Some Unconventional Problems in Number Theory

A mélange of simply posed conjectures with frustratingly elusive solutions.

PAUL ERDÖS
Hungarian Academy of Sciences
University of Colorado
Boulder, CO 80309

I state some curious, unusual, and mostly unsolved problems in various branches of number theory.

Factorial Powers

1. Put $f(n)=\Sigma(1/p)$ for $p<n$ and $p\mid\binom{2n}{n}$. In a previous paper [6] written with Graham, Ruzsa and Straus, we conjectured that there is an absolute constant C so that for all $n, f(n)<C$. I further conjectured for $n>4$, $\binom{2n}{n}$ is never squarefree. It is surprising that this simple conjecture presents so many difficulties.

Since $\binom{2n}{n}\equiv 0 \pmod 4$ except if $n=2^k$, we "only" have to prove that $\binom{2^{k+1}}{2^k}$ is divisible by the square of an odd prime for $k\geqslant 3$. But this does not seem easy. I conjecture that for $k>8$, 2^k is not the sum of distinct powers of 3. (However, $2^8=256=3^5+3^2+3+1$.) This conjecture would imply that for $k\geqslant 9$ $\binom{2^{k+1}}{2^k}\equiv 0 \pmod 3$, but as far as I see there is no method at our disposal to attack this conjecture. There is no doubt that for $n>n_0(k,\alpha)$, $\binom{2n}{n}\equiv 0 \pmod{p^\alpha}$ for some $p>k$. For $p>2, p^2\mid\binom{342}{171}$ and there is a good chance that this is the greatest $\binom{2n}{n}$ with this property. In other words, for $n>171$, the number $\binom{2n}{n}$ is perhaps divisible by the square of an odd prime.

2. Let $M(n;k)=[n+1,\ldots,n+k]$ be the least common multiple of the integers $n+i$ for $1\leqslant i\leqslant k$. I conjecture that for $m\geqslant n+k, M(n;k)\neq M(m;k)$, or more generally for $l\geqslant k$ and $m\geqslant n+k, M(n;k)\neq M(m;l)$. Unfortunately, I do not see any method to attack these very attractive conjectures. Probably $M(n;k)=M(m;l)$ has very few solutions when $m\geqslant n+k$ and $l>1$. I only know $M(4;3)=M(13;2)$ and $M(3;4)=M(19;2)$. If, similarly, we put $A(n;k)=\Pi_{i=1}^{k}(n+i)$, then I conjecture also that $A(n;k)=A(m;l)$ probably has very few solutions for $m\geqslant n+k$ and $l>1$.

Suppose that $k\geqslant 3$ and $m\geqslant n+k$. Observe that then, for each $k, M(n;k)>M(m;k)$ has infinitely many solutions. Yet I cannot decide whether the same is true for $M(n;k)>M(m;k+1)$. (The referee found two solutions, namely $M(96;7)>M(104;8)$ and $M(132;7)>M(139;8)$.) Let n_k denote the smallest solution of $M(n;k)>M(m;k)$. Try to determine or

estimate n_k. It is almost certainly the case that $n_k/k \to \infty$ and perhaps this will not be difficult to prove. It would be worthwhile to compute n_k for small values of k, for perhaps then one can formulate some reasonable conjectures. (Added in proof: $n_k/k \to \infty$ is indeed easy, but I have no good upper bound for n_k.)

Let u_k be the smallest integer for which $M(u_k,k) > M(u_k+1;k)$. It is easy to see that $u_k = (1+o(1))k$ and $u_k > k$. It seems to me that if $t < u_k$ and $T > t$ then $M(t;k) < M(T;k)$. Perhaps I overlooked a simple argument but I could not prove this.

Unusual Sieve Processes

3. Consider the integers of the form

$$n = ap^2 + b, \text{ where } a \geq 1, 0 < b < p, \text{ and } p \text{ is prime.} \tag{1}$$

It is easy to see by the sieve of Eratosthenes that almost all integers n are of the form (1), but I could not prove that every sufficiently large integer is of this form. In fact, this seems rather unlikely. In view of this I hoped that perhaps the equation

$$n = ak^2 + b, \text{ where } a \geq 1, 0 < b < k, k \text{ is an integer, } k > 2 \tag{2}$$

would be solvable for every sufficiently large n. Selfridge and Wagstaff made a preliminary computer search and in their opinion it is quite possible that (2) is not solvable for infinitely many n. It would be interesting to find some large (say of size 10^{13} or larger) values of n not of the form (2). Denote by $g(x)$ the number of integers $n < x$ not of the form (1), and by $G(x)$ those not of the form (2). Clearly $G(x) \leq g(x)$. It follows from the Brun-Selberg Sieve that $g(x) < c_1 x(\log x)^{-c_2}$. Probably $G(x) < x^c$ for $x > x_0(c)$ for some $c > 0$, and perhaps for all $c > 0$.

Let $u_1 < u_2, \ldots,$ be an infinite sequence of integers. It is probably not difficult to prove that the density of integers not of the form $n = au_i^2 + b$ for $a \geq 1$ and $0 < b < u_i$ exists and is positive if $\Sigma 1/u_i$ converges and is 0 otherwise. More generally (1) could be replaced by the equation

$$n = au_i^2 + b, \text{ where } a \geq 1 \text{ and } 0 < b < v_i \tag{3}$$

and one could try to find non-trivial conditions on $u_1 < u_2 < \cdots$ and $v_1 < v_2 < \cdots$ that (3) should be solvable for all sufficiently large n. I am not very hopeful of success. There is more hope if we only insist that almost all n should be of the form (3).

Barriers

4. Let $f(m) \geq 0$ for $1 \leq m < \infty$ be any positive function defined on the integers. Then n is called a **barrier** for $f(m)$ if for all $m < n$, $m + f(m) \leq n$. Clearly $\phi(m)$ and $\sigma(m)$ do not have barriers because they increase too fast. Let $V(m)$ be the number of distinct prime factors of m. Probably $V(m)$ has infinitely many barriers, but I am very far from being able to prove this. I cannot even prove that there is an $\epsilon > 0$ for which $\epsilon V(m)$ has infinitely many barriers. One could try to attack this problem by sieve methods, but it seems to me that these methods are not strong enough at present.

Let $\Omega(m)$ be the number of prime factors of m, multiple factors counted multiply. It seems certain that $\Omega(m)$ also has infinitely many barriers. But this, if true, is certainly unattackable by present day methods. Selfridge observed that $n = 99840$ is the largest barrier for $\Omega(m)$ less than 10^5. Selfridge and I then investigated $d(n)$, the number of divisors of n. Since $\max(d(n-1)+n-1, d(n-2)+n-2) \geq n+2$, the most we can hope here is that for infinitely many n,

$$\max_{m<n} (m + d(m)) = n + 2. \tag{4}$$

It is extremely doubtful whether (4) has infinitely many solutions. In fact it is quite possible that $\lim_{n\to\infty} \max_{m<n} (m + d(m) - n) = \infty$. Selfridge and I observed that 24 satisfies (4) and we convinced ourselves that if there is an $n > 24$ which satisfies (4), then this n must be enormously large, far beyond the range of our tables or computers.

It is not difficult to show that the product $F(m) = \Pi \alpha_i$ (where $m = \Pi p_i^{\alpha_i}$) of the number of prime factors of m has infinitely many barriers.

Translation Properties

5. Denote by A the sequence $1 \leqslant a_1 < a_2 < \cdots$. A is said to have the **translation property** if for every n there is a $t_n > 0$ so that u is in A if, and only if, $u + t_n$ is in A for every $1 \leqslant u \leqslant n$. It is not hard to show that the squarefree numbers have the translation property. (This must have been known, although perhaps it does not appear in this form in the literature.) More generally let $b_1 < b_2 < \cdots 1$ where $(b_i, b_j) = 1$ and $\Sigma 1/b_i < \infty$, and let A be the sequence of integers not divisible by any of the b's. It follows easily from the sieve of Eratosthenes that A has the translation property.

If the condition $\Sigma 1/b_i < \infty$ is dropped, the situation is much more complicated. If $\Sigma_{b_i < x}(1/b_i) = o(\log\log x)$, then it can be deduced by Brun's method that A has the translation property. If this condition is also dropped, I have no non-trivial result. I do not know if the integers which are sums of two squares have the translation property. I do not know what happens if we divide the primes into two disjoint classes $q_1 < q_2 < \cdots$; and $r_1 < r_2 < \cdots$, both having for every x more than $cx/\log x$ terms not exceeding x. Denote by $Q_1 < Q_2 < \cdots$ the integers composed of the primes $q_1 < q_2 < \cdots$. Can the sequence $Q_1 < Q_2 < \cdots$ have the translation property? Let $p_1 < p_2 < \cdots$ be the sequence of all primes. It is not hard to show that $p_k < p_{k+1} < \cdots$ can never have the translation property.

Let A have the translation property. The task of determining the smallest t_n which satisfies the definition of the translation property for A will not be easy. For example, if A is the sequence of squarefree numbers, I expect that $t_n > \exp n^c$. I am quite sure that t_n increases faster than polynomially; perhaps this will not be hard to prove.

6. It is extremely difficult to obtain results on the difference of consecutive primes. A well-known conjecture of Cramer states that

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log n)^2} = 1.$$

This conjecture is completely unattackable by present day methods and I expect that it will stay in this class for a very long time.

Let $Q_1 < Q_2 < \cdots$ be the sequence of consecutive squarefree numbers. It is curious that $Q_{n+1} - Q_n$ is almost as difficult to study as $p_{n+1} - p_n$. The best upper bound is, as far as I know, still due to Richert and Rankin [**10, 11**] who proved that for every $\varepsilon > 0$ and $n > n_0$, $Q_{n+1} - Q_n < n^{2/9+\varepsilon}$. There is no doubt that this inequality holds with $2/9 + \varepsilon$, replaced by ε, but the proof is nowhere in sight. Perhaps $Q_{n+1} - Q_n < c\log n$ holds, but I am very doubtful. It is easy to see that

$$\limsup_{n\to\infty} (Q_{n+1} - Q_n)\log\log n(\log n)^{-1} > \pi^2/6$$

and as far as I know this has never been improved.

I proved (in [**5**]) that for $0 \leqslant \alpha \leqslant 2$,

$$\lim_{x\to\infty} \frac{1}{x} \sum_{Q_n < x} (Q_{n+1} - Q_n)^\alpha = c_\alpha \tag{5}$$

and Hooley recently proved [**8**] that (5) holds for $\alpha \leqslant 3$. No doubt (5) holds for every α.

Miscellaneous Problems

7. There are many unconventional problems connected with the divisors of n. R. R. Hall and I have a long paper on this subject. Here I just state a conjecture of mine which is more than forty years old: The density of integers n which have two divisors $d_1 < d_2 < (1+\varepsilon)d_1$ is 1 for every $\varepsilon > 0$. I can prove that the density exists, but cannot prove that it is 1, even for large values of ε. A much stronger and more recently formulated conjecture is as follows: Denote by $d^+(n)$ the number of integers k for which n has at least one divisor t where $2^k < t < 2^{k+1}$. Then for almost all integers n, $d^+(n)/d(n) \to 0$ as $n \to \infty$.

8. Let $h(n)$ be the smallest integer so that every μ, where $1 \leq \mu < n!$, is the sum of $h(n)$ or fewer distinct divisors of $n!$. I proved $h(n) \leq n$. The proof by induction is easy. No doubt very much more is true: $h(n) = o(n)$ and probably $h(n) = o(n^\epsilon)$ and hopefully $h(n) < (\log n)^c$ for some c. (I was lead to $h(n)$ by studying $\frac{a}{b} = \frac{1}{x_1} + \cdots + \frac{1}{x_k}$ where $x_1 < \cdots < x_k$ and k is minimal.)

9. An old conjecture of Strauss and myself states that for every $n \geq 3$

$$\frac{4}{n} = \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3}$$

is solvable in integers x_1, x_2, x_3 where $1 \leq x_1 < x_2 < x_3$. This conjecture seems surprisingly difficult. A forthcoming paper of Strauss and Subbarao deals with some related questions.

10. Forty years ago I asked: does $x^y y^y = z^z$ have any nontrivial solutions in integers? Chao Ko found infinitely many solutions [1]; perhaps he found them all.

11. Put $p_{k+1} - p_k = d_k$ (where $\{p_k\}$ is the sequence of primes). Turan and I proved that both $d_{k+1} > d_k$ and $d_{k+1} < d_k$ have infinitely many solutions. But we could not prove that at least one of the inequalities $d_{k+2} > d_{k+1} > d_k$ and $d_{k+2} < d_{k+1} < d_k$ has infinitely many solutions. If our conjecture is false then, as we observed, there is a k_0 so that for $k > k_0, d_{k+1} - d_k$ alternates in sign. This is certainly not the case and perhaps the proof is not hard. I offer 100 dollars for a proof or disproof.

12. Let $1 = r_1 < \cdots < r_{\phi(n)} = n - 1$ be the $\phi(n)$ integers relatively prime to n. I conjectured nearly forty years ago that there is an absolute constant C so that

$$\sum_{i=1}^{\phi(n)-1} (r_{i+1} - r_i)^2 < C \frac{n^2}{\phi(n)}. \tag{6}$$

This does not look hard, but it has not yet been settled and I offer 250 dollars for a proof or disproof. No doubt (6) holds if 2 is replaced by any positive α (C must then be replaced by C_α). Hooley proved this for $\alpha < 2$.

This paper is based on remarks presented at the fifth annual Mathematics and Statistics Conference in October, 1977, at Miami University in Oxford, Ohio.

References

[1] Ko Chao, Note on the diophantine equation $x^y y^y = z^z$, J. Chinese Math. Soc., 2 (1940) 205–207 (Math. Rev. V. 2, p. 346).

[2] P. Erdös, On the density of some sequences of integers, Bull. Amer. Math. Soc., 54 (1948) 685–692.

[3] ———, On the difference of consecutive primes, Bull. Amer. Math Soc., 54 (1948) 885–889.

[4] ———, On the equation $\frac{1}{x_1} + \cdots + \frac{1}{x_k} = \frac{a}{b}$ (in Hungarian), Mat. Lapok, 1 (1950) 192–210. (MR 13, p. 208.)

[5] ———, Some problems and results in elementary number theory, Publ. Math. Debrecen, 2 (1951) 103–109. (MR 13, p. 627.)

[6] ———, R. L. Graham, I. Z. Ruzsa and E. Straus, On the prime factors of $\binom{2n}{n}$, Math. Comp., 29 (1975) 83–92.

[7] ———, and P. Turan, On some new questions on the distribution of prime numbers, Bull. Amer. Math. Soc., 54 (1948) 271–278.

[8] C. Hooley, On the intervals between consecutive terms of sequences, Proc. Symp. Pure Math. XXIV. Analytic Number Theory, Amer. Math. Soc., 1973, 129–140.

[9] W. H. Mills, Number theory conference, Boulder, Colorado, 1959.

[10] R. A. Rankin, Van der Corput's method and the theory of exponent pairs, Quart. J. Math., 6 (Ser. 2) (1955) 147–153.

[11] H. E. Richert, On the difference between consecutive squarefree numbers, J. London Math. Soc., 29 (1954) 16–20.