

7. Appendix: The number of fugitive primes.

by Andrew Granville

Theorem. Let $F(X_1, X_2, \dots, X_n) \in \mathbf{Z}[X_1, X_2, \dots, X_n]$ be a homogenous, non-zero polynomial of degree D say. For any given prime q , pick a primitive root $g \pmod{q}$, and define $\log a$ to be that power of g that gives $a \pmod{q}$. We call q a ‘fugitive’ prime if $F(\log 2, \log 3, \dots, \log p_n) \equiv 0 \pmod{q-1}$. There are $O(x \log \log \log x / \log x \log \log x)$ fugitive primes $q \leq x$.

Proof: We first deal with those primes $q \leq x$, for which $q-1$ does not have a prime factor in the interval $I = (\log \log x, (\log x)^{1/(n+2)})$. The number of such primes q is given by (where m is the product of the primes in I)

$$\begin{aligned} \sum_{q \leq x} \sum_{\substack{d|q-1 \\ d|m}} \mu(d) &= \sum_{d|m} \mu(d) \pi(x; d, 1) \\ &= \sum_{d|m} \mu(d) \frac{\pi(x)}{\phi(d)} + O\left(\sum_{d \leq x^{1/3}} \left| \pi(x; d, 1) - \frac{\pi(x)}{\phi(d)} \right|\right) \\ &= \pi(x) \prod_{p|m} \left(1 - \frac{1}{p-1}\right) + O\left(\frac{x}{\log^2 x}\right) \ll \frac{x}{\log x} \frac{\log \log \log x}{\log \log x}, \end{aligned}$$

using the Bombieri-Vinogradov Theorem (see section 28 of [Da]), Mertens’ Theorem and the Prime Number Theorem. Thus these primes may be included amongst the candidates for fugitive primes.

We shall show that for any prime p in the interval I , the number of fugitive primes $q \leq x$, which are $\equiv 1 \pmod{p}$ is $\ll x/p^2 \log x$. But then the number of fugitive primes $q \leq x$ for which $q-1$ has a prime factor in the interval I , is

$$\ll \sum_{p \in I} \frac{x}{p^2 \log x} \ll \frac{x}{\log x \log \log x},$$

and the Theorem follows.

So fix prime p in the interval I , and let α be a primitive p th root of unity. Once x is sufficiently large (so that p is), one has, as a trivial consequence of Legendre’s theorem, that there are $\leq Dp^{n-1}$ solutions $\mathbf{a} = (a_1, a_2, \dots, a_n) \in (\mathbf{Z}/p\mathbf{Z})^n$ to $F(a_1, a_2, \dots, a_n) \equiv 0 \pmod{p}$ (call the set of such solutions S_p). Now, for each fugitive prime $q \leq x$ which is $\equiv 1 \pmod{p}$, we must have $F(\log 2, \log 3, \dots, \log p_n) \equiv 0 \pmod{p}$, since p divides $q-1$, and so $\log p_j \equiv a_j \pmod{p}$ for $1 \leq j \leq n$, for some $\mathbf{a} \in S_p$. Therefore the number of

such fugitive primes is \leq the sum, over each $\mathbf{a} \in S_p$, of the number of primes $q \leq x$, $q \equiv 1 \pmod{p}$, for which

$$(*) \quad p_j^{(q-1)/p} \equiv \alpha^{a_j} \pmod{\mathbf{q}} \quad \text{for } 1 \leq j \leq n,$$

where \mathbf{q} is a fixed prime ideal divisor of q in $\mathbf{Q}(\alpha)$.

If p were fixed and x were sufficiently large then the number of such primes q (for each given $\mathbf{a} \in S_p$) would be $\sim x/p^{n+1} \log x$ (by the Chebotarev density theorem). However, we have x as a function of p (in fact, $x \geq e^{p^{n+2}}$), and since the discriminant of the field $\mathbf{Q}(\alpha, 2^{1/p}, 3^{1/p}, \dots, p_n^{1/p})$ divides $(2 \times 3 \times \dots \times p_n \times p^{n+1})^{p^{n+1}}$, we deduce immediately from Theorem 1.4 of [LMO] that the number of such primes q , is $O(x/p^{n+1} \log x)$. Then, from the above, the number of fugitive primes, for given prime p , is $\ll |S_p| x/p^{n+1} \log x \ll D p^{n-1} x/p^{n+1} \log x \ll x/p^2 \log x$. This completes the proof of the Theorem.

In order to improve this bound we need a wider range of uniformity than that provided in Theorem 1.4 of [LMO]. For example, suppose that for some small fixed $\delta > 0$, we know that there are $O(x/p^{n+1} \log x)$ primes $q \leq x$, $q \equiv 1 \pmod{p}$ satisfying (*), uniformly for primes $p < x^\delta$. The proof above is easily modified to show that there are $O(x \log \log x / \log^2 x)$ fugitive primes by taking I to be the interval $[\log x, x^\delta]$:

The primes $q \leq x$ for which $q-1$ has a prime factor in I , are dealt with as before. Replacing the combinatorial sieve in the argument above by Selberg's upper bound sieve method (see Theorem 7.1 of [HR]), one proves that there are $O(x \log \log x / \log^2 x)$ primes $q \leq x$, for which $q-1$ does not have a prime factor in I .

Our supposition is implied by a suitable generalization of the Riemann Hypothesis to the appropriate zeta-functions. However a much weaker 'averaged' version would evidently suffice, and since the number fields involved have several amenable properties, this might well be provable using currently known 'zero-density' techniques. It is thus plausible that the upper bound $O(x \log \log x / \log^2 x)$ can be proved unconditionally (though not without a considerable amount of tricky technical work).

On the other hand, we cannot see how to rule out more than a positive proportion of those primes q for which $(q-1)/2$ is also prime. This leaves us with little hope of improving our upper bound even to $o(x/\log^2 x)$ fugitive primes $\leq x$, let alone to what is presumably the correct order of magnitude, $O(\log \log x)$.

[Da] H. Davenport, *Multiplicative Number Theory*, Grad. Texts in Math. **74**, 2nd. edn., (Springer-Verlag, New York, 1980).

[HR] H. Halberstam and H.-E. Richert, *Sieve Methods*, L.M.S. Monographs **4**, (Academic Press, London, 1974).

[LMO] J.C. Lagarias, H.L. Montgomery and A.M. Odlyzko, *A bound for the least prime ideal in Chebotarev density theorem*, *Inventiones Math.* **54** (1979), 271-296.