

Operation Prime Factors

Leneen Sorokhaibam¹, Maria Thomas²

Affiliation

1. Department of Mathematics, St. Joseph's College (Autonomous), Bengaluru, Karnataka 560027.
2. Department of Statistics, Christ University, Bengaluru, Karnataka 560029.

Abstract

Sometimes factorization is easy. In this article we will be seeing a simple algorithm. It involves solving some simple equations of one variable. We will do this to reduce the size of the given number X. Everytime when X is divided by a prime number its size gets reduced. Secondly we look for a particular condition for $X = A.B + r = (A + a).(B - b)$; if b is an integer or not. We will be using simple arithmetic and put it in the simplest way.

Keywords: Prime Number, Integer Factorization, Fundamental Theorem Of Arithmetic.

Introduction

Here is a simple algorithm to find all the factors. We will be using prime numbers for that. This will not work only when the Fundamental theorem of arithmetic is wrong. For X is a composite number there is a prime number to factorize it. We do that by using the prime numbers less than X.

Theory:

Let $X = ax + b$; and x is a prime number. The divisor x takes 2, 3, 5 and so on; accordingly x gets decreased. If $b \neq 0$ for all cases $a \leq x$; then X is a prime number.

OPERATION_PRIME_FACTORS

```

Part 1.
{
i=0, c=0, y=0
  divide X by D[i] // D[i] contains prime numbers in
  increasing order

  if ( D[i] is a multiple of X )
  {
    c = c + 1
    X = q // q and y are quotient and remainder
    respectively
    print ( D[i] is a factor of X )
  }
  repeat Part 1 if D[i] or D[i+1] exactly divides X
}

```

```

Part 2.
{
  repeat 2.1, 2.1 2.3 if ( D[i] <= q )
  2.1. d = difference_( D[i], D[i+1] )
  2.2. q = quotient_( D[i], q, y, d )
  2.3. y = remainder_( D[i+1], R, y )
}

```

```

Part. 2.1. difference_( D[i], D[i+1] )
{
  d = D[i+1] - D[i]
  return d
}

```

```

Part. 2.2. quotient_( D[i], q, y, d )
  Let  $X = A.B + r = (A + a).(B - b)$ . If b is an integer then X
  is prime.
  If ( A + a ) does not exactly divide ( B.a - r ) then take R as
  the remainder.
  Let A, B and r be represented by D[i], q, y respectively.
  {
    b = (q*d - y)/( D[i+1] )
    if ( (q*d - y) is a multiple of D[i+1] )
    {
      c = c + 1
    }
  }
  print ( D[i+1] is a factor of X )
  q = q - b
  X = q
}
else: ( q = q - int b )
return q
}

```

```

Part. 2.3. remainder_( D[i+1], R, y )
  Let  $X = (A + a).(B - b) = K.(B - n.K - R)$ , where n.k is int
  b.
  Therefore remainder in K - R
  if ( R > 0 )
  {
    y = D[i+1] - R
  }

```

Received: 11.03.2021; Revised: 20.03.2021; Accepted: 01.04.2021

Corresponding Author

Ms. Maria Thomas
Research Scholar
Department of Statistics,
Christ University, Bengaluru, Karnataka.
Email: mdthomas215@gmail.com

Part 3.

```
{  
  if ( c == 0 )  
    print ( X is a prime number )  
  else  
    print ( X is a composite number )  
}
```

Conclusion

The algorithm ends only when all the factors are found or confirms that X is a prime number. In any of the steps mentioned above no big calculations are included. The numbers involved in Part.2.2 will be much smaller for large values of X. Since all prime numbers less than X indirectly or directly divide it, the conclusion can't be wrong.

Acknowledgement

The authors thank the Department of Mathematics, St. Joseph's College (Autonomous), Bengaluru and Christ University, Bengaluru for supporting this work.

Conflict of Interest

No known conflict of interest.

Funding Source

No funding was availed for this study.

References

- 1..Erik Lucero.Computing prime factors with a Josephson phase qubit quantum processor. Nature Physics (2012).
2. Gianluca Amato. Primitive abundant and weird numbers with many prime factors. Journal of Number Theory (2019).
3. Gregory Debruyne.Beurling numbers whose number of prime factors lies in a specified residue class. Journal of Number Theory (2020).
4. James Maynard.Dense Clusters of primes in subsets. Compositio Mathematica (2016).