Irish Math. Soc. Bulletin
Number 79, Summer 2017, 31–37
ISSN 0791-5578

Sums of Polynomial Residues

SAMUEL S. GROSS, JOSHUA HARRINGTON AND LAUREL MINOTT

Abstract. In an article in the Monthly from 1904, Orlando Stetson studied the sums of distinct residues of triangular numbers modulo a prime. Rather curiously, this sum is always the same residue class independent of the prime chosen. We extend Stetson's theorem to all polygonal numbers and find similar phenomenon. Extensions to sums of residues of general polynomials are also discussed.

1. Introduction

Recall that the $n^{\underline{\text{th}}}$ s-gonal number is the number of points that are needed to create a regular polygon with s sides, each of length $n-1$ (see figure 1).

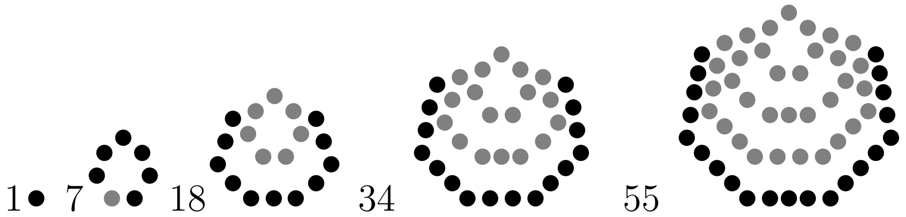

Figure 1. Heptagonal Numbers[1]

We denote these numbers by $P_s(n)$. Alternatively, we can use the algebraic description used by Stetson [5] and characterize these sequences with the recursions

$$\begin{aligned} P_s(1) &= 1 \\ P_s(n+1) - P_s(n) &= n(s-2)+1. \end{aligned} \tag{1}$$

For example, in the *triangular numbers*, or 3-gonal numbers, the difference of consecutive terms follow the pattern $2, 3, 4, \ldots$, while the difference of consecutive squares (4-gonal) follows the sequence

2010 *Mathematics Subject Classification.* 11C08, 11A07, 11B50.
Key words and phrases. Polynomial, Residues.
Received on 9-12-2016.

[1] Figure 1 created by Erica Maciejewski.

of odd numbers $3, 5, 7, \ldots$. Residues of squares, known as quadratic residues, have been well understood beginning as far back as the arithmeticae of Gauss [2].

Theorem 1.1 (Gauss, 1801). *For an odd prime p, there are $(p-1)/2$ distinct quadratic residues modulo p. The sum of these residues is divisible by p.*

A similar property was discovered by Stetson [5] for the triangular numbers.

Theorem 1.2 (Stetson, 1904). *For a prime $p \geq 5$, there are $(p-1)/2$ distinct triangular residues. The sum of these residues is congruent to $-1/16$ modulo p.*[2]

It is widely known that the sequence (1) of s-gonal numbers is generated by the function

$$P_s(n) = \frac{n^2(s-2) - n(s-4)}{2}. \tag{2}$$

We therefore observe that $2P_{2s+1}(x)$ and $P_{2s}(x)$ are quadratic polynomials in $\mathbb{Z}[x]$. It is natural to then ask about the residues of other quadratics, or about the residues of even more general polynomials. In Section 2 we revisit Stetson's work and in Section 3 we pick up where he left off in 1904 by investigating the more general sets of polygonal numbers and quadratics modulo a prime.

The question of sums of residues of more general polynomials is much more difficult. Although the results of the present work are mostly focused on sums of distinct residues of polygonal numbers, in Section 4 we provide conjectural result for a certain class of cubics, as well as a brief historical account of the complexity that arises in studying the residues of an arbitrary polynomial.

2. Stetson's Theorem

Being that Stetson's original work is over a century old, in this section we introduce our general notation, and reproduce the proof of Theorem 1.2 for completeness.

[2] We have adopted the convention of using fractions modulo p where it is understood that a number in the denominator represents the modular inverse of that number. For example, in Stetson's theorem above we mean the inverse of -16 modulo p.

Definition 2.1. Let p be a prime and $s \geq 3$ be an integer. The integer k is called an *s-gonal residue modulo p* if $k \not\equiv 0 \pmod{p}$ and $k \equiv P_s(n) \pmod{p}$ for some positive integer $n < p$. If no such n exists, we say that k is an *s-gonal non-residue* modulo p. Additionally, we define $\mathscr{S}_s(p)$ as the sum of the distinct s-gonal residues modulo p.

The following formulas can be found in most calculus texts, or obtained by induction.

Lemma 2.2. *Let n be a positive integer. Then*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2},$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^{n} \frac{k(k+1)}{2} = \frac{n(n+1)(n+2)}{6}.$$

Proof of Theorem 1.2. Let $p \geq 5$ be a prime. Notice that $P_3(p-1) \equiv 0 \pmod{p}$. For the remaining integers n satisfying $0 < n < p-1$ we have

$$P_3(n) \equiv P_3(p-n-1) \pmod{p}.$$

Since $0 \leq p-n-1 \leq p-1$, we deduce that the triangular residues in the interval $[1, p-1)$ come in pairs, except for the case when $n = (p-1)/2$. It follows that the set

$$\{P_3(1), P_3(2), \ldots, P_3\left((p-1)/2\right)\}$$

is the complete set of $(p-1)/2$ distinct triangular residues modulo p. Using the formulas given in (2) and Lemma 2.2 we may calculate $\mathscr{S}_3(p)$ and obtain $\mathscr{S}_3(p) \equiv -\frac{1}{16} \pmod{p}$. □

3. Generalizing Stetson's Theorem

Notice that the generating function for the s-gonal numbers given in (2) is a quadratic polynomial in n. With this observation, we prove an analogous result for all quadratic polynomials, and then apply this generalization to the polygonal numbers.

Definition 3.1. Let p be a prime and let $f(x)$ be a polynomial with integer coefficients. The integer k is called an *f-polynomial residue* *modulo* p if $k \not\equiv 0 \pmod{p}$ and $k \equiv f(n) \pmod{p}$ for some integer n. Additionally, we define $\mathscr{S}_f(p)$ to be the sum of the distinct f-polynomial residues modulo p.

Theorem 3.2. *Let $f(x) = ax^2 + bx + c$ be a quadratic polynomial with integer coefficients. For a prime $p \geq 5$ not dividing a we have*

$$\mathscr{S}_f(p) \equiv -\frac{b^2 - 4ac}{8a} \pmod{p}.$$

Proof. Let $f(x) = ax^2+bx+c$ be a quadratic polynomial with integer coefficients and let $p \geq 5$ be a prime not dividing a. For integers m and n we have that $f(n) \equiv f(m) \pmod{p}$ if and only if

$$\begin{aligned} 0 &\equiv an^2 + bn - am^2 - bm \\ &\equiv (n-m)\left(n + m + \frac{b}{a}\right), \end{aligned}$$

if and only if $n \equiv m \pmod{p}$ or $n \equiv -m - \frac{b}{a} \pmod{p}$, with both conditions occurring whenever $n \equiv -\frac{b}{2a} \pmod{p}$. Therefore outside of this last case the f-polynomial residues come in pairs. Using the equations from Lemma 2.2 we deduce that

$$\begin{aligned} \mathscr{S}_f(p) &\equiv \frac{\left(\sum_{i=0}^{p-1} f(i)\right) - f\left(-\frac{b}{2a}\right)}{2} + f\left(-\frac{b}{2a}\right) \pmod{p} \\ &\equiv \frac{1}{2}\left(-\frac{b^2}{4a} + c + \sum_{i=0}^{p-1} ai^2 + bi + c\right) \pmod{p} \\ &\equiv \frac{1}{2}\left(-\frac{b^2}{4a} + c + a \cdot \frac{p(p-1)(2p-1)}{6} + b \cdot \frac{p(p-1)}{2} + cp\right) \\ &\equiv -\frac{b^2 - 4ac}{8a} \pmod{p}. \end{aligned}$$

□

In the case of polygonal numbers, one may observe that the s-gonal residues still come in pairs. However, we no longer have the symmetry in the distribution of residues as in the 3-gonal case, where the residues occurred in pairs - one below $(p-1)/2$ and one above. For example, with the pentagonal numbers, $P_5(2) \equiv P_5(4) \pmod{17}$ with $(p-1)/2 = 8$. It is not even the case that the residues will come in pairs below and pairs above $(p-1)/2$, e.g. $P_5(7) \equiv P_5(15)$

(mod 17). Nonetheless, Theorem 3.2 provides an immediate corollary for polygonal numbers whenever s is even. In the case that s is odd and $P_s(n)$ has rational coefficients, it is enough to notice that the argument in Theorem 3.2 only requires that $2^{-1} \pmod{p}$ exists, which it does, and that $s \not\equiv 2 \pmod{p}$ in order to avoid division by 0.

Corollary 3.3. *Let $p \geq 5$ be a prime and $s \geq 3$ be an integer. If $s \not\equiv 2 \pmod{p}$, then there are $(p-1)/2$ distinct s-gonal residues modulo p, and*

$$\mathscr{S}_s(p) \equiv -\frac{1}{16}\frac{(s-4)^2}{(s-2)} \pmod{p}.$$

Remark 3.4. The special cases of $s = 2$ or p dividing a can be handled trivially. In the former, the 2-gonal numbers are simply $1, 2, 3, \ldots$. As such, the sum of distinct resudes modulo a prime p is 0. If p divides a, then $f(x) \equiv bx + c \pmod{p}$. If p also divides b, then $\mathscr{S}_f(p) \equiv c \pmod{p}$ as c is the only residue. On the other hand, if $\gcd(b, p) = 1$ then $0, b, 2b, \ldots, (p-1)b$ is a complete system of distinct residues, with sum 0 modulo p.

The case for higher degree polynomials is much more complicated, for reasons discussed in the next section. We have, however, attempted to investigate several classes of cubics, and we close this section with our most promising heuristic.

Conjecture 3.5. *Let a, b be integers and let $f(x) = ax^3 + bx^2$. For a prime $p \geq 5$ not dividing a,*

$$\mathscr{S}_f(p) = \begin{cases} \dfrac{2b^3}{81a^2} & \text{if } p \equiv 1 \pmod{6} \\ -\dfrac{2b^3}{81a^2} & \text{if } p \equiv 5 \pmod{6}. \end{cases}$$

In the context of this Conjecture, it is easy to see that without loss of generality $gcd(a, b) = 1$ with $0 < a \leq p-1$ and $0 \leq b \leq p-1$. Moreover, if x, y are distinct integers in $[0, p-1]$, then $f(x) \equiv f(y) \pmod{p}$ if and only if (x, y) is a root modulo p of $a(x^2 + xy + y^2) + b(x + y)$. We have not yet found a closed form solution for these roots, however we have computationally verified [4] Conjecture 3.5 for all primes ≤ 1500.

4. General Polynomials

The difficulty in extending to more general polynomials lies in the complexity of listing, or even just counting the number of distinct f polynomial residues. This latter problem has a rich history in the literature in a variety of forms, and effectively remains unsolved to this day. We conclude with a summary of the work in this area to date.

Let $V_n(f)$ denote the number of distinct residues of $f(x)$ modulo n. In 1915 Kantor [3] computed $V_p(f)$ for all primes p and $\deg f = 3$. Precise values for $V_p(f)$ for degrees ≥ 4 are unknown at present, although partial solutions have been given for a specific class of quartics. In particular, Sun [6] determines the value of $V_p(x^4 + ax^2 + bx)$. The counting method of Kantor does not appear to lend itself to results on the sums of residues of cubics, and neither does the technique of Sun extend to sums of residues of $x^4 + ax^2 + bx$.

In the most general case, a complex generating function [7] for $V_n(f)$ is given by

$$V_n(f) = n \sum_{u=0}^{n-1} \left(\sum_{t=0}^{n-1} \sum_{v=0}^{n-1} \exp\left\{ 2\pi i \frac{t}{n}(f(u) - f(v)) \right\} \right)^{-1}, \qquad (3)$$

which naturally lends itself to asymptotic estimates of $V_n(f)$. In 1954, Uchiyama [7] extended Weil's famous 1948 proof [11] of the Riemann Hypothesis for function fields and proved that if $q = p^k$ and $f^*(u, v) = (f(u) - f(v))/(u - v)$ is absolutely irreducible then $V_q(f) > q/2$. The example $f(x) = x^4 - x^2 + 1$ shows that the hypothesis on $f^*(u, v)$ cannot be dropped. However, a year later Carlitz proved [1] that on average $V_q(f)$ is indeed $> q/2$. A series of results followed [8, 9, 10] concerning the asymptotics for $V_q(f)$ over unitary polynomials and over polynomials of a fixed degree. We note that the main result of [10] depends on the Riemann Hypothesis.

References

[1] Leonard Carlitz: On the number of distinct values of a polynomial with coefficients in a finite field. *Proc. Japan Acad.*, 31:119–120, 1955.

[2] Carl Friedrich Gauss: *Disquisitiones Arithmeticae.* in commissis apud Gerh. Fleischer, jun., 1801.

[3] Richard Kantor: Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen. *Monatsh. Math. Phys.*, 26(1):24–39, 1915.

[4] W. A. Stein et al: *Sage Mathematics Software (Version 7.1).* The Sage Development Team, 2016. `http://www.sagemath.org`.

[5] Orlando S. Stetson: Triangular Residues. *Amer. Math. Monthly*, 11(5):106–107, 1904.

[6] Zhi-Hong Sun: On the number of incongruent residues of x^4+ax^2+bx modulo p. *J. Number Theory*, 119(2):210–241, 2006.

[7] Saburô Uchiyama: Sur le nombre des valeurs distinctes d'un polynôme à coefficients dans un corps fini. *Proc. Japan Acad.*, 30:930–933, 1954.

[8] Saburô Uchiyama: Note on the mean value of $V(f)$. *Proc. Japan Acad.*, 31:199–201, 1955.

[9] Saburô Uchiyama: Note on the mean value of $V(f)$. II. *Proc. Japan Acad.*, 31:321–323, 1955.

[10] Saburô Uchiyama: Note on the mean value of $V(f)$. III. *Proc. Japan Acad.*, 32:97–98, 1956.

[11] André Weil: *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

Samuel S. Gross is a mathematician and the Senior Cryptographer at Noblis, Inc. in Reston, Virginia. His research interests, apart from his day job as a cryptographer, lie in Number Theory, and especially connections between prime numbers and irreducible polynomials.

Joshua Harringon has been an Assistant Professor at Cedar Crest College for three years. His research interests are in number theory. His primary research interests are in the area of covering systems of the integers and studying the reducibility properties of polynomials.

Laurel Minott is an undergraduate student at Cedar Crest College. She is a biology and mathematics major and is currently in her junior year.

(S. Gross) Noblis Inc., Reston, Virginia

(J. Harrington and L. Minott) Cedar Crest College, Allentown, Pennsylvania

E-mail address, S. Gross: `samuel.gross@noblis.org`
E-mail address, J. Harrington: `joshua.harrington@cedarcrest.edu`
E-mail address, L. Minott: `ldminott@cedarcrest.edu`