References

1. V. J. Ferlini, Fibonacci relationships geometrically, *Math. Gaz.* **93** (November 2009) pp. 476-481.
2. D. Aharanov, A. F. Beardon and K. D. Driver, Fibonacci, Chebyshev and orthogonal polynomials, *Amer. Math. Monthly* **112** (2005) pp. 612-630.

10.1017/mag.2022.125 © The Authors, 2022
Published by Cambridge University Press on behalf of The Mathematical Association

A. F. BEARDON
Dept. Pure Mathematics & Mathematical Statistics, University of Cambridge, Wilberforce Rd, Cambridge CB3 0WB
e-mail: *afb@dpmms.cam.ac.uk*

106.34 A theorem on divisibility by congruence

Introduction

Elementary Number Theory deals with various methods for checking divisibility by some types of numbers, see [1, 2, 3, 4, 5, 6, 7]. This Note discusses a method using congruence relation to check divisibility by digit wise computation. It is slightly different from the method proposed by J. Weitsman [5]. In school days we studied simple methods to check the divisibility of an integer by 2, 3, 5, 6 and 9. Using the following theorem we can check divisibility of an arbitrary integer by 7 or a two-digit integer ending with the digits 9, 7, 3 or 1.

Divisibility by Congruence Relation

Let s, t, d be integers with $d > 0$. Then $s \equiv t \pmod{d}$ if, and only if, $s - t$ is divisible by d.

Theorem

Let $f(x) = \sum_{i=0}^{k} a_i x^i$ and $g(x) = \sum_{i=1}^{k} a_i x^{k-i}$ be polynomials with integer coefficients and let $st \equiv 1 \pmod{d}$. Then $f(t) \equiv 0 \pmod{d}$ if, and only if, $g(s) \equiv 0 \pmod{d}$.

Proof:

For $i = 0, 1, \ldots, k$; we have $s^i t^i \equiv 1 \pmod{d}$, since $st \equiv 1 \pmod{d}$. Multiplying both sides of the congruence relations by $a_i s^{k-i}$ and adding the $k+1$ relations, we have $\sum_{i=0}^{k} a_i s^k t^i \equiv \sum_{i=0}^{k} a_i s^{k-i} \pmod{d}$. Hence $s^k \sum_{i=0}^{k} a_i t^i \equiv \sum_{i=0}^{k} a_i s^{k-i} \pmod{d}$. That is, $s^k f(t) \equiv g(s) \pmod{d}$. The relation $s^k t^k \equiv 1 \pmod{d}$ implies s^k and d are relatively prime. Therefore, $f(t) \equiv 0 \pmod{d}$ if, and only if, $s^k f(t) \equiv 0 \pmod{d}$ if, and only if, $g(s) \equiv 0 \pmod{d}$.

https://doi.org/10.1017/mag.2022.126 Published online by Cambridge University Press

Corollary 1: Let $f(t) = \sum_{i=0}^{k} a_i t^i$, $g(t) = \sum_{i=0}^{k} a_i t^{k-i}$ and $st \equiv -1 \pmod{d}$. Then $f(t) \equiv 0 \pmod{d}$ if, and only if. $g(-s) \equiv 0 \pmod{d}$.

Corollary 2: Let $f(t) = \sum_{i=0}^{k} a_i t^i$, $g(t) = \sum_{i=0}^{k} a_i t^{k-i}$, $n = f(10) = \sum_{i=0}^{k} a_i 10^i$ and $a_i \in \{0, 1, 2, \ldots, 9\}$.

Case I: Suppose that $d = 10q - 1$ and $q \in \{1, 2, \ldots, 9\}$, that is $10q \equiv 1 \pmod{d}$. Then d divides n if, and only if, d divides $\sum_{i=0}^{k} a_i q^{k-i}$. That is

$$n = f(10) = \sum_{i=0}^{k} a_i 10^i$$

$$= \left(\left(\ldots\left(\left(a_k 10 + a_{k-1}\right)10 + a_{k-2}\right)10 + \ldots + a_2\right)10 + a_1\right)10 + a_0$$

if, and only if, d divides

$$m = \sum_{i=0}^{k} a_i q^{k-i} = a_k + q\left(a_{k-1} + q\left(a_{k-2} + \ldots + q\left(a_1 + a_0 q\right)\ldots\right)\right).$$

Algorithm: Let $u_0 = a_0$;

$$u_i = a_i + q u_{i-1}, \text{ for } i = 1, 2, \ldots, k.$$

Conclusion: $n \equiv 0 \pmod{d}$ if, and only if, $u_k \equiv 0 \pmod{d}$.

Modified algorithm: Let $v_0 = a_0$;

v_i is the remainder obtained when dividing $a_i + q v_{i-1}$ by d for $i = 1, 2, \ldots, k$.

Conclusion: $n \equiv 0 \pmod{d}$ if, and only if, $v_k \equiv 0 \pmod{d}$.

Case II: Suppose that $d = 10q + 1$, that is, $10q \equiv -1 \pmod{d}$. Then d divides n if, and only if, d divides $\sum_{i=0}^{k} (-1)^i a_i q^{k-i}$.

Example 1: Let $n = 92796$ and let $d = 19 = 2 \times 10 - 1$. So $q = 2$ is the multiplier.

Step 1: $v_0 = 6$;
Step 2: $6 \times 2 + 9 = 21 \equiv 2 \pmod{19}$, $v_1 = 2$;
Step 3: $2 \times 2 + 7 = 11 \equiv 11 \pmod{19}$, $v_2 = 11$;
Step 4: $11 \times 2 + 2 = 24 \equiv 5 \pmod{19}$, $v_3 = 5$;
Step 5: $5 \times 2 + 9 = 19 \equiv 0 \pmod{19}$, $v_4 = 0$.

https://doi.org/10.1017/mag.2022.126 Published online by Cambridge University Press

Summarize the steps as follows:

$$\begin{array}{rcccccc} a_i & : & 9 & 2 & 7 & 9 & 6 \\ v_{i-1}q + a_i & : & 19 & 24 & 11 & 21 & \\ v_i & : & (0) & 5 & 11 & 2 & 6 \end{array}$$

Hence $92796 \equiv 0 \pmod{19}$ and 92796 is divisible by 19.

Corollary 3: For checking divisibility by $d = 29, 39, 49, 59, 69, 79, 89$ we can use the multipliers $q = 3, 4, 5, 6, 7, 8, 9$ respectively in the modified algorithm. If the divisor d is a two-digit number ending with 1, then there exists a one-digit positive integer q such that $10q \equiv -1 \pmod{d}$. That is $10(-q) \equiv 1 \pmod{d}$. Therefore, the multipliers $-1, -2, -3, \ldots, -9$ respectively can be used to check divisibility by $d = 11, 21, 31, \ldots, 91$ in the modified algorithm. Since $7 \times 3 = 21$ and $7 \times 7 = 49$ we have $10 \times 2 \equiv -1 \pmod{7}$ and $10 \times 5 \equiv 1 \pmod{7}$. So -2 and 5 are the multipliers for checking divisibility by 7 in the modified algorithm. Similarly, 4 and -9 are the multipliers for $d = 13$. Divisibility by 15, 25,...,95 are the divisibility by 5 and divisibility by $3, 5, \ldots, 19$ respectively.

Example 2: Let $n = 863172$ and let $d = 7$. Then $10 \times (-2) \equiv 1 \pmod{7}$ and $q = -2$

$$\begin{array}{rcccccc} a_i & : & 8 & 6 & 3 & 1 & 7 & 2 \\ v_{i-1}q + a_i & : & 6 & -6 & -1 & -5 & 3 & \\ v_i & : & (6) & 1 & 6 & 2 & 3 & 2 \end{array}$$

That is, $863172 \not\equiv 0 \pmod{7}$. Hence 863172 is not divisible by 7.

Unsolved Problem: (Prove or disprove the following statement)

Let p_n be the nth prime, $T_1 = p_1$ and $T_n = p_n^{T_{n-1}}$. Then $T_n \equiv -1 \pmod{p_{n+1}}$.

Acknowledgements

This research work is partially supported by the University Grants Commission of India (MRP(S)-358/2005(X Plan)/KLKA019/UGC-SWRO).

References

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Text in Mathematics, Springer-Verlag (1976).
2. Y. Cherniavsky and A. Mouftakhov, Zbikowski's Divisibility Criterion, *College Math. J.* **45** (2014) pp. 17-21.
3. P. Cohn, Tests for divisibility, *Math. Gaz.* **27** (February 1943) pp. 28-29.
4. B. K. T. Maharaja, *Vedic Mathematics*, Motilal Banarsidass, Delhi (1978).
5. J. Weitsman, A general test for divisibility by primes, *Math. Gaz.* **64** (December 1980) pp. 255-262.

https://doi.org/10.1017/mag.2022.126 Published online by Cambridge University Press

6. J. Whittaker, A new divisibility algorithm, *College Math. J.* **16** (1985) pp. 268-276.
7. Wikipedia, *The Free Encyclopedia*, https://en.wikipedia.org/wiki/Divisibility rule#cite_note-12.

10.1017/mag.2022.126 © The Authors, 2022
Published by Cambridge University Press on behalf of The Mathematical Association

SABU SEBASTIAN
Department of Mathematics, Nirmalagiri College, Kannur-670701, Kerala, India
e-mail: *sabus@nirmalagiricollege.ac.in*

106.35 On the representation of rational numbers in the form $\frac{(\phi(m^r))^a}{(\phi(n^s))^b}$

In number theory, Euler's totient function $\phi(n)$ counts the positive integers up to a given integer n that are relatively prime to n (see, for example [1]). Recently, the following interesting result was proved:

Theorem 1: [Krachun and Sun, [2]] Any positive rational number q can be written as $q = \frac{\phi(m^2)}{\phi(n^2)}$, where m and n are positive integers.

Here we modify Krachun and Sun's proof and establish:

Theorem 2: Let a, b, r, s be positive integers such that $\gcd(ar, bs) = 1$. Then, given any positive rational number q, there exist infinitely many pairs of positive integers (m, n) such that $q = \frac{(\phi(m^r))^a}{(\phi(n^s))^b}$.

Proof:

Let $2 = p_1 < p_2 < p_3 < \ldots$ be the sequence of all primes. Let $Q_0 = \{1\}$ and for $k \in \mathbb{N}^+$ let $Q_k = \left\{\prod_{i=1}^{k} p_i^{\alpha_i} \mid \alpha_i \in \mathbb{Z}, 1 \leqslant i \leqslant k\right\}$ be the set of all positive rational numbers that can expressed as the product of integer powers of the first k primes.

We claim a stronger result: If $q \in Q_k$ then there exist positive integers $m, n \in Q_k$ such that $q = \frac{(\phi(m^r))^a}{(\phi(n^s))^b}$. We prove the claim by induction on k.

The base of the induction is $k = 0$. Since $\gcd(ar, bs) = 1$, Euclid's algorithm shows that there exists infinitely many pairs (x, y) of positive integers such that $arx - bsy = a - b$. Take $m = 2^x$, $n = 2^y$. Since $\phi(2^i) = 2^{i-1}$, we have:

$$\frac{(\phi(2^{rx}))^a}{(\phi(2^{sy}))^b} = \frac{2^{a(rx-1)}}{2^{b(sy-1)}} = 1.$$

So for $k = 0$, the claim holds.

https://doi.org/10.1017/mag.2022.126 Published online by Cambridge University Press