#A41 INTEGERS 16 (2016)

ON THE RELATIONSHIP BETWEEN THE NUMBER OF SOLUTIONS OF CONGRUENCE SYSTEMS AND THE RESULTANT OF TWO POLYNOMIALS

Dmitry I. Khomovsky
Lomonosov Moscow State University, Moscow, RF
khomovskij@physics.msu.ru

Received: 9/1/15, Revised: 12/31/15, Accepted: 5/31/16, Published: 6/10/16

Abstract

Let q be an odd prime and $f(x)$, $g(x)$ be polynomials with integer coefficients. If the system of congruences $f(x) \equiv g(x) \equiv 0 \pmod{q}$ has ℓ solutions, then $R(f(x), g(x)) \equiv 0 \pmod{q^\ell}$, where $R(f(x), g(x))$ is the resultant of the polynomials. Using this result we give new proofs of some known congruences involving the Lucas sequences.

1. Introduction

The resultant $R(f,g)$ of two polynomials $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ of degrees n and m, respectively, with coefficients in a field F is defined by the determinant of the $(m+n) \times (m+n)$ Sylvester matrix [10]

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & & & & \\ & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 & & & \\ & & \cdots & & & & & & & \\ & & & a_n & a_{n-1} & \cdots & \cdots & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & \cdots & b_0 & & & & \\ & b_m & b_{m-1} & \cdots & \cdots & b_0 & & & \\ & & \cdots & & & & & & \\ & & & \cdots & & & & & \\ & & & & b_m & b_{m-1} & \cdots & \cdots & b_0 \end{vmatrix}. \quad (1)$$

Let f, g, h and v be the polynomials below. Some important properties of the resultant are:

(*i*) If $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$ and $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$, then

$$R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_m^n \prod_{i=1}^{m} f(\beta_i) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j),$$

where α_i and β_j are the roots of $f(x)$ and $g(x)$, respectively, in some extension of F, each repeated according to its multiplicity. This property is often taken as the definition of the resultant.

(*ii*) f and g have a common root in some extension of F if and only if $R(f,g)=0$.

(*iii*) $R(f,g)=(-1)^{nm}R(g,f)$.

(*iv*) $R(fh,g)=R(f,g)\,R(h,g)$ and $R(f,gh)=R(f,g)\,R(f,h)$.

(*v*) If $g=vf+h$ and $\deg(h)=d$, then $R(f,g)=a_n^{m-d}R(f,h)$.

(*vi*) If p is a positive integer, then $R(f(x^p),g(x^p))=R(f(x),g(x))^p$.

All these properties are well-known [1, 7]. More details concerning the resultant can be found in [3, 4]. Another important classical result is (see [4]):

Lemma 1. *Let* $f=\sum_{i=0}^{n}a_ix^i$ *and* $g=\sum_{j=0}^{m}b_jx^j$ *be two polynomials of degrees* n *and* m*, respectively. Let, for* $k\geq 0$, $r_k(x)=r_{k,n-1}x^{n-1}+\cdots+r_{k,0}$ *be the remainder of* $x^kg(x)$ *modulo* $f(x)$*, i.e.,* $x^kg(x)=v_k(x)f(x)+r_k(x)$*, where* v_k *is some polynomial and* $\deg(r_k)\leq n-1$*. Then*

$$R(f,g)=a_n^m\begin{vmatrix} r_{n-1,n-1} & r_{n-1,n-2} & \cdots & r_{n-1,0}\\ r_{n-2,n-1} & r_{n-2,n-2} & \cdots & r_{n-2,0}\\ \vdots & & & \vdots\\ r_{0,n-1} & r_{0,n-2} & \cdots & r_{0,0}\end{vmatrix}. \tag{2}$$

In the next section we prove a theorem on the relationship between the number of solutions of the congruence system $f(x)\equiv g(x)\equiv 0 \pmod q$ and the resultant of two polynomials $R(f(x),g(x))$. Then using this result we give new proofs of some congruences involving the Lucas sequences.

2. Properties of the Resultant

A polynomial $f(x)$ with integer coefficients is called *not identically zero in* $\mathbb{Z}_q$ if at least one of its coefficients is not divisible by q. Let $A=(a_{i,j})$ be an arbitrary matrix. Then by $A^{<q>}$ we will denote the matrix $\left(a'_{i,j}\right)$ over $\mathbb{Z}_q$ of the same type such that $a'_{i,j}$ is the residue of $a_{i,j}$ modulo q.

Theorem 1. *Let* q *be a prime and* $f(x)$, $g(x)$ *be polynomials with integer coefficients that are not identically zero in* $\mathbb{Z}_q$*. If the system of congruences* $f(x)\equiv 0 \pmod q$ *and* $g(x)\equiv 0 \pmod q$ *has* ℓ *solutions, then* $R(f(x),g(x))\equiv 0 \pmod{q^\ell}$.

Proof. Let $\deg f = n$ and $\deg g = m$. Then we have that the system $f(x) \equiv g(x) \equiv 0 \pmod{q}$ has ℓ solutions by the theorem conditions and $\ell \leq \min[n, m]$ as the polynomials are not identically zero in $\mathbb{Z}_q$. Let $r_k(x) = r_{k,n-1}x^{n-1} + \cdots + r_{k,0}$ be the remainder of $x^k g(x)$ modulo $f(x)$, i.e., $x^k g(x) = v_k(x)f(x) + r_k(x)$, where $v_k(x)$ is some polynomial and $\deg(r_k) \leq n - 1$. Then we get the system of congruences

$$\begin{pmatrix} r_{n-1,n-1} & r_{n-1,n-2} & \cdots & r_{n-1,0} \\ r_{n-2,n-1} & r_{n-2,n-2} & \cdots & r_{n-2,0} \\ \vdots & & & \vdots \\ r_{0,n-1} & r_{0,n-2} & \cdots & r_{0,0} \end{pmatrix} \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \vdots \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{q}. \tag{3}$$

This system has at least ℓ solutions, since each congruence of (3) is derived from $f(x) \equiv 0 \pmod{q}$ and $g(x) \equiv 0 \pmod{q}$. Let $A = (a_{i,j})$ be a matrix of the system (3). With the help of the procedure analogous to row reduction using operations of swapping the rows and adding a multiple of one row to another row, we can reduce A to a matrix A_1 with integer coefficients such that $\det(A) = \pm \det(A_1)$ and $A_1^{<q>}$ is an upper triangular matrix. We can see that each solution of the system (3) is also a solution of the following system over $\mathbb{Z}_q$:

$$\left(A_1^{<q>}\right) \begin{pmatrix} x^{n-1} \\ x^{n-2} \\ \vdots \\ 1 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{q}, \tag{4}$$

so (4) has at least ℓ solutions. Note that the last ℓ congruences of (4) have degrees less than ℓ. On the other hand, these congruences have at least ℓ solutions. Hence all these congruences must be congruences with zero coefficients, i.e., the last ℓ rows of $A_1^{<q>}$ are zero rows. Therefore, all elements of the last ℓ rows of A_1 are divisible by q, so $\det(A) = \pm \det(A_1)$ is divisible by q^ℓ. Thus, by Lemma 1 we have $R(f, g) \equiv 0 \pmod{q^\ell}$. □

Remark. If one or both polynomials equal zero in $\mathbb{Z}_q$, then by property (i) we obtain that either $R(f, g) \equiv 0 \pmod{q^n}$ or $R(f, g) \equiv 0 \pmod{q^m}$. We do not consider this trivial case in Theorem 1.

Example. Let $f(x) = x^6 + 1$, $g(x) = (x + 1)^6 + 1$. The system of congruences $x^6 + 1 \equiv 0 \pmod{13}$ and $(x + 1)^6 + 1 \equiv 0 \pmod{13}$ has three solution in $\mathbb{Z}_{13}$: $x = 5, 6, 7$. The matrix of the system (3) for these polynomials is:

$$A = \begin{pmatrix} 1 & -6 & -15 & -20 & -15 & -6 \\ 6 & 1 & -6 & -15 & -20 & -15 \\ 15 & 6 & 1 & -6 & -15 & -20 \\ 20 & 15 & 6 & 1 & -6 & -15 \\ 15 & 20 & 15 & 6 & 1 & -6 \\ 6 & 15 & 20 & 15 & 6 & 1 \end{pmatrix}. \tag{5}$$

Since the resulting echelon form of matrices after row reduction is not unique, we obtain the reduced row echelon form of the matrix A, which is unique:

$$A_1^{<13>} = \begin{pmatrix} 1 & 7 & 11 & 6 & 11 & 7 \\ 0 & 1 & 9 & 11 & 1 & 11 \\ 0 & 0 & 1 & 8 & 3 & 11 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 7 & 4 & 8 \\ 0 & 1 & 0 & 4 & 0 & 3 \\ 0 & 0 & 1 & 8 & 3 & 11 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{6}$$

So we get $\det A \equiv 0 \pmod{13^3}$ and $R\left(x^6+1,(x+1)^6+1\right) \equiv 0 \pmod{13^3}$. This resultant is actually equal to $2^4 \times 5 \times 13^3$.

Corollary 1. *Let q be a prime and $f(x)$, $g(x)$ be polynomials of degrees n and m, respectively, with integer coefficients that are not identically zero in $\mathbb{Z}_q$. Let A be a matrix of the system* (3) *for $f(x), g(x)$. If $\operatorname{Rank} A = p$ in $\mathbb{Z}_q$, then $R(f,g) \equiv 0 \pmod{q^{n-p}}$. If the system $f(x) \equiv g(x) \equiv 0 \pmod q$ has ℓ solutions, then $n-p \geq \ell$. Moreover, if M is any $k \times k$ minor of the matrix A and $k > p$, then $M \equiv 0 \pmod{q^{k-p}}$.*

Proof. This follows from Theorem 1. □

The question about the relation of the multiplicity of q as a factor of $R(f,g)$ and the degree of common factor of the polynomials f and g modulo q was studied in [2]. This question is closely related to Theorem 1 and first appeared in [5].

3. The Congruences Involving the Terms of the Lucas Sequences

Theorem 2. *Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial of degree n with integer coefficients and q be an odd prime. Let $a_0 \not\equiv 0 \pmod q$ and let the congruence $f(x) \equiv 0 \pmod q$ have ℓ solutions. Then*

$$R(f(x), x^{q-1}-1) \equiv a_n^{q-1} \prod_{i=1}^{n} (\alpha_i^{q-1}-1) \equiv 0 \pmod{q^\ell}, \tag{7}$$

where α_i are the roots of $f(x)$, each repeated according to its multiplicity.

Proof. Consider $R(f(x), x^{q-1}-1)$. Since $f(x) = a_n \prod_{i=1}^{n}(x-\alpha_i)$, then

$$R\left(f(x), x^{q-1}-1\right) = a_n^{q-1} \prod_{i=1}^{n} (\alpha_i^{q-1}-1). \tag{8}$$

We know that q is an odd prime, so the congruence $x^{q-1}-1 \equiv 0 \pmod q$ has $q-1$ solutions (zero is not one of them). On the other hand, the congruence

$f(x) \equiv 0 \pmod{q}$ has ℓ nonzero solutions, as $a_0 \not\equiv 0 \pmod{q}$. Hence the system of congruences $f(x) \equiv x^{q-1} - 1 \equiv 0 \pmod{q}$ also has ℓ solutions. Then by Theorem 1 we have $R(f(x), x^{q-1} - 1) \equiv 0 \pmod{q^\ell}$. □

Theorem 3. *Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial of degree n with integer coefficients and q be an odd prime. Let $a_0 \not\equiv 0 \pmod{q}$ and let the congruence $f(x) \equiv 0 \pmod{q}$ have ℓ solutions. If b solutions of them are quadratic residues modulo q, then*

$$R(f(x), x^{\frac{q-1}{2}} - 1) \equiv a_n^{\frac{q-1}{2}} \prod_{i=1}^{n} (\alpha_i^{\frac{q-1}{2}} - 1) \equiv 0 \pmod{q^b} \tag{9}$$

and

$$R(f(x), x^{\frac{q-1}{2}} + 1) \equiv a_n^{\frac{q-1}{2}} \prod_{i=1}^{n} (\alpha_i^{\frac{q-1}{2}} + 1) \equiv 0 \pmod{q^{\ell-b}}, \tag{10}$$

where α_i are the roots of $f(x)$, each repeated according to its multiplicity.

Proof. Consider $R(f(x), x^{\frac{q-1}{2}} - 1)$. Since $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$, then

$$R\left(f(x), x^{\frac{q-1}{2}} - 1\right) = a_n^{\frac{q-1}{2}} \prod_{i=1}^{n} (\alpha_i^{\frac{q-1}{2}} - 1). \tag{11}$$

We know that $f(x) \equiv 0 \pmod{q}$ has b nonzero solutions which are quadratic residues modulo q. Hence the system of congruences $f(x) \equiv x^{\frac{q-1}{2}} - 1 \equiv 0 \pmod{q}$ has b solutions. Then by Theorem 1 we have $R(f(x), x^{q-1} - 1) \equiv 0 \pmod{q^b}$. Since $\ell - b$ solutions of $f(x) \equiv 0 \pmod{q}$ are quadratic nonresidues modulo q, then by analogy we prove that $R(f(x), x^{\frac{q-1}{2}} + 1) \equiv 0 \pmod{q^{\ell-b}}$. □

As an illustration of applications of Theorem 1 we consider the following theorem.

Theorem 4. *Let q be an odd prime and P, Q be any integers such that $Q \not\equiv 0 \pmod{q}$. If the Legendre symbol $\left(\frac{P^2-4Q}{q}\right)$ is equal to 1, then*

$$V_{q-1}(P, Q) \equiv Q^{q-1} + 1 \pmod{q^2}, \tag{12}$$

$$V^2_{\frac{q-1}{2}}(P, Q) \equiv \left(Q^{\frac{q-1}{2}} + 1\right)^2 \pmod{q^2}, \tag{13}$$

where $V_n(P, Q)$ is the n-th term of the Lucas sequence defined by the recurrence relation

$$V_0 = 2,\ \ V_1 = P,\ \ V_i = PV_{i-1} - QV_{i-2},\ \ i \geq 2. \tag{14}$$

Proof. The roots of $x^2 - Px + Q$ are $\alpha_1 = \frac{P-\sqrt{P^2-4Q}}{2}$, $\alpha_2 = \frac{P+\sqrt{P^2-4Q}}{2}$. Hence $R(x^2 - Px + Q, x^{q-1} - 1) = (\alpha_1\alpha_2)^{q-1} - (\alpha_1^{q-1} + \alpha_2^{q-1}) + 1 = 1 + Q^{q-1} - V_{q-1}(P, Q)$.

Since we know $\left(\frac{P^2-4Q}{q}\right) = 1$ and $Q \not\equiv 0 \pmod{q}$, then the system of congruences $x^2 - Px + Q \equiv x^{q-1} - 1 \equiv 0 \pmod{q}$ has two solutions. So by Theorem 1 we have $1 + Q^{q-1} - V_{q-1}(P,Q) \equiv 0 \pmod{q^2}$, thus we get (12). Now using the identity $V_{2n}(P,Q) = V_n^2(P,Q) - 2Q^n$, we obtain (13). □

Note that the congruences (12) and (13) are well-known [6, 8, 9], but here we give an alternative completely independent proof of these results.

Corollary 2. *Let q be an odd prime and k, P, Q be any integers such that $k^2 + Pk + Q \not\equiv 0 \pmod{q}$. If $\left(\frac{P^2-4Q}{q}\right) = 1$, then*

$$V_{q-1}(P+2k, k^2+Pk+Q) \equiv (k^2+Pk+Q)^{q-1} + 1 \pmod{q^2}, \tag{15}$$

$$V^2_{\frac{q-1}{2}}(P+2k, k^2+Pk+Q) \equiv \left((k^2+Pk+Q)^{\frac{q-1}{2}} + 1\right)^2 \pmod{q^2}. \tag{16}$$

Proof. Since $(P+2k)^2 - 4(k^2+Pk+Q) = P^2 - 4Q$, this corollary follows from Theorem 4. □

3.1. The Congruences Involving the Lucas Numbers

Let $P = 1$, $Q = -1$ and $\left(\frac{5}{q}\right) = 1$, i.e., by the Quadratic Reciprocity Law $q \equiv \pm 1 \pmod{5}$. Let an integer k satisfy $k^2 + k - 1 \not\equiv 0 \pmod{q}$, then by Corollary 2

$$V_{q-1}(1+2k, k^2+k-1) \equiv (k^2+k-1)^{q-1} + 1 \pmod{q^2}, \tag{17}$$

$$V^2_{\frac{q-1}{2}}(1+2k, k^2+k-1) \equiv (k^2+k-1)^{q-1} + 2(k^2+k-1)^{\frac{q-1}{2}} + 1 \pmod{q^2}. \tag{18}$$

If $k = 0$, then

$$L_{q-1} \equiv 2 \pmod{q^2}, \tag{19}$$

$$L^2_{\frac{q-1}{2}} \equiv 2 + 2(-1)^{\frac{q-1}{2}} \pmod{q^2}, \tag{20}$$

where L_n is the n-th Lucas number.

3.2. The Congruences Involving the Pell-Lucas Numbers

Let $P = 2$, $Q = -1$ and $\left(\frac{8}{q}\right) = 1$, i.e., by the Quadratic Reciprocity Law $q \equiv \pm 1 \pmod{8}$. Let an integer k satisfy $k^2 + 2k - 1 \not\equiv 0 \pmod{q}$, then by Corollary 2

$$V_{q-1}(2+2k, k^2+2k-1) \equiv (k^2+2k-1)^{q-1} + 1 \pmod{q^2}, \tag{21}$$

$$V^2_{\frac{q-1}{2}}(2+2k, k^2+2k-1) \equiv (k^2+2k-1)^{q-1} + 2(k^2+2k-1)^{\frac{q-1}{2}} + 1 \pmod{q^2}. \tag{22}$$

If $k = 0$, then

$$\widetilde{P}_{q-1} \equiv 2 \pmod{q^2}, \tag{23}$$

$$\widetilde{P}^2_{\frac{q-1}{2}} \equiv 2 + 2(-1)^{\frac{q-1}{2}} \pmod{q^2}, \tag{24}$$

where $\widetilde{P}_n$ is the n-th Pell-Lucas number defined by:

$$\widetilde{P}_0 = 2,\ \ \widetilde{P}_1 = 2,\ \ \widetilde{P}_i = 2\widetilde{P}_{i-1} + \widetilde{P}_{i-2},\ \ i \geq 2. \tag{25}$$

Acknowledgments. The author would like to thank Prof. K.A. Sveshnikov and Prof. R.M. Kolpakov for valuable suggestions. Also, the author is indebted to the referee for many useful comments.

References

[1] P.M. Cohn, *Algebra, Vol. 1*, Wiley, New York, 1980.

[2] D. Gómez-Pérez, J. Gutierrez, A. Ibeas and D. Sevilla. *Common factors of resultants modulo p*, Bull. Aust. Math. Soc. **79** (2009), 299–302.

[3] C. Helou, G. Terjanian, *Arithmetical properties of wendt's determinant*, Journal of Number Theory **115** (2005), 45–57.

[4] S. Janson, *Resultant and discriminant of polynomials*, Notes, September, **22** (2007).

[5] S. V. Konyagin and I. Shparlinski. *Character Sums with Exponential Functions and their Applications*, Cambridge University Press (1999).

[6] R. J. McIntosh, E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087–2094.

[7] P. Ribenboim, *Fermat's Last Theorem for Amateurs*, Springer, New York, 1999.

[8] Z.-H. Sun, Z.-W. Sun, *Fibonacci numbers and Fermats last theorem*, Acta Arith **60** (1992), 371–388.

[9] Z.W. Sun, R. Tauraso, *New congruences for central binomial coefficients*, Adv. in Appl. Math.

[10] B.L. van der Waerden, *Algebra, vol. 1*, F. Ungar Pub. Co., New York, 1977.