1980 II 13

The University of Calgary
2920 24 AVE. N.W.
CALGARY, CANADA
T2N 1N4

FACULTY OF SCIENCE
Department of Mathematics & Statistics
Area Code 403, Telephone 284-5202

Dear Carl,

Many thanks for your letter and the papers. Tomorrow I go to Memphis for a few days. Yesterday we made a very nice excursion into the Rockies, we walked for about 4 hours about 2000 feet altitude difference - despite my enormous age I still can walk fast + well uphill.

Can you prove that there are inf. many composite numbers n for which $2^{n-1} \equiv 3^{n-1} \equiv 1 \pmod{n}$? This should be easier than Carmichael numbers, but as far as I know it has not yet been done.

Your paper on the pseudoprimes is very nice.

Can you prove $\frac{\theta(x)}{C(x)} \to \infty$? or at least $\theta(x) - C(x) \to \infty$ i.e. there are inf many pseudoprimes which are not Carmichael numbers - this may be trivial, but perhaps $\theta(x) > (1+\varepsilon) C(x)$ will not be quite easy.

I am not sure if I wrote you the following annoying thing: I thought that I proved that for every $\varepsilon > 0$ $k > 0$

$$\sum_n \frac{1}{n^{1-\varepsilon} \ell_2(n)^k} = \infty$$

$\ell_2(n)$ is the exponent of $n \pmod 2$ - n for 2. But when asked I could not reconstruct the

proof - I wonder if I had a proof - I proved Chinese J. Math 1972 that if $f(n)$ is increasing then and $\sum_n \frac{1}{n f(n)} < \infty$ then also $\sum \frac{1}{n f(k_2(n))} < \infty$, but this does not help at all. Do you think that the number of pseudoprimes with respect to 2 and 3 are asymptotically equal.

I just thought of the following problem: choose a residue $u_p \bmod p$ at random (assume if necessary $\frac{p}{2} < u_p < p$. Let $q_1 < q_2 < \dots$ be the sequence of integers $q_i \equiv u_p \pmod p$ for every p. Is it true that almost surely $q_{i+1} - q_i < \dots$ then $\frac{q_{i+1} - q_i}{(\log q_i)^2} = 1$? The similar question can be asked for perhaps almost surely $q_{i+1} - q_i = o(\log q_i)$ or perhaps even

$$\max (q_{i+1} - q_i) = (1+o(1)) \frac{\pi^2}{12} \frac{\log q_i}{\log\log q_i}$$

if $q_i \not\equiv u_p \pmod{p^2}$ then

your results on amicable numbers are also very interesting. I tried to improve our bounds with Rieger, but was never successful. and your old bound

Can you prove that for inf many n there are "many" integer $n, n+1, \dots, n+f(n)$ so that the numbers $q(n+i)$, $0 \le i \le f(n)$ are all distinct $f(n)$ should be $> n^\varepsilon$ but I could not even prove that for every k, $\sum \frac{1}{f(n) (\log n)^k} = \infty$.

X 14. I am now on the plane to Chicago and Memphis. Unless I made a mistake $\overline{\lim}\ (q_{i+1}-q_i)/\log q_i = 1$ almost surely is indeed true and is not hard to prove – for the analog of squarefree numbers $\lim (q_{i+1}-q_i)/\log q_i = C$ holds almost surely.

It seems to me that our conjectures on p. 9 of our paper on $F_\varepsilon(n)$ are not hard to prove. The reason for $c_\varepsilon = d_\varepsilon$ is that you can obtain $F_\varepsilon(n)$ by an easy limiting process, define $F_\varepsilon^{(t)}(n)$ by permitting in $\sum_{d_i}$ only the values of d_i which are $\le t$ (i.e. $1 < d_i \le t$). It is easy to see that $\lim_{n\to\infty} F_\varepsilon^{(t)}(n)/n = C_\varepsilon^{(t)}$ exists and $\lim_{t\to\infty} C_\varepsilon^{(t)} = c_\varepsilon = d_\varepsilon$ q.e.d. – is this O.K. The monotonicity of c_ε will presumably also be easy.

I mail this letter tomorrow in Memphis and will phone before I leave the country next week. I return to the U.S. for the meeting in Tucson and plan to visit Athens either before or after my stay in Florida.

Let p_n be the smallest prime $\equiv 1 \pmod n$. m_n the smallest integer with $\varphi(m_n) \equiv 0 \pmod n$. $m_n/p_n \to 0$ for almost all n is perhaps true. Is it true that the number of $n < x$ for which $p_n < x$ is $(C+o(1))\frac{x}{\log x}$? It is between $\frac{1}{4}\frac{x}{\log x}$

and $\sim x/\log x$. Denote by $f(p)$ the number of integers m for which $p_m = p$, $f(p) \geq 1$ but presumably $f(p) = 1$ inf often in fact probably for $\sim x/\log x$ primes and ~~$f(p)$~~ $\overline{\lim} f(p) = \infty$. In $f(p) < (\log p)^{c_2}$.

Kind regards to you and your family and colleagues, au revoir

E. P.

$F(m)$ is the number of integers n for which $\varphi(n) \equiv 0 \pmod m$ and n is minimal. Perhaps it would be of some interest to estimate $F(m)$ from above as well as possible.

Put $\sum_{f_2(n)=d} p^{-c} = A(d)$. You would like to improve your estimate for $A(d)$ or at least you would like to improve $\sum_{d=1}^{x} A(d)$. Am I right in assuming that you would like to gain a factor $x^{-\varepsilon}$? Consider the primes $p < x^2$ for which $f_2(p) < x$. Can you prove that the number of these primes is $o(x^{2-\varepsilon})$? This I think would give the gain of $x^{-\varepsilon}$.

THE UNIVERSITY OF GEORGIA
DEPARTMENT OF MATHEMATICS
ATHENS, GEORGIA 30602

Oct. 31, 1980

Dear Paul,

Here is the paper I promised you.

There is some news about the prime testing algorithm. Andrew Odlyzko has been able to improve the Brudno theorem. He uses some recent analytic stuff on Linnik's theorem. (He used the same tools in his joint paper with you on $\frac{p-1}{2^n}$.) So he can prove that there is a square-free $m \le x$ such that the number of divisors d of the form $p-1$ is $\ge e^{c_1 \log x / \log\log x}$. This gives the running time for the algorithm $\le (\log n)^{c_1 \log\log\log n}$. This result is best possible for *this* algorithm except for the constant. Andrew's new proof doesn't yield any new information about the size of the divisors d which are $p-1$ (I don't think).

Yesterday I received from J. S. Pym, editor of the Journal of the London Math. Soc., a copy of our paper with Canfield and a note: "You should have received a letter from me about this paper." I don't have it, maybe I will today. I would guess he

is rejecting the paper, for otherwise why would he send us back a copy? Where should we send this long paper next?

Kind regards,

Carl

1980 XI 17

MAGYAR TUDOMÁNYOS AKADÉMIA
MATEMATIKAI KUTATÓ INTÉZETE
1053. BUDAPEST V., REÁLTANODA U. 13-15
TELEFON: 182 875

MATHEMATICAL INSTITUTE OF THE
HUNGARIAN ACADEMY OF SCIENCES
1053. BUDAPEST V., REÁLTANODA U. 13-15
TELEGRAPHIC ADDRESS: MATEMATIKA, BUDAPEST

Dear Carl,

Many thanks for your letter + nice proof of the upper bound for amicable numbers. Put $\sigma_1(n) = \sigma(n) - n$. Consider the integers for which $\sigma_k(n) = n$. Can you get a good estimation for the number of these integers $n < x$. I think this can be done for fixed k but it may be difficult to prove that the ~~natural~~ density of integers n for which $\sum_k \sigma_k(n) = n$ for some k is 0.

I am surprised that we have difficulty with our Ramanujan paper since I think it really is both good and interesting. It is possible that their objection only was that it is too long for the Journal - if this is the case we could send it to the Proc. London Math. Soc. if they have other objections the Journal of number theory or Acta Hungarica seem o.k.

By the way yesterday I saw the 'grapes of wrath' in the Hungarian T.V. I saw the movie 40 years ago in the U.S. and really made an enormous progress during these 40-45 years.

Let $\frac{1}{1} < a_1 < \dots < a_k = x$, $k > cx$. Is it then true that

there is a $y < x^{1+\varepsilon}$ for which y has more than $(\log x)^{\frac{1}{4}\log\log x}$ divisors among the a_i. η depends on F and ε? This we try to prove with Sarkozy.

Kind regards to all, hope to see you in Tucson

E. P.

The result of Ellipse is nice though not unexpected. Denote by $d_{p-1}(n)$ the number of divisors of n amongst the $p-1$. Put $\max_{n \le x} d(n) = D(x)$, $\max_{n \le x} d_{p-1}(n) = D_{p-1}(x)$. Is it true that $D_{p-1}(x)/D(x) \to 0$ but $D_{p-1}(x)/D(x)^{1-\varepsilon} \to \infty$. Both must be true - the question really is can one prove them.