J. Fac. Educ. Tottori Univ. (Nat. Sci.), 46 (1997) 17-25

Heuristic Asymptotic Formulae Concerning Prime Values of Polynomials

Kenichi SHIMIZU* Kazuo Goto[†]

(Received April 30, 1997)

1 Introduction

On the distribution of primes in arithmetic progressions, Dirichlet proved a very important theorem (Theorem 1, below) in 1837. And de la Vallée Poussin proved a density result (Theorem 2, below) concerning Dirichlet's theorem. But it is not hardly known anything on the distribution of prime values, which are attained by polynomials of higer degree. In 1923, Hardy and Littlewood [1] conjectured on quadratic polynomials (Conjecture 1, below).

In this paper, first, we consider a known conjecture (see Conjecture 2) of the heuristic asymptotic formula concerning polynomials of arbitrary degree; second, we deduce de la Vallée Poussin's theorem and the conjecture of Hardy and Littlewood from Conjecture 2. Third, we deduce an analogy of the conjecture of Hardy and Littlewood on certain cubic polynomial concerning a modular form of weight one.

2 Notation and Known Results

NOTATION. Let f(n) be an irreducible polynomial with integral coefficients and with a positive leading coefficient, and p a prime. We define p(x), P(X), N_p and \sim by

$$p(x) = \#\{n | 1 \le n \le x, |f(n)| \text{ is a prime}\},\$$

$$P(X) = \#\{n | 1 \le n, |f(n)| \le X, |f(n)| \text{ is a prime}\},\$$

$$N_p = \#\{n | f(n) \equiv 0 \pmod{p}, 1 \le n \le p\},\$$

$$A(x) \sim B(x) \text{ means } \lim_{x \to \infty} \frac{A(x)}{B(x)} = 1.$$

THEOREM 1 (Dirichlet). If a > 0 and $b \neq 0$ are integers that are relatively prime, then the arithmetic progression $\{an + b\}$ contains infinitely many primes.

THEOREM 2 (de la Vallée Poussin). For the arithmetic progression in Theorem 1, we put f(n) = an + b, then we have

$$P(X) \sim \frac{1}{\phi(a)} \frac{X}{\log X} \quad as \quad X \to \infty,$$

^{*} Department of Mathematics, Kenmei-Joshigakuin High School, Himeji, 670, Japan

[†] Department of Mathematics, Faculty of Education, Tottori University, Tottori, 680, Japan

where $\phi(x)$ is Euler's totient function.

Furthermore on the distribution of prime values of quadratic polynomials, it is known the conjecture of Hardy and Littlewood as follows.

CONJECTURE 1 (Hardy and Littlewood [1]). Let a > 0, b and c are integers such that gcd(a, b, c) = 1, a + b and c are not both even. Let $f(n) = an^2 + bn + c$ and the discriminant $D = b^2 - 4ac$ of f(n) is squarefree. We define $\varepsilon = 1$ if a + b is odd and $\varepsilon = 2$ otherwise. Then the number P(X) is given asymptotically by

$$P(X) \sim \frac{\varepsilon C}{\sqrt{a}} \frac{\sqrt{X}}{\log X} \prod_{\substack{p \ge 3 \\ p \mid a \\ p \mid b}} \frac{p}{p-1} \quad as \quad X \to \infty,$$

where $C = \prod_{\substack{p \ge 3 \\ p \neq a}} \left(1 - \frac{1}{p-1} \left(\frac{D}{p}\right)\right)$, and $\left(\frac{D}{p}\right)$ is Legendre's symbol.

It is known the following conjecture about the distribution of prime values of polynomials of arbitrary degree.

CONJECTURE 2. Let f(n) be a polynomial of degree m defined by Notation, then we have

$$p(x) \sim \frac{1}{m} \prod_{p} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} \frac{x}{\log x}$$

3 Relations between Conjecture 2 and Other Results

First, we describe how Conjecture 2 is presumed.

Setting X = f(x), we could say by a heuristic argument that p(x) is approximately equal to $x \prod_{p \le \sqrt{X}} \left(1 - \frac{N_p}{p}\right)$ for sufficiently large x.

We have

$$x \prod_{p \le \sqrt{X}} \left(1 - \frac{N_p}{p} \right) = \frac{x \prod_{p \le \sqrt{X}} \left(1 - \frac{N_p}{p} \right)}{\prod_{p \le \sqrt{X}} \left(1 - \frac{1}{p} \right)} \prod_{p \le \sqrt{X}} \left(1 - \frac{1}{p} \right)$$
$$= x \prod_{p \le \sqrt{X}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} \prod_{p \le \sqrt{X}} \left(1 - \frac{1}{p} \right).$$

We could also say $\prod_{p \le \sqrt{X}} \left(1 - \frac{1}{p}\right)$ is approximately equal to $\frac{\pi(X)}{X}$. Since $\frac{\pi(X)}{X} \sim$

 $\frac{1}{\log X}$ by the prime number theorem, we obtain that $x \prod_{p \le \sqrt{X}} \left(1 - \frac{N_p}{p}\right)$ is approximately equal to $x \prod_p \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} \frac{1}{\log X}$ for sufficiently large x.

Using $\log X = \log f(x) \sim m \log x$, we expect

$$p(x) \sim x \prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \frac{1}{\log X}$$
$$= x \prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \frac{1}{m \log x} = \frac{1}{m} \prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \frac{x}{\log x}$$

Thus we obtain Conjecture 2.

REMARK. We know the theorem of Mertens, that is,

$$\prod_{p\leq X} \left(1-\frac{1}{p}\right) \sim \frac{e^{-c}}{\log X},$$

where c is Euler's constant.

Although we have presumed Conjecture 2 by rougher approximation as above, we can justify this conjecture as follows.

Using Conjecture 2, we shall deduce de la Vallée Poussin's theorem (Theorem 2, above) and the conjecture of Hardy and Littlewood (Conjecture 1, above).

PROPOSITION 1. Conjecture 2 implies Theorem 2.

PROOF. We note $N_p = 0$ if p|a and $N_p = 1$ otherwise. Hence

$$\prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} = \prod_{p \mid a} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \prod_{p \nmid a} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}}$$
$$= \prod_{p \mid a} \frac{1 - \frac{0}{p}}{1 - \frac{1}{p}} \prod_{p \restriction a} \frac{1 - \frac{1}{p}}{1 - \frac{1}{p}}$$
$$= \prod_{p \mid a} \frac{1}{1 - \frac{1}{p}} = \frac{1}{\prod_{p \mid a} \left(1 - \frac{1}{p}\right)} = \frac{a}{\phi(a)}$$

Therefore from Conjecture 2, we obtain as x tends to infinity,

$$p(x) \sim \frac{a}{\phi(a)} \frac{x}{\log x}.$$
 (1)

Using (1), we show

$$P(X) \sim \frac{1}{\phi(a)} \frac{X}{\log X}.$$

We set X = f(x) (see Notation). It is clear that P(X) = p(x) and

$$\lim_{x \to \infty} \frac{ax}{\log x} / \frac{X}{\log X}$$
$$= \lim_{x \to \infty} a \cdot \frac{x}{X} \cdot \frac{\log X}{\log x}$$
$$= \lim_{x \to \infty} a \cdot \frac{x}{ax+b} \cdot \frac{\log (ax+b)}{\log x} = a \cdot \frac{1}{a} \cdot 1 = 1$$

Hence

$$\frac{ax}{\log x} \sim \frac{X}{\log X}$$

Thus

$$P(X) = p(x) \sim \frac{a}{\phi(a)} \frac{x}{\log x} \sim \frac{1}{\phi(a)} \frac{X}{\log X} \quad as \quad X \to \infty.$$

Therefore we get Theorem 2, which completes the proof of Proposition 1.

PROPOSITION 2. Conjecture 2 implies Conjecture 1.

To prove Proposition 2, we mention the following lemma.

LEMMA 1. Let $D = b^2 - 4ac$ be the discriminant of a quadratic polynomial $f(n) = an^2 + bn + c$, then we have

$$\frac{1-\frac{N_p}{p}}{1-\frac{1}{p}} = 1 - \frac{1}{p-1} \left(\frac{D}{p}\right) \quad (p \ge 3, \ p \not\mid a).$$

PROOF. In the quadratic polynomial, we have

$$N_{p} = 2 \iff \left(\frac{D}{p}\right) = 1,$$
$$N_{p} = 1 \iff \left(\frac{D}{p}\right) = 0,$$
$$N_{p} = 0 \iff \left(\frac{D}{p}\right) = -1,$$

for $p \ge 3$ and $p \nmid a$.

From these properties we get the following equations. If $N_p = 2$, then

$$\frac{1-\frac{N_p}{p}}{1-\frac{1}{p}} = \frac{1-\frac{2}{p}}{1-\frac{1}{p}} = 1 - \frac{1}{p-1} = 1 - \frac{1}{p-1} \left(\frac{D}{p}\right).$$

If $N_p = 1$, then

$$\frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \frac{1 - \frac{1}{p}}{1 - \frac{1}{p}} = 1 - \frac{0}{p - 1} = 1 - \frac{1}{p - 1} \left(\frac{D}{p}\right).$$

If $N_p = 0$, then

$$\frac{1-\frac{N_p}{p}}{1-\frac{1}{p}} = \frac{1}{1-\frac{1}{p}} = 1 - \frac{-1}{p-1} = 1 - \frac{1}{p-1} \left(\frac{D}{p}\right).$$

Therefore we complete the proof of Lemma 1.

PROOF of PROPOSITION 2. Let x be sufficiently large. In the case of the quadratic polynomial, Conjecture 2 means

$$p(x) \sim \frac{1}{2} \prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \frac{x}{\log x}.$$
 (2)

We have

$$\prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} = \frac{1 - \frac{N_{2}}{2}}{1 - \frac{1}{2}} \prod_{\substack{p \ge 3\\ p \nmid a}} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \prod_{\substack{p \ge 3\\ p \mid a}} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}}.$$
(3)

By Lemma 1, we get

$$\prod_{\substack{p \ge 3 \\ p \nmid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \nmid a}} \left(1 - \frac{1}{p - 1} \left(\frac{D}{p} \right) \right).$$
(4)

We show the following (5) and (6).

$$\frac{1 - \frac{N_2}{2}}{1 - \frac{1}{2}} = \varepsilon.$$
(5)

$$\prod_{\substack{p \ge 3\\p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3\\p \mid a\\p \mid b}} \frac{p}{p-1}.$$
(6)

First, we note that a + b and c are not both even. If a + b is odd, then $N_2 = 1$. Thus

$$\frac{1 - \frac{N_2}{2}}{1 - \frac{1}{2}} = 1 = \varepsilon.$$

If a + b is even, then $N_2 = 0$. So

$$\frac{1 - \frac{N_2}{2}}{1 - \frac{1}{2}} = 2 = \varepsilon.$$

Hence (5) is proved.

Second, the proof of (6) is shown as follows:

$$\prod_{\substack{p \ge 3 \\ p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} \prod_{\substack{p \ge 3 \\ p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}}.$$

If $p \ge 3$, p|a and p|b, then $N_p = 0$ and

$$\prod_{\substack{p \ge 3 \\ p \mid a \\ p \mid b}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a \\ p \mid b}} \frac{1 - \frac{0}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a \\ p \mid b}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a \\ p \mid b}} \frac{p}{p - 1}.$$

If $p \ge 3$, p | a and $p \not> b$, then $N_p = 1$ and

$$\prod_{\substack{p \ge 3 \\ p \mid a \\ p \neq b}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a \\ p \neq b}} \frac{1 - \frac{1}{p}}{1 - \frac{1}{p}} = 1.$$

Thus we have

$$\prod_{\substack{p \ge 3 \\ p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} \prod_{\substack{p \ge 3 \\ p \mid a}} \frac{1 - \frac{N_p}{p}}{1 - \frac{1}{p}} = \prod_{\substack{p \ge 3 \\ p \mid a}} \frac{p}{p - 1},$$

which proved (6).

Therefore, by (2), (3), (4), (5) and (6), we have

$$p(x) \sim \frac{1}{2} \prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \frac{x}{\log x} = \frac{\varepsilon}{2} \prod_{\substack{p \ge 3\\ p \neq a}} \left(1 - \frac{1}{p - 1} \left(\frac{D}{p} \right) \right) \prod_{\substack{p \ge 3\\ p \mid a \\ p \mid b}} \frac{p}{p - 1} \frac{x}{\log x}.$$

If we set $C = \prod_{\substack{p \ge 3 \\ p \nmid a}} \left(1 - \frac{1}{p-1} \left(\frac{D}{p} \right) \right)$, we have

$$p(x) \sim \frac{\varepsilon C}{2} \prod_{\substack{p \ge 3\\p \mid a\\p \mid b}} \frac{p}{p-1} \frac{x}{\log x} = \frac{\varepsilon C}{2} \frac{x}{\log x} \prod_{\substack{p \ge 3\\p \mid a\\p \mid b}} \frac{p}{p-1}.$$
(7)

Using (7) we show

$$P(X) \sim \frac{\varepsilon C}{\sqrt{a}} \frac{\sqrt{X}}{\log X} \prod_{\substack{p \ge 3 \\ p \mid a \\ p \mid b}} \frac{p}{p-1} \quad as \quad X \to \infty.$$

Setting X = f(x), we have

$$\frac{x}{\log x} \sim \frac{2}{\sqrt{a}} \frac{\sqrt{X}}{\log X}.$$
(8)

Because

$$\lim_{x \to \infty} \frac{x}{\log x} \left| \frac{2}{\sqrt{a}} \frac{\sqrt{X}}{\log X} = \lim_{x \to \infty} \frac{\sqrt{a}}{2} \frac{x}{\sqrt{X}} \frac{\log X}{\log x} = \frac{\sqrt{a}}{2} \frac{1}{\sqrt{a}} \cdot 2 = 1,$$

using

$$\lim_{x \to \infty} \frac{x}{\sqrt{X}} = \lim_{x \to \infty} \frac{x}{\sqrt{ax^2 + bx + c}} = \frac{1}{\sqrt{a}}$$
$$\lim_{x \to \infty} \frac{\log X}{\log x} = \lim_{x \to \infty} \frac{\log (ax^2 + bx + c)}{\log x} = 2.$$

Therefore we have obtained (8). From the above (7) and (8), we obtain

$$P(X) = p(x) \sim \frac{\varepsilon C}{2} \frac{x}{\log x} \prod_{\substack{p \ge 3 \\ p \mid b}} \frac{p}{p-1} \sim \frac{\varepsilon C}{2} \frac{2}{\sqrt{a}} \frac{\sqrt{X}}{\log X} \prod_{\substack{p \ge 3 \\ p \mid b}} \frac{p}{p-1}$$
$$= \frac{\varepsilon C}{\sqrt{a}} \frac{\sqrt{X}}{\log X} \prod_{\substack{p \ge 3 \\ p \mid b}} \frac{p}{p-1}.$$

This completes the proof of Proposition 2.

4 Analogy of the Conjecture of Hardy and Littlewood for Certain Cubic Polynomial

We study heuristic asymptotic formulae of cubic polynomials. The Galois group of every quadratic polynomial is abelian, but the situation changes completely in the case of a cubic polynomial.

If the Galois group of a cubic polynomial is abelian, then the law of factorization is described by congruences with respect to a certain modulus. For example, for the polynomial $n^3 - 3n - 1$, the prime factors of this polynomial are the form $p \equiv \pm 1$ (mod 18) except p = 3 and $N_p = 3$ for these primes. But if the Galois group is non-abelian, then the law of factorization is difficult and it is only known special cases.

In this section, we claim the possibility of obtaining a heuristic asymptotic formula of a cubic polynomial. We consider the polynomial $4n^3 - 4n^2 + 1$ which relates to the modular form of weight one. The Galois group of this polynomial is non-abelian and the arithmetic congruence relation is as follows.

THEOREM 3 (Hiramastu [2]). Let $f(n) = 4n^3 - 4n^2 + 1$, and let c(n) be the nth coefficient of the expansion of $\eta(2\tau)\eta(22\tau) = \sum_{n=1}^{\infty} c(n)q^n$. Then we have

$$N_p = c(p)^2 - \left(\frac{p}{11}\right) \quad (p \neq 2, 11),$$

where $\eta(\tau)$ is the Dedekind eta function

$$\eta(\tau) = e^{\frac{\pi i \tau}{12}} \prod_{n=1}^{\infty} (1 - e^{2\pi i n \tau}) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n), \quad q = e^{2\pi i \tau}.$$

By using c(p) in Theorem 3, we can obtain an asymptotic formula of the prime values of the cubic polynomial $4n^3 - 4n^2 + 1$.

THEOREM 4. Let $f(n) = 4n^3 - 4n^2 + 1$, then we have

$$p(x) \sim \frac{3}{5} \prod_{p \neq 2, 11} \left(1 - \frac{1}{p-1} c(p) \right) \frac{x}{\log x} \quad as \ x \to \infty.$$

PROOF. From the proof of Theorem 3, we have

$$N_p = 3 \iff c(p) = 2,$$

$$N_p = 1 \iff c(p) = 0,$$

$$N_p = 0 \iff c(p) = -1,$$

for primes $p \neq 2$, 11.

By using these properties, we get

$$\begin{split} &\prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \\ &= \frac{1 - \frac{N_{2}}{2}}{1 - \frac{1}{2}} \frac{1 - \frac{N_{11}}{11}}{1 - \frac{1}{11}} \prod_{c(p)=-1} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \prod_{c(p)=0} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \prod_{c(p)=2} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \\ &= (2 - N_{2}) \frac{11 - N_{11}}{10} \prod_{c(p)=-1} \frac{1 - \frac{0}{p}}{1 - \frac{1}{p}} \prod_{c(p)=0} \frac{1 - \frac{1}{p}}{1 - \frac{1}{p}} \prod_{c(p)=2} \frac{1 - \frac{3}{p}}{1 - \frac{1}{p}} \\ &= (2 - N_{2}) \frac{11 - N_{11}}{10} \prod_{c(p)=-1} \left(1 - \frac{-1}{p-1}\right) \prod_{c(p)=0} \left(1 - \frac{0}{p-1}\right) \prod_{c(p)=2} \left(1 - \frac{2}{p-1}\right) \\ &= (2 - N_{2}) \frac{11 - N_{11}}{10} \prod_{c(p)=-1} \left(1 - \frac{c(p)}{p-1}\right) \prod_{c(p)=0} \left(1 - \frac{c(p)}{p-1}\right) \prod_{c(p)=2} \left(1 - \frac{c(p)}{p-1}\right) \\ &= (2 - N_{2}) \frac{11 - N_{11}}{10} \prod_{p \neq 2, 11} \left(1 - \frac{1}{p-1}c(p)\right). \end{split}$$

Calculating N_2 and N_{11} , we get $N_2 = 0$ and $N_{11} = 2$. So

$$\prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} = 2 \cdot \frac{9}{10} \prod_{p \neq 2, 11} \left(1 - \frac{1}{p - 1} c(p) \right) = \frac{9}{5} \prod_{p \neq 2, 11} \left(1 - \frac{1}{p - 1} c(p) \right).$$

Therefore by Conjecture 2, we obtain as x tends to infinity,

$$p(x) \sim \frac{1}{3} \prod_{p} \frac{1 - \frac{N_{p}}{p}}{1 - \frac{1}{p}} \frac{x}{\log x} = \frac{3}{5} \prod_{p \neq 2, 11} \left(1 - \frac{1}{p - 1} c(p) \right) \frac{x}{\log x},$$

which completes the proof.

REMARKS. 1. In the same way as the proof of Proposition 1 and 2, we can show as x tends to infinity,

$$P(X) \sim \frac{9}{5\sqrt[3]{4}} \prod_{p \neq 2, 11} \left(1 - \frac{1}{p-1} c(p) \right) \frac{\sqrt[3]{X}}{\log X},$$

by using

$$\frac{x}{\log x} \sim \frac{3}{\sqrt[3]{4}} \frac{\sqrt[3]{X}}{\log X}.$$

2. We note that c(p) appears instead of Legendre symbol $\left(\frac{D}{p}\right)$ appearing in the conjecture of Hardy and Littlewood.

We give other examples which also relate to the modular forms of weight one (see [2], [3] and [4]). For such a polynomial, we can obtain the similar asymptotic formula.

EXAMPLE 1. If $f(n) = n^3 - 2$, then we have

$$N_p = c(p)^2 - \left(\frac{-3}{p}\right) \quad (p \neq 2, 3),$$

where c(p) is defined by $\eta(6\tau)\eta(18\tau) = \sum_{n=1}^{\infty} c(n)q^n$.

EXAMPLE 2. If $f(n) = n^3 - n - 1$, then we lave

$$N_p = c(p)^2 - \left(\frac{-23}{p}\right) \quad (p \neq 2, 23),$$

where c(p) is defined by $\eta(\tau)\eta(23\tau) = \sum_{n=1}^{\infty} c(n)q^n$.

References

- [1] Hardy, G. H. and Littlewood, J. E.: Some problems of partitio numerorum III: On the expression of a number as a sum of primes, Acta Math., 44, (1923), 1–70.
- [2] Hiramastu, T.: Higher reciprocity laws and modular forms of weight one, Comm. Math. Univ. St. Paul. 31 (1982), 75-85.
- [3] Hiramastu, T.: Some topics of automorphic forms of weight one (重さ1の保型形式についての いくつかの話題), RISM, Kyoto, Kokyuroku 513 (1984), 1–18.
- Serre, J-P.: Modular forms of weight one and Galois representations, Proc. Symposium on Algebraic Number Field, Akademic Press, London, 1977, 193–268.