Journal of Mathematics Research; Vol. 4, No. 3; 2012
ISSN 1916-9795 E-ISSN 1916-9809
Published by Canadian Center of Science and Education

Prime Sieve and Factorization Using Multiplication Table

Jongsoo Park (Corresponding author)
Mathology Sys
216 banjuk kongju Chungnam, 314-100, S. Korea
Tel: 82-10-6406-6552 E-mail: oofbird7@naver.com

Cheong Youn
Department of Computer Engineering, Chungnam National University
Taehakro 27 Goondong, Yoosunggu Taejeon, 305-764, S. Korea
Tel: 86-10-8888-7777 E-mail: cyoun@cnu.ac.kr

Received: February 2, 2012 Accepted: February 16, 2012 Online Published: May 28, 2012
doi:10.5539/jmr.v4n3p7 URL: http://dx.doi.org/10.5539/jmr.v4n3p7

Abstract

Using the properties of the table sieve, we can determine whether all given number, positive integer G, is a prime and whether it is possible to factor it out.

Keywords: Prime sieve, Integer factorization, Primality test

1. Introduction

The sieve of Eratosthenes was successful in filtering out composite numbers using the fact that it is easy to calculate multiples but it was not successful to find the relationship between filtered-out composite numbers. Our approach method has found a way to filter out all the primes using table multiplication. We could effectively find a factor of a given composite number.

2. Generating the Composite Number of the 12n+1, 5, 7, 11 Series

Every prime number except 2 and 3 is contained in the 12n+1, 5, 7, 11 series, is sorted into 4 kinds of remainder groups 1, 5, 7, and 11 and belongs to at least one of these 4 groups. Let us denote the set A_n is all elements of the 12n+1, 5, 7, 11 series (n=0, 1, 2); the set P_n is all elements of prime numbers as comprised in A_n; the set C_n is all elements of composite numbers as comprised in A_n.

2.1 Algorithmic Description

2.1.1 All Prime Numbers but 2 and 3 Exist in Forms of 12n+1, 5, 7, 11 with a Period of 12n

Proof.

(i) All natural numbers can be represented with a period of 12.

(ii) All even numbers but 2 are not prime numbers.

- Elements of 12n+2, 4, 6, 8,10,12 are all even.(n=0, 1, 2, ..., n)

- Therefore, all 12n+2, 4, 6, 8, 10, 12's but 2 are not prime numbers.

(iii) All 12n+3 but 3 are not prime numbers.

- 12n+3=(3·4)n+3 is a multiple of 3.

(iv) 12n+9 is not a prime number.

- 12n+9=(3·4)n+9 is a multiple of 3.

As a results, every prime number but 2 and 3 is contained in the periodic n A_n. So, let us denote this series as follows:

$$A_n = \begin{pmatrix} A_1, if remainder \equiv 1(mod 12) \\ A_5, if remainder \equiv 5(mod 12) \\ A_7, if remainder \equiv 7(mod 12) \\ A_{11}, if remainder \equiv 11(mod 12) \end{pmatrix}$$

In next equation, the A_n series are multiplied infinitely and we can find 10 basics equations which falls into one of the 4 groups.

2.1.2 All Elements of the $A_n \times A_n$ Table Multiplication are Contained in Set n A_n

Proof.

$$(12x + \alpha) \times (12y + \beta)$$

$$= 144xy + 12\beta x + 12\alpha y + \alpha\beta = \begin{pmatrix} \alpha\beta \in (1, 25, 49, 121), if remainder \equiv 1(mod 12) \\ \alpha\beta \in (5, 77), if remainder \equiv 5(mod 12) \\ \alpha\beta \in (7, 55), if remainder \equiv 7(mod 12) \\ \alpha\beta \in (11, 35), if remainder \equiv 11(mod 12) \end{pmatrix} \quad (1)$$

Therefore,

$$\alpha\beta \in (1, 5, 7, 11, 25, 35, 49, 55, 77, 121) \quad (2)$$

2.1.3 All Elements of the A_n Table Multiplication are Contained in the Set of then $A_n \times A_n$ Table Multiplication

Proof. For any element k of the set $A_n \in P_n$ or $k \in C_n$, If k is P_n

$$k \in (12x + \alpha) \times 1 \quad (3)$$

or

$$k \in 1 \times (12y + \beta) \quad (4)$$

otherwise

$$k \text{ is } C_n \ (P_n \times P_n, P_n \times C_n, C_n \times C_n\ )$$

Therefore, $C_n \geq 25$. Additionally, it is possible to find all values of n C_n of the 12n+1, 5, 7, 11 series in the results of a matrix-multiplication of $A_n \times A_n$ that are greater than 5.

<Table 1>

2.2 The Structure of a Matrix-multiplication of $A_n \times A_n$

Unlike prime numbers, which are unpredictable, the composite numbers are formed by sixteen arithmetic progression groups. This means that composite numbers in principle are predictable because whole composite numbers follow this rule. However, the composite numbers are made up of sixteen arithmetic progressions and it is difficult to see the whole of the arithmetic progressions, whose number increases, without necessary computations and information media that can store the computed results. If you can find the computed results of various arithmetic progressions intuitively, you can predict the rule that governs the composite numbers. This immediately means that you will be able to find the rule that governs the prime numbers. It is not a problem of whether or not the composite numbers are predictable but a problem of human perception.

See Table 1.

2.3 Symmetric Table and Asymmetric Table

Analyzing the table of the 12n+1, 5, 7, 11 series, by the values of horizontal axis α and vertical axis β, the table divides into a symmetric table if α=β, and into an asymmetric table if $\alpha \neq \beta$. Therefore, we can find the following results.

(i) Symmetric table, α=β

$$(12x + 1)(12y + 1), (x, y \geq 1) \quad (5)$$

$$(12x + 5)(12y + 5) \tag{6}$$

$$(12x + 7)(12y + 7) \tag{7}$$

$$(12x + 11)(12y + 11) \tag{8}$$

(ii) Asymmetric table, $\alpha \neq \beta$

$$(12x + 1)(12y + 5), (x, y \geq 1) \tag{9}$$

$$(12x + 1)(12y + 7), (x, y \geq 1) \tag{10}$$

$$(12x + 1)(12y + 11), (x, y \geq 1) \tag{11}$$

$$(12x + 7)(12y + 11) \tag{12}$$

$$(12x + 5)(12y + 7) \tag{13}$$

$$(12x + 5)(12y + 11) \tag{14}$$

However, the commutative law does not hold if $\alpha \neq \beta$. So, depending on the orders of α and β, the results are different for the diagonal elements. An asymmetric table has twelve cases.

3. Finding Factors from Composites in Arithmetic Progression

3.1 Substitution

We have seen that all the composite numbers but 2 and 3 can be represented in a form of (12x+α)(12y+β). Then, how can we determine if a given positive integer, G, is prime or composite?

Let G be an arbitrary positive integer.

(i) Check if G is a multiple of 2 or 3. If G is a multiple of one of these, it is a composite number.

(ii) If G is not a multiple of 2 or 3, G' s remainder R when divided by 12 is R $\in$ 1, 5, 7, 11 and R is the a number in the table multiplication elements, then G is a composite number. If R is not the same as any of the multiplication elements, then G is a prime number.

If a given number, G, is not a multiple of 2 or 3, we can express it as follows.

$$G = (12x + \alpha)(12y + \beta) = 144xy + 12\beta x + 12\alpha y + \alpha\beta \tag{15}$$

If we substitute $xy, \beta x + \alpha y$ with X and Y, respectively,

$$\beta x + \alpha y = Y, xy = X \tag{16}$$

The result is the following.

$$G = (12x + \alpha)(12y + \beta) = 144XY + 12Y + \alpha\beta = 12X + Y = C \; (C = \frac{G - \alpha\beta}{12}) \tag{17}$$

3.2 Determination of a Valid Domain

Let us apply the arithmetic mean and geometric mean to xy and $\beta x + \alpha y$. From $\beta x + \alpha y$=Y and $xy = X$,

$$y = \frac{-\beta x + Y}{\alpha} \tag{18}$$

When $x = 1$, X (xy) is the minimum. Therefore, the minimum of X (xy) is

$$X(xy) = \frac{-\beta + Y}{\alpha} \tag{19}$$

$$12X + Y = C \rightharpoonup 12X + \alpha X + \beta = C(substitution : Y = \alpha X + \beta) \tag{20}$$

$$\rightharpoonup (12 + \alpha)X = C - \beta$$

$$\rightharpoonup X = \frac{C - \beta}{12 + \alpha} \tag{21}$$

The maximum of X (xy) is

(i) If $x + y$ is even, then the maximum is achieved when $x = y$.

$$12X + Y = C \rightharpoonup 12x^2 + (\alpha + \beta)x - C = 0 \tag{22}$$

$$\rightharpoonup x = \frac{-(\alpha + \beta) \pm \sqrt{(\alpha + \beta)^2 + 4 \cdot 12C}}{24}$$

$$\rightharpoonup X(x = y) = [\frac{-(\alpha + \beta) \pm \sqrt{(\alpha + \beta)^2 + 4 \cdot 12C}}{24}]^2 \tag{23}$$

(ii) If $x + y$ is odd, then the maximum is achieved when $x + 1 = y$.

$$12X + Y = C \rightharpoonup 12x(x + 1) + \beta x + \alpha(x + 1) - C = 0 \tag{24}$$

$$\rightharpoonup 12x^2 + (\alpha + \beta + 12)x + \alpha - C = 0$$

$$\rightharpoonup x = \frac{-(\alpha + \beta + 12) \pm \sqrt{(\alpha + \beta + 12)^2 + 4 \cdot 12(C - \alpha)}}{24}$$

$$\rightharpoonup X(positive) = [\frac{-(\alpha + \beta + 12) \pm \sqrt{(\alpha + \beta + 12)^2 + 4 \cdot 12(C - \alpha)}}{24}]^2 \tag{25}$$

- If the maximum and minimum of $X(xy)$ is not an integer, then we can make it an integer by rounding it up.

If we can determine the valid domain, we can make the following table list of (X, Y).

See Table 2.

In $12X + Y = C$, X increases by 1 and Y decreases by 12. So, X and Y have properties of an arithmetic progression. Let two arithmetic progressions, X and Y, be $X = n + a$ and $Y = -12n + b$, respectively.

(X, Y) Tables pairs Is there an efficient method to find a valid set of (X, Y), which has an integer root, from (a_1, b_2), (a_2, b_2), (a_3, b_3), (a_4, b_4), (a_5, b_5), (a_6, b_6),..., (a_n, b_n).

3.3 Finding Factors: First Method

x, n, r is positive integer (x, r contatins zero), Since

$$X = \frac{-\beta x^2 + Yx}{\alpha} \tag{26}$$

$$\rightharpoonup n + a = \frac{-\beta x^2 + (-12n + b)x}{\alpha}, (substitution : X = n + a, Y = -12n + b)$$

$$\rightharpoonup \beta x^2 - (b - 12n)x + \alpha(n + a) = 0$$

$$\rightharpoonup x = \frac{(b - 12n) \pm \sqrt{(b - 12n)^2 - 4\alpha\beta(n + a)}}{2\beta} \tag{27}$$

Since x is zero or a positive integer, we can find integer roots (n, r) from

$$r^2 = (b - 12n)^2 - 4\alpha\beta(n + a) \tag{28}$$

$$\rightharpoonup 36r^2 = 36(12n - b)^2 - 4\alpha\beta(n + a)$$

$$\rightharpoonup 36r^2 = 36(144n^2 - 24bn + b^2 - 4\alpha\beta n - 4\alpha\beta a)$$

$$\rightharpoonup 36r^2 = 36(144n^2 - 24bn - 4\alpha\beta n + b^2 - 4\alpha\beta a)$$

$$\rightharpoonup 36r^2 = (72n - (6b + \alpha\beta))^2 - (6b + \alpha\beta)^2 + 36b^2 - 4 \cdot 36\alpha\beta a$$

$$\rightharpoonup (72n - (6b + \alpha\beta))^2 - 36r^2 = (6b + \alpha\beta)^2 - 36b^2 + 4 \cdot 36\alpha\beta a$$

$$\rightharpoonup (72n - (6b + \alpha\beta) + 6r) \cdot (72n - (6b + \alpha\beta) - 6r) = 12(12a + b) \cdot \alpha\beta + (\alpha\beta)^2 \tag{29}$$

If an integer root, (n, r), exists, then we can find integer (x, y).

3.4 Finding Factors: Second Method

In order to find (x, n) pairs that have integer roots, let us do the substitutions $\beta x + \alpha y = Y$, $xy = X$.

$$x, y = \frac{Y - \beta x}{\alpha} \tag{30}$$

$$\rightharpoonup X = \frac{-\beta x^2 + Yx}{\alpha}$$

$$\rightharpoonup n + a = \frac{-\beta x^2 + (-12n + b)x}{\alpha}, (substitution : X = n + a, Y = -12n + b)$$

$$\rightharpoonup (12x + \alpha)n = -\beta x^2 + bx - \alpha a$$

$$\rightharpoonup n = \frac{-\beta x^2 + bx - \alpha a}{12x + \alpha} \tag{31}$$

In order to find an integer root pair, (x, n), many iteration is required. But, this method is inefficient because all (X, Y) tables need to be iterated. However, from the graph of the function, we can discover the following properties. When the value of x is small, n increases faster. However, for a certain domain, the rate at which n increases is greatly reduced as x increases, and when n approaches its limit, n does not either increase or decrease as x increases. Therefore, we can confirm that the values of n congregate at certain domains. So, we have come up with the following idea to find integer root pair (x, n).

If we do the iteration in the domain 0~ k_x, on the x-axis (up to the point where n_{k+1}-n_k is greater than 1) and in the range n_k ~n_{k+1}, on the n-axis at the points where n_{k+1}-n_k, becomes less than 1, then we have the same effect as that of inspecting all the whole numbers.

4. Conclusion

Using the table, we have shown it possible to significantly reduce perceptive complexity. But, the uncertainty of the table directly reflects the irregularity of prime numbers (whether a given number is a prime number or a composite number and what the next prime number is). We can see that, since the complexity of a table as a given number, G, becomes larger and larger, it becomes harder to predict the next prime number. Then, is there a method to innovativly reduce the complexity of the table? It is hard to know at this time.

Acknowledgment

I am very grateful to Lim, sang-tae for their advice and for the patience they showed, assisting me. If you want a more understanding, you could refer to the original. (http://vixra.org/pdf/1003.0179v4.pdf)

References

Atkin, A. O. L., & Bernstein, D. J. (2004). Prime sieves using binary quadratic forms. *Math. Comp., 73*, 1023-1030. http://dx.doi.org/10.1090/S0025-5718-03-01501-1

Crandall, R., & Pomerance, C. (2005). *Prime Number* (A Computational Perspective), 2nd ed. Springer, pp. 121-156.

David Bressoud. (2008). *A Course in Computational Number Theory* (Key Curriculum Press). Wiley, pp. 97-143.

Davenport, H. (2008). *The Higher Arithmetic: An Introduction to the Theory of Numbers*, 8th ed. Cambridge University Press, pp. 1-9.

David M. Burton. (2005). *Elementary Number Theory*, 6th ed. McGraw Hill India, pp. 39-50.

Gareth A. Jones. (1998). *Elementary Number Theory*, Corrected edition. Springer, pp. 19-35.

Hans Riesel. (1994). *Prime Numbers and Computer Methods for Factorization* (Progress in Mathematics), 2nd ed. Birkhauser Boston, pp. 6-9.

Hardy, G. H. (2008). *An Introduction to the Theory of Numbers*, 6th ed. USA: Oxford University Press, pp. 17-21.

Ingham, A. E.. (1990). *The distribution of prime numbers*. Cambridge University Press, pp. 9-40, 86-107.

John Derbyshire. (2004). *Prime Obsession*. Plume, pp. 32-47.

Jong-Soo Park. (2010). Prime Sieve Using Multiplication Operation Table. [Online] Available: http://vixra.org/pdf/1003.0179v4.pdf

Kra, B. The Green-Tao Theorem on arithmetic progressions in the primes: an ergodic point of view, preprint.

Marcus Du Sautoy. (2004). *The Music of the Primes*. Harper Perennial, pp. 3-5.

Phillip J. Davis. (1999). *The Mathematical Experience*. Mariner Books, pp. 209-214.

Richard K. Guy. (2004). *Unsolved Problems in Number Theory*, 3rd ed. Problem Books in Mathematics, Springer, pp. 3-5.

Rose, H. E. (1995). *A Course in Number Theory*, 2nd ed. USA: Oxford University Press, pp. 237-245.

Tao, T. What is good mathematics? arXiv:math/0702396

Tom M. Apostol. (1976). *Introduction to Analytic Number Theory* (Undergraduate Texts in Mathematics), 1st ed. Springer, pp. 14-16, 146-155.

Table 1. The result list of multiplication table

Multiplication	Sign	Equation	Remainder
A_1xA_1	++	(12x+1)(12y+1)	1 (mod 12)
A_5xA_5	++	(12x+5)(12y+5)	1 (mod 12)
A_7xA_7	++	(12x+7)(12y+7)	1 (mod 12)
A_{11}xA_{11}	++	(12x+11)(12y+11)	1 (mod 12)
A_1xA_5	-+	(12x+1)(12y+5)	5 (mod 12)
A_7xA_{11}	-+	(12x+7)(12y+11)	5 (mod 12)
A_1xA_7	–	(12x+1)(12y+7)	7 (mod 12)
A_5xA_{11}	–	(12x+5)(12y+11)	7 (mod 12)
A_1xA_{11}	+-	(12x+1)(12y+11)	11 (mod 12)
A_5xA_7	+-	(12x+5)(12y+7)	11 (mod 12)

Table 2. Finding integer values of x and y

X	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	$a_1$0	...	a_n
Y	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9	$b_1$0	...	b_n