
Zbl 586.10003

Erdős, Paul; Pomerance, Carl

On the number of false witnesses for a composite number. (In English)

Math. Comput. 46, 259-279 (1986). [0025-5718]

This is a state of the art report on why the easy Fermat test for compositeness will always have many successes and many failures. Specifically let $F(n) = \#(a \bmod n : \quad a^{n-1} \equiv 1 \bmod n\}$, so if n is not prime, there are $F(n)$ "false witnesses". Since $F(n)$ is the order of a subgroup of $(\mathbb{Z}/n\mathbb{Z})*$ then $F(n)|\phi(n)$ and indeed $F(n) = \phi(n)$ for Carmichael numbers (only conjectured to be infinite).

The authors show $(\sum_{n\neq p, n\leq x} F(n))/n > x^{15/23}$ for x large (the $\sum_{n\neq p}$ denotes the exclusion of primes). Also, $(\prod_{n\leq x} F(n))^{1/x} = c_0(\log x)^c + ...$, and this estimate shows the "normal" order of F(n), ignoring sets of density 0. Similar results hold for the "Euler false witnesses", where $a^{(n-1)/2} \equiv (a/n) \bmod n$, and for the "strong false witnesses", where $a^{(n-1)/M} \equiv 1$ or else $a^{(n-1)/N} \equiv -1 \bmod n$ with $N|M = 2^k||n-1$. Many other special properties of $F(n)$ are givenfor both the normal and exceptional values. Only two are cited here: The most successful case, $F(n) = 1$ ($a = 1$ only), occurs for $(1 + o(1)x)/(e\gamma \log\log\log x)$ cases $\leq x$; and $F(n)$ normally has $\log\log\log\log n$factors.

The references go back to the first author [Q. J. Math., Oxf. Ser. 6, 205-213 (1935; Zbl 012.14905)] and the second author [Mathematika 27, 84- 89 (1980; Zbl 437.10001)], (papers generally dealing with factors of p-1). The authors note (in proof) that according to a private communication of *E. Fouvry* and *B. Rousselet*, the exponent 15/23 can be reduced to 17/25.

Harvey Cohn

Classification:
11A41 Elemementary prime number theory
11A15 Power residues, etc.
11N37 Asymptotic results on arithmetic functions

Keywords:
Euler test; strong pseudoprime tests; test for primality; computational number theory; state of the art report; easy Fermat test for compositeness; false witnesses