ON THE SUM AND DIFFERENCE OF SQUARES OF PRIMES

PAUL ERDÖS*.

[*Extracted from the Journal of the London Mathematical Society, Vol.* 12, 1937.]

Introduction.

It is well known that the number of solutions of the equation $m = x^2-y^2$ is equal to twice the absolute value of the difference between the number of even and the number of odd divisors of m. On the other hand, the number of solutions of the equation $n=x^2+y^2$ is equal to four times the difference between the number of divisors of n of the form $4k+1$ and the number of those of the form $4k+3$. From elementary results concerning the distribution of primes, it easily follows that for suitable m and n both the equations $m=x^2-y^2$ and $n=x^2+y^2$ have more than $m^{c_1/\log\log m}$ and $n^{c_2/\log\log n}$ solutions respectively [c_1, c_2, ... denote positive absolute constants]. In §1of this paper we shall prove that for suitable m the equation $m = p2-q2$, where p and q are primes, has more than $m^{c_3/\log\log m}$ solutions; in §2 we show that for suitable n the number of solutions of the equation $n = p^2+q^2$ is greater than $n^{c_4/(\log\log n)^2}$.

The proofs are elementary and similar to the proof of my results concerning the number of representations as the sum of k k-th powers†.

1. We put $A-3\ldots p_k$, the product of the first k odd primes, and estimate the number of solutions S of the congruence $p^2-q^2\equiv 0 \pmod A$, with $q<p<A$.

Suppose that $(a, A)=1$. It is well known that, if a is a quadratic residue mod A, the congruence $X^2\equiv a \pmod A$ has 2^k solutions. Hence the $\phi(A)$ residues mod A may be distributed into $\phi(A)/2^k$ classes, each containing 2^k residues, such that the squares of the residues of each class are all congruent to one another mod A.'

We now denote by $y_1, y_2, \ldots, y_{\phi(A)/2^k}$ the number of primes lying in the various classes and satisfying $p<A$, $p+A$. By well-known elementary theorems, the number of primes $p<A$ with $p+A$ is between $*A/\log A$ and $2A/\log A$.

Thus we evidently have

$$S=\tfrac{1}{2}[y_1^2+y_2^2+\ldots+y^2_{\phi(A)/2^k}-y_1-y_2-\ldots-y_{\phi(A)/2^k}]$$
$$>\tfrac{1}{2}[y_1^2+y_2^2+\ldots+y^2_{\phi(A)/2^k}]-\frac{A}{\log A}.$$

But
$$y_1+y_2+\ldots+y_{\phi(A)/2^k}>\frac{A}{2\log A},$$

* Received 1 October, 1936; read 12 November, 1936.
† *Journal London Math. Soc.*, 11 (1936), 133-136.

and, by a well-known elementary theorem, the sum of the squares of the y's is a minimum if they are all equal, i.e. if

$$y_i = \frac{A2^k}{2\log A\phi(A)} > \frac{2^{k-1}}{\log A}.$$

Hence $$S > \frac{2^{k-3}\phi(A)}{(\log A)^2}\frac{A}{\log A} > 2^{\frac{1}{3}\log A/\log\log A},$$

since, by the prime number theorem (or by a more elementary theorem), $k > \frac{1}{2}\log A/\log\log A$.

But the integers of the form p^2-q^2 with $q<p<A$ are all positive and less than A^2, so that we can always find a multiple of A, say m, less than A for which the equation $m = p^2-q^2$ has more than

$$2^{\frac{1}{3}\log A/\log\log A} > e^{\frac{1}{6}\log A/\log\log A} = A^{1/(6\log\log A)} > m^{1/(12\log\log m)}$$

solutions. Hence the result.

2. Hereweput $A = 5.13\ldots p_k$, where the p's are consecutive primes of the form $4A+1$. We write $A = a_1a_2\ldots a_x$, where $x = [10\log\log A]$, and all the a's have at least $[k/x]$ prime factors.

First we prove the following

LEMMA. *There exists an a_i such that the number of primes $p<A$ in each of at least $\frac{7}{8}\phi(a_i)$ residue classes* mod a_i *is greater than $A/\phi(a_i)(\log A)^2$.*

Proof. Suppose that the lemma is not true. For every a_i we divide the residues mod a_i into two classes. Class 1 contains the residues for which the number of primes in each of them is less than $A/\phi(a_i)(\log A)^2$; class 2 contains the other residues. Similarly we divide the primes $p<A$ into two groups : into group I we put those primes which are for at least one a_i congruent (mod a_i) to a residue of class 1, into group II all the other primes.

The number of primes $p \leqslant A$ congruent for a fixed modulus a_i to a residue of class 1 is evidently less than $A/(\log A)^2$, hence the total number of primes belonging to group I is less than

$$(\log Ax)\frac{10A\log\log A}{(\log A)^2}.$$

The number of residues mod A belonging for every a_i to class 2 is, in consequence of the multiplicativity of the residue-classes, less than

$$\tfrac{7}{8}\phi(a_1)\ \tfrac{7}{8}\phi(a_2)\ \ldots\ \tfrac{7}{8}\phi(a_x) = (\tfrac{7}{8})^x\phi(A) < A(\tfrac{7}{8})^{10\log\log A-1} < \frac{A}{(\log A)^{\frac{5}{4}}}.$$

Hence the number of primes belonging to group II is also less than $A/(\log A)^{\frac{5}{4}}$.

Thus the number of primes $p \leqslant$ A with $p+A$ would be less than

$$\frac{10A \log\log A}{(\log A)^2}+\frac{A}{(\log A)^{\frac{5}{4}}}<\frac{A}{2\log A},$$

which is not so. Hence the lemma is established.

Let us now consider an a_i for which the number of residues belonging to class 2 is greater than $\frac{7}{8}\phi(a_i)$. Let these residues be $z_1, z_2, \ldots, z_l$, $l > \frac{7}{8}\phi(a_i)$. We estimate the number of solutions S_1 of the congruence

$$z_\kappa^2+z_\lambda^2 \equiv 0 \pmod{a_i}.$$

Let ξ be a quadratic residue mod a_i; then the number of solutions of the congruence $\mu^2 \equiv \xi \pmod{a_i}$ is known to be $2^{V(a_i)}$, where $V(a_i)$ denotes the number of prime factors of a_i. Thus the number of quadratic residues mod a_i is $R=\phi(a_i)/2^{V(a_i)}$. Since the prime factors of a_i are all of the form $4A+1$, $-\xi$ is also a quadratic residue mod a_i.

Thus the quadratic residues fall into $\frac{1}{2}R$ pairs $(\xi_u, -\xi_u)$. We assert that, for at least $\frac{1}{4}R$ pairs, each of the congruences

$$z_k^2 \equiv \xi_u \pmod{a_i}, \quad z_k^2 \equiv -\xi_u \pmod{a_i}$$

has at least $2^{V(a_i)-1}$ solutions. For, if this is not so, then, for at least $\frac{1}{4}R$ pairs, one of the congruences has less than $2^{V(a_i)-1}$ solutions, i.e. for at least $\frac{1}{4}R$ quadratic residues ξ the congruence $z_k^2 \equiv \xi \pmod{a_i}$ has less than $2^{V(a_i)-1}$ solutions. But then the number of z_k is less than

$$\tfrac{1}{4}R\,2^{V(a_i)-1}+\tfrac{3}{4}R\,2^{V(a_i)}=\tfrac{7}{8}\phi(a_i)_1,$$

which is not so.

Hence
$$S_1 > \frac{\phi(a_i)}{2^{V(a_i)+2}}2^{2V(a_i)-2} = \frac{2^{V(a_i)}\phi(a_i)}{16}.$$

Thus, finally, the number of solutions of the congruence $p^2+q^2 \equiv 0 \pmod{a_i}$, with $p<A$, $q<A$, is greater than

$$\frac{\phi(a_i)2^{V(a_i)}A^2}{16\phi(a_i)^2(\log A)^*} > \frac{2^{V(a_i)}A^2}{16(\log A)^4 a_i} > \frac{A^2 2^{k/x}}{32(\log A)^4 a_i} > \frac{A^2 2^{\log A/40(\log\log A)^2}}{32(\log A)^4 a_i}$$
$$> \frac{A^2 2^{\log A/80(\log\log A)^2}}{a_i},$$

since, by the prime number theorem for arithmetical progressions (or by a more elementary theorem), $k > \frac{1}{4}$ log A/log log A.

But the integers of the form p^2+q^2 with $p, q < A$ are all less than $2A^2$. Hence there exists a multiple of a_i, say n, less than $2A^2$, for which the

equation $n = p^2+q^2$ has more than

$$2^{\{\log A/80 (\log\log A)^2\}-1} > e^{\log A/160 (\log\log A)^2} = A^{1/160 (\log\log A)^2} > n^{1/400 (\log\log A)^2}$$

solutions, which establishes the result.

Using a well-known result of Brun and Titchmarsh*, one can even prove that for an infinity of n the number of solutions of the equation $n = p^2+q^2$ is greater than $n^{c_5/\log\log n}$. Also, by a method similar to that used in § 1, we can prove the following theorem.

Let $a_1, a_2, \ldots$ be an infinite sequence of integers such that for an infinity of N the number of a's less than or equal to N is greater than $N^{1-(c_6/\log\log N)}$ with $c_6 < \frac{1}{2}\log 2$, then for an infinity of M the number of solutions of the equation $a_i^2 - a_r^2 = M$ is greater than $M^{c_7/\log\log M}$, where c, depends only upon c_6. These results I intend to consider in another paper.

The University,
Manchester.

* E. C. Titchmarsh, Rend. *di Palermo*, 54 (1930), 414-29.

Printed by C. F. Hodgsbn & Son, Ltd., Newton St., London, W.C.2.