MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 204
OCTOBER 1993, PAGES 927-930

# GENERALIZED REPUNIT PRIMES

HARVEY DUBNER

ABSTRACT. Generalized repunits have the form $(b^n - 1)/(b - 1)$. A table of generalized repunit primes and probable primes is presented for $b$ up to 99 and large values of $n$.

## 1. INTRODUCTION

Numbers of the form

$$M = \frac{b^n - 1}{b - 1} \tag{1}$$

are called repunits to base $b$. They consist of a string of $n$ 1's when written in base $b$. For $b = 2$, these are the Mersenne numbers, which have been studied extensively for hundreds of years. In [3], a truly prodigious amount of work has gone into factoring numbers of the form $b^n \pm 1$ for $b$ from 3 to 12 and values of $n$ up to about 300. In [8], Williams and Seah tabulated all the generalized repunits that are prime or probable prime for $b$ from 3 to 12 and $n$ up to 1000 (2000 for base 10).

The purpose of this paper is to present the results of computer searches for generalized repunit primes for bases up to 99.

## 2. METHOD

In searching for primes of the form (1) we need to consider only prime $n$, because $M$ factors algebraically when $n$ is composite. Similarly, $b$ must not be a perfect power, because $M$ factors algebraically when it is. It is known that all factors of $M$ have the form $2kn + 1$. We divided each $M$ by the first 20,000 numbers of this form and discovered a small factor about half the time. Each remaining $M$ was subjected to a Fermat test

$$a^{M-1} \equiv 1 \pmod{M} \tag{2}$$

for some $a \neq b$. If the congruence failed, then $M$ was composite. If it held, we tried (2) with a different $a$. If the second congruence held, $M$ was declared a probable prime (PRP). We tried to give a rigorous proof that each PRP was prime. We used UBASIC [4, 7] to do this for most PRP's up to 250 digits. The larger PRP's were sent to François Morain for his elliptic curve prime proving algorithm [1, 6]. The results are shown in Table 1.

Received by the editor March 31, 1992 and, in revised form, August 17, 1992.
1991 *Mathematics Subject Classification*. Primary 11A41.

TABLE 1. Prime repunits–Base $b$

$$\frac{b^n-1}{b-1}$$

| $b$ | $n$–for which $P$ is prime or PRP(*) | max $n$ tested |
|---|---|---|
| 2 | 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, 86243, 110503, 132049, 216091, 756839 | don't know |
| 3 | 3, 7, 13, 71, 103, 541, 1091* 1367* 1627* 4177* 9011* 9551* | 12006 |
| 4 | 2 Algebraic factors | |
| 5 | 3, 7, 11, 13, 47, 127, 149, 181, 619, 929, 3407* 10949* | 12238 |
| 6 | 2, 3, 7, 29, 71, 127, 271, 509, 1049* 6389* 6883* 10613* | 12658 |
| 7 | 5, 13, 131, 149, 1699* | 10738 |
| 8 | 3 Algebraic factors | |
| 9 | Algebraic factors | |
| 10 | 2, 19, 23, 317, 1031 | 20000 |
| 11 | 17, 19, 73, 139, 907* 1907* 2029* 4801* 5153* 10867* | 11092 |
| 12 | 2, 3, 5, 19, 97, 109, 317, 353, 701* 9739* | 10486 |
| 13 | 3, 7, 137, 283* 883* 991* 1021* 1193* 3671* | 9550 |
| 14 | 3, 7, 19, 31, 41, 2687* | 9282 |
| 15 | 3, 43, 73, 487* 2579* 8741* | 8836 |
| 16 | 2 Algebraic factors | |
| 17 | 3, 5, 7, 11, 47, 71, 419, 4799* | 8446 |
| 18 | 2 | 8286 |
| 19 | 19, 31, 47, 59, 61, 107, 337* 1061* | 8010 |
| 20 | 3, 11, 17, 1487* | 7872 |
| 21 | 3, 11, 17, 43, 271 | 8218 |
| 22 | 2, 5, 79, 101, 359* 857* 4463* | 7698 |
| 23 | 5, 3181* | 7458 |
| 24 | 3, 5, 19, 53, 71, 653* 661* | 7918 |
| 25 | Algebraic factors | |
| 26 | 7, 43, 347 | 7498 |
| 27 | 3 Algebraic factors | |
| 28 | 2, 5, 17, 457* 1423* | 7392 |
| 29 | 5, 151, 3719* | 7186 |
| 30 | 2, 5, 11, 163, 569* 1789* | 6976 |
| 31 | 7, 17, 31, 5581* | 6826 |
| 32 | Algebraic factors | |
| 33 | 3, 197, 3581* | 6760 |
| 34 | 13, 1492* 5851* 6379* | 6568 |
| 35 | 313* 1297* | 6690 |
| 36 | 2 Algebraic factors | |
| 37 | 13, 71, 181, 251, 463* 521* 7321* | 7488 |
| 38 | 3, 7, 401* 449* | 6562 |
| 39 | 349, 631* 4493* | 6378 |
| 40 | 2, 5, 7, 19, 23, 29, 541* 751* 1277* | 6636 |
| 41 | 3, 83, 269* 409* 1759* | 2698 |
| 42 | 2, 1319* | 2788 |
| 43 | 5, 13 | 2088 |
| 44 | 5, 31, 167 | 2140 |
| 45 | 19, 53, 167 | 2112 |
| 46 | 2, 7, 19, 67, 211* 433* | 2136 |
| 47 | 127 | 2052 |
| 48 | 19, 269* 349* 383* 1303* | 2016 |
| 49 | Algebraic factors | |
| 50 | 3, 5, 127, 139, 347, 661* 2203* | 2520 |
| 51 | none | 2616 |

TABLE 1 (continued)

$\frac{b^n-1}{b-1}$

| $b$ | $n$–for which $P$ is prime or PRP(*) | max $n$ tested |
|---|---|---|
| 52 | 2, 103, 257* | 2110 |
| 53 | 11, 31, 41, 1571* | 2178 |
| 54 | 3, 389* | 2380 |
| 55 | 17, 41, 47, 151, 839* 2267* | 2370 |
| 56 | 7, 157, 2083* 2389* | 2392 |
| 57 | 3, 17, 109, 151, 211, 661* | 2376 |
| 58 | 2, 41, 2333* | 2338 |
| 59 | 3, 13, 479* | 2446 |
| 60 | 2, 7, 11, 53, 173 | 2350 |
| 61 | 7, 37, 107, 769* | 2388 |
| 62 | 5, 17, 47, 163, 173, 757* | 2592 |
| 63 | 5 | 2556 |
| 64 | Algebraic factors | |
| 65 | 19, 29, 631* | 2620 |
| 66 | 2, 7, 19 | 2388 |
| 67 | 19, 367* 1487* | 2592 |
| 68 | 5, 7, 107 | 2500 |
| 69 | 61, 2371* | 2388 |
| 70 | 2, 29, 59, 541* 761* 1013* | 2477 |
| 71 | 31, 41, 157, 1583* | 2292 |
| 72 | 2, 7, 13, 109, 227 | 2310 |
| 73 | 5, 7 | 2682 |
| 74 | 5, 191* | 2286 |
| 75 | 19, 47, 73, 739* | 2250 |
| 76 | 41, 157, 439* 593* | 2590 |
| 77 | 5, 37 | 2520 |
| 78 | 2, 101, 257, 1949* | 2310 |
| 79 | 5, 109, 149, 659* | 2473 |
| 80 | 7 | 2590 |
| 81 | Algebraic factors | |
| 82 | 2, 23, 31, 41 | 3526 |
| 83 | 5 | 2476 |
| 84 | 17 | 3342 |
| 85 | 5, 19, 2111* | 3312 |
| 86 | 11, 43, 113* 509* 1069* 2909* | 3203 |
| 87 | 7, 17 | 2710 |
| 88 | 2, 61* 577* | 3460 |
| 89 | 3, 7, 43, 71* 109* 571* | 3510 |
| 90 | 3, 19, 97* | 3330 |
| 91 | none | 2332 |
| 92 | 439* | 3372 |
| 93 | 7 | 2376 |
| 94 | 5, 13, 37, 1789* | 2578 |
| 95 | 7, 523* | 2370 |
| 96 | 2 | 2467 |
| 97 | 17, 37, 1693* | 2440 |
| 98 | 13, 47 | 2136 |
| 99 | 5, 37, 47, 383* | 2388 |

Most of the calculations were done on four special-purpose number-theory computers [5]. Each computer can do a Fermat test on a 1000-digit number in about 20 seconds. For larger numbers the test time varies as the cube of the number of digits. Approximately one day of one computer was devoted to each base. Some of the latest calculations were done on an improved version of the special hardware which is about four to eight times faster.

Because of a programming error, values of $M$ were tested for $b = 4$, even though these numbers factor algebraically and should have been skipped. Surprisingly, several of these composite numbers were designated as PRP, the largest being a 76-digit number corresponding to $n = 127$. Since this was by far the largest composite PRP that was ever discovered accidentally by the author, this was investigated further.

For odd primes $n$,

$$M = \frac{4^n - 1}{3} = (2^n - 1) * \frac{2^n + 1}{3} = (3A + 1) * (A + 1). \tag{3}$$

In [2] it is shown that the number of test bases less than $M$ which satisfy (2) is

$$\prod (M - 1, p_i - 1), \quad \text{where } M = \prod p_i^{a_i}.$$

If both factors on the right of (3) are prime, the number of test bases less than $M$ which satisfy (2) is approximately $M/3$, so that the probability of two random bases satisfying (2) is about 1/9. In fact, for $n = 127$ and for $a$ up to 30, (2) is satisfied for $a = 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 24, 26, 27, 29$. It is customary to use a small prime for a test base. Here, if one of the first 10 primes is used as a test base, 7 out of 10 times an erroneous prime indication results. Since 3 and 13 were used as the test bases, this explained the PRP result. It is interesting to note that the first factor is a Mersenne prime.

Similar considerations hold for any $b$ which is a perfect square. If $M$ factors into two primes, then there is an unexpectedly large probability that $M$ will pass a Fermat test although it is composite. It is clear that the practice of using small test bases should be questioned. It would be desirable if a criterion could be established for choosing optimum test bases.

## Acknowledgment

The author wishes to thank François Morain for his efforts in verifying so many large primes.

## Bibliography

1. A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Raport de Recherche 1256, INRIA, Juin, 1990.
2. R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391–1417.
3. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, Amer. Math. Soc., Providence, RI, 1988.
4. C. Caldwell, *The near repdigit primes $A_nB$, $AB_n$, and UBASIC*, J. Recreational Math. **22** (2) (1990), 101–109.
5. H. Dubner and R. Dubner, *The development of a low-cost computer for number theory applications*, J. Recreational Math. **18** (1985-86), 81–86.
6. F. Morain, *Distributed primality proving and the primality of* $(2^{3539} + 1)/3$, Advances in Cryptology-EURODRYPT '90 (I. B. Damgard, ed.), pp. 110–123.
7. W. Neumann, *A public domain BASIC for mathematics*, Notices Amer. Math. Soc. **36** (1989), 557–559.
8. H. C. Williams and E. Seah, *Some primes of the form* $(a^n - 1)/(a - 1)$, Math. Comp. **33** (1979), 1337–1342.

449 Beverly Road, Ridgewood, New Jersey 07450
*E-mail address*: 70372.1170@compuserve.com