ON POLYNOMIALS AND ALMOST-PRIMES

BY G. J. RIEGER

Communicated by Ivan Niven, July 31, 1968

There exist infinitely many numbers \( n^2 - 2 \) having at most 3 prime factors [1], [3]. We prove here that there exist infinitely many numbers \( p^2 - 2 \) (\( p \) prime) having at most 5 prime factors; a similar result with the bound 7 instead of 5 can be found in [5] and, under the Riemann hypothesis, with the bound 5. We use the sieve-method, essentially in the version of Jurkat and Richert as given in [6], and also ideas of Kuhn, de Bruijn, and Bombieri.

Let

\[
\begin{align*}
  w(u) &= u^{-1} \quad \text{for } 1 \leq u \leq 2, \\
  (uw(u))' &= w(u - 1) \quad \text{for } u \geq 2, \\
  D(u) &= u \quad \text{for } 0 \leq u \leq 1, \\
  (u^{-1}D(u))' &= -u^{-2}D(u - 1) \quad \text{for } u \geq 1;
\end{align*}
\]

here we take the right-hand derivative for integers \( u \geq 0 \); let \( w \) be continuous at \( u = 2 \) and \( D \) be continuous at \( u = 1 \). Define

\[
\begin{align*}
  \lambda(u) &= e^\gamma u u^{-1}(uw(u) - D'(u - 1)) \\
  \Lambda(u) &= e^\gamma u u^{-1}(uw(u) + D'(u - 1))
\end{align*}
\]

where \( \gamma \) is the Euler constant.

Let \( P \) be the set of all primes \( p \equiv \pm 1 \mod 8 \); \( p_0 = 1 \); denote by \( p_j \) the \( j \)-th number of \( P \) in natural order. Denote by \( \mu \) the Moebius function and by \( \phi \) the Euler function; let

\[
\begin{align*}
  V(n) &= \sum_{p \mid n} \sum_{d \mid n} 1, \\
  Q &= \{ d : \mu(d) \neq 0 \land (p \mid d \Rightarrow p \in P) \}, \\
  f(d) &= 2^{-\nu(d)}\phi(d), \\
  g(d) &= f(d) \prod_{p \mid d} (1 - f(p)^{-1}) \quad (d \in Q), \\
  P(\rho) &= \prod_{1 \leq j \leq \rho} p_j, \\
  R(\rho) &= \prod_{1 \leq j \leq \rho} (1 - f(p_j)^{-1}), \\
  S(x, \rho) &= \sum_{1 \leq a \leq x; a \mid P(\rho)} g(a)^{-1}.
\end{align*}
\]

Using generating functions we find

---

\(^1\) Supported by National Science Foundation Grant GP 9038.
ON POLYNOMIALS AND ALMOST-PRIMES

\[ R(p) = \alpha e^{\gamma} \log p + O(1) \quad (\rho \geq 0), \]
\[ \sum_{1 \leq d \leq x; d \in \mathbb{Q}} g(d)^{-1} = \alpha \log x + O(1), \]

where
\[ \alpha = \frac{1}{2} \prod_{p \in \mathbb{P}} \left( 1 + \frac{3p - 1}{p^2(p - 3)} \right) \prod_{2 < p \in \mathbb{P}} (1 - p^{-2}). \]

After some calculations one arrives at (see also [6], (2.31))
\[ S(x, p) = e^{-\gamma} R(p) - D + O(x^{\rho}) \quad (x > 1, p \geq 0). \]

The number of elements of a finite set \( M \) of natural numbers is denoted by \( |M| \); let \( M^a := \{ m \in M : m \in a \} \),
\[ A(M^a, p) := |\{ m \in M^a : m \equiv a \mod p \}| \quad (p \geq 0). \]

For \( p \geq 0 \) and \( (a, P(p)) = 1 \) we have
\[ A(M^a, p) = |M^a| - \sum_{1 \leq j \leq p} A(M^a, P(p)) - 1 \]

Let
\[ \pi(x; d, r) := |\{ p : 2 \leq p \leq x \land p \equiv r \mod d \}|, \]
\[ \eta(x; d) := \max_{1 \leq r \leq d; (r, d) = 1} |\pi(x; d, r) - \frac{\lfloor x/d \rfloor}{\phi(d)}|. \]

For \( M = M(x) := \{ p^2 - 2 : 2 \leq p \leq x \} \) we have
\[ |M_d| - \frac{\lfloor x/d \rfloor}{\phi(d)} \leq 2^y \eta(x, d) \quad (d \in \mathbb{Z}). \]

Application of the sieve method gives:
For \( x \geq 2, M = M(x), t > 1, a \in \mathbb{Q}, \rho \geq 0, (a, P(p)) = 1 \) we have
\[ A(M^a, p) \leq \frac{\lfloor x \rfloor}{f(a)S(x, \rho)} + O(r_{x, a}(t^2)), \]

where
\[ r_x(x, a, v) := \sum_{1 \leq d \leq x; d \in \mathbb{Q}} 5^{y(d)} \eta(x, ad) \quad (v \geq 1). \]

For \( 0 \leq r \leq \rho, (a, P(p)) = 1 \) one finds easily
\[ r_r(x, a, v) + \sum_{r < j \leq \rho} r_{j-1}(x, a \phi_j, \frac{v}{\phi_j}) \leq r_x(x, a, v). \]
After some calculations one arrives at (see also [7, (4.18)]):

For \( x \geq 2, \ M = M(x), \ \rho > 0, \ (a, \ P(\rho)) = 1, \ \rho_\rho \leq t^2, \ y^* := \lim x/f(a) \) we have

\[
A(M_\rho, \rho) \leq \lambda \left( \frac{\log t^2}{\log \rho} \right) + O \left( \frac{r_\rho(x, a, t^2)}{y^* R(\rho)} \right) + O((\log \log 3t)^{-\gamma}),
\]

\[
\geq \lambda \left( \frac{\log t^2}{\log \rho} \right) - O \left( \frac{r_\rho(x, a, t^2)}{y^* R(\rho)} \right) - O((\log \log 3t)^{-\gamma}).
\]

Following Kuhn, define

\[
C(x; \rho, \sigma) := \left\{ \left\{ \rho - 2 : 2 \leq \rho \leq x \wedge (1 \leq j \leq \rho \Rightarrow p_j \geq (\rho - 2)) \right\} \wedge (\rho < j \leq \sigma \Rightarrow p_j \geq (\rho - 2)) \wedge \sum_{p_j \leq (\rho - 2)} 1 \leq 1 \right\}
\]

for \( x \geq 2, \ 1 \leq \rho < \sigma \). For \( u := \log t^2/\log \rho, \ v := \log t^2/\log \rho, \gamma > 9^{-2}, \ u^{-1} \]

\( + v^{-1} \leq 1 \) we get

\[
\frac{C(x; \rho, \sigma)}{\lim x R(\rho)} \geq \lambda(v) - \frac{1}{2} \int_u^\infty \lambda(v(1 - t^{-1}))t^{-1}dt - O \left( \frac{r_\rho(x, 1, t^2)}{\lim x R(\rho)} \right)
\]

\[ - O((\log \log 3t)^{-\gamma}).\]

For \( t^2 := x^{1/2}(\log x)^{-\beta} \) with suitable \( \beta > 0 \) and for arbitrary \( \sigma > 0 \) we have

\[ r_\rho(x, 1, t^2) = O(x(\log x)^{-\gamma}),\]

according to [2]. We choose \( z, \xi, \rho, \rho_* \) by virtue of

\[ \log z := \frac{1}{6} \log x^{1/2}, \ \log \xi := \frac{17}{21} \log x^{1/2}, \]

\[ \rho \leq z < \rho_\rho + 1, \ \rho_* \leq \xi < \rho_\rho + 1, \]

and write \( C(x) \) instead of \( C(x; \rho, \sigma) \). Since

\[ \lambda(6) - \frac{1}{2} \int_{21/17}^6 \lambda(6(1 - t^{-1}))t^{-1}dt > 0, \]

by [4], we get

**Theorem.** There exists a constant \( c > 0 \) such that

\[ C(x) > cx(\log x)^{-2} \quad (x \geq 2). \]
For any \( p \), counted in \( C(x) \), the number \( p^2 - 2 \) has

(i) no prime factors \( \leq x^{1/12} \),

(ii) at most one prime factor between \( x^{1/12} \) and \( x^{17/42} \)

(iii) prime factors larger than \( x^{17/42} \) otherwise;

since \( 5 \cdot 17/42 > 2 \), we have \( V(p^2 - 2) \leq 5 \).

These fractions can be improved upon, but we were unable to replace 5 by 4.

More details and related results will be contained in lecture notes. Compare also [6].

References


STATE UNIVERSITY OF NEW YORK AT BUFFALO, BUFFALO, NEW YORK 14214