A Geometrical Proof of a Theorem of Hurwitz.

By Dr Lester R. Ford.

(*Read 11th May 1917. Received 14th June 1917.*)

1. In the study of rational approximations to irrational numbers the following problem presents itself: Let ω be a real irrational number, and let us consider the rational fractions satisfying the inequality

$$\left| \frac{p}{q} - \omega \right| < \frac{k}{q^2}; \quad \text{......................} \quad (1)$$

how small can the positive quantity k be chosen with the certainty that there will always be an infinite number of fractions satisfying the inequality whatever the value (irrational) of ω?

Dirichlet proved by elementary means that if $k = 1$, there are infinitely many fractions satisfying the inequality. Later, Hermite gave a method, based on binary quadratic forms, of constructing an infinite suite of fractions approaching an irrational number, all of which satisfy the inequality when $k = 1/\sqrt{3}$; and it is easy to show that infinitely many of the fractions of the suite of Hermite also satisfy the inequality when $k = \frac{1}{2}$.

Finally, Hurwitz* gave the complete solution of the problem by establishing the following theorem:—

If $k = 1/\sqrt{5}$, *there are infinitely many rational fractions satisfying the inequality* (1) *whatever the value* (*irrational*) *of* ω.

If $k < 1/\sqrt{5}$, *there exist infintely many irrational numbers* (*and everywhere dense along the real axis*), *for each of which the inequality* (1) *is satisfied by only a finite number of rational fractions.*

* *Mathematische Annalen* **39** (1891), 279–84.

The problem was also solved by Borel, *Journal de Mathématiques*, 5th Ser., Vol. **9** (1903), 329—.

Since the present paper was read to the Society, there has come to hand the current issue of the *Journal de Mathématiques*, which contains a simple proof of the theorem by Humbert.

The proof given by Hurwitz depends upon continued fractions.

It is the object of the present paper to prove the theorem by considering the geometry of the classic modular division of the half-plane, and thus to exhibit anew the remarkable connexion between this geometry and the theory of numbers.

2. *Geometric statement of the problem.*—In the complex z-plane $(z = x + iy)$ let $z = \omega$ be an irrational point on the x-axis. Through this point let a perpendicular, L, to the x-axis be drawn. At each rational point p/q of the x-axis let a circle $S(p/q\,;\,h)$ be constructed which is tangent to the x-axis at the point p/q, lies in the upper half-plane, and whose radius is $1/2hq^2$. If $S(p/q\,;\,h)$ is intersected by the line L, the distance between p/q and ω is less than the radius, or

$$\left| \frac{p}{q} - \omega \right| < \frac{1}{2hq^2}, \quad \text{.........................(2)}$$

and this inequality is not satisfied unless the line and circle intersect. Our problem then is to determine how large h can be chosen with the certainty that L will intersect infinitely many S-circles.

3. *Connexion with the Modular Group.*—The relation of the preceding construction to the Modular Group of transformations

$$z' = \frac{az+b}{cz+d}, \quad ad - bc = 1 \quad \text{......................(3)}$$

where a, b, c, d are real integers, arises in the following manner. Consider the line $y = h$ parallel to the real axis. Writing $\bar{z} = x - iy$, the equation of this line can be put in the form

$$z - \bar{z} = 2ih. \quad \text{.......................... (4)}$$

Let us transform this line by means of (3). Putting for z its value from (3), $z = (-dz' + b)/(cz' - a)$, the equation (4) becomes after simplification

$$\left(z' - \frac{a}{c} - \frac{i}{2hc^2}\right)\left(\bar{z}' - \frac{a}{c} + \frac{i}{2hc^2}\right) = \frac{1}{4h^2c^4}. \quad \text{.........(5)}$$

This is a circle whose centre is $\dfrac{a}{c} + \dfrac{i}{2hc^2}$ and whose radius is $\dfrac{1}{2hc^2}$. It is then tangent to the x-axis at $x = a/c$; in other words, this is the circle $S(a/c\,;\,h)$.

Now if we take $a=p$, $c=q$, we can, provided p and q have no common factor, find integers b and d, such that $pd-qb=1$, and (3) is then a transformation carrying $y=h$ into $S(p/q\,;\,h)$. Thus the S-circles of the preceding section are all derived from the line $y=h$ by the set of transformations (3). Including the line $y=h$ as the S-circle of ∞, the set of S-circles is carried into itself by any one of the transformations (3).

To determine whether L intersects an infinite number of S-circles, we can transform the plane by means of a suitable modular transformation, and then investigate whether the semicircle into which L is carried intersects an infinite number of S-circles.

4. *Modular Division of the Half-plane.*—Let the region lying above the circle $x^2+y^2=1$ and between the lines $x=\pm\frac{1}{2}$ (the region D of the figure) be inverted in each of its sides; let the new regions be inverted in their sides; and so on *ad infinitum*. The whole upper half-plane is covered by the resulting network of triangles, and there is no overlapping. A few triangles are shown in broken lines in the figure. This division of the half-plane into triangles is called the modular division, for the reason that any triangle can be transformed into any other by the application of a suitable modular transformation. Each triangle has one of its vertices, which we shall call its *peak*, either on the x-axis or at infinity. Those on the x-axis are at rational points.

It is well known that the line L (Section 2) passes through infinitely many of these triangles, and that there is more than a finite number of corresponding peaks.*

Let p/q (in its lowest terms) be the x-coordinate of the peak of a triangle through which L passes. If we make the modular transformation

$$z'=\frac{q'z-p'}{qz-p} \qquad \text{.............................. (6)}$$

where p' and q' are integers, such that $qp'-q'p=1$, $z=p/q$ becomes $z'=\infty$, and the triangle in question becomes one with peak at ∞. $S(p/q\,;\,h)$ becomes $y=h$. L becomes a circle L'

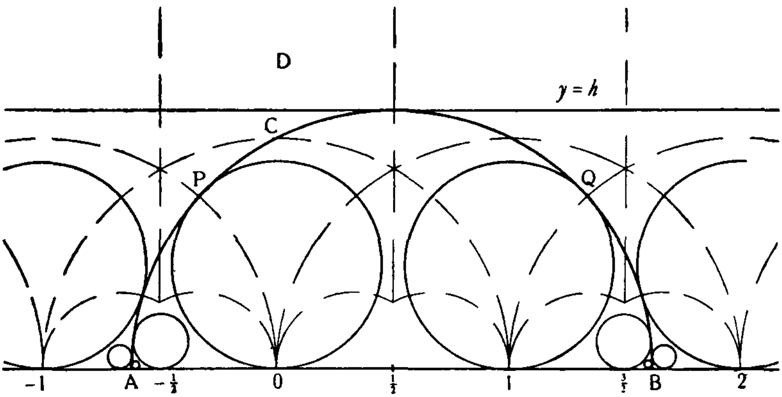
---

* Humbert has shown that the coordinates of these peaks are the fractions of Hermite mentioned in Section 1. *Journal de Mathématiques*, 7th Ser., Vol. 2 (1916), 79–103.

orthogonal to the x-axis. [This follows from well-known properties of the linear transformation: that circles, including straight lines, are carried into circles, and angles are preserved. The coefficients of the transformation being real, the x-axis is transformed into itself, and L therefore becomes a circle cutting it at a right angle as before.]

The two triangles which L' intersects on entering and on passing out of those whose peaks are at ∞ have peaks whose coordinatss are integers. By shifting to the right or left by means of a transformation of the form $z' = z \pm n$, we can without loss of generality suppose that one of these two triangles has its peak at the origin. L' then intersects the base of D.

5. *Proof of the first part of the theorem.*—Let us consider the following question: How large can h be chosen with the certainty



that every circle orthogonal to the x-axis and intersecting the base of D will intersect either $y = h$ or an S-circle at one of the integral points? Every such circle will have at least two integral points on its interior; for otherwise it would be entirely within one of the unit circles forming the bases of the triangles whose peaks are at ∞, and therefore could not intersect the base of D.

It is easily seen that the most favourable position of the circle, in order to avoid the intersections with the given S-circles, is when its centre is at $x = \frac{1}{2}$ (or $x = -\frac{1}{2}$), and it contains just two integral points on its interior. We shall now find the value of h for which a circle C with centre $x = \frac{1}{2}$ can be drawn just touching $y = h$,

https://doi.org/10.1017/S0013091500029692 Published online by Cambridge University Press

$S(0/1\,;\,h)$, and $S(1/1\,;\,h)$. The radius of each of these S-circles is $1/2h$. Since C touches $y=h$, its radius is h (see Fig.). The radius of C drawn to Q, the point of tangency of C and $S(1/1\,;\,h)$ passes through the centre of the latter circle; and by elementary geometry we get for the radius of C the value

$$\sqrt{\left(\frac{1}{2}\right)^2+\left(\frac{1}{2h}\right)^2}+\frac{1}{2h}.$$

Equating these values of the radius

$$\sqrt{\frac{1}{4}+\frac{1}{4h^2}}+\frac{1}{2h}=h, \qquad \text{(7)}$$

and solving for h, we find

$$h=\tfrac{1}{2}\sqrt{5}. \qquad \text{(8)}$$

When $h=\frac{1}{2}\sqrt{5}$ there are only two circles (the circle C just found, and a like circle with centre at $x=-\frac{1}{2}$) satisfying the conditions on L', that is, intersecting the x-axis orthogonally and intersecting the base of D, and which does not intersect either $y=h$ or one of the S-circles at the integral points.

Now it is impossible that L' coincide with C for the following reason. The points A, B, in which C intersects the x-axis, have the coordinates

$$A,\ \tfrac{1}{2}-\tfrac{1}{2}\sqrt{5}; \quad B,\ \tfrac{1}{2}+\tfrac{1}{2}\sqrt{5}. \qquad \text{(9)}$$

Both are irrational. Now one of the intersections of L' with the x-axis must be rational, for L is carried to L' by a transformation of the form (3). One of the intersections of L' with the x-axis is the transform of $z=\infty$ through which L passes; and $z=\infty$ becomes $z'=a/c$, a rational. For a like reason L' cannot coincide with the circle whose centre is $x=-\frac{1}{2}$.

We conclude then that when L is carried into L', the latter intersects one at least of the circles $S(0/1\,;\,\frac{1}{2}\sqrt{5})$, $y=\frac{1}{2}\sqrt{5}$, $S(a/1\,;\,\frac{1}{2}\sqrt{5})$, where $x=a$ is the peak of the triangle which L' enters in leaving the triangles with peaks at ∞. That is, of the S-circles of these three successive peaks of the triangles through which L' passes, one at least must be intersected.

If we now carry L' back to L, remembering that it was the peak of *any* triangle intersected by L that was carried to ∞, we can state that *of the S-circles of any three successive peaks of the triangles through which L passes, one at least is intersected when* $h=\frac{1}{2}\sqrt{5}$. Since these peaks are infinite in number, L intersects infinitely many S-circles.

Hence, according to Section 2, there are infinitely many fractions satisfying the inequality (2) when $h=\frac{1}{2}\sqrt{5}$, and ω is any irrational number whatsoever. This gives to k in (1) the value $1/\sqrt{5}$, and the first part of the theorem is established.

6. *Proof of the second part of the theorem.*—Let us return to the circle C. The coordinates (9) of its intersections with the x-axis are the roots of the equation

$$z^2 - z - 1 = 0. \qquad \qquad (10)$$

Writing this in the form

$$z = \frac{2z+1}{z+1},$$

we see that A and B are the fixed points of the transformation

$$z' = \frac{2z+1}{z+1}, \qquad \qquad (11)$$

which, since $ad - bc = 2\cdot 1 - 1\cdot 1 = 1$, is of the Modular Group. Since $a + d = 2 + 1 > 2$, this transformation is of the type called hyperbolic. Any circle through the fixed points is transformed into itself by a hyperbolic transformation. C is such a circle for the transformation (11).

Now, by this transformation $z=0$ becomes $z'=1$. Hence $S(0/1;\ \frac{1}{2}\sqrt{5})$ becomes $S(1/1;\ \frac{1}{2}\sqrt{5})$, and P, the point of tangency of the former circle with C, becomes Q, the point of tangency of the latter circle with C. The arc PQ is transformed into an arc of C beginning at Q, and extending in the direction of B. By continued repetitions of (11), the whole of the arc QB is covered by an infinite number of transforms of PQ; and by employing the transform inverse to (11), the whole of AP is likewise covered.

PQ is tangent to certain S-circles, and these are carried by repetitions of (11) into infinitely many others tangent to C. It is easy to find what these circles are. When $z=\infty$, $z'=2$; when

$z=1$, $z'=3/2$; when $z=2$, $z'=5/3$; etc. Hence $S(2/1;\ \frac{1}{2}\sqrt{5})$, $S(3/2;\ \frac{1}{2}\sqrt{5})$, $S(5/3;\ \frac{1}{2}\sqrt{5})$, etc., are tangent to C.

C is tangent to infinitely many S-circles when $h=\frac{1}{2}\sqrt{5}$, and intersects no others. Suppose now that $h>\frac{1}{2}\sqrt{5}$; the line $y=h$ lies above the line $y=\frac{1}{2}\sqrt{5}$ of the figure, and all the S-circles are decreased in size. Let a circle C' be drawn through A, B tangent to $y=h$. This circle is one of the fixed circles of (11). Since $z=\infty$ becomes $z'=2$, C' will also touch $S(2/1;\ h)$; and the arc between the points of tangency with $y=h$ and with $S(2/1;\ h)$ will, by repetitions of (11), cover the whole of C' between A and B. C' will thus touch infinitely many S-circles, and otherwise intersect none.

There will be no S-circles in the region between C' and C.

Let us now take B for the point ω. The line L, perpendicular to the x-axis at B, lies in the neighbourhood of B between C' and C, and intersects there no S-circles. The S-circles intersected lie above the intersection of L and C', and these can be but finite in number. Hence, when $h>\frac{1}{2}\sqrt{5}$, there are for the irrational point B only a finite number of fractions satisfying the inequality (2). Obviously the same is true at the point A.

If C and its tangent circles be transformed by means of any modular transformation, we get a circle C_1 orthogonal to the x-axis and tangent to S-circles along its entire length. To the extremities of C_1 the reasoning of the preceding paragraphs applies at once, showing that any number into which B is transformed by (3) [or A, but A itself is a transform of B by means of $z'=-1/z$] is a number for which only a finite number of fractions satisfy the inequality (2) when $h>\frac{1}{2}\sqrt{5}$. These numbers, *i.e.*

$$\frac{a\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)+b}{c\left(\frac{1}{2}+\frac{1}{2}\sqrt{5}\right)+d}$$

where a, b, c, d are integers and $ad-bc=1$, are all irrational; and, as is the case of the transforms of any real point, they are to be found in every interval of the real axis. Thus the second part of the theorem is established.