SOME VISIBILITY PROBLEMS IN POINT LATTICES

Thesis by

David F. Rearick

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1960

ACKNOWLEDGEMENTS

I am indebted to Professor T. M. Apostol for his interest, encouragement and advice, and to Mr. Howard C. Rumsey for many stimulating discussions of the material treated in this thesis. I wish to thank the California Institute of Technology for the assistantships and scholarships with which I have been so generously provided. Thanks are also due to Mrs. Linda Hopkins for her most competent job of typing the manuscript.

ABSTRACT

We say that one lattice point is <u>visible</u> from another if no third lattice point lies on the line joining them. A lattice point visible from the origin is called a <u>visible point</u>. We study the manner in which the visible points are distributed throughout the lattice and show that, in a k-dimensional lattice, the fraction of such points in an expanding region "usually" tends to $1/\zeta(k)$. On the other hand there exist arbitrarily large "gaps" containing no visible points. The following is a typical theorem: The maximum number of lattice points mutually visible in pairs is 2^k, and if $n \leq 2^k$, the "density" of points visible from each of a fixed set of n points, themselves mutually visible in pairs, is

$$\prod_p \left(1 - \frac{n}{p^k}\right) .$$

The last section is devoted to a study of the function $\phi_s(n,m)$, which is defined to be the number of distinct solutions of the congruence

$$x_1 + x_2 + \dots + x_s \equiv m \pmod n$$

having

$$(x_1, n) = \dots = (x_s, n) = 1.$$

A special case of this function arises in connection with a certain visibility problem. A typical result is that

$$\sum_{k \bmod n} \phi_s(n,m)\, \phi_s(n,m+k) = \phi_{2s}(n,k).$$

TABLE OF CONTENTS

§ 1. Counting Visible Points in a Rectangle.

Let L be the lattice consisting of all points in the plane with integer coordinates. We will say that two distinct lattice points (m,n) and (r,s) are <u>mutually visible</u>* if no other points of L lie on the line segment joining them. It is clear that (m,n) and (r,s) are mutually visible if, and only if, the differences m - r and n - s are relatively prime. For, if (u,v) is a point of L lying between the two it must satisfy

$$u = r + x(m - r)$$
$$v = s + x(n - s)$$

for some x, $0 < x < 1$. Since u and v are integers, x must be rational and its denominator must divide both m - r and n - s, and this is possible if, and only if, $(m - r, n - s) > 1$.**

In discussing visibility we lose no generality in restricting attention to the square lattice L. For suppose L' is a more general plane lattice, consisting of all points $m\omega_1 + n\omega_2$ where ω_1 and ω_2 are two non-zero complex numbers with non-real quotient. An argument similar to the one just given shows that the points $m\omega_1 + n\omega_2$ and $r\omega_1 + s\omega_2$ are mutually visible if, and only if, $(m - r, n - s) = 1$, that is, if (m,n) and (r,s) are mutually visible points of the square

---

* Or that (m,n) is visible from (r,s), or vice versa.

** The use of the notation (m,n) for both the lattice point and the g.c.d. should cause no confusion, as the meaning will always be clear from the context.

lattice L.

If (m,n) is visible from the origin, we shall say simply that (m,n) is a <u>visible point</u>. Note that the origin itself is not a visible point because visibility has been defined only between <u>distinct</u> points. Let V denote the set of all visible points of L. The first portion of this thesis is devoted to a study of properties of V and, in particular, to the manner in which the visible points are distributed throughout the lattice L.

Most of the results to be obtained have analogues in lattices of higher dimension, and the proofs are straightforward extensions of those given for the plane. Sometimes these analogues will be mentioned. In this connection we define mutual visibility between two points in a k-dimensional lattice in the same way as for two dimensions, and note that $(n_1, n_2, \ldots, n_k)$ and $(r_1, r_2, \ldots, r_k)$ are mutually visible if, and only if, $(n_1 - r_1, n_2 - r_2, \ldots, n_k - r_k) = 1$.

The first theorem gives an algebraic property of V and is unrelated to the rest of the work.

<u>Theorem 1.1</u>. Every unimodular transformation of L maps V onto itself.

Let T be the transformation

$$(1.1) \qquad \begin{aligned} m' &= am + bn \\ n' &= cm + dn \end{aligned}$$

where a, b, c and d are integers with $\Delta = ad - bc = \pm 1$. It is well known (see [1]) that T maps the whole lattice L onto itself in a one-to-one fashion. The inverse transformation T^{-1} is given by

$$\Delta m = dm' - bn' \tag{1.2}$$
$$\Delta n = -cm' + an'$$

Choose $(m,n) \in V$. By equations (1.2), any factor dividing both m' and n' also divides both m and n, so $(m',n') \in V$ and the mapping is <u>into</u>, i.e. $TV \subset V$. On the other hand, equations (1.1) show that any common divisor of m and n also divides both m' and n', so $T^{-1}V \subset V$ and the mapping is <u>onto</u>, i.e. $TV = V$.

Since there are infinitely many visible points, it is natural to ask how "dense" they are, in some sense, among all the points of V. One way of answering this question is well known.* We may count the number of visible points in a <u>square</u> centered at the origin, divide by the total number of lattice points in the square, and find the limit as the edge of the square tends to infinity. Let the square be the point set $\{(x,y) \mid |x| \le X,\ |y| \le X\}$ where x and y are real and X is positive. Since the visible points are distributed symmetrically in the four quadrants, it suffices to consider only the square $\{(x,y) \mid 0 < x \le X,\ 0 < y \le X\}$. Furthermore, since $(m,n) = (n,m)$, we need consider only the triangle $\{(x,y) \mid 0 < y \le x \le X\}$. For a fixed positive integer $n \le X$, the number of visible points on the line segment $x = n$, $0 < y \le n$ is $\phi(n)$, and hence the number in the triangle is

$$\sum_{n \le X} \phi(n).$$

---

* See Hardy and Wright [1], Ch. 18.

The average order of $\phi(n)$ is known to be $6n/\pi^2$, that is,

$$\sum_{n \leq X} \phi(n) \sim 3X^2/\pi^2 \,, \tag{1.3}$$

a result proved by Mertens in 1874. On the other hand, the total number of lattice points in the triangle is $1/2\ X^2 + O(X)$, so the fraction of visible points tends to $6/\pi^2$ as $X \to \infty$. Thus, in the sense of the above construction, the density of V in L is $6/\pi^2$.

This result depended strongly on the shape (i.e. squareness) of the expanding region. There is another known asymptotic formula similar to (1.3) which may be interpreted as saying that the density of visible points in an infinite <u>strip</u> approaches $6/\pi^2$ as the strip widens. Namely, we have the relation

$$\sum_{n \leq X} \phi(n)/n \sim 6X/\pi^2 \,, \tag{1.4}$$

which is given as an exercise in [2]. Consider the first-quadrant rectangle

$$Q(X,Y) = \left\{ (x,y) \mid 0 < x \leq X,\ 0 < y \leq Y \right\}. \tag{1.5}$$

Let $N'(X,Y)$ denote the number of visible points in $Q(X,Y)$ and, if $m \leq X$ is a positive integer, let $M(m,Y)$ denote the number of visible points on the line segment $x = m$, $0 < y \leq Y$. The total number of lattice points in $Q(X,Y)$ is $[X][Y]$ and the fraction of visible points is $N'(X,Y)/[X][Y]$. If we stretch the rectangle into a strip by letting $Y \to \infty$ first, and then widen the strip by letting $X \to \infty$, we obtain

$$\lim_{X\to\infty}\left(\lim_{Y\to\infty}\frac{N'(X,Y)}{[X][Y]}\right) = \lim_{X\to\infty}\frac{1}{X}\lim_{Y\to\infty} N'(X,Y)/Y$$

$$= \lim_{X\to\infty}\frac{1}{X}\sum_{m\le X}\lim_{Y\to\infty} M(m,Y)/Y$$

$$= \lim_{X\to\infty}\frac{1}{X}\sum_{m\le X}\frac{\phi(m)}{m}$$

$$= 6/\pi^2 \text{ by } (1.4).$$

The two examples just considered show that

$$\lim_{X,Y\to\infty}\frac{N'(X,Y)}{XY} = 6/\pi^2 \tag{1.6}$$

for the two special cases in which $Y = X$ or in which the double limit is evaluated as an iterated limit. We are led to suspect that (1.6) may hold as X and Y approach infinity independently, that is, as the rectangle $Q(X,Y)$ expands in an arbitrary manner. We shall indeed prove this, basing the proof on the following formula for counting the number of visible points in a rectangle:

__Theorem 1.2.__ The number $N'(X,Y)$ of visible points in $Q(X,Y)$ is exactly

$$\sum_{k=1}^{\infty}\mu(k)\left[\frac{X}{k}\right]\left[\frac{Y}{k}\right].$$

Here the sum is finite, of course, since the terms are zero when $k > \min(X,Y)$. In counting the visible points of a rectangle the ϕ-function no longer plays a role; the Möbius μ-function (see [1]) appears instead. The property we use is that

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right].$$

We have

$$N'(X,Y) = \sum_{\substack{m\le X\\ n\le Y\\ (m,n)=1}} 1 = \sum_{\substack{m\le X\\ n\le Y}} \sum_{d|(m,n)} \mu(d) = \sum_{d=1}^{\infty} \mu(d) \sum_{\substack{d|m,\ m\le X\\ d|n,\ n\le Y}} 1 .$$

Let $m = kd$, $n = ld$. Then

$$N'(X,Y) = \sum_{d=1}^{\infty} \mu(d) \sum_{k\le \frac{X}{d}} 1 \sum_{l\le \frac{Y}{d}} 1 = \sum_{d=1}^{\infty} \mu(d) \left[\frac{X}{d}\right]\left[\frac{Y}{d}\right].$$

From Theorem 1.2 we can deduce the "rectangle limit" result (1.6); that is to say,

$$\lim_{X,Y\to\infty} \frac{1}{XY} \; N'(X,Y) = 6/\pi^2$$

as X and Y increase independently. This result follows from

<u>Theorem 1.3</u>. $\dfrac{1}{XY} \; N'(X,Y) = 6/\pi^2 + O\left(\dfrac{\log Z}{Z}\right)$

where $Z = \min(X,Y)$.

If we write $\{\alpha\} = \alpha - [\alpha]$, then

$$\left[\frac{X}{k}\right]\left[\frac{Y}{k}\right] = \frac{XY}{k^2} - \left\{\frac{X}{k}\right\}\frac{Y}{k} - \left\{\frac{Y}{k}\right\}\frac{X}{k} + \left\{\frac{X}{k}\right\}\left\{\frac{Y}{k}\right\}.$$

Multiply both sides by $\mu(k)$ and sum on k from 1 to Z.

$$\frac{1}{XY} N'(X,Y) = \sum_{k\le Z} \frac{\mu(k)}{k^2} - \frac{1}{X} \sum_{k\le Z} \frac{\mu(k)}{k}\left\{\frac{X}{k}\right\} - \frac{1}{Y} \sum_{k\le Z} \frac{\mu(k)}{k} \left\{\frac{Y}{k}\right\}$$
$$+ \frac{1}{XY} \sum_{k\le Z} \left\{\frac{X}{k}\right\} \left\{\frac{Y}{k}\right\}.$$

The first term on the right tends to

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} = 6/\pi^2$$

as $Z \to \infty$, (see [1]), and the tail of the series is $O(1/Z)$. The absolute value of the sum of the three remaining terms is less than

$$\left(\frac{1}{X} + \frac{1}{Y}\right)\sum_{k \le Z} \frac{1}{k} + \frac{1}{XY} \sum_{k \le Z} 1 \le \frac{2}{Z} \sum_{k \le Z} \frac{1}{k} + \frac{1}{Z^2} \cdot Z$$

$$= \frac{2}{Z}\, O(\log Z) + O(1/Z)$$

$$= O\left(\frac{\log Z}{Z}\right).$$

As we shall show in § 3, the same limit, $6/\pi^2$, is obtained by counting the fraction of visible points in an expanding region of much more general shape. Temporarily restricting attention to the rectangle, however, we can generalize Theorem 1.3 as follows:

<u>Theorem 1.4</u>. The fraction of points (m,n) in $Q(X,Y)$ such that $(m,n) = k$ tends to $6/\pi^2 \cdot \frac{1}{k^2}$ as $X,Y \to \infty$.

Since the condition $(m,n) = k$ holds if, and only if, $m = km'$, $n = kn'$ where $(m',n') = 1$, the number of points in $Q(X,Y)$ with $(m,n) = k$ is equal to the number $N'\left(\frac{X}{k}, \frac{Y}{k}\right)$ of visible points in $Q\left(\frac{X}{k}, \frac{Y}{k}\right)$. Using Theorem 1.3 we obtain

$$\frac{1}{XY}\, N'\left(\frac{X}{k}, \frac{Y}{k}\right) = \frac{1}{k^2} \cdot \frac{1}{\frac{X}{k}\frac{Y}{k}}\, N'\left(\frac{X}{k}, \frac{Y}{k}\right) \to \frac{1}{k^2} \cdot \frac{6}{\pi^2}$$

as $X,Y \to \infty$.

This result has been obtained in the case of the square, $X = Y$, by Christopher [4], whose work is based on the asymptotic formula (1.3). Both Christopher and Hardy and Wright [1] use the term "probability" as a loose but descriptive way of talking about the density of a set of lattice points, and we shall adopt this language also. Thus, Theorem 1.4 could be described by saying that the probability that two randomly selected integers m and n have a g.c.d. equal to k is $\frac{6}{\pi^2} \cdot \frac{1}{k^2}$. No attempt will be made to justify this usage from the standpoint of measure theory.

§ 2. The Zeta-Distributions.

In the language of probability, Theorem 1.4 describes a distribution function $F_2(x) = \frac{6}{\pi^2} \sum_{k \leq x} \frac{1}{k^2}$, namely the probability that the g.c.d. of two randomly selected integers will be less than or equal to x. Since $F_2(x)$ is proportional to the partial sum $\sum_{k \leq x} \frac{1}{k^2}$ of the series for $\zeta(2)$, it may be called a ζ-distribution. There are corresponding ζ-distributions for all dimensions higher than 2. It is an easy matter to extend Theorems 1.3 and 1.4 to s dimensions by considering the number $N'(X_1, \ldots, X_s)$ of visible points in the box $Q(X_1, \ldots, X_s)$ given by $0 < x_i \leq X_i$ $(i = 1, 2, \ldots, s)$, and letting $Z = \min X_i$ tend to infinity. The corresponding theorems are:

__Theorem 2.1.__ $\frac{1}{X_1 X_2 \ldots X_s} N(X_1, \ldots, X_s) = \frac{1}{\zeta(s)} + O\left(\frac{\log Z}{Z^{s-1}}\right)$

__Theorem 2.2.__ The fraction of points $(n_1, n_2, \ldots, n_s)$ in $Q(X_1, X_2, \ldots, X_s)$ such that $(n_1, n_2, \ldots, n_s) = k$ tends to $\frac{1}{\zeta(s)} \cdot \frac{1}{k^s}$ as $Z \to \infty$.

Theorem 2.2 describes an entire family of ζ-distribution functions

$$F_s(x) = \frac{1}{\zeta(s)} \sum_{k \leq x} \frac{1}{k^s} .$$

It is interesting to compute their mean and variance.

__Theorem 2.3.__ The mean of $F_s(x)$ is $\frac{\zeta(s-1)}{\zeta(s)}$ if $s \geq 3$ and infinite if $s = 2$. The variance* is

$$\frac{\zeta(s-2)}{\zeta(s)} - \frac{\zeta^2(s-1)}{\zeta^2(s)}$$

---

* The formula for variance gives some incidental information about the ζ-function. Since the variance is positive, being equal to

if $s \geq 4$, infinite if $s = 3$, and indeterminate if $s = 2$.

Thus the "expected value" of the g.c.d. of two integers is infinite, whereas for s integers, $s \geq 3$, it is finite and tends to 1 as $s \to \infty$.

Let S be a set of positive integers. In view of the foregoing, we should expect that if m and n are randomly selected, the probability that their g.c.d. is in S should be

$$\frac{6}{\pi^2} \sum_{k \in S} \frac{1}{k^2} .$$

In other words, if f is the characteristic function of S, we should expect that

$$\lim_{X,Y \to \infty} \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y}} f((m,n)) = \frac{6}{\pi^2} \sum_{k=1}^{\infty} \frac{f(k)}{k^2} .$$

This is indeed true, and for a much larger class of functions f than those taking only the values 0 and 1.

$$\frac{1}{\zeta(s)} \sum_{k=1}^{\infty} \frac{(k - E_s)^2}{k^s}$$

where $E_s = \dfrac{\zeta(s-1)}{\zeta(s)}$, we have $\dfrac{\zeta(s-2)}{\zeta(s)} > \left(\dfrac{\zeta(s-1)}{\zeta(s)}\right)^2$. This holds in fact for all real $s > 3$, integral or otherwise, and induction yields the following theorem:

If s is real and greater than 3 and k is an integer, $1 < k < s - 1$, then

(2.1)
$$\frac{\zeta(s-k)}{\zeta(s)} > \left(\frac{\zeta(s-1)}{\zeta(s)}\right)^k .$$

This shows that $\dfrac{\zeta(s-k)}{\zeta(s)}$, considered as a function of k, is of at least exponential order.

<u>Theorem 2.4.</u> If $f(n) = O(n^{1-\epsilon})$ for some $\epsilon > 0$, then

$$\frac{1}{XY} \sum_{\substack{m \le X \\ n \le Y}} f((m,n)) = \frac{6}{\pi^2} \sum_{k=1}^{\infty} \frac{f(k)}{k^2} + O\left(\frac{\log Z}{Z^{\epsilon}}\right) .$$

This generalizes Theorem 1.3, which is the special case $f(n) = \left[\frac{1}{n}\right]$. Theorem 2.4 could be proved as was Theorem 1.3, by introducing the Möbius function, but it can be deduced more simply from the latter as follows:

$$\frac{1}{XY} \sum_{\substack{m \le X \\ n \le Y}} f((m,n)) = \frac{1}{XY} \sum_{k \le Z} f(k) \sum_{\substack{m \le X \\ n \le Y \\ (m,n) = k}} 1$$

$$= \sum_{k \le Z} \frac{f(k)}{k^2} \cdot \frac{1}{\frac{X}{k}\frac{Y}{k}} N'\left(\frac{X}{k},\frac{Y}{k}\right),$$

as in the proof of Theorem 1.4. For fixed k, Theorem 1.3 gives us

$$\frac{1}{\frac{X}{k}\frac{Y}{k}} N'\left(\frac{X}{k},\frac{Y}{k}\right) = \frac{6}{\pi^2} + O\left(\frac{\log \frac{Z}{k}}{\frac{Z}{k}}\right)$$

$$= \frac{6}{\pi^2} + kO\left(\frac{\log Z}{Z}\right)^{*}.$$

Hence

$$\frac{1}{XY} \sum_{\substack{m \le X \\ n \le Y}} f((m,n)) = \frac{6}{\pi^2} \sum_{k \le Z} \frac{f(k)}{k^2} + O\left(\frac{\log Z}{Z}\right) \sum_{k \le Z} \frac{f(k)}{k}$$

---

* The constant implied by the O - notation is now independent of k.

$$= \frac{6}{\pi^2} \sum_{k=1}^{\infty} \frac{f(k)}{k^2} + O\left(\frac{1}{Z^{\epsilon}}\right) + O\left(\frac{\log Z}{Z}\right) O\, Z^{1-\epsilon} .$$

An interesting special case occurs when $f(n) = d(n)$, the number of divisors of n. It is known (see [1]) that $d(n) = O(n^{\epsilon})$ for any $\epsilon > 0$, and that

$$\sum_{n=1}^{\infty} \frac{d(n)}{n^2} = \zeta^2(2) = \frac{\pi^4}{36} .$$

Hence

$$\lim_{X,Y\to\infty} \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y}} d((m,n)) = \frac{\pi^2}{6} ;$$

that is to say, the average number of divisors of (m,n), extended over all points of L, is $\frac{\pi^2}{6}$. Since $\frac{\pi^2}{6} < 2$, this shows that there must be plenty of points for which $d((m,n)) = 1$, i.e., visible points. We have thus obtained a bit more information concerning the density of V in L.

Theorem 2.4 generalizes immediately to dimensions higher than 2. A more interesting question is whether it can be extended downward to 1 dimension, that is, whether for certain f we may have

$$\lim_{X\to\infty} \frac{1}{X} \sum_{n\leq X} f(n) = \lim_{s\to 1+} \frac{1}{\zeta(s)} \sum_{k=1}^{\infty} \frac{f(k)}{k^s} . \tag{2.3}$$

It is too ambitious to expect to prove for a useful class of functions f, say bounded functions, that existence of the limit on the right implies existence of the limit on the left, which would be the direct analogue of Theorem 2.4. For, with $f = \mu$, this would prove that

$$\sum_{n \leq X} \mu(n) = o(X),$$

a result known to be equivalent in depth to the prime number theorem. We can, however, obtain a proof of (2.3) in the opposite direction.

<u>Theorem 2.5</u>. If f is bounded and the sequence $\{f(n)\}$ can be made to converge to L by the Cesaro (C,k) process for some k, then

$$\lim_{s \to 1+} (s - 1) \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

exists and is equal to L.

Equation (2.3) is the case (C,1). On the right, $\zeta(s)$ has been replaced by $\frac{1}{s-1}$, since the ζ-function has a simple pole at $s = 1$ with residue 1 and hence $(s - 1)\,\zeta(s) \to 1$ as $s \to 1+$.

To prove Theorem 2.5 we define

$$a_n = \frac{1}{n} \sum_{k=1}^{n} f(k) \text{ if } n \geq 1, \; a_0 = 0.$$

Then $$f(n) = na_n - (n - 1)\,a_{n-1}$$

$$= n(a_n - a_{n-1}) - (a_n - a_{n-1}) + a_n.$$

For $s > 1$,

$$(2.4) \quad \sum_{n=1}^{N} \frac{f(n)}{n^s} = \sum_{n=1}^{N} \frac{a_n - a_{n-1}}{n^{s-1}} - \sum_{n=1}^{N} \frac{a_n - a_{n-1}}{n^s} + \sum_{n=1}^{N} \frac{a_n}{n^s} .$$

We apply Abel's partial summation method to the first two series on the right. In the second, for example,

$$\sum_{n=1}^{N} \frac{a_n - a_{n-1}}{n^s} = \sum_{n=1}^{N} a_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) - 0 + \frac{a_N}{(N+1)^s} \quad .$$

If $|f(n)| \leq M$, then $|a_n| \leq M$ also, and hence

$$\left| \sum_{n=1}^{N} \frac{a_n - a_{n-1}}{n^s} \right| \leq M \sum_{n=1}^{N} \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + \frac{M}{(N+1)^s} = M,$$

and the same result holds in the other series in (2.4) where s is replaced by $s - 1$. Hence

$$\left| \sum_{n=1}^{N} \frac{f(n)}{n^s} - \sum_{n=1}^{N} \frac{a_n}{n^s} \right| \leq 2M, \text{ and}$$

$$(2.5) \left| \sum_{n=1}^{\infty} \frac{f(n)}{n^s} - \sum_{n=1}^{\infty} \frac{a_n}{n^s} \right| \leq 2M,$$

both series being convergent for $s > 1$.

Now suppose $a_n \to L$. In this case, given $\epsilon > 0$ we can find n_o such that $|a_n - L| < \epsilon$ when $n > n_o$.

$$\left| \sum_{n=1}^{\infty} \frac{a_n}{n^s} - L\, \zeta(s) \right| \leq \sum_{n=1}^{n_o} \frac{|a_n - L|}{n^s} + \epsilon \sum_{n=n_o+1}^{\infty} \frac{1}{n^s}$$

$$\leq 2M \sum_{n=1}^{n_o} \frac{1}{n^s} + \epsilon\, \zeta(s).$$

Multiply both sides by $s - 1$ and let $s \to 1+$.

$$\left| \lim_{s \to 1+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} - L \right| \leq 0 + \epsilon$$

Since this is true for all $\epsilon > 0$, we have

$$\lim_{s\to 1+} (s - 1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = L, \text{ and hence by (2.5),}$$

$$\lim_{s\to 1+} (s - 1) \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = L.$$

If $\{a_n\}$ does not converge but <u>its</u> sequence $\{b_n\}$ of Cesaro averages does, then (2.5) is still valid and it also holds with f(n) replaced by a_n and a_n by b_n. The triangle inequality then gives

$$\left| \sum_{n=1}^{\infty} \frac{f(n)}{n^s} - \sum_{n=1}^{\infty} \frac{b_n}{n^s} \right| \leq 4M \tag{2.6}$$

and the remainder of the proof holds with a_n replaced by b_n. This is the (C,2) case, and validity for (C,k) follows by induction.

We have seen that, if f takes only the values 0 or 1, Theorem 2.4 can be interpreted as a formula for the probability that f((m,n)) = 1 for two randomly selected integers m and n. It is perhaps worth diverging briefly to observe a similar visualization of certain Euler products in terms of probability.

Let f be multiplicative and suppose f takes only the values 0 or 1. Then the probability that f((m,n)) = 1 is

$$\frac{1}{\zeta(2)} \sum_{k=1}^{\infty} \frac{f(k)}{k^2} .$$

This expression has an Euler product, namely

$$\frac{1}{\zeta(2)} \sum_{k=1}^{\infty} \frac{f(k)}{k^2} = \prod_{p} \left(1 - \frac{1}{p^2}\right)\left(1 + \frac{f(p)}{p^2} + \frac{f(p^2)}{p^4} + \dots\right)$$

$$= \prod_{p} g(p)$$

where

$$g(p) = \frac{1 + \frac{f(p)}{p^2} + \frac{f(p^2)}{p^4} + \cdots}{1 + \frac{1}{p^2} + \frac{1}{p^4} + \cdots} \leq 1.$$

We will show that $g(p)$ represents the probability that the highest power of p dividing (m,n) is assigned the function value 1. For, if $\alpha \geq 1$, the probability that p^α divides both m and n is $\left(\frac{1}{p^\alpha}\right)^2$ and the probability that $p^\alpha \mid (m,n)$ but $p^{\alpha+1} \nmid (m,n)$ is $\left(\frac{1}{p^\alpha}\right)^2 - \left(\frac{1}{p^{\alpha+1}}\right)^2 = \frac{1}{p^{2\alpha}}\left(1 - \frac{1}{p^2}\right)$. The probability that $f(p^\alpha) = 1$ is just $f(p^\alpha)$ itself, since f assumes only the values 0 and 1. Hence $\left(1 - \frac{1}{p^2}\right)\frac{f(p^\alpha)}{p^{2\alpha}}$ is the probability that p^α is the highest power of p dividing (m,n) and that also $f(p^\alpha) = 1$. The sum over all α, which is $g(p)$, is the probability that the highest power of p dividing (m,n) is assigned the function value 1. It seems reasonable to assert that this event should be "independent" of the corresponding event for a different prime, and thus the infinite product can be regarded as the product of probabilities of independent events.

§ 3. Counting Visible Points in More General Regions.

Returning to the study of the density of V in L, we may ask for the limiting fraction of visible points in an expanding region of more general shape than a rectangle. Under what conditions can we be sure the limit exists, and if it exists must it be equal to $\frac{6}{\pi^2}$? One's imagination immediately pictures an amoeba-like region expanding by thrusting forth long tentacles toward special lattice points, and clearly nothing could be concluded if such pathology were allowed. We will discuss the case in which a region R which has a positive area expands by linear magnification about the origin. Depending on whether the origin is contained in the interior of R, or lies on its boundary, or is exterior to R, the expanding region will envelop the whole plane, or a portion of it, or will disappear into the distance.

To begin, R may be an arbitrary bounded point set. If $t > o$, let tR denote the image of R under the mapping $f(z) = tz$. Let $N(tR)$ be the number of lattice points, excluding the origin,* in tR. Let $N'(tR)$ be the number of visible points in tR. Theorem 1.2, which counts the visible points of a rectangle, is readily extended to give the following relationship between N and N'.

<u>Theorem 3.1</u>. $$N(R) = \sum_{k=1}^{\infty} N'\left(\frac{R}{k}\right)$$

$$N'(R) = \sum_{k=1}^{\infty} \mu(k) N\left(\frac{R}{k}\right) .$$

---

* The fact that magnification occurs about the origin makes this point somewhat exceptional. Excluding it simplifies the statement of Theorem 3.1.

Both sums are finite since $\frac{R}{k}$ eventually contains no lattice point except perhaps the origin. Theorem 3.1 is formally identical to a known inversion formula* satisfied by the Mobius function.

$$N(R) = \sum_{\substack{(m,n)\in R \\ (m,n)\neq(o,o)}} 1 = \sum_{d=1}^{\infty} \sum_{\substack{(m,n)\in R \\ (m,n)=d}} 1 = \sum_{d=1}^{\infty} \sum_{\substack{(m,n)\in \frac{R}{d} \\ (m,n)=1}} 1 = \sum_{d=1}^{\infty} N\left(\frac{R}{d}\right)$$

$$N'(R) = \sum_{\substack{(m,n)\in R \\ (m,n)=1}} 1 = \sum_{(m,n)\in R} \sum_{d|(m,n)} \mu(d) = \sum_{d=1}^{\infty} \mu(d) \sum_{\substack{(m,n)\in R \\ (m,n)=d}} 1$$

$$= \sum_{d=1}^{\infty} \mu(d) \sum_{\substack{(m,n)\in \frac{R}{d} \\ (m,n)\neq(o,o)}} 1 = \sum_{d=1}^{\infty} \mu(d) N\left(\frac{R}{d}\right).$$

Theorem 1.2 is, of course, the case $R = Q(X,Y)$.

From Theorem 3.1 we can deduce that as $t \to \infty$, $N'(tR)/N(tR) \to \frac{6}{\pi^2}$, under certain restrictions on R. Hereafter we shall write $N(t)$ and $N'(t)$ instead of $N(tR)$ and $N'(tR)$. Define $N_1(t)$ to be the number of lattice squares** contained entirely in tR, and $N_2(t)$ to be the number of lattice squares having at least one point in tR. Then we have the inequalities

$$(3.1) \qquad N_1(t) \leq N(t) \leq N_2(t).$$

---

* Hardy and Wright [1], p. 237.

** A lattice square is considered to contain its southwest corner and the open south and west edges, but no other boundary points.

We will now assume that R possesses a positive area $A(R)$ given by

$$(3.2) \qquad A(R) = \lim_{t\to\infty} \frac{N_1(t)}{t^2} = \lim_{t\to\infty} \frac{N_2(t)}{t^2} .$$

Then $A(tR) = t^2 A(R)$, and we will write $A(t)$ for $A(tR)$ and A for $A(1)$. From (3.1) and (3.2) we have

$$(3.3) \qquad N(t) \sim At^2.$$

Let $c = \text{l.u.b.} \left\{ t \,|\, N(t) = 0 \right\}$, which is finite because of (3.3) and greater than zero because R is bounded. For any $t > c$ let $k(t)$ be the largest integer k such that $N\left(\frac{t}{k}\right) > 0$. We note that

$$(3.4) \qquad k(t) = \left[\frac{t}{c}\right] \text{ or } \left[\frac{t}{c}\right] - 1.$$

For, by definition we must have

$$\frac{t}{k(t) + 1} \leq c \leq \frac{t}{k(t)}$$

and hence

$$k(t) \leq \frac{t}{c} \leq k(t) + 1 .$$

We may choose the size of R to be such that $c = 1$. Finally, let $P(t) = N(t) - A(t)$. Then

$$\frac{N'(t)}{N(t)} + o(1) = \frac{N'(t)}{At^2} = \frac{1}{At^2} \sum_{k=1}^{k(t)} \mu(k) N\left(\frac{t}{k}\right)$$

$$= \frac{1}{At^2} \sum_{k=1}^{[t]} \mu(k) \left(A\left(\frac{t}{k}\right) + P\left(\frac{t}{k}\right)\right)$$

$$= \sum_{k\leq t} \frac{\mu(k)}{k^2} + \frac{1}{At^2} \sum_{k\leq t} \mu(k) P\left(\frac{t}{k}\right) .$$

We have proved

<u>Theorem 3.2</u>. If R is bounded and has a positive area, then $N'(t)/N(t) \to \frac{6}{\pi^2}$ if, and only if,

$$\sum_{k\leq t} \mu(k)P\left(\frac{t}{k}\right) = o(t^2).$$

We shall be content with a very generous sufficient condition.

<u>Theorem 3.3</u>. The condition $P(t) = O(t)$ implies

$$\sum_{k\leq t} \mu(k)P\left(\frac{t}{k}\right) = o(t^2),$$

and this condition is satisfied, in particular, if R is a region whose boundary is a rectifiable curve.

If $|P(t)| \leq Mt$ for all $t > o$, then

$$\left|\sum_{k\leq t} \mu(k)P\left(\frac{t}{k}\right)\right| \leq Mt \sum_{k\leq t} \frac{1}{k} \leq M't \log t = o(t^2).$$

Suppose R is bounded by a curve C of length S. Then C can pass through no more than $4[S] + 4$ lattice squares. For suppose we cut C into $[S]$ arcs of unit length plus one arc of length $\{S\}$, and arrange these individually in the lattice to maximize the total number of squares passed through. Each segment can pass through at most four squares, giving a maximum total of $4[S] + 4$, and this is also a maximum total for the original curve C since it constituted one of the possible arrangements of the segments. Thus the boundary tC of tR can pass through at most $4[tS] + 4$ squares.

But since $N_1(t) \leq N(t) \leq N_2(t)$ and $N_1(t) \leq A(t) \leq N_2(t)$, we have $|P(t)| = |N(t) - A(t)| \leq N_2(t) - N_1(t)$, and $N_2(t) - N_1(t)$ is the number of squares with at least one point inside and at least one point outside of tR. The boundary curve tC must pass through each of these squares, so there cannot be more than $4[tS] + 4$ of them. Thus $|P(t)| \leq N_2(t) - N_1(t) \leq 4[tS] + 4 = O(t)$.

We note that the condition $P(t) = O(t)$ is satisfied, in particular, if R is convex, for bounded convex sets have rectifiable boundaries.

Theorems 3.2 and 3.3 do not furnish a direct generalization of Theorem 1.3 because we have considered only the case in which R expands by linear magnification about the origin. In a similar manner we could treat the case of expansion under the transformation $f(x,y) = (t_1 x, t_2 y)$, of which the rectangle in Theorem 1.3 is a special case. However, we shall not pursue the details here.

§ 4. Irregularities of Distribution.

We have seen that the fraction of visible points in a region R "usually" tends to $\frac{6}{\pi^2}$ as R is allowed to expand. This means that the visible points must be distributed with a certain degree of uniformity throughout the lattice. On the other hand, the results which we shall obtain in this section show that the distribution cannot be too uniform.

We begin with the following question: Is there a finite subset T of L such that every point of L is visible from at least one point of T? If such a set T exists, we will say that T surveys L. The next theorem enables us to reduce this question to one dealing with the distribution of visible points.

Theorem 4.1. The lattice L can be surveyed by a finite subset if, and only if, V does not contain arbitrarily large square gaps.*

Suppose the distribution of visible points is such that V contains no square gaps with side as great as k. Then any square of side k contains a point visible from the origin. It also contains a point visible from any other point (m,n), for otherwise some translate of this square would contain no points visible from the origin, and would thus be a square gap of side k. Hence any square subset of L of side k surveys L.

Conversely, assume L contains arbitrarily large square gaps and suppose T surveys L. Then any translate of T must also survey L. Let T' be a translate of T located in the interior of a square gap

---

* That is, regions of form $0 < m - m_0 \leq k$, $0 < n - n_0 \leq k$ belonging to L - V.

large enough to cover it. Then no point of T' is visible from the origin, which contradicts the fact that T' surveys L.

The next theorem along with Theorem 4.1, shows that no finite subset surveys L.

Theorem 4.2. The set V contains arbitrarily large square gaps. In fact, there is a gap of side at least k lying within the square $Q(2^{k^4}, 2^{k^4})$.

We shall use a constructive method, based on the Chinese Remainder Theorem, to locate a gap of side k. Let $p_0, p_1, \ldots, p_{k^2-1}$ be k^2 distinct primes. For $r = 0, 1, \ldots, k-1$ define

$$m_r = \prod_{i=rk}^{rk+k-1} p_i \ .$$

The m's are prime in pairs and by the Chinese Remainder Theorem the system of congruences

$$(4.1) \qquad x \equiv r \pmod{m_r},\ r = 0, 1, \ldots, k-1$$

has solutions; call one of them x_0. Now define

$$M_s = \prod_{i=0}^{k-1} p_{ik+s} \quad \text{for } s = 0, 1, \ldots, k-1.$$

The M's are prime in pairs and the system

$$(4.2) \qquad y \equiv s \pmod{M_s},\ s = 0, 1, \ldots, k-1$$

has a solution y_0. We will show that the lattice point (x_0, y_0) forms the upper right-hand corner of a gap of side at least k. We must verify that, for $0 \leq r < k$, $0 \leq s < k$ we have $(x_0 - r, y_0 - s) > 1$. But $x_0 - r$ is divisible by m_r and $y_0 - s$ by M_s, and $(m_r, M_s) > 1$ because the prime factor p_{rk+s} is common to both m_r and M_s.

To get the bound on x_o and y_o mentioned in the theorem, we start out with the <u>first</u> k^2 primes, and make use of Bertrand's Postulate which implies that the nth prime, p_n, cannot exceed 2^n. Since the solution x_o of (4.1) is unique modulo the product of the m's, we can choose x_o to lie between 1 and

$$\prod_{r=o}^{k-1} m_r = \prod_{n=1}^{k^2} p_n .$$

Similarly, we can choose y_o to lie between 1 and

$$\prod_{s=o}^{k-1} M_s = \prod_{n=1}^{k^2} p_n .$$

But

$$\prod_{n=1}^{k^2} p_n \leq \prod_{n=1}^{k^2} 2^n \leq 2^{1/2 k^2(k^2+1)} \leq 2^{k^4} . \tag{4.3}$$

This bound on

$$\prod_{n=1}^{k^2} p_n$$

is, of course, very weak, and can be improved to k^{Ak^2} if we use the prime number theorem in the form $\theta(x) \sim x$, where $\theta(x) = \sum_{p \leq x} \log p$. Bertrand's Postulate uses only the fact that $\theta(x) < 2x \log 2$. Using the stronger theorem, we have

$$\log \prod_{n=1}^{k^2} p_n = \sum_{p \leq p_{k^2}} \log p = \theta(p_{k^2}) \sim p_{k^2} \sim 2k^2 \log k$$

where the last step uses the prime number theorem again in the form $p_n \sim n \log n$. Thus

$$\prod_{n=1}^{k^2} p_n = \exp\left(2k^2 \log k + o(k^2 \log k)\right)$$

$$= k^{2k^2 + o(k^2)} \leq k^{Ak^2}$$

for a suitable constant A. For sufficiently large k we may take A = 3.

§ 5. Joint Visibility.

We turn now to the following kind of question: If T is a finite subset of L, what is the density of those lattice points visible from each point of T? We shall consider only the two simplest cases, namely those in which T consists of just two points, or in which all points of T are themselves mutually visible in pairs. As in § 1, we shall interpret "density" as meaning the limiting fraction of such points in a rectangle centered at the origin, as the dimensions of the rectangle approach infinity independently.

Suppose first that T consists of two distinct points, (u,v) and (w,z). Let Q and Q_1 be two congruent rectangles, with Q centered at (o,o) and Q_1 centered at (w,z). We wish to count the number of lattice points in Q which are jointly visible from both (u,v) and (w,z). But this cannot differ from the corresponding number in Q_1 by more than the number of lattice points in the region $Q-Q_1$ (in the language of set theory), and the area of $Q-Q_1$ is of smaller order than the areas of Q and Q_1. Therefore, the fractions of such points in Q and Q_1 tend to the same limit. Hence we may assume that the rectangle is centered at one of the two points of T, and furthermore we may choose this point to be the origin, i.e. $(w,z) = (o,o)$. In fact, we may restrict attention only to the first-quadrant portion $Q(X,Y)$ of this rectangle, where as before $Q(X,Y) = \{(x,y) \mid 0 < x \leq X,\ 0 < y \leq Y\}$. For, although the distribution of points jointly visible from (u,v) and (o,o) may not have quadrant symmetry, we will see that the density computed from $Q(X,Y)$ depends only on the g.c.d. (u,v) and hence is unaffected by replacing u by $-u$ or v by $-v$.

Our problem is thus reduced to counting the number of lattice points in $Q(X,Y)$ which are visible from both (u,v) and (o,o). Such points (m,n) are characterized by $(m,n) = (m-u, n-v) = 1$.

In addition to $Z = \min(X,Y)$ it will be convenient to introduce the notation

$$\bar{\bar{Z}} = \max_{(m,n)\in Q(X,Y)} \left(\max\{(m,n),\ (m-u, n-v)\}\right).$$

We have* $\bar{\bar{Z}} \le [Z] + \max(|u|,|v|) \le AZ$.

The fraction of points in $Q(X,Y)$ visible from both (u,v) and (o,o) is

$$\frac{1}{XY} \sum_{\substack{m\le X \\ n\le Y \\ (m,n)=(m-u,n-v)=1}} 1 = \frac{1}{XY} \sum_{\substack{m\le X \\ n\le Y}} \ \sum_{d\,|\,(m,n)} \mu(d) \sum_{d'\,|\,(m-u,n-v)} \mu(d')$$

$$(5.1) \qquad = \frac{1}{XY} \sum_{d,d'\le \bar{\bar{Z}}} \mu(d)\,\mu(d') \sum_{\substack{m\le X \\ n\le Y \\ d\,|\,(m,n) \\ d'\,|\,(m-u,n-v)}} 1$$

For fixed d and d', the sum on the right is equal to

$$(5.2) \qquad \frac{1}{XY} \sum_{\substack{m\le X \\ d|m \\ d'|m-u}} 1 \sum_{\substack{n\le Y \\ d|n \\ d'|n-v}} 1 = \frac{1}{XY} \sum_{\substack{a \\ da\equiv u \pmod{d'} \\ a\le \frac{X}{d}}} 1 \sum_{\substack{a' \\ da'\equiv v \pmod{d'} \\ a'\le \frac{Y}{d}}} 1$$

---

* In this section A will represent a positive constant whose value is not necessarily the same every time it appears.

The first sum on the right in (5.2) is the number of solutions not exceeding $\frac{X}{d}$ of the congruence

$$da \equiv u \pmod{d'}.$$

This is zero unless $(d,d')|u$. If $(d,d')|u$ then there are exactly (d,d') solutions (mod d') and hence $\left[\frac{X}{d\ d'}\right](d,d') + \theta$ solutions not exceeding $\frac{X}{d}$, where $0 \le \theta \le (d,d')$. Similarly, the second sum on the right in (5.2) is equal to zero unless $(d,d')|v$, and in that case is equal to $\left[\frac{Y}{d\ d'}\right](d,d') + \theta'$ where $0 \le \theta' \le (d,d')$. Line (5.1) becomes

$$\frac{1}{XY} \sum_{\substack{d,d' \le \bar{Z} \\ (d,d')|(u,v)}} \mu(d)\ \mu(d')\left(\left[\frac{X}{d\ d'}\right](d,d') + \theta\right)\left(\left[\frac{Y}{d\ d'}\right](d,d') + \theta'\right) . \tag{5.3}$$

We want now to extract the principal term

$$\frac{1}{XY} \sum_{\substack{d,d' \le \bar{Z} \\ (d,d')|(u,v)}}' \mu(d)\ \mu(d') \left[\frac{X}{d\ d'}\right]\left[\frac{Y}{d\ d'}\right] (d,d')^2 \tag{5.4}$$

and show that the error terms R and S tend to zero as $X, Y \to \infty$, where

$$R = \frac{1}{XY} \sum_{\substack{d,d' \le \bar{Z} \\ (d,d')|(u,v)}} \mu(d)\ \mu(d')\left(\theta\left[\frac{Y}{d\ d'}\right] + \theta' \left[\frac{X}{d\ d'}\right]\right)(d,d')$$

and

$$S = \frac{1}{XY} \sum_{\substack{d,d' \le \bar{Z} \\ (d,d')|(u,v)}} \mu(d)\ \mu(d')\ \theta\ \theta'$$

For R we have the estimate

$$|R| \leq \frac{1}{XY} \sum_{d,d' \leq \overline{Z}} \left(\frac{Y}{d\ d'} + \frac{X}{d\ d'}\right)(u,v)^2 \leq \frac{2}{Z} \sum_{d \leq AZ} \frac{1}{d} \sum_{d' \leq AZ} \frac{1}{d'}\ (u,v)^2$$

$$\leq \frac{A}{Z} \log^2 Z \to 0 \text{ as } Z \to \infty.$$

The error term S cannot be estimated by simply replacing the μ's by 1 and the θ's by (u,v), but we may treat it as follows. When $d\ d' > \max(X,Y)$, line (5.3) reduces to S, and by reversing the steps between (5.1) and (5.3) we have

$$S = \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y}} \sum_{\substack{d \mid (m,n) \\ d' \mid (m-u,n-v) \\ d\ d' > \max(X,Y)}} \mu(d)\ \mu(d')\ .$$

Now it is safe to replace the μ's by 1.*

$$|S| \leq \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y}} \sum_{\substack{d \mid (m,n) \\ d' \mid (m-u,n-v) \\ d\ d' > Z}} 1 \quad \leq \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y \\ (m,n)(m-u,n-v) > Z}} d((m,n))d((m-u,n-v))$$

It is known** that the divisor function $d(n)$ is of order $O(n^{\epsilon})$ for any $\epsilon > 0$, so, with $\epsilon = \frac{1}{6}$,

$$d((m,n))d((m-u,n-v)) \leq A(m,n)^{\frac{1}{6}}(m-u,n-v)^{\frac{1}{6}} \leq AZ^{\frac{1}{3}}.$$

---

* I am indebted to Howard Rumsey for demonstrating that the fact that $S \to 0$ does not depend on special properties of the μ-function, and for providing an alternative proof.

** See [1], Chap. 18.

$$|S| \leq AZ^{1/3} \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y \\ (m,n)(m-u,n-v) > Z}} 1$$

$$\leq AZ^{1/3} \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y \\ (m,n) > Z^{1/2} \text{ or } (m-u,n-v) > Z^{1/2}}} 1$$

$$\leq AZ^{1/3} \frac{1}{XY} \Bigg(\sum_{\substack{m \leq X \\ n \leq Y \\ (m,n) > Z^{1/2}}} 1 + \sum_{\substack{m \leq X \\ n \leq Y \\ (m-u,n-v) > Z^{1/2}}} 1 \Bigg)$$

$$\leq AZ^{1/3} \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y \\ (m,n) > Z^{1/2}}} 1 = AZ^{1/3} \sum_{Z^{1/2} < d \leq Z} \frac{1}{XY} \sum_{\substack{m \leq X \\ n \leq Y \\ (m,n) = d}} 1$$

$$\leq AZ^{1/3} \sum_{Z^{1/2} < d \leq Z} \frac{1}{d^2} \cdot \frac{d^2}{XY} \sum_{\substack{m \leq \frac{X}{d} \\ n \leq \frac{Y}{d} \\ (m,n) = 1}} 1$$

$$\leq AZ^{1/3} \sum_{Z^{1/2} < d \leq Z} \frac{1}{d^2} \left(\frac{6}{\pi^2} + A \frac{\log \frac{Z}{d}}{\frac{Z}{d}} \right) \text{ by Theorem 1.3.}$$

$$|S| \leq AZ^{1/3} \sum_{d > Z^{1/2}} \frac{1}{d^2} + AZ^{-2/3} \log Z \sum_{d \leq Z} \frac{1}{d}$$

$$\leq AZ^{1/3 - 1/2} + AZ^{-2/3} \log^2 Z = O(Z^{-1/6}).$$

We now return to (5.4) and estimate the error incurred by removing the greatest integer signs. The sum in (5.4) is

$$(5.5) \qquad \sum \frac{\mu(d)\mu(d')(d,d')^2}{(d\ d')^2} - \frac{1}{XY} \sum \mu(d)\mu(d') \left(\frac{X}{d\ d'} \left\{ \frac{Y}{d\ d'} \right\} + \frac{Y}{d\ d'} \left\{ \frac{X}{d\ d'} \right\} \right) (d,d')^2 + \frac{1}{XY} \sum \mu(d)\mu(d') \left\{ \frac{X}{d\ d'} \right\} \left\{ \frac{Y}{d\ d'} \right\} (d,d')^2$$

where the sums are over $d \leq \overline{Z}$, $d' \leq \overline{Z}$, $(d,d') \mid (u,v)$. The first error term in (5.5) can be estimated by the same method used for R above and is found to be

$$O\left(\frac{\log^2 Z}{Z} \right),$$

while the second error term is in magnitude less than

$$\frac{1}{XY} \sum_{d,d' \leq \overline{Z}} \frac{X}{d\ d'} (u,v)^2 \leq \frac{A}{Z} \sum_{d,d' \leq AZ} \frac{1}{d\ d'} = O\left(\frac{\log^2 Z}{Z} \right) .$$

As $X,Y \to \infty$, the surviving term in (5.5) is

$$F((u,v)) = \sum_{\substack{d,d'=1 \\ (d,d') \mid (u,v)}}^{\infty} \frac{\mu(d)\mu(d')(d,d')^2}{(d\ d')^2} = \sum_{a \mid (u,v)} a^2 \sum_{\substack{d,d'=1 \\ (d,d')=a}}^{\infty} \frac{\mu(d)\mu(d')}{(d\ d')^2}$$

$$F((u,v)) = \sum_{a \mid (u,v)} a^2 \sum_{\substack{m,n=1 \\ (m,n)=1}}^{\infty} \frac{\mu(am)\mu(an)}{a^4 (mn)^2}$$

$$= \sum_{a \mid (u,v)} \frac{\mu^2(a)}{a^2} \sum_{\substack{m,n=1 \\ (a,mn)=1}}^{\infty} \frac{\mu(mn)}{(mn)^2}$$

$$= \sum_{a \mid (u,v)} \frac{\mu^2(a)}{a^2} \sum_{\substack{k=1 \\ (a,k)=1}}^{\infty} \frac{\mu(k)}{k^2}\, d(k)$$

$$= \sum_{a \mid (u,v)} \frac{\mu^2(a)}{a^2} \prod_{p \nmid a} \left(1 - \frac{2}{p^2}\right)$$

$$F((u,v)) = C \sum_{a \mid (u,v)} \frac{\mu^2(a)}{a^2} \prod_{p \mid a} \left(1 - \frac{2}{p^2}\right)^{-1}$$

$$\text{where } C = \prod_{p} \left(1 - \frac{2}{p^2}\right) > 0 .$$

The form of this last expression shows that $\frac{1}{C} F((u,v))$ is a multiplicative function of the g.c.d. (u,v). Evaluating it on prime powers, we have

$$\frac{1}{C} F(p^{\alpha}) = \sum_{k=0}^{1} \frac{\mu^2(p^k)}{p^{2k}} \prod_{p\, p^k} \left(1 - \frac{2}{p}\right)^{-1} = 1 + \frac{1}{p^2 - 2} .$$

Hence $\frac{1}{C} F((u,v)) = \prod_{p \mid (u,v)} \frac{p^2 - 1}{p^2 - 2}$. We have proved

Theorem 5.1. The density of points visible from both (u,v) and (o,o) depends only on the g.c.d. (u,v) and is equal to C $\prod_{p|(u,v)} \frac{p^2-1}{p^2-2}$, where C = $\prod_p \left(1 - \frac{2}{p^2}\right)$.

This formula shows that the density of points mutually visible from (u,v) and (o,o) is minimized by choosing (u,v) and (o,o) to be mutually visible themselves, and this minimum value is C.* On the other hand, the density is always less than

$$C \prod_p \frac{p^2-1}{p^2-2} = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{6}{\pi^2},$$

as it should be, since this is the fraction of points visible from one point alone.

We note that the density of lattice points visible from either (u,v) or (o,o) is

$$\frac{6}{\pi^2} + \frac{6}{\pi^2} - C \prod_{p|(u,v)} \frac{p^2-1}{p^2-2},$$

by the "cross-classification" principle. If an independent expression were derived for this density, the constant C could be evaluated. However, the work would be much more difficult than that above, because the functions involved are not multiplicative.

In generalizing Theorem 5.1 to a finite set T consisting of more than two points, we will simplify the counting process by assuming that all points of T are mutually visible in pairs. For a two-dimensional

---

* By numerical calculation and estimation of the tail of the product we obtain the inequalities

$$0.321 < C < 0.323.$$

lattice L, the only case to consider is that of three points, in view of the following observation.

<u>Theorem 5.2</u>. It is impossible to find five points of L mutually visible in pairs. More generally, in an s-dimensional lattice the largest possible number of points mutually visible in pairs is 2^s.

Since 2^s is the number of vertices of an s-dimensional unit cube, it is certainly possible to find 2^s points mutually visible in pairs. Suppose, on the other hand, that we pick any set T of $2^s + 1$ lattice points. If we reduce each such point modulo 2, component by component, we obtain $2^s + 1$ points each having all components 1 or 0. By the Dirichlet box principle, some two of these points must be identical, meaning that the original two points from which they came have the same parity, component by component. Since the componentwise differences are all divisible by 2, these two points cannot be mutually visible.

<u>Theorem 5.3</u>. In a two-dimensional lattice L the density of points visible from each of three given points mutually visible in pairs is

$$\prod_p \left(1 - \frac{3}{p^2}\right) .$$

Let the three points be (u,v), (w,z) and (o,o), with $(u,v) = (w,z) = (u - w, v - z) = 1$. This time let

$$\bar{\bar{Z}} = \max_{(m,n)\in Q(X,Y)} \left(\max \left\{ (m,n),\ (m - u, n - v),\ (m - w, n - z) \right\} \right) .$$

Again $\bar{\bar{Z}} \leq AZ$ where $Z = \min(X,Y)$. The fraction of points in Q(X,Y) visible from all members of T is

$$(5.6)\quad \frac{1}{XY}\sum_{\substack{m\le X\\ n\le Y\\ (m,n)=(m-u,n-v)\\ =(m-w,n-z)=1}} 1 = \frac{1}{XY}\sum_{\substack{m\le X\\ n\le Y}}\ \sum_{d_1\mid(m,n)}\mu(d_1)\sum_{d_2\mid(m-u,n-v)}\mu(d_2)\sum_{d_3\mid(m-w,n-z)}\mu(d_3)$$

$$= \frac{1}{XY}\sum_{d_1,d_2,d_3\le \bar{Z}}\mu(d_1)\mu(d_2)\mu(d_3)\sum_{\substack{m\le X\\ d_1\mid m\\ d_2\mid m-u\\ d_3\mid m-w}} 1 \sum_{\substack{n\le Y\\ d_1\mid n\\ d_2\mid n-v\\ d_3\mid n-z}} 1$$

Note that d_1, d_2, d_3 must be prime in pairs because of the conditions $(u,v) = (w,z) = (u-w,v-z) = 1$. Thus the system

$$m \equiv o \pmod{d_1}$$

$$m \equiv u \pmod{d_2}$$

$$m \equiv w \pmod{d_3}$$

has a unique solution (mod $d_1 d_2 d_3$) by the Chinese Remainder Theorem, and $\left[\frac{X}{d_1 d_2 d_3}\right] + \theta$ solutions not exceeding X, where $\theta = 0$ or 1. Line (5.6) becomes

$$\frac{1}{XY}\sum_{d_1,d_2,d_3\le \bar{Z}}\mu(d_1)\mu(d_2)\mu(d_3)\left(\left[\frac{X}{d_1 d_2 d_3}\right]+\theta\right)\left(\left[\frac{Y}{d_1 d_2 d_3}\right]+\theta'\right)$$

where also $0 \le \theta' \le 1$. The error terms can be shown to tend to zero by the same methods used before, giving finally

$$\sum_{d_1,d_2,d_3=1}^{\infty}\frac{\mu(d_1 d_2 d_3)}{(d_1 d_2 d_3)^2}$$

as the density of points visible from each of (u,v), (w,z) and (o,o). Letting $k = d_1 d_2 d_3$, this becomes

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \sum_{d_1 d_2 d_3 = K} 1 \quad . \tag{5.7}$$

We may consider k to be square-free due to the presence of $\mu(k)$. The number of ways k can be represented in the form $k = d_1 d_2 d_3$ is then just $3^{\nu(k)}$, where $\nu(k)$ is the number of prime divisors of k. Line (5.7) reduces to

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} 3^{\nu(k)} = \prod_{p} \left(1 - \frac{3}{p^2} \right),$$

the Euler product representation holding since $3^{\nu(k)}$ is multiplicative.

Since

$$\prod_{p} \left(1 - \frac{3}{p^2} \right) > 0,$$

Theorem 5.3 shows that there are infinitely many ways of choosing four points mutually visible in pairs, besides the vertices of a unit square. It also provides a method of constructing a set E of lattice points, of positive density

$$\prod_{p} \left(1 - \frac{3}{p^2} \right),$$

such that no two points of E are mutually visible--namely, let E be the set of all points visible from each of three mutually visible points. If any two points of E could see one another, we would have five points mutually visible in pairs.

The higher-dimensional analogue of Theorems 5.1 and 5.3 is the following:

<u>Theorem 5.4</u>. Let T be a set in an s-dimensional lattice consisting of

n points mutually visible in pairs. The density of points visible from each point of T is

$$\prod_{p} \left(1 - \frac{n}{p^s}\right)$$

if $n \leq 2^s$, and zero if $n > 2^s$.

The proof is a direct extension of the method used in proving Theorem 5.3.

§ 6. Some Identities Involving Visible Points.

The results of this section are certain identities based on the following principle. Suppose

$$\sum_{(m,n)\in L}{}' f(m,n)$$

is an absolutely convergent infinite series summed over all points of the lattice L excluding the origin. We can rearrange the series by summing first over all multiples (km,kn) of a visible point (m,n) and then over all $(m,n) \in V$, i.e.

$$(6.1) \qquad \sum_{(m,n)\in L}{}' f(m,n) = \sum_{(m,n)\in V} \sum_{k=1}^{\infty} f(km,kn).$$

In certain cases it may happen that the inside sum can be put into closed form, thus converting the original sum over L into a new sum over V. The same idea holds for absolutely convergent infinite products, namely

$$(6.2) \qquad \prod_{(m,n)\in L}{}' f(m,n) = \prod_{(m,n)\in V} \prod_{k=1}^{\infty} f(km,kn).$$

Let us apply this process to the Weierstrass $\wp$-function defined by

$$(6.3) \qquad \wp(z) = \frac{1}{z^2} + \sum_{(m,n)\in L}{}' \left(\frac{1}{(m\omega_1+n\omega_2-z)^2} - \frac{1}{(m\omega_1+n\omega_2)^2} \right)$$

where z is a complex variable and ω_1 and ω_2 are fixed non-zero complex numbers with non-real ratio. We write ω for a general point $m\omega_1 + n\omega_2$ and, with a slight abuse of notation, write L for the lattice of all such ω and V for the set of visible ω, that is, those ω for which $(m,n) = 1$. Then

$$(6.4) \qquad \wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) .$$

The series (6.4) converges absolutely for every fixed $z \notin L$ since

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega(2z-z^2)}{\omega^4 (1 - \frac{z}{\omega})^2} \right| \leq \frac{A}{|\omega|^3} ,$$

and

$$\sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{|\omega|^3}$$

converges. Hence

$$(6.5) \qquad \wp(z) = \frac{1}{z^2} + \sum_{\omega \in V} \sum_{k=1}^{\infty} \left(\frac{1}{(z-k\omega)^2} - \frac{1}{k^2 \omega^2} \right)$$

$$= \frac{1}{z^2} + \sum_{\omega \in V} \left(\sum_{k=1}^{\infty} \frac{1}{(z-k\omega)^2} - \frac{\pi^2}{6\omega^2} \right)$$

since in the 1-dimensional sum on k the two parts converge separately, the value of the second being

$$\frac{1}{\omega^2} \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6\omega^2} .$$

Now if w is a complex number different from an integer multiple of π, then the partial fraction expansion of $\csc^2 w$ is

$$\csc^2 w = \sum_{k=-\infty}^{\infty} \frac{1}{(w-k\pi)^2} = 2 \sum_{k=1}^{\infty} \frac{1}{(w-k\pi)^2} + \frac{1}{w^2} .$$

Putting $w = \frac{\pi z}{\omega}$, we obtain from (6.5) the formula

$$(6.6) \qquad \wp(z) = \frac{1}{z^2} + \frac{1}{2} \sum_{\omega \in V} \left(\frac{\pi^2}{\omega^2} \csc^2 \frac{\pi z}{\omega} - \frac{1}{z^2} - \frac{\pi^2}{3\omega^2} \right)$$

which expresses $\wp(z)$ as a sum extended over the visible points of the lattice generated by ω_1 and ω_2.

In (6.5), another way of putting the sum on k in closed form is to introduce the Hurwitz zeta-function $\zeta(s,a)$, defined for real $s > 1$ and complex a not a negative integer or zero, by

$$\zeta(s,a) = \sum_{k=0}^{\infty} \frac{1}{(k+a)^s} \quad .$$

Then

$$(6.7) \qquad \wp(z) = \frac{1}{z^2} + \sum_{\omega \in V} \left(\sum_{k=0} \frac{1}{\omega^2 (k + \frac{z}{\omega})^2} - \frac{1}{z^2} - \frac{\pi^2}{6\omega^2} \right)$$

$$= \frac{1}{z^2} + \sum_{\omega \in V} \left(\frac{1}{\omega^2} \zeta(2, \tfrac{z}{\omega}) - \frac{1}{z^2} - \frac{\pi^2}{6\omega^2} \right).$$

Similar expressions hold for the Weierstrass ζ- and σ-functions, namely:

$$(6.8) \qquad \zeta(z) = \frac{1}{z} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2} \right)$$

$$= \frac{1}{z} + \frac{1}{2} \sum_{\omega \in V} \left(\frac{\pi}{\omega} \cot \frac{\pi z}{\omega} - \frac{1}{z} + \frac{\pi^2}{3\omega^2} z \right)$$

$$(6.9) \qquad \sigma(z) = z \prod_{\substack{\omega\in L\\ \omega\neq 0}} \left(1-\frac{z}{\omega}\right) \exp\left(\frac{z}{\omega}+\frac{1}{2}\frac{z^2}{\omega^2}\right)$$

$$= z \prod_{\omega\in V} \frac{1}{\Gamma(1-\frac{z}{\omega})} \exp\left(-\gamma\frac{z}{\omega}+\frac{\pi^2}{12}\frac{z^2}{\omega^2}\right)$$

where in (6.9) $\Gamma(z)$ is the gamma function and γ is Euler's constant. The gamma function arises from the 1-dimensional product on k, which is recognized as the Weierstrass product representation of

$$\frac{1}{\Gamma(1-\frac{z}{\omega})} \exp\left(-\gamma\frac{z}{\omega}\right).$$

The "invariants" g_2 and g_3 associated with the $\wp$-function are easily expressed as sums over the visible points, namely:

$$(6.10) \qquad \begin{aligned} g_2(\omega_1,\omega_2) &= 60\sum_{\substack{\omega\in L\\ \omega\neq 0}}\frac{1}{\omega^4} = 60\sum_{k=1}^{\infty}\frac{1}{k^4}\sum_{\omega\in V}\frac{1}{\omega^4} = \frac{\pi^4}{90}\cdot 60\sum_{\omega\in V}\frac{1}{\omega^4} \\ g_3(\omega_1,\omega_2) &= 140\sum_{\substack{\omega\in L\\ \omega\neq 0}}\frac{1}{\omega^6} = \frac{\pi^6}{945}\cdot 140\sum_{\omega\in V}\frac{1}{\omega^6}. \end{aligned}$$

If we put $G_2(\omega_1,\omega_2) = 60\sum_{\omega\in V}\frac{1}{\omega^4}$ and

$G_3(\omega_1,\omega_2) = 140\sum_{\omega\in V}\frac{1}{\omega^6}$, then

$$g_2 = \frac{\pi^4}{90}\, G_2 \text{ and}$$

$$g_3 = \frac{\pi^6}{945}\, G_3 .$$

The condition $g_2^3 - 27g_3^2 \neq 0$ becomes $49\,G_2^3 - 1080\,G_3^2 \neq 0$, and Klein's modular invariant

$$J(\omega_1, \omega_2) = \frac{g_2^3}{g_2^3 - 27g_3^2}$$

may be written

$$J(\omega_1, \omega_2) = \frac{49G_2^3}{49G_2^3 - 1080G_3^2} \quad .$$

§ 7. A Generalization of the Euler ϕ-Function.

In § 5 we considered the limiting fraction of points in a rectangle $Q(X,Y)$ which are visible from both (o,o) and (u,v). Let us now put $(u,v) = (m,o)$ and allow $Q(X,Y)$ to expand by making $X \to \infty$ first, holding Y constant, and finally letting $Y \to \infty$. The limiting fraction of points in $Q(X,Y)$ visible from both (o,o) and (m,o) is

$$\lim_{Y\to\infty} \frac{1}{Y} \sum_{n \leq Y} F(m,n),$$

where

$$F(m,n) = \lim_{X\to\infty} \frac{1}{X} \sum_{\substack{x \leq X \\ (x,n)=1 \\ (x-m,n)=1}} 1. \tag{7.1}$$

For fixed m and n, $F(m,n)$ is the average value of the function $f(x)$, where $f(x) = 1$ if $(x,n) = (x-m,n) = 1$ and $f(x) = 0$ otherwise. Since $f(x)$ is periodic with period n, the average need only be extended over the interval $1 \leq x \leq n$, and we have

$$F(m,n) = \frac{1}{n} \sum_{\substack{x \leq n \\ (x,n)=1 \\ (x-m,n)=1}} 1.$$

If we define y by $x + y = n + m$, then

$$F(m,n) = \frac{1}{n} \sum_{\substack{x \leq n \\ x+y=n+m \\ (x,n)=(y,n)=1}} 1 = \frac{1}{n} \phi(n,m) \tag{7.2}$$

where $\phi(n,m)$ is the number of ordered pairs of integers (x,y) satisfying $x + y = n + m$, $1 \leq x \leq n$, $(x,n) = (y,n) = 1$. The function $\phi(n,m)$ which

$$x_1 \equiv x \pmod{n},\ 1 \leq x_1 \leq n$$
$$y_1 \equiv y \pmod{n},\ m \leq y_1 \leq m + n - 1.$$

Then $x_1 + y_1 \equiv m \pmod{n}$ and $1 \leq x_1 + y_1 - m < 2n$, which implies $x_1 + y_1 = n + m$. Conversely, any pair (x_1, y_1) satisfying this last condition with $(x_1, n) = (y_1, n) = 1$ automatically satisfies (7.3). Since there is a one-to-one correspondence between the pairs (x, y) satisfying (7.3) and the pairs (x_1, y_1) satisfying Alder's condition, there are the same number of each, and therefore the two definitions of $\phi(n, m)$ are equivalent.

It is now natural to define, for positive integral s, a new function $\phi_s(n, m)$ to be the number of distinct solutions (mod n) of the congruence

$$(7.4) \qquad x_1 + x_2 + \dots + x_s \equiv m \pmod{n} \text{ with}$$
$$(x_1, n) = (x_2, n) = \dots = (x_s, n) = 1.$$

With this notation the Alder function is $\phi_2(n, m)$ and the Euler function $\phi_2(n, o)$. In the degenerate case $s = 1$, we have $\phi_1(n, m) = \left[\frac{1}{(n, m)}\right]$.

A number of properties of $\phi_s(n, m)$ will be derived, beginning with the following theorem linking it to Ramanujan's sum $C_n(m) = \sum_{k \bmod n}^{*} e\left(\frac{km}{n}\right)$. Here $e(x) = \exp(2\pi i x)$ and the sum on k is over any <u>reduced</u> residue system (mod n). Omission of the asterisk will mean summation over any <u>complete</u> residue system.

<u>Theorem 7.3</u>. If s is a positive integer, the s th power of $C_n(m)$ is given by

$$(7.5)\quad C_n^s(m) = \sum_{j \bmod n} \phi_s(n,j)e\left(\frac{jm}{n}\right).$$

Furthermore,

$$(7.6)\quad \phi_s(n,m) = \frac{1}{n} \sum_{j \bmod n} C_n^s(j)e\left(\frac{jm}{n}\right).$$

Equation (7.5) states that $\phi_s(n,j)$ is the coefficient of the j th term in the finite Fourier expansion of the s th power of $C_n(m)$. Equations (7.5) and (7.6) are equivalent, being a "Fourier transform pair" (see [7]), and we need only prove (7.5). We have

$$C_n^s(m) = \sum_{x_1 \bmod n}^{*} e\left(\frac{x_1 m}{n}\right) \sum_{x_2 \bmod n}^{*} e\left(\frac{x_2 m}{n}\right) \cdots \sum_{x_s \bmod n}^{*} e\left(\frac{x_s m}{n}\right)$$

$$= \sum_{x_1 \bmod n}^{*} \sum_{x_2 \bmod n}^{*} \cdots \sum_{x_s \bmod n}^{*} e\left(\frac{m}{n}(x_1 + x_2 + \ldots x_s)\right)$$

$$= \sum_{j \bmod n} e\left(\frac{jm}{n}\right) \sum_{\left.\begin{array}{c} x_1 \bmod n \\ x_2 \bmod n \\ \vdots \\ x_s \bmod n \end{array}\right\} x_1 + x_2 + \ldots + x_s \equiv j \pmod n}^{*} 1$$

$$= \sum_{j \bmod n} \phi_s(n,j)e\left(\frac{jm}{n}\right).$$

Since $C_n(m)$ reduces to $\phi(n)$ when $m = n$ and to the Möbius function $\mu(n)$ when $m = 1$, substitution of these values in the first line of Theorem 7.3 gives the following corollary:

<u>Corollary 7.1.</u> $$\phi^s(n) = \sum_{j \bmod n} \phi_s(n,j)$$

$$u^s(n) = \sum_{j \bmod n} \phi_s(n,j)e\left(\frac{j}{n}\right).$$

The second line of Theorem 7.3 leads to an evaluation of $\phi_s(n,m)$ as a divisor sum, namely:

<u>Theorem 7.4.</u> $$\phi_s(n,m) = \frac{\phi^s(n)}{n} \sum_{d|n} \frac{\mu^s(d)}{\phi^s(d)} \; C_d(m) .$$

The proof is based on the formula

$$C_n(m) = \frac{\phi(n)\mu\left(\frac{n}{(n,m)}\right)}{\phi\left(\frac{n}{(n,m)}\right)} \tag{7.7}$$

given by Anderson and Apostol [7] and others. Substitution of (7.7) in (7.6) yields

$$\phi_s(n,m) = \frac{\phi^s(n)}{n} \sum_{j \bmod n} \frac{\mu^s\left(\frac{n}{(n,j)}\right)}{\phi^s\left(\frac{n}{(n,j)}\right)} \; e\left(\frac{jm}{n}\right). \tag{7.8}$$

Next, the order of summation is changed, first running over all j such that $(n,j) = d$, and finally over all $d|n$.

$$\phi_s(n,m) = \frac{\phi^s(n)}{n} \sum_{d|n} \frac{\mu^s\left(\frac{n}{d}\right)}{\phi^s\left(\frac{n}{d}\right)} \sum_{\substack{j \bmod n \\ (n,j)=d}} e\left(\frac{j}{d}\, m / \frac{n}{d}\right) \qquad \text{Let } j = dk$$

$$= \frac{\phi^s(n)}{n} \sum_{d|n} \frac{\mu^s\left(\frac{n}{d}\right)}{\phi^s\left(\frac{n}{d}\right)} \sum_{\substack{k \bmod \frac{n}{d} \\ \left(\frac{n}{d},k\right)=1}} e\left(km / \frac{n}{d}\right) .$$

The inside sum is $C_{\frac{n}{d}}(m)$, yielding Theorem 7.4 with the sum on d running backward. We now have

<u>Corollary 7.2</u>. The function $\phi_s(n,m)$ is multiplicative in the variable n,

i.e. $\phi_s(n\,n',m) = \phi_s(n,m)\,\phi_s(n',m)$ if $(n,n') = 1$.

For, $C_d(m)$ is multiplicative in d, as are $\mu(d)$ and $\phi(d)$, and by a well known theorem the divisor sum in Theorem 7.4 is multiplicative in n.

From Theorem 7.4 we derive the following product representation:

<u>Theorem 7.5</u>. $\phi_s(n,m) = \dfrac{\phi^s(n)}{n} \displaystyle\prod_{p\mid(n,m)} \left(1 - \frac{(-1)^{s-1}}{(p-1)^{s-1}}\right) \prod_{\substack{p\mid n\\ p\nmid m}} \left(1 - \frac{(-1)^s}{(p-1)^s}\right)$.

For multiplicative f, the sum

$$\sum_{d\mid n} \mu^s(d) f(d)$$

has the Euler product

$$\prod_{p\mid n} (1 + (-1)^s f(p)).$$

For fixed m, if we let $f(d) = \dfrac{C_d(m)}{\phi^s(d)}$, Theorem 7.4 yields

$$\phi_s(n,m) = \frac{\phi^s(n)}{n} \prod_{p\mid n} \left(1 + (-1)^s \frac{C_p(m)}{(p-1)^s}\right).$$

The well known formula

$$C_n(m) = \sum_{d\mid(n,m)} d\mu\left(\frac{n}{d}\right)$$

shows that $C_p(m) = p-1$ or -1 according as $p\mid m$ or $p\nmid m$, and substitution of these values gives Theorem 7.5.

The product form reveals some interesting properties of $\phi_s(n,m)$ in light of its definition as the number of solutions of a congruence. For example, if s is odd and both m and n are even, or if s and n are even and m is odd, then one of the factors in Theorem 7.5 is zero and $\phi_s(n,m) = 0$. Conversely, aside from the case $s = 1$, these are the only conditions under which the product can vanish, which proves

<u>Corollary 7.3</u>. For $s \geqslant 2$, the congruence (7.4) is insoluble if and only if n is even and s and m have opposite parity. For $s = 1$ there is, of course, no solution unless $(m,n) = 1$.

Another consequence of Theorem 7.5 is the following:

<u>Corollary 7.4</u>. If s is even, the number of solutions of the congruence (7.4) is maximized, for fixed n, by taking $m = 0$, and minimized by taking $m = 1$. If s is odd the reverse is true.

We turn our attention now to a certain functional equation satisfied by $\phi_s(n,m)$.

<u>Theorem 7.6</u>. The function $\phi_s(n,m)$ satisfies the functional equation

$$\sum_{m \bmod \langle n,n'\rangle} \phi_s(n,m)\phi_s(n',m+k) = \frac{\phi^s(\langle n,n'\rangle)}{\phi^s((n,n'))} \; \phi_{2s}((n,n'),k).$$

The left-hand side is essentially the <u>cross-correlation function</u> of the functions $\phi_s(n,-)$ and $\phi_s(n',-)$. Here $\langle n,n'\rangle$ denotes the l.c.m. of n and n'. If $n' = n$ we have the following corollary:

<u>Corollary 7.5</u>. $$\sum_{m \bmod n} \phi_s(n,m)\phi_s(n,m+k) = \phi_{2s}(n,k).$$

That is, the <u>autocorrelation</u> <u>function</u> of $\phi_s(n,-)$ is $\phi_{2s}(n,-)$.

The proof of Theorem 7.6 is based on the following lemma which asserts that the cross-correlation function is the "inner product" of the two Fourier series:

<u>Lemma</u>. If f and g are periodic with common period M and have the respective Fourier series

$$(7.9) \qquad f(m) = \sum_{j \bmod M} a_j\, e\left(\frac{jm}{M}\right),\quad g(m) = \sum_{j \bmod M} b_j\, e\left(\frac{jm}{M}\right),\ \text{then}$$

$$(7.10) \qquad \frac{1}{M} \sum_{m \bmod M} \bar{f}(m)\, g(m+k) = \sum_{j \bmod M} \bar{a}_j\, b_j\, e\left(\frac{jk}{M}\right).$$

Here a bar denotes complex conjugate. Since our functions and Fourier coefficients are real-valued, the bars can be removed, but they are needed in the proof of the lemma.

We substitute in the left hand side of (7.10) the series (7.9) for f and g, replacing all terms in the former series by their complex conjugates.

$$\frac{1}{M} \sum_{m \bmod M} \sum_{i \bmod M} \bar{a}_i\, e\left(\frac{-im}{M}\right) \sum_{j \bmod M} b_j\, e\left(\frac{jm+jk}{M}\right)$$

$$= \frac{1}{M} \sum_{i \bmod M} \sum_{j \bmod M} \bar{a}_i\, b_j\, e\left(\frac{jk}{M}\right) \sum_{m \bmod M} e\left(\frac{jm-im}{M}\right)$$

The last sum on the right is equal to M if $i \equiv j \pmod M$ and is equal to zero otherwise. This expression thus reduces to (7.10), proving the lemma.

To prove Theorem 7.6, let $f(m) = \phi_s(n,m)$ and $g(m) = \phi_s(n',m)$.

The respective Fourier series are given by Theorem 7.3 and have periods n and n'. To get a common period $M = \langle n,n' \rangle$, we may write

$$\phi_s(n,m) = \frac{1}{n} \sum_{j \bmod M} a_j \, e\left(\frac{jm}{M}\right) \quad \text{where } a_j = C_n^s\left(\frac{j(n,n')}{n'}\right) \text{if } \frac{n'}{(n,n')} \mid j$$

$$= 0 \text{ otherwise}$$

$$\phi_s(n',m) = \frac{1}{n'} \sum_{j \bmod M} b_j \, e\left(\frac{jm}{M}\right) \quad \text{where } b_j = C_{n'}^s\left(\frac{j(n,n')}{n}\right) \text{if } \frac{n}{(n,n')} \mid j$$

$$= 0 \text{ otherwise.}$$

The lemma now gives

$$\sum_{m \bmod M} \phi_s(n,m)\, \phi_s(n',m+k) = \frac{M}{n\,n'} \sum_{\substack{j \bmod M \\ \frac{n\,n'}{(n,n')^2} \mid j}} C_n^s\left(\frac{j(n,n')}{n'}\right) C_{n'}^s\left(\frac{j(n,n')}{n}\right) e\left(\frac{jk}{M}\right).$$

If we put $N = (n,n')$ and let $j = i\,\frac{M}{N}$, then i ranges over a complete residue system (mod N) and the right side becomes

$$(7.11) \qquad \frac{1}{N} \sum_{i \bmod N} C_n^s\left(\frac{in}{N}\right) C_{n'}^s\left(\frac{in'}{N}\right) e\left(\frac{ik}{N}\right) .$$

Substitution of the formula (7.5) for Ramanujan's sum gives, after a little juggling,

$$(7.12) \qquad \frac{\phi^s(n)\, \phi^s(n')}{N} \sum_{i \bmod N} \frac{\mu^{2s}\left(\frac{N}{(N,i)}\right)}{\phi^{2s}\left(\frac{N}{(N,i)}\right)} \, e\left(\frac{ik}{N}\right) ,$$

and reference to (7.8) shows that this last summation is equal to $\frac{N\,\phi_{2s}(N,k)}{\phi^{2s}(N)}$. The form of the right side of Theorem 7.6 is reached by applying the identities

$$\frac{N\,\phi(n)\,\phi(n')}{\phi(N)} = \phi(n\,n') = \phi(M\,N) = \frac{N\,\phi(M)\,\phi(N)}{\phi(N)} .$$

REFERENCES

[1] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Third Edition, Oxford (1954).

[2] F. Mertens, Journal für Math., 77, 289-338 (1874).

[3] W. J. Leveque, Topics in Number Theory, Vol. I, Addison-Wesley (1956).

[4] J. Christopher, Am. Math. Monthly, 63, No. 6, 399-401 (1956).

[5] H. L. Alder, Am. Math. Monthly, 65, No. 9, 690-692 (1958).

[6] V. A. Golubev, Mathesis, Tome LXVII, 11-20 (1958).

[7] D. R. Anderson and T. M. Apostol, Duke Math. Journal, 20, No. 2, 211-216 (1953).