ON POLYNOMIALS AND ALMOST-PRIMES

BY G. J. RIEGER[1]

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

$$w(u) := u^{-1} \qquad \text{for } 1 \leqq u \leqq 2,$$
$$(uw(u))' := w(u-1) \qquad \text{for } u \geqq 2,$$
$$D(u) := u \qquad \text{for } 0 \leqq u \leqq 1,$$
$$(u^{-1}D(u))' := -u^{-2}D(u-1) \qquad \text{for } u \geqq 1;$$

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

$$\left.\begin{aligned} \lambda(u) &:= e^{\gamma}u^{-1}(uw(u) - D'(u-1)) \\ \Lambda(u) &:= e^{\gamma}u^{-1}(uw(u) + D'(u-1)) \end{aligned}\right\} \quad (u \geqq 1)$$

where γ is the Euler constant.

Let P be the set of all primes $p \equiv \pm 1 \bmod 8$; $p_0 := 1$; denote by p_j the jth number of P in natural order. Denote by μ the Moebius function and by ϕ the Euler function; let

$$V(n) := \sum_{p^a | n} \sum 1, \qquad Q := \{d : \mu(d) \neq 0 \wedge (p \mid d \Rightarrow p \in P)\},$$

$$f(d) := 2^{-V(d)}\phi(d), \qquad g(d) := f(d) \prod_{p|d} (1 - f(p)^{-1}) \quad (d \in Q),$$

$$P(\rho) := \prod_{1 \leqq j \leqq \rho} p_j, \qquad R(\rho) := \prod_{1 \leqq j \leqq \rho} (1 - f(p_j)^{-1}),$$

$$S(x, \rho) := \sum_{1 \leqq a \leqq x;\, a | P(\rho)} g(a)^{-1}.$$

Using generating functions we find

[1] Supported by National Science Foundation Grant GP 9038.

$$R(\rho)^{-1} = \alpha e^{\gamma} \log p_\rho + O(1) \qquad (\rho \geqq 0),$$
$$\sum_{1 \leq d \leq x; d \in Q} g(d)^{-1} = \alpha \log x + O(1),$$

where

$$\alpha := \frac{1}{2} \prod_{p \in P} \left(1 + \frac{3p-1}{p^2(p-3)}\right) \prod_{2<p \notin P} (1 - p^{-2}).$$

After some calculations one arrives at (see also [6], (2.31))

$$S(x, \rho) = e^{-\gamma} R(\rho)^{-1} D\left(\frac{\log x}{\log p_\rho}\right) + O\left(1 + \frac{\log x}{\log p_\rho}\right) \qquad (x > 1, \rho \geqq 0).$$

The number of elements of a finite set M of natural numbers is denoted by $|M|$; let $M_a := \{m : m \in M \wedge a \mid m\}$,

$$A(M_a, \rho) := |\{m : m \in M_a \wedge (m, P(\rho)) = 1\}| \qquad (\rho \geqq 0).$$

For $\rho \geqq 0$ and $(a, P(\rho)) = 1$ we have

$$A(M_a, \rho) = |M_a| - \sum_{1 \leq j \leq \rho} A(M_{ap_j}, j-1).$$

Let

$$\pi(x; d, r) := |\{p : 2 \leqq p \leqq x \wedge p \equiv r \bmod d\}|,$$
$$\eta(x, d) := \max_{1 \leq r \leq d; (r,d)=1} \left|\pi(x; d, r) - \frac{\text{li } x}{\phi(d)}\right|.$$

For $M = M(x) := \{p^2 - 2 : 2 \leqq p \leqq x\}$ we have

$$\left| |M_d| - \frac{\text{li } x}{f(d)} \right| \leqq 2^{V(d)} \eta(x, d) \qquad (d \in Q).$$

Application of the sieve method gives:

For $x \geqq 2$, $M = M(x)$, $t > 1$, $a \in Q$, $\rho \geqq 0$, $(a, P(\rho)) = 1$ we have

$$A(M_a, \rho) \leqq \frac{\text{li } x}{f(a) S(x, \rho)} + O(r_\rho(x, a, t^2)),$$

where

$$r_\rho(x, a, v) := \sum_{1 \leq d \leq v; d \mid P(\rho)} 5^{V(ad)} \eta(x, ad) \qquad (v \geqq 1).$$

For $0 \leqq \tau \leqq \rho$, $(a, P(\rho)) = 1$ one finds easily

$$r_\tau(x, a, v) + \sum_{\tau < j \leq \rho} r_{j-1}\left(x, ap_j, \frac{v}{p_j}\right) \leqq r_\rho(x, a, v).$$

After some calculations one arrives at (see also [7, (4.18)]):

For $x \geqq 2$, $M = M(x)$, $\rho > 0$, $(a, P(\rho)) = 1$, $p_\rho \leqq t^2$, $y^* := \operatorname{li} x/f(a)$ we have

$$A(M_a, \rho) \leqq \Lambda\left(\frac{\log t^2}{\log p_\rho}\right) + O\left(\frac{r_\rho(x, a, t^2)}{y^* R(\rho)}\right) + O((\log\log 3t)^{-7}),$$
$$\geqq \lambda\left(\frac{\log t^2}{\log p_\rho}\right) - O\left(\frac{r_\rho(x, a, t^2)}{y^* R(\rho)}\right) - O((\log\log 3t)^{-7}).$$

Following Kuhn, define

$$C(x; \rho, \sigma) := \left| \left\{ p^2 - 2 : 2 \leqq p \leqq x \wedge (1 \leqq j \leqq \rho \Rightarrow p_j \nmid (p^2 - 2)) \right.\right.$$
$$\left.\left. \wedge (\rho < j \leqq \sigma \Rightarrow p_j^2 \nmid (p^2 - 2)) \wedge \sum_{p_j \mid (p^2-2);\, \rho < j \leqq \sigma} 1 \leqq 1 \right\} \right|$$

for $x \geqq 2$, $1 \leqq \rho < \sigma$. For $u := \log t^2/\log p_\sigma$, $v := \log t^2/\log p_\rho > 9^{-2}$, $u^{-1} + v^{-1} \leqq 1$ we get

$$\frac{C(x; \rho, \sigma)}{\operatorname{li} xR(\rho)} \geqq \lambda(v) - \frac{1}{2}\int_u^v \Lambda(v(1 - t^{-1}))t^{-1}dt - O\left(\frac{r_\sigma(x, 1, t^2)}{\operatorname{li} xR(\rho)}\right)$$
$$- O((\log\log 3t)^{-7}).$$

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

$$r_\sigma(x, 1, t^2) = O(x(\log x)^{-3}),$$

according to [2]. We choose z, ξ, p_ρ, p_σ by virtue of

$$\log z := \frac{1}{6}\log x^{1/2}, \quad \log \xi := \frac{17}{21}\log x^{1/2},$$
$$p_\rho \leqq z < p_{\rho+1}, \quad p_\sigma \leqq \xi < p_{\sigma+1},$$

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*

$$C(x) > cx(\log x)^{-2} \qquad (x \geqq 2).$$

For any p, counted in $C(x)$, the number p^2-2 has
(i) *no prime factors* $\leqq x^{1/12}$,
(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* $V(p^2-2)\leqq 5$.

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

1. N. C. Ankeny and H. Onishi, *The general sieve*, Acta Arith. **10** (1964), 31–62.
2. E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225.
3. A. A. Buchstab, *A combinatorital strengthening of the Eratosthenes sieve method*, Russian Math. Surveys **22** (1967), 205–233.
4. W. B. Jurkat and H.-E. Richert, *An improvement of Selberg's sieve method*. I, Acta Arith. **11** (1965), 217–240.
5. B. V. Levin, *A one-dimensional sieve*, Acta Arith. **10** (1965), 387–397.
6. R. J. Miech, *Primes, polynomials, and almost primes*, Acta Arith. **11** (1965), 35–56.
7. W. Schaal, *Obere und untere Abschaetzungen in algebraischen Zahlkoerpern mit Hilfe des linearen Selbergschen Siebes*, Acta Arith. **13** (1968), 267–313.

State University of New York at Buffalo, Buffalo, New York 14214