + h$ $(h < n)$, so that $kh \equiv q \pmod{n}$.

Now suppose another such number h_1 exists.

Then $k(h - h_1) \equiv 0 \pmod{n}$.

$\therefore$ since k is prime to n, $h - h_1$ must be a multiple of n, which is impossible, since h and h_1 are unequal and each less than n.

$\therefore$ h is the only number less than n such that $kh \equiv q \pmod{n}$.

§ 2. If P is an odd prime and q is given, only two, if any, numbers k and $P - k$ less than P exist such that $k^2 \equiv q \pmod{P}$.

For suppose two others k_1 and $P - k_1$ exist and let k and k_1 be the odd members of these pairs.

Then $k^2 - k_1^2 = (k + k_1)(k - k_1) \equiv 0 \pmod{P}$.

$\therefore$ since $k - k_1$ is not zero, $k + k_1$ must be a multiple of P, which is impossible, since $k + k_1$ is even, but less than $2P$.

Hence k and $P - k$ are the only numbers, if any, less than P such that $k^2 \equiv q \pmod{P}$.

§ 3. (*a*) If P is a prime of the form $4m + 1$, and q is given, not a multiple of P, two and only two numbers k and $P - k$ less than P exist such that $k^2 + q^2 \equiv 0 \pmod{P}$.

(*b*) If P is a prime of the form $4m - 1$, no numbers satisfy the congruence $x^2 + q^2 \equiv 0 \pmod{P}$.

(*a*) Consider all the $4m$ numbers less than P. By §1, each number h may be paired with a number h_1 so that $hh_1 \equiv q^2 \pmod{P}$.

If $q \equiv r$, $r < P$, then r and $P - r$ can only be paired with themselves, forming squares congruent with q^2; by § 2, they are the only two such numbers less than P. Remove them.

The remaining $4m - 2$ numbers may be put into $2m - 1$ pairs (h, h_1). Each pair (h, h_1) may in turn be associated with a "conjugate" pair $(P - h, P - h_1)$.

Since the number of pairs is odd, a certain pair $(k, P - k_1)$ is left over. But its conjugate $(P - k, k_1)$ exists. Hence it must be identical with $(k, P - k_1)$, so that, since k is not equal to $P - k$, we have $k = k_1$, and $\therefore$ $k(P - k) \equiv q^2$, *i.e.* $k^2 + q^2 \equiv 0 \pmod{P}$.

Also by § 2, k and $P-k$ are the only such numbers less than P. Moreover k and q can both be less than $\frac{1}{2}P$, so that we may write $P.Q = k^2+q^2$, where Q is less than $\frac{1}{2}P$.

(b) Now let P be of the form $4m-1$.

Removing as before r and $P-r$, where $q \equiv r$, we have left $4m-4$ numbers, which may, as in (a), be put in pairs (h, h_1).

Assume a pair $(k, P-k)$ exists. Remove it.

There remains an odd number of pairs, $2m-3$.

$\therefore$ by reasoning similar to that of (a), there must be among these a pair $(l, P-l)$.

But then we should have *four* numbers k, l, $P-k$, $P-l$, all satisfying the congruence $x^2+q^2 \equiv 0 \pmod{P}$, which is impossible, by § 2.

Hence our assumption is wrong, and there is no number less than P, and therefore no number at all, satisfying $x^2+q^2 \equiv 0 \pmod{P}$.

Thus is proved the negative part of Girard's Theorem, that a prime of the form $4m-1$ cannot be a factor of the sum of two squares which do not both contain that prime.

Hence the only factors of the sum of two squares prime to each other are primes of the form $4m+1$ or the prime 2.

§ 4. We shall now generalize a theorem of Euler, and prove that if $p^2+q^2 = N_0 . N_1 . N_2 . N_3 \ \ldots \ N_k$, where N_0, N_1, N_2, ... etc. are prime factors of p^2+q^2, and if all the factors except N_k are given as the sums of two squares (necessarily prime to each other), then N_k is also the sum of two squares.

Let $N_0 = a_0^2+b_0^2$, $N_1 = a_1^2+b_1^2$, ... etc.

Then $p^2+q^2 = (a_0^2+b_0^2)(a_1^2+b_1^2) \ \ldots \ N_k$.

Since a_0 is prime to b_0, we may find c and d such that

$$a_0 d - b_0 c = p.$$

Let $q = a_0 c + b_0 d + e$.

Then $(a_0 d - b_0 c)^2 + (a_0 c + b_0 d + e)^2 = (a_0^2+b_0^2)(a_1^2+b_1^2) \ \ldots \ N_k$,

i.e. $(a_0^2+b_0^2)(c^2+d^2) + e^2 + 2e(a_0 c + b_0 d) = (a_0^2+b_0^2)(a_1^2+b_1^2) \ \ldots \ N_k$.

$\therefore \ e\{e + 2(a_0 c + b_0 d)\}$ is a multiple of the prime $a_0^2+b^2$.

$\therefore$ either e or $e+2(a_0 c + b_0 d)$ is a multiple.

https://doi.org/10.1017/S1757748900001766 Published online by Cambridge University Press

If $e = M(a_0^2 + b_0^2)$, then $e\{e + 2(a_0 c + b_0 d)\} = (a_0^2 + b_0^2)\{M^2(a_0^2 + b_0^2) + 2M(a_0 c + b_0 d)\}$; and if $e + 2(a_0 c + b_0 d) = M(a_0^2 + b_0^2)$, then $e\{e + 2(a_0 c + b_0 d)\} = (a_0^2 + b_0^2)\{M^2(a_0^2 + b_0^2) - 2M(a_0 c + b_0 d)\}$.

In any case, dividing by $(a_0^2 + b_0^2)$, we have

$$c^2 + d^2 + M^2(a_0^2 + b_0^2) \pm 2M(a_0 c + b_0 d) = (a_1^2 + b_1^2)(a_2^2 + b_2^2) \ldots N_k,$$

i.e. $(Ma_0 \pm c)^2 + (Mb_0 \pm d)^2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) \ldots N_k$,
which we may write $p_1^2 + q_1^2 = N_1 . N_2 . N_3 . \ldots N_k$.

From this we may derive in a similar manner

$$p_2^2 + q_2^2 = N_2 . N_3 . N_4 \ldots N_k,$$

and so on, and finally $p_k^2 + q_k^2 = N_k$, was to be proved.

§ 5. It may now be shown that every prime of the form $4m + 1$ is the sum of two squares.

By § 3 (*a*), if P is such a prime, we may find Q, R, S ..., primes of form $4m + 1$ less than P, such that $P . Q . R . S \ldots = a^2 + b^2$.

Now, by § 4, P is the sum of two squares if the lower primes Q, R, S ... are the sums of two squares.

Each of Q, R, S ... is in its turn the sum of two squares if still lower primes of the form $4m + 1$ are sums of two squares.

Thus ultimately the condition that P is the sum of two squares is that the lowest prime of the form $4m + 1$ shall be the sum of two squares.

This condition is satisfied, since $5 = 2^2 + 1^2$.

Hence P is the sum of two squares.

§ 6. Lastly, to show that the prime P is the sum of two squares in one way only.

Suppose it can be so expressed in two distinct ways, *i.e.* let $P = a^2 + b^2 = c^2 + d^2$, where a, b, c, d are prime to P, and $a > c > d > b$.

Then ac is not equal to bd, and, since $\frac{a}{b}$ is not equal to $\frac{c}{d}$, ad is not equal to bc. .....(i).

Since $(d^2 - b^2)P$, *i.e.* $d^2(a^2 + b^2) - b^2(c^2 + d^2)$ or $a^2 d^2 - b^2 c^2$, is a multiple of P, either $ad + bc$ or $ad - bc$ is a multiple of P, rP. .....(ii).
Similarly either $ac - bd$ or $ac + bd$ is a multiple of P, sP.

https://doi.org/10.1017/S1757748900001766 Published online by Cambridge University Press

Now if $ad + bc$ is a multiple of P, $ac + bd$ cannot be, for, squaring and adding, we should have $P^2 + 4abcd$ a multiple of P, which is impossible, since a, b, c, d are prime to P.

Hence either $ad + bc$ and $ac - bd$ are multiples together, or

$ad - bc$ and $ac + bd$ are multiples together.

In either case, square and add. Then $(a^2 + b^2)(c^2 + d^2)$, *i.e.* $P^2 = (r^2 + s^2) P^2$, so that $r^2 + s^2 = 1$.

Hence one of r or $s = 0$, *i.e.* $ad = bc$ or $ac = bd$, both of which are impossible, by (i). Hence our supposition is wrong, and P can be expressed in one way only as the sum of two squares.

A. C. AITKEN.

Theorem regarding a regular polygon and a circle cutting its sides, with corollary and application to trigonometry.

1. *Theorem.*

If a circle cut all the sides (produced if necessary) of a regular polygon, the algebraic sum of the intercepts, on the sides, between the vertices and the circle is zero.

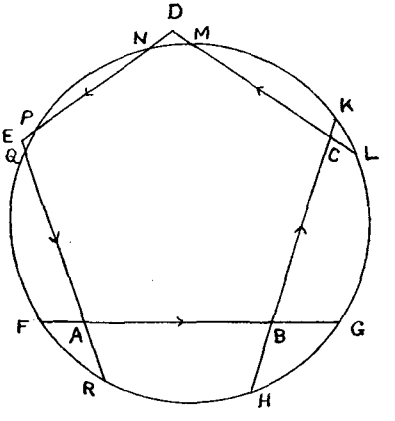

Fig. 1

Consider the case of a regular pentagon $ABCDE$ whose sides are cut by a circle as shown in Fig. 1. Let $AB = x$.

https://doi.org/10.1017/S1757748900001766 Published online by Cambridge University Press