Hindu methods for finding factors or divisors of a number *

1 Introduction

Factoring or finding divisors of a number does not appear as a subject of treatment in any early work on Hindu arithmetic. There are, however, reasons to believe that the ordinary method of factoring a number by successive division by 2, 3, 5, etc. was well known but being much too elementary was not considered suitable for inclusion in an arithmetical work. Even in Mahāvīrācārya's (850 AD) voluminous *Gaṇitasārasaṅgraha* where we have explicit references to factorisation no rule has been stated for the purpose. Śrīpati (1039 AD) is probably the first Hindu writer who has formally dealt with the subject of factoring a number in his *Siddhāntaśekhara*. Besides stating the ordinary method based on successive division, he gives an additional method for factoring a non-square number by expressing it as a difference of two squares. This latter method was subsequently stated in its complete form by another notable Hindu mathematician Nārāyaṇa (1356 AD) who, in his *Gaṇitakaumudī*, devoted a full chapter to the subject of factoring and finding all possible divisors of a number. It is interesting to note that the method of factoring a non-square number in its complete form in which it was stated by Nārāyaṇa, was rediscovered in Europe about two centuries later by the French mathematician Fermat. The object of the present paper is to throw light on the methods given by Śrīpati and Nārāyaṇa and to invite attention of historians of mathematics to them.

2 Srīpati's rule

Śrīpati[1] states his rules for factoring a number as follows:

द्वाभ्यां द्वाभ्यां भाज्यराशिं समे तत् आदिस्थाने पञ्चके पञ्चकेन ।
एवं कुर्याद्यावदोजं तु तावत् त्र्याद्यैर्हारैर्भाज्यराशिं भजेत्तु ॥

* K. S. Shukla, *Gaṇita*, Vol. 17, No. 2 (1966), pp. 109–117.

[1] Śrīpati, *Siddhāntaśekhara*, Part II, edited by Babuaji Misra, Calcutta (1947), ch. xiv, vv. 36–37.

A. Kolachana et al. (eds.), *Studies in Indian Mathematics and Astronomy*,
Sources and Studies in the History of Mathematics and Physical Sciences,
https://doi.org/10.1007/978-981-13-7326-8_13

वर्गश्चेत्तन्मूलमेवास्य हारं नो चेदासन्नं पदं द्विघ्नमस्मिन् ।
रुपं युक्त्वा शेषहीने कृतिः स्यात् तन्मूलं तद्युक्तमूलं युतोने ॥

(Rule 1). So long as the dividend (i.e. the number to be factored) is even, it is to be divided out by 2 again and again; whenever 5 happens to occur in the unit's place, it should be divided by 5; this should be done until the dividend is reduced to an odd number (with unit's digit different from 5), and then (the prime numbers) 3 etc. should be tried as divisors.

(Rule 2). If the dividend is a perfect square, its square root itself is a divisor; if not, its nearest square root should be multiplied by 2, then increased by 1, and then diminished by the residue of the square root; if the resulting number is a perfect square, find the square root of this perfect square and also the square root of the dividend as increased by this perfect square, and take their sum and difference. (Thus are obtained the two factors of the dividend).

Rule 1 gives the ordinary method of factoring a number. Rule 2 may be symbolically expressed as follows:

Let N be a non-square number, equal to $a^2 + r$ say. Then if

$$2a + 1 - r = b^2,$$

we have

$$N + b^2 = a^2 + r + (2a + 1 - r) = (a + 1)^2,$$

so that

$$\begin{aligned} N &= (a + 1)^2 - b^2 \\ &= (a + b + 1)(a - b + 1). \end{aligned}$$

3 Nārāyaṇa's rules

Nārāyaṇa[2] states his rules as follows:

असकृद् विभजेद् द्वाभ्यां समराशिं यावदेति वैषम्यम् ।
सत्सु प्रथमस्थाने पञ्चसु भाज्ये च पञ्चभिश्छिन्द्यात् ॥
न समो भाज्यः प्रथमः तस्मिन् यदि पञ्चकं स्थाने ।
अच्छेद्याः कल्प्यन्ते त्रिसप्तकैकादशादयश्छेदाः ॥
यावच्छेदप्राप्तिस्तावद् हरसाधनं क्रियते ।
भाज्यो वर्गश्चेत् तन्मूलं छेदो द्विधा भवति ॥

[2] Nārāyaṇa, *Gaṇitakaumudī*, Part II, edited by Padmakara Dvivedi, Benaras (1942), ch. xi, rules 2–9(i).

अपदप्रदस्तु भाज्यः कयेष्टकृत्या युतात् पदं भाज्यात् ।
पदयोः संयुतिवियुती हारौ परिकल्पितौ भाज्यौ ॥
राश्योस्तु तयोः प्राग्वत् कुर्वीतच्छेदशोधनं सुधिया ।
अपदप्रदस्य राशेः पदमासन्नं द्विसङ्गुणं सैकम् ॥
मूलावशेषहीनं वर्गश्चेत् क्षेपकश्च कृतिसिद्ध्यै ।
वर्गो न भवेत् पूर्वासन्नपदं द्विगुणितं त्रिसंयुक्तम् ॥
आद्याद् द्युत्तरवृद्ध्या तावद् यावद् भवेद् वर्गः ।
असमानानां पूर्वहताः परे पुरःस्थास्तथा चान्ये ॥
तुल्यानां पूर्वघ्नः परः पृथक् तेऽन्यहरनिघ्नाः ।

(Rule 1). If the number is even, divide it by 2 again and again until it becomes odd; if there is 5 in the unit's place, divide by 5. If the number to be divided is neither even, nor there is 5 in the unit's place, the prime numbers 3, 7, 11, etc. should by tried as divisors. One should find out the divisors until it is possible to do so.

(Rule 2). In case the number to be divided is a perfect square, its square root is a twice repeated factor. If the number to be divided is a non-square number, find an optional square number which added to the dividend gives a perfect square. The sum and the difference of their square-roots are the divisors of that (non-square) number, which are to be treated as dividends. The intelligent should now proceed, as before, to find out the divisors of those numbers.

(The method of finding the optional square number contemplated above is as follows): Find out the nearest square root of the non-square number, multiply that by 2, and then subtract therefrom the residue of the square root: in case it is a perfect square, it is to be taken as the number to be added to the dividend to make it a perfect square. In case the above number is not a perfect square, it should be further increased by the successive terms of the arithmetic series whose first term is twice the nearest square root (of the non-square number) plus 3, and common difference 2, until it becomes a perfect square.

(Rule 3). In the case of unequal divisors (thus obtained) (proceed as follows): (Having set down the divisors one after another) multiply the succeeding divisors by the preceding ones and by the product of the preceding ones taken two, three, ..., all at a time, and set down the products (thus obtained) ahead of those divisors.

In the case of equal divisors (proceed as follows): (Having set down the divisors one after another) multiply each of the succeeding

> divisors by (the product of) the preceding ones.
>
> Each of these should be severally multiplied by the other numbers (i.e. by those due to unequal divisors).
>
> (Thus are obtained all the divisors of the given number).

Rule 2 above may be symbolically expressed as follows:
Let N be a non-square number, equal to $a^2 + r$ say. If

$$2a + 1 - r = b^2,$$

then

$$N + b^2 = a^2 + r + (2a + 1 - r) = (a + 1)^2,$$

so that

$$\begin{aligned} N &= (a + 1)^2 - b^2 \\ &= (a + b + 1)(a - b + 1). \end{aligned}$$

If, however,

$$2a + 1 - r = c$$

where c is not a perfect square, then we add to c as many terms of the series

$$(2a + 3) + (2a + 5) + (2a + 7) + \dots$$

as are necessary to make the resulting sum a perfect square. Let r terms of the series be added and we have

$$c + [(2a + 3) + (2a + 5) + \cdots + (2a + 2r + 1)] = k^2.$$

Then

$$N + k^2 = (a + r + 1)^2,$$

so that

$$N = (a + r + 1)^2 - k^2 = (a + r + k + 1)(a + r - k + 1).$$

Rule 3 gives the method for writing down all possible divisors of the given number N. Let

$$N = a \times a \times a \times b \times c \times d.$$

Then all the divisors of N are:

(1) b, c, d, bc, bd, cd, bcd,

(2) a, a^2, a^3,

(3) ba, ba^2, ba^3; ca, ca^2, ca^3; da, da^2, da^3;
bca, bca^2, bca^3; bda, bda^2, bda^3; cda, cda^2, cda^3;
$bcda$, $bcda^2$, $bcda^3$;

3.1 Examples

Nārāyaṇa[3] illustrates the above rules by the following examples:

Ex. 1. Mathematician, quickly tell me the numbers by which the number 2048 is exactly divisible; also those numbers by which the number 3125 is exactly divisible.

We have

$$2048 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2,$$

so that all possible divisors of 2048 are 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 and 2048.

Also

$$3125 = 5 \times 5 \times 5 \times 5 \times 5,$$

so that all possible divisors of 3125 are 5, 25, 125, 625, 3125.

Ex. 2. Tell me if you know the numbers by which 7520 is exactly divisible; also the numbers by which 10201 is exactly divisible.

We have

$$7520 = 2 \times 2 \times 2 \times 2 \times 2 \times 5 \times 47.$$

Therefore all possible divisors of 7520 are

(1) 5, 47, 235

(2) 2, 4, 8, 16, 32

(3) 10, 20, 40, 80, 160; 94, 188, 376, 752, 1504; 470, 940, 1880, 3760, 7520.

Also

$$10201 = 101 \times 101.$$

Therefore the divisors of 10201 are 101 and 10201 only.

Ex. 3. O you, proficient in mathematics, tell me, if you know the subject of finding divisors, the numbers by which the number 1161 is exactly divisible.

We have

$$1161 = 34^2 + 5$$

and

$$2 \times 34 + 1 - 5 = 8^2,$$

[3] *Ibid*, ch. xi, Exs. 1 to 6.

therefore
$$1161 + 8^2 = 35^2,$$
so that
$$1161 = 35^2 - 8^2 = 43 \times 27 = 3 \times 3 \times 3 \times 43.$$
Therefore, all possible divisors of 1161 are 3, 9, 27, 43, 129, 387, 1161.

Ex. 4. If you are fully proficient in the subject of finding divisors, quickly tell me the numbers by which 1001 is exactly divisible.

Because
$$1001 = 31^2 + 40,$$
and
$$2 \times 31 + 1 = 63,$$
and
$$63 - 40 + 65 + 67 + \ldots + 89 = 32^2,$$
therefore
$$1001 + 32^2 = 45^2.$$
Therefore,
$$1001 = 45^2 - 32^2 = 77 \times 13 = 7 \times 11 \times 13.$$
Therefore, all possible divisors of 1001 are 7, 11, 13, 77, 91, 143, 1001.

Ex. 5. Friend, if you are fully proficient in mathematics, quickly tell me, the numbers by which 4620 is exactly divisible.

Proceeding as before, we have
$$4620 = 2 \times 2 \times 3 \times 5 \times 7 \times 11.$$
Therefore, all the divisors of 4620 are

(1) 3, 5, 7, 11, 15, 21, 33, 35, 55, 77, 105, 165, 231, 385, 1155

(2) 2, 4

(3) 6, 10, 14, 22, 30, 42, 66, 70, 110, 154, 210, 330, 462, 770, 2310, 12, 20, 28, 44, 60, 84, 132, 140, 220, 308, 420, 660, 924, 1540, 4620.

Ex. 6. Friend, if you are versed in mathematics, quickly tell me the numbers by which 3927 is exactly divisible.

Proceeding as before, we have $3972 = 3 \times 7 \times 11 \times 17$, so that all possible divisors of 3927 are 3, 7, 11, 17, 21, 33, 51, 77, 119, 187, 231, 357, 561, 1309, 3927.

4 Nārāyaṇa's rule rediscovered by Fermat

Rule 2 of Nārāyaṇa was rediscovered by the French mathematician Fermat about 1643 AD. In a letter written about that time, Fermat explains his method as follows:[4]

> An odd number not a square can be expressed as the difference of two squares in as many ways as it is the product of two factors, and if the squares are relatively prime the factors are. But if the squares have a common divisor d, the given number is divisible by $\sqrt{d}$. Given a number n, for examples 2027651281, to find if it be prime or composite and the factors in the latter case. Extract the square root of n. I get $r = 45029$, with the remainder 40440. Subtracting the latter from $2r + 1$, I get 49619, which is not a square in view of the ending 19. Hence I add $90061 = 2 + 2r + 1$ to it. Since the sum 139680 is not a square, as seen by the final digits, I again add to it the same number increased by 2, i.e., 90063, and I continue until the sum becomes a square. This does not happen until we reach 1040400, the square of 1020. For by an inspection of the sums mentioned it is easy to see that the final one is the only square (by their endings except for 499944). To find the factors of n, I subtract the first number added, 90061, from the last, 90081. To half the difference add 2. There results 12. The sum of 12 and the root r is 45041. Adding and subtracting the root 1020 of the final sum 1040400, we get 46061 and 44021, which are the two numbers nearest to r whose product is n. They are the only factors since they are primes. Instead of 11 additions, the ordinary method of factoring would require the division by all the numbers from 7 to 44021.

It may be added that at the time of writing his letter to Mersenne, December 26, 1638, Fermat had no such method.[5] This shows that the method was well known in India long before Fermat rediscovered it. Although Nārāyaṇa was the first to state the method in its complete form, the credit of the first inception of the method is indeed due to Śrīpati.

[4] *Cf.* Dickson, L.E., "History of the Theory of Numbers," Vol. I, p. 357.
[5] *Ibid*, p. 357, footnote.

5 Nārāyaṇa's alternative rule

Nārāyaṇa[6] gives the following as an alternative method for finding the divisors of a number:

> इष्टोनासन्नपदं हारः स्यादिष्टवर्गशेषयुतिः ॥
> हारहृता चेच्छुध्यति तेनावश्यं हृतो भाज्यः ।
> न विशुध्यति चेदिष्टं स्वधिया परिकल्पयेदन्यत् ॥
>
> The nearest square root (of the given number) as diminished by an optional number is the "divisor". If the optional number squared plus the residue of the square root is exactly divisible by the 'divisor' the given number shall be exactly divisible by the same. If not, one should apply one's intellect to choose another (appropriate) optional number.

Let $N = a^2 + r$. Then choosing λ as an optional number, we can write

$$\begin{aligned} N &= a^2 - \lambda^2 + \lambda^2 + r \\ &= (a+\lambda)(a-\lambda) + \lambda^2 + r \\ \therefore \frac{N}{a-\lambda} &= a + \lambda + \frac{\lambda^2 + r}{a-\lambda}. \end{aligned}$$

Therefore, if $\lambda^2 + r$ is exactly divisible by $a - \lambda$, then N is also exactly divisible by $a - \lambda$. Hence the rule.

Ex. 7. Quickly tell me, proficient in mathematics, the numbers by which 120 is exactly divisible, and also those by which 231 is exactly divisible.[7]

Here $120 = 10^2 + 20$. Choosing $\lambda = 2$, we see that $a - \lambda = 8$ is an exact divisor of 120. Thus

$$120 = 8 \times 15$$

so that

$$120 = 2 \times 2 \times 2 \times 3 \times 5.$$

All possible divisors of 120 are therefore

(1) 3, 5, 15

(2) 2, 4, 8

(3) 6, 12, 24; 10, 20, 40; 30, 60, 120.

---

[6] Nārāyaṇa, *Gaṇitakaumudī*, Part II, edited by Padmakara Dvivedi, Benaras (1942), ch. xi, rule 9(ii)–10.

[7] *Ibid*, ch. xi, Ex. 7.

Again $231 = 15^2 + 6$. Choosing $\lambda = 4$, we see that $a - \lambda = 11$ is an exact divisor of 231. Thus

$$231 = 11 \times 21$$

so that

$$231 = 3 \times 7 \times 11.$$

Hence all possible divisors of 231 are 3, 7, 11, 21, 33, 77, 231.