

Unsolved Problems in Intuitive Mathematics
Volume I

Richard K. Guy

Unsolved Problems in Number Theory



Unsolved Problems in Intuitive Mathematics
Volume I

Richard K. Guy

Unsolved Problems in Number Theory

With 17 Figures

Springer-Verlag
New York Heidelberg Berlin



Richard K. Guy
Department of Mathematics and Statistics
The University of Calgary
Canada T2N 1N4

AMS Classification (1980): 10-01

Library of Congress Cataloging in Publication Data

Guy, Richard K.

Unsolved problems in number theory.

(Unsolved problems in intuitive mathematics; v. 1)

(Problem books in mathematics)

Includes indexes.

1. Numbers, Theory of—Problems, exercises, etc.

I. Title. II. Series: Guy, Richard K. Unsolved problems in intuitive mathematics; v. 1. III. Series: Problem books in mathematics.

QA43.G88 vol. 1 [QA141]

510'.76s 81-14551
[512'.7'076] AACR2

© 1981 by Springer-Verlag New York Inc.

All rights reserved. No part of this book may be translated or reproduced in any form without written permission from Springer-Verlag, 175 Fifth Avenue, New York, New York 10010, U.S.A.

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90593-6 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90593-6 Springer-Verlag Berlin Heidelberg New York

Preface

To many laymen, mathematicians appear to be problem solvers, people who do "hard sums". Even inside the profession we classify ourselves as either theorists or problem solvers. Mathematics is kept alive, much more than by the activities of either class, by the appearance of a succession of unsolved problems, both from within mathematics itself and from the increasing number of disciplines where it is applied. Mathematics often owes more to those who ask questions than to those who answer them. The solution of a problem may stifle interest in the area around it. But "Fermat's Last Theorem", because it is not yet a theorem, has generated a great deal of "good" mathematics, whether goodness is judged by beauty, by depth or by applicability.

To pose good unsolved problems is a difficult art. The balance between triviality and hopeless unsolvability is delicate. There are many simply stated problems which experts tell us are unlikely to be solved in the next generation. But we have seen the Four Color Conjecture settled, even if we don't live long enough to learn the status of the Riemann and Goldbach hypotheses, of twin primes or Mersenne primes, or of odd perfect numbers. On the other hand, "unsolved" problems may not be unsolved at all, or may be much more tractable than was at first thought.

Among the many contributions made by Hungarian mathematician Erdős Pál, not least is the steady flow of well-posed problems. As if these were not incentive enough, he offers rewards for the first solution of many of them, at the same time giving his estimate of their difficulty. He has made many payments, from \$1.00 to \$1000.00.

One purpose of this book is to provide beginning researchers, and others who are more mature, but isolated from adequate mathematical stimulus, with a supply of easily understood, if not easily solved, problems which

they can consider in varying depth, and by making occasional partial progress, gradually acquire the interest, confidence and persistence that are essential to successful research.

But the book has a much wider purpose. It is important for students and teachers of mathematics at all levels to realize that although they are not yet capable of research and may have no hopes or ambitions in that direction, there are plenty of unsolved problems that are well within their comprehension, some of which will be solved in their lifetime. Many amateurs have been attracted to the subject and many successful researchers first gained their confidence by examining problems in euclidean geometry, in number theory, and more recently in combinatorics and graph theory, where it is possible to understand questions and even to formulate them and obtain original results without a deep prior theoretical knowledge.

The idea for the book goes back some twenty years, when I was impressed by the circulation of lists of problems by the late Leo Moser and co-author Hallard Croft, and by the articles of Erdős. Croft agreed to let me help him amplify his collection into a book, and Erdős has repeatedly encouraged and prodded us. After some time, the Number Theory chapter swelled into a volume of its own, part of a series which will contain a volume on Geometry, Convexity and Analysis, written by Hallard T. Croft, and one on Combinatorics, Graphs and Games by the present writer.

References, sometimes extensive bibliographies, are collected at the end of each problem or article surveying a group of problems, to save the reader from turning pages. In order not to lose the advantage of having all references collected in one alphabetical list, we give an Index of Authors, from which particular papers can easily be located provided the author is not too prolific. Entries in this index and in the General Index and Glossary of Symbols are to problem numbers instead of page numbers.

Many people have looked at parts of drafts, corresponded and made helpful comments. Some of these were personal friends who are no longer with us: Harold Davenport, Hans Heilbronn, Louis Mordell, Leo Moser, Theodor Motzkin, Alfred Rényi and Paul Turán. Others are H. L. Abbott, J. W. S. Cassels, J. H. Conway, P. Erdős, Martin Gardner, R. L. Graham, H. Halberstam, D. H. and Emma Lehmer, A. M. Odlyzko, Carl Pomerance, A. Schinzel, J. L. Selfridge, N. J. A. Sloane, E. G. Straus, H. P. F. Swinnerton-Dyer and Hugh Williams. A grant from the National (Science and Engineering) Research Council of Canada has facilitated contact with these and many others. The award of a Killam Resident Fellowship at The University of Calgary was especially helpful during the writing of a final draft. The technical typing was done by Karen McDermid, by Betty Teare and by Louise Guy, who also helped with proof-reading. The staff of Springer-Verlag in New York has been courteous, competent and helpful.

In spite of all this help, many errors remain, for which I assume reluctant responsibility. In any case, if the book is to serve its purpose it will start becoming out of date from the moment it appears; it has been becoming out

of date ever since its writing began. I would be glad to hear from readers. There must be many solutions and references and problems which I don't know about. I hope that people will avail themselves of this clearing house. A few good researchers thrive by rediscovering results for themselves, but many of us are disappointed when we find that our discoveries have been anticipated.

*Calgary 81:08:13

Richard K. Guy

Contents

Glossary of Symbols

xi

Introduction

1

Some general references. Notation.

A. Prime Numbers

3

A1. Prime values of quadratic functions. **4** **A2.** Primes connected with factorials. **6** **A3.** Mersenne primes. Repunits. Fermat numbers. Primes of the form $k \cdot 2^n + 1$. **7** **A4.** The prime number race. **9** **A5.** Arithmetic progressions of primes. **10** **A6.** Consecutive primes in A.P. **12** **A7.** Cunningham chains. **12** **A8.** Gaps between primes. Twin primes. **13** **A9.** Patterns of primes. **15** **A10.** Gilbreath's conjecture. **16** **A11.** Increasing and decreasing gaps. **17** **A12.** Pseudoprimes. Euler pseudoprimes. Strong pseudoprimes. **17** **A13.** Carmichael numbers. **18** **A14.** "Good" primes and the prime number graph. **19** **A15.** Congruent products of consecutive numbers. **19** **A16.** Gaussian primes. Eisenstein-Jacobi primes. **20** **A17.** A formula for the n th prime. **22** **A18.** The Erdos-Selfridge classification of primes. **29** **A19.** Values of n making $n - 2^k$ prime. Odd numbers not of the form $\pm p^a \pm 2^b$. **23**

B. Divisibility

25

B1. Perfect numbers. **25** **B2.** Almost perfect, quasi-perfect, pseudo-perfect, harmonic, weird, multiply perfect and hyperperfect numbers. **27** **B3.** Unitary perfect numbers. **30** **B4.** Amicable numbers. **31** **B5.** Quasi-amicable, or betrothed numbers. **33** **B6.** Aliquot sequences. **33** **B7.** Aliquot cycles. Sociable numbers. **34** **B8.** Unitary aliquot sequences. **35** **B9.** Superperfect numbers. **36** **B10.** Untouchable numbers. **37** **B11.** Solutions of $m\sigma(m) = n\sigma(n)$. **38** **B12.** Analogs with

$d(n)$, $\sigma_k(n)$. 38 **B13**. Solutions of $\sigma(n) = \sigma(n+1)$. 38 **B14**. An irrationality problem. 39 **B15**. Solutions of $\sigma(q) + \sigma(r) = \sigma(q+r)$. 39 **B16**. Powerful numbers. 40 **B17**. Exponential-perfect numbers. 40 **B18**. Solutions of $d(n) = d(n+1)$. 41 **B19**. $(m, n+1)$ and $(m+1, n)$ with same sets of prime factors. 42 **B20**. Cullen numbers. 42 **B21**. $k \cdot 2^n + 1$ composite for all n . 42 **B22**. Factorial n as the product of n large factors. 43 **B23**. Equal products of factorials. 44 **B24**. The largest set with no member dividing two others. 44 **B25**. Equal sums of geometric progressions with prime ratios. 45 **B26**. Densest set with no l pairwise coprime. 45 **B27**. The number of prime factors of $n+k$ which don't divide $n+i$, $0 \leq i < k$. 46 **B28**. Consecutive numbers with distinct prime factors. 46 **B29**. Is x determined by the prime divisors of $x+1$, $x+2, \dots, x+k$? 47 **B30**. A small set whose product is square. 47 **B31**. Binomial coefficients. 47 **B32**. Grimm's conjecture. 47 **B33**. Largest divisor of a binomial coefficient. 48 **B34**. If there's an i such that $n-i$ divides $\binom{n}{i}$. 50 **B35**. Products of consecutive numbers with the same prime factors. 50 **B36**. Euler's totient function. 50 **B37**. Does $\phi(n)$ properly divide $n-1$? 51 **B38**. Solutions of $\phi(m) = \sigma(n)$. 52 **B39**. Carmichael's conjecture. 53 **B40**. Gaps between totatives. 54 **B41**. Iterations of ϕ and σ . 54 **B42**. Behavior of $\phi(\sigma(n))$ and $\sigma(\phi(n))$. 55 **B43**. Alternating sums of factorials. 56 **B44**. Sums of factorials. 56 **B45**. Euler numbers. 56 **B46**. The largest prime factor of n . 57 **B47**. When does $2^a - 2^b$ divide $n^a - n^b$? 57 **B48**. Products taken over primes. 57

C. Additive Number Theory

58

C1. Goldbach's conjecture. 58 **C2**. Sums of consecutive primes. 59 **C3**. Lucky numbers. 59 **C4**. Ulam numbers. 60 **C5**. Sums determining members of a set. 61 **C6**. Addition chains. Brauer chains. Hansen chains. 62 **C7**. The money-changing problem. 63 **C8**. Sets with distinct sums of subsets. 64 **C9**. Packing sums of pairs. 65 **C10**. Modular difference sets and error correcting codes. 66 **C11**. Subsets of three with distinct sums. 68 **C12**. The postage stamp problem. 68 **C13**. The corresponding modular covering problem. Harmonious labelling of graphs. 71 **C14**. Maximal sum-free sets. 72 **C15**. Maximal zero-sum-free sets. 73 **C16**. Non-averaging sets. Non-dividing sets. 74 **C17**. The minimum overlap problem. 74 **C18**. The n queens problem. 75 **C19**. Is a weakly independent sequence the finite union of strongly independent ones? 77 **C20**. Sums of squares. 77

D. Some Diophantine Equations

79

D1. Sums of like powers. Euler's conjecture. 79 **D2**. The Fermat problem. 81 **D3**. Figurate numbers. 82 **D4**. Sums of l k th powers. 83 **D5**. Sum of 4 cubes. 84 **D6**. An elementary solution of $x^2 = 2y^4 - 1$. 84 **D7**. Sum of consecutive powers made a power. 85 **D8**. A pyramidal diophantine equation. 86 **D9**. Difference of two powers. 86 **D10**. Exponential diophantine equations. 87 **D11**. Egyptian fractions. 87

D12. Markoff numbers. 93 **D13.** The equation $x^x y^y = z^z$. 94
D14. $a_i + b_j$ made squares. 95 **D15.** Numbers whose sums in pairs make squares. 95 **D16.** Triples with the same sum and same product. 96
D17. Product of blocks of consecutive integers not a power. 97
D18. Is there a perfect cuboid? Four squares whose sums in pairs are square. Four squares whose differences are square. 97 **D19.** Rational distances from the corners of a square. 103 **D20.** Six general points at rational distances. 104 **D21.** Triangle with integer sides, medians and area. 105 **D22.** Simplexes with rational contents. 105 **D23.** The equation $(x^2 - 1)(y^2 - 1) = (z^2 - 1)^2$. 105 **D24.** Sum equals product. 105
D25. Equations involving factorial n . 105 **D26.** Fibonacci numbers of various shapes. 106 **D27.** Congruent numbers. 106 **D28.** A reciprocal diophantine equation. 109

E. Sequences of Integers 110

E1. A thin sequence with all numbers equal to a member plus a prime. 110
E2. Density of a sequence with l.c.m. of each pair less than x . 111
E3. Density of integers with two comparable divisors. 111 **E4.** Sequence with no member dividing the product of r others. 111 **E5.** Sequence with members divisible by at least one of a given set. 111 **E6.** Sequence with sums of pairs not members of a given sequence. 111 **E7.** A series and a sequence involving primes. 112 **E8.** Sequence with no sum of a pair a square. 112 **E9.** Partitioning the integers into classes with numerous sums of pairs. 112 **E10.** Theorem of van der Waerden. Partitioning the integers into classes; at least one contains an A.P. Szemerédi's theorem. 112
E11. Schur's problem. Partitioning integers into sum-free classes. 116
E12. The modular version of Schur's problem. 117 **E13.** Partitioning into strongly sum-free classes. 118 **E14.** Rado's generalizations of van der Waerden's and Schur's problems. 119 **E15.** A recursion of Lenstra. 120
E16. Collatz's sequence. 120 **E17.** Conway's permutation sequences. 121
E18. Mahler's Z-numbers. 122 **E19.** Are the integer parts of the powers of a fraction infinitely often prime? 122 **E20.** Davenport-Schinzel sequences. 122 **E21.** Thue sequences. 124 **E22.** Cycles and sequences containing all permutations as subsequences. 125 **E23.** Covering the integers with A.P.s. 126 **E24.** Irrationality sequences. 126 **E25.** Silverman's sequence. 126 **E26.** Epstein's Put-or-Take-a-Square game. 126
E27. Max and mex sequences. 127 **E28.** B_2 -sequences. 127
E29. Sequence with sums and products all in one of two classes. 128
E30. MacMahon's prime numbers of measurement. 129 **E31.** Three sequences of Hofstadter. 129 **E32.** B_2 -sequences formed by the greedy algorithm. 130 **E33.** Sequences containing no monotone A.P.s. 130

F. None of the Above

132

F1. Gauss's lattice point problem. 132 **F2.** Lattice points with distinct distances. 132 **F3.** Lattice points, no four on a circle. 133 **F4.** The no-three-in-line problem. 133 **F5.** Quadratic residues. Schur's conjecture. 135 **F6.** Patterns of quadratic residues. 136 **F7.** A cubic analog

of a Pell equation. 138 **F8.** Quadratic residues whose differences are quadratic residues. 138 **F9.** Primitive roots. 138 **F10.** Residues of powers of two. 139 **F11.** Distribution of residues of factorials. 139 **F12.** How often are a number and its inverse of opposite parity? 139 **F13.** Covering systems of congruences. 140 **F14.** Exact covering systems. 141 **F15.** A problem of R.L. Graham. 142 **F16.** Products of small prime powers dividing n . 142 **F17.** Series associated with the ζ -function. 142 **F18.** Size of the set of sums and products of a set. 143 **F19.** Partitions into distinct primes with maximum product. 143 **F20.** Continued fractions. 144 **F21.** All partial quotients one or two. 144 **F22.** Algebraic numbers with unbounded partial quotients. 144 **F23.** Small differences between powers of 2 and 3. 145 **F24.** Squares with just two different decimal digits. 146 **F25.** The persistence of a number. 146 **F26.** Expressing numbers using just ones. 146 **F27.** Mahler's generalization of Farey series. 147 **F28.** A determinant of value one. 148 **F29.** Two congruences, one of which is always soluble. 148 **F30.** A polynomial whose sums of pairs of values are all distinct. 148

Index of Authors Cited 149

General Index 157

Introduction

Number theory has fascinated both the amateur and the professional for a longer time than any other branch of mathematics; so that much of it is now of considerable technical difficulty. However, there are more unsolved problems than ever before, and though many of these are unlikely to be solved in the next generation, this probably won't deter people from trying. They are so numerous that they have already filled more than one volume so that the present book is just a personal sample.

Erdős recalls that Landau, at the International Congress in Cambridge in 1912, gave a talk about primes and mentioned four problems (see A1, A7, C1 below) which were unattackable in the present state of science, and says that in 1980 they still are.

Here are some good sources of problems in number theory.

- P. Erdős, Some unsolved problems, *Michigan Math. J.* **4** (1957) 291–300.
- P. Erdős, On unsolved problems, *Publ. Math. Inst. Hungar. Acad. Sci.* **6** (1961) 221–254.
- P. Erdős, *Quelques Problèmes de la Théorie des Nombres*, Monographies de l'Enseignement Math. #6, Geneva, 1963, 81–135.
- P. Erdős, Extremal problems in number theory, *Proc. Symp. Pure Math.* **8**, Amer. Math. Soc., Providence, 1965, 181–189.
- P. Erdős, Some recent advances and current problems in number theory, in *Lectures on Modern Mathematics* **3**, Wiley, New York, 1965, 196–244.
- P. Erdős, Résultats et problèmes en théorie des nombres, *Seminar Delange-Pisot-Poitou* **24**, 1972–73.
- P. Erdős, Problems and results in combinatorial number theory, in *A Survey of Combinatorial Theory*, North-Holland, 1973, 117–138.
- P. Erdős, *Problems and Results in Combinatorial Number Theory*, Bordeaux, 1974.
- Paul Erdős, Problems and results in combinatorial number theory III, *Springer Lecture Notes in Math.* **626** (1977) 43–72; MR **57** #12442.
- P. Erdős, Combinatorial problems in geometry and number theory, *Amer. Math. Soc. Proc. Sympos. Pure Math.* **34** (1979) 149–162.

- Paul Erdős, A survey of problems in combinatorial number theory, in *Combinatorial Mathematics, Optimal Designs and their Applications* (Proc. Symp. Colo. State Univ. 1978) Ann. Discrete Math. 6 (1980) 89–115.
- Paul Erdős, Problems and results in number theory and graph theory, *Congressus Numerantium XXVII* (Proc. 9th Manitoba Conf. Num. Math. Comput. 1979) Utilitas Math., Winnipeg, 1980, 3–21.
- P. Erdős and R. L. Graham, *Old and New Problems and Results in Combinatorial Number Theory*, Monographies de l'Enseignement Math. No. 28, Geneva, 1980.
- Pál Erdős and András Sárközy, Some solved and unsolved problems in combinatorial number theory, *Math. Slovaca*, 28 (1978) 407–421; MR 80i:10001.
- H. Fast and S. Świerczkowski, *The New Scottish Book*, Wrocław, 1946–1958.
- Heini Halberstam, Some unsolved problems in higher arithmetic, in Ronald Duncan and Miranda Weston-Smith (eds.) *The Encyclopaedia of Ignorance*, Pergamon, Oxford and New York, 1977, 191–203.
- Proceedings of Number Theory Conference*, Univ. of Colorado, Boulder, 1963.
- Report of Institute in the Theory of Numbers*, Univ. of Colorado, Boulder, 1959.
- Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, Chelsea, New York, 2nd ed. 1978; MR 80e:10003.
- W. Sierpiński, *A Selection of Problems in the Theory of Numbers*, Pergamon, 1964.
- S. Ulam, *A Collection of Mathematical Problems*, Interscience, New York, 1960.

Throughout this volume, “number” means natural number, c is an absolute positive constant, not necessarily the same each time it appears, and ε is an arbitrarily small positive constant. We use Donald Knuth’s “floor” ($\lfloor \rfloor$) and “ceiling” ($\lceil \rceil$) symbols for “the greatest integer not greater than” and “the least integer not less than.”

The notation $f(x) = O(g(x))$ and $f(x) \ll g(x)$ mean that there are constants c_1, c_2 such that $c_1 g(x) < f(x) < c_2 g(x)$ for all sufficiently large x ; while $f(x) \sim g(x)$ means that $f/g \rightarrow 1$, and $f(x) = o(g(x))$ means that $f/g \rightarrow 0$, as $x \rightarrow \infty$.

The book has been partitioned, somewhat arbitrarily at times, into six sections:

- A. Prime numbers
- B. Divisibility
- C. Additive number theory
- D. Diophantine equations
- E. Sequences of integers
- F. None of the above.

A. Prime Numbers

We can partition the positive integers into three classes:

- the unit, 1
- the primes, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...
- the composite numbers, 4, 6, 8, 9, 10, ...

A number greater than 1 is **prime** if its only positive divisors are 1 and itself; otherwise it's **composite**. Primes have interested mathematicians at least since Euclid, who showed that there were infinitely many.

Denote the n th prime by p_n , e.g., $p_1 = 2$, $p_2 = 3$, $p_{99} = 523$; and the number of primes not greater than x by $\pi(x)$, e.g., $\pi(2) = 1$, $\pi(3\frac{1}{2}) = 2$, $\pi(1000) = 168$. The greatest common divisor (g.c.d.) of m and n is denoted by (m, n) . If $(m, n) = 1$, we say that m and n are **coprime**; for example, $(14, 15) = 1$.

Dirichlet's theorem tells us that there are infinitely many primes in any arithmetic progression,

$$a, a + b, a + 2b, a + 3b, \dots$$

provided $(a, b) = 1$. An article, giving a survey of problems about primes and a number of further references, is

A. Schinzel and W. Sierpiński, Sur certains hypothèses concernant les nombres premiers, *Acta Arith.* 4 (1958) 185–208 (erratum 5 (1959) 259); *MR* 21 #4936.

Table 7 (D27) can be used as a table of primes < 1000 .

The general problem of determining whether a large number is prime or composite, and in the latter case of determining its factors, has fascinated number theorists down the ages. With the advent of high speed computers, considerable advances have been made, and a special stimulus has recently

been provided by the application to cryptanalysis. Some other references appear after Problem A3.

- Leonard Adleman and Frank Thomson Leighton, An $O(n^{1/10.89})$ primality testing algorithm, *Math. Comput.* **36** (1981) 261–266.
- Leonard M. Adleman, Carl Pomerance and Robert S. Rumely, On distinguishing prime numbers from composite numbers (to appear)
- R. P. Brent, An improved Monte Carlo factorization algorithm, *BIT*, **20** (1980), 176–184.
- John D. Dixon, Asymptotically fast factorization of integers, *Math. Comput.* **36** (1981) 255–260.
- Richard K. Guy, How to factor a number, *Congressus Numerantium XVI Proc. 5th Manitoba Conf. Numer. Math.*, Winnipeg, 1975, 49–89.
- H. W. Lenstra, Primality testing, *Studieweek Getaltheorie en Computers*, Stichting Mathematisch Centrum, Amsterdam, 1980, 41–60.
- G. L. Miller, Riemann's hypothesis and tests for primality, *J. Comput. System Sci.*, **13** (1976) 300–317.
- J. M. Pollard, Theorems on factorization and primality testing, *Proc. Cambridge Philos. Soc.* **76** (1974) 521–528.
- J. M. Pollard, A Monte Carlo method for factorization, *BIT* **15** (1975) 331–334; *MR* **50** #6992.
- R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Communications A.C.M.*, Feb. 1978.
- R. Solovay and V. Strassen, A fast Monte-Carlo test for primality, *SIAM J. Comput.* **6** (1977) 84–85; erratum **7** (1978) 118; *MR* **57** #5885.
- H. C. Williams, Primality testing on a computer, *Ars Combin.* **5** (1978) 127–185. *MR* **80d**:10002.
- H. C. Williams and R. Holte, Some observations on primality testing, *Math. Comput.* **32** (1978) 905–917; *MR* **57** #16184.
- H. C. Williams and J. S. Judd, Some algorithms for prime testing using generalized Lehmer functions, *Math. Comput.* **30** (1976) 867–886.

A1. Are there infinitely many primes of the form $a^2 + 1$? Probably so, and in fact Hardy and Littlewood (their Conjecture E) guessed that the number, $P(n)$, of such primes less than n , was asymptotic to $c\sqrt{n}/\ln n$,

$$P(n) \sim c\sqrt{n}/\ln n \quad ?$$

i.e., that the ratio of $P(n)$ to $\sqrt{n}/\ln n$ tends to c as n tends to infinity. The constant c is

$$c = \prod \left\{ 1 - \frac{\left(\frac{-1}{p}\right)}{p-1} \right\} = \prod \left\{ 1 - \frac{(-1)^{(p-1)/2}}{p-1} \right\} \approx 1.3727$$

where $\left(\frac{-1}{p}\right)$ is the Legendre symbol (see F5) and the product is taken over all odd primes. They make similar conjectures, differing only in the value of c , for the number of primes represented by more general quadratic expressions. But we don't know of any integer polynomial, of degree greater than one, for which it has been proved that it takes an infinity of prime values. Is there even one prime $a^2 + b$ for each $b > 0$?

Iwaniec has shown that there are infinitely many n for which $n^2 + 1$ is the product of at most two primes, and his result extends to other irreducible quadratics.

Ulam and others noticed that the patterns formed by the prime numbers when the sequence of numbers is written in a "square spiral" seems to favor diagonals which correspond to certain "prime-rich" quadratic polynomials. For example, the main diagonal of Figure 1 corresponds to Euler's famous formula $n^2 + n + 41$.

421	420	419	418	417	416	415	414	413	412	411	410	409	408	407	406	405	404	403	402
422	347	346	345	344	343	342	341	340	339	338	337	336	335	334	333	332	331	330	401
423	348	281	280	279	278	277	276	275	274	273	272	271	270	269	268	267	266	329	400
424	349	282	223	222	221	220	219	218	217	216	215	214	213	212	211	210	265	328	399
425	350	283	224	173	172	171	170	169	168	167	166	165	164	163	162	209	264	327	398
426	351	284	225	174	131	130	129	128	127	126	125	124	123	122	161	208	263	326	397
427	352	285	226	175	132	97	96	95	94	93	92	91	90	121	160	207	262	325	396
428	353	286	227	176	133	98	71	70	69	68	67	66	89	120	159	206	261	324	395
429	354	287	228	177	134	99	72	53	52	51	50	65	88	119	158	205	260	323	394
430	355	288	229	178	135	100	73	54	43	42	49	64	87	118	157	204	259	322	393
431	356	289	230	179	136	101	74	55	44	41	48	63	86	117	156	203	258	321	392
432	357	290	231	180	137	102	75	56	45	46	47	62	85	116	155	202	257	320	391
433	358	291	232	181	138	103	76	57	58	59	60	61	84	115	154	201	256	319	390
434	359	292	233	182	139	104	77	78	79	80	81	82	83	114	153	200	255	318	389
435	360	293	234	183	140	105	106	107	108	109	110	111	112	113	152	199	254	317	388
436	361	294	235	184	141	142	143	144	145	146	147	148	49	150	151	198	253	316	387
437	362	295	236	185	186	187	188	189	190	191	192	193	194	195	196	197	252	315	386
438	363	296	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	314	385
439	364	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	384
440	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383

Figure 1. Primes (in bold) Form Diagonal Patterns.

The only result for expressions (*not* polynomials!) of degree greater than 1 is due to Pyateckii-Šapiro, who proved that the number of primes of the form $[n^c]$ in the range $1 < n < x$ is $(1 + o(1))x/(1 + c)\ln x$ if $1 \leq c \leq 12/11$.

Martin Gardner, The remarkable lore of prime numbers, *Scientific Amer.* **210** #3 (Mar. 1964) 120–128.

G. H. Hardy and J. E. Littlewood, Some problems of 'partitio numerorum' III: on the expression of a number as a sum of primes, *Acta Math.* **44** (1922) 1–70.

Henryk Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.* **47** (1978) 171–188; *MR* **58** #5553.

Carl Pomerance, A note on the least prime in an arithmetic progression, *J. Number Theory* **12** (1980) 218–223.

I. I. Pyateckii-Sapiro, On the distribution in sequences of the form $[f(n)]$, *Mat. Sbornik* N.S. 33 (1953) 559–566; *MR* 15, 507.

A2. Are there infinitely many primes of the form $n! + 1$? The only values of $n \leq 230$ which give primes are 1, 2, 3, 11, 27, 37, 41, 73, 77, 116, and 154. It is not known if $n! - 1$ or

$$X = 1 + \prod_{i=1}^k p_i$$

is prime infinitely often. The only values of $p_k \leq 1031$ for which X is prime are $p_k = 2, 3, 5, 7, 11, 31, 379, 1019$, and 1021.

Let q be the least prime greater than X . Then R. F. Fortune conjectures that $q - X + 1$ is prime for all k . It is clear that it is not divisible by the first k primes, and Selfridge observes that the truth of the conjecture would follow from one of Schinzel, that for $x > 8$ there is always a prime between x and $x + (\ln x)^2$. The first few fortunate primes are 3, 5, 7, 13, 23, 17, 19, 23, 37, 61, 67, 71, 47, 107, 59, 61, 109, 89, 103, 79, ... The answers to the questions are probably "yes," but it does not seem conceivable that such conjectures will come within reach either of computers or of analytical tools in the foreseeable future.

More hopeful, but still difficult, is the following conjecture of Erdős and Stewart: are $1! + 1 = 2$, $2! + 1 = 3$, $3! + 1 = 7$, $4! + 1 = 5^2$, $5! + 1 = 11^2$ the only cases where $n! + 1 = p_k^a p_{k+1}^b$ and $p_{k-1} \leq n < p_k$? [Note that $(a, b) = (1, 0), (1, 0), (0, 1), (2, 0)$, and $(0, 2)$ in these five cases.]

Erdős also asks if there are infinitely many primes p for which $p - k!$ is composite for each k such that $1 \leq k! < p$; for example, $p = 101$ and $p = 211$. He suggests that it may be easier to show that there are infinitely many integers n ($l! < n \leq (l+1)!$) all of whose prime factors are greater than l , and for which all the numbers $n - k!$ ($1 \leq k \leq l$) are composite.

David Silverman noticed that the product

$$\prod_{i=1}^m \frac{p_i + 1}{p_i - 1}$$

is an integer for $m = 1, 2, 3, 4$ and 8 and asked if it ever is again.

I. O. Angell and H. J. Godwin, Some factorizations of $10^n \pm 1$, *Math. Comput.* 28 (1974) 307–308.

Alan Borning, Some results for $k! \pm 1$ and $2 \cdot 3 \cdot 5 \cdots p \pm 1$, *Math. Comput.* 26 (1972) 567–570.

Martin Gardner, Mathematical Games, *Sci. Amer.* 243 #6 (Dec. 1980) 18–28.

Solomon W. Golomb, On Fortune's conjecture, *Math. Mag.* (to appear)

S. Kravitz and D. E. Penney, An extension of Trigg's table, *Math. Mag.* 48 (1975) 92–96.

Mark Templer, On the primality of $k! + 1$ and $2 \cdot 3 \cdot 5 \cdots p + 1$, *Math. Comput.* 34 (1980) 303–304.

A3. Primes of special form have been of perennial interest, especially the **Mersenne primes** $2^p - 1$ (p is necessarily prime, but that is *not* sufficient! $2^{11} - 1 = 2047 = 23 \times 89$) in connexion with perfect numbers (see B1) and **repunits**, $(10^p - 1)/9$.

The powerful Lucas-Lehmer test, in conjunction with successive generations of computers, and more sophisticated techniques in using them, continues to add to the list of primes for which $2^p - 1$ is also prime:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203,
2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, ...

Their number is undoubtedly infinite, but proof is again hopelessly beyond reach. Suppose $M(x)$ is the number of primes $p \leq x$ for which $2^p - 1$ is prime. Find a convincing heuristic argument for the size of $M(x)$. Gillies gave one suggesting that $M(x) \sim c \ln x$, but some people do not believe this. Pomerance has an argument for $M(x) \sim c(\ln \ln x)^2$ but he says this doesn't agree with the facts.

D. H. Lehmer puts $S_1 = 4$, $S_{k+1} = S_k^2 - 2$, supposes that $2^p - 1$ is a Mersenne prime, notes that $S_{p-2} \equiv 2^{(p+1)/2}$ or $-2^{(p+1)/2} \pmod{2^p - 1}$ and asks: which?

Selfridge conjectures that if n is a prime of the form $2^k \pm 1$ or $2^{2k} \pm 3$, then $2^n - 1$ and $(2^n + 1)/3$ are either both prime or neither of them are. Moreover if both are prime, then n is of one of those forms. Is this an example of "the strong law of small numbers"?

If p is a prime, is $2^p - 1$ always **squarefree** (does it never contain a repeated factor)? This seems to be another unanswerable question. It is safe to conjecture that the answer is "No!" This *could* be settled by computer if you were lucky. As D. H. Lehmer has said about various factorization methods, "Happiness is just around the corner." Selfridge puts the computational difficulties in perspective by proposing the problem: find fifty more numbers like 1093 and 3511. (Fermat's theorem tells us that if p is prime, then p divides $2^p - 2$; the primes 1093 and 3511 are the only ones less than 3×10^9 for which p^2 divides $2^p - 2$.)

The corresponding primes for $(10^p - 1)/9$ are 2, 19, 23, 317, 1031, the last two of which were found by Hugh Williams quite recently, subject to final tests being completed in the last case. Repunits > 1 are known never to be squares. Are they ever cubes? When are they squarefree?

The **Fermat numbers**, $F_n = 2^{2^n} + 1$, are also of continuing interest; they are prime for $0 \leq n \leq 4$ and composite for $5 \leq n \leq 19$ and for many larger values of n . Hardy and Wright give a heuristic argument which suggests that only a finite number of them are prime. Selfridge would like to see this strengthened to support the conjecture that all the rest are composite.

Because of their special interest as potential factors of Fermat numbers, and because proofs of their primality are comparatively easy, numbers of the form $k \cdot 2^n + 1$ have received special attention, at least for small values