MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 183-202

Primes at a Glance

By R. K. Guy, C. B. Lacampagne, and J. L. Selfridge

To Dan Shanks: May he stay on form and again become the product of three of the first four primes

Abstract. Let $N = B - L$, $B \geqslant |L|$, $\gcd(B, L) = 1$, $p \mid BL$ for all primes $p \leqslant \sqrt{N}$. Then N is 0, 1 or a prime. Writing N in this form suggests a primality and a squarefreeness test. If we also require that when the prime $q \mid BL$ and $p < q$ then $p \mid BL$, we say that $B - L$ is a *presentation* of N. We list all presentations found for any N. We believe our list is complete.

Just glance at

$$349 = 910 - 561 = 2 \cdot 5 \cdot 7 \cdot 13 - 3 \cdot 11 \cdot 17.$$

Surely 349 is a prime, since it is less than 19^2 and each prime less than 19 appears in exactly one of the two operands. How much more pleasant it is to test 349 for primality by glancing at this difference than by using some other prime testing algorithm.

We aim to find a pair of integers B and L with

$$N = B - L, \tag{1}$$

$$B \geqslant |L|, \tag{2}$$

$$\gcd(B, L) = 1, \tag{3}$$

$$\text{if } p \leqslant \sqrt{N}\text{, then } p \text{ divides } BL. \tag{4}$$

These conditions eliminate composite values of N. We show that for given N, not composite, there are infinitely many choices for B. But we seek *presentations* of N, those which satisfy the additional condition

$$\text{if } q \mid BL \text{ and } p < q\text{, then } p \mid BL. \tag{5}$$

We believe strongly that this condition leads us to a finite list of presentations; i.e., a finite set of N and a finite set of B for each N. We know that the set of B is finite for fixed N, $N > 1$.

Condition (5) could be replaced by various other conditions which would cut down the infinite list, but this condition seems more attractive to us than any similar condition on the prime factors of BL.

When $N = 1$ there is a relation between our work and that of D. H. Lehmer [1]. Lehmer found all pairs of consecutive integers S and $S + 1$ composed of primes up to 41. We are interested in the special case when each of the first k primes is a factor of $S(S + 1)$. These presentations with $N = 1$ are listed at the beginning of Table 4. We know from [1] that there are no presentations with $N = 1$ and $19 < p_k < 43$.

Received June 3, 1986; revised July 10, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A41.

Algorithms to test if N is prime or squarefree. Theorem 1 below leads us to primality and squarefreeness testing algorithms. The primality test is implicit in the work of Lehmer [2]. We hope that the squarefreeness test will find practical use.

THEOREM 1. $N > 1$ *is prime if and only if it satisfies conditions* (1) *through* (4).

Proof. If $N > 1$ satisfies conditions (1) through (4), then it is prime since it has no prime factor $p \leqslant \sqrt{N}$.

If N is prime, split the product of all primes less than $\sqrt{N}$ into two factors u and v with $\gcd(u, v) = 1$. Since the Diophantine equation $ux - vy = 1$ has infinitely many solutions (x, y) with $x > 0$, put $B = u(Nx + v)$, $L = v(Ny + u)$. Now $N = B - L$, and since $\gcd(N, B) = 1$, we have $\gcd(B, L) = 1$, and conditions (1) through (4) are satisfied.

Primality test. Let $p_k < N < p_{k+1}^2$ and let $M = p_1 \cdots p_k$ be the product of the first k primes, and $M = QN + R$, $0 \leqslant R < N$. If $R = 0$, then N is composite and has no prime factor greater than p_k. If $R \neq 0$, let $G = \gcd(N, R)$. Then $G = 1$ if and only if N is prime.

Examples. Since $7 < 70 < 11^2$, take $M = 210$. Now 70 divides 210, so 70 is composite and has no prime factor greater than 7.

$$101 \text{ is prime because } 210 = 2 \cdot 101 + 8 \text{ and } \gcd(101, 8) = 1.$$
$$91 \text{ is composite since } 210 = 2 \cdot 91 + 28 \text{ and } \gcd(91, 28) = 7.$$

Note that the algorithm sometimes serves to factor the number.

Testing for primality using this algorithm takes only one long division and one (short) gcd. For $N < 10^6$ it is faster or about as fast to prove primality using this algorithm as to use a strong pseudoprime test with two bases (which requires about 40 squarings, 40 multiplications and 40 (or 80) divisions). Should you wish to test $N < 10^6$ by this method, you would need to store the product of the primes up to 997. This requires 44 32-bit words. For $N < 10^3$, 10^4 or 10^5 the number of 32-bit words is 2, 4 or 14.

Squarefreeness test. Express N as the product $\prod_{i=1}^{r} F_i^i$ where the F_i are squarefree. Thus F_i is the product of those prime factors of N which occur to exactly the ith power. For example, 8400 has $F_1 = 21$, $F_2 = 5$, $F_3 = 1$, $F_4 = 2$.

Choose k so that $p_k < N < p_{k+1}^3$. Now $M = p_1 \cdots p_k$ can be taken considerably smaller than for the primality test.

As before, write $M = QN + R$. If $R = 0$, N is squarefree and has no prime factor greater than p_k. Otherwise, let $D_0 = N$ and $G_0 = \gcd(N, R)$. Let $D_1 = D_0/G_0$ and $G_1 = \gcd(D_1, G_0)$. Continue with $D_i = D_{i-1}/G_{i-1}$ and $G_i = \gcd(D_i, G_{i-1})$ until $G_r = 1$.

Now see if D_r is a square. If so, and $D_r > 1$, then it is the square of a prime greater than p_k, and $F_1 = G_0/G_1$, $F_2^2 = (G_1/G_2)^2 D_r$. If D_r is not a square, $F_1 = (G_0/G_1)D_r$ and $F_2 = G_1/G_2$. In any case, $F_i = G_{i-1}/G_i$ for $3 \leqslant i \leqslant r$.

Examples. Since $3 < 106 < 5^3$, we can use $M = 6$. Then $G_0 = \gcd(6, 106) = 2$, $D_1 = 106/2 = 53$, and $G_1 = \gcd(53, 2) = 1$. Since 53 is not square, 106 is squarefree.

For $N = 1200$, take $M = 210$. Then $G_0 = 30$, $D_1 = 40$, $G_1 = 10$, $D_2 = 4$, $G_2 = 2$, $D_3 = 2$, $G_3 = 2$, $D_4 = 1$, $G_4 = 1$. Thus $(F_1, F_2, F_3, F_4) = (3, 5, 1, 2)$.

For $N = 3468$, take $M = 30030$. Then $G_0 = 6$, $D_1 = 578$, $G_1 = 2$, $D_2 = 289$, $G_2 = 1$. Since D_2 is a square, $F_1 = G_0/G_1 = 3$, $F_2^2 = (G_1/G_2)^2 D_2 = 2^2 17^2$, and $N = 3 \cdot 34^2$.

For $N = 323$, take $M = 30$ and find that N is squarefree, but the test does not tell whether N is prime or the product of two primes each of which is greater than 5.

For $N = 3000$, take $M = 30030$, finding that the squarefree part of 3000 is 3, and the cubeful part is 10^3.

To test $N < 10^6$ you need store only four 32-bit words for the product of the primes below the cube root of N. To test $N < 10^9$ you need 44 32-bit words.

Presentations of primes as sums. Our presentations have $B > 0$, but we may have $L < 0$, e.g., $5 = 3 - (-2)$. We write this difference as a sum and refer to the presentation as a sum also. So our presentations include

$$\begin{aligned} 5 &= 3 + 2, \\ 11 &= 2 \cdot 3 + 5, \\ 29 &= 3 \cdot 5 + 2 \cdot 7, \\ 97 &= 5 \cdot 11 + 2 \cdot 3 \cdot 7. \end{aligned}$$

When we try to find such a presentation which uses the primes up to 13, the smallest candidate is

$$347 = 2 \cdot 7 \cdot 13 + 3 \cdot 5 \cdot 11.$$

But take a second glance: 347 violates property (4) because 17 does not divide BL. In fact, we show easily that there are only finitely many sums $B + |L|$ which satisfy conditions (1) through (4).

THEOREM 2. 167 *is the largest N having a sum* $N = B + |L|$ *satisfying conditions* (1) *through* (4).

Proof. Larger primes must have 13 dividing a summand, and by the arithmetic mean/geometric mean inequality,

$$u + v \geqslant 2\sqrt{uv} \geqslant 2\sqrt{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13} > 17^2.$$

For $p_k \geqslant 13$, $2\sqrt{2 \cdot 3 \cdots p_k} > p_{k+1}^2$ follows by induction. To see this, use the fact that $2p_k > p_{k+1}$, so for $p_k \geqslant 17$,

$$p_k^5 > p_k(p_{k+1}/2)^4 \geqslant 17(p_{k+1}/2)^4 > p_{k+1}^4$$

and $\sqrt{p_k} > (p_{k+1}/p_k)^2$.

There are 106 sums satisfying conditions (1) through (4). Of these, 87 also satisfy condition (5). These are given in Table 1. Table 1 gives all such presentations for primes less than or equal to 149 and for 167. It is easy to check that neither 151, 157, nor 163 can be written as a sum satisfying conditions (1) through (4).

Presentations with fixed L.

Remark 1. 29 is the largest prime which can be presented as $N = B - 1$, and 31 is the largest prime which can be presented as $N = B + 1$.

Here $p_1 p_2 \cdots p_k \mid B$ and $N < p_{k+1}^2$. Remark 1 follows immediately from $p_1 p_2 \cdots p_k > p_{k+1}^2$ for $p_k \geqslant 7$.

Just the following numbers can be presented as $N = B - 1$:

$$0 = 1 - 1, \quad 5 = 2 \cdot 3 - 1, \quad 17 = 2 \cdot 3^2 - 1,$$
$$1 = 2 - 1, \quad 7 = 2^3 - 1, \quad 23 = 2^3 3 - 1,$$
$$3 = 2^2 - 1, \quad 11 = 2^2 3 - 1, \quad 29 = 2 \cdot 3 \cdot 5 - 1.$$

For $N = B + 1$, $N = 2, 3, 5, 7, 13, 19$, and 31.

TABLE 1

Complete list of sum presentations of primes $N = B + L$

Only $p_i < \sqrt{N}$ used			First $p > \sqrt{N}$ also used	
B +	L =	N	= B +	L
1	1	**2**		
		3	2	1
2^2	1	**5**	3	2
		7	2^2	3
			$2 \cdot 3$	1
2^3	3	**11**	$2 \cdot 3$	5
3^2	2			
3^2	2^2	**13**	$2 \cdot 5$	3
$2^2 3$	1			
3^2	2^3	**17**	$2^2 3$	5
			$3 \cdot 5$	2
2^4	3	**19**	$2 \cdot 5$	3^2
$2 \cdot 3^2$	1		$3 \cdot 5$	2^2
		23	$3 \cdot 5$	2^3
			$2 \cdot 3^2$	5
			$2^2 5$	3
$2^2 5$	3^2	**29**	$3 \cdot 5$	$2 \cdot 7$
$2^3 3$	5			
2^4	$3 \cdot 5$	**31**	$3 \cdot 7$	$2 \cdot 5$
5^2	$2 \cdot 3$			
$2 \cdot 3 \cdot 5$	1			
5^2	$2^2 3$	**37**	$2 \cdot 3 \cdot 5$	7
3^3	$2 \cdot 5$			
$2^2 3^2$	5	**41**	$3 \cdot 7$	$2^2 5$
			$5 \cdot 7$	$2 \cdot 3$
5^2	$2 \cdot 3^2$	**43**	$2^2 7$	$3 \cdot 5$
$2^3 5$	3			
3^3	$2^2 5$	**47**	$5 \cdot 7$	$2^2 3$
2^5	$3 \cdot 5$		$2 \cdot 3 \cdot 7$	5
$3^2 5$	2			

Only $p_i < \sqrt{N}$ used			First $p > \sqrt{N}$ also used	
B +	L =	N	= B +	L
$5 \cdot 7$	$2 \cdot 3^2$	**53**		
$5 \cdot 7$	$2^3 3$	**59**		
$3^2 5$	$2 \cdot 7$			
$2^3 5$	$3 \cdot 7$	**61**		
$2 \cdot 3 \cdot 7$	5^2	**67**		
$2^2 3 \cdot 5$	7			
$2^2 3^2$	$5 \cdot 7$	**71**		
$2 \cdot 5^2$	$3 \cdot 7$			
$2^3 7$	$3 \cdot 5$			
$3^2 5$	$2^2 7$	**73**		
$3^2 7$	$2 \cdot 5$			
$2 \cdot 5 \cdot 7$	3			
7^2	$2 \cdot 3 \cdot 5$	**79**		
$2 \cdot 5 \cdot 7$	3^2			
$2^4 3$	$5 \cdot 7$	**83**		
$3^2 7$	$2^2 5$			
$2 \cdot 3^3$	$5 \cdot 7$	**89**		
$3 \cdot 5^2$	$2 \cdot 7$			
$2^2 3 \cdot 7$	5			
$2 \cdot 5 \cdot 7$	3^3	**97**	$5 \cdot 11$	$2 \cdot 3 \cdot 7$
$2 \cdot 3^2 5$	7			
$2^3 7$	$3^2 5$	**101**	$2 \cdot 3 \cdot 11$	$5 \cdot 7$
$2^4 5$	$3 \cdot 7$			
$3^2 7$	$2^3 5$	**103**	$2 \cdot 5 \cdot 7$	$3 \cdot 11$
$3 \cdot 5^2$	$2^2 7$			
$2^3 3^2$	$5 \cdot 7$	**107**	$7 \cdot 11$	$2 \cdot 3 \cdot 5$
$3 \cdot 5 \cdot 7$	2			
$2^2 3 \cdot 5$	7^2	**109**		
$2^2 3 \cdot 7$	5^2			
$3 \cdot 5 \cdot 7$	2^2			
$3^2 7$	$2 \cdot 5^2$	**113**		
$2 \cdot 7^2$	$3 \cdot 5$			
$3 \cdot 5 \cdot 7$	2^3			
$3 \cdot 5 \cdot 7$	$2 \cdot 11$	**127**		
$2 \cdot 5 \cdot 11$	$3 \cdot 7$	**131**		
$7 \cdot 11$	$2^2 3 \cdot 5$	**137**		
$2^2 3 \cdot 7$	$5 \cdot 11$	**139**		
$3 \cdot 5 \cdot 7$	$2^2 11$	**149**		
		151		
		157		
		163		
$2 \cdot 3^2 5$	$7 \cdot 11$	**167**		
$2^2 3 \cdot 11$	$5 \cdot 7$			

Remark 1 can be generalized. For fixed L, there are only a finite number of presentations and an easy algorithm for determining all of them. We have already done this if L is negative (Table 1). Sometimes there are no presentations.

Remark 2. There is no presentation when B or L is a prime $p \geqslant 11$ or when B or L is mp, $m \leqslant 6$ and $p \geqslant 13$.

Also, there are no presentations for some other values of L, for example $L = 36$, 48, or 54. On the other hand, if $B = 36$, 48, or 54, we can use various values of L including ± 35.

Table 2 gives presentations of the largest possible N for each positive L up to 56. If Table 4 is indeed complete, then the reader can complete Table 2 by subtracting and sorting, with $L = 10906571664989$ the last entry.

TABLE 2

Presentation of largest prime $N = B - L$ for fixed $L \leqslant 56$

$N =$	B $-$	L	$N =$	B $-$	L	$N =$	B $-$	L
29	30	1	no pres.		17	107	140	33
103	105	2	17	35	18	no pres.		34
67	70	3	no pres.		19	163	198	35
101	105	4	43	63	20	no pres.		36 to 39
79	84	5	89	110	21	41	81	40
29	35	6	83	105	22	no pres.		41
113	120	7	no pres.		23	83	125	42
97	105	8	11	35	24	no pres.		43
61	70	9	101	126	25	61	105	44
53	63	10	no pres.		26	109	154	45
no pres.		11	113	140	27	no pres.		46 to 48
23	35	12	137	165	28	101	150	49
no pres.		13	no pres.		29	97	147	50
151	165	14	47	77	30	no pres.		51 to 54
139	154	15	no pres.		31	113	168	55
89	105	16	73	105	32	109	165	56

Presentations using primes up to p_k. For k fixed, there are only a finite number of presentations using the first k primes. This follows from a theorem of Mahler, which unfortunately does not give a bound. We prove this for $p_k \leqslant 3$ and list our conjectured bounds on B in Table 3.

First, the presentations using no primes:

$$0 = 1 - 1, \quad 1 = 1 + 0, \quad 2 = 1 + 1.$$

$p_k = 2$. Next, the presentations using the prime 2 only:

$$1 = 2 - 1, \qquad 3 = 2 + 1 \qquad 5 = 2^2 + 1, \qquad 7 = 2^3 - 1.$$
$$= 2^2 - 1,$$

$p_k = 3$. We would like to find all presentations using only powers of 2 and 3. We know that N must be 1 or a prime less than 25. First we display the three presentations of 1:

$$1 = 3 - 2 = 2^2 - 3 = 3^2 - 2^3.$$

TABLE 3

Least and greatest B and count for given p_k

Least B	N	p_k	Greatest B	N	Count
1	0,1,2		1	0,1,2	3
2	1,3	**2**	8	7	5
3	1,5	**3**	256	13	29
6	1,11	**5**	32805	37	77
15	1,29	**7**	250047	47	196
55	13,97	**11**	3294225	53	192
182	17	**13**	8859375	239	225
715	1	**17**	95954936	311	176
3135	41	**19**	172078592	257	129
15015	157	**23**	22630400000	593	104
113883	263	**29**	4021054856	401	45
1344005	971	**31**	135689153600	929	35
11874891	1601	**37**	216745267200	59	17
46149730	991	**41**	1214151347500	1213	7
17118816000	433	**43**	17118816000	433	1
10906571667510	2521	**47**	10906571667510	2521	1
					1242

TABLE 4

Main table of presentations of $N = B - L$

(**N** *on left*: p_k *above*: *B in body of table*.)

		2	3	5	7	11	13	17	19
0	1								
1	1	2	3	6	15	385	1716	715	633556
			4	10	21	441	2080	12376	
			9	16	36	540	123201	194481	
				25	126	3025			
				81	225	9801			
					2401				
	ϕ	2			4375				
2	1								
3	—	2							
		4							
		2	3	5					
5		4	3						
			6						
			8						
			9						
			32						
7		8	4	10					
			6	12					
			9	15					
			16	25					
				27					
				135					
				250					

TABLE 4 (*continued*)

	3	5	7	11	13	17	19
11	8	6	21				
	9	15	35				
	12	20	56				
	27	36	60				
		75	81				
			200				
			686				
			875				
13	9	10	28	55			
	12	15	48	90			
	16	18	63	343			
	256	25	160	363			
		40	175	3388			
		45	405	6250			
			525	151263			
			1728				
17	9	12	35	77	182		
	18	15	42	105	875		
	81	20	45	297	3185		
		27	80	567	67392		
		32	192	605			
		125	360	1232			
			392	1617			
			5120				
19	16	10	40	154	910	1020	
	18	15	49	250	1540	4114	
	27	24	54	264		5544	
		25	75	294		56595	
		64	6144	1944			
		100		2560			
		144		2835			
				4375			
23	24	15	30	198	660	75735	22253
	27	18	35	275	2025	2025023	
	32	20	63	968	4235		
		48	98	1815	5600		
		50	128	3773	34398		
		648	135				
		2048					

TABLE 4 (*continued*)

	5	7	11	13	17	19	23	29	31
29	20	15	84	260	5265	—	2437149		
	24	35	99	315	5775				
	30	50		1485	224939				
	45	189		3549					
	54	225		35750					
	125	245		59319					
		729							
		1029							
		2430							
31	16	21	66	616	2275	4420	240856		
	25	45	196	1890	231231	41800			
	30	175	220	8281		5836831			
	36	4000	231	40656					
	40		735						
	81		1120						
	256		1375						
37	25	30	70	2457	373527	22477	92092		
	27	42	147						
	40	72	352						
	45	100	847						
	162	112	1225						
	32805	135	2662						
		280							
		625							
41	36	21	140	195	1911	3135	884925	—	8402240
	45	35	525	756	4760		1382576		159398280
	50	56	770	1001	21216				
	81	90	825						
		105	2541						
		125							
		216							
		441							
		10976							
43	25	28	120	693	2695	—	—	—	5260948
	40	63	175	715					
	45	70	5488	1408					
	48	168		3718					
	75	288		9360					
	243	343		35035					
		448		5767168					
		1323							
47	27	35	77	572	—	—	—	5056527	
	32	42	110	3575					
	45	75	245	15972					
	50	147	432	47432					
	72	672	495	59535					
		250047	1125	78125					
			24057						

TABLE 4 (*continued*)

	7	11	13	17	19	23	29	31	37
53	35	165	273	54978	218348	55913			
	60	350	1925	983178	392445	3105375			
	63	693	4928	1596725		39721605			
	98	900	7203						
	200	15488	13013						
	245	3294225							
	2240								
59	35	224	455	12155	42959	—	—	—	216745267200
	45	539	605	45500	112710				
	80	675	2600	297440					
	84	1760	3920						
	140	14700	7605						
	315								
	500								
61	40	105	490	10890	37791	818125			
	70	336	880		3620925	553864311			
	75	385	1755						
	96	600							
	196								
	250								
	3645								
67	42	165	210	33880	46750	4475317	—	34897072	
	60	375	847	165375					
	70	672	4225	216580					
	112	1782	13377	999702					
	147	3840	1574640						
	175	42592							
	567								
71	36	126	2535	3536	1218750	328308695			
	50	176	18375	16731	7260071				
	56	225		34391					
	120	231		11275335					
	1296	896							
		1100							
		1331							
		6000							
		6875							
		46656							
73	45	150	385	3388	60588	632320			
	63	220	528	413343	1836765				
	70	315	1690						
	105	3993	2548						
	108		7938						
	343								
	448								
	640								
	1225								
	1323								
79	49	154	429	—	5434	—	1526175		
	70	189	924				27025999		
	84	2079	1080						
	100		3159						
	135		5929						
	175		86515						
	324								
	1024								

TABLE 4 (*continued*)

	7	11	13	17	19	23	29	31
83	48	105	468	2618	17100			
	63	308	2288	261443				
	90	363		1812608				
	98	875						
	125	1568						
	245	160083						
	1875							
	19683							
89	54	110	18954	2520	10374			
	75	210	154880	9945	24960			
	84	264		12584				
	105	320		36125				
	189	539		49049				
	224	980						
	65625							
97	70	55	825	1287	23562	—	7223040	4295577
	90	132	2275	30855				
	105	385	19305	47872				
	112	405	28125	316875				
	147	847	61347					
	160	35937	86625					
	972							
101	56	66	231	26400	183141	36611676		
	80	486	1001					
	105	605	2376					
	126		114345					
	150							
	245							
	1701							
	3125							
103	63	70	1078	1650	56628	193648	—	5124843750
	75	180	1573	31603				
	105	378	2028	149175				
	175	495	6655	778855				
	243	2695	11088	4851495				
	250							
	343							
	5103							
107	72	77	1430	770	1630827	215985		
	105	140	1680	2912		3216320		
	135	275	5915	17787				
	147	800	1664000					
	350	1232						
	450	8192						
	875	42875						
109	60	154	2475	5005	—	2880514		
	84	165		7480				
	105	175		26520				
	144	550						
	189	1089						
	784	3234						
113	63	168	308	3003	—	182988	2077383	31821903
	98	245	1400	397488		734825		
	105	960	2310			2548260		
	120	1323	2808			51271025		
	140	1485	9408					
	225		16038					
	288		22113					
	3200		58080					

TABLE 4 (*continued*)

	11	13	17	19	23	29	31
127	105 490 567 847 2800 8575	715 2002 3900 78975	40222	31977 60775 83980 346060 1100512	4494672	1754935	75004875 336394240
131	110 231 1155 1715 2156 7875	495 560 20580	1496 2210 83006	301796			
137	77 165 242 1215 1512 8712	462 1320 3465 823680	1820 4862 157437 637637	—	74750 297297		
139	84 154 315 825 1470 4374	594 81675	1309 26880 48334 93639	270864	1182775		
149	105 275 875 1029 5000 6804 180224	429 539 4725 11979 57024	8619 51200	333944			
151	165 231 396 756 4375	385 1911 8775	31941 294151	11305 35035 182476 360126	18993216	—	2533440
157	220 297 172032	9075 14157 33957	1092 14080 32032 70227	254320	15015 1859872		
163	198 240 625 3430 6400 7203	273 735 2275 6435 15288 1146880	—	5027913	—	394128 129324195	
167	90 132 1575	440 882 1287 45927	41327 60500	289575 11790792			

TABLE 4 (*continued*)

	13	17	19	23	29	31	37
173	693	13923	38610	—	139403		
	3575	27200					
		845325					
179	1089	4004	8330				
	1859	73304	88179				
	4235	1713660	161109				
	5184		1042899				
181	286	1105	—	81900			
	2106	3366					
	4900	10296					
		1783600					
191	455	3740	665856	—	—	—	396785151
	1001		3322055				
	8316						
193	1183	6160	14025	—	4955143		
	7200	12348	62073				
	557568	32368					
197	1352	5202	3031875	—	—	139553765	
	3200	9360	49212800				
	274625	53900					
		203840					
		790272					
199	364	4840	18525	79135			
	1144	6370	273780	676039			
	1200	66759		17448574			
	2695	4685824					
	8064						
211	715	—	7735	—	—	2369851	
	1485		165376				
	11011						
	66550						
223	1848	—	146523				
	4095		935935				
	7098						
	9295						
	1063348						
227	3087	1547	3230				
	16562	6545					
		9152					
229	385	6664	—	646875			
		21250					
		148104					
		156000					
		4758325					
233	728	4160	183260	2585088			
	5733	20825					
	456533						

TABLE 4 (*continued*)

	13	17	19	23	29	31
239	330	4914	280280			
	525	25025	339864			
	624					
	1625					
	4719					
	11250					
	8859375					
241	780	2145	28665	427570		
	2100	4641	116424945			
	11616	2348125				
	20625					
	55296					
251	1001	1560	9975	—	1837836	
	3276	7986				
	10976	67626				
	17576					
	35000					
257	455	2805	276507	21252	—	76580735
	572	4235	172078592			
	1232	1127357				
	2457					
	7007					
	170625					
263	770	858	399168	—	113883	
	1638	13013	454860			
	3773	17280				
	6500					
	30888					
269	819	10829	12518324	—	50581800	
	18144	11319				
		244205				
271	546	1155	1982251			
	700	8125	2478175			
	726	23595				
	1701	74800				
277	420	32725	12597			
	550	125125				
	585					
	4732					
	77077					
	199927					
281	1001	1386	7106			
	1100	26741	54621			
	3185		278460			
	43940					
283	1053	3003	97240	242902800	54553408	10868910
	1375	5145	799708			
	7290		1329468			
	29403					
	499408					

TABLE 4 (*continued*)

	17	19	23	29	31	37
293	2295	17765				
	7293					
	401408					
	449280					
307	2925	29700				
	4675	3493875				
	104125					
311	20111					
	95954936					
313	18513	8398				
	53625	116688				
	187500					
	250563					
317	11900	31920	328757	737352		
	12285		5226837	4585625		
	28917					
	635250					
331	2431	8976	—	7540435	621537280	
	2541	81081				
	4335					
	48841					
337	1724800	—	326040	2525860		
347	7497	16055	—	533715		
	22022					
	57222					
349	910	625974	336490			
	6069					
	30184					
	537600					
353	3213	29393	—	—	—	32232200
359	1430	134064	2653464			
	14399					

TABLE 4 (*continued*)

	19	23	29	31	37	41	43
367	7150	2785552					
	1009375						
373	88825						
379	35700	119680	—	4885545			
	1860859						
	32368000						
383	53865	200583	1691228				
389	3315	—	—	—	181748637525		
397	—	8008462					
401	247401	—	4021054856	2003001			
409	122265						
419	—	—	12128480				
421	4620						
	14820						
	3221925						
431	14189175	127929375					
433	—	—	—	—	—	—	17118816000
439	44044						
	168399						
443	77520	97020	—	7058700000			
		384813					
		984998					
449	230945	—	42204149				
	1449624						
457	372400						
461	4641						
463	452200	—	—	—	542842300		
	6495853						
467	65637	30107					
	315392	2880267					
		104867840					
479	25350	16286595	—	—	3970234604		
487	—	207207					
491	270215	120666	1762475	111473477375			
	17346560						
499	206250	33649	2091544				
503	25935	3076983	—	—	196815528		
	92378						
509	51714	1344189					
521	14535						
	32175						
	87465						
	339405						
523	79420	52003					

TABLE 4 (*continued*)

			23	29	31	37	41
541	547		prime values of N in lightface have no presentation				
		557	—	482885	—	124208630	
				2891445			
	563	**569**	124355				
			75109944				
		571	544180	19829446			
			707200				
			1366936				
		577	664240				
		587	1138592				
			1461915				
		593	1785168	607563			
			22630400000				
	599	**601**	8438976				
		607	1077375				
		613	302005				
			3287988				
		617	1454355				
		619	15249				
	631	**641**	60792680				
		643	156975				
			16159500				
			77931958				
			3587353308				
	647	**653**	142025				
	659	**661**	425425				
		673	447678	885115			
		677	112112	1210007552			
			269192				
		683	465290	—	—	6236361450	
		691	1311000				
		701	—	71413056			
		709	15295	3297184			
		719	4956644	1329354			
		727	30218265	—	—	775681270	
	733	**739**	374374				
	743	**751**	5703126	859180			
		757	21505	1108304197			
			1562275				
			21037500				
761	769	**773**	—	9604133	14987973		
		787	305767	—	—	—	1869878472
			490758912				
	797	**809**	—	—	73547100		
		811	9970155				
		821	205751	143310141			
			7863401				
	823	**827**	—	—	—	—	252167630
		829	82225				
			47887840				
	839						

TABLE 4 (*continued*)

				29	31	37	41
	853		**857**	17131257	—	—	4659016505
859	863			primes in lightface have no presentation			
877	881		**883**	5428423			
			887	910455			
				226915575			
			907	—	13657732		
			911	—	2461722536		
			919	1284894	35083785		
				10560979			
			929	12065625	135689153600		
			937	—	3878875		
	941		**947**	—	8787725		
					762215400		
			953	—	78531235328		
		967	**971**		1344005		
	977	983	**991**		—	—	46149730
997	1009	1013	**1019**		—	71349135	
			1021		—	—	198878700
		(8)*	**1087**		3768492000		
			1091		—	68103125	
			1093		—	187943925	
		(11)	**1187**		1163335667		
			1193		—	83741850	
			1201		100140625		
			1213		—	—	1214151347500
			1217		—	—	10378757220
		(5)	**1259**		5630473134		
		(7)	**1303**		8061768		
		(6)**					
		1373	**1381**			486159625	
		(23)	**1553**			12308642073	
		(6)	**1601**			11874891	

	47
2521	10906571667510

*The numbers in parentheses indicate the number of primes between boldface entries.
**There are 6 primes between 1303 and 1369.

We also find

$$
\begin{array}{lll}
5 = 3 + 2 & 13 = 3^2 + 2^2 & 23 = 2^3 3 - 1 \\
\quad = 2 \cdot 3 - 1 & \quad = 2^2 3 + 1, & \quad = 3^3 - 2^2. \\
\quad = 3^2 - 2^2, & & \\
7 = 2^2 + 3 & 17 = 3^2 + 2^3 & \\
\quad = 2 \cdot 3 + 1 & \quad = 2 \cdot 3^2 - 1, & \\
\quad = 3^2 - 2, & & \\
11 = 2^3 + 3 & 19 = 2^4 + 3 & \\
\quad = 3^2 + 2 & \quad = 2 \cdot 3^2 + 1, & \\
\quad = 2^2 3 - 1, & &
\end{array}
$$

Now let us find all presentations of the form

$$N = |2^a - 3^b| \quad \text{with } a > 2.$$

Since $3^b \equiv 1$ or $3 \pmod 8$, we must have $3^b - 2^a$ when $N \equiv 1$ or $3 \pmod 8$ and $2^a - 3^b$ when $N \equiv 5$ or $7 \pmod 8$.

There are no further solutions of $3^b - 2^a = 1$, since if $16 \mid 3^b - 1$ then $4 \mid b$ and $3^4 - 1 \mid 3^b - 1$, which implies that $5 \mid 2^a$.

So we start with presentations of 5 and find

$$5 = 2^3 - 3.$$

If there is another presentation of 5 with $a > 2$, then the exponent of 2 must be greater than 3 and the exponent of 3 must be greater than 1. We write

$$2^{a+3} - 3^{b+1} = 2^3 - 3$$
$$\text{or} \quad (2^a - 1)2^3 = (3^b - 1)3.$$

Since $3 \mid 2^a - 1$ it follows that $2 \mid a$, and since $2^3 \mid 3^b - 1$ it follows that $2 \mid b$. Evidently, $a = 2$ and $b = 2$ is a solution. So we add

$$5 = 2^5 - 3^3$$

to our list, making five solutions.

We now prove that this list is complete. Suppose there is a presentation of 5 where the exponent of 2 is greater than 5 and the exponent of 3 is greater than 3. Then

$$2^{a+5} - 3^{b+3} = 2^5 - 3^3$$

with a and b positive, and

$$(2^a - 1)2^5 = (3^b - 1)3^3.$$

Now $2^2 \equiv 1 \pmod 3$, so $2^{18} \equiv 1 \pmod{3^3}$ and $2^{54} \equiv 1 \pmod{3^4}$. Thus $18 \mid a$ but $27 \nmid a$. Also $3^2 \equiv 1 \pmod{2^3}$, so $3^8 \equiv 1 \pmod{2^5}$. Thus $8 \mid b$ but $16 \nmid b$. (We can use the tables of factorizations [3] to look up factors of $2^a - 1$ and $3^b - 1$.) In this case, we find that $41 \mid 3^8 - 1$, so $41 \mid 3^b - 1$ and $41 \mid 2^a - 1$, and hence $20 \mid a$. We find that $11 \mid 2^{10} - 1$, so $11 \mid 3^b - 1$, and hence $5 \mid b$. Also $7 \mid 2^3 - 1$, so $7 \mid 2^a - 1$, $7 \mid 3^b - 1$, $6 \mid b$ and $30 \mid b$. Now $271 \mid 3^{30} - 1$, so $271 \mid 2^a - 1$, and hence $135 \mid a$, which is a contradiction since $27 \nmid a$. So all solutions of $5 = 2^a - 3^b$ are indeed listed above. Our method finds all solutions and leads to a contradiction when there are no other solutions.

We use the following notation for the argument above.

$$5 = 2^{a+5} - 3^{b+3} \Rightarrow$$
$$(2^a - 1)2^5 = (3^b - 1)3^3$$
$$18 \mid a \quad \text{and} \quad 27 \nmid a \qquad 8 \mid b \quad \text{and} \quad 16 \nmid b$$
$$41 \mid 3^8 - 1 \Rightarrow 41 \mid 2^a - 1 \Rightarrow 20 \mid a$$
$$11 \mid 2^{10} - 1 \Rightarrow 11 \mid 3^b - 1 \Rightarrow 5 \mid b$$
$$7 \mid 2^3 - 1 \Rightarrow 7 \mid 3^b - 1 \Rightarrow 6 \mid b \Rightarrow 30 \mid b$$
$$271 \mid 3^{30} - 1 \Rightarrow 271 \mid 2^a - 1 \Rightarrow 135 \mid a \Rightarrow 27 \mid a \Rightarrow\Leftarrow$$

There is only one more presentation of 7 with $p_k = 3$,

$$7 = 2^4 - 3^2.$$

Proof. $7 = 2^{a+4} - 3^{b+2} \Rightarrow$

$$(2^a - 1)2^4 = (3^b - 1)3^2$$
$$6 \mid a \quad \text{and} \quad 9 \nmid a \qquad 4 \mid b \quad \text{and} \quad 8 \nmid b$$
$$7 \mid 2^3 - 1 \Rightarrow 7 \mid 3^b - 1 \Rightarrow 6 \mid b \Rightarrow 12 \mid b$$
$$73 \mid 3^{12} - 1 \Rightarrow 73 \mid 2^a - 1 \Rightarrow 9 \mid a \Rightarrow\Leftarrow$$

There is only one more presentation of 11 with $p_k = 3$,

$$11 = 3^3 - 2^4.$$

Proof. $11 = 3^{b+3} - 2^{a+4} \Rightarrow$

$$(2^a - 1)2^4 = (3^b - 1)3^3$$
$$18 \mid a \quad \text{and} \quad 27 \nmid a \qquad 4 \mid b \quad \text{and} \quad 8 \nmid b$$
$$19 \mid 2^{18} - 1 \Rightarrow 19 \mid 3^b - 1 \Rightarrow 18 \mid b$$
$$757 \mid 3^9 - 1 \Rightarrow 757 \mid 2^a - 1 \Rightarrow 756 \mid a \Rightarrow 27 \mid a \Rightarrow\Leftarrow$$

For 13, we start with

$$13 = 2^4 - 3$$
$$13 = 2^{a+4} - 3^{b+1} \Rightarrow$$
$$(2^a - 1)2^4 = (3^b - 1)3$$
$$4 \mid b \quad \text{and} \quad 80 \mid 3^b - 1. \qquad \text{Thus } 5 \mid 2^a - 1 \text{ and } 4 \mid a.$$

Now $a = 4$ and $b = 4$ is evidently a solution. So

$$13 = 2^8 - 3^5.$$

The presentations of 13 given above, plus these two, complete the list of presentations of 13 using only powers of 2 and 3.

Proof. $13 = 2^{a+8} - 3^{b+5} \Rightarrow$

$$(2^a - 1)2^8 = (3^b - 1)3^5$$
$$162 \mid a \quad \text{and} \quad 243 \nmid a \qquad 64 \mid b \quad \text{and} \quad 128 \nmid b$$
$$193 \mid 3^{16} - 1 \Rightarrow 193 \mid 2^a - 1 \Rightarrow 96 \mid a$$
$$257 \mid 2^{16} - 1 \Rightarrow 257 \mid 3^b - 1 \Rightarrow 256 \mid b \Rightarrow 128 \mid b \Rightarrow\Leftarrow$$

There is only one more presentation of 17 with $p_k = 3$,

$$17 = 3^4 - 2^6.$$

Proof. $17 = 3^{b+4} - 2^{a+6} \Rightarrow$

$$(2^a - 1)2^6 = (3^b - 1)3^4$$
$$54 \mid a \quad \text{and} \quad 162 \nmid a \qquad 16 \mid b \quad \text{and} \quad 32 \nmid b$$
$$193 \mid 3^{16} - 1 \Rightarrow 193 \mid 2^a - 1 \Rightarrow 96 \mid a$$
$$257 \mid 2^{16} - 1 \Rightarrow 257 \mid 3^b - 1 \Rightarrow 256 \mid b \Rightarrow 32 \mid b \Rightarrow\Leftarrow$$

There is only one more presentation of 19 with $p_k = 3$,

$$19 = 3^3 - 2^3.$$

Proof. $19 = 3^{b+3} - 2^{a+3} \Rightarrow$

$$(2^a - 1)2^3 = (3^b - 1)3^3$$
$$18 \mid a \quad \text{and} \quad 27 \nmid a \qquad 2 \mid b \quad \text{and} \quad 4 \nmid b$$
$$73 \mid 2^9 - 1 \Rightarrow 73 \mid 3^b - 1 \Rightarrow 12 \mid b \Rightarrow 4 \mid b \Rightarrow\Leftarrow$$

There is only one more presentation of 23 with $p_k = 3$,

$$23 = 2^5 - 3^2.$$

Proof. $23 = 2^{a+5} - 3^{b+2} \Rightarrow$

$$\begin{aligned}
&(2^a - 1)2^5 = (3^b - 1)3^2 \\
&6 \mid a \quad \text{and} \quad 9 \nmid a \qquad 8 \mid b \quad \text{and} \quad 16 \nmid b \\
&7 \mid 2^3 - 1 \Rightarrow 7 \mid 3^b - 1 \Rightarrow 6 \mid b \Rightarrow 24 \mid b \\
&73 \mid 3^{12} - 1 \Rightarrow 73 \mid 2^a - 1 \Rightarrow 9 \mid a \Rightarrow\!\Leftarrow
\end{aligned}$$

This method can be extended to all N which are relatively prime to six and which can be written in the form $|2^a \pm 3^b|$. (All $N < 103$ except 53, 71 and 95.)

$p_k \geq 5$. For $p_k \geq 5$, we wrote two programs to find presentations. One starts with fixed N and uses the first k primes to consider all 2^k possible cases, depending on whether each prime is a factor of B or L. For each N and for each case, the program finds the smallest B and L and increments them by the product of the first k primes. Each such pair below the bound is checked, and if condition (5) is satisfied, the presentation is listed.

The second program backtracks through the sums of the logarithms of nonzero powers of primes $\leq p_k$ below the logarithm of the bound. For each pair of sums that is equal (within a given epsilon), the program computes N and lists it if $N < p_{k+1}^2$. For k small or for k large, the second program is faster.

Table 3 gives the smallest and largest B and the count of the number of presentations found for each p_k. Table 4 gives all presentations that we have found. We remark that at least one presentation was found for each prime less than 23^2. Notice the two "connected" presentations:

$$23 = 2048 - 2025 = 2025 - 2002.$$

We have searched for presentations up to 10^{14}. From this and from Table 4, the reader can judge whether there are likely to be any presentations still outstanding.

We would like to thank Richard Blecksmith for helpful discussions about the second program and for the use of his personal computer.

Mathematics and Statistics Department
University of Calgary
Calgary, Alberta, Canada T2N 1N4

Department of Mathematics
The University of Michigan—Flint
Flint, Michigan 48502-2186

Department of Mathematical Sciences
Northern Illinois University
DeKalb, Illinois 60115

1. D. H. LEHMER, "On a problem of Störmer," *Illinois J. Math.*, v. 8, 1964, pp. 59–79.

2. D. H. LEHMER, "On the converse of Fermat's Theorem," *Amer. Math. Monthly*, v. 43, 1936, pp. 347–354.

3. JOHN BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, BRYANT TUCKERMAN & S. S. WAGSTAFF, JR., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, Contemp. Math., vol. 22, Amer. Math. Soc., Providence, R. I., 1983.