PACIFIC JOURNAL OF MATHEMATICS
Vol. 97, No. 1, 1981

CONSECUTIVE INTEGERS FOR WHICH $n^2 + 1$ IS COMPOSITE

BETTY GARRISON

Let $\mathscr{P} = \{p_k\}_{k=0}^{\infty}$ where $p_0 = 2$ and p_k, $k > 0$, is the kth prime in the sequence of positive integers congruent to 1 modulo 4. Thus $\mathscr{P}$ contains the prime divisors of all the integers n^2+1. For each $t=0, 1, \cdots$ let $P(t)=\prod_{k=0}^{t} p_k$. It will be shown that for each sufficiently large integer t there exists a sequence $\mathscr{C}_t$ of consecutive integers n such that (i) $(n^2 + 1, P(t)) > 1$ **for all n in $\mathscr{C}_t$,** (ii) **card** $\mathscr{C}_t \geqq [(1 - \varepsilon)\lambda p_t]$, $0 < \varepsilon < 1$, **for a certain positive constant λ, and** (iii) $p_t < n < P(t)$ **for all n in $\mathscr{C}_t$.**

Viggo Brun [1] has shown that $\lim_{x\to\infty} U(x)/N(x) = 0$, where $U(x)$ is the number of primes $\leqq x$ of the form $n^2 + 1$ and $N(x)$ is the total number of integers $\leqq x$ of that form. Hence there exist arbitrarily long sequences of consecutive integers n for which $n^2 + 1$ is composite. Somewhat later Chang [2] proved a theorem which implies that if $C(t)$ is the maximum length of a sequence of consecutive integers each divisible by at least one of the first t primes $q_1, \cdots, q_t$, then $C(t) \geqq cq_t \log q_t/(\log\log q_t)^2$ for all sufficiently large t. Rankin [9] has improved Chang's result to $C(t) \geqq e^{\gamma-\varepsilon} t \log^2 t \log\log\log t/(\log\log t)^2$, while Iwaniec [6] has shown $C(t) \ll (t \log t)^2$. Obtaining estimates for $C(t)$ is a part of a problem posed by Jacobsthal [7], and the principal result of the present paper might be regarded as a generalization of that problem, also. The methods of proof here more akin to those of Chang and Erdös [3] than to those of Brun or Rankin.

In what follows the notation p_k, p_t, etc. will always indicate elements of sequence $\mathscr{P}$ defined above. For each odd prime p_k in $\mathscr{P}$ there exist integers $\pm a_k$ representing the two residue classes modulo p_k whose elements n have the property that p_k divides $n^2 + 1$. For each $t = 1, 2, \cdots$ let $\mathscr{S}_t$ denote the system $x \not\equiv 1 \pmod 2$ and $x \not\equiv \pm a_k \pmod{p_k}$ for all $k = 1, \cdots, t$. Clearly $n^2 + 1$ is relatively prime to $P(t)$ if and only if n satisfies $\mathscr{S}_t$. By the Chinese Remainder Theorem, any complete residue system modulo $P(t)$ contains $Q(t) = \prod_{k=1}^{t} (p_k - 2)$ solutions of $\mathscr{S}_t$. If the integers in a complete residue system modulo $P(t)$ are consecutive, then $P(t)/Q(t)$ represents an average distance between consecutive solutions of $\mathscr{S}_t$ in that system.

The following Lemma will serve to define the previously mentioned constant λ as well as to yield an asymptotic equality needed later. The first part of the proof is a variation of one given by Hardy and Wright [5, p. 349] and Halberstam and Roth [4, p.

277] for $\prod_{p \leqq x} p/(p-1)$.

LEMMA. *There exists a constant* λ *such that* $0.648 < \lambda < 0.649$ *and* $\prod_{k=1}^{t} p_k/(p_k - 2) \sim \lambda \log p_t$ *as* $t \to \infty$.

Proof. For each odd prime p in $\mathscr{P}$ let $s(p) = -\log(1 - 2/p) - 2/p = 2^2/2p^2 + 2^3/3p^3 + 2^4/4p^4 + \cdots$. Then $2/p^2 < s(p) < (2^2/p^2 + 2^3/p^3 + 2^4/p^4 + \cdots)/2 = 2/p(p-2)$. Each $s(p)$ is postive and $\sum 2/p(p-2)$ converges. Therefore, $\sum_{k=1}^{\infty} s(p) = b > 0$ and $\sum_{k=1}^{t} s(p_k) = b - \varepsilon(t)$ where $\lim_{t \to \infty} \varepsilon(t) = 0$. Hence we have

$$\sum_{k=1}^{t} \log p_k/(p_k - 2) = \sum_{k=1}^{t} 2/p_k + b - \varepsilon(t) .$$

Mertens [8, pp. 56–58] has shown that

$$\sum_{\substack{p \equiv 1 \pmod 4, \\ p \leqq G}} \frac{1}{p} = \frac{1}{2} \log \log G + a + f(G) ,$$

where $a = -0.2867420562 \cdots$ and $f(G) = O(1/\log G)$. Hence

$$\prod_{k=1}^{t} p_k/(p_k - 2) = \exp(2a + b - \varepsilon(t) + O(1/\log p_t)) \log p_t ,$$

and, letting $\lambda = e^{2a+b}$, $\prod_{k=1}^{t} p_k/(p_k - 2) \sim \lambda \log p_t$.

We next obtain upper and lower bounds for b. One easily proves $p_k > p_k - 2 > 6k$ for all $k > 3$. (Note $p_{k+2} - p_k \geqq 12$ while $6(k+2) - 6k = 12$.) Therefore, $b = \sum_{k=1}^{100} s(p_k) + \varepsilon(100) < 0.140595 + \sum_{k=101}^{\infty} 2/p_k(p_k - 2) < 0.140595 + \sum_{k=101}^{\infty} 2/36k^2 = 0.140595 + (\pi^2/6 - \sum_{k=1}^{100} 1/k^2)/18 < 0.14115$. Also, $b > \sum_{k=1}^{100} s(p_k) > 0.14059$.

Thus we have $-0.57349 + 0.14059 < 2a + b < -0.57348 + 0.14115$, so $0.648 < \lambda < 0.649$. $\square$

We use the notation $\pi(x; 4, 1)$ in the usual way to denote the number of primes $p \leqq x$ such that $p \equiv 1 \pmod 4$, and recall that the prime number theorem for primes in arithmetic progression gives $\pi(x; 4, 1) \sim x/(2 \log x)$. The Lemma implies $P(t)/Q(t) \sim 2\lambda \log p_t$ as $t \to \infty$. Here and in the statement of the following Theorem the constant λ is the same as in the Lemma, and the notation $[r]$ indicates the greatest integer $\leqq r$.

THEOREM. *Let* ε *be a fixed real number,* $0 < \varepsilon < 1$. *Then for each sufficiently large* p_t *in* $\mathscr{P}$ *there exists an integer* X *such that* $X + h$ *is not a solution of* $\mathscr{S}_t$ *for* $h = 1, 2, \cdots, [(1 - \varepsilon)\lambda p_t]$, *and* $p_t \leqq X \leqq P(t) - p_t$.

Proof. For the ε of the statement of the Theorem, choose δ so that $\delta \leqq (1-(1-\varepsilon)^{1/2})/2$ and $0 < \delta < 3/14$. Now choose a prime p_t in $\mathscr{P}$ large enough so that (i) $(1-2\delta/3)x/2\log x < \pi(x; 4, 1) < (1+2\delta/3)x/2\log x$ for all $x > \delta p_t$, (ii) $(1-2\delta/3)2\lambda \log p_s < P(s)/Q(s) < (1+2\delta/3)2\lambda\log p_s$ for all $p_s > \delta p_t$, and (iii) $\log(\delta p_t) > (1-2\delta/3)\log p_t$. Let p_r be the smallest prime in $\mathscr{P}$ which is greater than δp_t. For any integer y let $N(y)$ be the number of solutions of $\mathscr{S}_r$ in the interval $(y, y+(1-\varepsilon)\lambda p_t]$.

We have $\sum_{y=1}^{P(r)} N(y) = [(1-\varepsilon)\lambda p_t]Q(r)$, since each of the $Q(r)$ solutions of $\mathscr{S}_r$ is counted in exactly $[(1-\varepsilon)\lambda p_t]$ terms on the left. Hence there exists an integer x such that $1 \leqq x \leqq P(r)$ and

$$\begin{aligned} N(x) &\leqq (1-\varepsilon)\lambda p_t \frac{Q(r)}{P(r)} \\ &< \frac{(1-2\delta)^2\lambda p_t}{(1-2\delta/3)2\lambda\log p_r} \\ &< (1-2\delta)\frac{p_t}{2\log p_t} . \end{aligned}$$

Also, the number of primes in $\mathscr{P}$ between p_r and p_t is

$$\begin{aligned} &\pi(p_t; 4, 1) - \pi(p_r; 4, 1) \\ &\quad > (1-2\delta/3)\frac{p_t}{2\log p_t} - (1+2\delta/3)\frac{\delta p_t}{2\log \delta p_t} \\ &\quad > (1-2\delta/3)\frac{p_t}{2\log p_t} - \frac{(1+2\delta/3)\delta p_t}{(1-2\delta/3)2\log p_t} \\ &\quad > (1-2\delta)\frac{p_t}{2\log p_t} \\ &\quad > N(x) . \end{aligned}$$

Let $x+h_1,\ x+h_2, \cdots,\ x+h_{N(x)}$ be the solutions of $\mathscr{S}_r$ in $(x, x+(1-\varepsilon)\lambda p_t]$. There exists X in the interval $[1, P(t)]$ such that $X \equiv x \pmod{P(r)}$, $X \equiv a_k - h_{k-r} \pmod{p_k}$ for $k = r+1, \cdots, r+N(x)$, and $X \equiv 0 \pmod{p_k}$ for $k = r+N(x)+1, \cdots, t$. This X satisfies the conditions of the Theorem except for the possibility that $X = P(t)$. If so, then we use the integer X' such that $X' \equiv X \equiv 0 \pmod{P(t-1)}$, $X' \equiv 1 \pmod{p_t}$, $P(t-1) \leqq X' \leqq P(t)$. □

References

1. V. Brun, *Om fordelingen av primtallene i forskjellige talklasser*, Nyt Tidsskrift for Matematik (B), **27** (1916), 45-58.

2. T.-H. Chang, *Über aufeinanderfolgende Zahlen, von dener jede mindestens einer von n linearen Kongruenzen genügt, deren Moduln die ersten n Primzahlen sind*, Schr. Math. Semin. u. Inst. angew. Math. Univ. Berlin, **4** (1938), 35-55.

3. P. Erdös, *Problems and results on the differences of consecutive primes*, Publ. Math.

Debrecen, **1** (1949), 33-37.
4. H. Halberstam and F. K. Roth, *Sequences*, Volume 1, Oxford Univ. Press, London, 1966.
5. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th Edition, Oxford Univ. Press, London, 1962.
6. H. Iwaniec, *On the error term in the linear sieve*, Acta Arith., **19** (1971), 1-30.
7. E. Jacobsthal, *Über Sequenzen ganzer Zahlen von denen keine zu n teilerfremd ist, I-III*, Norske Vidensk. Selsk. Forh. Trondheim, **33** (1960), 117-139.
8. F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. reine u. angew. Math., **78** (1874), 46-62.
9. R. A. Rankin, *The difference between consecutive prime numbers V*, Proc. Edinburgh Math. Soc., **13** (1962-1963), 331-332.

Received March 25, 1980 and in revised form March 27, 1981.

SAN DIEGO STATE UNIVERSITY
SAN DIEGO, CA 92182