PB-144

T. Naur: Integer Factorization

TRYK: DAIMI/RECAU

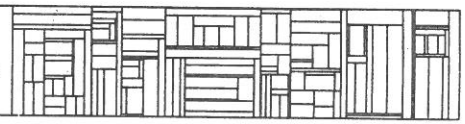
ISSN 0105-8517

INTEGER FACTORIZATION

Thorkil Naur

DAIMI PB-144
May 1982

Computer Science Department
AARHUS UNIVERSITY
Ny Munkegade – DK 8000 Aarhus C – DENMARK
Telephone: 06 – 12 83 55



Contents

1. Introduction

This paper gives a summary of methods for factoring large integers and presents particular factorizations obtained by these methods using the computer facilities at DAIMI. We assume the reader is familiar with simple facts from algebra and number theory. An overview of this mathematical background appears in appendix A.

The factorization problem can be stated very briefly as follows: Given an integer N > 1, find two other integers u > 1 and v > 1 such that N = u*v or determine that no such u and v exist. In the latter case, N is prime. This process may be further applied to u and v, their factors, and so on, obtaining in the end the complete prime factorization of N.

This seemingly innocent problem has fascinated mathematicians (and other kinds of people) for centuries and a host of surprisingly different methods have been devised for solving it.

The particular factorizations reported in this paper were obtained by a combination of methods selected primarily for their usefulness (i.e. efficiency and ease of implementation). A short description of each method is included, referring the reader to more detailed information where appropriate. Other methods that may be of general interest are also mentioned.

Overview

In section 2, the well known method of trial division is discussed. Although one should not expect this method to complete the factorization of even a moderately large number (25 digits, say) within reasonable time, the method is useful as part of other methods and also has certain merits of its own.

Improvements of the trial division method in the direction of eliminating in advance some of the possible divisors of the number to be factored lead indirectly to the continued fraction method described in section 3.

Integer Factorization

The continued fraction method is surely the best practical factorization method known today. Unlike trial division, the time required by this method to complete a factorization does not depend appreciably on the size of the factors. In the author's implementation, 40-45 digit numbers can be factored reasonably fast, and 55 digit numbers can also be handled, if one is prepared to wait a few weeks for the result. The continued fraction method is an ingenious combination of several techniques. To help the understanding of the method, we try to make the connections with other methods clear.

In sections 2 and 3 it is assumed that the number N to be factored is composite, i.e. it is known that $u > 1$, $v > 1$ exist such that $N = u*v$. In section 4, methods are described which are applicable when N is suspected to be prime. These methods thus test N for primality. (Trial division can establish the primality of N, but the methods of section 4 are usually much faster.) Some of the methods need auxiliary factors of numbers related to N, before N can be tested for primality. The "probabilistic" tests require no such information, but there is always a small, controllable probability that a number declared prime by such a method is, in fact, composite.

In section 5 Pollard's methods for factoring are described. Each of these methods may succeed in discovering a factor somewhat above the reasonable limit for trial division. The P-1 method will find all prime factors p of N with p-1 having only small prime factors. The Rho method is based on a cycle-finding algorithm by Floyd and will find a prime factor p in roughly $p^{1/2}$ operations.

In section 6 we explain how the various methods can be combined in the attempt to factor some number N. First, we illustrate the use of the methods by discussing some rather large examples. Then we give a summary of the combined strategy.

In section 7, the results obtained by combining the methods from sections 2-5 are described. These results are tabulated in appendices and comprise factorizations of Fibonacci numbers, Lucas numbers, and numbers of the form $2^n \pm 1$. The main body of these tables consists of previously known factorizations included for the reader's convenience. The more interesting factorizations are

marked with an "*".

Author's apology

To the reader who may be wondering what the practical, real-life application of factorization methods and results may be, the author would like to answer: "None, whatsoever." This answer would have been true a few years ago, before the discovery of public-key crypto-systems. In these systems for communicating encoded messages, the breaking of the code apparently depends on one's ability to factor very large numbers. While the discovery of these systems has stimulated a great deal of interest in methods for factoring and especially testing for primality, the present author has no intention of including an account of public-key crypto-systems in an attempt to justify his interest in factoring (the interested reader is referred to Rivest, Shamir, and Adleman[31]). Rather, he shamelessly admits that this interest is based solely on curiosity and a certain satisfaction in watching one number after the other "crack" under the slow, but in the end, overwhelming pressure of the various factorization methods.

The author cannot resist the temptation to include the following qoutation (copied from Knuth[13, p. 398]):

> The problem of distinguishing prime numbers from composites, and of resolving composite numbers into their prime factors, is one of the most important and useful in all of arithmetic. ... The dignity of science seems to demand that every aid to the solution of such an elegant and celebrated problem be zealously cultivated.
> C. F. Gauss, "Disquisitiones Arithmeticae," Art. 329 (1801).

2. Trial division

Trial division is probably the first method that comes into consideration when attempting to factor a number N: If N = u*v with u > 1, v > 1, u and v must be one of 2, 3, 4, ... , N-1 and trial division in its simplest form consists of dividing N by its possible divisors in turn. If the trial division of N by u, say, leaves a zero remainder, a factorization N = u*(N/u) has been obtained.

Since there are more numbers divisible by a particular small divisor than numbers divisible by a large divisor, it makes sense to test the possible divisors starting with 2 and working upwards. This ordering also has the effect that a divisor discovered by trial division is in fact prime, otherwise its factors would have been discovered earlier. (Most factorization methods will be described informally, as above. We always assume that N is the number to be factored. Variables like a, b, i, j, k, u, v, x, and y denote integers, unless otherwise stated. The letters p, q, and r denote primes.)

Since obviously the time required to find a factor of a number by trial division is closely related to the number of possible trial divisors, most improvements of the trial division method attempt to eliminate some of the trial divisors in advance. Other improvements attempt to make the division process itself faster, by replacing some of the divisions by cheaper operations, but these techniques will not be described here.

The first step in the direction of eliminating trial divisors is based on the simple observation that a composite number N cannot have two or more factors strictly larger that the square root of N. Thus it is sufficient to try as divisors only the numbers 2, 3, 4, ... , [sqrt(N)], where "sqrt" denotes the square root function and "[x]" is the greatest integer less that or equal to the real number x. N is prime if it is not divisible by any number less than its square root.

Example 1.

Let us factor the number N = 77 by trial division. Since [sqrt(77)] = 8, it is sufficient to try as possible divisors 2, 3, 4, 5, 6, 7, and 8. It is easy to check that 2, 3, 4, 5, and 6 do not divide 77, but 7 does, so we have obtained 77 = 7*(77/7) = 7*11. Since 7 was found as the result of trial division, it is prime. The other factor 11 is also prime, since [sqrt(11)] = 3 is below the limit already tried for 77.

A second observation leading to a shorter list of divisors is that the list need not contain a number u whose factors occur prior to u in the list. This condition actually restricts the trial divisors to all primes below [sqrt(N)]. Thus in the above example, it was unnecessary to divide 77 by 4 and 6, since both 4 and 6 are divisible by 2.

If N is not too large, it is convenient to generate and save beforehand a list of all primes below some limit and take the sequence of trial divisors from this list. If trial division is desired above some limit that makes this method too expensive (e.g. to continue above 100000, 9592 primes must be saved), a reasonable compromise is to eliminate only the trial divisors divisible by a fixed set of small primes. For example, to eliminate even trial divisors, we may use the sequence 2, 3, 5, 7, 9, 11, ..., where the next term after the second is calculated by adding 2. Or we may use 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, ... (where we alternately add 2 and 4 after the third term) to eliminate numbers divisible by 2 and 3. In both cases, the sequence still contains composite numbers (like 9 in the first or 25 in the second case), but the sequence is still significantly shorter than using all integers. See Wunderlich and Selfridge[41] for an efficient implementation of trial division using these ideas.

If the number N to be factored has the special form $a^n \pm b^n$, we can use a result proved by Legendre about 1798: If $N = a^n \pm b^n$ and gcd(a,b) = 1, then all prime factors p of N have the form 2*k*n+1, except if p = 2 or p divides $a^m \pm b^m$ for some m < n (p is an algebraic factor, see section 7.1). (For $N = a^n - b^n$, this

result is only valid for odd n.)

This fact is of course very useful for factoring numbers of the form $a^n \pm b^n$ by trial division. For example, all factors of $2^{32}+1$ (= $2^{32}+1^{32}$) have the form $64*k+1$, because $2^{32}+1$ has no algebraic factors. For k = 10, we get the factor 641 of $2^{32}+1$.

2.1. Quadratic residues

Another idea, due to Legendre, is restricting the possible factors of N to particular forms, using the theory of quadratic residues. Since this idea is important and also present in the continued fraction method, we will discuss the theory in some detail. It should be noted that this method has mostly been used for factoring comparatively small numbers by hand calculation. It is not particularly well suited for computer implementation.

We say that a number m is a quadratic residue modulo N if gcd(m,N) = 1 and there exists a solution x to the congruence

$$x^2 \equiv m \text{ (modulo N)}, \qquad (1)$$

i.e. if N divides x^2-m for some x (see Appendix A for more information on congruences). Formally, we write QR(m,N) if the above condition is satisfied. Note that m may be negative; QR(m,N) implies QR(m+k*N,N) for any k.

Now, if N = u*v, QR(m,N) implies QR(m,u), i.e. a quadratic residue modulo N is also a quadratic residue modulo any of N's factors. To see why, note that $a \equiv b$ (modulo N) implies $a \equiv b$ (modulo u) for any factor u of N. Therefore the x satisfying $x^2 \equiv m$ (modulo N) also satisfies $x^2 \equiv m$ (modulo u), and QR(m,u) is established.

Example 2.

QR(15,77) (15 is a quadratic residue modulo 77), since $13^2 - 15 = 169 - 15 = 154 = 2*77$, i.e. $x = 13$ satisfies $x^2 \equiv 15$ (modulo 77). 15 is therefore also a quadratic residue modulo 7, which divides 77. Similarly, QR(-10,77) as the calculation $12^2 + 10 = 144 + 10 = 154 = 2*77$ shows.

Knowing a quadratic residue m modulo N, where N is to be factored, thus restricts the possible divisors of N to the set

$$\{ 2 \leq u \leq [\mathrm{sqrt}(N)] \mid QR(m,u) \}, \qquad (2)$$

i.e. the set of trial divisors u for which m is a quadratic residue modulo u.

In general, only about half of the trial divisors will survive the condition QR(m,u) for a particular m. In addition, knowing several quadratic residues $m_1, \ldots, m_n$ of N with no common divisors, the restrictions imposed by each m_i is independent and only about $1/2^n$ of the divisors will be left for actual trial.

Two questions are still left open: How do we use the condition QR(m,u) imposed by a quadratic residue m modulo N to construct a sequence of trial divisors fulfilling the condition? And how do we find the necessary quadratic residues modulo N?

To answer the first question, it can be shown that the primes in $\{u \mid QR(m,u)\}$ must belong to certain arithmetic progressions with a period of at most $4*|m|$. For example, the primes in $\{u \mid QR(2,u)\}$ have one of the forms $8*k \pm 1$. These progressions have been extensively tabulated to aid the factorization process (see e.g. Kraitchik[15, vol. I, p. 164]). Since the number of arithmetic progressions a prime in $\{u \mid QR(m,u)\}$ must belong to becomes larger with m, the elimination is only practical for small m ($|m| < 200$, say).

Example 3.

As the calculation $15^2+6 = 231 = 3*77$ shows, -6 is a quadratic residue modulo 77. The primes in {u|QR(-6,u)} have one of the forms

$$24*k + \{1,5,7,11\},\ k \geq 0.$$

The only possible primes in $\{ 2 \leq u \leq [\mathrm{sqrt}(77)] \mid QR(-6,u) \}$ are therefore 5 and 7, which must be tried as divisors of N. If the quadratic residue -10 of 77 is taken into account, 5 is also eliminated, and only 7 is left over for trial.

The only problem left is finding a number of quadratic residues modulo N. It is quite easy to find some quadratic residue modulo N: Simply take a number x, square it, and reduce the result modulo N. But as the above discussion shows, only reasonably small quadratic residues are really useful for factoring N. Having some initial set of quadratic residues, new quadratic residues may be obtained by certain transformations to be described next:

If we have a quadratic residue m modulo N and $m = n*a^2$, we can show that n is also a quadratic residue modulo N: Since $QR(n*a^2,N)$, we have

$$x^2 \equiv n*a^2 \ (\mathrm{modulo}\ N) \qquad (3)$$

for some x. Now $\gcd(n*a^2,N) = 1$ by definition and therefore $\gcd(a,N) = 1$, so a has an inverse element (modulo N), i.e. a number b exists such that $a*b \equiv 1$ (modulo N). Multiplying both sides of (3) by b^2, we obtain

$$x^2 * b^2 \equiv n * a^2 * b^2 \text{ (modulo N)}$$

and using $a*b \equiv 1$

$$(x*b)^2 \equiv n \text{ (modulo N)}$$

and QR(n,N) follows. A quadratic residue can thus be reduced to its square-free part.

Example 4.

QR(60,77), since $26^2 - 60 = 8*77$. Now $60 = 2^2 * 3*5$ and removing the square 2^2, we obtain QR(15,77).

Quadratic residues can of course be multiplied to obtain new residues. Although the product at first is larger than the initial quadratic residues, common factors may form squares in the product and result in a reduced quadratic residue.

Example 5.

Multiplying the modulo 77 quadratic residues -10 and 15 we obtain QR(-150,77). But $-150 = (-1)*2*3*5^2$, so 5^2 can be removed to obtain QR(-6,77).

It remains to be specified how the initial set of quadratic residues modulo N is formed. Kraitchik[15] calculated $x^2 - k*N$ for values of x near sqrt(k*N) to obtain small residues. In Legendre's original method, the expansion of sqrt(k*N) in a regular continued fraction supplies the initial quadratic residues, as we shall see in section 3. Using the expansion idea ensures that the initial quadratic residues formed satisfy $0 < |u| < 2*\text{sqrt}(k*N)$.

In summary, N may be factored as follows:

1. Form a set of initial quadratic residues modulo N by ad hoc methods like Kraitchik or by expanding sqrt(k*N) in a continued fraction.

2. Reduce the set of quadratic residues to obtain numerically small residues. Notice that a complete prime factorization of each initial quadratic residue is necessary to perform the reduction.

3. Use each of the resulting quadratic residues to eliminate a portion of trial divisors over the entire desired range.

4. Try as divisors in N the hopefully small number of trial divisors left over from the elimination process.

The above method has been used for many years for factoring by hand calculation and is not particularly well suited for use in a computer. As shown in section 3, the information obtained by quadratic residues can be utilized in a much better way by a computer than forming trial divisor sequences. The above material is thus primarily included to ease the introduction to the continued fraction method.

2.2. Timing

The section on trial division is concluded with some information concerning the expected running time required to factor a number N by trial division without using quadratic residues. The running time obviously depends heavily on the size of N's factors. If N is a power of 2, the factorization is completed almost immediately, while if N is prime, all divisors below sqrt(N) must be tried to establish this fact.

In Knuth and Pardo[14] it is shown that the probability that the k'th largest prime factor of N is less than N^x, where x is real, $0 < x < 1/2$, approaches a limit $F_k(x)$ as N approaches infinity. The tabulated values of $F_k(x)$ given in the paper enables one to estimate the probability that the factorization will be

completed in $O(N^x)$ steps, for varying x. For example, in about 45 percent of all cases, the factorization will be completed in $O(N^{1/3})$ steps.

So although trial division is not well suited for factoring large numbers completely, the method has certain advantages:

1. The method often succeeds in quickly removing 1 or 2 small factors, reducing the size of the number and thereby the running time of the more general methods.

2. The factors produced by trial division are guaranteed to be prime. This property is not shared by any other factorization method.

3. Having trial divided N unsuccessfully up to some limit B, at least it is known that N has no factors below B. This information is not easily obtained by any other method and is useful as part of some tests for primality discussed in section 4. Also, a factor u of N discovered by other methods is known to be prime if $u < B^2$.

Trial division will be part of any factorization attempt.

3. The continued fraction method

In this section the continued fraction method for factoring large integers is described. The description is a summary of Morrison and Brillhart[22], where more detailed information can be found. The method combines Legendre's quadratic residues generated by expanding sqrt(k*N) in a continued fraction and Kraitchik's use of quadratic residues to factor without forming any sequence of trial divisors. The first more or less complete description of the method is probably the account given in Lehmer and Powers[20]. In the rest of this section, we assume that the number N to be factored is odd and composite.

We start by continuing for a moment the discussion of quadratic residues from the preceding section. Suppose that while forming the initial set of quadratic residues modulo N, a square quadratic residue is discovered. A solution to the congruence

$$X^2 \equiv Y^2 \text{ (modulo N)} \qquad (1)$$

has been found. This congruence is of course trivial if $X \equiv Y$ or $X \equiv -Y$ (modulo N), so let us assume that this is not the case. By definition, (1) implies $N \mid (X^2 - Y^2)$, so $N \mid (X-Y)*(X+Y)$. The additional requirements $X \pm Y$ and $X \pm -Y$ (modulo N) ensure that $N \not\mid (X-Y)$ and $N \not\mid (X+Y)$. But N divides the product (X-Y)*(X+Y), so gcd(X-Y,N) and gcd(X+Y,N) are proper factors of N, which can easily be calculated by Euclid's algorithm.

Example 1.

As usual N = 77. Now $36^2 - 8^2 = 1232 = 16*77$ and 77 divides neither 36+8 = 44 nor 36-8 = 28, so X = 36 and Y = 8 fulfill the above conditions. Factors of 77 can therefore be found by calculating gcd(36+8,77) = gcd(44,77) = 11 and gcd(36-8,77) = 7.

Kraitchik's idea is to find square-sets (called S-sets in Morrison and Brillhart[22] and cycles in Kraitchik[15]) defined as sets of congruences

$$X_i^2 \equiv Y_i \text{ (modulo N)}, \tag{2}$$

which, when multiplied, form an instance of (1). This principle had been known before Kraitchik, but apparently only formulated for more specialized cases.

Example 2.

With N = 77, $10^2 \equiv 23$ (modulo N) and $32^2 \equiv 23$ (modulo N). Multiplying these congruences gives $(10*32)^2 \equiv 23^2$ (modulo N) or, in reduced form, $12^2 \equiv 23^2$ (modulo N), since 10*32 mod N = 12. As before, N may be factored: gcd(12-23,77) = gcd(-11,77) = 11 and gcd(12+23,77) = 7.

Finding a square-set is closely related to the reduction performed to obtain numerically small quadratic residues. In particular, the complete factorization of the non-square side of each congruence must be available. The main difference is that while forming small quadratic residues, the square parts of the congruences are simply discarded. To use the square-set idea, all the information must be preserved.

We are now ready to present the continued fraction method in a more precise form. In the first sub-section 3.1, the algorithm for expanding sqrt(k*N) in a regular continued fraction is given. This expansion supplies the set of congruences from which square-sets will be extracted. In sub-section 3.2, the algorithm for finding square-sets is described. This algorithm assumes that the complete factorization of the non-square parts of the congruences are available.

3.1. Expansion phase

In this sub-section we describe the algorithm for expanding sqrt(k*N) into a regular continued fraction. Since a complete understanding of this algorithm is unnecessary to understand the factorization method, the algorithm will simply be presented without further comment. The reader interested in the theory behind the algorithm is referred to Knuth[13, pp. 339-343]. In this section we use almost the same notation as Morrison and Brillhart[22].

The expansion algorithm generates the tuples

$$(A_n, Q_n, q_n, r_n, P_n),\ n = 1, 2, \ldots \tag{3}$$

using the recursion formulas

$$\begin{aligned} q_{n+1} &= [(g+P_n)/Q_n] \\ r_{n+1} &= (g+P_n) \bmod Q_n \\ A_{n+1} &= (q_{n+1} * A_n + A_{n-1}) \bmod N \\ P_{n+1} &= g - r_{n+1} \\ Q_{n+1} &= Q_{n-1} + q_{n+1} * (r_{n+1} - r_n). \end{aligned} \tag{4}$$

Initially, $g = [\mathrm{sqrt}(k*N)]$, $A_{-1} = 0$, $A_0 = 1$, $Q_{-1} = k*N$, $Q_0 = 1$, $r_0 = g$, and $P_0 = 0$.

This algorithm is normally used to express sqrt(k*N) as a continued fraction, i.e.

$$\mathrm{sqrt}(k*N) = q_1 + 1/(q_2 + 1/(q_3 + \ldots)). \tag{5}$$

In the present application, the important property is the congruence

$$A_n^2 \equiv (-1)^n * Q_n \quad (\text{modulo } N), \tag{6}$$

which exactly states that $(-1)^n * Q_n$ is a quadratic residue modulo N. The advantage of using this algorithm is that the Q_n are small compared to N:

$$0 < Q_n < 2*\text{sqrt}(k*N). \tag{7}$$

We may thus with a little luck find a complete factorization of at least some of the Q_n by trial division. The pairs (A_n, Q_n) where Q_n is too difficult to factor by trial division are simply discarded. In this manner, only Q_n having small prime factors are saved for later use in the square-set construction.

We don't mind throwing away Q_n with large factors, however. The reason is that a Q_n having a large prime factor is almost worthless anyway, because a Q_m must be found having the same large prime factor, before Q_n has any chance of being part of a square-set. And such coincidences occur more infrequently, the larger factors we allow in our Q_n.

An attempt will thus be made to factor the Q_n over a relatively small fixed set of primes, called the factorbase, both to save trial divisions and to discard pairs (A_n, Q_n) having little chance of entering a square-set.

Example 3.

The following table shows some of the expansion of sqrt(k*N) for N = 77, k = 2 in a regular continued fraction (g = [sqrt(2*77)] = 12). We have also listed the complete factorization of Q_n over the factorbase {2, 3, 5} when possible.

n	A_n	Q_n	factors	q_n	r_n	P_n
-1	0	154	-	-	-	-
0	1	1	1	-	12	0
1	12	10	2*5	12	0	12
2	25	9	3*3	2	4	8
3	62	6	2*3	2	2	10
4	57	15	3*5	3	4	8
5	42	7	-	1	5	7
6	64	15	3*5	2	5	7
7	29	6	2*3	1	4	8
8	74	9	3*3	3	2	10
9	23	10	2*5	2	4	8
10	43	1	1	2	0	12
11	54	10	2*5	24	0	12
12	74	9	3*3	2	4	8
13	48	6	2*3	2	2	10
14	64	15	3*5	3	4	8
15	35	7	-	1	5	7
16	57	15	3*5	2	5	7
17	15	6	2*3	1	4	8
18	25	9	3*3	3	2	10
19	65	10	2*5	2	4	8
20	1	1	1	2	0	12
21	12	10	2*5	24	0	12
22	25	9	3*3	2	4	8

Fig. 3.1

The congruence (6) gives for n=7 that $29^2 \equiv -6$ (modulo 77), the sign appearing because n is odd.

The reader may have wondered why sqrt(k*N) is expanded and not simply sqrt(N). One reason is that the continued fraction expansion is periodic. Note, for example, that the lines for n = 2 and n = 22 in the above example are identical. It may happen that the period is short and cannot supply a sufficient number of pairs (A_n, Q_n). In this case another multiplier k must be used.

Another reason is that for a particular k, about half of the primes can beforehand be excluded as possible divisors of the corresponding Q_n (see

Morrison and Brillhart[22, p. 191]). Selecting k carefully, it may be possible to include more small primes as possible divisors of the Q_n than using k = 1. This advantage should be weighed against the resulting increased size of the Q_n for k > 1 (cf. (7)), since larger Q_n will be more difficult to factor. See Morrison and Brillhart[22, p. 200] and Knuth[13, pp. 383-384] for a discussion of the selection of k.

Also the selection of the number of small primes in the factorbase should be considered carefully. A large factorbase will produce more factored Q_n, but time may be wasted in performing numerous trial divisions in vain. On the other hand, if a too small factorbase is used, the pairs (A_n, Q_n) will be generated more slowly, since Q_n divisible by only small primes are rare. Again, refer to Morrison and Brillhart[22, p. 192] and Knuth[13, p. 384] for a discussion.

To summarize, the result of the expansion is a set of pairs (A_n, Q_n) for which (7) holds and Q_n is completely factored over the factorbase. A sufficient number of such pairs are generated to make the existence of at least a few square-sets among them likely.

For easier reference, we renumber the pairs to make the indices consecutive (remember, some of the pairs may have been thrown away) and remove the dependence of n in the congruence. Thus if

$$(A_{n_1}, Q_{n_1}), (A_{n_2}, Q_{n_2}), \ldots$$

is our set of pairs, we define

$$X_1 = A_{n_1} \qquad Y_1 = (-1)^{n_1} * Q_{n_1}$$

$$X_2 = A_{n_2} \qquad Y_2 = (-1)^{n_2} * Q_{n_2}$$

$$\cdots\cdots \qquad \cdots\cdots$$

We thus have a set of pairs (X_i, Y_i), where

$$X_i^2 \equiv Y_i \pmod{N}$$

and all Y_i have been completely factored over the factorbase and the number -1.

3.2. Finding Square-sets

In this section, we describe how square-sets are discovered among the pairs (X_i, Y_i) supplied by the expansion process.

We are interested in finding a set of indices $\{i_1, \ldots, i_k\}$ such that the product of the corresponding Y_i is a square:

$$Y_{i_1} * Y_{i_2} * \ldots * Y_{i_k} = Y^2. \qquad (8)$$

Notice that no reduction modulo N is done here. If we now set

$$X = (X_{i_1} * X_{i_2} * \ldots * X_{i_k}) \bmod N, \tag{9}$$

then

$$X^2 \equiv X_{i_1}^2 * \ldots * X_{i_k}^2 \text{ (modulo N)}, \tag{10}$$

and since

$$X_i^2 \equiv Y_i \text{ (modulo N)} \tag{11}$$

individually, we get

$$X^2 \equiv Y^2 \text{ (modulo N)}$$

precisely as desired. This congruence may fail to factor N (if $X \equiv Y$ or $X \equiv -Y$ (modulo N)), but usually several square-sets exist and we simply try one of the others. If no square-sets exist, we must go back and expand some more to get more pairs (X_i, Y_i).

The prime factorizations of the Y_i are now used to discover the index set $\{i_1, \ldots, i_k\}$ in the following way: Let $\{p_1, \ldots, p_m\}$ be the set of primes occurring in the factorizations of all the Y_i. This set includes the factorbase and the additional "prime" -1. The square free part of any Y_i is now represented by an m-dimensional row-vector V_i with elements in {0,1}. The j'th component of V_i is 1 if and only if p_j divides Y_i to an odd power. In particular, if $p_j \nmid Y_i$, then the j'th component of V_i is zero. Clearly, the

square free part of $Y_{i'} * Y_{i''}$ can be represented in the same way, by adding the vectors $V_{i'}$ and $V_{i''}$ componentwise modulo 2.

Example 4.

Consider the lines for n = 9 and n = 14 of the continued fraction expansion for sqrt(2*77) on page 17. Setting

$$X_1 = 23 \qquad Y_1 = -10 = (-1)*2*5$$
$$X_2 = 64 \qquad Y_2 = 15 = 3*5$$

for these lines and $(p_1, p_2, p_3, p_4) = (-1, 2, 3, 5)$, we have

$$V_1 = (1,1,0,1)$$
$$V_2 = (0,0,1,1).$$

Thus the 4th component of V_1 is 1 since $p_4 = 5$ divides Y_1 to an odd power, while the first component of V_2 is zero since Y_2 is positive. Multiplying the congruences, we get $(23*64)^2 \equiv -10*15$ (modulo N), where the square free part of $-10*15 = (-1)*2*3*5^2$ is clearly represented by $V_1+V_2 = (1,1,1,0)$, where we add componentwise modulo 2.

The problem of finding a square product of Y_i is equivalent to finding a sum of V_i, where all components are zeroes, since this means that all p_j divide the product to an even power.

If the sum of a set of V_i is the zero vector, this set constitutes a set of linearly dependent vectors. Such sets can be discovered by a process similar to

Gauss-elimination:

First form the matrix, where each row is a V_i. Notice that this is not necessarily a square matrix. Then reduce this matrix by adding rows to a form, where for each j, only one row has its leftmost 1 in column j. (By interchanging rows, it is thus possible to convert the matrix into an upper triangular matrix.)

This is accomplished by performing the following operation for j = 1, 2, ... , m: If more than one row has its leftmost 1 in column j, add one of these to all the others.

As the reduction proceeds, a record must be kept of the actual contents of each row as a sum of V_i. When the reduction is completed, the reduced matrix is searched for occurrences of zero rows. Each zero row corresponds to a square-set. Since each row is recorded as a sum of V_i, we can calculate X = the corresponding product (9) of X_i modulo N and Y^2 = the product (8) of the Y_i.

The square root of Y^2 is then calculated and Y reduced modulo N. (A neat algorithm for calculating Y, avoiding the square root of an extremely large number to be taken, is given in Morrison and Brillhart[22, p. 190].)

If $X \equiv Y$ or $X \equiv -Y$ (modulo N), the factorization attempt has failed and the next square-set must be tried. Otherwise N = u*v is a proper factorization, where u = gcd(X-Y,N) (or u = gcd(X+Y,N)), and v = N/u. If u and v are not both primes (see the tests for primality in section 4), different factorizations of N into 2 factors must be found using other square-sets, until all prime factors are found. If, for example, N = p*q*r with p, q, and r primes, the factorizations N = p*(q*r) and N = (p*q)*r are sufficient to discover the complete factorization.

Notice that failure to factor N should not be taken as an indication that N is prime. If N is the product of two primes, about half the square-sets will fail to factor N, so failures occur frequently. However, the expansion is usually carried to a point where several square-sets exist before processing the pairs

(X_i, Y_i). And once a few square-sets have appeared, many more will result by adding just a few more pairs.

Example 5.

Let us see the elimination process in action. For the purpose of this example, we select the congruences for n = 4, 8, 9, 14, 17 on page 17 for use. Thus

$X_1 = 57 \qquad Y_1 = 15 = 3*5$

$X_2 = 74 \qquad Y_2 = 9 = 3*3$

$X_3 = 23 \qquad Y_3 = -10 = (-1)*2*5$

$X_4 = 64 \qquad Y_4 = 15 = 3*5$

$X_5 = 15 \qquad Y_5 = -6 = (-1)*2*3$

Forming the matrix as specified above with $(p_1, p_2, p_3, p_4) = (-1, 2, 3, 5)$, we get

1	0	0	1	1
2	0	0	0	0
3	1	1	0	1
4	0	0	1	1
5	1	1	1	0

Starting in column 1, row 3 is added to row 5 to eliminate the 1 in row 5 and we get

1	0	0	1	1
2	0	0	0	0
3	1	1	0	1
4	0	0	1	1
3+5	0	0	1	1

(We record which rows are summed to the left.) Since no row has its leftmost 1 in column 2, we proceed to column 3, adding row 1 to row 4 and 5:

1	0	0	1	1
2	0	0	0	0
3	1	1	0	1
1+4	0	0	0	0
1+3+5	0	0	0	0

No row has its leftmost 1 in column 4, so the reduction is completed.

Inspecting the reduced matrix, the 2nd, 4th, and 5th rows are seen to contain only zeroes. Thus $\{(X_2, Y_2)\}$; $\{(X_1, Y_1), (X_4, Y_4)\}$; and $\{(X_1, Y_1), (X_3, Y_3), (X_5, Y_5)\}$ are square-sets, as can be seen on the record of added rows.

For the first square-set we find X = 74, Y = sqrt(3^2) = 3, but since X+Y = 77, this congruence fails to factor 77.

For the second square-set, X = (57*64) mod 77 = 29, Y = sqrt(15*15) = 15, and factorization is possible: gcd(29+15,77) = 11; gcd(29-15,77) = 7.

The last square-set fails to factor 77, since X = (57*23*15) mod 77 = 30 and Y = sqrt(15*(-10)*(-6)) = 30, so X = Y. But if we are able to verify by other means that 7 and 11 are both primes, the factorization we have already obtained is, of course, enough.

3.3. Concluding remarks

Nobody has been able to explain fully "why" this peculiar method is able to factor large numbers so successfully. Most of the time is spent in the trial division of the Q_n and many suggestions have been given to speed up this part of the work (see Knuth[13, p.384]).

A heuristic analysis in Wunderlich[40] following ideas by R. Schroeppel indicates that the continued fraction method will factor N in $O(N^{e(N)})$ operations, where e(N) is roughly sqrt(3*ln(ln(N))/ln(N)).

A more precise result has been obtained by Dixon[10], who shows that the method still works efficiently if the continued fraction apparatus is replaced by a random sequence of numbers to generate the initial quadratic residues.

Experience shows, however, that a well-tuned implementation of the continued fraction method can perform better than indicated by the above estimate. To give an impression of the performance of the continued fraction method, a table is given of the runtime required by the method in the author's implementation to factor typical numbers in the 30-51 digit range. It should be noted that the calculations are performed by a single-user experimental system (see Appendix C). Since the factoring program can be stopped and restarted easily at any time, no significant inconveniences are imposed on other users of the system.

Number of digits	Approximate time
30-31	0.3 hours
32-33	0.5 -
34-35	0.9 -
36-37	1.5 -
38-39	2.5-4.0 -
40-41	4.5-5.5 -
42-43	9.2-13.7 -
44-45	10.0-37.0 -
46-47	1.2-1.9 * 24 hours
48-49	2.5-3.5 - -
50-51	6.2-12.8 - -

Fig. 3.2

As can be seen, the running time steadily increases from less than an hour for 35 digit numbers to about 24 hours for 45 digit numbers and about a week for 50

digit numbers. An analysis of such empirical observations to obtain a formula giving the estimated running time appears in Wunderlich[40].

4. Primality testing

Having described trial division and the continued fraction method, both of which are primarily suited for discovery of factors of composite numbers, we proceed in this section to describe methods for testing a number for primality.

The recent discovery of strikingly efficient probabilistic methods for testing large numbers for primality has to some extent placed other methods in the background. Since this section is not exclusively concerned with these probabilistic methods, we emphasize that unless explicitly stated otherwise, a number declared prime by a method in this section is prime, with no inherent possibility of error.

In the first sub-section 4.1, we introduce Fermat's theorem and describe several ways to extend the theorem to obtain a primality test using prime factors of N-1, where N is the number to be tested. The theory of these tests is relatively easy to understand, with some knowledge of group theory (see Appendix A).

In the next section 4.2, we give an overview of the many extensions and generalizations of the simple tests from section 4.1. In these extended tests, knowledge of factors of $N\pm1$, N^2+1, and $N^2\pm N+1$ can be combined in the attempt to prove N prime.

In sub-section 4.3, the probabilistic tests are described. These tests require no auxiliary factorizations, but there is always a small, controllable probability that a number declared prime by such a method is composite.

In the last section 4.4, we discuss how the primality tests may be used in conjunction with the other methods.

Williams[35] gives an extensive overview of these and other methods for primality testing. This paper also contains a large bibliograpy, covering much material not mentioned here.

4.1. Using factors of N-1

In 1640, Fermat discovered that for p prime,

$$a^{p-1} \equiv 1 \text{ (modulo } p) \tag{1}$$

whenever a is not a multiple of p. (We use p, q, and r to denote primes.) This theorem is easy to prove using a little group theory (we use the notation and results from Appendix A):

Let $M_N = \{ 1 \leq x \leq N-1 \mid \gcd(x,N) = 1 \}$. As is well known, this set is a group G_N using multiplication modulo N as composition rule. If in particular N is prime, then $\text{ord}(G_N) = N-1$, since all $1 \leq x \leq N-1$ have $\gcd(x,N) = 1$.

To prove Fermat's theorem, assume that a belongs to G_p. Then $\text{ord}(a) \mid \text{ord}(G_p)$ and $\text{ord}(G_p) = k*\text{ord}(a)$ for some k. Therefore

$$a^{p-1} \bmod p = a^{\text{ord}(G_p)} \bmod p = a^{k*\text{ord}(a)} \bmod p = 1^k = 1, \tag{2}$$

and Fermat's theorem is proved for $1 \leq a \leq p-1$.

If $a = a'+k*p$,

$$a^{p-1} \bmod p = (a'+k*p)^{p-1} \bmod p = a'^{p-1} \bmod p, \tag{3}$$

since all terms except a'^{p-1} in the expansion of $(a'+k*p)^{p-1}$ by the binomial formula are divisible by p. We now select k such that a' belongs to G_p and Fermat's theorem is proved.

The converse of Fermat's theorem is unfortunately not true. For example, $4^{14} \bmod 15 = 1$, but $15 = 3*5$. But Fermat's theorem can be extended to obtain a

useful test for primality. If

$$a^{N-1} \bmod N = 1 \tag{4}$$

for some a, not a multiple of N, the implication is that ord(a)|N-1 and one way of proceeding is to test whether in fact ord(a) = N-1. This is the case, if

$$a^{m} \bmod N \neq 1 \tag{5}$$

for all $1 \leq m < N-1$ by the definition of ord(a). But the number of values a^{m} mod N to be tested is exceedingly large if N is large, so some time saving idea is needed.

Such an idea was discovered by Lehmer in 1927 (see Lehmer[18]). He extended Fermat's theorem by the condition that

$$a^{(N-1)/p} \bmod N \neq 1 \tag{6}$$

for all prime divisors p of N-1. These conditions ensure that $\mathrm{ord}(a) \nmid (N-1)/p$ for any $p|(N-1)$. But $\mathrm{ord}(a)|(N-1)$, therefore ord(a) = N-1 is the only possibility. Since $\mathrm{ord}(a)|\mathrm{ord}(G_N)$ and $\mathrm{ord}(G_N) \leq N-1$, also $\mathrm{ord}(G_N) = N-1$ and N is therefore prime. (Note: a^{m} mod N can be calculated in O(ln(m)) multiplications with reduction modulo N.)

For this test to work, the complete prime factorization of N-1 must be found, so testing N for primality rests on our ability to factor N-1. Furthermore, we must be able to find some a for which ord(a) = N-1.

The last part is seldom any problem, however: We first note that G_N is cyclic if N is prime, so an a with ord(a) = N-1 (a generator) always exists. In fact, generators are rather numerous and experience shows that if we simply try a = 2, 3, 4, ... in the above conditions, we usually find an a with ord(a) = N-1 very

quickly.

Example 1.

Let us attempt to prove the primality of N = 7 using the factors of 7-1 = 2*3. We must find an a with ord(a) = 6. First we try a = 2 and calculate: $2^{7-1} \bmod 7 = 2^{6} \bmod 7 = 64 \bmod 7 = 1$, so ord(2)|6. Unfortunately, $2^{(7-1)/2} \bmod 7 = 2^{3} \bmod 7 = 8 \bmod 7 = 1$, so ord(2) also divides 3 and therefore ord(2) < 6.

Our next choice is a = 3: $3^{7-1} \bmod 7 = 3^{6} \bmod 7 = 729 \bmod 7 = 1$, so again ord(3)|6. Also $3^{(7-1)/2} \bmod 7 = 3^{3} \bmod 7 = 27 \bmod 7 = 6$, and $3^{(7-1)/3} \bmod 7 = 3^{2} \bmod 7 = 9 \bmod 7 = 2$, so ord(3)$\not|$3 and ord(3)$\not|$2. Therefore ord(3) = 6, ord(G_7) = 6, and 7 is prime

Obtaining the complete factorization of N-1 is usually the most difficult part of proving a number prime by this method. However, already in 1914, Pocklington gave a generalization of the above condition that enables a primality test to be performed, even if the complete factorization of N-1 is not known (see Pocklington[25] and also Lehmer[18]): If

$$\begin{aligned} a^{N-1} \bmod N &= 1 \\ \gcd(a^{(N-1)/p} - 1, N) &= 1 \end{aligned} \qquad (7)$$

for some prime p dividing N-1, then all prime factors of N have the form $p^b * k+1$, where b is the highest power to which p divides N-1.

If several prime factors of N-1 are known, the implications by using this test for all of these factors may be combined: If N-1 = F*R, gcd(F,R) = 1, and the condition (7) is satisfied for each prime divisor p of F, then all prime factors of N have the form k*F+1. (Notice that a different a may be used in (7) for each p|F. By the way, one should not expect this theorem to be of any use in

factoring. Usually, if N is composite, is is difficult to find an a satisfying the first part of (7).)

Clearly, N is prime if F > sqrt(N), since the least possible prime factor of N of the form k*F+1 is F+1. Thus only the prime factors of N-1 up to sqrt(N) need be known.

In Brillhart, Lehmer and Selfridge[5], these ideas are carried considerably further. One of the interesting new ideas introduced in this paper is using the condition

$$\begin{aligned} a^{N-1} \bmod N &= 1 \\ \gcd(a^{(N-1)/R}-1, N) &= 1, \end{aligned} \qquad (8)$$

when R > 1. This condition has the same form as (7) using R as an additional "prime" factor. (8) does not imply that factors of N are of the form k*R+1, rather any prime factor q of N has the form k*r+1, where r is some prime factor of R, depending on q. This condition is useful, if it is known that all prime factors of R are above some limit B, which will be the case, if trial division to B has been attempted for factoring R.

Combining these ideas, it can be proved that if the condition (7) is satisfied for all p|F, (8) is satisfied, R has no factors below B, and B*F > sqrt(N), then N is prime. This test can be further developed to require knowledge of factors of N-1 only to about $N^{1/3}$ before N can be tested (Brillhart, Lehmer and Selfridge[5, p. 626]).

An interesting situation arises, when R (the unfactored part of N-1) itself is suspected to be prime: If $a^{R-1} \bmod R = 1$ for some a, we recursively attempt to prove the primality of R using factors of R-1. If we succeed in proving the primality of R, a complete factorization of N-1 has been obtained, and N is easily tested using (4) and (6). On the other hand, if R-1 = F'*R' with a lower bound B' on the factors of R', but F' is not large enough to settle the primality of R, the conditions (7) and (8) will usually establish the lower

bound F'*B' on the factors of R. This bound can replace B and perhaps enable N to be tested. (This idea appears in a more general form in Williams and Judd[38, pp. 168-169] and is attributed to Selfridge.)

4.2. Using factors of other numbers

In this sub-section, we give an overview of generalizations and extensions of the tests described in the previous section. The major problem with the tests given so far is that a more or less complete factorization of N-1 is required for testing N for primality. One way of proceeding is to find tests using factors of other numbers than N-1 in the proof of primality. Thus, if N-1 is difficult to factor, these other numbers might be easier.

A test requiring factors of N+1 was first discussed by Lucas[21]. It is based on the sequences U_k and V_k, known as Lucas sequences, defined by

$$U_0 = 0,\ U_1 = 1,\ U_{k+2} = P*U_{k+1} - Q*U_k,\ k \geq 0 \qquad (9)$$
$$V_0 = 2,\ V_1 = P,\ V_{k+2} = P*V_{k+1} - Q*V_k,$$

where P and Q are integers such that $D = P^2 - 4*Q \neq 0$. (Although the V_k may not occur directly in the primality tests, they are necessary to calculate the U_k efficiently, see Appendix A.)

For the sequence U_k, the following generalization of Fermat's theorem can be proved: If p is a prime not dividing 2*Q, then

$$U_{p+e} \equiv 0 \text{ (modulo p)}, \qquad (10)$$

where e = 1 or -1 depending on p and the selection of P and Q.

As for Fermat's theorem, also composite N may fulfill $U_{N+e} \bmod N = 0$, but a similar converse as (6) for Fermat's theorem may be proved for Lucas sequences:

If for properly selected P and Q

$$U_{N+1} \bmod N = 0 \tag{11}$$

and for each prime q dividing N+1

$$U_{(N+1)/q} \bmod N \neq 0, \tag{12}$$

then N is prime.

Given an N to be tested, the "proper selection" of P and Q is easy to perform. The selection ensures that e = 1 in (10), so the test depends on the factors of N+1, not N-1.

Example 2.

We try to establish the primality of N = 11 using factors of $11+1 = 2^2 * 3$. The author gives his solemn word that P = 1, Q = -4 are properly selected, i.e. such that if 11 is prime, e = 1 in (10), so the test depends on the factors of N+1 = 12 as desired. Although more efficient methods are available for calculating $U_m \bmod N$ when m is large (see Appendix A), we give the whole sequence modulo 11 for the purpose of this example:

i	U_i	U_i mod 11
0	0	0
1	1	1
2	1	1
3	5	5
4	9	9
5	29	7
6	65	10
7	181	5
8	441	1
9	1165	10
10	2929	3
11	7589	10
12	19305	0

Fig. 4.1

(For example, $U_5 = U_4 + 4*U_3 = 9+4*5 = 29$.) By inspecting this table, we find $U_{11+1} \bmod 11 = U_{12} \bmod 11 = 0$, $U_{(11+1)/2} \bmod 11 = U_6 \bmod 11 = 10 \neq 0$, and $U_{(11+1)/3} \bmod 11 = U_4 \bmod 11 = 9 \neq 0$. Therefore 11 is prime.

Had we, however, attempted to use P = 1, Q = -5 (also properly selected), the sequence would be:

i	U_i	U_i mod 11
0	0	0
1	1	1
2	1	1
3	6	6
4	11	0
5	41	8
6	96	8
7	301	4
8	781	0
9	2286	9
10	6191	9
11	17621	10
12	48576	0

Fig. 4.2

We see that although $U_{12} \bmod 11 = 0$, also $U_4 \bmod 11 = 0$, so this sequence fails to prove the primality of 11.

In Brillhart, Lehmer and Selfridge[5] more methods for testing N for primality using factors of N+1 are given. In fact, for each primality test that uses factors of N-1, a comparable test is given for the N+1 case. In particular, N can be tested for primality if the product of known factors of N+1 is about

$N^{1/3}$.

A new possibility also introduced in this paper is the idea of combining the knowledge of factors of N-1 and N+1 into a single test for primality. For example, it is shown that N can be tested for primality, if $F_1^2 * F_2^3 * B / 2 > N$ or $F_1^2 * F_2^3 * B / 2 > N$. Here $N-1 = F_1 * R_1$, $N+1 = F_2 * R_2$, so F_1 and F_2 are the completely factored parts of N-1 and N+1, respectively, and all factors of R_1 and R_2 are larger than B.

Further extensions have been shown possible in Williams and Judd[38] and [39]. These papers describe methods for testing N for primality using factors of N-1, N+1, N^2+1, and $N^2 \pm N+1$. In the last developement of these rather complicated tests, it is shown that N often can be tested for primality if $N < 1 * K^3$, where K is the product of known factors of the 5 above-mentioned polynomials in N and the factor 1 is small (see Williams and Holte[37]).

4.3. Probabilistic tests

The methods described so far for testing N for primality all require factorization to a certain extent of numbers related to N. Although most 70-100 digit numbers are within reach of these methods, larger numbers cause considerable trouble. It would be nice, then, to have primality tests not depending on the rather expensive operation of factoring.

Such a method was first given by Soloway and Strassen[32]. This method does not depend on factoring and works very efficiently, but the result of using the method is unfortunately not entirely reliable: In a very few cases, a number declared prime by the method may, in fact, be composite.

We describe here a similar method first given by Rabin[29]. For ease of reference, we define some terminology attributed to J. Brillhart in Pomerance, Selfridge and Wagstaff[28]:

A number N is probable prime to the base a, $1 < a < N$, if

$$a^{N-1} \bmod N = 1. \tag{13}$$

(For many years, the term "pseudoprime" has been used to denote a number satisfying (13). This somewhat unfortunate use of words had become "stuck", but will hopefully be abandoned with the appearance of Pomerance, Selfridge and Wagstaff[28], where "pseudoprime" means a composite probable prime.)

We also define an odd number $N = 1+d*2^s$, d odd, to be a strong probable prime to the base a, $1 < a < N$, if either

$$a^{d} \bmod N = 1 \tag{14}$$

or

$$a^{d*2^r} \bmod N = N-1 \tag{15}$$

for some r, $0 \leq r < s$.

It is easy to prove that all primes are strong probable primes to any base, so if N is not a strong probable prime for some base, N is composite (see Pomerance, Selfridge and Wagstaff[28] or Knuth[13, p. 379]).

The important point, proved by Rabin[30], is that an odd composite number can never be a strong probable prime to more than 1/4 of the possible bases. Thus, to test N for primality, select m random numbers a_i, $1 < a_i < N$, and determine whether N is a strong probable prime for all bases a_i. If for some base, N is not a strong probable prime, N is composite. Otherwise, declare N to be prime with probability of error less than $(1/4)^m$. Clearly, by selecting m large enough, the probability of erroneously declaring a composite number prime can

become as small as desired.

In Pomerance, Selfridge and Wagstaff[28], empirical results are presented concerning composite strong probable primes to small, preselected bases. A composite strong probable prime is called a strong pseudoprime. It is shown, for example, that only 13 numbers below $25*10^9$ are strong pseudoprimes to all of the bases 2, 3, 5; only one of these is also strong pseudoprime to the additional base 7; and none survives if, finally, the base 11 is included. Thus we can say that any number N below $25*10^9$ is prime if and only if N is a strong probable prime to all the bases 2, 3, 5, 7, and 11.

In Pomerance, Selfridge and Wagstaff[28], a Lucas probable prime is defined to be a number N such that

$$U_{N+1} \bmod N = 0,$$

for properly selected P and Q (see section 4.2 for Lucas sequences and also Baillie and Wagstaff[2]). It is found that no number N below $25*10^9$ is a strong pseudoprime to the base 2 and at the same time Lucas probable prime using a fixed algorithm for selecting P and Q appropriately. In fact, no such number has yet been found, so perhaps the combination of strong probable primality and Lucas probable primality is a sufficient condition for primality.

4.4. Applying primality tests

How are such tests used, then, in conjunction with the factorization methods?

First of all, before too much effort is spent searching for factors of the number N to be factored, test whether N is a probable prime to some small base, say 3, i.e. see if $3^{N-1} \bmod N = 1$. If N is not a base 3 probable prime, N is composite, and the factorization attempts continue. If, on the other hand, N is a probable prime to the base 3, N is suspected to be prime and the methods of this section should be used in an attempt to establish the primality of N.

The same test should also be applied whenever factors of a composite number are discovered.

Depending on one's view or intended "use" of N, it may be sufficient to test our base 3 probable prime using Rabin's probabilistic method. On the other hand, it is surely more satisfactory to establish the primality of N once and for all with no possibility of error, particularly if N is to be published in a factorization of general interest. Also, if N is a probable prime to the base 3, this is in practice a very strong indication that N is prime. Rabin[30] proves that a composite N will be strong probable prime to at most 1/4 of the possible bases, but the number of such bases will usually be much smaller.

Thus, in the author's experience, while factoring hundreds of numbers, no N has ever turned up satisfying the following conditions: N is provably composite; N is large (more than 20 digits, say); and N is probable prime to base 3. (Most of the base 3 probable primes the author has met, have been proved prime using the non-probabilistic methods, while lower bounds on the factors have been produced for the rest, using the methods of Brillhart, Lehmer and Selfridge[5].)

In other words, if the author meets a large base 3 probable prime N, he "knows" that N is prime, and no additional strong probable prime tests will increase his confidence in this conclusion. Rather, he attempts to produce sufficient material to establish the primality of N once and for all.

5. Pollard's methods

In this section, we describe briefly two simple methods for factoring discovered by J. M. Pollard. Each of these methods may succeed in finding a fairly large factor of the number N to be factored. In the rest of this section, N is assumed composite.

The P-1 method

The first simple method is given at the end of Pollard[26]. It is based on the idea that if p-1 divides Q, then p divides $a^Q - 1$ for a not a multiple of p. To see why, write (p-1)*k = Q for some k. Then

$$a^Q \bmod p = a^{(p-1)*k} \bmod p = 1^k \bmod p = 1, \qquad (1)$$

because $a^{p-1} \bmod p = 1$ by Fermat's theorem. Therefore $(a^Q - 1) \bmod p = 0$ or p divides $(a^Q - 1)$.

If p-1 divides Q for some prime factor p of N, we can find p by calculating

$$b = a^Q \bmod N \qquad (2)$$
$$d = \gcd(b-1, N)$$

for some small a. By (1), p divides b-1 and since p divides N, we have p dividing d. (If $q-1 \mid Q$ for some other prime factor q of N, we also have q dividing d. Thus we may find a product of prime factors of N instead of just a single prime factor.)

To attempt a factorization of some number N, we must decide on a value of Q. Unfortunately, given some N, it is apparently not easier to discover the factors of p-1 for some prime factor p of N than finding p itself. We can only hope

that the prime factors of p-1 are not too large for some p dividing N, just as we hope that the factors of N are small when attempting to factor N by trial division.

We therefore use

$$Q = p_1^{c_1} * p_2^{c_2} * \ldots * p_m^{c_m}, \tag{3}$$

where p_i is the i'th prime and $c_i > 0$, up to some prime p_m. The c_i should be chosen large enough to make $p_i^{c_i+1} \nmid (p-1)$ unlikely. For sufficiently large i, $c_i = 1$ is surely enough, while for small i, c_i should be larger.

The method fails if d = N, i.e. if N is the product of primes p all having $p-1 \mid Q$. In this case, a smaller Q should be tried.

In practice, we calculate the sequence

$$b_1 = 3, \quad b_{i+1} = b_i^{(p_i^{c_i})} \bmod N, \quad i > 0 \tag{4}$$

and then calculate

$$d_i = \gcd(b_i - 1, N) \tag{5}$$

at regular intervals. For example, we might calculate d_{100}, d_{200}, ... etc. If $1 < d_i < N$, we have found the desired factorization, while the calculations are continued if $d_i = 1$. If $d_i = N$, we backtrack to the previous d_i and calculate the intervening d_i individually.

Example 1.

Returning to N = 77, we choose all $c_i = 1$ in the attempt to factor 77. The following table shows how the calculations proceed:

i	p_i	b_i	d_i
1	2	3	1
2	3	9	1
3	5	36	7
4	7	1	77

Fig. 5.1

For example, $b_3 = 9^3 \bmod 77 = 36$ and $d_3 = \gcd(36-1,77) = 7$.

If the number to be factored has the form $N = a^n \pm b^n$, we mentioned in section 2 that the non-trivial prime factors of N have the form p = 2*k*n+1. Thus the P-1 method will succeed more often on such N, since p-1 is always divisible by 2*n. It may be advisable to use $b_1 = 3^{2*n} \bmod N$ is these cases.

It is difficult to say anything general about the runtime required by the P-1 method to factor a number N. Potentially, the method is able to discover factors as large as Q+1, but in many cases, p-1 has a large prime factor for all p dividing N. In these cases, the factorization of N by the P-1 method is very time consuming.

The Rho-method

The other simple method is from Pollard[27]. The method is based on Floyd's cycle-finding algorithm given in Knuth[13, exercise 3.1-6b].

Let f(x) be any polynomium with integer coefficients and consider the sequences

$$x_0 = y_0 = A,\ x_{m+1} = f(x_m) \bmod N,\ y_{m+1} = f(y_m) \bmod p, \qquad (6)$$

where p is any prime divisor of the number N to be factored. Since $0 \leq y_m < p$, the sequence y_m will eventually repeat itself, i.e. we find $y_m = y_{m+n}$ for some $m \geq 0$ and $n > 0$. From this point, $y_{m+i} = y_{m+n+i}$ for all $i \geq 0$.

Floyd has shown that for any periodic sequence like y_m, a j exists such that $y_{2*j} = y_j$. At this point, p divides $x_{2*j} - x_j$, since $y_m = x_m \bmod p$, and therefore p divides $\gcd(x_{2*j} - x_j, N)$.

The method selects some $u_0 = v_0 = A$ and calculates

$$u_i = f(u_{i-1}) \bmod N$$
$$v_i = f(f(v_{i-1})) \bmod N$$
$$d_i = \gcd(u_i - v_i, N)$$

for $i > 0$, until hopefully finding $d_i > 1$.

What is the expected number of steps this method requires to find a factor p of N? In Knuth[13, pp. 7-8] it is shown that if f(x) is a random mapping, the average value of j such that $y_{2*j} = y_j$ will be of the order sqrt(p). If we select a quadratic polynomium for f, e.g. $f(x) = x^2 + 1$, experience shows that this estimate in fact holds, although f is not really random. This method will therefore usually find a factor p of N in O(sqrt(p)) steps, where each step consists of 2 multiplications modulo N and calculating a gcd. In fact, most of these calculations of greatest common divisors can be replaced by multiplications modulo N as suggested in Pollard[27].

Recently, Brent[3] has discovered an improved cycle-finding method which leads to a factorization method about 24 percent faster than using Floyd's method.

Example 2.

We select $f(x) = x^2+1$, $u_0 = v_0 = 1$ for factoring N = 77. The calculations proceed as follows:

i	u_i	v_i	$v_i - u_i$	$\gcd(v_i - u_i)$
0	1	1	0	77
1	2	5	3	1
2	5	61	56	7
3	26	61	35	7
4	61	61	0	77
5	26	61	35	7

Fig. 5.2

So the factor 7 is discovered after 2 iterations.

6. Combining the methods

In this section, we illustrate how the numerous factorization methods can be combined, by applying the methods to factor some rather large numbers, all different from 77.

The numbers selected for factorization are obtained from the sequence of primes p_i, defined by Mullin[23]: Let $p_1 = 2$, and define, for $i > 1$

$$q_i = p_1 * p_2 * \ldots * p_{i-1} + 1 , \qquad (1)$$

p_i = largest prime factor of q_i.

Thus the i'th element of the sequence can be obtained by factoring q_i.

The first few elements of the sequence are easily obtained:

i	q_i	p_i
1	-	2
2	3	3
3	7	7
4	43	43

Fig. 6.1

For example, $q_4 = 2*3*7+1 = 43$ is prime, as is easily verified by trial division, and we get $p_4 = 43$ (the largest prime factor of 43).

Coming to $q_5 = 2*3*7*43+1 = 1807$, trial division shows that $1807 = 13*139$ with 139 prime, so $p_5 = 139$. Also p_6 and p_7 can be obtained using trial division for factoring q_6 and q_7:

i	q_i	factors of q_i	p_i
5	1807	13*139	139
6	251035	5*50207	50207
7	12603664039	23*1607*340999	340999

Fig. 6.2

Continuing, we calculate

$$q_8 = 4297836833293963.$$

Using trial division up to 10000, we find

$$q_8 = 23 * 79 * q_8',$$
$$q_8' = 2365347734339.$$

Since $3^{q_8'-1} \bmod q_8' = 1$, we strongly suspect that q_8' is prime and therefore attempt to factor $q_8'-1$ to prove q_8' prime using the methods of section 4.1. Trial division shows that

$$q_8'-1 = 2 * q_8''$$
$$q_8'' = 1182673867169$$

with no other factors below 10000. But we find $3^{q_8''-1} \bmod q_8'' = 1$ and therefore calculate

$$q_8''-1 = 2^5 * q_8'''$$

$$q_8''' = 36958558349$$

and since also q_8''' is a base 3 probable prime, finally

$$q_8'''-1 = 2^2 * 17 * 1511 * 359701.$$

This is our first complete factorization. Using these factors, we find (see section 4.1):

i	p_i	$3^{(q'''-1)/p_i} \bmod q_8'''$
1	2	36958558348 ($\equiv -1$)
2	17	25801290698
3	1511	12038366693
4	359701	30101748291

Fig. 6.3

Thus ord(3) = $q_8'''-1$ and q_8''' is prime.

Now the factorization of $q_8''-1$ is complete, and a similar calculation shows that q_8'' is also prime. Yet another of these calculations shows that q_8' is prime using the completed factorization of $q_8'-1$, so

$$q_8 = 23 * 79 * 2365347734339$$

is a complete factorization, and

$$p_8 = 2365347734339.$$

Now the numbers become really large. We find

$$q_9 = 17 * q'_9$$
$$q'_9 = 597992859775916203474633007$$

with no other factors below 10^6. Unfortunately, q'_9 is not a base 5 probable prime, and therefore not prime, so we have to find a factor of this 27 digit number. Using Pollard's P-1 method, we discover the factor q''_9 of q'_9:

$$q''_9 = 127770091783.$$

This factorization is manageable, since the factors of

$$q''_9-1 = 2 * 3 * 41 * 17923 * 28979$$

are reasonably small. This factorization of q''_9-1 can also used to prove q''_9 prime. But the factors of q'_9 are known to exceed $B = 10^6$ and therefore the factors of q''_9, being a divisor of q'_9, must also exceed B. Since $q''_9 < B^2 = 10^{12}$, we can thus immediately conclude that q''_9 is prime, without performing any primality test.

We are left with

$$q_9 = 17 * 127770091783 * q_9'''$$

$$q_9''' = 46802256414711 29$$

and fortunately q_9''' is a base 3 probable prime. We prove that q_9''' is actually prime using the factorizations

$$q_9'''-1 = 2^3 * 7 * 83 * q_9''''$$

$$q_9'''' = 1006933227511$$

with q_9'''' proved prime using

$$q_9''''-1 = 2 * 3 * 5 * 7 * 1483 * 3233257.$$

Thus q_9''' is the largest prime factor of q_9, and

$$q_9 = 17 * 127770091783 * 46802256414711 29$$

is a complete prime factorization. Hence

$$p_9 = 46802256414711 29.$$

We are now ready to find p_{10} and calculate

$$q_{10} = 89 * 839491 * 556266121 * q'_{10}$$
$$q'_{10} = 114478267940052360053963923 7,$$

where q'_{10} is composite. The largest factor 556266121 was found using a few thousand iterations of Pollard's Rho method. Neither continuing the Rho method nor using the P-1 method within reasonable limits produce more factors of q'_{10}, so we must rely on the continued fraction method to factor this 28 digit number. About 10 minutes of continued fraction expansion is sufficient to find

$$q'_{10} = q''_{10} * q'''_{10},$$
$$q''_{10} = 836312735653,$$
$$q'''_{10} = 1368845206580129,$$

where the factors are proved prime using the factorizations

$$q''_{10}-1 = 2^2 * 3 * 179 * 4211 * 92459,$$
$$q'''_{10}+1 = 2 * 3 * 5 * 131 * q''''_{10},$$
$$q''''_{10}-1 = 2^2 * 3 * 5 * q'''''_{10},$$
$$q'''''_{10}-1 = 2 * 3 * 137 * 293 * 24103.$$

Notice that $q'''_{10}+1$ was used instead of $q'''_{10}-1$ to prove the primality of q'''_{10}. Also, had we been a little more patient, Pollard's P-1 method would have discovered q''_{10}, since the prime factors of $q''_{10}-1$ are not too large.

Thus we have q_{10} completely factored:

$$q_{10} = 89 * 839491 * 556266121 * 836312735653 * 1368845206580129$$

and

$$p_{10} = 1368845206580129$$

To find p_{11} (Reader, are you still with us?), we calculate

$$q_{11} = 1307 * q'_{11}$$
$$q'_{11} = 4982995137009568184369075814598250139640628982618679807 7,$$

and the 56 digit q'_{11} is composite. Neither trial division nor extensive use of Pollard's methods produce any factors of q'_{11}, so we must sit down for a few months or so, waiting for a sufficient continued fraction expansion. After a total expansion time of about 35 * 24 hours (this happened between September 27. and November 29. 1978), the prime factorization

$$q'_{11} = 560302394853703828058 87 * 889340324577880670089824574922371$$

was discovered. (We spare the reader another boring session of auxiliary factorizations, establishing the primality of each of these factors.)

Therefore

$$p_{11} = 889340324577880670089824574922371.$$

Finally,

$$q_{12} = 11 * q'_{12},$$

$$q'_{12} = 526552101441922187274938173986568879512780073240 9-$$

$$4989279256866973951973060775459738108526 09$$

and no factors of q'_{12} can easily be discovered. Since q'_{12} is a 91 digit number, the continued fraction method is out of the question, and we must stop here. Summarizing, we have found:

i	p_i
1	2
2	3
3	7
4	43
5	139
6	50207
7	340999
8	2365347734339
9	4680225641471129
10	136884520658 0129
11	889340324577880670089824574922371

Fig. 6.4

with little hope of ever finding p_{12}. Notice that $p_{10} < p_9$, so one of Mullin's questions concerning the sequence, namely if it is ascending, can be answered with "No".

In summary, an attempt to factor a large number N roughly follows the following procedure:

1. Trial divide to 10^6. If the current trial divisor at some point exceeds the square root of the remaining factor, the factorization is completed.

2. Use Pollard's two methods simultaneously. Since each of the methods can be broken into smaller steps, we simply execute one step from each alternately. In the author's implementation, a "step" takes about 1-5 minutes of execution time and comprises either 10000 iterations of the Rho method or increasing the product Q in the P-1 method by all primes in an interval of 20000.

   In the author's experience, none of the methods, executing in this manner, have any significant tendency to find more factors than the other, although the P-1 method with luck is able to discover much larger factors than the Rho method.

   Composite factors occur, but usually their prime factorization can be discovered by renewed trial division or by using the "opposite" method of the one that discovered the composite factor.

   If the number is outside the reach of the continued fraction method (more than about 55 digits), we usually give up after having performed $5*10^5$ iterations of the Rho method and Q in the P-1 method is the product of all primes below 10^6.

3. Having executed a suitable number of steps of Pollard's methods (fewer steps for smaller numbers), we use the continued fraction method, if the size of the number allows the factorization to be completed within reasonable time. At an early point of the expansion, it is possible to obtain a rather accurate estimate of the expansion time required to complete the factorization. This estimate serves to relieve the tension and makes the operator less impatient. Only in very few cases has a number factored by the continued fraction method turned out to be the product of more than two primes.

4. After the first few trial divisions, we test whether N is a probable prime to the base 3. This test is also performed on both factors of a newly discovered factorization, except that factors discovered by trial division are not tested, since they are known to be prime.

   The author has implemented the primality tests from Brillhart, Lehmer and Selfridge[5] that use factors of $N\pm1$. Therefore, the factorization of both these numbers is attempted simultaneously. If a complete factorization of one of these numbers is found or sufficient factors are discovered to test N for primality, the factorization attempts are interrupted and N is tested for primality. We shall not discuss the possibility that N turns out to be composite, since this almost never happens anyway.

The basic difference between the above strategy for factoring and the strategies described elsewhere is the systematic use of Pollard's methods instead of using extensive trial division and the difference of squares method. (The difference of squares method attempts to find a representation of N as $N = x^2 - y^2 = (x-y)*(x+y)$; see for example Brillhart and Selfridge[6].) Apparently, Pollard's P-1 method has been used previously only to discover factors of numbers related to a number N in the attempt to prove N prime (see for example Williams and Judd[38] and [39]). Also, Brent's improvement of Pollard's Rho method was used recently to discover the factorization of $2^{256}+1$ (see Brent and Pollard[4]).

The present project in fact started by investigating many known factorizations to discover whether they could have been obtained more easily using Pollard's P-1 method. Encouraged by the results of this investigation, the author decided to include the P-1 method in his strategy. Also, the Rho method turned out to be generally superior to extensive trial division and was also included.

Although the Rho method is able to discover factors faster than the trial division method, we lose the advantage of being able to set a lower limit on the factors of the number to be factored. By a rather extensive calculation it would be possible to give a table of the smallest prime not discovered by the

Rho method after a certain number of iterations, but the author has not performed these calculations.

Pollard's methods have produced new factorizations in many cases where the use of other methods would have been too expensive. For example, the factorization of the 67 digit composite factor of the Lucas number V_{352} was completed by the discovery of a 22 digit prime factor using the P-1 method (see Appendix E). And the Rho method discovered a 12 digit factor of the 60 digit Mersenne number $2^{199}-1$ (see Appendix F). Pollard's methods have also succeeded in some cases to discover a large factor of some number, thereby bringing the remaining factor within reach of the continued fraction method.

Another difference in the above strategy is the large numbers we allow to be factored by the continued fraction method. The author has not seen larger numbers factored by the continued fraction method than the 45 digit Mersenne number $2^{149}-1$. The factorization of $2^{149}-1$ is attributed to R. Schroeppel in Brillhart, Lehmer and Selfridge[5]. The main reason we are able to factor much larger numbers is that a reasonably fast computer is available which can be used almost exclusively for factorization (see Appendix C).

7. Results

This section describes the results obtained by the author using the factorization methods given in the previous sections.

The first sub-section 7.1 is concerned with so-called algebraic factors. In many factorization projects, the numbers attacked have the form $a^n \pm b^n$. Numbers of these forms often have a priori factorizations easily obtained by manipulating the expressions $a^n - b^n$ and $a^n + b^n$ (for example, $a^{2*n} - b^{2*n} = (a^n - b^n)*(a^n + b^n)$). Such factorizations reduce the overall effort of the factorization attempt.

Sub-section 7.2 describes the format of the factorization tables given in Appendices D-I.

Section 7.3 is concerned with Fibonacci and Lucas numbers. We give some references containing earlier work on these numbers. Section 7.4 contains similar information for numbers of the form $2^n \pm 1$.

Finally, in section 7.5, we prove the primality of a large probable prime discovered by Williams[36].

7.1. Algebraic factors

For various reasons, many of the numbers attacked in factorization projects have one of the forms $a^n - b^n$ or $a^n + b^n$. This section briefly discusses the possibility of discovering a priori factorizations (algebraic factorizations) of numbers of these forms.

Consider first the formulas

$$x^2 - y^2 = (x-y) * (x+y)$$

$$x^3 - y^3 = (x-y) * (x^2+x*y+y^2)$$

$$x^4 - y^4 = (x-y) * (x^3+x*y^2+x^2*y+y^3)$$

and so on. If we set $x = a^n$ and $y = b^n$, we obtain factorizations of $a^{k*n} - b^{k*n}$.

In general, it can be shown that $a^m - b^m$ divides $a^n - b^n$ if and only if m divides n.

Example 1.

Consider $N = 2^6 - 1 = 63$. Setting a = 2 and b = 1 we get $N = a^6 - b^6$. Since $6 = 2*3$, $a^2 - b^2 = 3$ and $a^3 - b^3 = 7$ divide 63. Removing these factors, we obtain $2^6 - 1 = 3^2 * 7$. (We also have $a^1 - b^1$ dividing 63, but this is useless since a-b = 1.)

We define an algebraic factor of $a^n - b^n$ to be some d > 1 dividing $a^n - b^n$ which also divides $a^m - b^m$ for some m, $0 < m < n$. Non-algebraic factors are called primitive.

For $a^n + b^n$, we observe that $a^n + b^n = a^n - (-b)^n$ whenever n is odd. Thus $a^m + b^m$ divides $a^n + b^n$ if m divides n and n/m is odd. The converse can also be shown, i.e. if $a^m + b^m$ divides $a^n + b^n$, then m divides n and n/m is odd.

Example 2.

We show that $2^n + 1$ has non-trivial algebraic factors if n is divisible by an odd prime: Let n = p*m, where p is an odd prime. Now, $2^m + 1$ divides $2^n + 1$ because n/m = p is odd, and since $m \geq 1$, we have $2^m + 1 \geq 3$. (In particular $2^n + 1$ is divisible by 3 if n itself is an odd prime.) Consequently, $2^n + 1$

cannot be prime unless $n = 2^k$.

We also define a factor $d > 1$ dividing a^n+b^n to be algebraic if d divides a^m+b^m for some m, $0 < m < n$.

The final kind of algebraic factorization is the so-called Aurifeuillian factorizations. Already Euler in 1742 noted the identity $a^4+4*b^4 = (a^2+2*a*b+2*b^2) * (a^2-2*a*b+2*b^2)$. Apparently, Aurifeuille was the first to discover, about 1871, that setting $a = 1$ and $b = 2^k$, we get

$$2^{4*k+2}+1 = (2^{2*k+1}-2^{k+1}+1) * (2^{2*k+1}+2^{k+1}+1)$$

which is applicable to every fourth number of the form 2^n+1. Lucas generalized this factorization about 1878 to obtain numerous similar results. We shall not discuss Aurifeuillian factorizations in detail here. See Cunningham and Woodall[8] for further information.

7.2. Table format

The factorization tables are given in Appendices D-I. Each table gives the factorization as far as known to the author of a particular class of numbers. Each class is indexed by a variable, perhaps restricted to the odd numbers. All numbers in a particular class having its index within specified bounds are included in the corresponding table. For each number, we give its index followed by its factors.

All factors are prime, unless enclosed in parenthesis or square brackets. Factors in parenthesis are composite, while those in square brackets are probable primes to at least one base. No composite factors have less than 54 digits, while the probable primes are generally somewhat larger.

Factors are normally separated by "*". If algebraic factors are present, however, they appear before the primitive factors, and the last algebraic factor

is separated from the first primitive factor by ":". To compress the table, we use "^" for exponentiation instead of raising the exponent.

Very large numbers may be written on more than one line. A number is continued on the next line if terminated by "-".

We have put an "*" immediately before the index of the more interesting factorizations. Interesting factorizations are those which have not, to the best of the author's knowledge, been published or mentioned before and which have their second-largest known primitive prime factor larger than 10^{10}.

The tables have been generated by a program written for the occasion. This program takes as input a "raw" list permanently residing on a machine-readable medium. The list is updated by one of the factorization programs when a new factorization is found. As a safeguard, the table-generating program also checks that factors occurring in the raw list really divide the intended number. Thus the tables are believed to be free of errors.

To make this work manageable, we can unfortunately not give due credit to the original discoverer of the many known factorizations appearing in the tables. We give references to a few main sources in the sections below and also mention that many factorizations are known for numbers with indices outside the limits of the present tables.

Finally, we have not given any details of the actual methods used to obtain the various factorizations. Hopefully, the examples given in section 6 are sufficient to demonstrate our general strategy.

7.3. Fibonacci and Lucas numbers

The Fibonacci sequence 0, 1, 1, 2, 3, 5, 8, 13, ... in which the next number is the sum of the preceding two was used by Leonardo Pisano (Fibonacci) in 1202 in a problem on the number of offspring of a pair of rabbits. Since about 1878 when Lucas showed that the more general recurring sequences discussed in section 4.2 are useful for testing large numbers for primality, Fibonacci's sequence and its companion sequence (the Lucas sequence) 2, 1, 3, 4, 7, 11, 18, 29, ... have

been investigated.

Formally, the sequences are defined by:

$$U_0 = 0,\ U_1 = 1,\ U_{n+2} = U_{n+1} + U_n,\ n \geq 0$$
$$V_0 = 2,\ V_1 = 1,\ V_{n+2} = V_{n+1} + V_n.$$

These sequences are thus special cases (P = 1, Q = -1) of the sequences discussed in section 4.2.

It is easy to prove the following closed forms of the n'th terms of the sequences:

$$U_n = (a^n - b^n)/\mathrm{sqrt}(5),$$
$$V_n = a^n + b^n,$$
$$a = (1+\mathrm{sqrt}(5))/2,\ b = (1-\mathrm{sqrt}(5))/2.$$

These formulas show that the elements of the Fibonacci and Lucas sequences may have algebraic factors.

We showed in section 7.1 that 2^n+1 has algebraic factors if n is divisible by an odd prime. This argument is not valid for V_n, however, since $V_1 = 1$ (in contrast to $2^1+1 = 3$). Thus V_n has algebraic factors if n is composite and $n \neq 2^k$.

The table for U_n (Appendix D) covers the factorization of U_n for odd n, $1 \leq n \leq 399$. For even indices, $U_{2*n} = U_n * V_n$, and the factorization of U_{2*n} can therefore easily be deduced from other entries.

Integer Factorization

The following Aurifeuillian-like factorization is given in Jarden[11]:

$$V_{10*k+5}/V_{2*k+1} = (5*U_{2*k+1}^2 - 5*U_{2*k+1} + 1) * (5*U_{2*k+1}^2 + 5*U_{2*k+1} + 1)$$

This identity is helpful for factoring every 10'th Lucas number. We ought perhaps (like Jarden) to give separate tables for each of these two factors, but instead the reader is simply warned that factorizations of V_{10*k+5} may appear overly impressive. The table for V_n (Appendix E) covers all n, $0 \leq n \leq 500$.

Factorization tables for U_n and V_n are given in Jarden[11, pp. 36-59], which also contains a history of the investigation of these numbers.

Further factorizations appear in Morrison and Brillhart[22], while many probable prime divisors of Fibonacci and Lucas numbers are proved prime in Williams and Judd[38] and [39] and Williams and Holte[37]. The author has been able to verify many of these primality proofs using the methods in Brillhart, Lehmer and Selfridge[5]. The exceptions are the probable prime divisors of U_n for $n \geq 400$ (since they have not been investigated by the present author), and V_n for n = 368, 388, 403, 443, 446, and 470. For the 62 digit probable prime divisor of V_{307}, $N = V_{307}/1229$, for example, the primality test was made possible by the discovery of a 10 digit factor of N+1 using Pollard's Rho method. Similarly, an additional 12 digit factor of N+1 was discovered by Pollard's P-1 method for N = the 76 digit probable prime divisor of V_{476}.

7.4. 2^n-1 and 2^n+1

Numbers (and particularly, primes) of the form 2^n-1 have been extensively investigated since Euclid about 2200 years ago showed that $2^{n-1}*(2^n-1)$ is a perfect number if 2^n-1 is prime. A perfect number is the sum of all divisors of

the number, excluding the number itself as divisor. For example, for $n = 2$, $2^n-1 = 3$ is prime and therefore $2^{n-1}*(2^n-1) = 2*3 = 6$ is a perfect number. We may verify this by adding the divisors of 6 (excluding 6 itself): $1+2+3 = 6$.

In 1644, Mersenne gave his famous statement that 2^n-1 is prime for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$, and 257 and composite for all other $n \leq 257$ (see Dickson[9, pp. 12-13]). Therefore numbers of the form 2^n-1 are known as Mersenne numbers, sometimes only if n is prime, at other times only if n is one of the 55 primes below 257. (The reader can check for himself in Appendix F the degree of correctness of Mersenne's statement.)

If $N = 2^n-1$, the factors of $N+1 = 2^n$ are, of course, readily available, and this fact has been used to develop specialized primality tests for these numbers (see Lucas[21] and Lehmer[19]). In fact, since Lucas in 1872 stated that $2^{127}-1$ is prime, the largest known primes have always been of this form, except for a few months in 1951. Currently, the largest known prime is $2^{44497}-1$. (The corresponding idea can unfortunately not be used as successfully to discover large primes of the form $N = 2^n+1$ using the factors of $N-1$, since 2^n+1 cannot be prime unless $n = 2^k$.)

As for Fibonacci's sequence, we give only the factorization of 2^n-1 in the range $1 \leq n \leq 299$ for odd n, since $2^{2*n}-1 = (2^n-1)*(2^n+1)$ (see Appendix F).

The Aurifeuillian factorization

$$2^{4*k+2}+1 = (2^{2*k+1}-2^{k+1}+1) * (2^{2*k+1}+2^{k+1}+1)$$

is valid for every fourth 2^n+1. Therefore, in addition to the factorization table for 2^n+1 for all n, $0 \leq n \leq 300$ (Appendix G), we give tables for $2^n-2^{(n+1)/2}+1$ and $2^n+2^{(n+1)/2}+1$ for odd n, $1 \leq n \leq 299$ (Appendices H and I). Thus, the factorization of $2^{4*k+2}+1$ appear twice if $0 \leq 4*k+2 \leq 300$.

For the early investigation of numbers of the form $2^n \pm 1$, see Cunningham and Woodall[8], Dickson[9], Archibald[1], Kraitchik[16], and Uhler[34]. For the more recent results, see Brillhart and Selfridge[6], Brillhart, Lehmer and Selfridge[5], Brent and Pollard[4], Cormack and Williams[7], and the references given there. The last two papers are concerned with the factorization of the numbers $F_k = 2^n+1$ where $n = 2^k$, called Fermat's numbers. Notice that $2^{3*n}+1 = (2^n+1) * (2^{2*n}-2^n+1)$ (and similarly for $2^{3*n}-1$), so factorization tables often only specify the last factor.

7.5. A large prime

In a paper concerning primes with interesting digit patterns, Williams[36] discusses numbers of 4 different forms and tabulates primes of these forms which have no more than 100 digits. The tables include all such primes, except for an 84 digit base 13 probable prime which was not settled, because too little information was found to demonstrate its primality, even using the tests of Williams and Judd[38] and [39], as extended by Williams and Holte[37].

The number in question is N(83,3), where

$$N(n,r) = (10^{n+1}+9*r-10)/9, \quad (1 \leq r \leq 9).$$

In decimal notation, N(83,3) appears as the interesting string of 83 unit digits followed by the digit 3.

The author attempted to prove the primality of N(83,3) using factors of N(83,3)-1 and N(83,3)+1 and discovered that

$$N(83,3)-1 = 2^3 * 1531 * 7618224009731 * R_1$$

$$N(83,3)+1 = 2 * 3 * 187250699177 * R_2.$$

The largest factors of N(83,3)-1 and N(83,3)+1 were found using Pollard's P-1 method, while the smaller factors were given by Williams. Although the additional factors would probably be sufficient for Williams' tests to work, a lower bound of about $3*10^{12}$ would have to be established on the (composite) remaining factors R_1 and R_2 for the N±1 tests to succeed.

At this point, it was discovered that N(83,3)-1, surprisingly enough, has an algebraic factorization:

$$N(83,3)-1 = (10^{84}+8)/9 = ((10^{28})^3+2^3)/9 = (10^{28}+2)*(10^{56}-2*10^{28}+4)/9.$$

This factorization applies to N(3*m+2,3) in general. The large factor of N(83,3)-1 divides $10^{28}+2$ and gives the complete factorization

$$10^{28}+2 = 2 * 3 * 1531 * 142895917147 * 7618224009731$$

and therefore the additional factor 142895917147 of N(83,3)-1.

With these factors, a lower bound of 50 on the (still composite) remaining factors of N(83,3)±1 was sufficient to prove N(83,3) prime.

References

[1] R. C. Archibald, "Mersenne's Numbers," Scripta Math., 3(1935), 112-119.

[2] R. Baillie and S. S. Wagstaff, "Lucas Pseudoprimes," Math. Comp., 35(1980), 1391-1417.

[3] R. P. Brent, "An Improved Monte Carlo Factorization Algorithm," BIT, 20(1980), 176-184.

[4] R. P. Brent and J. M. Pollard, "Factorization of the Eighth Fermat Number," Math. Comp., 36(1981), 627-630.

[5] J. Brillhart, D. H. Lehmer and J. L. Selfridge, "New Primality Criteria and Factorizations of $2^m \pm 1$," Math. Comp., 29(1975), 620-647.

[6] J. Brillhart and J. L. Selfridge, "Some Factorizations of $2^n \pm 1$ and Related Results," Math. Comp., 21(1967), 87-96.

[7] G. V. Cormack and H. C. Williams, "Some Very Large Primes of the Form $k*2^m+1$," Math. Comp., 35(1980), 1419-1421.

[8] A. J. C. Cunningham and H. J. Woodall, "Factorization of $(y^n \pm 1)$," London, 1925.

[9] L. E. Dickson, "History of the Theory of Numbers," vol. 1, New York, 1952.

[10] J. D. Dixon, "Asymptotically Fast Factorization of Integers," Math. Comp., 36(1981), 255-260.

[11] D. Jarden, "Recurring Sequences," 3rd ed., Riveon Lematematica, Jerusalem, 1973.

[12] D. E. Knuth, "The Art of Computer Programming," vol. 1, Addison Wesley, 1969.

[13] D. E. Knuth, "The Art of Computer Programming," vol. 2, second ed., Addison Wesley, 1981.

[14] D. E. Knuth and L. T. Pardo, "Analysis of a simple factorization algorithm," Theoretical Computer Science, 3(1976), 321-348.

[15] M. Kraitchik, "Théorie des nombres," vol. I-II, Gauthier-Villars, Paris, 1922-1926.

[16] M. Kraitchik, "On the Factorization of $2^n \pm 1$," Scripta Math., 18(1952), 39-52.

[17] P. Landrock, "Algebra I," Matematisk Institut, Aarhus Universitet, September 1978 (in danish).

[18] D. H. Lehmer, "Tests for Primality by the Converse of Fermat's Theorem," Bull. Amer. Math. Soc., 33(1927), 327-340.

[19] D. H. Lehmer, "An Extended Theory of Lucas Functions," Ann. of Math., 31(1930), 419-448.

[20] D. H. Lehmer and R. E. Powers, "On Factoring Large Numbers," Bull. Amer. Math. Soc., 37(1931), 770-776.

[21] E. Lucas, "Théorie des fonctions numeriques simplement periodiques," Amer. J. Math., 1(1878), 184-240, 289-321.

[22] M. A. Morrison and J. Brillhart, "A Method of Factoring and the Factorization of F_7," Math. Comp., 29(1975), 183-205.

[23] A. A. Mullin, "Recursive Function Theory," Bull. Amer. Math. Soc., 69(1963), 737.

[24] T. Naur, "Faktorisering af store heltal," DAIMI Internal Report, 1978 (in danish).

[25] H. C. Pocklington, "The Determination of the Prime or Composite Nature of Large Numbers by Fermat's Theorem," Proc. Cambridge Philos. Soc., 18(1914-16), 29-30.

[26] J. M. Pollard, "Theorems on Factorization and Primality Testing," Proc. Cambridge Philos. Soc., 76(1974), 521-528.

[27] J. M. Pollard, "A Monte Carlo Method for Factorization," BIT, 15(1975), 331-334.

[28] C. Pomerance, J. L. Selfridge and S. S. Wagstaff, "The Pseudoprimes to $25*10^9$," Math. Comp., 35(1980), 1003-1026.

[29] M. O. Rabin, "Probabilistic Algorithms," in: J. F. Traub (ed.), Algorithms and Complexity, Recent Results and New Directions, Academic Press, New York, 1976, 21-40.

[30] M. O. Rabin, "Probabilistic Algorithms for Testing Primality," J. Number Theory, 12(1980), 128-138.

[31] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Comm. ACM., 21(1978), 120-126.

[32] R. Soloway and V. Strassen, "A Fast Monte Carlo Test for Primality," Siam J. Comput., 6(1977), 84-85.

[33] B. D. Shriver and P. Kornerup, "A Description of the MATHILDA Processor," DAIMI PB-52, Dept. of Computer Science, University of Aarhus, Denmark, 1975.

[34] H. C. Uhler, "A Brief History of the Investigations on Mersenne Numbers and the Latest Immense Primes," Scripta Math., 18(1952), 122-131.

[35] H. C. Williams, "Primality Testing on a Computer," Ars. Combinatoria, 5(1978), 127-185.

[36] H. C. Williams, "Some Primes with Interesting Digit Patterns," Math. Comp., 32(1978), 1306-1310.

[37] H. C. Williams and R. Holte, "Some Observations on Primality Testing," Math. Comp., 32(1978), 905-917.

[38] H. C. Williams and J. S. Judd, "Determination of the Primality of N by Using Factors of $N^2 \pm 1$," Math. Comp., 30(1976), 157-172.

[39] H. C. Williams and J. S. Judd, "Some Algorithms for Prime Testing Using Generalized Lehmer Functions," Math. Comp., 30(1976), 867-886.

[40] M. C. Wunderlich, "A Running Time Analysis of Brillhart's Continued Fraction Factoring Method," Springer Lecture Notes in Math., 751(1979), Number theory, Carbondale 1979 proc., 328-342

[41] M. C. Wunderlich and J. L. Selfridge, "A Design for a Number Theory Package with an Optimized Trial Division Routine," Comm. ACM., 17(1974), 272-276.

Appendix A.

Mathematical background

In this appendix we define the mathematical notations and concepts used in this paper and give the most important results concerning these concepts.

All letters stand for integers, unless otherwise stated. The notation for [ ], mod and congruences follows the exposition in Knuth[12, pp. 37-39], while the group theoretic results are taken from Landrock[17].

We first define

|a| = absolute value of a
[a] = the greatest integer $\leq$ a, a is real,
x mod y = x-y*[x/y], if y$\neq$0.
y|x y divides x (x mod y = 0)
y$\not|$x y does not divide x
gcd(x,y) = the greatest common divisor of x and y

It is easy to see that if x mod y $\neq$ 0, it has the same sign as y, and |x mod y| < |y|. x mod y is the remainder when x is divided by y.

A related concept is the congruence notation introduced by Gauss:

$$x \equiv y \text{ (modulo } z)$$

(read "x is congruent to y modulo z") means that x mod z = y mod z or z|(x-y). The basic properties of congruences are:

- If $a \equiv b$ and $x \equiv y$, then $a+x \equiv b+y$ and $a*x \equiv b*y$ (modulo m). It follows that if $a \equiv b$, then $a^n \equiv b^n$ (modulo m).

- If a*x ≡ b*y and a ≡ b, gcd(a,m) = 1, then x ≡ y (modulo m).

- a ≡ b (modulo m) if and only if a*n ≡ b*n (modulo m*n).

- If gcd(r,s) = 1, then a ≡ b (modulo r*s) if and only if a ≡ b (modulo r) and a ≡ b (modulo s).

Thus we can add subtract, multiply, and take powers modulo m just as we do ordinarily. For example, a*b ≡ (a mod m) * (b mod m) (modulo m), so when performing calculations modulo m, reduction can be performed after each addition, subtraction, and multiplication.

In number theory, the integers (as an example of a so-called unique factorization domain) are normally divided into zero and the sets of units, primes, and composite numbers. Zero is the identity with respect to addition and units are the elements a = 1 and a = -1 for which a*x = 1 has a solution x. A number a is composite if there exist non-units u and v such that a = u*v. For primes a, every solution to a = u*v has one of u or v equal to a unit.

If we restrict our attention to the positive integers, these properties ensure that every number N > 1 has a unique representation as a product of primes (except for the order of the factors).

We also need some results from group theory: Let M be some set with composition rule * (so that a*b belongs to M if a and b do). Then G = (M,*) is a group if * is associative, G has a neutral element, and every element has an inverse element. We will only need finite groups, and define ord(G) = number of elements in G.

If N is a sub-set of M, a*b belongs to N whenever a and b do, and H = (N,*) itself is a group, then H is called a sub-group of G.

If g is any element of G, we may consider the intersection of all sub-groups of G containing g. This definition makes sense, since G itself is such a sub-group. Since the intersection of two sub-groups is also a sub-group, the result is thus a sub-group which we denote by <g> and call the sub-group generated by

g. Also, g is called the generator of <g>. We write $ord_G(g) = ord(<g>)$, or simply ord(g) = ord(<g>), if no mistakes are possible.

In general, ord(H)|ord(G) when H is a sub-group of G. In particular, ord(g)|ord(G) for any element g of G. Also, ord(g) is the least positive integer n such that $g^n = e$ (the neutral element), where we have defined $g^1 = g$ and $g^{n+1} = g^n * g$. (Sometimes, ord(g) if defined as the least n such that $g^n = e$.) Finally, if $g^z = e$, it can be proved that ord(g)|z.

All this machinery will be applied to the group $G_N = (\{ 1 \leq x \leq N-1 \mid gcd(x,N) = 1\}, *)$ with multiplication modulo N as composition. It is easy to see, for example, that $ord(G_N) = N-1$ if and only if N is prime. If a belongs to G_N and N is prime, we have $ord(a) | ord(G_N) = N-1$, so ord(a)*k = N-1 for some k. Thus we have Fermat's theorem $a^{N-1} \equiv a^{ord(a)*k} \equiv 1^k \equiv 1$ (modulo N).

If N is prime, it can be proved that G_N is cyclic, i.e. $G_N = <g>$ for some generator g belonging to G_N. G_N may also be cyclic for certain composite values of N. If G_N is cyclic, the generators are called primitive roots.

In section 4.2 we define the Lucas sequences

$$U_0 = 0,\ U_1 = 1,\ U_{n+2} = P*U_{n+1} - Q*U_n$$

$$V_0 = 2,\ V_1 = P,\ V_{n+2} = P*V_{n+1} - Q*V_n$$

The formulas $a^{2*k} = (a^k)^2$ and $a^{2*k+1} = (a^{2*k})*a$ can be used to calculate a^m mod N in O(ln(m)) operations modulo N by considering the binary representation of the number m (see Knuth[13, pp. 441-442]). Correspondingly, the formulas

$$U_{2*k} = U_k * V_k, \qquad V_{2*k} = V_k^2 - 2*Q^k$$

$$U_{2*k+1} = (P*U_{2*k} + V_{2*k})/2, \qquad V_{2*k+1} = (D*U_{2*k} + P*V_{2*k})/2$$

can be used to calculate $U_m \bmod N$ and $V_m \bmod N$ in $O(\ln(m))$ operations modulo N. The division by 2 modulo N is easy, if N is odd: Simply add N before dividing, if the numerator is odd.

Appendix B.

Multi precision arithmetic

In describing the various methods for factoring large integers, we have assumed that the normal operations of addition, subtraction, multiplication, division, and taking a remainder are available for arbitrarily large numbers. This is, however, usually not the case. Thus these operations must be simulated using the limited-precision operations normally available. An excellent discussion of algorithms for performing these operations on multi-precision integers can be found in Knuth[13, pp. 250-299].

For the number-theoretic applications described here, the most natural representation of a multi-precision number is as a radix b number, where b is near the wordlength of the computer. Thus each number is represented as a sequence of digits d with $0 \leq d < b$.

Various more or less natural data structures can be used to support this representation. Using fixed-size vectors to contain the digits limits the size on the numbers. But this representation may, of course, be used if some reasonable upper limit can be placed on the size of the numbers.

Another idea is using linked lists to contain the digits. In this case, the size of the numbers is only limited by the implicit restrictions on the amount of storage. On the other hand, the operations are generally more difficult to implement in this representation, and also some efficiency is usually lost due to the necessary storage management.

Finally, it must be decided whether one should use some of the asymptotically fast algorithms for multiplication and division (see Knuth[13, pp. 278-299]). In the author's experience, these algorithms are faster than the traditional algorithms only for numbers much larger than those considered here. If very large numbers are desired, the more complicated algorithms should be considered, but for the 20-100 digit numbers involved in factorization attempts, this is generally not worth-while.

Appendix C.

Implementation overview

This Appendix contains a short overview of the author's implementation of factorization methods.

Most of the hard work is performed by the locally-developed, micro-programmable computers Rikke and Mathilda (see Shriver and Kornerup[33]). The author has developed a set of micro-programmed procedures for multi-precision arithmetic using Mathilda's internal registers for all storage of numbers. This limits the capacity to 16 multi-precision numbers of 16*62 bits (about 300 decimal digits), so 150 digit numbers can be handled conveniently.

Mathilda can multiply two n-bit integers in roughly $n^2/100$ microseconds (only valid if n is large, say > 100), while division is slightly slower (see Naur[24]).

The author has also implemented a more general (but slower) set of procedures for multi-precision arithmetic in PASCAL for DAIMI's PDP-10 computer. These procedures use linked lists for storage of numbers.

Using the procedures for multi-precision arithmetic in Mathilda, trial division and Pollard's methods have been implemented. Factors discovered by these methods are transferred to the PDP-10 and processed by a PASCAL program, whose main purpose is to test factors for primality, update factorization lists, and produce documentation for each factorization.

The expansion part of the continued fraction method also runs on Mathilda. The output produced by the expansion is transferred to the PDP-10, where it is processed to discover factorizations. Any factors found are again processed by the documentation program.

Appendix D.

Fibonacci numbers

Table of factorization of Fibonacci's sequence U_n defined by $U_0 = 0$, $U_1 = 1$, $U_{n+2} = U_{n+1} + U_n$. The table covers all odd n, $1 \leq n \leq 399$. The formula $U_{2*n} = U_n * V_n$ supplies the even entries (see Appendix E for factors of V_n).

1. 1
3. 2
5. 5
7. 13
9. 2 : 17
11. 89
13. 233
15. 2 * 5 : 61
17. 1597
19. 37 * 113
21. 2 * 13 : 421
23. 28657
25. 5^2 : 3001
27. 2 * 17 : 53 * 109
29. 514229
31. 557 * 2417
33. 2 * 89 : 19801
35. 5 * 13 : 141961
37. 73 * 149 * 2221
39. 2 * 233 : 135721
41. 2789 * 59369
43. 433494437
45. 2 * 5 * 17 * 61 : 109441
47. 2971215073
49. 13 : 97 * 6168709
51. 2 * 1597 : 6376021
53. 953 * 55945741
55. 5 * 89 : 661 * 474541
57. 2 * 37 * 113 : 797 * 54833
59. 353 * 271026097
61. 4513 * 55500349 7
63. 2 * 13 * 17 * 421 : 35239681
65. 5 * 233 : 14736206161
67. 269 * 116849 * 1429913
69. 2 * 28657 : 137 * 829 * 18077
71. 6673 * 46165371073
73. 9375829 * 86020717
75. 2 * 5^2 * 61 * 3001 : 230686501
77. 13 * 89 : 988681 * 4832521
79. 157 * 92180471494753
81. 2 * 17 * 53 * 109 : 2269 * 4373 * 19441
83. 99194853094755497
85. 5 * 1597 : 9521 * 3415914041
87. 2 * 514229 : 173 * 3821263937
89. 1069 * 1665088321800481
91. 13^2 * 233 : 741469 * 159607993
93. 2 * 557 * 2417 : 4531100550901
95. 5 * 37 * 113 : 761 * 29641 * 67735001
97. 193 * 389 * 3084989 * 361040209

99. 2 * 17 * 89 * 19801 : 197 * 18546805133
101. 743519377 * 770857978613
103. 519121 * 5644193 * 512119709
105. 2 * 5 * 13 * 61 * 421 * 141961 : 8288823481
107. 1247833 * 8242065050061761
109. 827728777 * 32529675488417
111. 2 * 73 * 149 * 2221 : 14590003055137 21
113. 677 * 27260240146681402 7129
115. 5 * 28657 : 1381 * 2441738887963981
117. 2 * 17 * 233 * 135721 : 29717 * 395896856 93
119. 13 * 1597 : 159512939815855788121
121. 89 : 9741581346638144559 6089
123. 2 * 2789 * 59369 : 685419577339 49701
125. 5^3 * 3001 : 158414167964045700001
127. 27941 * 5568053048227732210073
129. 2 * 433494437 : 257 * 5417 * 8513 * 39639893
131. 10663404174917105958145721 69
133. 13 * 37 * 113 : 3457 * 42293 * 351301301942501
135. 2 * 5 * 17 * 53 * 61 * 109 * 109441 : 111476995436 7361
137. 191347024000932780814494239 17
139. 277 * 2114537501 * 855267229376890 93
141. 2 * 2971215073 : 108289 * 1435097 * 142017737
143. 89 * 233 : 8581 * 19295841537568504 96621
145. 5 * 514229 : 3496199969307370798 90201
147. 2 * 13 * 97 * 421 * 6168709 : 293 * 3529 * 347502052673
149. 110557 * 162709 * 4000949 * 85607646594577
151. 5737 * 28116666245258116464699 15877
153. 2 * 17^2 * 1597 * 6376021 : 7175323114950564593
155. 5 * 557 * 2417 : 21701 * 12370533881 * 61182778621
157. 313 * 11617 * 7636481 * 10424204306491346737
159. 2 * 953 * 55945741 : 317 * 97639037 * 229602768949
161. 13 * 28657 : 8693 * 612606107755058997065597
163. 977 * 4892609 * 33365519393 * 32566223208133
165. 2 * 5 * 61 * 89 * 661 * 19801 * 474541 : 86461 * 518101 * 900241
167. 1810470079 3 * 196634431869334560856572 1
169. 233 : 337 * 89909 * 104600155609 * 126213229732669
171. 2 * 17 * 37 * 113 * 797 * 54833 : 6841 * 5741461760879844361
173. 163934378572 1 * 389678749007629271532733
175. 5^2 * 13 * 3001 * 141961 : 701 * 172312037302011893083 01
177. 2 * 353 * 2710260697 : 2191261 * 805134061 * 1297027681
179. 21481 * 156089 * 34188166409038989295346 13769
181. 8689 * 422453 * 81757892372385475745514 61093
183. 2 * 4513 * 555003497 : 1097 * 14297347971975757800833
185. 5 * 73 * 149 * 2221 : 17029455131913055569070976 18161
187. 89 * 1597 : 373 * 10157807305963434099105034917037
189. 2 * 13 * 17 * 53 * 109 * 421 * 35239681 : 38933 * 955921950316735037
* 191. 4870723671313 * 757810806256989128439975793
193. 9465278929 * 10209304320323269339768260084 97
195. 2 * 5 * 61 * 233 * 135721 * 14736206161 : 889992508374998776 81
197. 15761 * 25795969 * 227150265697 * 7171851071258865 49
199. 397 * 43678216920100204826117137855005526 9633
201. 2 * 269 * 116849 * 1429913 : 505026070439624716931599 9021
203. 13 * 514229 : 1217 * 56470541 * 25869827006567339946595 33
205. 5 * 2789 * 59369 : 821 * 125598581 * 364481178578913215364 01
207. 2 * 17 * 137 * 829 * 18077 * 28657 : 40723531557736276012221964 81
209. 37 * 89 * 113 : 57314120955051297736679165379998262001
211. 22504837 * 38490197 * 800972881 * 804754238584495 93021
213. 2 * 6673 * 46165371073 : 1277 * 185790722054921374395775013
215. 5 * 433494437 : 2607553541 * 67712817361580804952011621
217. 13 * 557 * 2417 : 433 * 44269 * 217221773 * 2191174861 * 6274653314021
219. 2 * 9375829 * 86020717 : 123953 * 4139537 * 3169251245945843761
* 221. 233 * 1597 : 203572412497 * 90657498718024645326392940193
223. 4013 * 108377 * 251534189 * 16434461004641013889615607 0813
225. 2 * 5^2 * 17 * 61 * 3001 * 109441 * 230686501
: 1198166198205095705361 6001

227. 23609 * 52195341379830251590788471136194672857273 77

229. 457 * 2749 * 40487201 * 132605449901 * 4783156029762036179 8553

231. 2 * 13 * 89 * 421 * 19801 * 988681 * 4832521 : 916425960174815923518 8401

* 233. 139801 * 2504739041963 3 * 631484089583693149557829547141

235. 5 * 2971215073 : 389678426275593986752662955603693114561

237. 2 * 157 * 92180471494753 : 1668481 * 40762577 * 7698999052751136773

* 239. 10037 * 62141 * 22285365795973180 57 * 28546908862296149233369

241. 11042621 * 7005329677 * 134287488928964476326795282473927 3

243. 2 * 17 * 53 * 109 * 2269 * 4373 * 19441 : 448607550257
- * 160004111243064030705 61

245. 5 * 13 * 97 * 141961 * 6168709 : 1289550739140244601926514848431956 41

* 247. 37 * 113 * 233 : 40910073861 7 * 467730604336790467692631214732815 3

249. 2 * 99194853094755497 : 1033043205255409 * 23812215284009787769

* 251. 582416774750273 * 219370803294651220261871241996569619 13

* 253. 89 * 28657 : 4322114369 * 2201228236641589 * 13784973033380476120 61

255. 2 * 5 * 61 * 1597 * 9521 * 6376021 * 3415914041 : 207786443969 41
- * 20862774425341

* 257. 5653 * 3297197867164590564552 1 * 12300267217193134713607146 49

* 259. 13 * 73 * 149 * 2221 : 1553 * 404656773793
- * 304126674229577198514879922364 9

261. 2 * 17 * 173 * 514229 * 3821263937 : 2089 * 20357 * 36017 * 40193
- * 322073 * 6857029027549

263. 4733 * 93629 * 92836229646390194235291216984425664630893902 81

* 265. 5 * 953 * 55945741 : 15901 * 2741218753681 * 92691859945746812592082758 1

* 267. 2 * 1069 * 1665088321800481 : 1228874251532 89 * 6445587734970304287730 9

* 269. 5381 * 2517975182669813 * 321709447478106 41 * 1693604398296487898 53

271. (193270471243015279782059101964580241188515112465021394429)

273. 2 * 13^2 * 233 * 421 * 135721 * 741469 * 159607993 : 640457
- * 14835473303439058865152 73

275. 5^2 * 89 * 661 * 3001 * 474541 : 7239101 * 15806979101
- * 55272784044541995358218 01

277. (34680978881583392867975816521049546284341699716466948344 57)

279. 2 * 17 * 557 * 2417 * 4531100550901 : 11717 * 594960058508093
- * 627983053225270632 1

281. 174221 * 119468273 * 1142059735200417842620494388293215303693455057

283. 10753 * 825229 * 15791401 * 4441118888488058431632357842986308632648 81

285. 2 * 5 * 37 * 61 * 113 * 761 * 797 * 29641 * 54833 * 67735001
- : 95673461671504632850248033060 1

287. 13 * 2789 * 59369 : 19816007100185326779670069250749018457050106438220 1

```
* 289. 1597 : 577 * 1733 * 98837 * 101232653 * 106205194357
       - * 658078658277725444483848541

* 291. 2 * 193 * 389 * 3084989 * 361040209 : 766744157389944997 73
       - * 227993117754975870677

  293. ( 765409046775693637841588453834897634076806499397895451209 5813 )

  295. 5 * 353 * 2710260697 : 1181 * 35401 * 75521 * 160481 * 737501
       - * 1120969250625390660846912 1

  297. 2 * 17 * 53 * 89 * 109 * 197 * 19801 * 18546805133 : 593 * 4157
       - * 1360418597 * 123692430687502422800 33

  299. 233 * 28657 : 205699287723427520846348534202713928205604028486051715 21

  301. 13 * 433494437 : 638069274527140473407781568463692789694353659667285 21

* 303. 2 * 743519377 * 770857978613 : 85502243896744 81
       - * 960496579172798748513694 21

* 305. 5 * 4513 * 555003497 : 2441 * 6101 * 204152539662476988 01
       - * 6472776707179982409438 61

* 307. 613 * 9143689 * 53070278677389 37
       - * 21691384151398801439039258352068147185 7

  309. 2 * 519121 * 5644193 * 512119709 : 617 * 318889 * 32386142297
       - * 8833645636274593230408 61

  311. 837833 * 6872477 * 603717553
       - * 1272232704013218608925801029523104780183 8093

  313. 1877 * 5009
       - * ( 123149057322573777281207034204319380530029006035226343539 81 )

  315. 2 * 5 * 13 * 17 * 61 * 421 * 109441 * 141961 * 35239681 * 8288823481
       - : 9761221 * 1205700287454923702715 01

  317. 1307309
       - * ( 607041952441352370857840833442507569992718408685433235721 833 )

* 319. 89 * 514229 : 1913 * 578029 * 1435522969 * 1535414556003613
       - * 18626243184683463348283529

  321. 2 * 1247833 * 8242065050061761
       - : 2644387026552261937524585811210551514149289 21

* 323. 37 * 113 * 1597 : 1109581873 * 855426446443577
       - * 22469617515216274972459349854327642081

  325. 5^2 * 233 * 3001 * 14736206161 : 1301 * 4235401 * 605416501 * 880262501
       - * 492847069677875690583 01

  327. 2 * 827728777 * 325296754884 17 : 653 * 1746181
       - * 158954614142727267943384636436638045 7

  329. 13 * 2971215073 : 1973 * 26321
       - * 127391874411097592672469891375644477141948573020237

  331. 29129 * 22966686648632120276391228028485200841318497622533370591664502461

* 333. 2 * 17 * 73 * 149 * 2221 * 1459000305513721 : 12653 * 1241348489339 57
       - * 9305077315575902267675937 61

  335. 5 * 269 * 116849 * 1429913
       - : 204041065458951029061541285201868911330032176511447663 61
```

337. 673 * (17837529232379628036669423497684 74-
- 3160484330947334862793699313361729)

339. 2 * 677 * 272602401466814027129 : 149161 * 258317
- * 220987865057977688874221534869142003 3

341. 89 * 557 * 2417
- : (6867180628341459279903726088514944642549474398661420231850820 01)

* 343. 13 * 97 * 6168709 : 46649 * 5449038756620509
- * 1089441709440098759783067514822344147023 93

345. 2 * 5 * 61 * 137 * 829 * 1381 * 18077 * 28657 * 2441738887963981 : 186301
- * 2501386404496144797315281460498 1

347. 324097 * 1434497
- * (3175788042970178108496328207406705420531625152312048862639097)

349. 1358309 * 2663569
- * (1068412388387034626965744049401584087191428119546068717075269)

351. 2 * 17 * 53 * 109 * 233 * 29717 * 135721 * 39589685693 : 2623373
- * 8023861 * 65790321679740490371744098034257

353. 736357
- * 359802011012573915498603609235632625259749492479918321872573852016 89

* 355. 5 * 6673 * 46165371073 : 4261 * 75309701 * 309273161 * 9207609261398081
- * 4927972264339186419280 1

357. 2 * 13 * 421 * 1597 * 6376021 * 1595129398158557881 21 : 1429 * 258469
- * 2765386623983625846388162309296 1

359. 4754204377346982207473680271667493829-
- 27701417016557193662268716376935476241

* 361. 37 * 113 : 6567762529 * 1196762644057 * 3150927827816930878141597
- * 1202012651071473478300924 1

363. 2 * 89 * 19801 * 974158134663814455960 89
- : 9490559604335963796081847699035385001836615801

* 365. 5 * 9375829 * 86020717 : 210241 * 27583781 * 758275080626801
- * 4810862617792334756259918335429 41

* 367. 733 * 17969789 * 75991753 * 5648966761 * 43397676601 * 114150315493
- * 7973572356247014991344442 01

* 369. 2 * 17 * 2789 * 59369 * 68541957733949701 : 8117 * 199261 * 84738793193
- * 9382599520669 * 11783851863335 1469

371. 13 * 953 * 55945741 : 207017
- * 1066891454330692360911118469915492770211286402568532457966113

373. 2237 * 9697 * 371509 * 20580649
- * 2416423364226955152383303968756154137928463542120118369457

375. 2 * 5^3 * 61 * 3001 * 230686501 * 1584141679640457000 01 : 9001 * 169501
- * 41510105455501 * 99062934069446535 01

* 377. 233 * 514229 : 1042642517 53 * 361575655741
- * 6081465853455679816708931999854492020150600942 37

379. 757 * 11889989 * (799012033863629446107001779701812 2-
- 10353551738609813062636353527061277)

381. 2 * 27941 * 5568053048227732210073 : 18995897
- * 3185450213669826966828420712039093359617657693

383. 1639241 * (3007034464158937575779479804251302203-
- 600723327873699115371190827635349861 7)

385. 5 * 13 * 89 * 661 * 141961 * 474541 * 988681 * 4832521 : 37807001
- * 75954341 * 13837648441 * 26387109578026731486922 21

* 387. 2 * 17 * 257 * 5417 * 8513 * 39639893 * 433494437 : 773 * 116101
- * 14279673833 * 380740013616392459856867145001086 09

389. 2333 * (37913363633273683512015308307265273616 6-
- 611992395913462463538527396257433249033)

391. 1597 * 28657 : 1493656753
- * 338762936677630378451801742610189355161885481434677266302778878 57

393. 2 * 106634041749171059581457216 9 : 2006657
- * 14166370809465639279785209838707244230608281939 93

395. 5 * 157 * 92180471494753 : 1472561
- * 14895360564424284043176235656343818553339488658236279764524 1

397. (4155355428193732411129703918568823891960 7-
- 027651133206312776412602212507675416588777)

399. 2 * 13 * 37 * 113 * 421 * 797 * 3457 * 42293 * 54833 * 351301301942501
- : 10590095734001255295041660945986426267087302 01

Appendix E.

Lucas numbers

Table of factorizations of Lucas numbers V_n defined by $V_0 = 2$, $V_1 = 1$, $V_{n+2} = V_{n+1} + V_n$. The table covers all n, $0 \le n \le 500$. Since

$$V_{10*k+5}/V_{2*k+1} = (5*U_{2*k+1}^2 - 5*U_{2*k+1} + 1) * (5*U_{2*k+1}^2 + 5*U_{2*k+1} + 1),$$

the factorizations for V_{10*k+5} may appear overly impressive.

0. 2
1. 1
2. 3
3. 2^2
4. 7
5. 11
6. 2 * 3^2 : 1
7. 29
8. 47
9. 2^2 : 19
10. 3 : 41
11. 199
12. 2 * 7 : 23
13. 521
14. 3 : 281
15. 2^2 * 11 : 31
16. 2207
17. 3571
18. 2 * 3^3 : 107
19. 9349
20. 7 : 2161
21. 2^2 * 29 : 211
22. 3 : 43 * 307
23. 139 * 461
24. 2 * 47 : 1103
25. 11 : 101 * 151
26. 3 : 90481
27. 2^2 * 19 : 5779
28. 7^2 : 14503
29. 59 * 19489
30. 2 * 3^2 * 41 : 2521
31. 3010349
32. 1087 * 4481
33. 2^2 * 199 : 9901
34. 3 : 67 * 63443
35. 11 * 29 : 71 * 911
36. 2 * 7 * 23 : 103681
37. 54018521
38. 3 : 29134601
39. 2^2 * 521 : 79 * 859
40. 47 : 1601 * 3041

41. 370248451
42. 2 * 3^2 * 281 : 83 * 1427
43. 6709 * 144481
44. 7 : 263 * 881 * 967
45. 2^2 * 11 * 19 * 31 : 181 * 541
46. 3 : 4969 * 275449
47. 6643838879
48. 2 * 2207 : 769 * 3167
49. 29 : 599786069
50. 3 * 41 : 401 * 570601
51. 2^2 * 3571 : 919 * 3469
52. 7 : 103 * 102193207
53. 119218851371
54. 2 * 3^4 * 107 : 11128427
55. 11^2 * 199 : 331 * 39161
56. 47 : 107450884 81
57. 2^2 * 9349 : 229 * 95419
58. 3 : 347 * 1270083883
59. 709 * 8969 * 336419
60. 2 * 7 * 23 * 2161 : 241 * 20641
61. 5600748293801
62. 3 : 3020733700601
63. 2^2 * 19 * 29 * 211 : 1009 * 31249
64. 127 * 186812208641
65. 11 * 521 : 131 * 2081 * 24571
66. 2 * 3^2 * 43 * 307 : 261399601
67. 4021 * 24994118449
68. 7 : 23230657239121
69. 2^2 * 139 * 461 : 691 * 1485571
70. 3 * 41 * 281 : 12317523121
71. 688846502588399
72. 2 * 47 * 1103 : 10749957121
73. 151549 * 11899937029
74. 3 : 11987 * 81143477963
75. 2^2 * 11 * 31 * 101 * 151 : 12301 * 18451
76. 7 : 1091346396980401
77. 29 * 199 : 229769 * 9321929
78. 2 * 3^2 * 90481 : 12280217041
79. 32361122672259149
80. 2207 : 23725145626561
81. 2^2 * 19 * 5779 : 3079 * 62650261
82. 3 : 163 * 800483 * 350207569
83. 35761381 * 6202401259
84. 2 * 7^2 * 23 * 14503 : 167 * 65740583
85. 11 * 3571 : 1158551 * 12760031
86. 3 : 31319571151657828 1
87. 2^2 * 59 * 19489 : 349 * 947104099
88. 47 : 93058241 * 562418561
89. 179 * 222355026409 88369
90. 2 * 3^3 * 41 * 107 * 2521 : 10783342081
91. 29 * 521 : 689667151970161
92. 7 : 253367 * 9506372193863
93. 2^2 * 3010349 : 63799 * 35510749
94. 3 : 563 * 5641 * 4632894751907
95. 11 * 9349 : 191 * 41611 * 87382901
96. 2 * 1087 * 4481 : 11862575248703
97. 3299 * 566785575021 41579
98. 3 * 281 : 5881 * 6102530946 9041
99. 2^2 * 19 * 199 * 9901 : 991 * 2179 * 1513909
100. 7 * 2161 : 9125201 * 5738108801
101. 809 * 7879 * 2010629467 18741
102. 2 * 3^2 : 67 * 409 * 63443 * 66265118449
103. 619 * 1031 * 525748002643 8961
104. 47 * 3329 * 106513889 * 325759201
105. 2^2 * 11 * 29 * 31 * 211 : 71 * 911 * 21211 * 767131
106. 3 * 1483 * 2969 * 1076012367720403
107. 47927441 * 4798364833 12919

108. 2 * 7 * 23 * 6263 * 103681 * 177962167367
109. 128621 * 788071 * 593985111211
110. 3 * 41 * 43 * 307 : 599968549286568 01
111. 2^2 * 54018521 : 4441 * 146521 * 1121101
112. 2207 : 223 * 449 * 1154149773784223
113. 4126704278449210374707 71
114. 2 * 3^2 * 29134601 : 227 * 26449 * 212067587
115. 11 * 139 * 461 : 1151 * 5981 * 324301 * 686551
116. 7 : 299281 * 834428410879506721
117. 2^2 * 19 * 79 * 521 * 859 : 1052645985555841
118. 3 : 15247723 * 100049587197598387
119. 29 * 3571 : 239 * 10711 * 27932732439809
120. 2 * 47 * 1103 * 1601 * 3041 : 23735900452321
121. 199 : 974207332084918690 44199
122. 3 : 19763 * 21291929 * 248486601 19363
123. 2^2 * 370248451 : 4767481 * 71884877 71
124. 7 : 743 * 467729 * 337587408304601 83
125. 11 * 101 * 151 : 251 * 112128001 * 28143378001
126. 2 * 3^3 * 83 * 107 * 281 * 1427 : 1461601 * 764940961
127. 509 * 5081 * 487681 * 13822681 * 19954241
128. 119809 * 469816763452337987 5583
129. 2^2 * 6709 * 144481 : 308311 * 761882591401
130. 3 * 41 * 90481 : 3121 * 4242647604145 0801
131. 1049 * 414988698461 * 5477332620091
132. 2 * 7 * 23 * 263 * 881 * 967 : 5281 * 66529 * 152204449
133. 29 * 9349 : 10694421739 * 2152958650459
134. 3 : 6163 * 20191246924 9 * 27056226821 63
135. 2^2 * 11 * 19 * 31 * 181 * 541 * 5779 : 271 * 811 * 42391 * 119611
136. 47 : 562627837283291940137654881
137. 541721291 * 7898248787093905 8281
138. 2 * 3^2 * 4969 * 275449 : 16561 * 162563 * 1043766587
139. 30859 * 25327912 9 * 14331800109223159
140. 7^2 * 2161 * 14503 : 1180214486624 7038881
141. 2^2 * 6643838879 : 79099591 * 139509555271
142. 3 : 283 * 569 * 2820403 * 9799987 * 35537616083
143. 199 * 521 : 1957099 * 2120119 * 1784714380021
144. 2 * 769 * 2207 * 3167 : 11556157812483852 2881
145. 11 * 59 * 19489 : 120196353941 * 1322154751061
146. 3 : 29201 * 37125857850184727260 788881
147. 2^2 * 29 * 211 * 599786069 : 65269 * 620929 * 8844991
148. 7 : 10661921 * 1140872880487019539 98401
149. 952111 * 4434539 * 326303953580324 5519
150. 2 * 3^2 * 41 * 401 * 2521 * 570601 : 601 * 871295471 72401
151. 1511 * 109734721 * 217533000184835774779
152. 47 : 562766385967 * 2206456200865197103
153. 2^2 * 19 * 919 * 3469 * 3571 : 13159 * 8293976826829399
154. 3 * 43 * 281 * 307 : 15252467 * 900164950225760603
155. 11 * 3010349 : 311 * 29138888651 * 82383707574 1
156. 2 * 7 * 23 * 103 * 102193207 : 1249 * 944918421835514 89
157. 39980051 * 161888565752865178188491 71
158. 3 : 21803 * 5924683 * 14629892449 * 184715524801
159. 2^2 * 119218851371 : 785461 * 452381929918 2451
160. 1087 * 4481 : 641 * 87813224044397487420 1601
161. 29 * 139 * 461 : 1289 * 1917511 * 965840862268529759
162. 2 * 3^5 * 107 * 11128427 : 1828620361 * 67829769479 87
163. 1043201 * 6601501 * 168645467119223044 5929
164. 7 : 26845714114300270282479059039 65201
165. 2^2 * 11^2 * 31 * 199 * 331 * 9901 * 39161 : 51164521 * 1550853481
* 166. 3 : 6464041 * 245329617161 * 10341247759646081
167. 766531 * 10384992769358454232012 7327909
168. 2 * 47 * 1103 * 1074508848 1 : 1156139395104815 15041
169. 521 : 5961078143640 89 * 67104039422084 9329
170. 3 * 41 * 67 * 63443 : 1361 * 40801 * 1161465421195403 2961
171. 2^2 * 19^2 * 229 * 9349 * 95419 : 162451 * 1617661 * 7038398989
172. 7 : 126117711915911646784404045944033521
173. 78889 * 6248069 * 16923049609 * 171246170261359
174. 2 * 3^2 * 347 * 1270083883 : 97787 * 528295667 * 5639710969

175. 11 * 29 * 71 * 101 * 151 * 911 : 54601 * 560701 * 7517651 * 51636551
176. 2207 : 1409 * 6086461133983 * 319702847642258783
177. 2^2 * 709 * 8969 * 336419 : 10884439 * 10511761735170685 9
178. 3 : 52805445356674722912771491192965462 01
179. 359 * 1066737847220321 * 6693225427948464744 1
180. 2 * 7 * 23 * 241 * 2161 * 20641 * 103681 : 8641 * 13373763765986881
181. 97379 * 213732615041977 51 * 32242356485644069
182. 3 * 281 * 90481 : 232961 * 611057863429488653480848 1
183. 2^2 * 560074829380 1 : 14686239709 * 533975715909289
184. 47 : 367 * 3730902316048 1 * 4417209581003819171 03
185. 11 * 54018521 : 26527271839851 * 2918000731816531
186. 2 * 3^2 * 30207337006 01 : 15917507 * 859886421593527043
187. 199 * 3571 : 1871 * 90567423440850652626509739043 1
188. 7 : 18049 * 100769 * 153037630649666194962091443041
189. 2^2 * 19 * 29 * 211 * 1009 * 5779 * 31249 : 379 * 85429 * 912871 * 1258740001
190. 3 * 41 * 29134601 : 2281 * 4561 * 782747561 * 17479555349080 1
191. 22921 * 395586472506832921 * 9102575599540574 39
192. 2 * 127 * 186812208641 : 383 * 5662847 * 6803327 * 19073614849
193. 303011 * 76225351 * 935527893146187207403151261
194. 3 : 195163 * 4501963 * 5644065667 * 23501170270005449 47
195. 2^2 * 11 * 31 * 79 * 131 * 521 * 859 * 2081 * 24571 : 1951 * 2731 * 866581 * 37928281
196. 7^3 * 14503 : 3016049 * 6100804791163473872231629367
* 197. 314985871191113 39 * 47019072228950683502498 89
198. 2 * 3^3 * 43 * 107 * 307 * 261399601 : 11166702227 * 107631289945436 3
199. 2389 * 4503769 * 360369604148119698107878471182 89
200. 47 * 1601 * 3041 : 124001 * 6996001 * 316043883417481735600 1
201. 2^2 * 4021 * 24994118449 : 2686039424221 * 940094299967491
202. 3 : 5474974184961446665431676138350901782970 01
203. 29^2 * 59 * 19489 : 27482320982833748894442899762822 69
204. 2 * 7 * 23 * 23230657239121 : 1223 * 4700399650239027549232 07
205. 11 * 370248451 : 1231 * 5741 * 2170732312961 * 111359800682371
206. 3 : 81163 * 462353921445862223671914407266727309 87
207. 2^2 * 19 * 139 * 461 * 691 * 1485571 : 364368440253429838004091 2641
208. 2207 : 7489 * 45045727 * 39586709834808244008811690207
209. 199 * 9349 : 419 * 20669776469 * 29597073640509671463165 91
210. 2 * 3^2 * 41 * 83 * 281 * 1427 * 2521 * 12317523121 : 721561 * 140207234004601
* 211. 33128448586319 * 37686950263205064956159526897 71
212. 7 : 250410161 * 11524703090550631152989172306262816 1
213. 2^2 * 688846502588399 : 1279 * 1882921 * 4925862451984793263 9

214. 3 : 21401 * 374929 * 226981241 * 126192465881 * 7670563424420 09

215. 11 * 6709 * 144481 : 431 * 1291 * 1721 * 1266715025281 * 66163448516461

216. 2 * 47 * 1103 * 10749957121 : 3023 * 19009 * 447901921 * 48265838239823

217. 29 * 3010349 : 18229 * 125024551 * 11260169813534893704769219

218. 3 : 1307 * 92450386728982480582715993408788566033584 3

219. 2^2 * 151549 * 11899937029 : 439 * 12748437199 * 145282738021003201

220. 7 * 263 * 881 * 967 * 2161 : 28000766314448537788816636954032 01

* 221. 521 * 3571 : 23371270440229730 21 * 35314950421248638631 41

222. 2 * 3^2 * 11987 * 81143477963 : 443 * 55927129 * 6870470209 * 8336942267

223. 209621 * 191782505151874799799825102831271417475449

224. 1087 * 4481 : 2689 * 49663363104137577284063175156062753 29

225. 2^2 * 11 * 19 * 31 * 101 * 151 * 181 * 541 * 12301 * 18451 : 221401 * 15608701 * 3467131047901

226. 3 : 6329 * 2151521 * 122464427 * 340404115357679693157474408 67

* 227. 39499 * 5098421 * 4311537234701 * 3173513869617946787973 01

228. 2 * 7 * 23 * 1091346396980401 : 62929 * 307826903 * 6549468879336 8423

229. 6871 * 1049904189467736674107369996852082658660076 31

* 230. 3 * 41 * 4969 * 275449 : 3116523496881881 * 22247004553118573472 41

231. 2^2 * 29 * 199 * 211 * 9901 * 229769 * 9321929 : 4621 * 19630381 * 201562805274601

232. 47 : 463 * 929 * 12527 * 277007 * 435612319760812779786551586739 67

233. 818757341 * 6911530261 * 873757179900549251563653697571

234. 2 * 3^3 * 107 * 90481 * 12280217041 : 467 * 21529 * 123944171348849444948627

235. 11 * 6643838879 : 941 * 6581 * 8461 * 119851 * 842432231 * 334814174837 21

236. 7 : 12743 * 13687 * 5974828049 * 28713074479853139217088887310 89

237. 2^2 * 32361122672259149 : 637293949 * 399660629491 * 1027912163389

238. 3 * 67 * 281 * 63443 : 75683 * 3465148147 * 5835151623058416367986 8441

239. 479 * 7649 * 24216191671442408226762026802756956706931169

240. 2 * 769 * 2207 * 3167 * 23725145626561 : 281490241 * 19996532728329638 41

241. 1156801 * 4645999 * 43219877626484550971962471774087607599

* 242. 3 * 43 * 307 : 200872171147 * 3564873012035809 * 13253086025993542387

243. 2^2 * 19 * 3079 * 5779 * 62650261 : 59779 * 120074026624398979403194983601

* 244. 7 : 487 * 52471477541626010209 * 55009022301464381514054890 47

245. 11 * 29 * 71 * 911 * 599786069 : 491 * 1471 * 88972241 * 4353947431 * 459807660691

246. 2 * 3^2 * 163 * 800483 * 350207569 : 67031206681
- * 467245054218823096711 21

247. 521 * 9349 : 383839 * 768548899 * 290083919457843606390381671754 1

248. 47 : 1952755969 * 7348335052866163494100349104492982785852 9

249. 2^2 * 35761381 * 6202401259 : 499 * 43084912634851 * 57208759126 1946589

250. 3 * 41 * 401 * 570601 : 1353439001 * 546516794800 1 * 8481757477058963800 1

251. 15061 * 170179 * 712841 * 156367054755171345450617435377220672 81

* 252. 2 * 7^2 * 23 * 167 * 14503 * 103681 * 65740583 : 503 * 4322424761927
- * 57138516058176 1

* 253. 139 * 199 * 461 : 133430974590378670 49 * 43958971527497857699509704 9

* 254. 3 : 1523 * 347366417511089201 * 76252069628164074340107412376147

255. 2^2 * 11 * 31 * 919 * 3469 * 3571 * 1158551 * 12760031 : 1021 * 53551
- * 95881 * 162716451241291

* 256. 34303 * 73327699969 * 125960894984050328038716298487435392001

* 257. 2107028233569599 * 125090447782502159 * 19450422614687907585 31

* 258. 2 * 3^2 * 313195711516578281 : 7772507 * 73254041816089 * 258422401920467

259. 29 * 54018521 : 2591 * 330666900546898116460968438563218940272271

260. 7 * 103 * 2161 * 102193207 : 21183761 * 57089761 * 1932300241
- * 5836312049326721

261. 2^2 * 19 * 59 * 349 * 19489 * 947104099
- : 12164543129760895694936797580733 1201

262. 3 : 523 * 4239161 * 85478893333404265392486994139536898703478906 7

263. 1579 * 924709 * 2098741 * 3001949101336686906107454320302466346629

264. 2 * 47 * 1103 * 93058241 * 562418561 : 8938447751328 47
- * 3068718630789795983

265. 11 * 119218851371 : 1061 * 17491 * 124021 * 7627231 * 14161601
- * 7387245659821938 1

266. 3 * 281 * 29134601 : 978347 * 186313849 * 3336915203
- * 260850954958365322168 9

267. 2^2 * 179 * 22235502640988369 : 3739 * 10592159405591345863754645197840 09

268. 7 : 4289 * 6387083201 * 5320236363458221470387433671224543829638 89

* 269. 13451 * 49098524855733491 * 290341026883813109 * 860882346042166879

270. 2 * 3^4 * 41 * 107 * 2521 * 11128427 * 10783342081 : 12315241
- * 1008735474200737565746 81

* 271. 59621 * 899179 * 92206663291 * 87426439096566323815478492553863521

* 272. 2207 : 4470047 * 7378607647 * 42848407775681 * 22418916493081610610604 9

273. 2^2 * 29 * 79 * 211 * 521 * 859 * 689667151970161 : 1836084445651
- * 1032512153239041931

* 274. 3 : 547 * 27947 * 864095167197522752 09 * 46196393961267734345849014360 1

275. 11^2 * 101 * 151 * 199 * 331 * 39161 : 92401 * 6982111964759801
- * 9645373591547077978O1

276. 2 * 7 * 23^2 * 253367 * 9506372193863 : 3365543 * 4333249681
- * 184234636098622253 29

* 277. 1109 * 5923369 * 1003666289 * 322458613167451 * 364764609953549748026435 9

278. 3 : 65609 * 6374987189597262064995389911513607380047098090282908 9

279. 2^2 * 19 * 63799 * 3010349 * 35510749 : 2870911 * 3599504551
- * 379039987657071537444 1

280. 47 * 1601 * 3041 * 10745088481 : 6135922241 * 1641543120 01
- * 1326451946603465248 1

* 281. 20567460049 * 46415343154434259 * 5567813533108035935034668181456 1

282. 2 * 3^2 * 563 * 5641 * 4632894751907 : 1129 * 183407723
- * 1568243714391295376547405323

* 283. 1699 * 252605941501 * 3242389994481538649597245382891516783783147 71

284. 7 : 3216560992972227366621179154981622382892385030297218550560 1

285. 2^2 * 11 * 31 * 191 * 229 * 9349 * 41611 * 95419 * 87382901 : 571 * 32491
- * 2069101 * 119130001 * 411677941

* 286. 3 * 43 * 307 * 90481 : 5147 * 24411299961202 43
- * 1309286103565237065660869690928 1

* 287. 29 * 370248451 : 256579 * 319973431 * 101731310703289
- * 1063584102563925624654 1

* 288. 2 * 1087 * 4481 * 1186257524870 3 : 270143 * 25033626656641
- * 1974737795746080149567

289. 3571 : 878516651 * 795954394282744053474161101150396077552743674481

290. 3 * 41 * 347 * 1270083883 : 5801 * 52201 * 96281 * 6854280100961
- * 3729619722745664971 61

291. 2^2 * 3299 * 56678557502141579 : 5496409 * 320657355925861
- * 4959318126280687189

* 292. 7 : 839207 * 121355783 * 2864461601 * 4953066392881
- * 1045794092558661358680161

293. 287141 * 5960509502940253048701057221464223567758321718855621163 1

294. 2 * 3^2 * 83 * 281 * 1427 * 5881 * 6102530946904 1 : 587
- * 1150184101339307 * 19077379176318892 9

295. 11 * 709 * 8969 * 336419 : 12391 * 552241 * 335838031 * 99979884881
- * 828729698728489156 1

* 296. 47 : 15400289 * 19088449 * 77894162661647 * 893117811524 81
- * 754276330346432303

297. 2^2 * 19 * 199 * 991 * 2179 * 5779 * 9901 * 1513909 : 220862269
- * 136947 1729429 * 13709621794968000 1

298. 3 : (6326966570068963358877914055630914277681129551393421226761700 1)

* 299. 139 * 461 * 521 : 599 * 2233531 * 1194215681621 * 143236388738249
- * 4019722252253785636 1

300. 2 * 7 * 23 * 241 * 2161 * 20641 * 9125201 * 5738108801 : 1201 * 148669201
- * 9602982001 * 1599014169601

* 301. 29 * 6709 * 144481 : 3948887931709 1 * 1050474234583201
- * 6895296934481238429951 71

* 302. 3 : 70963651961 * 95305716283 * 641196574939183885009590289769167242190 27
-

303. 2^2 * 809 * 7879 * 201062946718741 : 77569 * 3334819 * 42669355669
- * 372020433490130642 89

* 304. 2207 : 607 * 1823 * 20063 * 91807 * 1156984541407 * 12441241017224321
- * 526019705785467 83

305. 11 * 5600748293801 : 86011 * 30727531 * 11868899378561
- * 2851671040957030569903401

306. 2 * 3^3 * 67 * 107 * 409 * 63443 * 66265118449 : 4283 * 18531361
- * 1687789138735396421450174049 47

307. 1229 * 1173961011742920365128276840708532407016977552376382872681 0201

* 308. 7^2 * 263 * 881 * 967 * 14503 : 7872253927 * 962352052496900234 3
- * 19352989806727787610 41

* 309. 2^2 * 619 * 1031 * 5257480026438961 : 1270029990781
- * 2216051880587916003268636813231

* 310. 3 * 41 * 3020733700601 : 1805019110667134254990 01
- * 9113162636597558947796254 01

311. 34211 * 2890615644252691924572487628689034423952562309093965400390309
-

312. 2 * 47 * 1103 * 3329 * 106513889 * 325759201 : 740687 * 71467343
- * 2523953243611786839361080 01

313. 2588996112033034187216561572494455300468300730442011523322577 17521
-

314. 3 : 142934683 * 97692260970483045511485583064960868271982906796663352 9507
-

315. 2^2 * 11 * 19 * 29 * 31 * 71 * 181 * 211 * 541 * 911 * 1009 * 21211
- * 31249 * 767131 : 631 * 1051224514831 * 19830007655010 01

316. 7 : 675607 * 2319007420428612252696320362317709507108778046806540448675 43
-

317. (1774524334209840819478601135200322570341117256884368267719803156571)
-

318. 2 * 3^2 * 1483 * 2969 * 1076012367720403 : 14627 * 346656889
- * 571574914649 63 * 116171668216510969

319. 59 * 199 * 19489 : 625728071
- * 3244717997032785202133960753338269100531044576583 1

* 320. 127 * 186812208641 : 623795558318030998672729 61
- * 5079180256659675431743744001

321. 2^2 * 47927441 * 479836483312919 : 809013091
- * 1634328947188978143200766705028850 71

* 322. 3 * 281 * 4969 * 275449 : 643 * 770867 * 25154641 * 163674763583689
- * 8357802723902097130683089

323. 3571 * 9349
- : (9537900571078530123166941650941639789639700035084989156042 01)

324. 2 * 7 * 23 * 6263 * 103681 * 177962167367 : 647 * 12340209383
- * 1734217181663215208317263414712 81

325. 11 * 101 * 131 * 151 * 521 * 2081 * 24571 : 3251 * 843701
- * 3558039391073701 * 1459055656827600978264885 1

326. 3 : (44962398121108954966886417239466 00-
- 120754312204117277413326859700948 1)

327. 2^2 * 128621 * 788071 * 593985111211 : 1358359 * 802006741 * 8541593161
* 9738994441963883623 9

328. 47 : 75136012657511269192604205282056462108788202141739768847624750968 01
-

329. 29 * 6643838879 : 659
- * (450019298152789198636062500456739147530309066679874517 9)

330. 2 * 3^2 * 41 * 43 * 307 * 2521 * 261399601 * 59996854928656801 : 1321
- * 817081 * 3666961 * 6064257279413810 41

* 331. 526291 * 54184296181 * 4386848568249611
- * 1195795459010394227506385297803918292 9

332. 7 : 97607
- * 3542562803359306968528223771202195633542893296819842168040162903

333. 2^2 * 19 * 4441 * 146521 * 1121101 * 54018521 : 1999 * 14678641
- * 4456602417097387136846427511699279 9

* 334. 3 : 821641 * 7162963 * 501870477 47 * 14167898020159929481
- * 5047527656672037363667798 01

335. 11 * 4021 * 249941184 49 : 91822921898111541916190307 1
- * 1010052140879271906648306231 1

336. 2 * 223 * 449 * 769 * 2207 * 3167 * 11541497737842 23 : 18143 * 416187743
- * 1368322369 * 1292528726309580 481

337. 21569 * 340819559
- * 3651575156022459933890370204120436853816552382514920496951

* 338. 3 * 90481 : 2027 * 141283 * 404112157123 * 47806156571279752464 1
- * 2892106995173496522201467

* 339. 2^2 * 4126704278449210374707 71 : 4460727628352882983 9
- * 954423225346040964978868549

* 340. 7 * 2161 * 23230657239121 : 5441 * 897601 * 17276792316211992881
- * 3834936832404134644974961

341. 199 * 3010349 : 2729 * 12959 * 347821
- * 24968047172542592952969282984682443824284389694771

342. 2 * 3^3 * 107 * 227 * 26449 * 29134601 * 212067587 : 683 * 20521 * 47881
- * 636873121998730 7 * 32496874088653692 1

343. 29 * 599786069 : 2094359 * 1837202669
- * 719710830963897294902092020293408330803742219 9

344. 47 : 9303823
- * (17823334116600291940694790043616513053650800047283435529491816 47)

345. 2^2 * 11 * 31 * 139 * 461 * 691 * 1151 * 5981 * 324301 * 686551 * 1485571
- : 4831 * 4641631 * 117169733521 * 3490125311294161

346. 3 : (6801461934056876469033811675350952 66-
- 5397003330448384917711848684619550 81)

347. 662771
- * (4981357021879030064663206649577472622964683465724876903387571953149)

```
* 348. 2 * 7 * 23 * 299281 * 834428410879506721 : 560589524253219666621 83
     - * 1185031046372137517381447

  349. ( 864343652971263621068393977129950801-
     -                                    5208953449658400255583723507306897001 )

* 350. 3 * 41 * 281 * 401 * 570601 * 12317523121 : 2801 * 28001
     - * 248773766357061401 * 735819236231634124380 5801

  351. 2^2 * 19 * 79 * 521 * 859 * 5779 * 1052645985555841 : 65597689
     - * 211040877766481874593768540032840086 49

* 352. 1087 * 4481 : 3891324187650256896001
     - * 193173463452275472610870771841043917435848 3201

  353. 592429953134577297805108237673547307 9-
     -                                    828684892148137487426453470557362837 1

  354. 2 * 3^2 * 15247723 * 100049587197598387
     - : 34908553115258945939423461603039303226018704284 01

  355. 11 * 688846502588399 : 43137227648024611864 9946839441
     - * 47450950412826764989920353256 1

  356. 7 : 63367
     - * 56576847195928571407926224888950947454797421902788598305582784501610 3

  357. 2^2 * 29 * 211 * 239 * 919 * 3469 * 3571 * 10711 * 27932732439809
     - : 203796218669120410092853068780009984382 81

* 358. 3 : 316590102769
     - * ( 691761871535184886617885661346831172632417347966345833225068929 )

  359. 719 * 1648529
     - * ( 896886254071077987926885668123271339039771087126000364568813909649 )

  360. 2 * 47 * 1103 * 1601 * 3041 * 10749957121 * 23735900452321 : 5208481
     - * 2563987147105929622138082038024801

  361. 9349 : ( 29769598024793909252216621696 8010538-
     -                                    261985888767087088691369301670380349 )

  362. 3 : ( 150108234066949126752175199839660 76670-
     -                                    537479312685305263348655541278023236 01 )

  363. 2^2 * 199 * 9901 * 974207332084918690441 99 : 9439 * 2435731 * 363397849
     - * 113587940877973425619561 4761

  364. 7^2 * 103 * 14503 * 102193207 : 727 * 193649 * 800801 * 8303168327
     - * 16837195415021202231416510299184298 41

  365. 11 * 151549 * 11899937029 : 514651 * 7015301 * 8942501 * 9157663121
     - * 3252336525249736694804553589211

  366. 2 * 3^2 * 19763 * 21291929 * 24848660119363 : 102481 * 10225307
     - * 21791641 * 7181634929637355776701081412683

* 367. 2298889 * 19997474011
     - * ( 10863526509586353737296146242101468487755841994251137331963 51 )

  368. 2207 : 245087 * 11079007
     - * 13484292549345009218015967701713491137426073107017330576389569

* 369. 2^2 * 19 * 4767481 * 370248451 * 7188487771 : 739 * 26024651929
     - * 18736753266019 * 37625492610616575081340 9

  370. 3 * 41 * 11987 * 81143477963 : 1481
     - * ( 11939952491306142175725173848307099580979926808298722812 41 )
```

371. 29 * 119218851371 : 6679
- * (1482382086217377279390361548089656125425746385946933007673215 9)

372. 2 * 7 * 23 * 743 * 467729 * 337587408304601 83 : 1489
- * 9846508328097754140479671079843145561996079420 9

373. 2239 * 400254035815230315691149177295200682 7-
- 3516094100108818109883490482374673843 9

* 374. 3 * 43 * 67 * 307 * 63443 : 2243 * 49369 * 3827019260681
- * 158636198775636049 * 1281280767267251812597555038 7

375. 2^2 * 11 * 31 * 101 * 151 * 251 * 12301 * 18451 * 112128001 * 2814337800 1
- : 751 * 2251 * 468535826053501 * 79208139733005002475 1

376. 47^2 : 10779169 * 3547078721
- * (44947020721079138879299205175365355971624787134356804666927)

377. 59 * 521 * 19489 : (10253239069038176381674000058896144 -
- 4871825750242737403352969185463828 01)

378. 2 * 3^4 * 83 * 107 * 281 * 1427 * 1461601 * 11128427 * 764940961 : 2267
- * 32507 * 18788923389546130048317121725489105289

379. 342912379 * (468956426231922484189006878505762 24-
- 5432735158374232784872789019462636 31)

380. 7 * 2161 * 1091346396980401 : 15062006801
- * 10464175859779336956429177063263482687731703854280 1

381. 2^2 * 509 * 5081 * 487681 * 13822681 * 19954241 : 3049 * 7357111
- * 13487637940319141560417976471439835482057 49

382. 3 : 55009 * (41278468010826232294987989146753769 11-
- 26121544705841249788533558444097773089)

383. 7901291 * (139498057082906624745268659250252596 2-
- 7786363661205338813784311459416148669)

384. 2 * 119809 * 469816763452337987558 3 : 885503 * 1359361 * 1769526527
- * 74374487830388257301623938403 83

385. 11^2 * 29 * 71 * 199 * 331 * 911 * 39161 * 229769 * 9321929 : 3851
- * 84100171 * 582276311 * 1097233061 * 11121181527413179938 11

386. 3 : 3089 * (503836902657223829848872583007718745 13-
- 4365118887847314148719783452199512893 29)

387. 2^2 * 19 * 6709 * 144481 * 308311 * 761882591401 : 1549
- * 2818422944804059040851279339520173127497879598470 9

388. 7 : 6983 * 4716437207
- * 5302128857446935216982971462475831424585281386810339485459853126241

389. (19778441050644629292778177456846206031337 -
- 5636781248121680777914937609483512587905 1)

* 390. 2 * 3^2 * 41 * 2521 * 3121 * 90481 * 12280217041 * 424264760414508 01
- : 54975368761 * 21266115836255859456110149801

* 391. 139 * 461 * 3571 : 10949 * 2476673936041
- * 834484880498372128537891307445941852925566419249911616229

392. 47 * 10745088481 : 12653761 * 1016307041
- * 1290038175039560430642984778500260607762641561539198721

* 393. 2^2 * 1049 * 414988698461 * 5477332620091 : 32845130922638389
- * 432743702808878906877493417505847418 09

394. 3 : 787 * 553963 * 2214453361
- * 75733316348119072779289451259214525577285148414506608325413512 41

395. 11 * 32361122672259149 : 2371 * 12641 * 121661 * 383941 * 1552351
- * 1713511 * 9263072321 * 59861941347 1 * 4828253906741

396. 2 * 7 * 23 * 263 * 881 * 967 * 5281 * 66529 * 103681 * 152204449 : 3169
- * 63361 * 46046881 * 102551329 * 151409133906803874308734561

397. (92916572081139318245632867021034772931170-
- 3280022257792611731676921503296 93382842121)

398. 3 : (50114057248470989800353010491579327921534-
- 24437631530180417587178386881134507763 1001)

* 399. 2^2 * 29 * 211 * 229 * 9349 * 95419 * 10694421739 * 2152958650459 : 28729
- * 519499 * 561434197549 * 252171167457207277136719

* 400. 2207 * 23725145626561 : 107420801 * 177736001 * 51793685214662401
- * 760158710112872948977300866780 4801

401. 1775629 * 6238759
- * 57490131422237119538947323064108369354763411739839193426140731363438441

* 402. 2 * 3^2 * 6163 * 201912469249 * 2705622682163 : 1609 * 2915186157721
- * 36250499854335186207246297549451509565 69

403. 521 * 3010349 : 25054511
- * 42430536084158188102317698250762108075724699403871413365975546725791

404. 7 : 4057630561 * (94980864493017855394747046575330922 27-
- 53418121073070754200766445460986250 41)

405. 2^2 * 11 * 19 * 31 * 181 * 271 * 541 * 811 * 3079 * 5779 * 42391 * 119611
- * 62650261 : 1621 * 4861 * 21871 * 33211 * 31603395781
* 765486110284343388 1

* 406. 3 * 281 * 347 * 1270083883 : 7307 * 646907976 41
- * (402171113610461934467871267326224268132806671326627993 23)

407. 199 * 54018521 : 205129 * 4792019 * 3473266369
* 311379581597016565173529362255085372911306092656839779

408. 2 * 47 * 1103 * 562627837283291940137654881 : 2447 * 23663
- * 54743034422498424015130804728038333162819380 81

409. 1427411 * 3165661 * (662111936141029718431755554171926240-
- 0962964820416865593466710019322399431)

* 410. 3 * 41^2 * 163 * 800483 * 350207569 : 6287749041815 21
- * 14386018829678116716 1 * 2322429099336692919718294260481

* 411. 2^2 * 541721291 * 7898248787093905828 1 : 242491 * 104446810724929
- * 18070186267894449189347092077457768249

412. 7 : 823 * 294167 * (74785251120539959276633179637783797804-
- 60240176709402001652472664523276205328 1)

413. 29 * 709 * 8969 * 336419 : 545161
- * (60631996794193058415047618833948969971546733440991730934196331960 41)

414. 2 * 3^3 * 107 * 4969 * 16561 * 162563 * 275449 * 1043766587 : 827
- * 12207203 * 14789789754543553284121041098687612252733688 81

415. 11 * 35761381 * 6202401259 : 6170221 * 5216440441 * 12933833823941
- * 1528527683761524871 * 345802651979922515711

416. 1087 * 4481 : 419329 * 727169
- * 584875731540300882607396508321487635244484155302074048573424052273281

417. 2^2 * 30859 * 253279129 * 14331800109223159 : 1669
- * 187952307304802321819479869699444098231355628492527 5779

* 418. 3 * 43 * 307 * 29134601 : 7907723 * 4692901883 * 722601451307
- * 735029402811219021533646778504622751006567116 27

419. 839 * 897499 * (488680861194429699747880618401628074889-
- 39515324111938586468510977834072294586 59)

420. 2 * 7^2 * 23 * 167 * 241 * 2161 * 14503 * 20641 * 65740583
- * 11802144866247903888 1 : 13076262780531942679085440491796970310241

421. 1995541 * (48276512612973213820980908142916854723033-
- 24070656903515615825450430354040016692661)

422. 3 : 9283 * (55972483929253746769104666646642815121590 8-
- 14111122020490347810626248336388079009734 7)

423. 2^2 * 19 * 79099591 * 6643838879 * 139509555271
- : 45264835826305023025994480174162867658245141981616910310 41

424. 47 : 1022689 * (84902020034534884564976156975426171520 97-
- 61035335142460608476479242988546336036929)

425. 11 * 101 * 151 * 3571 * 1158551 * 12760031 : 51001 * 2968201
- * 1371955936801 * 162772761635424602875 1 * 22054919149909719709751

426. 2 * 3^2 * 283 * 569 * 2820403 * 9799987 * 35537616083 : 16187
- * (231831376524428981758491938848781498324238537222056 0723)

427. 29 * 5600748293801 : 1709 * 81131 * 2649109
* 28976745988106598776226499445178106786437891789745656067626 91

* 428. 7 : 21596023 * 33640801 * 386610981607
- * 14226487668919186789993296389690885649349284625925731081620816 1

429. 2^2 * 79 * 199 * 521 * 859 * 9901 * 1957099 * 2120119 * 178471438002 1
- : 301159 * 539665699 * 1349538077674055461741903165711845661

430. 3 * 41 * 3131957115165782 81 : (19009224041130225522765582216181963-
- 18440126316087090324393162044397512 1)

431. 188779 * (62765250509393565431126001091707169437573 1-
- 64348522021003242975954303210977170719115 81)

432. 2 * 769 * 2207 * 3167 * 11556157812483852288 1 : 863
- * (17882556104918988343681249012711242048293607273131239855 67)

* 433. 12361187009 * 203421415129 * (12336483443684554593107485116769128-
- 16993316998007914907057560127231561)

434. 3 * 281 * 3020733700601 : 39929 * 541562561
- * (91150443504449047208530975243303087962180298077506784918943129)

435. 2^2 * 11 * 31 * 59 * 349 * 19489 * 947104099 * 120196353941
- * 1322154751061 : 1741 * 6091 * 13921 * 560281 * 12869041 * 7820838901
* 11841524567731

436. 7 : 2856113921 * 65726057579801176540614251079285551239 51-
- 935721209971684457028902423210582614036 81

437. 139 * 461 * 9349 : (35490972831566639031171752005207282232101-
- 81480710080894936231309107771222898705520 1)

438. 2 * 3^2 * 29201 * 37125857850184727260788881 : 7883 * 88370003
- * 5049205307 * 501210633555112203395744292840696029987

439. 4391 * 826061911 * (153461003915925866597933020160675982831 6-
799010945958677430510680831886807496 1149)

440. 47 * 1601 * 3041 * 93058241 * 562418561 : 21121
- * (356063239983684716396472783096244812436514347497914564942638081)

* 441. 2^2 * 19 * 29 * 211 * 1009 * 31249 * 65269 * 620929 * 8844991 * 599786069
- : 35281 * 8064211318124446 9 * 16247350756640617732192770750349

442. 3 * 67 * 63443 * 90481 : 883 * (23144037622865659188103351910937241 1489-
352727119604537366472338408602052211227)

443. 2659 * 135559 * 10584684975846732318396834211076966961959 7-
364220025447451777767309795219865130104285 9

* 444. 2 * 7 * 23 * 10661921 * 1140872880487019539984 01 : 887 * 2663 * 17761
- * 21423730326721 * 175358325117577112755922815666434960 1

445. 11 * 179 * 22235502640988369 : 643431044 71 * 196317700541 * 3565818352751
- * 125411827011535 1 * 4038760158986869098778 91

446. 3 : 175723 * 9237507401 * 331881380821075796562141706309693205920-
00209031832916941301394332906693246 8947

447. 2^2 * 952111 * 4434539 * 3263039535803245519 : 1789 * 595079479
- * 44572961316701091570454843936327625650477556780221

448. 127 * 186812208641 : 2687 * 285823 * (232214329811154585889273966512142-
511196424238040176072346656800511518721)

449. 369079 * (185494542666084711288660043036300924391371 44-
921110069944834110570651856281674163245147269)

* 450. 2 * 3^3 * 41 * 107 * 401 * 601 * 2521 * 570601 * 10783342081
- * 871295471724 01 : 1801 * 18637456318905481020 1
* 427694148584338087778220001

451. 199 * 370248451 : 4274579 * 5690967143522108253316958252008566288 4-
377962564222829999842181652894123123019

452. 7 : 2568263 * 81890647 * (19698880947083317936110069371677334727 53-
732092073716280447479204474593368460856 1)

453. 2^2 * 1511 * 109734721 * 21753300018483577477 9 : 335221 * 89526391
- * 10837399157311960843528910542685545748152881169441

* 454. 3 : 907 * 4791205378649 * (582391924113642026461397280948842156172-
143005326327306833308882962511558106506 7)

455. 11 * 29 * 71 * 131 * 521 * 911 * 2081 * 24571 * 689667151970161 : 17291
- * 50051 * 6320315821 * 4000643765894231 * 1130482648241980059327164 51

456. 2 * 47 * 1103 * 562766385967 * 2206456200865197103 : 386689 * 446881
* 185686849 * 4811741337219550924899248009733187502976 1

* 457. 143392891 * 48175086409 * 864351271995241
* 53865562038701008975397146407705442118820462326130285905669299

458. 3 : 1734674441830928894654682150591788721361808658 47-
642115150876882787982326965619685734718473208401

459. 2^2 * 19 * 919 * 3469 * 3571 * 5779 * 13159 * 8293976826829399
- : 154299749864027149993751874047074120474406405738506793485056 1

* 460. 7 * 2161 * 253367 * 9506372193863 : 217121 * 28677143808961
- * 600563757845565671628554017335086529258894394197418401

461. (22044596563281958654386414816932362277824947836 1-
- 1825603299680947699969896531672713952679171877051)

462. 2 * 3^2 * 43 * 83 * 281 * 307 * 1427 * 15252467 * 261399601
- * 900164950225760603 : 9241 * 28643
* 4747855442294388893378042286885457893986 27

* 463. 106332581 * 585919814281 * (926345284665871319903157205872478107 29-
- 8808392626821865209715640677056086010 89)

464. 2207 : (42311920969017046353198779211375086214492622256-
- 4124547288235361992017515497215673448793480 1601)

465. 2^2 * 11 * 31^2 * 311 * 63799 * 3010349 * 35510749 * 29138888651
- * 823837075741 : 1861 * 4651 * 16741 * 65101 * 565441 * 257750431
* 5104614261828646351

* 466. 3 : 13049 * 668243 * 17387541121 * (537488630969109690333681744398223 57-
- 8464534820167596434882378273597344419585 23)

467. 72176719 * (548063475811036026534297351054363697772637485-
- 9402065732290366191951074440586011171554108 41)

468. 2 * 7 * 23 * 103 * 1249 * 103681 * 102193207 * 944918421835514 89
- : 154327947644963469960847969236759843528697605046042671289344 1

* 469. 29 * 4021 * 24994118449 : 4691 * 2009966099 * 10812055185331
- * 34855471623316061805334304216035149131456351321717668885 9

470. 3 * 41 * 563 * 5641 * 4632894751907 : 16921 * 276222761
- * 19809950476703891759635852223863606381827838846342829232189869441

471. 2^2 * 39980051 * 161888565752865178188491 71 : 412341661
- * (25398135225116023021244204344040954390479297029605059380 1)

472. 47 : 1889 * (4941244934461640419661691157198736338794368429 7-
- 8373504606323195311760096128910415986917473020 9)

473. 199 * 6709 * 144481 : 31219 * 2159719 * (5457779608551230987482022827 87-
- 5655258942758208742763418359384046295387326854 1)

* 474. 2 * 3^2 * 21803 * 5924683 * 14629892449 * 184715524801 : 947 * 10279163
- * 8411395441 * 59223094130623540 09 * 37694344249258413099158188 9

475. 11 * 101 * 151 * 191 * 9349 * 41611 * 87382901 : 4751 * 16051201
- * 662274006922117144633042051 * 33781171015631627701406786489962619501

476. 7^2 * 14503 * 23230657239121 : 146609 * 124234067210162251532295145371 76-
- 4077620872877495523069552841671585715920772 9

* 477. 2^2 * 19 * 785461 * 119218851371 * 4523819299182451 : 49721203549
- * (3039305569616059528396944640772754177580503048537217909)

* 478. 3 : 63289027012612845672 1 * 4146124755824254011197546970662762320 16-
- 4758443697460091641243037362105014072881

479. 4717331869 * (27001211418771783705332179653092071193122645 6-
- 3240331642900562827552075018751788960763231371)

480. 2 * 641 * 1087 * 4481 * 1186257524870 3 * 87813224044397487420160 1
- : 31683700840010757662911544164118268671878460597406912 1

* 481. 521 * 54018521 : 76984462699 * (153911639591633757414508049808791409727-
- 1974975991680210019638676050273388781673 9)

482. 3 : 1327427 * (135491078199542159622746327380294475971216779 27-
- 70249027518702236983577600567082278230924852676 3)

* 483. 2^2 * 29 * 139 * 211 * 461 * 691 * 1289 * 1485571 * 1917511
* 965840862268529759 : 9661 * 236235695207989
* 995264815850055684164903573745584428 9

484. 7 * 263 * 881 * 967 : (900661730939867977920948119962413626073646497 4-
- 8785923052927166884636822288020309306413352801)

485. 11 * 3299 * 56678557502141579 : 971 * 2569733895941
- * 127380262737031838209714 1 * 34962478192749096461017520292718749827531

486. 2 * 3^6 * 107 * 11128427 * 1828620361 * 6782976947987
- : 17174107866559209832245996776509546318861182768126017871860347845227

487. 4871 * 122846467354664998673916230710497626221725181854 3-
- 8861897071677544155742514633524323079001198211109 9

488. 47 : (2060015955112740750392183261728214529878595829447 4-
- 14767968703555760247543408523645973524444021834720 1)

489. 2^2 * 1043201 * 6601501 * 168645467119223044592 9 : 5869
- * (57457486097856050818137353773384734887812815694120941557252424 19)

490. 3 * 41 * 281 * 5881 * 12317523121 * 6102530946904 1 : 7841 * 99961
- * 631121 * 335376831950743865049700325022637455647789529603261267 61

491. 3929 * (1043877012389440283821397383206528470801951346690 3-
- 3055455550899464840963908923804540010836416404003 1)

492. 2 * 7 * 23 * 26845714114300270282479059039652 01 : 983 * 7775569
* (1004390214500100771136711075558819671210561503730349685063)

493. 59 * 3571 * 19489 : 2004539 * (13045499592454153822129218596042362499 17-
- 342890760805989194119180827977439656839153358059)

494. 3 * 90481 * 29134601 : 188707 * 4041907 * 28802635946826115861940959106 3-
- 875340157193957175318517752029683779842088195344 9

495. 2^2 * 11^2 * 19 * 31 * 181 * 199 * 331 * 541 * 991 * 2179 * 9901 * 39161
- * 1513909 * 51164521 * 1550853481 : 914116501 * 1808388451
* 3943480033796491 * 2331783722604006 1

496. 2207 : (2060948933161650864096993823200017257422131940717 5-
- 7835139435761204082946621259566053365028233489104 01)

* 497. 29 * 688846502588399 : 9941 * 173907259 * 849570487921
* (250835815435630228721389536312389584575185122404883996159713899 9)

* 498. 2 * 3^2 * 6464041 * 245329617161 * 10341247759646081 : 20276569
- * 93750172283 * 212216314620580244514251999177476639338737695720283

499. 10979 * (175497001114088085933746655956963092999544079469 29-
- 021878466893380681490766909826821172874540110264631)

500. 7 * 2161 * 9125201 * 5738108801 : 4001 * (98375634984245252948700557353-
- 28936277440019167305729867044789837874436790334600 1)

Appendix F.

2^n-1

Table of factorizations of 2^n-1 for odd n, $1 \leq n \leq 299$. The formula $2^{2*n}-1 = (2^n-1)*(2^n+1)$ supplies the even entries (see Appendix G for 2^n+1).

1. 1
3. 7
5. 31
7. 127
9. 7 : 73
11. 23 * 89
13. 8191
15. 7 * 31 : 151
17. 131071
19. 524287
21. 7^2 * 127 : 337
23. 47 * 178481
25. 31 : 601 * 1801
27. 7 * 73 : 262657
29. 233 * 1103 * 2089
31. 2147483647
33. 7 * 23 * 89 : 599479
35. 31 * 127 : 71 * 122921
37. 223 * 616318177
39. 7 * 8191 : 79 * 121369
41. 13367 * 164511353
43. 431 * 9719 * 2099863
45. 7 * 31 * 73 * 151 : 631 * 23311
47. 2351 * 4513 * 13264529
49. 127 : 4432676798593
51. 7 * 131071 : 103 * 2143 * 11119
53. 6361 * 69431 * 20394401
55. 23 * 31 * 89 : 881 * 3191 * 201961
57. 7 * 524287 : 32377 * 1212847
59. 179951 * 3203431780337
61. 2305843009213693951
63. 7^2 * 73 * 127 * 337 : 92737 * 649657
65. 31 * 8191 : 145295143558111
67. 193707721 * 761838257287
69. 7 * 47 * 178481 : 10052678938039
71. 228479 * 48544121 * 212885833
73. 439 * 2298041 * 9361973132609
75. 7 * 31 * 151 * 601 * 1801 : 100801 * 10567201
77. 23 * 89 * 127 : 581283643249112959
79. 2687 * 202029703 * 1113491139767
81. 7 * 73 * 262657 : 2593 * 71119 * 97685839
83. 167 * 57912614113275649087721
85. 31 * 131071 : 9520972806333758431
87. 7 * 233 * 1103 * 2089 : 4177 * 9857737155463
89. 618970019642690137449562111
91. 127 * 8191 : 911 * 112901153 * 23140471537
93. 7 * 2147483647 : 658812288653553079
95. 31 * 524287 : 191 * 420778751 * 30327152671
97. 11447 * 13842607235828485645766393
99. 7 * 23 * 73 * 89 * 599479 : 199 * 153649 * 33057806959
101. 7432339208719 * 341117531003194129

103. 2550183799 * 3976656429941438590393
105. 7^2 * 31 * 71 * 127 * 151 * 337 * 122921 : 29191 * 106681 * 152041
107. 16225927682921336339157801028127
109. 745988807 * 870035986098720987332873
111. 7 * 223 * 616318177 : 321679 * 26295457 * 319020217
113. 3391 * 23279 * 65993 * 1868569 * 1066818132868207
115. 31 * 47 * 178481 : 14951 * 4036961 * 2646507710984041
117. 7 * 73 * 79 * 8191 * 121369 : 937 * 6553 * 86113 * 7830118297
119. 127 * 131071 : 239 * 20231 * 629830483367 * 131105292137
121. 23 * 89 : 727 * 178639387836316422785827021027 9
123. 7 * 13367 * 164511353 : 3887047 * 177722253954175633
125. 31 * 601 * 1801 : 269089806001 * 4710883168879506001
127. 170141183460469231731687303715884105727
129. 7 * 431 * 9719 * 2099863 : 11053036065049294753459639
131. 263 * 1035079443105516238671861923746823 4569
133. 127 * 524287 : 1635372208527253988514343257209 59
135. 7 * 31 * 73 * 151 * 631 * 23311 * 262657 : 271 * 348031 * 4997161783080 1
137. 32032215596496435569 * 543904218360020429015 9
139. 562576724868 7 * 123876132205208335762278423601
141. 7 * 2351 * 4513 * 13264529 : 437557827 1 * 64667503525325872 9
143. 23 * 89 * 8191 : 724153 * 158822951431 * 5782172113400990737
145. 31 * 233 * 1103 * 2089 : 267989515778386281469002749414499 1
147. 7^3 * 127 * 337 * 443267679859 3 : 27416723625287255350687 27
149. 866562685662821831 51 * 8235109336690846723986161
151. 18121 * 55871 * 165799 * 2332951 * 728908883388253664437433
153. 7 * 73 * 103 * 2143 * 11119 * 131071 : 919 * 755824884241793470834383 19
155. 31^2 * 2147483647 : 311 * 11471 * 73471 * 4649919401 * 18158209813151
157. 852133201 * 60726444167 * 1654058017289 * 213438736861041 7
159. 7 * 6361 * 69431 * 20394401 : 6679 * 13960201 * 540701761 * 229890275929
161. 47 * 127 * 178481 : 1289 * 3188767 * 45076044553 * 1480860771531578248 1
163. 150287 * 704161 * 110211473 * 27669118297 * 362304545701296757 21
165. 7 * 23 * 31 * 89 * 151 * 881 * 3191 * 201961 * 599479
: 204856883529738048676023 1

167. 2349023 * 7963830476685650737777861629608744849069564 9

* 169. 8191 : 4057 * 6740339310641 * 33407622839523953295063270230 33

171. 7 * 73 * 32377 * 524287 * 1212847 : 93507247 * 3042645634792541312037847

* 173. 730753 * 1505447 * 70084436712553223 * 1552857432885722776798 87

175. 31 * 71 * 127 * 601 * 1801 * 122921 : 39551 * 60816001
* 5353476247914885528371 51

177. 7 * 179951 * 3203431780337 : 184081 * 27989941729 * 9213624084535989031

179. 359 * 1433 * 14894591093600398664569401970954337216649519991 21

181. 43441 * 1164193 * 7648337 * 792387109728529562534464766576467267 1

183. 7 * 2305843009213693951 : 367 * 55633 * 372017086253051463039733520 41

* 185. 31 * 223 * 616318177 : 15878556979927 91 * 7248808599285760001152755641

187. 23 * 89 * 131071 : 707983 * 10326708167438438609988500562789506664915 37

189. 7^2 * 73 * 127 * 337 * 92737 * 262657 * 649657 : 1560007
* 2076174855442583929707535 27

* 191. 383 * 7068569257 * 39940132241 * 332584516519201 * 87274497124602996457

* 193. 13821503 * 6165444023324834061655 9 * 14732265321145317331353282383

195. 7 * 31 * 79 * 151 * 8191 * 121369 * 145295143558111
: 13430419684509926257281457335 1

197. 7487 * 26828803997912886929710867041891989490486893845712448833

* 199. 164504919713 * 488416409388394117766004909858632430297754360079 9

201. 7 * 193707721 * 761838257287 : 1609 * 22111
- * 87449423397425857942678833145441

203. 127 * 233 * 1103 * 2089 : 136417 * 121793911
- * 113480555808832720110908560531753611 13

* 205. 31 * 13367 * 164511353 : 2940521 * 70171342151
- * 365572506550879718167407895968 1

207. 7 * 47 * 73 * 178481 * 10052678938039 : 79903 * 634569679 * 2232578641663
- * 421664824 63639

* 209. 23 * 89 * 524287 : 94803416684681 * 1512348937147247
- * 53469505413239602323196 57

211. 15193 * (21661351376570868717895993978244592970219652019134862941467 9)

* 213. 7 * 228479 * 48544121 * 212885833 : 66457 * 2849881972114740679
- * 4205268574191396793

* 215. 31 * 431 * 9719 * 2099863 : 1721 * 731516431 * 514851898711
- * 29792728974404776444486219 1

* 217. 127 * 2147483647 : 5209 * 62497 * 62687039338403640331 51
- * 37842880443142448408263 3

* 219. 7 * 439 * 2298041 * 9361973132609 : 3943 * 671165898617413417
- * 48153146152043477173 21

221. 8191 * 131071 : 1327
- * 23654543984183997726050862092143634585528398662470692 33

* 223. 18287 * 196687 * 1466449 * 2916841 * 146949526239878012380 9
- * 59624259998711612841506 3

225. 7 * 31 * 73 * 151 * 601 * 631 * 1801 * 23311 * 100801 * 10567201 : 115201
- * 617401 * 1348206751 * 1386136982629935 1

227. (215679573337205118357336120696157045389097155380324579848828881993727)

229. 1504073 * 20492753
- * (279897994260644052961160286863820919861232985396595065 19)

231. 7^2 * 23 * 89 * 127 * 337 * 599479 * 5812836432491129 59 : 463
- * 49823976511782561513383022047620 57

233. 1399 * 135607 * 622577
- * 116868129879077600270344856324766260085066532853492178431

* 235. 31 * 2351 * 4513 * 13264529 : 2391314881 * 72296287361
- * 732023003951580058454735371469747 51

* 237. 7 * 2687 * 202029703 * 1113491139767 : 1423 * 49297
- * 2372882351234560927 9 * 3135737341709009343 1

239. 479 * 1913 * 5737 * 176383 * 134000609
- * 71100087178244581231050142792537540968637680628 79

241. 22000409
- * 160619474372352289412737508720216839225805656328990879953332340439

* 243. 7 * 73 * 2593 * 71119 * 262657 * 97685839 : 487 * 167537836 18801
- * 19297170568857 7 * 37129901632511583 43

245. 31 * 71 * 127 * 122921 * 4432676798593 : 1471
- * 252359902034571016856214298851708529738525821631

* 247. 8191 * 524287 : 15809 * 6459570124697 * 402004106269663
- * 1282816117617265060453496956212169

249. 7 * 167 * 57912614113275649087721 : 1621324657
- * 82415946901671373595522744184328557 40327

251. 503 * 54217 * (132686104398972053177 6085755060905-
- 614293539359890335258028914694596 97)

253. 23^2 * 47 * 89 * 178481 : 4103188409
- * (893165453106007309002842289513930850163184879519052329 7)

255. 7 * 31 * 103 * 151 * 2143 * 11119 * 131071 * 9520972806333758431 : 106591
- * 949111 * 57024515776397755458643151

257. (2315841784746323908471419700173758157 06-
- 5399693312811280789151680158262592798 71)

259. 127 * 223 * 616318177 : 2499285769
- * 212343709608800988060277501855527137068669705789639 70119

261. 7 * 73 * 233 * 1103 * 2089 * 4177 * 9857737155463
- : 32801702501410292344998866375296008088651141296588 1

* 263. 23671 * 13572264529177
- * (46133875424292438138593897007663657098446474746628629049833121)

* 265. 31 * 6361 * 69431 * 20394401 : 29324808311 * 1977487384 49921
- * 3661411012473529463443561902776676348 1

* 267. 7 * 6189700196426901374495621 11 : 78903841 * 28753302853087
- * 24124332437713924084267316537353

269. 13822297 * [6862598850481177425936467066155294891-
- 536390184503541637191246347787378306 3]

* 271. 15242475217 * 248927757868131890277330541567820045-
- 256364273970773286542188386932989391

* 273. 7^2 * 79 * 127 * 337 * 911 * 8191 * 121369 * 112901153 * 23140471537
- : 108749551 * 4093204977277417 * 869775958019498449 93

275. 23 * 31 * 89 * 601 * 881 * 1801 * 3191 * 201961
- : (155672127676980623071739663722374757386075105902228986 3442401)

277. 1121297 * (2165649346499777791833321041195507196 84-
- 705171673087005634079598195092857334543)

* 279. 7 * 73 * 2147483647 * 658812288653553079 : 16183 * 34039 * 1437967
- * 833732508401263 * 203443983695186729988861 7

281. 80929 * 480092152930526528418604432730793388437 3-
- 72719062916759443910689552299987694203 19

* 283. 9623 * 68492481833
- * 2357954301179899322285089392956587038384416787385150267731105748319467 3

* 285. 7 * 31 * 151 * 191 * 32377 * 524287 * 1212847 * 420778751 * 303271526 71
- : 1491477035689218775711 * 25349242986637720573561

* 287. 127 * 13367 * 164511353 : 171377165 27
- * 5195439087774865574425619296320622091927289554884381784222891 3

289. 131071 : 12761663 * (5946410163583764888314713012024172277-
- 48890142216011074060565686979088758207)

291. 7 * 11447 * 1384260723582848564576639 3 : 272959 * 2065304407 * 5434876633
* 1170711644777651877659556633665719

293. (15914343565113172548972231940698266883214596-
82551512695809484726058110390440106801705779 1)

* 295. 31 * 179951 * 3203431780337 : 4721 * 132751 * 5794391 * 128818831
- * 3812358161 * 452824604065751 * 4410975230650827973711

297. 7 * 23 * 73 * 89 * 199 * 153649 * 262657 * 599479 * 33057806959 : 8950393
* 17088661882314173808183095080729277164831359943 3

* 299. 47 * 8191 * 178481 : 599 * 9341359 * 14718679249
- * (17998495450989130910415950680845333217092929856890964617843 9)

Appendix G.

2^n+1

Table of factorizations of 2^n+1 for all n, $0 \leq n \leq 300$. Since $2^{4*n+2}+1 = (2^{2*n+1}-2^{n+1}+1) * (2^{2*n+1}+2^{n+1}+1)$, separate tables are given for factorizations of the last two forms (see Appendices H and I).

0. 2
1. 3
2. 5
3. 3^2 : 1
4. 17
5. 3 : 11
6. 5 : 13
7. 3 : 43
8. 257
9. 3^3 : 19
10. 5^2 : 41
11. 3 : 683
12. 17 : 241
13. 3 : 2731
14. 5 : 29 * 113
15. 3^2 * 11 : 331
16. 65537
17. 3 : 43691
18. 5 * 13 : 37 * 109
19. 3 : 174763
20. 17 : 61681
21. 3^2 * 43 : 5419
22. 5 : 397 * 2113
23. 3 : 2796203
24. 257 : 97 * 673
25. 3 * 11 : 251 * 4051
26. 5 : 53 * 157 * 1613
27. 3^4 * 19 : 87211
28. 17 : 15790321
29. 3 : 59 * 3033169
30. 5^2 * 13 * 41 : 61 * 1321
31. 3 : 715827883
32. 641 * 6700417
33. 3^2 * 683 : 67 * 20857
34. 5 : 137 * 953 * 26317
35. 3 * 11 * 43 : 281 * 86171
36. 17 * 241 : 433 * 38737
37. 3 : 1777 * 25781083
38. 5 : 229 * 457 * 525313
39. 3^2 * 2731 : 22366891
40. 257 : 4278255361
41. 3 : 83 * 8831418697
42. 5 * 13 * 29 * 113 : 1429 * 14449
43. 3 : 2932031007403
44. 17 : 353 * 2931542417
45. 3^3 * 11 * 19 * 331 : 18837001
46. 5 : 277 * 1013 * 1657 * 30269
47. 3 : 283 * 165768537521
48. 65537 : 193 * 22253377

49. 3 * 43 : 4363953127297
50. 5^3 * 41 : 101 * 8101 * 268501
51. 3^2 * 43691 : 307 * 2857 * 6529
52. 17 : 858001 * 308761441
53. 3 : 107 * 2805981076243 3
54. 5 * 13 * 37 * 109 : 246241 * 279073
55. 3 * 11^2 * 683 : 2971 * 48912491
56. 257 : 5153 * 54410972897
57. 3^2 * 174763 : 571 * 160465489
58. 5 : 107367629 * 536903681
59. 3 : 2833 * 37171 * 1824726041
60. 17 * 241 * 61681 : 45622845 61
61. 3 : 7686143364045646 51
62. 5 : 5581 * 8681 * 49477 * 384773
63. 3^3 * 19 * 43 * 5419 : 77158673929
64. 274177 * 67280421310721
65. 3 * 11 * 2731 : 131 * 409891 * 7623851
66. 5 * 13 * 397 * 2113 : 312709 * 4327489
67. 3 : 7327657 * 6713103182899
68. 17^2 : 354689 * 287934790 2817
69. 3^2 * 2796203 : 139 * 168749965921
70. 5^2 * 29 * 41 * 113 : 7416361 * 47392381
71. 3 : 56409643 * 1395259814848 1
72. 97 * 257 * 673 : 577 * 487824887233
73. 3 : 1753 * 17959180384107062 7
74. 5 : 149 * 593 * 184481113 * 231769777
75. 3^2 * 11 * 251 * 331 * 4051 : 1133836730401
76. 17 : 1217 * 148961 * 2451701494075 3
77. 3 * 43 * 683 : 617 * 78233 * 35532364099
78. 5 * 13^2 * 53 * 157 * 1613 : 313 * 1249 * 3121 * 21841
79. 3 : 2014876366024381957843 63
80. 65537 : 414721 * 44479210368001
81. 3^5 * 19 * 87211 : 163 * 135433 * 272010961
82. 5 : 10169 * 181549 * 12112549 * 43249589
83. 3 : 499 * 1163 * 2657 * 155377 * 13455809771
84. 17 * 241 * 15790321 : 3361 * 889598824 81
85. 3 * 11 * 43691 : 2683142303606535261 1
86. 5 : 173 * 101653 * 500177 * 1759217765581
87. 3^2 * 59 * 3033169 : 960767918716136 11
88. 257 : 229153 * 11978243 3 * 43872038849
89. 3 : 179 * 62020897 * 1858477404602061 7
90. 5^2 * 13 * 37 * 41 * 61 * 109 * 1321 : 181 * 54001 * 29247661
91. 3 * 43 * 2731 : 224771 * 1210483 * 25829691707
92. 17 : 2912800092436188882115586 41
93. 3^2 * 715827883 : 529510939 * 2903110321
94. 5 : 3761 * 7484047069 * 1407374715781 13
95. 3 * 11 * 174763 : 2281 * 3011347479614249131
96. 641 * 6700417 : 1844674406941458432 1
97. 3 : 971 * 1553 * 31817 * 1100876018364883721
98. 5 * 29 * 113 : 197 * 19707683773 * 4981857697937
99. 3^3 * 19 * 67 * 683 * 20857 : 5347 * 242099935645987
100. 17 * 61681 : 401 * 340801 * 2787601 * 3173389601
101. 3 : 8451004001521529343311354702 51
102. 5 * 13 * 137 * 953 * 26317 : 409 * 3061 * 13669 * 1326700741
103. 3 : 415141630193 * 8142767081771726171
104. 257 : 7891988172627109114376362368 1
105. 3^2 * 11 * 43 * 281 * 331 * 5419 * 86171 : 211 * 664441 * 1564921
106. 5 : 15358129 * 586477649 * 1801439824104653
107. 3 : 643 * 8411574744904788148863556780 1
108. 17 * 241 * 433 * 38737 : 33975937 * 138991501037953
109. 3 : 104124649 * 2077756847362348863128179
110. 5^2 * 41 * 397 * 2113 : 415878438361 * 3630105520141
111. 3^2 * 1777 * 25781083 : 3331 * 17539 * 107775231312019
112. 65537 : 449 * 2689 * 183076097 * 3584298484609 93
113. 3 : 227 * 48817 * 636190001 * 4910033693446 60409
114. 5 * 13 * 229 * 457 * 525313 : 131101 * 160969 * 275415303169
115. 3 * 11 * 2796203 : 691 * 1884103651 * 345767385170491

116. 17 : 59393 * 82280195167144119832390568177
117. 3^3 * 19 * 2731 * 22366891 : 530230622637030768 1801
118. 5 : 1181 * 3541 * 157649 * 174877 * 5521693 * 104399276341
119. 3 * 43 * 43691 : 823679683 * 14316255316556095 9297
120. 97 * 257 * 673 * 4278255361 : 394783681 * 46908728641
121. 3 * 683 : 117371 * 1105418458279780045573606 1107
122. 5 : 733 * 1709 * 3456749 * 36814058 1013 * 667055378149
123. 3^2 * 83 * 8831418697 : 739 * 165313 * 131943179130295 93
124. 17 : 290657 * 3770202641 * 1141629180401976895873
125. 3 * 11 * 251 * 4051 : 229668251 * 551948541833628 8303251
126. 5 * 13 * 29 * 37 * 109 * 113 * 1429 * 14449 : 40388473189 * 118750098349
127. 3 : 56713727820156410577229101238628035243
128. 5964958912749721 7 * 57046892006851290547 21
129. 3^2 * 2932031007403 : 1033 * 1591582393 * 15686603697451
130. 5^2 * 41 * 53 * 157 * 1613 : 521 * 51481 * 34110701 * 108140989558681
131. 3 : 1049 * 4744297 * 18233112868120778178439181361 1
132. 17 * 241 * 353 * 2931542417 : 7393 * 1761345169 * 9861827 3953
133. 3 * 43 * 174763 : 4523 * 10678829044384829528438209 7033
134. 5 : 269 * 15152453 * 42875177 * 2559066073 * 9739278030221
135. 3^4 * 11 * 19 * 331 * 87211 * 18837001 : 811 * 15121 * 385838642647891
136. 257 : 383521 * 236817974387 3 * 3732007224707997 64577
137. 3 : 1097 * 15619 * 32127963626435681 * 10549821202759 2977
138. 5 * 13 * 277 * 1013 * 1657 * 30269 : 5415624023749 * 70334392823809
139. 3 : 4506937 * 5154263952466179530007417425036 5699
140. 17 * 61681 * 15790321 : 84179842077657862011867889681
141. 3^2 * 283 * 165768537521 : 1681003 * 35273039401 * 111349165273
142. 5 : 569 * 148587949 * 4999465853 * 5585522857 * 472287102421
143. 3 * 683 * 2731 : 2003 * 6156182033 * 10425285443 * 15500487753323
144. 193 * 65537 * 22253377 : 1153 * 6337 * 38941695937 * 278452876033
145. 3 * 11 * 59 * 3033169 : 7553921 * 99980285472471530088384541 1
146. 5 : 293 * 9929 * 649301712182209 * 9444732965601851473921
147. 3^2 * 43 * 5419 * 4363953127297 : 748819 * 26032885845392093851
148. 17 : 20988936657440586486151264256610222593863921
149. 3 : 1193 * 650833 * 38369587 * 79845595735042598563591246 57
150. 5^3 * 13 * 41 * 61 * 101 * 1321 * 8101 * 268501 : 1201 * 63901 * 13334701 * 1182468601

* 151. 3 : 18717738334417 * 508340508241007796773064606214 99

* 152. 257 : 27361 * 6939446046394048 1 * 1169955781771735890448 1

153. 3^3 * 19 * 307 * 2857 * 6529 * 43691 : 123931 * 26159806891 * 27439122228481

154. 5 * 29 * 113 * 397 * 2113 : 8317 * 869467061 * 3019242689 * 76096559910757

155. 3 * 11 * 715827883 : 11161 * 5947603221397891 * 291260560431685 21

156. 17 * 241 * 858001 * 308761441 : 84159375948762099254554456081

* 157. 3 : 15073 * 2350291 * 17751783757817897 * 96833299198971305921

158. 5 : 317 * 381364611866507317969 * 60446290980621507572531 3

159. 3^2 * 107 * 28059810762433 : 6043 * 44751303665181020844276987 37

160. 641 * 6700417 : 3602561 * 94455684953484563055991838558081

161. 3 * 43 * 2796203 : 81034674927597923271498003615644102652 19

162. 5 * 13 * 37 * 109 * 246241 * 279073 : 3618757 * 106979941 * 168410989 * 4977454861

* 163. 3 : 11281292593 * 1023398150341859 * 337570547050390415041769

164. 17 : 13121 * 8562191377 * 122438641224656121551063920565523 53

165. 3^2 * 11^2 * 67 * 331 * 683 * 2971 * 20857 * 48912491 : 415365721
- * 2252127523412251

166. 5 : 997 * 13063537 * 46202197673 * 209957719973 * 148067197374074653

167. 3 : 623574031927851911766905528625614088386531218336 43

168. 97 * 257 * 673 * 5153 * 54410972897 : 2017 * 25629623713
- * 1538595959564161

* 169. 3 * 2731 : 4929910764223610387 * 185262386460110867327426140 43

170. 5^2 * 41 * 137 * 953 * 26317 : 1021 * 4421 * 550801 * 23650061
- * 722690435284374 6841

171. 3^3 * 19^2 * 571 * 174763 * 160465489 : 191774583879402681163497666122 11

* 172. 17 : 3855260977 * 640821507674234 57 * 142534327510312632737 2769

* 173. 3 : 347 * 4153 * 35374479827 * 47635010587 * 164346424772818922162 3609

174. 5 * 13 * 107367629 * 536903681 : 349 * 29581 * 27920807689
- * 22170214192500421

175. 3 * 11 * 43 * 251 * 281 * 4051 * 86171 : 1051 * 110251 * 347833278451
- * 34010032331525251

176. 65537 : 5304641 * 2755095654778488426047776238280116663497 61

177. 3^2 * 2833 * 37171 * 1824726041 : 13099 * 445376254389 7
- * 189868549646599927 3

178. 5 : 1069 * 57901779199499995610614 9 * 123794003928545064364330189

* 179. 3 : 58745093521 * 43478681906658793734959505627757077071438 03

180. 17 * 241 * 433 * 38737 * 61681 * 4562284561 : 168692292721
* 46977549506243496 1

181. 3 : 1811 * 31675363 * 17810163630112624579342811733978085990447 907

182. 5 * 29 * 53 * 113 * 157 * 1613 : 1093^2 * 4733 * 8861085190774909
- * 5563385259123251 57

183. 3^2 * 768614336404564651 : 17723039943798878297697950773025614 51

* 184. 257 : 43717618369 * 549675408461419937 * 39702995674729028797917 77

185. 3 * 11 * 1777 * 25781083 : 1481 * 28136651
- * 77842936539788760854061833087328 1

186. 5 * 13 * 5581 * 8681 * 49477 * 384773 : 373 * 95108821572763 3
- * 4611545283086450689

187. 3 * 683 * 43691 : 219116582537688808475015771642457906201586577613 1

* 188. 17 : 1198107457 * 23592342593 * 4501946625921233 * 1813523068524760695 37

189. 3^4 * 19 * 43 * 5419 * 87211 * 77158673929 : 379 * 119827 * 127391413339
- * 56202143607667

190. 5^2 * 41 * 229 * 457 * 525313 : 761 * 54721 * 27669663125095374 1
- * 241692362066080720 1

191. 3 : 10461836225644467939726315705346110693503925740773390085483

192. 274177 * 67280421310721 : 769 * 44249982694530359355647316431477068 9

* 193. 3 : 6563 * 35679139 * 1871670769 * 74550999758440 49
* 1280761337388845898643

194. 5 : 389 * 3881 * 4657 * 5821 * 3555339061 * 4959325597 * 394563864677
\- * 17637260034881

195. 3^2 * 11 * 131 * 331 * 2731 * 409891 * 7623851 * 22366891 : 107251
\- * 571403921126076957182161

196. 17 * 15790321 : 7057 * 273617 * 1007441 * 375327457 * 1405628248417
* 3645655619978 41

* 197. 3 : 197002597249 * 13489593528538113 13 * 25195157386725301225914401 0843

198. 5 * 13 * 37 * 109 * 397 * 2113 * 312709 * 4327489 : 42373 * 235621
\- * 8463901912489 * 1597560728227 3

199. 3 : 267823007376498379256993682056860433753700498963798805883563

200. 257 * 4278255361 : 1601 * 25601 * 82471201
\- * 43236320312700288550654317261 8401

201. 3^2 * 7327657 * 6713103182899 : 2011 * 9649 * 6324667
\- * 59151549118532676874448563

202. 5 : 809 * 9491060093 * 5218735279937 * 600503817460697
\- * 534250373638732486 57

203. 3 * 43 * 59 * 3033169 : 596834617 * 369202271 3
\- * 252715814615565962418688965855731

204. 17^2 * 241 * 354689 * 2879347902817 : 8161 * 40932193 * 1467129352609
\- * 7375399858353 13

205. 3 * 11 * 83 * 8831418697
\- : 212582056338943753339024389383459784675730486 3651

206. 5 : 41201 * 17325013 * 520379897 * 473000157711296729
* 1170700974576566230059 77

207. 3^3 * 19 * 139 * 2796203 * 168749965921
: 611314287240422783484044389824161303296 9

* 208. 65537 : 928513 * 18558466369 * 23877647873 * 21316654212673
\- * 7156684702671112 97

* 209. 3 * 683 * 174763 : 419 * 341062328465463944070 7
\- * 160779201878039402409551431700 3

210. 5^2 * 13 * 29 * 41 * 61 * 113 * 1321 * 1429 * 14449 * 7416361 * 47392381
\- : 421 * 146919792181 * 1041815865690181

* 211. 3 : 4643 * 9878177 * 5344743097 * 199061567251
\- * 22481127512575175864234185190299

212. 17 : 1692645313
\- * (228741095328993655528152185934252940490841504438551857)

213. 3^2 * 56409643 * 139525981484 81 : 5113 * 17467 * 102241
\- * 203525545766301306933226271929

214. 5 : 857 * 843589 * 8174912477117 * 2352856910 4401
\- * 37866809061660057264219253397

215. 3 * 11 * 2932031007403 : 9084611
\- * 599046083787056613774301826087116989241307 21

216. 97 * 257 * 577 * 673 * 487824887233 : 209924353 * 4261383649
- * 249290608182653604517081 93

217. 3 * 43 * 715827883 : 16233337
- * 1405086085901642802259342330988668427458089059 47

218. 5 : 5669 * 666184021 * 74323515777853 * 1746518852140345553
- * 17185764601280956696 9

* 219. 3^2 * 1753 * 17959180387410706 27 : 9070197542196643
- * 3278244690156222434135906137

220. 17 * 353 * 61681 * 2931542417 : 109121 * 148721 * 3404676001
- * 11035465708081 * 2546717317681681

* 221. 3 * 2731 * 43691 : 443 * 4714692062809
- * 450751357540644651584540145836674148752691 3

222. 5 * 13 * 149 * 593 * 184481113 * 231769777 : 3109 * 1398316729
- * 4345052821 * 145303029800169087354 1

* 223. 3 : 219256122131
- * 204934959209050439504076504509181712603183031547084055 13

224. 641 * 6700417
- : (627710173392517912684516887184569188435362943871574081536 1)

225. 3^3 * 11 * 19 * 251 * 331 * 4051 * 18837001 * 1133836730401 : 4714696801
- * 2819414729537101777586472 01

226. 5 : 58309 * 2362153 * 150791162139013261783 69
* 10384593717069655112945804582584321

* 227. 3 : 297371 * 34546315797142103 87
* 6998217065826544471311754525871203110339965 9

228. 17 * 241 * 1217 * 148961 * 245170149407 53 : 90289 * 9036489073
- * 2903405716492099337900007499 3

229. 3 : 18754643
- * 153334171410037943391643424472654261588519461824519634843722 97

230. 5^2 * 41 * 277 * 1013 * 1657 * 30269 : 461 * 5981 * 15096281 * 1021622741
- * 7834788541 * 35900691276519040818 1

231. 3^2 * 43 * 67 * 617 * 683 * 5419 * 20857 * 78233 * 35532364099 : 14323
- * 7018079616527704034924570385105 7

232. 257 : 929 * 5569 * 8353 * 39594977
- * 15694604006012505869851221169365594050637743819041

233. 3 : 467 * 27961
- * 3523693740136601394725745315688906781550405630076207428391209 13

234. 5 * 13^2 * 37 * 53 * 109 * 157 * 313 * 1249 * 1613 * 3121 * 21841 : 7489
- * 21061 * 348661 * 111238828506 1 * 37024440548701366 9

* 235. 3 * 11 * 283 * 165768537521 : 328006342451 * 461797907949997211
- * 2354573745100921150868346 91

236. 17 : 1889 * 11329 * 84961 * 765373489
* 4667813439458532797392797231517680422795032583489

237. 3^2 * 2014876366024381957843 63 : 647011 * 13664473
- * 1377569469289849218474470921659987 3

238. 5 * 29 * 113 * 137 * 953 * 26317 : 2381 * 9521 * 42841 * 823481
- * 536296539263941 * 18292898984156916156396101

239. 3 : 340337
- * (865243892954328763149122536751767863337164779260761616731654311899)

240. 193 * 65537 * 414721 * 22253377 * 44479210368001 : 23041
- * 14768784307009061644318236958041601

* 241. 3 : 2411 * 10411181203
- * (469256702683715825268862614984478252452809014962290428515 47)

242. 5 * 397 * 2113 : 3389 * 91961 * 40369625840108070148092 13
- * 13392725398336683869589204684 00193

* 243. 3^6 * 19 * 163 * 87211 * 135433 * 272010961 : 1459 * 139483
- * 10429407431911334611 * 9181250516025688 99753

* 244. 17 : 977 * 37831175201
- * (44990997735694705478430495237762030756941538919564241286913)

* 245. 3 * 11 * 43 * 281 * 86171 * 4363953127297 : 491 * 15162868758218274451
- * 5064728203579612588500033064 1

246. 5 * 13 * 10169 * 181549 * 12112549 * 43249589 : 2953 * 802333429
- * 6027043735173469 * 125965976976392564317

247. 3 * 2731 * 174763 : 207481 * 10049443 * 355011619
- * 213379941663827592701819558102368170760508803

248. 257 : 8929 * [19710742227301430191978141446603 93-
- 25387889623676342705850752210599969]

* 249. 3^2 * 499 * 1163 * 2657 * 155377 * 13455809771 : 9202419446683
- * 338809829056758737705201652562794 8593

250. 5^4 * 41 * 101 * 8101 * 268501 : 7001 * 28001 * 96001 * 3775501
- * 47970133603445383501 * 9429186693217124 3501

251. 3 : 238451
- * 505834572395185468850566542884631380649090312167736435890119912860 8233

252. 17 * 241 * 433 * 3361 * 38737 * 15790321 * 88959882481 : 1009 * 21169
- * 2627857 * 269389009 * 14752046791901285 71777

* 253. 3 * 683 * 2796203 : 4049 * 85009 * 31797547 * 81776791273
- * 28225515294603308476042620861490152426 89

254. 5 : 509 * 18797 * 26417 * 72118729 * 140385293 * 2792688414613
- * 8988357880501 * 9013356691791351770949 7

255. 3^2 * 11 * 307 * 331 * 2857 * 6529 * 43691 * 2683142303606535261 1 : 12241
- * 41856298635756 1 * 5136614945549475393 1

256. 1238926361552897
- * 9346163971535797776916355819960689658405123754163818858028032 1

* 257. 3 : 37239639534523
- * (207291818941070689731090144208461044358640967598948126539875681 7)

258. 5 * 13 * 173 * 101653 * 500177 * 1759217765581 : 17029 * 46957
- * 96758771543686753 * 59516319662966858346861 49

259. 3 * 43 * 1777 * 25781083
- : (15674387597066558351998609628396777807819329150528738391263023885 1)

* 260. 17 * 61681 * 858001 * 308761441 : 42641 * 5746001 * 2400573761
- * 65427463921 * 17330834391887481052192384 1

* 261. 3^3 * 19 * 59 * 3033169 * 9607679187161361 1 : 523 * 6929826139
- * 345341290183269055 3 * 335638564505157027 61

262. 5 : 269665073 * 642811237 * 2745098189 * 810791440841
- * 12450751815271172041 * 3085446954097694273 09

263. 3 : 1579 * 92051 * (339904538980610598731207571677867 98-
- 87251916629809165388262620062478 2107)

* 264. 97 * 257 * 673 * 229153 * 119782433 * 43872038849 : 16875081675650881
- * 869453889972104428282594949923 21

* 265. 3 * 11 * 107 * 28059810762433
- : (59836529357134758526082346043436582252063106464231801956 1687971)

266. 5 * 29 * 113 * 229 * 457 * 525313 : 1597 * 2129 * 126848469231149
- * 679253585011429 * 449329386292232535250647435097

267. 3^2 * 179 * 62020897 * 18584774046020617 : 3739 * 4273
- * 799336446517079299871633769103325135089545331 3

268. 17 : 75041 * (37178452055311499239627180638943704 54-
- 480914019476911447668359054669033312 81)

269. 3 : (31618959834403142430329783639705711371 13-
- 29238126975833537078842730941452670118571)

270. 5^2 * 13 * 37 * 41 * 61 * 109 * 181 * 1321 * 54001 * 246241 * 279073
- * 29247661 : 541 * 30241 * 49681 * 165041853060421 * 166242935471754241

271. 3 : 1627 * (77735611147887258587166032304132050082 6-
- 869669642227003164299551889222993657329)

272. 65537 : 5441 * (21281073776366651780284822120974177 03-
- 77111325319898744458909489790324886 41)

* 273. 3^2 * 43 * 2731 * 5419 * 224771 * 1210483 * 22366891 * 25829691707 : 547
- * 105310750819 * 29265311314715720577912752682 7

274. 5 : 189061 * 168434085820849 * 20687567010495774491714761 3
- * 92152570791184058739061733088636270 1

275. 3 * 11^2 * 251 * 683 * 2971 * 4051 * 48912491
- : 16571548087550218188206306330834006188611355744089553953096 01

276. 17 * 241 * 2912800092436188882115586 41
- : (10174244254711295325200644161598832689111329815494248 1)

* 277. 3 : 25792643401363
- * 313828000939967901734463105154262276920587713495384512820233434582 2857

278. 5 : 557 * 1408349 * 15736774913 * 492717674609 * 12763660054721
- * 125116389129996763586027250922976428790 9

* 279. 3^3 * 19 * 529510939 * 715827883 * 2903110321 : 26227 * 119232435043
- * 85384915399027 * 64443653761406111990221 87

280. 257 * 5153 * 4278255361 * 54410972897 : 4481 * 557761 * 736961
- * 342124938170536803983033419004621122511 6161

281. 3 : 563 * (230037761068766023791528941009297679886 60-
- 82698699987591772424404664185062409956777)

282. 5 * 13 * 3761 * 7484047069 * 140737471578113 : 1129 * 5641 * 1768141
- * 54865357 * 180846660913 * 27009726848416765399906 9

283. 3 : 1699 * 62827 * 2486265371 * (19520023475743393993745416514568 70-
- 5439204416824204556768195319549841)

284. 17 : 2273 * 1433633 * 561089862628529469701880307617682 1751-
- 71538701774485416358584106265670728689

285. 3^2 * 11 * 331 * 571 * 2281 * 174763 * 160465489 * 30113474796142491 31
- : 1101811 * 1565399070589631354726923722004116936 1

286. 5 * 53 * 157 * 397 * 1613 * 2113 : 25741 * 958673 * 3426853 * 9467173
* 417016557089611564 9 * 66152134935110533966893766129 7

287. 3 * 43 * 83 * 8831418697 : 1723 * (1526248324930356396710912223714122 7-
376508917584181421669149004824245 37)

* 288. 641 * 6700417 * 184467440694145843 21 : 3457 * 816769
- * 1562985901350085709953 * 1422346738975853644793916289

289. 3 * 43691 : 72251 * 79187 * 1077971
- * (1230412337921150834061640052681035181786429742009751539987008491003)

290. 5^2 * 41 * 107367629 * 536903681 : 17401 * 168781 * 244716883381
- * 390209519243007072 1 * 120045415019548110853022141 41

* 291. 3^2 * 971 * 1553 * 31817 * 1100876018364883721 : 25609 * 5636963037465601
* 581546606903256979 * 996955034272550265 61

292. 17 : (4680689283856815455580068217852431436239587-
3016220961641455433119356187954120788285464 1)

293. 3 : 587 * 26371 * 33403 * (1025928988351831662044095959792167736 1-
598095416654999480428811798476740090801)

294. 5 * 13 * 29 * 113 * 197 * 1429 * 14449 * 19707683773 * 4981857697937
- : 540961 * 40544859693521152369 * 17059410504738323992180849

295. 3 * 11 * 2833 * 37171 * 1824726041
- : 1003890377714991094612674101710875457061194219156059132543172818859101 1

296. 257 : 80513 * [6152896135288560374679945371974689688835 1-
681517425644081045653736005815642604514 57]

* 297. 3^4 * 19 * 67 * 683 * 5347 * 20857 * 87211 * 2420999356459 87 : 23761
* 694387 * 6215074747201 * 1497386689717526522806369894554 7

298. 5 : 1789 * 12961064789 * 14641916303149 * 272433866023955884372436021 21
- * 1101180895197174591531324233692764 1

299. 3 * 2731 * 2796203 : 2393 * (1857865853553681419830219300769353664 4-
657842577220295668204930105806809574587)

300. 17 * 241 * 401 * 61681 * 340801 * 2787601 * 3173389601 * 456228456 1
- : 14615030311274778250999793695434731225480429568 01

Appendix H.

$2^n-2^{(n+1)/2}+1$

Table of factorizations of $2^n-2^{(n+1)/2}+1$ for odd n, $1 \leq n \leq 299$. Since $2^{4*n+2}+1 = (2^{2*n+1}-2^{n+1}+1) * (2^{2*n+1}+2^{n+1}+1)$, some of these factorizations also occur in the table for 2^n+1 (see Appendix G). Algebraic factors of $2^n-2^{(n+1)/2}+1$ are taken to be those also dividing $2^{2*m}+1$ for $m < n$.

1. 1
3. 5 : 1
5. 5^2 : 1
7. 113
9. 13 : 37
11. 5 : 397
13. 5 : 1613
15. 13 * 41 : 61
17. 137 * 953
19. 5 : 229 * 457
21. 5 * 29 : 14449
23. 277 * 30269
25. 41 : 101 * 8101
27. 5 * 109 : 246241
29. 5 : 107367629
31. 5581 * 384773
33. 13 * 2113 : 312709
35. 5^2 * 29 : 47392381
37. 5 : 149 * 184481113
39. 13^2 * 53 * 157 : 313 * 1249
41. 181549 * 12112549
43. 5 : 175921765581
45. 5^2 * 109 * 1321 : 181 * 54001
47. 140737471578113
49. 113 : 4981857697937
51. 5 * 26317 : 409 * 3061 * 13669
53. 5 : 18014398241046653
55. 41 * 2113 : 41587438361
57. 13 * 525313 : 131101 * 160969
59. 5 : 1181 * 3541 * 157649 * 174877
61. 5 : 733 * 1709 * 368140581013
63. 13 * 37 * 113 * 1429 : 118750098349
65. 41 * 53 * 157 : 108140989558681
67. 5 : 269 * 42875177 * 2559066073
69. 5 * 1013 * 1657 : 70334392823809
71. 4999465853 * 472287102421
73. 9444732965601851473921
75. 5^3 * 1321 * 268501 : 63901 * 13334701
77. 5 * 29 * 397 : 869467061 * 3019242689
79. 604462909806215075725313
81. 13 * 37 * 279073 : 3618757 * 4977454861
83. 5 : 13063537 * 1480671974074653
85. 5^2 * 26317 : 1021 * 4421 * 550801 * 23650061
87. 13 * 536903681 : 2217021419250042 1
89. 1069 * 57901779199499995 6106149

91. 5 * 29 * 1613 : 1093^2 * 8861085190774909
93. 5 * 8681 * 49477 : 461154528308645068 9
95. 41 * 525313 : 761 * 241692362066080720 1
97. 389 * 4657 * 49593255 97 * 17637260034881
99. 5 * 109 * 397 * 4327489 : 42373 * 159756072822 73
101. 5 : 9491060093 * 5342503736387324865 7
103. 41201 * 520379897 * 4730001577112967 29
105. 13 * 41 * 61 * 113 * 1429 * 7416361 : 1041815865690181
107. 5 : 857 * 37866809061660057264219253397
109. 5 : 7432351577785 3 * 1746518852140345553
111. 13 * 593 * 231769777 : 1453030298001690873541
113. 10384593717069655112945804582584321
115. 5^2 * 1013 * 1657 : 461 * 5981 * 35900691276519040818 1
117. 5 * 109 * 1613 * 3121 * 21841 : 7489 * 370244405487013669
119. 113 * 137 * 953 : 2381 * 42841 * 823481 * 536296539263941
121. 2113 : 3389 * 91961 * 40369625840108070148092 13
123. 5 * 10169 * 43249589 : 802333429 * 6027043735173469
125. 5^4 * 268501 : 28001 * 96001 * 9429186693217124350 1
127. 509 * 26417 * 140385293 * 9013356691791351770949 7
129. 13 * 173 * 101653 * 500177 : 59516319662966858346861 49
131. 5 : 642811237 * 2745098189 * 3085446954097694273 09
133. 5 * 29 * 229 * 457 : 1597 * 4493293862922325352506474350 97
135. 13 * 37 * 41 * 61 * 279073 * 29247661 : 541 * 49681 * 165041853060421
137. 189061 * 92152570791184058739061733088636270 1
139. 5 : 1408349 * 15736774913 * 492717674609 * 12763660054721
141. 5 * 3761 * 7484047069 : 1129 * 1768141 * 54865357 * 180846660913
143. 53 * 157 * 2113 : 958673 * 66152134935110533966893766129 7
145. 41 * 536903681 : 168781 * 12004541501954811085302214141
147. 5 * 29 * 197 * 14449 * 19707683773 : 540961 * 40544859693521152369
* 149. 5 : 12961064789 * 11011808951971745915313242336927641
151. 28544953854119197621164963810352643584420741 13
153. 13 * 37 * 137 * 953 * 1326700741 : 2582029 * 4260133 * 12458723489217613
155. 5^2 * 8681 * 49477 : 37201 * 87421 * 52597081 * 248658996938348096 41
* 157. 5 : 2790467761 * 5941035366826969 * 2203942033439148343973
159. 13 * 15358129 * 586477649 : 207973 * 30007459254393181618012897
161. 113 * 277 * 30269 : 3221 * 169373 * 209160253 * 27037028118448801270021
163. 5 : 653 * 9781 * 7807049 * 4826612561 * 971613420158567993294 7173
165. 5^2 * 397 * 1321 * 4327489 * 3630105520141 : 661 * 3301 * 8581
- * 12127627350301

167. 187072209578355573530071639244871112681892570202113

* 169. 53 * 157 : 677 * 615946323850313 * 215656329382891550920192462661

171. 5 * 109 * 229 * 457 * 275415303169 : 4598533 * 414356063712278353559190 73

* 173. 5 : 13625405957 * 175739665310505752968877740350313227534889

175. 41 * 101 * 113 * 8101 * 7416361 : 701
- * 243006592469351719855032275196 3101

177. 13 * 5521693 * 104399276341 : 709 * 12037 * 2995240087117909078735942093

* 179. 5 : 31815461 * 4161150138309903362 21 * 11575709336636595278866333

* 181. 5 : 9413 * 178925762979037 * 3830538323149121 * 95016376135553173181

183. 13 * 3456749 * 667055378149 : 5080081 * 4209508589941 * 19125556519918081

185. 41 * 593 * 231769777 : 1392776941 * 4964166554103541
- * 125871072511565076 1

* 187. 5 * 397 * 26317 : 26509131221 * 35155077044989397
* 402929206562919183985 3

189. 5 * 29 * 109 * 14449 * 246241 * 40388473189 : 757
- * 456376431053626339473533320957

191. 25212001 * 5972216269 * 208442527153792520909384850034470049446 77

193. 773 * (1624088417952569408495676435479544179453581140199350727 7)

195. 5^2 * 521 * 1321 * 1613 * 3121 * 21841 * 51481 * 34110701 : 2341
- * 723447661 * 8925278993793241

* 197. 5 : 4729 * 1079423677 * 152874915601
- * 5148036970917050130439411855366400 9

199. 797 * 10081167153444104614441418396101802392231785037514425526 29

201. 13 * 15152453 * 9739278030221 : 3217 * 192961 * 214473433 * 71848008781
- * 175132692529

203. 5 * 29^2 * 107367629 : 28474083676894571496726280348891354240661831606009

* 205. 5^2 * 10169 * 43249589 : 61213422340181
- * 764015570526610702664053401802697 21

207. 13 * 37 * 277 * 30269 * 54156240237 49 : 829 * 853669 * 26785337149
- * 4968170811091506859 21

209. 2113 * 525313
- : (7412273714692824494293268130021826310122558175990916 49)

211. 5 : 95110361 * 692040084811035904765399505762494136748583495458599 7077

213. 5 * 569 * 148587949 * 5585522857 : 266677 * 1396429 * 18369973
- * 40524027877 * 20111008087273

215. 41 * 173 * 101653 * 500177 : 129001
- * 1131832377932535124189124787988905860893840561

217. 113 * 5581 * 384773
: 867988564747274927163124868127898657976489313137639569

* 219. 5 * 293 * 9929 * 649301712182209 : 877 * 1013533 * 704710824913
- * 1424068687655254366706 17

221. 5 * 1613 * 26317
- : (158777255042257565172049601729905231608119893621090301769 01)

223. 95768689
- * (1407555378937610798591333702345012798966237668393127706912 17)

* 225. 13 * 37 * 41 * 61 * 101 * 1201 * 8101 * 29247661 * 1182468601
- : 413150254353901 * 3192261504216112476901

227. 5 : (43135914667441023671467224139231 40-
4923981944248202813145368713022669)

* 229. 5 : 2749 * 5523481 * 84948746297 * 6211454306149
- * 215358059798758478041282728260139 97

231. 13 * 113 * 1429 * 2113 * 8317 * 312709 * 76096559910757
- : 3931002956111648245378728475226109181

233. 30757
- * (448791907324548154074503746287155793437224647112081444788151182253)

* 235. 5^2 * 3761 * 7484047069 : 941 * 894434441 * 3357909154141
- * 38425816980821 * 722501809616926841

237. 5 * 317 * 3813646118665073179 69 : 151681
- * 2408840984250243046611173150925486103064449

239. 883423532389192164791648750371459256584513952652893606156996040365965313
-
241. 353369412955676865916659500148583702899651180218140617043559828202455040 1
-
* 243. 5 * 109 * 246241 * 106979941 * 168410989 : 3333950193493
* 1753477469677913202190537606674204157

* 245. 5^2 * 29 * 197 * 47392381 * 19707683773 : 306178659371201
- * 1372226516822701 * 1008787906424294727221

247. 53 * 157 * 525313 : 515737
* 1003198718770634131850180074656407339351581886584164464223 13

* 249. 13 * 997 * 46202197673 * 209957719973 : 136453 * 218166829 * 41732461753
- * 57914874054272283787177 09

* 251. 5 : 1912621 * 57762875981
- * (6550601480990604338005798095640999072287322310242181482277)

* 253. 5 * 397 * 1013 * 1657 : 6994042018866541
* 6211095415428845718023045687903315012830989259295 29

255. 13 * 41 * 61 * 137 * 953 * 1326700741 * 7226904352843746841 : 51001
- * 2949879781 * 611787251461 * 15455023589221

* 257. 229887342 97
* 1007381161062241802842574173831975781810739698060547170245057092631 3

259. 5 * 29 * 149 * 184481113
- : (2324142199257037224075349680459152992437029352688075605024646600 21)

261. 5 * 109 * 349 * 29581 * 107367629 * 27920807689
- : 219681126844282487641411054552829164292094374447461

263. (14821387422376473014217086081112052205 21-
3113519331257181635156759293972302528513)

265. 41 * 15358129 * 586477649 : 1061 * 3181
- * 4756594885524903060764846976454486760319939645324949564 1

* 267. 5 * 123794003928545064364330189 : 3401264941 * 11221454641
- * 1003805584154595697911113729202066 1

* 269. 5 : 2153 * 3229 * 5381 * 4273873 * 1633401082697
- * 391869517930421432788515 7 * 185382112947811828276076281

271. 10474693 * (3622325905044068682146172720064144471-
3805585951185187405476222442 7178428941)

* 273. 13^2 * 53 * 113 * 157 * 313 * 1249 * 1429 * 4733 * 5563385259123251 57
: 503413 * 467811806281 * 2757007179515465669468544 97

* 275. 5^3 * 397 * 268501 * 3630105520141 : 12101 * 35201 * 69861742060 1
- * 18735216413769901 * 2251172339268843846064 01

277. 5 : 1109 * (437932572638802766212683026786185506456 8-
0821998779077741118733674691977527385753)

279. 13 * 37 * 373 * 5581 * 384773 * 9510882157276 33 : 1117 * 140617
- * 16876658717031589479860902742568825114336243721

281. 91568909 * [4243075326420519154420550990344373124 8-
1773796224996983001701169936733055251 89]

283. 5 : 3108270227561166513471139050917630250627 84-
9827446163307471742778796333223910258298061

285. 5^2 * 229 * 457 * 1321 * 54721 * 275415303169 * 27669663125095374 1
- : 185821 * 247381 * 3996146881 * 2348041208209891332684 1

287. 113 * 181549 * 12112549 : 2297 * 16073
- * 271045976052226203446586369309057196585379669221190596056698263 21

* 289. 137 * 953 : 7698961 * 21886549 * 113478990853
- * 39841016052722109417874918118447229080523618788169942631 3

291. 5 * 3881 * 5821 * 3555339061 * 394563864677 : 580837 * 856752889
- * 50455592168903227107903715726570129520096917

* 293. 5 : 22396921 * 796088615657 * (17851264859864792782699664244183 0-
- 022499681356862625633687425548906 69)

295. 41 * 5521693 * 104399276341 : 677321 * 824821 * 533194801
- * 904180137721102617056229880450944144447468882982 1

297. 13 * 37 * 2113 * 235621 * 279073 * 312709 * 8463901912489
- : (14395319900697912562721731235410947916411839815137202 89)

299. 5 * 1013 * 1613 * 1657 : 6542689297 * (11499423839656726888268551656897 -
- 27788225835680565585702198104620631941 3)

Appendix I.

$2^{n}+2^{(n+1)/2}+1$

Table of factorizations of $2^{n}+2^{(n+1)/2}+1$ for odd n, $1 \leq n \leq 299$. Since $2^{4*n+2}+1 = (2^{2*n+1}-2^{n+1}+1) * (2^{2*n+1}+2^{n+1}+1)$, some of these factorizations also occur in the table for $2^{n}+1$ (see Appendix G). Algebraic factors of $2^{n}+2^{(n+1)/2}+1$ are taken to be those also dividing $2^{2*m}+1$ for $m < n$.

1. 5
3. 13
5. 41
7. 5 : 29
9. 5 : 109
11. 2113
13. 53 * 157
15. 5^2 : 1321
17. 5 : 26317
19. 525313
21. 13 * 113 : 1429
23. 5 : 1013 * 1657
25. 5^3 : 268501
27. 13 * 37 : 279073
29. 536903681
31. 5 : 8681 * 49477
33. 5 * 397 : 4327489
35. 41 * 113 : 7416361
37. 593 * 231769777
39. 5 * 1613 : 3121 * 21841
41. 5 : 10169 * 43249589
43. 173 * 101653 * 500177
45. 13 * 37 * 41 * 61 : 29247661
47. 5 : 3761 * 7484047069
49. 5 * 29 : 197 * 19707683773
51. 13 * 137 * 953 : 1326700741
53. 15358129 * 586477649
55. 5^2 * 397 : 3630105520141
57. 5 * 229 * 457 : 275415303169
59. 5521693 * 10439276341
61. 3456749 * 667055378149
63. 5 * 29 * 109 * 14449 : 40388473189
65. 5^2 * 1613 : 521 * 51481 * 34110701
67. 15152453 * 97392780302221
69. 13 * 277 * 30269 : 5415624023749
71. 5 : 569 * 148587949 * 5585522857
73. 5 : 293 * 9929 * 64930171218220 9
75. 13 * 41 * 61 * 101 * 8101 : 1201 * 1182468601
77. 113 * 2113 : 8317 * 7609655991075 7
79. 5 : 317 * 3813646118665073179 69
81. 5 * 109 * 246241 : 106979941 * 168410989
83. 997 * 46202197673 * 209957719973
85. 41 * 137 * 953 : 722690435284374 6841
87. 5 * 107367629 : 349 * 29581 * 27920807689
89. 5 : 123794003928545064364330189

91. 53 * 113 * 157 : 4733 * 5563385259123251 57
93. 13 * 5581 * 384773 : 373 * 95108821572763 3
95. 5^2 * 229 * 457 : 54721 * 276696631250953741
97. 5 : 3881 * 5821 * 355533906 1 * 394563864677
99. 13 * 37 * 2113 * 312709 : 235621 * 8463901912489
101. 809 * 5218735279937 * 6005038174606 97
103. 5 : 17325013 * 11707009745765662300597 7
105. 5^2 * 29 * 1321 * 14449 * 47392381 : 421 * 146919792181
107. 843589 * 817491247711 7 * 23528569104401
109. 5669 * 666184021 * 17185764601280956696 9
111. 5 * 149 * 184481113 : 3109 * 1398316729 * 4345052821
113. 5 : 58309 * 2362153 * 150791162139013261783 69
115. 41 * 277 * 30269 : 15096281 * 1021622741 * 7834788541
117. 13^2 * 37 * 53 * 157 * 313 * 1249 : 21061 * 348661 * 1112388285061
119. 5 * 29 * 26317 : 9521 * 18292898984156916156396101
121. 5 * 397 : 13392725398336683869589204684001 93
123. 13 * 181549 * 12112549 : 2953 * 125965976976392564317
125. 41 * 101 * 8101 : 7001 * 3775501 * 47970133603445383501
127. 5 : 18797 * 72118729 * 279268841461 3 * 8988357880501
129. 5 * 1759217765581 : 17029 * 46957 * 96758771543686753
131. 269665073 * 81079144084 1 * 12450751815271172041
133. 113 * 525313 : 2129 * 12684846923114 9 * 6792535850114 29
135. 5^2 * 109 * 181 * 1321 * 54001 * 246241 : 30241 * 16624293547 1754241
* 137. 5 : 168434085820849 * 20687567010495774491714761 3
139. 557 * 125116389129996763586027250922976428790 9
141. 13 * 14073747157811 3 : 5641 * 27009726848416765399906 9
143. 5 * 397 * 1613 : 25741 * 3426853 * 9467173 * 417016557089611564 9
145. 5^2 * 107367629 : 17401 * 244716883381 * 390209519243007072 1
147. 13 * 113 * 1429 * 4981857697937 : 17059410504738323992180849
* 149. 1789 * 14641916303149 * 272433866023955884372436021 21
* 151. 5 : 437368927017637926120 1 * 1305303239018992106700 77
153. 5 * 109 * 409 * 3061 * 13669 * 26317 : 613 * 318194713
- * 2384951978791432 09

155. 41 * 5581 * 384773 : 8973817381 * 57805828745692758010628581

157. 18268770466636286477546120855244518477157892096 1

159. 5 * 1801439824104653 : 10177 * 797186200486710330329346259 3

161. 5 * 29 * 1013 * 1657 : 1933 * 298817 * 115927640417
- * 17935157473638791517 7

163. 11692013098647223345629483497433542615764159168513

165. 13 * 41 * 61 * 2113 * 312709 * 415878438361 : 391249826881
- * 13379250952981

* 167. 5 : 75005713 * 27395325377910797 * 18208260781190156536114609

* 169. 5 * 1613 : 180201997 * 125903673079 7 * 40894687672970399229384165 7

171. 13 * 37 * 131101 * 160969 * 525313 : 25309 * 5675149 * 39291697
- * 99463730244517

* 173. 7152893721041 * 16738150851865747003221742320699421816 81

175. 5^3 * 29 * 268501 * 47392381 : 10382137934478419409082933558714 61401

177. 5 * 1181 * 3541 * 157649 * 174877 : 31153 * 5397793 * 94789873
- * 208478583167506 57

179. 1301260549 * 588850381287433028279084110474400181861465037

181. (3064991081731777716716694056776498445808238794165452801)

* 183. 5 * 733 * 1709 * 368140581013 : 12836737570021 * 4141949587337965308991 81

$2^{n}+2^{(n+1)/2}+1$

185. 5^2 * 149 * 184481113 : 29246281 * 567471221
- * 429988183417207835068617400 1

* 187. 137 * 953 * 2113 : 5237 * 551353793 * 1819762572673
- * 1353220459171186012 73437

189. 13 * 37 * 113 * 1429 * 279073 * 118750098349
- : 304832756195865229284807891468769

* 191. 5 : 3821 * 89618875387061 * 183308515384266544265228323416514343359 7

* 193. 5 : 3089 * 148997 * 144020306447044058 77 * 3787913000270896356776522859 73

195. 13^2 * 41 * 53 * 61 * 157 * 313 * 1249 * 108140989558681 : 468781
- * 720453772427518446437641

197. 52009 * 3862163385805798697201354795194661512726441364448411929

199. 5 : (160693804425899027554196209234369790372265945258578624171213)

201. 5 * 269 * 42875177 * 2559066073 : 10453 * 132661
- * 157049009596512937742705213957 53

* 203. 113 * 536903681 : 9810958633253 * 215974685494939586649025043316706457 57

* 205. 41^2 * 181549 * 12112549 : 821 * 269896441 * 82777720757144341
- * 75839980140761136 1

207. 5 * 109 * 1013 * 1657 * 70334392823809 : 3313 * 18217 * 318781 * 6542857
* 25395382141805460457

* 209. 5 * 229 * 397 * 457 : 6689 * 2039731321 * 149832750683283097
- * 193738524141656406560309 3

211. (32910091146424120843099383651147821396038863379488555157023621 13)

213. 13 * 4999465853 * 472287102421 : 853 * 189997
- * 26461853284868541296931699111393 49

215. 5^2 * 1759217765581 : 370661 * 1952201 * 4538991421 * 260125854015641
- * 14013452701711 01

* 217. 5 * 29 * 8681 * 49477 : 31249 * 7767296685070052037029 93
- * 13933554603291368158475899 7

* 219. 13 * 9444732965601851473921 : 371335727233
- * 18478609113710122023550126425157

* 221. 53 * 137 * 157 * 953 : 1210509821 * 2291059412513
- * 11184984408988805620629591771946 63477

223. 5 : 11597 * 6530333
- * (3559902010861722174506435824307200761380056925224554514 1)

225. 5^3 * 109 * 181 * 1321 * 54001 * 63901 * 268501 * 13334701 : 695701
- * 307116398490301 * 6269989892198401

227. 5449 * 83132849 * 694512857 * 5661492593
- * 12109000865024524054532128491937658291 3

* 229. 602633653 * 33074236421 * 441855207898941550335 73
- * 97959333591579135491397766 9

231. 5 * 29 * 397 * 14449 * 4327489 * 869467061 * 3019242689
- : 365212445341097287826412838353955921

233. 5 : 3108221
- * 88819248654333958717025023153463354575210175965320723483310427 3

```
* 235. 41 * 140737471578113 : 87255998201 * 3237811125343321
     - * 3386948380275557006547764404 1

* 237. 13 * 60446290980621507572531 3 : 18890331057055511701
     - * 14878405589115192810390787 69

* 239. 5 : 77852679293
     - * 22694749632556930857114329483875821148175572635464579475012 01

* 241. 5 : 2640397 * 15594629 * 76119208744309
     - * 22548642839647422711240905438079181931856287 3

* 243. 13 * 37 * 279073 * 3618757 * 4977454861 : 2917 * 4861 * 26129603777437
     - * 15778453094691989880197773477

  245. 41 * 113 * 7416361 * 4981857697937 : 7439220181
     - * 44399394252774652151567131602624448846381

  247. 5 * 229 * 457 * 1613 : 104729 * 2638949
     - * ( 96951586673795060921320591010774110105930479418097556 1 )

* 249. 5 * 13063537 * 148067197374074653 : 1993 * 804851665141843353 73
     - * 583117579691967491546961181

  251. 5021 * ( 72067372807530991973443403336416991 0-
                                                  475952521914260554092589753456528053 )

* 253. 277 * 2113 * 30269 : 25301 * 109297 * 756550961 * 2569737193 * 9623862953
     - * 156296877661 * 1010273603076596 33

  255. 5^2 * 409 * 1021 * 1321 * 3061 * 4421 * 13669 * 26317 * 550801 * 23650061
     - : 15571321 * 42515530888344717190444817256 01

  257. 5 : 28564009 * 360197837
     - * 450172145601416513714489770722304316747285148965228502932072 9

  259. 113 * 593 * 231769777 : 6217
     - * [ 95939636762858215798954006118918120543747719436645753636592 73 ]

  261. 13 * 37 * 536903681 * 22170214192500421 : 7309
     - * 88544086062101280800732676713543809008487793569

* 263. 5 : 119929 * 731141 * 99972364781
     - * 33815322934709348729340206164586405164149466120265140526 9

* 265. 5^2 * 18014398241046 53 : 51941 * 24082141 * 31213331016701
     - * 33716583668208510447368101472499412321

  267. 13 * 1069 * 57901779199499995610614 9 : 2137 * 928574737
     - * 14851642607221752942766012585821135190909

  269. 8609 * ( 11018338889907007467881211629587307946 7-
                                                  30529335856584745435704961581782138940 9 )

  271. 5 : 97561 * 77782621746976293634537859119211270170-
                                                  17123583828869656300351035087381155797

  273. 5 * 29 * 1093^2 * 1613 * 3121 * 14449 * 21841 * 8861085190774909
     - : 1948129 * 319475398781398849939742864389565 9569

* 275. 41 * 101 * 2113 * 8101 * 415878438361
     : ( 20593921044475850123723906047526192805451892283530357383578 01 )

  277. 232681 * 98002601 * 1093620377
     - * ( 97374150430885676446908559928590590464796201034099789397745 53 )

* 279. 5 * 109 * 8681 * 49477 * 461154528308645068 9 : 775844757937
     - * 11597860091842789406056581538727084419553 17
```

281. 5 : 3373 * 3827221 * (601947888102537035190929595540237358926123516438440188762697385235262737 57)

283. 155413511378058325673556952545881512531392602876034158026702846618408024437320444805 13

* 285. 13 * 41 * 61 * 761 * 131101 * 160969 * 525313 * 2416923620660807201
- : 1457772869697961 * 643261967877279035519771508 61

* 287. 5 * 29 * 10169 * 43249589 : 10333 * 17160693383233
* (219896977606524314758590198869677872743778299194748860 09)

289. 5 * 26317 : 936361 * (807270431064154764644491240324941672525937851280918921932897738745158062709 7)

* 291. 13 * 389 * 4657 * 4959325597 * 17637260034881
- : (193141591858052401987107321657551447171623396995686179 1941)

293. 5861 * 12893 * 60488093 * (348171431203738171372864500024395275354396054489757627550627879083351878 9)

295. 5^2 * 1181 * 3541 * 157649 * 174877 : (220855883508674180911337583348079324042745872250255696779298498158788 61)

* 297. 5 * 109 * 397 * 42373 * 246241 * 4327489 * 15975607282273 : 2377 * 22573
* 155399494141 * 4712151755917 * 4152325999427578629795 7

* 299. 53 * 157 * 277 * 30269 : 20333 * 956801 * 15595841 * 19294368341
- * 6339840806910833 * 3933458213662739074597183318390454 09