FBA

Abstract

One of the most difficult challenges in number theory and cryptography is the problem of factoring large integers since factoring large numbers more than 200 digits remain difficult. This difficulty has been useful in proving the strength of the RSA encryption scheme, which uses two large numbers of similar size. In this work, we introduce factorisation by bases algorithms (FBA) and implement it on the RSA-numbers defined by the RSA challenge. We analyse the time spent on factoring to check the speed and efficiency of the algorithm.

Introduction

Integer factorization is the task of computing the divisors of natural numbers. It is a problem with a long and fascinating history, and it is certainly among the most influential in algorithmic number theory. While there is a variety of algorithms significantly faster than the brute-force search for divisors, it is still an open problem to construct a technique that efficiently factors general numbers with hundreds to thousands of digits. The hardness of this problem is fundamental for the security of widely used cryptographical schemes, most prominently the RSA cryptosystem. Nevertheless, there is no proof for its hardness besides the fact that decades of efforts have failed to construct a more efficient technique. Quite regularly, there are set new records1 concerning the factorization of numbers of certain size, mostly due to improved implementations of the best available algorithms and advances in the hardware and computing power. In addition, the bound for the deterministic integer factorization problem has been improved multiple times in recent years ([11], [12], [10], [14]). On the other hand, there has only been little progress in the development of new techniques for practical integer factorization since the invention of the Number Field Sieve ([19]) in the 1990s. One of the earlier algorithms with sub-exponential runtime was by Dixon ([7]) in 1981.

Background

Let N be the number we want to factorize. We will always assume that N is odd, composite and not a perfect power of another number. We will also assume that N is made up of 2 prime factors, p and q. We will explain properties of factorisation by bases techniques using one number in base 10.

Lemma: N can be converted into a polynomial given a base.

Example: 667 in base 10 is

Now 667 is built by two prime factors which are 23 and 29. If both of them are converted into base 10 they become, and respectively.

which is different from the first form of N gotten. (A1)

From this derivation we notice that cannot be factorised to give us p and q because the discriminant was imaginary. Furthermore, we also notice that for any converted form of N we get we cannot factorise if also the discriminant is imaginary. From (A1) we noticed that a change of the form happened with h=2 and k=2 (A2) which results in, . This becomes the obtained equation.

If we say

We obtain the discriminant: which reduces to

(A3)

To solve such a problem is quite complex. We want to reduce the equation to 2 variables which can be easily solved either as Diophantine equations or through some ingenious method. There are many ways to do this such as:

1. Insert a value for 1 variable, for example, if m=12,

of which this is a conic function. (A4)

1. Insert a value for 10k+h, for example, if 10k+h=22, and m squared is M

of which we solve it by Diophantine solutions then try to relate back. (A5)

1. Eliminate squared variables, for example, if h=m,

which is still some conic section. (A6). Another example is we get.

which is a simpler equation to work with (A7).

1. Reference k and h to m, by defining them as and (A8)

CASE I (A4)

Given Here if we insert a value for m for example, 12 we get: which is a conic section. We will refer to this paper written by on solving conic sections.

Note: Since this one is a conic section and to find the values of h,k we will need to factorise N using SIQS or ECM, hence this one will not have an algorithm.

CASE II (A5)

Given Let if we solve it, we get We will now only be left with finding m of which by Diophantine solutions, we know that m is of a specific parametric solution.

Let

Note: This one will have an algorithm. Name it ALGORITHM 1.

CASE III (A6)

Given If we say that

we get . The solutions are put in the table below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| h | -8 | 4 | 137 | -224 | -15 | -7 |
| k | 157 | 5 | 12 | 13 | 24 | -204 |
| m | 1570.020 | 50.159 | 182.123 | 258.990 | 240.468 | 2040.012 |

As seen from the table above, no value of h and k could produce an integer value of m. If we are to link up the function to Pythagoras theorem we obtain this identity.

Note: Dishonoured this one. Does not have an algorithm.

CASE IV (A8)

Given We can relate h and k to m by using these formulas, and . If we expand the solution, we obtain,

The discriminant becomes: . The is 10672=667\*16. This means that to find integer solutions, must be found. Of which such an answer can be answered by Dixon’s method. Other than that method we can use the coefficients. 74704=667\*112 and 64032=667\*96. If we let be fractions of the form then we mean that , meaning that the two must be factors of 96, which results in the solutions.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | ±96 | ±1 | ±2 | ±48 | ±32 | ±3 | ±4 | ±24 | ±8 | ±12 | ±16 | ±6 |
|  | ±1 | ±96 | ±48 | ±2 | ±3 | ±32 | ±24 | ±4 | ±12 | ±8 | ±6 | ±16 |

If we use, as integers we have a total of combinations and the same number squared of combinations also applies if we use them as fractions, that is; .

If we are to go back to the original form with only variables, we notice that and . For the discriminant we get,

Making unknowns subjects of the knowns, for example, making subject of B, we get.

And for N=667 in base 10, we obtain.

Well, this means that we now have 2 equations of which we can use to find solutions. We now have four variables of which we need a third equation to reduce all the variables to one variable which can easily be solved with. From the other cases above, we noticed that Case II gave us a breakthrough by giving us values of k and h as variables of m. Meaning; is the answer we want. Therefore,

(T1)

(T2)

(T3)

If we solve for M=34 we get.

However, we know that finding the correct M which will produce the desired prime factors is challenging, therefore, we use the next method.

If we have,

(T1)

(T2)

And then substitute (T1) into (T2), we have,

(T4)

Which means, if we put a value for we find and conversely.

But even if we know the relationship between h and k and the value of o, it’s not enough for us to determine m. Let’s assume h and k are related to m by and .

Substituting in (T4) we obtain.

We then insert a value for m and o.

After this we assume that will be fractions, hence we will use like what we wanted to do above. Which gives us this solution:

In which we iterate until we get desirable prime solutions.

Examples:

Let m=12 and o=48

For there we no solutions

For

For

Rather than all this rubbish, since we know that the combination of m and o is very strict, why not iterate one over the other.

(T1)

(T2)

Then insert either m or o as fixed value, then iterate the one left as free.

Note: ALGORITHM 2

CASE V

In this case we introduce a rather unpopular method of factorising. Suppose we want to factorise N, we derive a secondary N, name it to N2, then we factorise it instead. The factorisation of N2 will lead to the factorisation of N using relationships which existed between the two numbers. This is the approach in this scenario.

Given we have,

(T1)

(T2)

We establish a relationship between h and k except that of the form and then insert a value for o and solve using (T2). This will give results of h and k basing on the square of m, ie, both h and k will consist of some solution in which we have to find where all the values are integers. We solve assuming that it won’t relate to N, hence factorising N will not happen if we are to solve it by Alpetron calculators.

Example.

(T2)

The solutions are:

The solutions are:

Which shows that they are not related to N.

Note: Make ALGORITHM 3

CASE VI

Let’s have then it show that for the discriminant we have

Here we can insert any value for b and m and get deterministic results.

For example, for N = 667, x = 10, we have:

If b=30 and m=12 we get: . The solution set for 6 values is shown in the table below.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| a | -26 | -10 | -2 | 2 | 4 | 5 |
| c | 8 | 9 | 11 | 15 | 23 | 39 |

And the solutions

If we substitute x with 10 for all the solutions, we will find none equating to 667 and its multiples. However, if we try to find solutions for x such that we get the prime solutions, for example.

For

Using x=27, for the solutions of x to find p and q, we get:

But finding solutions such that takes time especially when resolving large numbers, since current methods require us to factorise N first.

The solution to this problem is covered in the next step.

Here we put C to be C-N for f(x).

Using N=667, x=10, we get.

Let b=-24 and m=10, we get:

As for the solution sets, we have:

And if we take all the solutions of we have:

We had no f(10)=667 or its multiples.

Assuming S is a group and using the preliminary laws of algebra, a group is said to be associative, commutative and contains and identity element as well as an inverse. In our case, let the identity be the prime factor we want to find. Then we have whereby \* is addition.

Examples:

Therefore p=gcd(e, N) ALGORITHM 4