ON A PROBLEM OF BERZSENYI REGARDING THE GCD OF POLYNOMIAL EXPRESSIONS

Les Reid

Abstract. Let $G(m,k) = \max\{\mathrm{GCD}((n+1)^m + k, n^m + k) \mid n \in \mathbb{N}\}$. The fact that $G(1,k) = 1$ is trivial and Berzsenyi has shown that $G(2,k) = |4k+1|$. We give explicit formulas for $G(m,k)$ for $m = 3, 4, 5$.

1. Introduction. In the May/June 1995 issue of *Quantum* [1], George Berzsenyi defined

$$G(m,k) = \max\{\mathrm{GCD}((n+1)^m + k, n^m + k) \mid n \in \mathbb{N}\}.$$

It is obvious that $G(1,k) = 1$. Berzsenyi showed that $G(2,k) = |4k+1|$ and asked what could be said about larger values of m. Subsequently, Stan Wagon asked whether $G(5,5) = 1$ in his Problem of the Week 805 [3]. In this article we obtain explicit formulas for $G(3,k)$ (as reported in [2]), $G(4,k)$, and $G(5,k)$.

2. Preliminaries. We first note that *a priori* there is no guarantee that $G(m,k)$ exists. In fact, for $m = 6$ and $k = -1$, we have $n^2 + n + 1$ as a common factor of both $(n+1)^6 - 1$ and $n^6 - 1$, so $\mathrm{GCD}((n+1)^6 - 1, n^6 - 1)$ grows without bound as n increases. However, if $\mathrm{GCD}((x+1)^m + k, x^m + k) = 1$ in $\mathbb{Q}[x]$, then $G(m,k)$ exists.

More generally, suppose that $f(x) \in \mathbb{Z}[x]$ with $\mathrm{GCD}(f(x+1), f(x)) = 1$ in $\mathbb{Q}[x]$. Since $\mathbb{Q}[x]$ is a Euclidean Domain there exist $p(x), q(x) \in \mathbb{Q}[x]$ such that $p(x)f(x+1) + q(x)f(x) = 1$. Clearing denominators, we obtain $a(x), b(x) \in \mathbb{Z}[x]$ and $A \in \mathbb{Z}$ such that $a(x)f(x+1) + b(x)f(x) = A$. The last equation shows that $\mathrm{GCD}(f(n+1), f(n))$ divides A, hence $\max\{\mathrm{GCD}(f(n+1), f(n)) \mid n \in \mathbb{N}\}$ exists.

We need the following lemma.

Lemma 2.1. If $f(x) \in \mathbb{Z}[x]$ and $\mathrm{GCD}(f(x+1), f(x)) = 1$ in $\mathbb{Q}[x]$, we will denote $\max\{\mathrm{GCD}(f(n+1), f(n)) \mid n \in \mathbb{N}\}$ (which exists by the argument above) by G. We have

a) If $d_1 | \mathrm{GCD}(f(n_1+1), f(n_1))$ and $d_2 | \mathrm{GCD}(f(n_2+1), f(n_2))$, then there is an $n_3 \in \mathbb{N}$ such that $\mathrm{LCM}(d_1, d_2) | \mathrm{GCD}(f(n_3+1), f(n_3))$.

b) If $d | \mathrm{GCD}(f(n+1), f(n))$ for some $n \in \mathbb{N}$, then $d | G$.

c) $\mathrm{GCD}(f(n+G+1), f(n+G)) = \mathrm{GCD}(f(n+1), f(n))$.

Proof.

a) We have $f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \dots$, where $\frac{f^{(i)}(x)}{i!} \in \mathbb{Z}[x]$. If $d|f(n+1)$ and $d|f(n)$, then for all $u \in \mathbb{Z}$, $f(n+ud+1) = f(n+1) + f'(n+1)ud + \dots$ is a multiple of d as is $f(n+ud) = f(n) + f'(n)ud + \dots$. Let $a = \mathrm{GCD}(d_1, d_2)$ and $d_2 = ab$. By the argument above, $f(n_1 + sd_1 + 1)$ and $f(n_1+sd_1)$ are both multiples of d_1 for all $s \in \mathbb{Z}$ and $f(n_2+tb+1)$ and $f(n_2+tb)$ are both multiples of b for all $t \in \mathbb{Z}$. But since d_1 and b are relatively prime, we can find $s, t \in \mathbb{N}$ such that $tb - sd_1 = n_1 - n_2$ (we can force s and t in $\mathbb{N}$ by replacing t by $t + d_1y$ and s by $s + by$ for y sufficiently large). Letting $n_3 = n_1 + sd_1 = n_2 + tb$, we have both d_1 and b as factors of both $f(n_3+1)$ and $f(n_3)$. Since d_1 and b are relatively prime, $d_1b = \mathrm{LCM}(d_1, d_2)$ is also a factor of both $f(n_3+1)$ and $f(n_3)$.

b) There is some $N \in \mathbb{N}$ such that $\mathrm{GCD}(f(N+1), f(N)) = G$. Applying the result from part a) with $d_1 = d, n_1 = n, d_2 = G, n_2 = N$ we have

$$\mathrm{LCM}(d, G)|\mathrm{GCD}(f(n_3+1), f(n_3)) \leq G.$$

But this implies that $\mathrm{LCM}(d, G) = G$ and hence, $d|G$.

c) If $d|f(n+1)$ and $d|f(n)$, then by the result from part b), $d|G$ so $G = dt$. Using the argument from part b), $d|f(n+dt+1) = f(n+G+1)$ and $d|f(n+dt) = f(n+G)$. Similarly, if $d|f(n+G+1)$ and $d|f(n+G)$, then $d|G$ and $d|f(n+G-dt+1) = f(n+1)$ and $d|f(n+G-dt) = f(n)$.

Note that part c) of the lemma shows that $\mathrm{GCD}(f(x+1), f(x))$ is periodic with period G. Consequently, we may replace $\mathbb{N}$ by $\mathbb{Z}$ in the definition of $G(m,k)$ (or more generally, G).

3. $\mathbf{G(3,k)}$.

Theorem 3.1.

$$G(3,k) = \begin{cases} 27k^2+1 & \text{if } k \equiv 0 \mod 2 \\ (27k^2+1)/4 & \text{if } k \equiv 1 \mod 2. \end{cases}$$

Proof.

Case 1: $k = 2j$. Let $D = 27k^2 + 1$. If we take

$$a(n,k) = 6n^2 - (9k+3)n + 9k + 1 \text{ and}$$

$$b(n,k) = 6n^2 - (9k-15)n - 18k + 10,$$

then

$$a(n,k)((n+1)^3 + k) - b(n,k)(n^3 + k) = 27k^2 + 1.$$

Hence, $G(3,k)|D$.

If we choose $n = 54j^2(6j+1)$, then

$$(n+1)^3 + k$$

$$= (108j^2+1)(314928j^7 + 157464j^6 + 23328j^5 + 2916j^4 + 756j^3 + 54j^2 + 2j + 1)$$

and

$$n^3 + k = (108j^2+1)(2j)(157464j^6 + 78732j^5 + 11664j^4 - 108j^2 + 1).$$

But $108j^2 + 1 = 27k^2 + 1 = D$, so $G(3,k)|D$ by part b) of Lemma 2.1. Therefore, $G(3,k) = D$.

Case 2: $k = 2j+1$. Let

$$a(n,j) = n^4 + (j+1)n^3 + 3n^2 - (7j+5)n + (2j^2 + 12j + 6) \text{ and}$$

$$b(n,j) = n^4 + (j+4)n^3 + (3j+9)n^2 - (4j-8)n + (2j^2 - 14j - 2).$$

Note that

$$a(n,j)((n+1)^3 + k) - b(n,j)(n^3 + k) = 54j^2 + 54j + 14.$$

But

$$\begin{aligned} a(n,j) &= n^4 + (j+1)n^3 + 3n^2 - (7j+5)n + (2j^2 + 12j + 6) \\ &\equiv n + (j+1)n + n + (j+1)n + 0 \equiv 0 \mod 2 \end{aligned}$$

and

$$\begin{aligned} b(n,j) &= n^4 + (j+4)n^3 + (3j+9)n^2 - (4j-8)n + (2j^2 - 14j - 2) \\ &\equiv n + jn + (j+1)n + 0 + 0 \equiv 0 \mod 2. \end{aligned}$$

Therefore, $a(n,j)/2$ and $b(n,j)/2$ are both integers and

$$(a(n,j)/2)((n+1)^3+k) - (b(n,j)/2)(n^3+k) = 27j^2+27j+7 = (27k^2+1)/4 = D/4.$$

Hence, $G(3,k)|(D/4)$.

Choose $n = -3j-2$. Then

$$(n+1)^3 + k = -j(27j^2+27j+7) \text{ and } n^3 + k = -(j+1)(27j^2+27j+7),$$

so $(D/4)|G(3,k)$ by part b) of Lemma 2.1. Therefore, $G(3,k) = D/4$.

4. $\mathbf{G(4,k)}$.

Theorem 4.1.

$$G(4,k) = \frac{p_1^{\alpha_1} \dots p_r^{\alpha_r} |16k+1|}{5^{\epsilon(k)}}, \text{where } \epsilon(k) = \begin{cases} 1 & \text{if } k \equiv 4 \mod 5 \\ 0 & \text{otherwise} \end{cases}$$

and the prime factorization of $|4k-1|$ is $p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}$ with $p_i \equiv 1 \mod 4$ and $q_i \equiv 3 \mod 4$.

Proof. Letting

$$a(n,k) = 20n^3 - 10n^2 - (16k-4)n + (24k-1) \text{ and}$$

$$b(n,k) = 20n^3 + 70n^2 - (16k-84)n - (40k-35)$$

we have

$$a(n,k)((n+1)^4+k) - b(n,k)(n^4+k) = (4k-1)(16k+1),$$

so $G(4,k)|(4k-1)(16k+1)$.

If $n = 8k$, then

$$(n+1)^4 + k = (16k+1)(256k^3 + 112k^2 + 17k + 1) \text{ and}$$

$$n^4 + k = (16k+1)(256k^3 - 16k^2 + k),$$

so by part b) of Lemma 2.1 $(16k+1)|G(4,k)$.

Let $|4k-1| = p_1^{\alpha_1} \dots p_r^{\alpha_r} q_1^{\beta_1} \dots q_s^{\beta_s}$ be the prime factorization of $|4k-1|$ with $p_i \equiv 1 \mod 4$ and $q_i \equiv 3 \mod 4$. For a given p_i, since $p_i \equiv 1 \mod 4$ we can find a λ_i such that $\lambda_i^2 \equiv -1 \mod p_i^{\alpha_i}$ and since p_i is odd we can find a μ_i such that $2\mu_i \equiv 1 \mod p_i^{\alpha_i}$. Note that we also have $4k \equiv 1 \mod p_i^{\alpha_i}$. If $n = \mu_i(\lambda_i - 1)$, then

$$2^4((n+1)^4 + k) = (2\mu_i(\lambda_i - 1) + 2)^4 + 16k \equiv (\lambda_i + 1)^4 + 4$$

$$\begin{aligned} &= \lambda_i^4 + 4\lambda_i^3 + 6\lambda_i^2 + 4\lambda_i + 1 + 4 \\ &\equiv 1 - 4\lambda_i - 6 + 4\lambda_i + 1 + 4 \equiv 0 \mod p_i^{\alpha_i}. \end{aligned}$$

Similarly,

$$2^4(n^4 + k) = (2\mu_i(\lambda_i - 1))^4 + 16k \equiv (\lambda_i - 1)^4 + 4$$

$$\begin{aligned} &= \lambda_i^4 - 4\lambda_i^3 + 6\lambda_i^2 - 4\lambda_i + 1 + 4 \\ &\equiv 1 + 4\lambda_i - 6 - 4\lambda_i + 1 + 4 \equiv 0 \mod p_i^{\alpha_i}. \end{aligned}$$

By part b) of Lemma 2.1, $p_i^{\alpha_i}|G(4,k)$.

Using part a) and b) of Lemma 2.1 and the results above, $\text{LCM}(16k + 1, p_1^{\alpha_1} \dots p_r^{\alpha_r})$ divides $G(4,k)$. If $k \not\equiv 4 \mod 5$, then $4k-1$ and $16k+1$ are relatively prime and hence, $\text{LCM}(p_1^{\alpha_1} \dots p_r^{\alpha_r}, 16k+1) = p_1^{\alpha_1} \dots p_r^{\alpha_r}(16k+1)$. If $k \equiv 4 \mod 5$, then $\text{GCD}(4k-1, 16k+1) = 5$ and hence, one of the $p_i = 5$, so $\text{LCM}(p_1^{\alpha_1} \dots p_r^{\alpha_r}, 16k+1) = p_1^{\alpha_1} \dots p_r^{\alpha_r}(16k+1)/5$.

To finish the proof, we must show that none of the q_i are factors of $G(4,k)$ and that when $k \equiv 4 \mod 5$, 5 cannot appear to a higher power than already exhibited. To prove the former, consider the equation

$$(2n+5)(n^4 + k) - (2n-3)((n+1)^4 + k) = 10n^2 + 10n + 8k + 3. \qquad (1)$$

If q_i were a factor of $G(4,k)$, we would have $10n^2+10n+8k+3 \equiv 0 \mod q_i$. Since q_i is a factor of $4k-1$, we have $4k \equiv 1 \mod q_i$. Therefore,

$$10n^2+10n+8k+3 \equiv 10n^2+10n+2+3 \equiv 5(2n^2+2n+1) \equiv 0 \mod q_i.$$

Since $q_i \equiv 3 \mod 4$ and $\mathrm{GCD}(5,q_i)=1$, it follows that $2n^2+2n+1 \equiv 0 \mod q_i$. But this implies that $(2n+1)^2 \equiv -1 \mod q_i$ which is impossible since $q_i \equiv 3 \mod 4$.

If $k \equiv 4 \mod 5$, we must show that if $4k-1 = u5^i$ and $16k+1 = v5^j$, where u and v are not divisible by 5, then 5^{i+j} does not divide $G(4,k)$. Suppose that it did. Since we've seen above that $(16k+1)|G(4,k)$, we'd have $5^i(16k+1)|G(4,k)$. Note that since $k \equiv 4 \mod 5$ we have $i > 0$ and $j > 0$. The equation

$$(2n^2-2n+1)((n+1)^4+k)-(2n^2+6n+5)(n^4+k) = (4k-1)(2n+1)$$

shows that we would have $(4k-1)(2n+1) \equiv 0 \mod 5^i(16k+1)$. This implies that $u(2n+1) \equiv 0 \mod (16k+1)$, and since u is relatively prime to $16k+1$, $(2n+1) \equiv 0 \mod (16k+1)$. Hence, $n \equiv 8k \mod (16k+1)$, so $n = 8k+(16k+1)t$. Now Equation (1) shows that $10n^2+10n+8k+3 \equiv 0 \mod 5^i(16k+1)$. However, this yields

$$\begin{aligned}10n^2+10n+8k+3 &= 10(8k+(16k+1)t)^2+10(8k+(16k+1)t)+8k+3\\ &= (16k+1)(10(16k+1)t^2+10(16k+1)t+40k+3)\\ &\equiv 0 \mod 5^i(16k+1),\end{aligned}$$

which implies that

$$10(16k+1)t^2+10(16k+1)t+40k+3 \equiv 0 \mod 5^i.$$

But this is a contradiction since the left-hand side is congruent to $3 \mod 5$.

5. $\mathbf{G(5,k)}$.

Theorem 5.1.

$$G(5,k) = \begin{cases} (3125k^4+625k^2+1)/11 & \text{if } k \equiv \pm 1 \mod 11 \\ 3125k^4+625k^2+1 & \text{otherwise} \end{cases}$$

Proof. Denote $3125k^4 + 625k^2 + 1$ by D.

Case 1: If $k \not\equiv \pm 1 \mod 11$, then $D \not\equiv 0 \mod 11$. Let

$$a(n,k) = (1250k^2 + 70)n^4 - (625k^2 + 275k + 35)n^3 - (125k^2 - 275k - 15)n^2$$
$$- (625k^3 - 500k^2 + 200k + 5)n + 1250k^3 - 375k^2 + 125k + 1$$

and

$$b(n,k) = (1250k^2 + 70)n^4 + (5625k^2 - 275k + 315)n^3$$
$$+ (9250k^2 - 1100k + 540)n^2 - (625k^3 - 6125k^2 + 1575k - 420)n$$
$$- 1875k^3 + 875k^2 - 875k + 126.$$

Then

$$a(n,k)((n+1)^5 + k) - b(n,k)(n^5 + k) = D, \tag{2}$$

and consequently $G(5,k)|D$.

On the other hand, since D is always odd and in this case $D \not\equiv 0 \mod 11$, there is a positive integer λ such that $-22\lambda \equiv 1 \mod D$. Let $n = \lambda(625k^3 + 90k + 11)$. We have

$$-22^5((n+1)^5 + k) = (-22\lambda(625k^3 + 90k + 11) - 22)^5 - 22^5 k$$
$$\equiv ((625k^3 + 90k + 11) - 22)^5 - 22^5 k \equiv 0 \mod D.$$

The last congruence is demonstrated by explicitly factoring the polynomial $(625k^3 + 90k - 11)^5 - 22^5 k$ using a computer algebra system such as *Mathematica.* Since 22 is relatively prime to D, we conclude that $(n+1)^5 + k \equiv 0 \mod D$. A similar argument shows that $n^5 + k \equiv 0 \mod D$, so by Lemma 2.1 $D|G(5,k)$ and hence, $G(5,k) = D$.

Case 2: If $k \equiv \pm 1 \mod 11$, one can check that $a(n,k)$ and $b(n,k)$ are both divisible by 11, so by Equation (2) $G(5,k)|(D/11)$. One can also check that D is divisible by 121. Denoting $D/121$ by R, we wish to show that $(11R)|G(5,k)$. Note that since R is odd, there is a positive integer λ such that $-2\lambda \equiv 1 \mod R$.

We are reduced to considering subcases:

Case 2a: If $k = 11\ell + 1$ with $\ell \not\equiv 3, 9 \mod 11$, then $R \not\equiv 0 \mod 11$. By the Chinese Remainder Theorem, we can find an n such that

$$\begin{aligned} &n \equiv \lambda(75625\ell^3 + 20625\ell^2 + 1965\ell + 66) \mod R \\ &\quad \text{and} \\ &n \equiv 6 \mod 11. \end{aligned}$$

We have

$$\begin{aligned} -2^5((n+1)^5 + k) &= (-2\lambda(75625\ell^3 + 20625\ell^2 + 1965\ell + 66) - 2)^5 - 2^5(11\ell + 1) \\ &\equiv (75625\ell^3 + 20625\ell^2 + 1965\ell + 66 - 2)^5 - 2^5(11\ell + 1) \\ &\equiv 0 \mod R, \end{aligned}$$

where as before the latter congruence is shown by explicit factorization. Since $(n+1)^5 + k \equiv (6+1)^5 + 1 \equiv 0 \mod 11$, we have $(n+1)^5 + k \equiv 0 \mod 11R$. A similar argument shows that $n^5 + k \equiv 0 \mod 11R$, therefore $(D/11)|G(5,k)$.

For the remaining cases, we provide the appropriate choice of n and leave it to the reader (and a suitable computer algebra system) to verify the results.

Case 2b: If $k = 11\ell - 1$ with $\ell \not\equiv 2, 8 \mod 11$, then $R \not\equiv 0 \mod 11$ and we can find an n such that

$$\begin{aligned} &n \equiv \lambda(75625\ell^3 - 20625\ell^2 + 1965\ell - 64) \mod R \\ &\quad \text{and} \\ &n \equiv 3 \mod 11. \end{aligned}$$

Case 3: Let

$$P = 75625\ell^3 + 20625\ell^2 + 1965\ell + 66 \text{ and}$$

$$Q = 75625\ell^3 - 20625\ell^2 + 1965\ell - 64.$$

If $k = 11\ell + 1$ and $\ell \equiv 3 \mod 11$, take $n = \lambda P + R$.
If $k = 11\ell + 1$ and $\ell \equiv 9 \mod 11$, take $n = \lambda P + 10R$.
If $k = 11\ell - 1$ and $\ell \equiv 2 \mod 11$, take $n = \lambda Q + R$.
If $k = 11\ell - 1$ and $\ell \equiv 8 \mod 11$, take $n = \lambda Q + 10R$.

In each case, a calculation shows that $(11R)|\mathrm{GCD}((n+1)^5 + k, n^5 + k)$ and hence, $(D/11)|G(5, k)$.

6. Conclusion. We have computed $G(3, k), G(4, k)$, and $G(5, k)$. Preliminary calculations indicate that there are similar, albeit more complicated, formulas for $G(6, k)$ and $G(7, k)$, the nature of the formulas depending on the parity of m.

In [1], Berzsenyi also asks to find m and k such that $G(m, k) = 1$. The author recklessly conjectures that $G(m, k) = 1$ if and only if $k = 0$, but currently has no proof of this claim.

An additional question is to find m and k such that $G(m, k)$ exists. In Section 2, we saw that $G(m, k)$ does not exist when $m = 6$ and $k = -1$. It is not difficult to show that $G(m, k)$ does not exist if m is a multiple of 6 and $k = -1$, but the author is unaware if there are any other cases.

Finally, we return to Wagon's problem. From the results of Section 5, we see that $G(5, 5) = 3125(5)^4 + 625(5)^2 + 1 = 1968751$, not 1, but the first n for which $\mathrm{GCD}((n + 1)^5 + 5, n^5 + 5) > 1$ is when $n = 533360$. This is a good example to illustrate that just because a result is true for a large number of examples, it is not necessarily true in general.

References

1. G. Berzsenyi, “Maximizing the Greatest,” *Quantum,* 3 (May/June 1995), 39.
2. G. Berzsenyi, “Lost in a Forest,” *Quantum,* 6 (November/December 1995), 41.
3. S. Wagon, “Problem of the Week 805, “True or False?”, http://mathforum.org/wagon/spring96/p805.html.

Les Reid
Department of Mathematics
Southwest Missouri State University
Springfield, MO 65804
email: les@math.smsu.edu