Filomat 37:29 (2023), 9973–9979
https://doi.org/10.2298/FIL2329973H

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

The GCD for finite geometric series

R.E. Hartwig[a], Pedro Patrício[b,*]

[a] *Mathematics Department, N.C.S.U., Raleigh, NC 27695-8205, U.S.A.*
[b] *CMAT – Centro de Matemática and Departamento de Matemática, Universidade do Minho, 4710-057 Braga, Portugal*

Abstract. The Greatest Common Divisor is given for a pair of finite geometric eries.

1. Introduction

We continue our investigation [5] of finite Geometric series – also called Geometric Progressions – of the form

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

by computing the Greatest Common Divisor (gcd for short)

$$\Gamma = (G_n(x^p), G_m(x^q)),$$

for a pair of such progressions, in terms of the four parameters (n, p, m, q).

Geometric series (in their finite form) play an important role in the Hyperpower Iteration ([2]) and in the Picard Iteration ([3]). On the other hand, one may use the *resultant* $R(a(x), b(x))$ ([1])

$$R(a(x), b(x)) = \det \left[\begin{array}{cccccccccc} a_n & a_{n-1} & a_{n-2} & \cdots & & a_0 & 0 & & & \\ 0 & a_n & a_{n-1} & \cdots & & & a_1 & a_0 & & \\ \vdots & & & \cdots & & & & \ddots & \ddots & \\ \vdots & & & & & & & & a_1 & a_0 \\ \hline \vdots & & & & & b_m & b_{m-1} & \cdots & b_1 & b_0 \\ \vdots & & & & b_m & b_{m-1} & \cdots & b_1 & b_0 & 0 \\ 0 & & & \cdots & & & & & & \vdots \\ b_m & b_{m-1} & b_{m-2} & \cdots & & & & & & 0 \end{array} \right]$$

2020 *Mathematics Subject Classification*. Primary 13F07; Secondary 11A05.
Keywords. Finite geometric series; Greatest common divisor
Received: 03 February 2022; Accepted: 20 June 2023
Communicated by Dijana Mosić
Research supported by Portuguese Funds through FCT (Fundação para a Ciência e a Tecnologia) within the Projects UIDB/00013/2020 and UIDP/00013/2020.
* Corresponding author: Pedro Patrício
Email addresses: hartwig@unity.ncsu.edu (R.E. Hartwig), pedro@math.uminho.pt (Pedro Patrício)

of $a(x) = \sum_{i=0}^{n} a_i x^i, b(x) = \sum_{i=0}^{m} b_i x^i \in \mathbb{C}[x]$ to check if $a(x)$ and $b(x)$ are co-prime. This happens exactly when

$$R(a(x), b(x)) \neq 0.$$

For instance, $G_4(x) = x^3 + x^2 + x + 1$ and $G_3(x^2) = x^4 + x^2 + 1$ are co-prime, since their resultant is

$$R(G_4(x), G_3(x^2) = \det \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix} = -3.$$

We shall need several preliminary results dealing with such progressions and their relation to the binomal $x^n - 1 = (x-1) \cdot G_n(x)$ and shall employ a string of basic facts for gcds of polynomials over a field $\mathbb{F}$ with $char(\mathbb{F}) = 0$.

2. Some background results

The greatest common divisor and the least common multiple of of a and b will be denoted by (a, b) and $[a, b]$, respectively.

For elements from an Euclidean domain we recall that:

1. (Switching Lemma) If $(a, c) = 1 = (b, d)$, then

$$(ab, cd) = (a, d)(b, c) \tag{2}$$

2. Using this we have the gcd product rule :

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

where $a' = a/(a, c), c' = c/(a, c), b'' = b/(b, d), d'' = d/(b, d)$, with $(a', c') = 1 = (b'', d'')$.

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

For integers m and n, let $L = [m, n] = lcm(m, n) = \frac{mn}{d}$. Also set $m = dm'$ and $n = dn'$ so that $L = mn' = mn' = m'n'd$.

Now suppose that $n = mq + r$, where $0 \leq r < m \leq n$. Then

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

which shows 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,

$$G_d = \frac{x^d - 1}{x - 1} = (G_m, G_n) \text{ and } (G_m, G_n) = 1 \Leftrightarrow (m, n) = 1.$$

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

$$G_m(x)G_n(x)|G_L(x)G_d(x)|G_{mn}(x)G_d(x). \tag{3}$$

For $x \neq 1$, we have

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

and thus for all x

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

which we refer to as the *Product Rule*.

Since $char(\mathbb{F}) = 0$, we know that $G_n(1) = n \neq 0$ and thus by the remainder theorem $(x-1) \nmid G_n(x)$, or $(x-1, G_n(x)) = 1$. Replacing x by x^{mk} then gives

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

We are left with the Linking Lemma (LL):

Lemma 2.1 (Linking Lemma (LL)). *For any m, n and k,*

$$(G_m(x), G_n(x^{km})) = 1. \tag{4}$$

3. The GCD computation

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

Consider the gcd

$$\Gamma = \Gamma^{m,q}_{n,p} = (G_n(x^p), G_m(x^q)) = (G_n(x^{p'w}), G_m(x^{q'w})) = (G_n(y^{p'}), G_m(y^{q'})),$$

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

Assuming that $(p,q) = 1$, we may use the Product Rule to rewrite Γ as

$$\Gamma = \left(\frac{G_{np}}{G_p}, \frac{G_{mq}}{G_q}\right) = \frac{1}{G_pG_q}(G_qG_{np}, G_pG_{mq}) = \frac{1}{G_pG_q}\Gamma'.$$

The computation of the gcd $\Gamma^{m,q}_{n,p}$ requires a suitable splitting of the four parameters (n,p,m,q). To this end we define:

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

and in addition set $r = \hat{m}\bar{q}$ and $s = \hat{p}.\bar{n}$.

Because $(m'n') = 1 = (p,q)$, we know from (2) that $e = (m'q, n'p) = (m',p)(n',q) = fg$.

Moreover

$$np = n'dp = \bar{n}gd\hat{p}f = de(\bar{n}\hat{p}) = des,$$

as well as

$$mq = m'dq = \hat{m}fd\bar{q}g = de(\hat{m}fd\bar{q}) = der.$$

Consequently $(np, mq) = (des, der) = de(r,s)$. Now because all four partial gcds equal one, i.e. $(\hat{p},\bar{q}) = 1 = (\hat{m},\bar{n}) = (\hat{p},\hat{m}) = (\bar{n},\bar{q})$, we may conclude by the Switching Lemma (2) that

$$(r,s) = 1.$$

We next recall a Basic Lemma:

Lemma 3.1 (Basic (n,1,n,q)). *The following are equivalent:*

1. $G_n(x)|G_n(x^q)$.
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

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

From the LL we deduce that $G_d = 1$ and thus (3) follows.
Conversely, from (3) we always have that

$$G_qG_n|G_{qn}G_d$$

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

We generalize this to

Lemma 3.2 (Key (n,1,m,q)). *The following are equivalent:*

1. $G_n(x)|G_m(x^q)$
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 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 $G_n = G_eG_{n''}(x^e)|G_m(x^{q'e})$. By the LL, with exponent e, we see that $G_e = 1$ 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, by (3.1), $G_nG_q|G_{nq}$ and since $n|m$ we also have $G_{nq}|G_{mq}$. Combining these we arrive at $G_nG_q|G_{mq}$ giving (2). □

Related is the following $(n,1,n,q)$ gcd result

Lemma 3.3 (Halfway Lemma).

$$\Gamma = (G_n(x), G_n(x^q)) = G_{n''}(x^t), \text{ where } (n,q) = t, n = n''t, \text{and } q = q''t.$$

Proof. $\Gamma = (G_t(x)G_{n''}(x^t), G_{n''t}(x^{q''t})) = (G_{n''}(x^t), G_{n''t}(x^{q''t}))$ since $(G_t(x), G_{n''t}(x^{q''t})) = 1$ by the Linking Lemma. Thus $\Gamma = (G_{n''}(x^t), G_{n''}(x^{q''t})G_t(x^{n''q''t})) = (G_{n''}(y), G_{n''}(y^{q''})G_t(y^{n''q''}))$ where $y = x^t$. Again by the LL, $(G_{n''}(y), G_t(y^{n''q''})) = 1$, which gives

$$\Gamma = (G_{n''}(y), G_{n''}(y^{q''})) = G_{n''}(y), \tag{5}$$

because by (3.1) the condition $(n'', q'') = 1$ ensures that $G_{n''}(y)|G_{n''}(y^{q''})$. □

We next consider $\Gamma' = (G_qG_{np}, G_pG_{mq})$ in which $G_{np} = G_{des} = G_{de}G_s(x^{de})$ and $G_{mq} = G_{der} = G_{de}G_r(x^{de})$. Then by the product rule

$$\Gamma' = (G_qG_{des}, G_pG_{der}) = (G_qG_{de}G_s(x^{de}), G_pG_{de}G_r(x^{de})) = G_{de}\Gamma'',$$

where

$$\Gamma'' = (G_qG_s(x^{de}), G_pG_r(x^{de}).)$$

Now since (p,q) = 1 = (r,s) we may use the switching lemma (2) to arrive at

$$\Gamma'' = (G_q, G_r(x^{de})).(G_s(x^{de}), G_p) = \Delta.\Omega$$

Also, as $q = g\bar{q}$ and r = $\bar{q}\hat{m}$ we see that the first factor becomes

$$\Delta = (G_g \cdot G_{\bar{q}}(x^g), G_{\bar{q}}(x^{de}) \cdot G_{\hat{m}}(x^{de\bar{q}})).$$

Because $g|de|de\bar{q}$ and $\bar{q}|de\bar{q}$ we may apply the Linking Lemma to conclude that
(i) $(G_g, G_{\bar{q}}(x^{dfg})G_{\hat{m}}(x^{df\bar{q}g})) = 1$;
(ii) $(G_{\bar{q}}(y), G_{\hat{m}}(y^{df\bar{q}})) = 1$, where $y = x^g$.

This means that we are left with

$$\Delta = (G_{\bar{q}}(y), G_{\bar{q}}(y^{df})).$$

From (5) we see that

$$\Delta = G_{q''}(y^t)$$

where $y = x^g$ and $t = (\bar{q}, df)$. Similarly, since $s = \hat{p}\bar{n}$

$$\Omega = (G_s(x^{de}), G_p) = (G_{\hat{p}}(x^{de})G_{\bar{n}}(x^{\hat{p}de}), G_p).$$

Again, as $p|\hat{p}de$ the Linking Lemma reduces Ω to

$$\Omega = (G_{\hat{p}}(x^{de}), G_{\hat{p}}(x^f)G_f). \tag{6}$$

Lastly because $f|de$, the Linking Lemma again gives

$$\Omega = (G_{\hat{p}}(x^{de}), G_{\hat{p}}(x^f)) = (G_{\hat{p}}(z^{dg}), G_{\hat{p}}(z)) \tag{7}$$

with $z = x^f$. Recalling that $(\hat{p}, dg) = (\hat{p}, d) = h$ and $\hat{p} = p''h$ we get

$$\Omega = G_{p''}(z^h) = G_{p''}(x^{fh})$$

Combining the above parts we may conclude that

$$\Gamma = \frac{G_{de}}{G_pG_q} G_{q''}(x^{gt})G_{p''}(x^{fh}).$$

By the product rule this may be rewritten as in the following theorem:

Theorem 3.4. *For the parameters as above, with* $(p, q) = 1$,

$$\Gamma^{m,q}_{n,p} = (G_n(x^p), G_m(x^q)) = \frac{G_{de}}{G_{hf}G_{tg}}. \tag{8}$$

Alternatively, as $de = dfg = (\tilde{d}h)fg = (d''t)fg$, we may use the product rule to rewrite G_{de} as

$$G_{de} = G_{(\tilde{d}g)hf} = G_{hf}G_{\tilde{d}g}(x^{hf}) = G_{(d''f)tg} = G_{tg}G_{d''f}(x^{tg}).$$

This shows that

$$\Gamma = \frac{G_{\tilde{d}g}(x^{hf})}{G_{tg}} = \frac{G_{d''f}(x^{tg})}{G_{hf}}.$$

We may use this expression for the gcd of two geometric series, to establish the divisibility condition for such series. Indeed we have

Corollary 3.5. *$G_n(x^p)$ divides $G_m(x^q)$ if and only if $n|m, p|\frac{m}{n}$ and $(q, n) = 1$.*

Proof. Suppose $(G_n(x^p), G_m(x^q)) = G_n(x^p)$. Using (8) we get

$$G_{de} = G_n(x^p) \cdot G_{hf} \cdot G_{tg}.$$

Setting $x = 1$ shows that

$$de = dfg = n \cdot hf \cdot tg,$$

which implies that $d = n, h = 1, t = 1$. Thus $d = n|m$ and $m' = \frac{m}{n}$. Moreover $n' = \frac{n}{d} = 1$ and hence $g = 1$ and $de = nf$.

Using this in (3) gives

$$G_{nf} = G_f \cdot G_n(x^p) \text{ or } G_n(x^f) = G_n(x^p).$$

This tells us (using degrees) that $p = f = (m', p)$ ensuring that $p|m'$ or $p|\frac{m}{n}$.

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

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

$$G_{np}|G_p \cdot G_{pnw}(x^q) \text{ or } G_n(x^p)|G_m(x^q),$$

as desired. □

4. Remarks and Examples

1. Even though these results compute the gcd implicitly, the actual polynomial ratio is not so easy to find. The same thing happens with the division of two Geometric series.
2. There are numerous ways to investigate the character of the polynomials, such as sliding division, Toeplitz matrices, Recurrence relations, etc., which we address at a later time.

4.1. *Examples*

We present several non-trivial examples. We will use the **Duplication Rules**:

(a) If n is odd then $G_n(x^{2m}) = G_n(x^m)G_n(-x^m)$.

(b) If n is even, say $n = 2k$, then $G_{2k}(x^q) = G_k(x^q)G_2(x^{qk})$.
In particular $G_{2k}(x^{2r}) = G_k(x^{2r})(x^{2kr} + 1)$.

These follow from the binomial identities:

$$G_n(x^{2m}) = \frac{x^{2mn} - 1}{x^{2m} - 1} = \frac{(x^{mn} - 1)(x^{mn} + 1)}{(x^m - 1)(x^m + 1)} = G_n(x^m)G_n(-x^m).$$

1. Consider $\Gamma^{6,4}_{12,3} = (G_{12}(x^3), G_6(x^4))$. The parameters are:

$n = 12$,	$m = 6$,	$d = (12, 6) = 6$,	$m' = 1$,
$n' = 2$,	$p = 3$,	$q = 4$,	$f = (m', p) = \hat{m} = \frac{m'}{f} = 1$,
$\hat{p} = \frac{p}{f} = p = 3$,	$g = (n', q) = 2$,	$\bar{n} = \frac{n'}{g}$,	$\bar{q} = \frac{q}{g} = 4/2 = 2$,
$h = (\hat{p}, d) = (3, 6) = 3$,	$\tilde{p} = \frac{\hat{p}}{h} = 3/3 = 1$,	$\tilde{d} = \frac{d}{h} = 6/3 = 2$,	$t = (\bar{q}, d) = (2, 6) = 2$,
$q'' = \frac{q}{t} = 1$,	$d'' = \frac{d}{t} = 3$.		

These show that $de = dfg = 6 \cdot 1 \cdot 2 = 12$, $hf = 3 \cdot 1 = 3$ and $tg = 2 \cdot 2 = 4$..
We end up with

$$\Gamma^{6,4}_{12,3} = \frac{G_{12}}{G_3 \cdot G_4} = \frac{G_3(x^4)}{G_4(x)} = \frac{1 + x^4 + x^8}{1 + x + x^2} = x^6 - x^5 + x^3 - x + 1.$$

This may actually be rewritten as $(x^4 - x^2 + 1)(x^2 - x + 1) = G_3(x^2)G_3(-x)$.
The reason for this is that

$$G_3(x^4) = G_3(x^2)G_3(-x^2) = G_3(x)G_3(-x)G_3(-x^2)$$

The latter is a special case of the Duplication Rule.

2. For computing $\Gamma^{10,3}_{18,5}$, the gcd of $G_{18}(x^5)$ and $G_{10}(x^3)$, we obtain the parameters

$$\begin{array}{llll} d=2, & f=3, & g=5, & r=3, \\ s=1, & \hat{m}=3, & \bar{n}=\hat{p}=\bar{q}=h=t=1, & \tilde{d}=d''=2, \end{array}$$

from which

$$(G_{18},(x^5),G_{10}(x^3)) = \frac{G_{10}(x^3)}{G_5} = \frac{G_{2\cdot 5}(x^3)}{G_5} = \frac{G_2(x^3)G_5(x^6)}{G_5} = \frac{G_5(x^3)}{G_5}G_2(x^3)G_5(-x^3).$$

Using Lemma 3.1, we have $G_5|G_5(x^3)$, and by long division we obtain

$$G_5\cdot(x^8-x^7+x^5-x^4+x^3-x+1)=G_5(x^3),$$

from which

$$(G_{18},(x^5),G_{10}(x^3)) = (x^8-x^7+x^5-x^4+x^3-x+1)G_2(x^3)G_5(-x^3)$$

and hence

$$\Gamma^{10,3}_{18,5} = x^{23}-x^{22}+x^{20}-x^{19}+x^{18}-x^{16}+x^{15}+x^8-x^7+x^5-x^4+x^3-x+1.$$

References

[1] Barnett, S., *Matrices in control theory: with applications to linear programming*, Van Nostrand Reinhold, 1971.
[2] Chen, X., Hartwig, R.E., *The Picard iteration and its application*, Linear Multilinear Algebra, 54 (5), pp. 329–341, 2006.
[3] Hartwig, R.E., Semrl, P., *Constrained convergence*, Rocky Mountain J. Math., 29 (1), pp. 177–195, 1999.
[4] Patrício, P., Hartwig, R.E., *From Euclid to Corner Sums, a Trail of Telescoping Tricks*, Filomat, 35(14), pp. 4613-4636, 2021.
[5] Patrício, P., Hartwig, R.E., *Divisibility of finite Geometric Series*, Bull. Malaysian Math. Sci. Soc. 46:161, 2023.