THE REPRESENTATION OF AN INTEGER AS THE SUM OF THE SQUARE OF A PRIME AND OF A SQUARE-FREE INTEGER

Paul Erdös*.

[*Extracted from the Journal of the London Mathematical Society, Vol.* 10, 1935.]

Denote throughout by n a sufficiently large integer, by p, q, r, s, t odd primes, by f a square-free integer, by x, y, m integers. I prove the following

Theorem. *Primes p and square-free integers f exist such that*

$$n = p^2 + f \quad when \quad n \not\equiv 1 \pmod 4$$

$$n = 4p^2 + f \quad when \quad n \equiv 1 \pmod 4.$$

These results are similar to those of Estermann†,

$$n = p + f, \quad n = x^2 + f.$$

Assume first that $n \not\equiv 1 \pmod 4$. It is sufficient to show that we can find a prime p such that $n - p^2$ is square free. We use two formulae for the number N of primes $p \leqslant X$ of the form $km + l$, $m = 0, 1, 2, \ldots$. The first,

$$N = \frac{X}{\phi(k) \log X} + O\left(\frac{X}{(\log X)^2}\right),$$

---

* Received 2 February, 1935; read 14 February, 1935.

† T. Estermann, "Einige Sätze über quadratfreie Zahlen", *Math. Annalen*, 105 (1931), 653–662.

is given by the prime number theorem. The second,

$$N < \frac{cX}{\phi(k) \log (X/k)},$$

where c is a number independent of k, l, X, is given immediately by the method of Brun. We note that

$$\sum_{2}^{\infty} \frac{1}{m(m+1)} = \frac{1}{2}, \quad \sum_{p} \frac{1}{p(p-1)} < \frac{1}{2} - \frac{1}{3.4} = \frac{5}{12},$$

and we determine A so great that

$$\sum_{p>A} \frac{8c}{p(p-1)} < \tfrac{1}{6}.$$

We now divide the odd primes less than $\sqrt{n}$ into four classes q, r, s, t typified by

$$(1) \quad q < A,$$

$$(2) \quad A \leqslant r < (\log n)^2,$$

$$(3) \quad (\log n)^2 \leqslant s < \frac{\sqrt{n}}{(\log n)^2},$$

$$(4) \quad \frac{\sqrt{n}}{(\log n)^2} \leqslant t < \sqrt{n}.$$

We now find how often $n-p^2$, where p is a prime less than $\sqrt{n}$, is divisible by the square of a prime less than $\sqrt{n}$. If $n-p^2 \equiv 0 \pmod{q^2}$, then p belongs to at most two arithmetical progressions of difference q^2, and hence the number of these p is, at most,

$$\frac{4\sqrt{n}}{q(q-1)\log n} + O\left(\frac{\sqrt{n}}{(\log n)^2}\right).$$

Hence, summing for q, the number of p's for which $n-p^2$ is divisible by at least one of the q's is less than

$$\frac{\sqrt{n}}{\log n} \sum_{q} \frac{4}{q(q-1)} + O\left(\frac{\sqrt{n}}{(\log n)^2}\right) < \frac{5\sqrt{n}}{3\log n} + O\left(\frac{\sqrt{n}}{(\log n)^2}\right).$$

Similarly, by Brun's result, the number of the primes p for which $n-p^2$ is divisible by an r^2 is less than

$$\sum_{r} \frac{\sqrt{n}}{\log(\sqrt{n}/r^2)} \frac{2c}{r(r-1)} < \frac{\sqrt{n}}{\log n} \sum_{r} \frac{8c}{r(r-1)} < \frac{\sqrt{n}}{6\log n},$$

since $r^2 < (\log n)^4 < n^{\frac{1}{4}}$.

Since there are at most two suitable residues mod s^2, the number of primes p for which $n-p^2$ is divisible by an s^2 is less than

$$2\sum_{s}\left(\left[\frac{\sqrt{n}}{s^2}\right]+2\right) < 2\sum_{m>(\log n)^2}\frac{\sqrt{n}}{m^2}+O\left(\frac{\sqrt{n}}{(\log n)^2}\right)=O\left(\frac{\sqrt{n}}{(\log n)^2}\right).$$

Finally, if $n-p^2$ is divisible by a t^2, we have

$$n-p^2 = Bt^2, \quad B < (\log n)^4.$$

But Rademacher* and Estermann† have established that the equation

$$ax^2+by^2 = n,$$

in which $a > 0$, $b > 0$ are given integers, has at most $2d(n)$ solutions, where $d(n)$ denotes the number of divisors of n.

Hence the number of primes p for which $n-p^2$ is divisible by a t^2 is less than

$$2(\log n)^4 d(n) = O\left(\frac{\sqrt{n}}{(\log n)^2}\right).$$

Thus the number of p's such that $n-p^2$ is divisible by the square of a prime is less than

$$\frac{11\sqrt{n}}{6\log n}+O\left(\frac{\sqrt{n}}{(\log n)^2}\right).$$

But the number of the $p \leqslant \sqrt{n}$ is $2\sqrt{n}/\log n+O\{\sqrt{n}/(\log n)^2\}$ and so $n-p^2$ is square free for $\frac{1}{6}(\sqrt{n}/\log n)+O\{\sqrt{n}/(\log n)^2\}$ primes p. This proves the theorem when $n \not\equiv 1 \pmod 4$.

Similarly we can prove the result for $n \equiv 1 \pmod 4$.

We can prove similarly the more general theorem

$$n = p^k+g,$$

where k is a given exponent and g is free from k-th power divisors. The proof requires a lemma, proved by Oppenheim‡, that the equation

$$ax^k+by^k = n,$$

in which a, b, k, n are given positive integers, has less than $\{k(k-1)+1\}\,d(n)$ solutions in positive integers x, y.

The University,
Manchester.

* Evelyn and Linfoot, "On a problem of additive theory of numbers", *Journal für Math.*, 164 (1931), 133.

† T. Estermann, *ibid.*

‡ Evelyn and Linfoot, *ibid.*

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