THE USE OF VEDIC MATHEMATICS IN MODULAR ARITHMETIC AND PRIME FACTORISATION

Usha Sundararaman , Dubai

Introduction

Vedic Mathematics concepts like the nine-point circle as well as digital roots can be used to study various aspects of modular arithmetic, and can be of particular use in the identification of prime numbers. Primes are of interest, as prime factorisation is commonly used to secure public-key encryption systems. Finding the two prime factors of a very large prime number can be very difficult and time-consuming.

This paper discusses how the prime factors of some relatively big numbers can be found by making use of "osculators" in the Vedic method of Division by Primes. Modular Arithmetic is used to help explain why the process works. Before attempting to find a factor of a number, it it useful to know that it is, indeed factorisable (i.e. it is not prime). Digital roots can be of great help in this regard as, for instance, a number (other than 3) is not prime if its digital root is 3, 6 or 9. (Such numbers are divisible by 3.)

Some Important Definitions

A ***prime number*** is an integer (a whole number) that only has 1 and itself as factors.

Modular arithmetic involves carrying out addition (and other operations) not on a line, but on a circle: the values "wrap around", always staying less than a fixed number called the modulus. The way DVD's store or satellites transmit large amounts of data without corrupting it, involves the use of modular arithmetic. Reed-Solomon error correcting codes employ modular arithmetic. Cryptographic codes which keep, for example, our banking transactions secure are also closely connected to the theory of modular arithmetic.

The ***digital root*** of a number is found by adding all the digits in the number together. If the answer to this digit sum contains more than two digits, these *digits are again added together. This process is repeated until the answer only* contains one digit. For instance, the digit sum of 9023 is 14. The digit sum of 14 - and therefore also the final digital root of 9023 - is 5.

The ***modulo*** operation finds the remainder after the division of one number by another. For example, 15 mod 7 = 1, as there is a remainder of 1 when 15 is divided by 7. The congruence $28 \equiv 35 \pmod{7}$ means that both 28 and 35 yield the same remainder when divided by 7. The congruence $x \equiv 0 \pmod{7}$ means that x has a remainder of zero when divided by 7, i.e. x is divisible by 7.

Identifying whether a number is Prime or not

The process of finding a prime factor of a very large number, and thus identifying it as non-prime, is very often based on trial and error. Modular arithmetic (as well as methods in Vedic Mathematics – shown in the next section) can be usefully employed to facilitate the process.

Table 1 shows the digital roots of all the prime numbers below 200. We see (with the exception of the number 3) that the roots are either 1, 2, 4, 5, 7 or 8. This is because all numbers which have digital roots of 3, 6 or 9 are divisible by 3, and are thus not prime (except for the number 3 itself).

Table 1: The Digital Roots of Primes below 200

Digital Root	1	2	3	4	5	6	7	8	9
		2	3		5		7		
		11		13				17	
	19				23				
		29		31					
	37				41				
				43					
		47						53	
					59		61		
				67				71	
	73						79		
		83						89	
							97		
		101		103				107	
	109				113				
	127				131				
		137		139	149		151		
				157					
	163				167				
		173						179	
	181								
		191		193				197	
	199								

In Table 2, the Sieve of Eratosthenes is shown for numbers from 1001 to 1100. The “sifting” (identification as non-prime) process follows the following steps:

All even numbers (divisible by 2) and numbers ending on a 5 (divisible by 5) are eliminated (shaded light grey) .

The digital roots of the remaining numbers are calculated. Those with digitals roots of 3, 6 and 9 are also eliminated (shaded slightly darker grey). Such numbers are divisible by 3.

Table 2: The Sieve of Eratosthenes

1001	1002	1003	1004	1005	1006	1007	1008	1009	1010
1011	1012	1013	1014	1015	1016	1017	1018	1019	1020
1021	1022	1023	1024	1025	1026	1027	1028	1029	1030
1031	1032	1033	1034	1035	1036	1037	1038	1039	1040
1041	1042	1043	1044	1045	1046	1047	1048	1049	1050
1051	1052	1053	1054	1055	1056	1057	1058	1059	1060
1061	1062	1063	1064	1065	1066	1067	1068	1069	1070
1071	1072	1073	1074	1075	1076	1077	1078	1079	1080
1081	1082	1083	1084	1085	1086	1087	1088	1089	1090
1091	1092	1093	1094	1095	1096	1097	1098	1099	1100

The remaining numbers (in white) might or might not be prime. They now need to be tested for divisibility by primes other than 2, 3 or 5.

The following section explains how Modular Arithmetic can be used to help find some of the prime factors (specifically 7 and 13) of all the (as yet, unidentified) non-primes remaining in Table 2. As will be shown later, there are twelve numbers which are not prime.

Checking for Divisibility by 7 and 13 using Modular Arithmetic

Divisibility by 7:

Let N be a number divisible by 7. This means that $N = 7K$ where K is an integer.

We can write $N = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10a_1 + a_0 = 7K$

$N = 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + a_1) + a_0 = 7K$

Let $(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + a_1) = A$ and $a_0 = B$, then $N = 10A + B = 7K$

Adding and then also subtracting $20B$ yields

$N = 10A + B - 20B + 20B = 7K$

which yields

$N = 10(A - 2B) = 7(K - 3B)$

Since, 10 mod 7 = 3, for N to be divisible by 7, it follows that when the factor $(A - 2B)$ is divided by 7, the remainder must be 0, i.e. $(A - 2B) \equiv 0 \pmod 7$.

We thus see that if N is divisible by 7, then $N = (10A + B) \equiv (A - 2B) \pmod 7$.

Example: Is 2023 divisible by 7?

$A = 202$, $B = 3$, $(A - 2B) = (202 - 2*3) = 196$

The process is now repeated for 196:

$A = 19$, $B = 6$, $(A - 2B) = (19 - 2*6) = 7$

Thus $(A - 2B) \equiv 0 \pmod 7$, and thus 2023 is shown to be divisible by 7.

Divisibility by 13:

Let N be a number divisible by 13. This means that $N = 13K$ where K is an integer.

We can write $N = 10^n a_n + 10^{n-1} a_{n-1} + \ldots + 10a_1 + a_0 = 13K$

$N = 10(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + a_1) + a_0 = 13K$

Let $(10^{n-1}a_n + 10^{n-2}a_{n-1} + \ldots + a_1) = A$ and $a_0 = B$, then

$N = 10A + B = 13K$

Adding and then also subtracting 40B yields

$N = 10A + B - 40B + 40B = 13K$

which yields

$N = 10(A + 4B) = 13(K - 3B)$

Since, 10 mod 13 = 10, for N to be divisible by 13, it follows that when (A + 4B) is divided by 13, the remainder must be 0, i.e. $(A + 4B) \equiv 0 \pmod{13}$.

We thus see that if N is divisible by 13, then $N = (10A + B) \equiv (A + 4B) \pmod 7$.

Example: Is 50661 divisible by 13?

$A = 5066$, $B = 1$, $(A + 4B) = (5066 + 4*1) = 5070$

The process is now repeated for 5070: $A = 507$, $B = 0$, $(A + 4B) = 507$

The process is repeated for 507: $A = 50$, $B = 7$, $(A + 4B) = 78$

The process is repeated for 78: $A = 7$, $B = 8$, $(A + 4B) = 39$

If the process is repeated for 39: $A = 3$, $B = 9$, $(A + 4B) = 39$

we see that 39 is again obtained. The process can now be terminated, since $39 \equiv 0 \pmod{13}$, thus $(A + 4B) \equiv 0 \pmod{13}$. Thus 50661 is shown to be divisible by 13.

In the test for divisibility of a number $N = (10A + B)$ by 7, the value of $(A - 2B)$ is determined. This value is, itself, then written in the form $(10A' + B')$ and the value of $(A' - 2B')$ is determined. The process is repeated until a final $(A'' - 2B'')$ value is found for which $(A'' - 2B'') \equiv 0 \pmod 7$.

In the test for divisibility of a number $N = (10A + B)$ by 13, the value of $(A + 4B)$ is determined. This value is, itself, then written in the form $(10A' + B')$ and the value of $(A' + 4B')$ is determined. The process is repeated until a final $(A'' + 2B'')$ value is found for which $(A'' + 4B'') \equiv 0 \pmod{13}$.

These modulo proofs for divisibility by the primes 7 and 13 can be extended to other prime numbers as well.

Table 3 summarises the $(A \pm nB)$ values which are employed in the identification of the twelve (previously unidentified) non-primes in Table 2. The prime divisors have been found to be 7, 11, 13, 17, 19, 23 and 29.

Table 3: The application of $(A \pm nB)$ values for prime divisors 7 to 29

	Divi-sor	$(A \pm nB)$ value	Initial A	Initial B	Final A	Final B	Final Step
1001	7	$(A - 2B) \equiv 0 \pmod{7}$	100	1	9	8	9 - 2*8 = -7
1003	17	$(A - 5B) \equiv 0 \pmod{17}$	100	3	8	5	8 - 5*5 = -17
1007	19	$(A+2B) \equiv 0 \pmod{19}$	100	7	11	4	11 + 2*4 =19
1027	13	$(A+4B) \equiv 0 \pmod{13}$	102	7	13	0	13 + 4*0 = 13
1037	17	$(A - 5B) \equiv 0 \pmod{17}$	103	7	6	8	6 - 5*8 = -34 $-34 \equiv 0 \pmod{17}$
1043	7	$(A - 2B) \equiv 0 \pmod{7}$	104	3	9	8	9 - 2*8 = -7
1057	7	$(A - 2B) \equiv 0 \pmod{7}$	105	7	9	1	$9-2*1=7 \equiv 0$
1067	11	$(A - B) \equiv 0 \pmod{11}$	106	7	9	9	9 - 9 = 0
1073	29	$(A+3B) \equiv 0 \pmod{29}$	107	3	11	6	11 + 3*6 = 29
1079	13	$(A+4B) \equiv 0 \pmod{13}$	107	9	14	3	14 + 4*3 = 26 $26 \equiv 0 \pmod{13}$
1081	23	$(A+7B) \equiv 0 \pmod{23}$	108	1	11	5	11 + 7*5 = 46 $46 \equiv 0 \pmod{23}$
1099	7	$(A - 2B) \equiv 0 \pmod{7}$	109	9	9	9	9 - 2*1= 7

It can be observed that every prime divisor has a particular the $(A \pm nB)$ value associated with it.

The Relationship between $(A \pm nB)$ Values and the Osculators (Vestana) Employed in Vedic Mathematics Divisibility Tests

Although osculators can generally be used to check for the divisibility of a number by any integer, the ensuing discussion focuses specifically on the use of Vedic Mathematics osculators in testing for divisibility by prime numbers.

The divisibility test involves multiplying digits by an *osculator* from right to left. The osculator for a particular divisibly check equals the n in the expression $(A \pm nB)$ related to the divisor being investigated. It can be seen from the examples below that division by numbers ending in the digits 3 and 9 have positive osculators (or n-values) associated with them, while division by numbers ending in the digits 1 and 7 have negative osculators. Positive n-values for numbers ending on 1 and 7 can, however, also be employed.

Positive Osculators

Divisors ending on the digit 9 have positive osculators. It can be shown that the n-values 09, 19, 29, 59, … have the respective osculators 0+1=1, 1+1=2, 2+1=3, 5+1=6, etc.

Divisors ending on the digit 3 also have positive osculators. To find the osculator, the divisor must be multiplied by 3, so that the final digit becomes a 9. For instance, in the case of $13 \times 3 = 39$, the osculator becomes the Ekadhika of 3, i.e. $3 + 1 = 4$. (The Ekadhika is the multiplier used on application of the sutra *Ekadhikena Purvena*.)

To test a number N for divisibility by 13, the last digit of the number must be multiplied by the osculator (4) and then added to the digit to its left. If this sum is greater than 13, the largest possible multiple of 13 must be subtracted from it, so that a number below 13 is obtained. This number is then again multiplied by the osculator 4, and the process continues until the last (left-most) digit of the numerator has been added. If the final sum obtained is 13, or a small multiple of 13, the number N is confirmed to be divisible by 13, i.e. $N \equiv 0 \pmod{13}$.

Example: Is 1027 divisble by 13?

Using the modular arithmetic approach, and finding $(A + 4B)$, we find that

$102 + (4 \times 7) = 130$, which is clearly divisible by 13. Therefore 1027 is divisible by 13.

The divisibility of 1027 by 13 can also be tested using the osculator 4. Firstly, write the last digit 7 in the bottom line as shown below.

1	0	2	7
12	16	28	
13	3	4	7

Steps: 1) $(4 \times 7) = 28$

2) $28 + 2 = 30$; but $30 > 13$, so $30 - 2(13) = 4$. Write this 4 to the left of the 7.

3) (4×4) = 16

4) 16 + 0 = 16; but 16 > 13, so 16 – 1(13) = 3. Write this 3 to the left of the 4.

5) (4×3) = 12

6) 12 + 1 = 13

Because the final sum obtained is 13, 1027 is confirmed to be divisible by 13.

Negative Osculators

Divisors ending on the digit 1 can be assigned positive or negative osculators. It can be shown that the *n*-values for the primes 11, 31, 41, 51, … have the respective negative osculators -1, -3, -4, -5 etc. (Positive osculators can be used when the numbers get too large.)

Divisors ending on the digit 7 can also have positive or negative osculators. The negative osculator for the divisor 7 is -2. This corresponds to the *n*-value obtained for the divisor 7 in the expression (*A* - 2*B*). The positive osculator for the divisor 7 can be shown to be 5. This corresponds to an *n*-value obtained for the divisor 7 in an expression (*A* + 5*B*).

Example: Is 1043 divisible by 7?

Using the modular arithmetic approach, and finding (*A* - 2*B*), we find that

104 - (2×3) = 98. Repeating the process, we obtain 9 – (2×8) = -7.

As -7 ≡ 0 (mod 7), 1043 is confirmed to be divisible by 7.

The divisibility of 1043 by 7 can also be tested using the osculator -2. A process similar to that discussed previously, is carried out:

$$\begin{array}{cccc} 1 & 0 & 4 & 3 \\ \overline{8} & 4 & \overline{6} & \\ \hline \overline{7} & 4 & \overline{2} & 3 \end{array}$$

As -7 ≡ 0 (mod 7), 1043 is confirmed to be divisible by 7.

The application of the positive osculator 5 yields:

$$\begin{array}{cccc} 1 & 0 & 4 & 3 \\ 20 & 25 & 15 & \\ \hline 21 & 4 & 5 & 3 \end{array}$$

As 21 ≡ 0 (mod 7), 1043 is confirmed to be divisible by 7.

The number 1043 can be written ss a sum of multiples of 7: 1043 = 700 + 280 + 63

700 ≡ 0 (Mod7), 280 ≡ 0(Mod7), 63 ≡ 0(Mod7)

By the modulo addition property, 1043 ≡ 0(Mod7)

An Example of a Divisibility Test for the Number 8801

The method described below involves attempting to write the number being investigated as a sum of multiples of the divisor (as far as it is possible). The modulo addition property is then employed.

Is 8801 a prime number?

a) Check for divisibility by 7

Attempt to write 8801 as the sum of multiples of 7:

$8801 = 8400 + 350 + 49 + 2$

$8400 \equiv 0(\text{Mod}7)$, $350 \equiv 0(\text{Mod}7)$, $49 \equiv 0(\text{Mod}7)$, and $2 \equiv 2(\text{Mod}7)$

By the modulo addition property, $8801 \equiv 2(\text{Mod}7)$, therefore, 8801 is not divisible by 7.

b) Check for divisibility by 11

Attempt to write 8801 as the sum of multiples of 11:

$8801 = 8800 + 1$

$8800 \equiv 0(\text{Mod}11)$, $1 \equiv 1(\text{Mod}11)$

By the modulo addition property, $8801 \equiv 1(\text{Mod}11)$, therefore, 8801 is not divisible by 11.

c) Check for divisibility by 13

Attempt to write 8801 as the sum of multiples of 13:

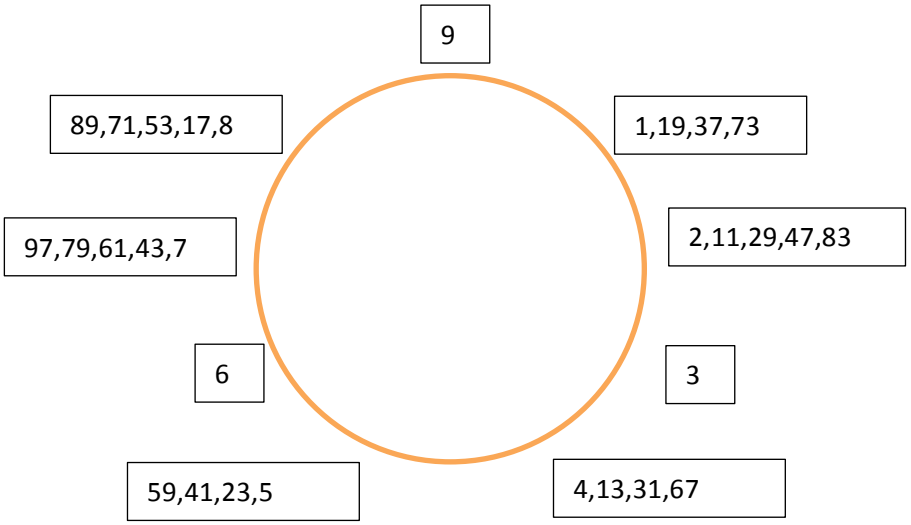
$8801 = 7800 + 910 + 91$

$780\ 0 \equiv 0(\text{Mod}13)$, $910 \equiv 0(\text{Mod}13)$, $91 \equiv 0(\text{Mod}13)$

By the modulo addition property, $8801 \equiv 0(\text{Mod}13)$, therefore, 8801 is divisible by 13.

Conclusion: 8801 is not a prime number.

Primes between 1 and 100 - arranged according to their digital roots - on a Nine Point circle



As illustrated in the diagram, the primes between 1 and 100 have been arranged at nine different positions around a circle. All the primes with digital roots equal to 1 (i.e. 1, 19, 37 and 73) are placed at the first position; those with digital roots equal to 2 (i.e. 2, 11, 29, 47 and 83) are placed at the second position, and so forth. As no primes (other than 3) have digital roots of 3, 6 and 9, there are no prime numbers (other than 3) situated at positions 3, 6 and 9.

Arranging larger and larger primes this way can be a technique to help investigate possible patterns which might emerge.

Conclusion

This paper has illustrated how modular processes underlie the working of the osculators in Vedic Mathematics divisibility checks. Modular arithmetic provides a quick and efficient method to help find the prime factors of relatively large numbers.

References

Bharati Krishna Tirthaji Maharaja, (1965). Vedic Mathematics. Delhi: Motilal Banarasidas. Chapter 29

Sundararaman, Usha, (2018), Vedic Maths in Education: Number System, Modular Arithmetic and Vedic Sutras, Proceedings of 3rd International Vedic Mathematics Conference