Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.7

Primes of the Form $(\mathbf{b^n+1})/(\mathbf{b+1})$

Harvey Dubner
449 Beverly Road, Ridgewood, New Jersey 07450
Torbjörn Granlund
Notvarpsgränd 1, 1tr SE-116 66 Stockholm, Sweden
Email addresses: hdubner1@compuserve.com and tege@swox.se

Abstract

Numbers of the form $(b^n+1)/(b+1)$ are tested for primality. A table of primes and probable primes is presented for b up to 200 and large values of n.

1999 *Mathematics Subject Classification*: Primary 11A41
Keywords: prime numbers, generalized repunits

1 Introduction

A truly prodigious amount of computation has been devoted to investigating numbers of the form $b^n \pm 1$. The Cunningham project, to factor these numbers for b from 2 to 12, is perhaps the longest running computer project of all time [4]. The range of b has been extended to 100 and even further in special cases [1][2] . The Mersenne numbers, 2^n-1 have been studied extensively for hundreds of years and the largest known prime is almost always a Mersenne prime. In [6], generalized repunit primes of the form $(b^n - 1)/(b - 1)$ were tabulated for bases up to 99 and large values of n.

The purpose of this paper is to present the results of computer searches for primes of the form,

$$Q(b, n) = \frac{b^n + 1}{b + 1} \tag{1}$$

for bases up to 200 and large values of n.

2 Prime Search

For certain values of n in (1) the denominator cannot divide the numerator and are thus excluded from this study, and Q has algebraic factors for certain other values of b, n so that it cannot be prime. The algebraic factors of $b^n + 1$ can be determined using the theory of cyclotomic polynomials [4], but virtually all the important results can be obtained by simple long division. Trying long division, it is easy to see that the denominator cannot divide the numerator when n is even, and always divides it when n is odd. Also, if n is odd and composite then $b^k + 1$ will divide $b^n + 1$ when k divides n so that Q cannot be prime. Thus Q can be prime only if n is an odd prime.

For certain special forms of b, Q has algebraic factors for all n. If $b = c^t$ is a perfect power where t is greater than 2 and not a power of 2 then Q has algebraic factors and is almost always composite. There are rare cases when Q may be prime for small n but again $Q(b, n)$ can only be prime when n is prime.

It is well known that all factors of $b^n + 1$ with n an odd prime must be primes of the form $p = 2kn + 1$. We divided each $Q(b, n)$ by all primes of this form with $k < 100,000$, finding a small factor about half the time. Each remaining Q was subjected to a Fermat test

$$a^{Q-1} = 1 \pmod{Q}$$

for some $a \neq b$. If the congruence failed, then Q was composite. If it held then we tried the test again with a different a. If both tests succeeded, Q was declared a probable prime (or *prp*).

About a day was devoted to each value of b using computers with a frequency of about 500 MegaHertz. Almost all the prp searching was done by the second author.

3 Prime Proving

Small prp's up to 12 digits were proved prime by simple division. For prp's up to about 800 digits the prime proving program, APRT-CLE of UBASIC was used [5]. This program has an upper test limit of about 830 digits.

For prp's greater than 800 digits and up to 1200 digits we used the VFYPR program of Tony Forbes, which is an extended version of the UBASIC program, that can test prp's up to 1600 digits and is about twice as fast as UBASIC [7]. For a Pentium/500 it takes about 40 hours to test a 1200-digit prp and the test time increases as about the 4th power of the number of digits. The test limit of 1200 digits was arbitrarily chosen because of computer time availability.

One other prime-proving method was used in a few cases. The BLS method is based on being able to factor $Q-1$ so that the factored part exceeds $\sqrt[3]{Q}$ [3]. Since

$$\frac{b^n+1}{b+1} - 1 = \frac{b(b^{n-1}-1)}{b+1}$$

the BLS method in this case can sometimes use the extensive results of previous factorizations for the Cunningham project and other projects to reduce prime proving times from hours to seconds.

The results are shown in the accompanying tables. An asterisk indicates a probable prime. [Numbers in square brackets give the appropriate sequence numbers in the On-Line Encyclopedia of Integer Sequences.]

References

[1] R. P. Brent, H. J. J. te Riele, *Factorizations of* $a^n \pm 1$, $13 \le a < 100$, CWI Report NM-R9212, June 1992.

[2] R. P. Brent, P. L. Montgomery, H. J. J. te Riele, *Update 1 to: Factorizations of* $a^n \pm 1$, $13 \le a < 100$, CWI Report NM-R9419, September 1994.

[3] J. Brillhart, D. H. Lehmer, J. I. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620-647.

[4] J. Brillhart, D. H. Lehmer, J. I. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorization of* $b^n \pm 1$*,* $b = 2, 3, 5, 7, 10, 11, 12$ *up to high powers*, Amer. Math. Soc., Providence, RI, 1988

[5] H. Cohen, A. K. Lenstra, *Implementation of a new primality test*, Math. Comp. **48** (1987), 103-121.

[6] H. Dubner, *Generalized repunit primes*, Math. Comp. **61** (Oct 1993), 927-930.

[7] T. Forbes (tonyforbes@ltkz.demon.co.uk), personal communication concerning VFYPR prime proving program.

Table 1: Primes of form $Q(b,n) = (b^n + 1)/(b + 1)$

b	n for which Q is prime or prp(*)	max n tested
2	3 5 7 11 13 17 19 23 31 43 61 79 101 127 167 191 199 313 347 701 1709 2617 3539 5807* 10501* 10691* 11279* 12391* 14479* [A978]	32000
3	3 5 7 13 23 43 281 359 487 577 1579 1663 1741 3191 9209* 11257* 12743* 13093* 17027* [A7658]	25000
4	3 Algebraic	
5	5 67 101 103 229 347 4013* [A57171]	20000
6	3 11 31 43 47 59 107 811 2819* 4817* 9601* [A57172]	20000
7	3 17 23 29 47 61 1619* 18251* [A57173]	20000
8	Algebraic	
9	3 59 223 547 773 1009 1823* 3803* [A57175]	20000
10	5 7 19 31 53 67 293 641 2137* 3011* [A57176]	20000
11	5 7 179 229 439 557 6113* [A57177]	10000
12	5 11 109 193 1483* [A57178]	10000
13	3 11 17 19 919 1151 2791* 9323* [A57179]	10000
14	7 53 503 1229 [A57180]	10000
15	3 7 29 1091* 2423* [A57181]	10000
16	3 5 7 23 37 89 149 173 251 307 317 [A57182]	10000
17	7 17 23 47 967 6653* 8297* [A57183]	10000
18	3 7 23 73 733 941 1097 1933* 4651* [A57184]	10000
19	17 37 157 163 631 7351* [A57185]	10000
20	5 79 89 709 797 1163* 6971* [A57186]	10000
21	3 5 7 13 37 347 [A57187]	10000
22	3 5 13 43 79 101 107 227 353 7393* [A57188]	10000
23	11 13 67 109 331 587 [A57189]	10000
24	7 11 19 2207* 2477* 4951* [A57190]	10000
25	3 7 23 29 59 1249* 1709* 1823* 1931* 3433* 8863* [A57191]	10000
26	11 109 227 277 347 857 2297* 9043*	10000
27	Algebraic	
28	3 19 373 419 491 1031*	10000
29	7	10000
30	139 173 547 829 2087* 2719* 3109*	10000
31	109 461 1061*	10000
32	Algebraic	
33	5 67 157	10000
34	3	10000
35	11 13 79 127 503 617 709 857 1499* 3823*	10000
36	31 191 257 367 3061*	10000
37	5 7 2707*	10000
38	5 167 1063* 1597* 2749* 3373*	8000
39	3 13 149	8000
40	53 67 1217* 5867* 6143*	8000
41	17 691	8000
42	3 709 1637*	8000
43	5 7 19 251 277 383 503 3019* 4517*	8000
44	7	8000
45	103 157	8000
46	7 23 59 71 107 223 331 2207* 6841*	8000
47	5 19 23 79 1783* 7681*	8000
48	5 17 131	8000
49	7 19 37 83 1481*	8000
50	1153*	8000

Table 2: Primes of form $Q(b,n) = (b^n + 1)/(b + 1)$ - continued

b	n for which Q is prime or prp(*)	max n tested
51	3 149 3253*	6000
52	7 163 197 223 467 5281*	6000
53		6000
54	7 19 67 197 991*	6000
55	3 5 179 229 1129* 1321* 2251*	6000
56	37 107 1063* 4019*	6000
57	53 227	6000
58	3 17 1447*	6000
59	17 43 991*	6000
60	3 937* 1667* 3917*	6000
61	7 41 359	6000
62	11 29 167 313	6000
63	3 37 41 2131* 4027*	6000
64	Algebraic	
65	19 31	6000
66	7 17 211 643	6000
67	3 2347* 2909* 3203*	6000
68	757* 773*	6000
69	11 211 239 389 503 4649*	6000
70	3 61 97	6000
71	5 37 5351*	6000
72	3 7 79 277 3119*	6000
73	7	6000
74	13 31 37 109	6000
75	5 83	6000
76	3 5 191 269	6000
77	37 317	6000
78	3 7 31 661* 4217*	6000
79	3 107 457 491 2011*	6000
80	5 13 227 439	6000
81	3 5 701* 829* 1031* 1033*	6000
82	293 1279*	6000
83	19 31 37 43 421 547 3037*	6000
84	7 13 139 359 971* 1087* 3527*	6000
85	167 3533*	6000
86	7 17 397	6000
87	7 467	6000
88	709* 1373*	6000
89	13 59 137 1103* 4423*	6000
90	3 47	6000
91	3 11 43 397	6000
92	37 59 113	6000
93	89 571 601 3877*	6000
94	71 307 613 1787* 3793*	6000
95	43	6000
96	37 103 131 263	6000
97		6000
98	19 101	6000
99	7 37 41 71	6000
100	3 293 461	6000

Table 3: Primes of form $Q(b,n) = (b^n + 1)/(b + 1)$ - continued

b	n for which Q is prime or prp(*)	max n tested
101	7 229	6000
102	3	6000
103		6000
104	673* 839* 1031*	6000
105	11 149 1187* 1627*	6000
106	3 7 19 23 31 3989*	6000
107	103 983*	6000
108	13 223	6000
109	59 79 811*	6000
110	23 101	6000
111	3 5 23 53 383 2039*	6000
112	3	6000
113		6000
114	7 13 1801*	6000
115	7 31 293	6000
116	113 1481* 2089*	6000
117	271	6000
118	3 23 109 2357*	6000
119	29 53 797*	6000
120	3 31 43 263 4919*	6000
121	5 13 97 1499*	6000
122	293 3877*	6000
123	29 739*	6000
124		6000
125	Algebraic	
126	5 13 47 163 239 4523*	6000
127	317 1061*	6000
128	7 Algebraic	
129	17 227 1753*	6000
130	467	6000
131	5 101 3389* 3581*	6000
132	3 101 157 1303*	6000
133	5 7 17 59 79 157	6000
134	13 1171*	6000
135	5 7 2671*	6000
136	5 7 23 59 199 2053*	6000
137	101 241 353 1999*	6000
138	103 577*	6000
139	3 17 47 2683* 2719*	6000
140	59	6000
141	5 1471*	6000
142	3	6000
143	7 17 19 47 103 4423*	6000
144	3 23 41 317 3371*	6000
145	7 23 281	6000
146	17 1439*	6000
147	11 151	6000
148	3 7 31 43 163 317 1933* 5669*	6000
149	17 769*	6000
150		6000

Table 4: Primes of form $Q(b,n) = (b^n + 1)/(b + 1)$ - continued

b	n for which Q is prime or prp(*)	max n tested
151	3 367 3203*	6000
152	13 19	6000
153	13 1063* 5749*	6000
154	3 29 263 601* 619* 809* 1217* 2267*	6000
155	5	6000
156	3 1301*	6000
157	5 157 809* 1861* 2203*	6000
158	5 769* 5023*	6000
159	283 449 1949*	6000
160	11 37 1907*	6000
161	31 331 1483*	6000
162	3 1823*	6000
163	3 11 31 661* 1999* 4079*	6000
164	7 103 541 1109*	6000
165	3 5 383	6000
166	17 5437*	6000
167	17 59 1301* 3167*	6000
168	3 31 1741* 2099*	6000
169	3 7 109	6000
170	7	6000
171	13 149 257 4967*	6000
172	37 283 647* 4483* 5417*	6000
173	7 59 569* 2647*	6000
174	3 3191*	6000
175		6000
176	5 31 269 479 599* 809* 1307*	6000
177	3 5 19 419	6000
178	61 167 227	6000
179	827* 5011*	6000
180	5 13	6000
181	449 2687* 4877*	6000
182	1487*	6000
183	11	6000
184	19 79 149	6000
185	11	6000
186		6000
187		6000
188		6000
189	3 31 71	6000
190	3 19 1153*	6000
191	479 1163*	6000
192	109 197 587 727* 1997* 2441*	6000
193	3 11 67 3253*	6000
194	19 31	6000
195	3 13 19 43 89 1087* 1949* 2939*	6000
196	43 1049* 5441*	6000
197	31 37 101 163	6000
198	37 151 937*	6000
199	313 2579* 5387*	6000
200	7 277	6000

(Concerned with sequences A000978, A007658, A057171, A057172, A057173, A057175, A057176, A057177, A057178, A057179, A057180, A057181, A057182, A057183, A057184, A057185, A057186, A057187, A057188, A057189, A057190, and A057191.)

Received September 10, 2000; published in Journal of Integer Sequences November 28, 2000.

Return to Journal of Integer Sequences home page