# THE RELATION BETWEEN THE CLASS NUMBER AND THE DISTRIBUTION OF PRIMES

N. C. ANKENY AND S. CHOWLA

We shall present here a very simple proof of a connection of the distribution of primes and the class number of a quadratic imaginary algebraic number field. All constants in the following are easily computable. No other method is available to compute the class number with exact constants. The following method, however, is based on a conditional hypothesis.

Let $d \equiv 3 \pmod 4$ and a prime; $k(d)$ the class number of the field $R((-d)^{1/2})$ where $R$ is the rational numbers; $\pi(z;\, d,\, t)$ the number of primes not greater than $z$ and congruent to $t \pmod d$.

THEOREM. *If* $\pi(z; d, t) < Az/(d-1) \log z$ *for any* $z$ *with* $d < z < e^{c(d)^{1/2}/r}$ *and for all* $t$ *which are nonresidues* $(\bmod\ d)$; *where*

$$A < 2,\ c = (1/25)(1 - A/2),$$

*then* $h(d) > r$ *for* $d > N = N(A, r)$.

PROOF. By hypothesis the number of primes not greater than $z$ and quadratic residues of $k$ must be not less than $(1 - A/2)(z/\log z)$, as the maximum number of primes which are nonresidues is $(A/2)(z/\log z)$.

If[1] $h(d) = s \leqq r$, these primes must be represented by one of the following $s$ reduced forms:

$$a_i x^2 + b_i xy + c_i y^2 = \frac{1}{4a_i}\left((2a_i x + b_i y)^2 + dy^2\right)$$

where $0 < a_i \leqq (d/3)^{1/2}$, $|b_i| \leqq (d/3)^{1/2}$ for $i = 1, 2, \cdots, s$.

We shall now compute an upper bound on the number of all numbers not greater than $z$ for $d < z < e^{c(d)^{1/2}/r}$ and represented by one of the above $s$ forms.

Now

$$(2a_i x + b_i y)^2 + dy^2 \leqq 4a_i z$$

has at most $2(4a_i z/d)^{1/2} + 1$ different positive and negative integer solutions for $y$, as clearly by above $|y| \leqq (4a_i z/d)^{1/2}$. Hence, for a fixed $y$,

Received by the editors September 18, 1949.

[1] We shall assume here that all the elementary facts on the representation of numbers by binary quadratic forms are known. E. Landau, *Vorlesungen über Zahlentheorie*, vol. 1.

$$\begin{aligned} |2a_ix| &\leqq (4a_iz)^{1/2} + |b_iy| \\ &\leqq (4a_iz)^{1/2}\left(1 + \frac{|b_i|}{d^{1/2}}\right). \end{aligned}$$

Therefore, there are at most $2(z/a_i)^{1/2}(1+|b|/d^{1/2})+1$ different solutions for $x$.

Therefore, at most

$$\left(4\left(\frac{a_iz}{d}\right)^{1/2}+1\right)\left\{2\left(\frac{z}{a_i}\right)^{1/2}\left(1+\frac{|b|}{d^{1/2}}\right)+1\right\}$$

$$< \left(5\left(\frac{a_iz}{d}\right)^{1/2}\right)\left(5\left(\frac{z}{a_i}\right)^{1/2}\right) = 25\frac{z}{d^{1/2}}$$

(utilizing our bounds on $a_i$ and $b_i$) numbers not greater than $z$ can be represented by any one form.

Therefore, at most $25(z/d^{1/2})s$ numbers not greater than $z$ can be represented by all $s$ forms. Therefore,

$$\begin{aligned} 25\frac{sz}{d^{1/2}} &\geqq \left(1-\frac{A}{2}\right)\frac{z}{\log z}, \\ \log z &\geqq \frac{1}{25s}\left(1-\frac{A}{2}\right)d^{1/2} \\ &\geqq \frac{1}{25r}\left(1-\frac{A}{2}\right)d^{1/2} \\ &\geqq \frac{c}{r}d^{1/2} \end{aligned}$$

which is a contradiction to the definition of $z$.

It is interesting to note that Viggo Brun has shown $\pi(z;\ d,\ t) < Az/d \log z$ for $z \geqq d^{1+\epsilon}$, but the $A$ is about 6. Selberg's recent work yields an improvement in the value $A$, to $A$ slightly greater than 2.

The above method works for any positive $d$. When $d \equiv 3 \pmod 4$ and a prime, the problem of the greatest $d$ such that $h(d)=1$ has not yet been settled.

PRINCETON UNIVERSITY, AND
INSTITUTE FOR ADVANCED STUDY