

# NOTES

Edited by William Adkins

---

## On Goldbach's Conjecture for Integer Polynomials

---

Filip Saidak

---

**1. INTRODUCTION.** We give a short proof of the fact that every monic polynomial  $f(x)$  in  $\mathbb{Z}[x]$  can be written in the form  $f(x) = g(x) + h(x)$ , where  $g(x)$  and  $h(x)$  are both irreducible monic polynomials in  $\mathbb{Z}[x]$ . For the number  $\mathfrak{R}(f; y)$  of representations of  $f(x)$  as a sum of two irreducible monics  $g(x)$  and  $h(x)$  in which all coefficients of  $g(x)$  and  $h(x)$  are bounded in absolute value by  $y$  we prove that

$$y^d \ll_f \mathfrak{R}(f; y) \ll_f y^d$$

as  $y \rightarrow \infty$ , where the notation “ $\ll_f$ ” means that the constant could depend on (the degree and coefficients of) the polynomial  $f(x)$ .

**2. CONJECTURE OF GOLDBACH.** In a letter to Euler (dated June 7, 1742), Ch. Goldbach conjectured that every even integer  $n$  greater than three could be written as a sum of two prime numbers. In spite of over two and a half centuries of effort by many great mathematicians this enigmatic conjecture still remains open today. The best results to date are the theorems of I. M. Vinogradov [11] and J.-R. Chen [3] stating, respectively, that a sufficiently large odd integer is always a sum of at most three primes and that a sufficiently large even integer is a sum of a prime and an integer with at most two prime factors.

However, as D. Hayes [8] noticed in 1965, the situation is considerably simpler for polynomials with integer coefficients. In fact, he proved the following result:

**Theorem 1.** *If  $f(x)$  is a monic polynomial in  $\mathbb{Z}[x]$  with  $\deg(f) = d \geq 1$ , then there exist irreducible monic polynomials  $g(x)$  and  $h(x)$  in  $\mathbb{Z}[x]$  with the property that  $f(x) = g(x) + h(x)$ .*

In what follows we give a shorter proof of this interesting theorem. We also describe a counting method that aids us in obtaining a new quantitative generalization.

**3. PROOF OF THEOREM 1.** A polynomial of degree  $n$  over an integral domain  $Z$  is an expression of the form

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

where the coefficients  $a_i$  ( $0 \leq i \leq n$ ) belong to  $Z$  and  $a_n \neq 0$ . The collection of all such polynomials is denoted by  $Z[x]$ . In this paper we consider only the special case  $Z = \mathbb{Z}$ , the set of all integers, and whenever we say that  $f(x)$  is “irreducible,” we mean irreducible over  $\mathbb{Z}[x]$ .

In order to prove Theorem 1, a couple of lemmas are required. First, we recall the remarkable criterion of Eisenstein [6]:

**Lemma 1.** Let  $p$  be a prime, and let  $f(x)$  be a polynomial with coefficients  $a_i$  in  $\mathbb{Z}$ . If  $p \mid a_i$  when  $0 \leq i \leq n - 1$  but  $p \nmid a_n$  and  $p^2 \nmid a_0$ , then  $f(x)$  is irreducible over  $\mathbb{Z}[x]$ .

In addition, one needs the well-known Chinese Remainder Theorem (see [10]):

**Lemma 2.** If  $\gcd(m_i, m_j) = 1$  ( $1 \leq i < j \leq k$ ), then there exists a unique solution modulo  $m_1 m_2 \cdots m_k$  of the  $k$  simultaneous congruences  $x \equiv a_i \pmod{m_i}$ .

**Corollary.** For any coprime integers  $a$  and  $b$  with  $|a| < |b|$  there exist  $u$  and  $v$  in  $\mathbb{Z}$  such that

$$1 = au + bv. \tag{1}$$

The number of solutions  $(u, v)$  with  $|u|, |v| < y$  is at least  $[(2y + 1)/|b|]$ , where  $[x]$  signifies the integer part of  $x$ .

*Proof.* By Lemma 2, the existence of a solution of (1),  $(u_0, v_0)$  say, is obvious. In order to count how many solutions  $(u, v)$  there can be within a given distance of the origin, just notice that if  $(u_0, v_0)$  is a solution, then so is  $(u_1, v_1) = (u_0 - b, v_0 + a)$ . Thus, every interval  $[n + 1, n + a]$  contains the second coordinate  $v$  of a solution  $(u, v)$ , and every interval  $[n + 1, n + b]$  contains the first coordinate  $u$  of a solution  $(u, v)$ . There are  $2y + 1$  integers within the distance  $y$  of the origin, and therefore, since  $|b| > |a|$ , the number of solutions of (1) must be at least  $[(2y + 1)/|b|]$ . ■

Now it is possible to give a very short proof of Hayes’s result:

*Proof.* Write  $f(x) = x^d + F_{d-1}x^{d-1} + \cdots + F_1x + F_0$ . Lemma 1 says that for any prime  $p$  the polynomial  $g(x) = x^d + pG_{d-1}x^{d-1} + \cdots + pG_1x + G_0$  is irreducible as long as  $G_0 \equiv p \pmod{p^2}$ . Similarly, for a prime  $q$  the polynomial  $h(x) = x^{d-1} + qH_{d-2}x^{d-2} + \cdots + qH_1x + H_0$  is irreducible if  $H_0 \equiv q \pmod{q^2}$ . Moreover, if  $p \neq q$ , then we can always choose integers  $G_i$  and  $H_i$  such that  $pG_i + qH_i = F_i$  ( $1 \leq i \leq d - 1$ ). Thus, if we can find (a) a prime  $p$  such that  $p \mid (F_{d-1} - 1)$  and (b) integers  $G_0$  and  $H_0$  with  $G_0 + H_0 = F_0$ , then we are done!

For (a), notice that if  $F_{d-1} - 1 \neq \pm 1$ , then it suffices to take for  $p$  any of the prime factors of  $F_{d-1} - 1$ , while if  $F_{d-1} - 1 = \pm 1$ , then changing the variables (all conclusions are invariant under such operations) to consider  $F^*(x) := F(x + 2)$  evidently gives  $F_{d-1}^* - 1 \neq \pm 1$ , and we can do the same.

For (b) we note that for each  $F_0$  in  $\mathbb{Z}$  and each pair of distinct primes  $p$  and  $q$  there exist integers  $x$  and  $y$  such that  $x$  is congruent to  $p$  modulo  $p^2$ ,  $y$  is congruent to  $q$  modulo  $q^2$ , and  $x + y = F_0$ . Just let  $(p^2)_q^{-1}$  be the multiplicative inverse of  $p^2$  modulo  $q^2$ , then the desired pair  $(x, y)$  is simply

$$\begin{aligned} x &= p - (p^2)_q^{-1}(p^2)(q + p - F_0), \\ y &= F_0 - p + (p^2)_q^{-1}(p^2)(q + p - F_0), \end{aligned} \tag{2}$$

as one can verify. This gives an explicit decomposition of  $f(x)$ . ■

**Remark.** Theorem 1 remains true if one drops the monotonicity condition. The proof is analogous to the one given. In fact, the general situation is simpler, since one does not have to worry about the restriction (a) in the foregoing proof and one has more freedom in choosing the primes  $p$  and  $q$ . We have:

**Theorem 2.** If  $f(x)$  is an arbitrary polynomial with integer coefficients and  $\deg(f) = d \geq 1$ , then there exist irreducible polynomials  $g(x)$  and  $h(x)$  in  $\mathbb{Z}[x]$  with the property that  $f(x) = g(x) + h(x)$ .

**4. THEOREM 3 AND PROOF.** For a given monic polynomial  $f(x)$  we define  $\mathfrak{R}(f; y)$  to be the number of ways of writing  $f(x)$  in the form  $f(x) = g(x) + h(x)$ , where  $g(x)$  and  $h(x)$  are irreducible polynomials with integral coefficients  $g_i$  and  $h_i$ , respectively, satisfying  $|g_i| \leq y$  and  $|h_i| \leq y$ .

Note that Theorem 1 implies that  $\mathfrak{R}(f; y) \geq 1$  as  $y \rightarrow \infty$ . Here we prove:

**Theorem 3.** If  $f(x)$  in  $\mathbb{Z}[x]$  is monic with  $\deg(f) = d \geq 1$ , then there exists a constant  $A(f)$  depending only on  $d$  and the coefficients of  $f(x)$  such that

$$\mathfrak{R}(f; y) > A(f)y^d \tag{3}$$

as  $y \rightarrow \infty$ .

**Remark.** The total number of monic polynomials of degree  $d$  with integer coefficients whose absolute values are bounded by  $y$  is  $(2y + 1)^d$ . Hence, trivially  $\mathfrak{R}(f; y) < By^d$ , where  $B$  is a constant depending only on  $d$  (and  $B < 2^{d+1}$ ). Thus, from Theorem 3 we are able to deduce a Chebyshev-type estimate:

$$y^d \ll_f \mathfrak{R}(f; y) \ll_f y^d. \tag{4}$$

*Proof of Theorem 3.* Following the argument in our proof of Theorem 1, we make the restrictions (a) and (b) on the choice of prime numbers  $p$  and  $q$  quantitative.

(a) As noted earlier, either  $F_{d-1} \neq \pm 1$  or  $F_{d-1}^* \neq \pm 1$ , where  $F_{d-1}^* = F_{d-1} + 2d$  is the second coefficient of  $f(x + 2)$ . In either case, we can always choose the prime  $p$  with  $2 < p < |F_{d-1}| + 2d$ , where  $F_{d-1}$  and  $d$  are fixed quantities (depending only on  $f(x)$ ). The choice  $q = 2$  is then clearly permissible and ensures that  $q \neq p$ . By Corollary 1, finding integers  $G_i$  and  $H_i$  ( $0 \leq i \leq d - 2$ ) such that  $pG_i + qH_i = F_i$  and  $-y < G_i, H_i < y$  can be done in at least  $[(2y + 1)/(pF_i)]$  different ways, when  $F_i \neq 0$ . Hence, the number of possible ways of choosing the two  $(d - 1)$ -tuplets  $(G_0, \dots, G_{d-2})$  and  $(H_0, \dots, H_{d-2})$  is at least  $\tau(f; y)$ , where

$$\tau(f; y) = \frac{(2y + 1)^{d-1}}{p^{d-1}} \cdot \prod_{\substack{0 \leq i \leq d-2 \\ F_i \neq 0}} \frac{1}{F_i}.$$

(b) It remains to estimate the number of ways in which we can choose the last coefficients of the polynomials  $g(x)$  and  $h(x)$ . But this is easy. By Lemma 2 and (2) there is at least one such choice modulo  $4p^2$ , giving us at least  $(2y + 1)/4p^2$  options (i.e., more than  $y/(2p^2)$ ). Therefore, since the quantities  $d, F_0, \dots, F_{d-1}, q = 2$ , and  $p < |F_{d-1}| + 2d$  are all fixed, as  $y \rightarrow \infty$  we evidently have

$$\begin{aligned} \mathfrak{R}(f; y) &> \tau(f; y) \frac{y}{2p^2} > \tau(f; y) \cdot \frac{y}{2(|F_{d-1}| + 2d)^2} \\ &= y^d \left\{ \frac{2^{d-2}}{(|F_{d-1}| + 2d)^d} \cdot \prod_{\substack{0 \leq i \leq d-2 \\ F_i \neq 0}} \frac{1}{F_i} \right\} \\ &= A(f)y^d, \end{aligned}$$

which proves (3) and also gives us an explicit choice of the constant  $A(f)$ . ■

**Remark.** Note that (3) and (4) are stronger than what we would obtain using trivial density arguments. The simplicity of the proof of Theorem 3 arises from the fact that, while primes have density zero in the set of all integers, the density of irreducible polynomials among all polynomials is 1 (see Serre [9]). Therefore,

$$y^{d-\epsilon} \ll_f \mathfrak{R}(f; y) \ll_f y^d \tag{5}$$

is clearly true for any  $\epsilon > 0$ . But this falls short of the stronger result (4).

**5. FINAL REMARKS.** We close with a few comments about the applicability of the foregoing “polynomial” methods and their relation to the classical problems concerning prime numbers.

**Remark 1.** A result similar to Theorem 3 could be obtained for decomposition of polynomials  $f(x)$  in  $\mathbb{Z}[x]$  that are not necessarily monic, in this case producing an analogous estimate  $y^{d+1} \ll \mathfrak{R}^\#(f; y) \ll y^{d+1}$ . However, in this situation it would seem more natural to assume that each of  $f(x)$ ,  $g(x)$ , and  $h(x)$  has a positive leading coefficient, which would complicate matters slightly.

**Remark 2.** The simple density argument of Serre [9] suggests that the true integer equivalent of Theorem 3 is perhaps the “composite” Goldbach theorem: every integer  $n$  greater than eleven can be written as a sum of two composite numbers. Of course, here the proof is trivial (see [10]): if  $n$  is even, write  $n = 4 + (n - 4)$ ; if  $n$  is odd, write  $n = 9 + (n - 9)$ . This shows that the quantitative Theorem 3 has very little in common with the famous conjecture of Hardy and Littlewood [7] stating that, in Goldbach’s original conjecture, the number  $r(N)$  of Goldbach representations of  $N$  satisfies

$$r(N) \sim \frac{N}{(\log N)^2} \prod_{p \nmid N} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p \mid N} \left(1 + \frac{1}{p-1}\right) \tag{6}$$

as  $N \rightarrow \infty$ .

We do not know whether, in place of (5), an asymptotic estimate for  $\mathfrak{R}(f; y)$  can be obtained. But there seems to be no reason why it couldn’t be done.

**Remark 3.** If, instead of polynomials with integer coefficients, one considers an analogue of Goldbach’s conjecture for polynomials with coefficients in a given finite field, then the situation becomes much more complicated. It starts to resemble the classical problem of Goldbach, where unconditional theorems are rare and often fall short of the desired estimates. In fact, the analogue of Vinogradov’s three primes theorem was proved only recently by Effinger and Hayes [4]. The reader is urged to consult their monograph [5] for details.

**ACKNOWLEDGMENTS** This note was written while the author visited Macquarie University in Sydney in 2002. He would like to thank Hugh Williams for support, and Alf van der Poorten and Igor Shparlinski for pleasant working conditions and for many informative discussions. Thanks are also due to Florian Luca for sending me a sketch of a clever proof of Bouniakowski’s conjecture for integer polynomials.

REFERENCES

---

1. T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1983.
2. C. Betts, Additive and subtractive irreducible monic decompositions in  $\mathbf{Z}[x]$ , *C. R. Math. Acad. Sci. Soc. R. Can.* **20** (1998) 86–90.

3. J.-R. Chen, On the representation of a large even integer as the sum of a prime and the product of at most two primes, *Kexue Tongbao* **17** (1966) 365–386.
4. G. W. Effinger and D. R. Hayes, A complete solution to the polynomial 3-primes problem, *Bull. Amer. Math. Soc. (N.S.)* **24** (1991) 363–369.
5. ———, *Additive Number Theory of Polynomials over a Finite Field*, Clarendon Press, Oxford, 1991.
6. G. Eisenstein, Über die Irreducibilität und einige andere Eigenschaften der Gleichung, *J. Math.* **39** (1850) 160–182.
7. G. H. Hardy and J. E. Littlewood, Some problems of “Partitio numerorum” III.: On the expression of a number as a sum of primes, *Acta Math.* **44** (1922) 1–70.
8. D. Hayes, A Goldbach theorem for polynomials with integer coefficients, this MONTHLY **72** (1965) 45–46.
9. J.-P. Serre, *Topics in Galois Theory*, Jones & Bartlett, Boston, 1992.
10. W. Sierpiński, *Elementary Theory of Numbers*, PAN, Warsaw, 1964.
11. I. M. Vinogradov, Representation of an odd number as a sum of three primes, *Dokl. Akad. Nauk SSSR* **15** (1937) 291–294 (Russian).

*Department of Mathematics, University of Calgary, Alberta, T2N 1N4, Canada*

---

## Moment Sums Associated with Binary Linear Forms

---

P. Shiu

---

**1. INTRODUCTION.** Let  $a$  and  $b$  be coprime integers exceeding 1, and denote by  $\mathcal{S}$  the set of nonnegative integers  $m$  less than  $ab$  for which the linear Diophantine equation

$$ax + by = m \tag{1.1}$$

is soluble with  $x$  and  $y$  nonnegative. J. J. Sylvester [4] found that the largest number  $m$  for which (1.1) is not soluble is the odd number

$$M = ab - a - b \tag{1.2}$$

(see, for example, [2, Theorem 1.8.2] for the proof). The corresponding problem with more than two variables (known as the *coin problem* of Frobenius) is much more difficult, and many useful references on this are given in [1, Problem C7]. Here we introduce a simple criterion for  $m$  to belong to  $\mathcal{S}$ , which is then used to evaluate the moment sums

$$S_r = \sum_{m \in \mathcal{S}} m^r \quad (r = 0, 1, 2, \dots). \tag{1.3}$$

Let  $B_r = B_r(0)$ , where  $B_r(x)$  are the Bernoulli polynomials defined by the generating function

$$\frac{te^{xt}}{e^t - 1} = \sum_{r \geq 0} \frac{B_r(x)t^r}{r!},$$

and write