It is proved that for any integer \( n \geq 0 \), there is a circle in the plane that passes through exactly \( n \) lattice points.

© 1998 Academic Press

In his problem book [1] for high school students, Steinhaus proved that for any integer \( n \geq 0 \), there is a circle in the plane that encloses exactly \( n \) lattice points. Here we prove the next.

**THEOREM.** For any \( n \geq 0 \), there is a circle that passes through exactly \( n \) lattice points.

**LEMMA.** For any \( k \geq 0 \), the number of integral solutions \((X, Y)\) of the equation
\[ X^2 + Y^2 = 5k \]  
(1)
is equal to \( 4(k+1) \).

**PROOF.** Let us count, instead, the number of gaussian integers \( z \in \mathbb{Z}[i] \) satisfying \( |z|^2 = 5^k \).
Suppose that \( z \in \mathbb{Z}[i] \) satisfies \( |z|^2 = 5^k \). If \( k \geq 1 \) then, since \( 5 = (1+2i)(1-2i) \) divides \( 5^k = z\overline{z} \) and since \( 1+2i, 1-2i \) are primes, \( z \) is divisible by one of \( 1+2i, 1-2i \). Hence we can write \( z \) as
\[ z = u(1+2i)^r(1-2i)^{k-r}, \]  
(2)
where \( 0 \leq r \leq k \) and \( u \in \{ \pm 1, \pm i \} \). Since \( \arg(1+2i) \) is irrational, by varying \( r \) and \( u \) in the expression (2), we obtain exactly \( 4(k+1) \) distinct solutions \( z \in \mathbb{Z}[i] \), of the equation \( |z|^2 = 5^k \).

This lemma also follows directly from the following remarkable result due to Jacobi: the number of integral solutions of \( X^2 + Y^2 = m \) is equal to four times the excess of the number of divisors of \( m \) of the form \( 4j+1 \) over those of the form \( 4j+3 \).

**PROOF OF THEOREM.** First, the even case \( n = 2(k+1) \). Consider the circle represented by the equation
\[ (2x - 1)^2 + (2y)^2 = 5^k. \]  
(3)
The number of integral solutions of (3) is equal to the number of integral solutions \((X, Y)\) of (1) in which \( X \) is odd. Since such solutions comprise half the solutions of (1), equation (3) has \( 2(k+1) = n \) solutions. Hence the circle represented by (3) passes through exactly \( n \) lattice points.

Next, the odd case \( n = 2\ell + 1 \). Let \( k = 2\ell \). Then, since \( 5^k = 25^\ell \equiv 1 \pmod{8} \), any integral solution \((X, Y)\) of (1) must satisfy either \( X \equiv \pm 1 \), \( Y \equiv 0 \pmod{4} \) or \( X \equiv 0, Y \equiv \pm 1 \pmod{4} \).

Now, consider the circle represented by the equation
\[ (4x - 1)^2 + (4y)^2 = 5^k. \]  
(4)
The number of integral solutions of (4) is equal to the number of integral solutions \((X, Y)\) of (1) such that

\[ X \equiv -1 \pmod{4}. \]  

(5)

If \((X, Y) = (A, B)\) is an integral solution of (1) with \(A \neq 0, B \neq 0\), then 

\[(\pm A, \pm B), (\pm B, \pm A)\]

are eight distinct solutions of (1), and just two of them satisfy (5). On the other hand, in the four solutions \((0, \pm 5\ell), (\pm 5\ell, 0)\) of (1), just \((-5\ell, 0)\) satisfies (5). Hence the number of those integral solutions \((X, Y)\) of (1) that satisfies (5) is equal to

\[
\frac{4(k + 1) - 4}{4} + 1 = k + 1.
\]

Hence the circle (4) passes through exactly \(k + 1 = n\) lattice points. \(\square\)

REFERENCES


Received 20 January 1997 and accepted 17 September 1997

H. MAEHARA  
Ryukyu University,  
Okinawa,  
Japan

M. MATSUMOTO  
Keio University,  
Yokohama,  
Japan