Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 24, 2018, No. 2, 28–31
DOI: 10.7546/nntdm.2018.24.2.28-31

A GCD problem and a Hessenberg determinant

M. Hariprasad

Department of Computational and Data Sciences
Indian Institute of Science, Bangalore-560012, India
e-mail: mhariprasadkansur@gmail.com

Received: 31 December 2016 Accepted: 7 May 2018

Abstract: In this article we give a proof that, when two integers a and b are coprime ($(a, b) = 1$ i.e. greatest common divisor (GCD) of a and b is 1), then GCD of $a + b$ and $\frac{a^p+b^p}{a+b}$ is either 1 or p for a prime number p. We prove this by linking the problem to a certain type of Hessenberg determinants.
Keywords: Greatest common divisor, Binomial coefficients, Hessenberg determinants.
2010 Mathematics Subject Classification: 11A05, 15B36, 11C20.

1 Introduction

For integers a and b let (a, b) denote the greatest common divisor (GCD). The book [1] has an exercise: If $(a, b) = 1$ then prove that $(a + b, a^2 - ab + b^2)$ is either 1 or 3. Here we prove a generalized version of this problem by linking it to linear algebra. We prove that if $(a, b) = 1$, then $(a + b, \frac{a^p+b^p}{a+b})$ is either 1 or factors of p when p is an odd number. When p is a prime number, then $(a + b, \frac{a^p+b^p}{a+b})$ is either 1 or p.

2 Results

Lemma 2.1. *If $(a, b) = 1$, and some $d > 1$ is such that $d|(a + b)$ then $d \nmid a$ and $d \nmid b$.*

Proof. Suppose $d|a$ then $d|(a+b-a)$, which is $d|(b)$. But $(a, b) = 1$ and $d > 1$. By contradiction d will not divide a. Similarly for b. $\square$

Lemma 2.2. *For an odd integer* p*,*

$$\sum_{n=1}^{(p-1)/2} (-1)^{n-1}(p-2n)\binom{p}{n} = p.$$

Proof. For a real $x > 0$, consider $(x - \frac{1}{x})^p$. By expanding this with binomial theorem we get

$$\left(x - \frac{1}{x}\right)^p = \sum_{n=0}^{p}(-1)^n\binom{p}{n}x^{p-n}\left(\frac{1}{x}\right)^n, \tag{1}$$

$$\left(x - \frac{1}{x}\right)^p = \sum_{n=0}^{p}(-1)^n\binom{p}{n}x^{p-2n}. \tag{2}$$

Differentiating equation 1 with respect to x,

$$p\left(x - \frac{1}{x}\right)^{p-1}\left(1 + \frac{1}{x^2}\right) = \sum_{n=0}^{p}(-1)^n\binom{p}{n}(p-2n)x^{p-2n-1}. \tag{3}$$

Substitute $x = 1$ in equation 3, we get

$$0 = 2\left(\sum_{n=0}^{(p-1)/2}(-1)^n\binom{p}{n}(p-2n)\right), \tag{4}$$

$$p = \sum_{n=1}^{(p-1)/2}(-1)^{n-1}\binom{p}{n}(p-2n). \tag{5}$$

□

Consider the lower Hessenberg matrices,

$$H_n = \begin{bmatrix} \binom{2n+1}{1} & 1 & 0 & 0 & \cdots & 0 \\ \binom{2n+1}{2} & \binom{2n-1}{1} & 1 & 0 & \cdots & 0 \\ \binom{2n+1}{3} & \binom{2n-1}{2} & \binom{2n-3}{1} & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \ddots & \ddots & 0 \\ \binom{2n+1}{n-1} & \binom{2n-1}{n-2} & \binom{2n-3}{n-3} & \cdots & 5 & 1 \\ \binom{2n+1}{n} & \binom{2n-1}{n-1} & \binom{2n-3}{n-2} & \cdots & 10 & 3 \end{bmatrix}.$$

With $H_0 = 1$ and $H_1 = \begin{bmatrix} 3 \end{bmatrix}$ and $H_2 = \begin{bmatrix} 5 & 1 \\ 10 & 3 \end{bmatrix}$, etc.

Lemma 2.3. *Determinant of the matrix* H_n *is* $2n + 1$*.*

Proof. We can see $det(H_1) = 3$ and $det(H_2) = 5$. Now by using principle of strong induction and expanding the determinant along the first row of H_n we get the identity in Lemma 2.2 which proves Lemma 2.3. □

Theorem 2.4. *If* $(a, b) = 1$ *then for an odd number* $p = 2n + 1$*,* $(a + b, \frac{a^p+b^p}{a+b}) = d$*, where* d *is a divisor of* p*.*

Proof. Suppose $d|(a+b)$ and $d|\frac{a^p+b^p}{a+b}$ then we know that d divides any linear combination of $(a+b)^k$ and $\frac{a^p+b^p}{a+b}$. We prove that this linear combination can give $p(ab)^{\frac{p-1}{2}}$. Then from Lemma 2.1 we deduce $d|p$. Let us suppose a^p+b^p can be expressed in terms of $(a+b)^k$ for $k = 1,3,5,\cdots p$. So

$$a^p + b^p = \sum_{k=0}^{(p-1)/2} C_k (a+b)^{2k+1} a^{\frac{p-1}{2}-k} b^{\frac{p-1}{2}-k} \tag{6}$$

The equation 6 represents the linear combination of different powers of $(a+b)$. If we write this equation into the matrix form by considering as the first row as coefficient of a^p, second row as coefficients of $a^{p-1}b$, similarly k^{th} row as coefficients of $a^{p-k}b^k$ and row $(p+1)$ having coefficients for b^p. We get the system,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{2} & \binom{2n-1}{1} & 1 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{3} & \binom{2n-1}{2} & \binom{2n-3}{1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \ddots & \ddots & 0 & 0 \\ \binom{2n+1}{n-1} & \binom{2n-1}{n-2} & \binom{2n-3}{n-3} & \binom{2n-5}{n-4} & \cdots & 1 & 0 \\ \binom{2n+1}{n} & \binom{2n-1}{n-1} & \binom{2n-3}{n-2} & \binom{2n-5}{n-3} & \cdots & 3 & 1 \\ \binom{2n+1}{n} & \binom{2n-1}{n-1} & \binom{2n-3}{n-2} & \binom{2n-5}{n-3} & \cdots & 3 & 1 \\ \binom{2n+1}{n-1} & \binom{2n-1}{n-2} & \binom{2n-3}{n-3} & \binom{2n-5}{n-4} & \cdots & 1 & 0 \\ \vdots & \vdots & \cdots & \iddots & \iddots & 0 & 0 \\ \binom{2n+1}{3} & \binom{2n-1}{2} & \binom{2n-3}{1} & 1 & \cdots & 0 & 0 \\ \binom{2n+1}{2} & \binom{2n-1}{1} & 1 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ \vdots \\ c_{(p-1)/2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{7}$$

Now because of the symmetry in binomial coefficients we can consider only the upper part of the matrix,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{1} & 1 & 0 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{2} & \binom{2n-1}{1} & 1 & 0 & \cdots & 0 & 0 \\ \binom{2n+1}{3} & \binom{2n-1}{2} & \binom{2n-3}{1} & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \cdots & \ddots & \ddots & 0 & 0 \\ \binom{2n+1}{n-1} & \binom{2n-1}{n-2} & \binom{2n-3}{n-3} & \binom{2n-5}{n-4} & \cdots & 1 & 0 \\ \binom{2n+1}{n} & \binom{2n-1}{n-1} & \binom{2n-3}{n-2} & \binom{2n-5}{n-3} & \cdots & 3 & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ \vdots \\ c_{\frac{p-1}{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \end{bmatrix} \tag{8}$$

The equation (8) can be written as

$$Lx = b \tag{9}$$

We need to find the $c_{\frac{p-1}{2}}$ which is the $((p+1)/2, 1)$ element in the matrix L^{-1}. Note that determinant of L is 1.

And $(-1)^{(p-1)/2}det(H_{(p-1)/2})$ is the corresponding $((p+1)/2, 1)$ entry of L^{-1}. This is the determinant obtained by removing the first row and last column of the matrix L. From Lemma 2.3 it is nothing but $\pm p$.

Then from equation (6) we get

$$p(ab)^{\frac{p-1}{2}} = \pm \left(\frac{a^p + b^p}{a+b} - \sum_{k=0}^{((p-1)/2)-1} C_k (a+b)^{2k} \right), \tag{10}$$

d divides RHS of equation (10), so it divides LHS, which proves the theorem. □

References

[1] Apostol, T. M. (2013) *Introduction to Analytic Number Theory*, Springer Science & Business Media.