Bull. Malays. Math. Sci. Soc. (2023) 46:161
https://doi.org/10.1007/s40840-023-01556-5

BULLETIN *of the* MALAYSIAN MATHEMATICAL SCIENCES SOCIETY
http://www.springer.com/mathematics/journal/40840

Divisibility of Finite Geometric Series

Robert E. Hartwig[1] **· Pedro Patrício**[2]

Received: 26 May 2022 / Revised: 20 June 2023 / Accepted: 6 July 2023 /
Published online: 17 July 2023

Abstract

We give necessary and sufficient conditions for the divisibility of two finite geometric series $G_n(x) = 1 + x + x^2 + \cdots + x^{n-1}$ over a field of characteristic zero.

Keywords Finite geometric series · Divisibility · Greatest common divisor

Mathematics Subject Classification 13F07 · 11A05

1 Introduction

The geometric series

$$G_n(x) = 1 + x + x^2 + \cdots + x^{n-1}$$

(also called geometric progression or GP for short) is an important two-parameter concept used in many branches of mathematics, such as in power series, convergence, telescoping matrix theory [4], number theory [2, 3] and algebraic curves, and has applications in cryptography [1].

For convenience, we shall write G_n for $G_n(x)$, when there is no risk of confusion. It is well known that $(x-1)G_n(x) = x^n - 1$. As such, it is clear that many of the properties of $G_n(x)$ follow from those of $x^n - 1$. We shall refer to the latter as the "binomial" of the geometric progression.

Communicated by See Keong Lee.

✉ Pedro Patrício
pedro@math.uminho.pt

Robert E. Hartwig
hartwig@unity.ncsu.edu

1 Mathematics Department, N.C.S.U., Raleigh, NC 27695-8205, USA

2 CMAT – Centro de Matemática and Departamento de Matemática, Universidade do Minho, 4710-057 Braga, Portugal

When q is a prime power, say $q = p^e$, the geometric ratio $G_n(q)$ corresponds to the number of points and of hyperplanes of the projective space $\mathbb{P}^{n-1}(\mathbb{F}_q)$; if it is a prime number, then $G_n(q)$ is called a *projective prime*.

The case $G_2\left(2^{2^e}\right)$ turns into a Fermat number, whereas $2^n - 1 = G_n(2)$ is a Mersènne number. As in these two particular cases, it is conjectured that there exist infinitely many projective primes.

As in the Mersènne numbers, the primality of $G_n(q)$ implies the primality of n. Indeed, we may use the Product Rule (see (1)) that we will address later to write $G_n(q) = G_{dt}(q) = G_d(q)G_t(q^d)$, assuming $n = dt$ is a non-trivial factorization.

Our aim is investigate the fundamental question of when $G_n(x^p)$ divides $G_m(x^q)$—as a polynomial. This four-parameter problem will be referred to as the (n, p, m, q) property.

As always, we shall build on the simpler cases, such as the $(n, 1, n, q)$ and $(n, 1, m, q)$ cases, where $m = n$ and $p = 1$, or just when $p = 1$.

All our results will be over a field $\mathbb{F}$ with $char(\mathbb{F}) = 0$. The greatest common divisor and the least common multiple of a and b will be denoted by (a, b) and $[a, b]$, respectively.

We shall need a multitude of preliminary results, which are needed to build our case.

2 Building Blocks

Given integers m and n, let $(m, n) = d$ and suppose that $n = mq + r$, where $0 \le r < m \le n$. Then,

$$x^n - 1 = x^r(x^{mq} - 1) + x^r - 1 = (x^m - 1)x^r G_q(x^m) + x^r - 1.$$

This shows at once that

$$m|n \Leftrightarrow x^m - 1|x^n - 1 \Leftrightarrow G_m(x)|G_n(x)$$

and hence that

$$(x^m - 1, x^n - 1) = x^d - 1 = (x - 1)(G_m, G_n).$$

Consequently,

$$G_d = \frac{x^d - 1}{x - 1} = (G_m, G_n)$$

and thus

$$(G_m, G_n) = 1 \Leftrightarrow (m, n) = 1.$$

Next, let $L = [m, n] = lcm(m, n) = \frac{mn}{d}$. We also set $m = dm'$ and $n = dn'$ so that $L = mn' = nm' = m'n'd$.

We now observe that if $n|L$ and $m|L$, then $x^n-1|x^L-1$ and $x^m-1|x^L-1$. Hence, $[x^m-1, x^n-1]|x^L-1|x^{mn}-1$, and thus

$$\frac{(x^m-1)(x^n-1)}{(x^d-1)}|x^L-1|x^{mn}-1$$

which may be expressed as

$$G_m(x)G_n(x)|G_L(x)G_d(x)|G_{mn}(x)G_d(x).$$

For $x \neq 1$, we have

$$\frac{G_{np}(x)}{G_p(x)} = \frac{x^{np}-1}{x-1}.\frac{x-1}{x^p-1} = \frac{x^{np}-1}{x^p-1} = G_n(x^p),$$

and thus for all x

$$G_{np}(x) = G_p(x)G_n(x^p), \tag{1}$$

which we refer to as the Product Rule.

It immediately extends to larger products such as

$$G_{abc} = G_aG_{bc}(x^a) = G_aG_b(x^a)G_c(x^{ab}).$$

A further consequence of the Product Rule is the “q equals one lemma":

Lemma 2.1 (The $q=1$ case) *The following are equivalent:*

(i) $(n, p, n, 1)$ *holds.*
(ii) $G_n(x^p)|G_n(x)$.
(iii) $G_{np}|G_nG_p$.
(iv) $n=1$ *or* $p=1$.

Proof The equivalence of (ii)–(iii) follows from the definition and the Product Rule.

If (iii) holds, then using degrees we see that $(np-1) \leq (n-1)+(p-1)$, which tells us that

$$(n-1)(p-1) \leq 0.$$

Since $n \geq 1$ and $p \geq 1$, it follows that (iv) must hold. Lastly, it is clear that (iv) implies (ii). □

The following is a key result, which critically depends on the fact that char($\mathbb{F}$) = 0. This will be referred to it as the Linking Lemma with parameter m and links the sub- and superscripts in the two GPs, each of which contains the parameter m.

Lemma 2.2 (Linking Lemma) *For any m, n and k,*

$$(G_m(x), G_n(x^{km})) = 1.$$

Proof We begin by noting that $G_n(1) = n$, which when $char(\mathbb{F}) = 0$ cannot be equal to 0. Now by the remainder theorem

$$G_n(x) = (x-1)Q(x) + G_n(1)$$

and thus as $G_n(1) \neq 0$, we conclude that $(x-1) \not| G_n(x)$, or

$$(x-1, G_n(x)) = 1.$$

Replacing x by x^{mk} gives $\left(x^{mk}-1, G_n(x^{mk})\right) = 1$ and so

$$\Big((x-1)G_m(x)G_k(x^m), G_n(x^{mk})\Big) = 1.$$

This means that for any m, n and k

$$\Big(G_m(x), G_n(x^{mk})\Big) = 1.$$

□

We use both the Product Rule and the Linking Lemma in the following Basic Lemma, which is a first step in our investigation of $G_n(x^p)|G_m(x^q)$.

Lemma 2.3 *((n,1,n,q)) The following are equivalent:*

(1) $G_n(x)|G_n(x^q)$ *i.e.* $(n, 1, n, q)$ *holds.*
(2) $G_n(x)G_q(x)|G_{qn}(x)$.
(3) $(q, n) = 1$.

Proof From the Product Rule, it is clear that (1) ⇔ (2).

Let $(q, n) = d$ and $q = q'd$, $n = n'd$ and suppose that (1) holds. Then,

$$G_n(x)|G_n(x^q) \Rightarrow G_{n'd}(x)|G_n(x^{q'd}) \Rightarrow G_d G_{n'}(x^d)|G_n(x^{q'd}).$$

By the Linking Lemma, we now get $G_d = 1$ and thus (3) follows.
Conversely, we always have that

$$G_q G_n | G_{qn} G_d$$

and hence, if $d = 1$, then (2) follows. □

We can immediately extend this to

Lemma 2.4 (Key (n,1,m,q)) *The following are equivalent:*

(1) $G_n(x)|G_m(x^q)$ *i.e. (n,1,m,q) holds.*
(2) $G_n(x)G_q(x)|G_{mq}(x)$.
(3) $(n,q)=1$ *and* $n|m$.

Proof The equivalence of (1) and (2) follows again from the Product Rule.

Let $(m,n)=d$ and $m=m'd, n=n'd$. Also set $(n,q)=e$ and $n=n''e, q=q''e$. Then, $G_n(x)=G_e(x)G_{n''}(x^e)|G_m(x^{q''e})$. By the Linking Lemma, with exponent e, we see that $G_e(x)=1$ and thus $e=(q,n)=1$. Applying the Basic Lemma, we get $G_nG_q|G_{nq}$. Combining this with (2), we conclude that

$$G_nG_q|(G_{mq},G_{nq})=G_{(mq,nq)}=G_{qd}.$$

This implies that $G_n|G_{dq}$ and thus $n|dq$. Since $(n,q)=1$, it follows that $n|d$, and we may conclude that $n=d$ and $n|m$ so that (3) follows.

Conversely, if $(n,q)=1$, then Lemma 2.3, $G_nG_q|G_{nq}$ and since $n|m$, we also have $G_{nq}|G_{mq}$. Combining these, we arrive at $G_nG_q|G_{mq}$ giving (2). □

3 The Polynomial Ratio

In what follows, we shall need several polynomial results dealing with greatest common divisors. In particular, we recall

Lemma 3.1 *Over an Euclidean domain,*

1. *The gcd Product Rule holds:*

$$(ab,cd)=(a,c)(b,d)(a'b',c'd'),$$

where $a'=a/(a,c), c'=c/(a,c), b'=b/(b,d), d'=d/(b,d)$.

2.

$$(ab,cd)=1 \text{ if and only if } 1=(a,c)=(a,d)=(b,c)=(b,d).$$

We now come to a refinement of the four parameters m, n, p and q, indicating the interaction between them.

Given p and q, let $(p,q)=w$ and set $p=p'w$ and $q=q'w$, with $(p',q')=1$.

Consider the rational ratio

$$R=\frac{G_m(x^q)}{G_n(x^p)}=\frac{G_m(x^{q'w})}{G_n(x^{p'w})}=\frac{G_m(y^{q'})}{G_n(y^{p'})},$$

where $y=x^w$. Thus, without loss of generality we may assume that $(p,q)=1$; otherwise, in the final answer replace x by x^w.

We begin by establishing the desired splitting of our four parameters. As such, we define:

$$\begin{array}{llll} d=(m,n), & m=m'd, & n=n'd, & \text{with } (m',n')=1 \\ f=(m',p), & m'=\hat{m}f, & p=\hat{p}f, & \text{with } (\hat{m},\hat{p})=1 \\ g=(n',q), & n'=\bar{n}g, & q=\bar{q}g, & \text{with } (\bar{n},\bar{q})=1 \\ h=(\hat{p},d), & \hat{p}=\tilde{p}h, & d=\tilde{d}h, & \text{with } (\tilde{p},\tilde{d})=1 \\ t=(\bar{q},d), & \bar{q}=q''t, & d=d''t, & \text{with } (q'',d'')=1. \end{array}$$

Further, we set $r=\hat{m}\bar{q}$ and $s=\hat{p}\bar{n}$.

Because $(m',n')=1=(p,q)$, we know that $e=(m'q,n'p)=(m',p)(n',q)=fg$.

We also observe that

$$(s,r)=(\hat{p}\cdot\bar{n},\hat{m}\bar{q})=1,$$

because all four partial gcds equal one, i.e. $(\hat{p},\bar{q})=1=(\hat{m},\bar{n})=(\hat{p},\hat{m})=(\bar{n},\bar{q})$.

From the Product Rule, we know that

$$R \text{ is a polynomial} \Leftrightarrow G_n(x^p)|G_m(x^q) \Leftrightarrow \frac{G_{np}}{G_p}\Big|\frac{G_{mq}}{G_q} \Leftrightarrow G_qG_{np}|G_pG_{mq}.$$

Now $np=(de)(\hat{p}\bar{n})=(de)s$ and $mq=(de)\hat{m}\bar{q}=(de)r$ and hence

$$R \text{ is a polynomial} \Leftrightarrow G_qG_{de}G_{\hat{p}\bar{n}}(x^{de})|G_pG_{de}G_{\hat{m}\bar{q}}(x^{de}) \Leftrightarrow G_qG_s(x^{de})|G_pG_r(x^{de}).$$

Because $(p,q)=1=(r,s)$, we know that $(G_p(x),G_q(x))=1=(G_r(x^{de}), G_s(x^{de}))$. And thus R will be a polynomial if and only if both of the following conditions hold:

$$\text{(I)}\quad G_q(x)|G_r(x^{de}) \text{ and (II)}\quad G_s(x^{de})|G_p.$$

Let us now examine these two conditions.

Turning to condition (I), we have $q=g\bar{q}$ and $r=\hat{m}\bar{q}$, and thus

$$G_q(x)|G_r(x^{de}) \Leftrightarrow G_g(x)G_{\bar{q}}(x^g)|G_{\bar{q}}(x^{de})G_{\hat{m}}(x^{de\bar{q}}).$$

Since g divides de, we can use the Linking Lemma to conclude that G_g is coprime to both factors of the RHS. As such, we must have $G_g=1$, and thus $g=1$. This means that $n'=\bar{n}$ and $q=\bar{q}$.

We are left with

$$G_{\bar{q}}|G_{\bar{q}}(x^{de})G_{\hat{m}}(x^{de\bar{q}}).$$

Again, the Linking Lemma implies that

$$(G_{\bar{q}},G_{\hat{m}}(x^{de\bar{q}}))=1$$

which leaves us with

$$G_{\bar{q}}|G_{\bar{q}}(x^{de}).$$

Using the Basic $(n, 1, n, q)$ Lemma, we arrive at $(\bar{q}, de) = (q, de) = 1$. This shows that

$$t = (q, d) = 1 \tag{2}$$

in addition to $(q, e) = (q, f) = 1$.

Turning to the second condition (II) with $e = f$, we see that splitting $s = \hat{p}\bar{n}$ and $p = \hat{p}f$, we deduce that

$$G_s(x^{df})|G_p \Leftrightarrow G_{\hat{p}}(x^{df}) \cdot G_{\bar{n}}(x^{de\hat{p}})|G_f \cdot G_{\hat{p}}(x^f).$$

Because $f|df|df\hat{p}$ and $\hat{p}|df\hat{p}$, we may conclude that

$$G_{\bar{n}}(x^{de\hat{p}}) = 1$$

and thus we must have

$$\bar{n} = 1.$$

This ensures that $n' = \bar{n} \cdot g = 1$ and hence $n = d = (m, n)$ or

$$n|m.$$

We are left with

$$G_{\hat{p}}(x^{de})|G_{\hat{p}}(x^f).$$

Comparing degrees

$$(\hat{p} - 1)df \le (\hat{p} - 1)f$$

or by using the "q equals one Lemma", we see that either $\hat{p} = 1$ or $d = 1$. In the latter case, we get $n = n'd = 1 \cdot 1 = 1$, which is excluded.

On the other hand, when $\hat{p} = 1$, $p = f = (m', p)$ so that $p|m' = \frac{m}{d} = \frac{m}{n}$.

Combining these results with (2), we see that if R is a polynomial, then $n|m$, $p|\frac{m}{n}$ and $(n, q) = 1$.

Conversely, suppose $n|m$, $p|\frac{m}{n}$ and $(q, n) = 1$.

The latter shows that $(q, pn) = (q, p)(q, n) = 1$. Next, let $m = m'n$, $m' = p$ and $m = npw$. As np divides npw, and $(np, q) = 1$, we see by the Key $(n, 1, m, q)$ Lemma that $G_{np}|G_{npw}(x^q)$. Hence,

$$G_{np}|G_pG_{pnw}(x^q) \text{ or } G_n(x^p)|G_m(x^q).$$

We have proven

Theorem 3.1

$$\frac{G_m\,(x^q)}{G_n\,(x^p)} \textit{ is a polynomial}$$

if and only if

$$n|m,\ \ p|\frac{m}{n},\ \ (n, q) = 1.$$

4 Remarks

The above establishes when the ratio R will be a polynomial. However, it does not tell us what the actual polynomial is or when it will again be a GP. Also, the ratio question is a first step towards the computation of the gcd of two GPs. These topics will involve geometric series of the form $G_n(-x)$ with negative arguments and will be addressed in a later examination.

We close with a couple of non-trivial examples.

1. The (6, 3, 18, 5) case, with $n = 6$, $p = 3, m = 18, q = 5$. In this case, it is clear that $3|(18/6)$ and $(5, 6) = 1$. The GPs are $G_{18}(x^5) = x^{85} + x^{80} + x^{75} + x^{70} + x^{65} + x^{60} + x^{55} + x^{50} + x^{45} + x^{40} + x^{35} + x^{30} + x^{25} + x^{20} + x^{15} + x^{10} + x^5 + 1$, and $G_6(x^3) = x^{15} + x^{12} + x^9 + x^6 + x^3 + 1$. The quotient $R = \frac{G_{18}(x^5)}{G_6(x^3)}$ equals $x^{70} - x^{67} + x^{65} - x^{62} + x^{60} - x^{57} + x^{55} + x^{50} - x^{49} + x^{45} - x^{44} + x^{40} - x^{39} + x^{35} - x^{31} + x^{30} - x^{26} + x^{25} - x^{21} + x^{20} + x^{15} - x^{13} + x^{10} - x^8 + x^5 - x^3 + 1$.
2. The (4, 1, 4, 3) case, with $n = 4$, $p = 1, m = 4, q = 3$. The GPs are $G_4(x^3) = x^9 + x^6 + x^3 + 1$ and $G_4(x) = x^3 + x^2 + x + 1$. This time, $R = \frac{G_4(x^3)}{G_4(x)} = x^6 - x^5 + x^3 - x + 1 = G_3(-x^2)G_3(-x)$.

Acknowledgements This research was partially financed by Portuguese Funds through FCT (Fundação para a Ciência e a Tecnologia) within the Projects UIDB/00013/2020 and UIDP/00013/2020. The authors thank an anonymous referee for his/her careful reading of the manuscript and valuable corrections.

Funding Open access funding provided by FCT|FCCN (b-on).

Data availability No new data were created or analysed during this study. Data sharing is not applicable to this article.

Declarations

Conflict of interest The authors have no conflicts of interest to declare.

References

1. Bac, D.H., Binh, N., Quynh, N.X.: New algebraic structure based on cyclic geometric progressions over polynomial ring applied for cryptography. In: Proceedings—CIS Workshops 2007, International Conference on Computational Intelligence and Security Workshops, art. no. 4425610, pp. 777–780 (2007)
2. Nathanson, M.B.: Geometric progressions in syndetic sets. Archiv der Mathematik **115**(4), 413–417 (2020)
3. Patil, B.R.: Geometric progressions in syndetic sets. Archiv der Mathematik **113**(2), 157–168 (2019)
4. Patrício, P., Hartwig, R.E.: From euclid to corner sums, a trail of telescoping tricks. Filomat **35**(14), 4613–4636 (2021)