The Number of Distinct Values of a Polynomial with Coefficients in a Finite Field[*]

By Saburô Uchiyama
Mathematics Department, Tokyo Metropolitan University

(Communicated by Z. Suetuna, M.J.A, Dec 13, 1954)
(Translated Google Translate and Joshua E. Hill, June 21, 2011)

Given a polynomial $f(X)$ of degree $n \geq 2$ with integer coefficients and a positive integer m, we denote the number of distinct values $f(k)$ $(k = 0, 1, ..., m-1)$ modulo m as $W(m)$. As one can easily see the function $W(m)$ can be written as

$$W(m) = m \sum_{u=0}^{m-1} \left(\sum_{t=0}^{m-1} \sum_{v=0}^{m-1} \exp \left\{ 2\pi i \frac{t}{m} \left(f(u) - f(v) \right) \right\} \right)^{-1}$$

This function is multiplicative, that is to say that if two positive integers m_1 and m_2 with $(m_1, m_2) = 1$ then $W(m_1 m_2) = W(m_1) W(m_2)$.

In number theory it would be interesting to determine the value of $W(m)$ for given polynomials with integer coefficients. R. D. von Sterneck and R. Kantor have completely solved this problem for cubic and quadratic polynomials[1], but we do not yet know enough to find the value of $W(m)$ in the special case where m is prime[2] for polynomials of degree 4 or greater.

Later we will study the value of the function $W(p)$ (p an odd prime) for some polynomials, setting a lower bound for $W(p)$ when p tends to infinity. We will then consider the similar problem of prime ideals in algebraic number fields.

1. Using finite fields we can simplify and unify the entire account in the following.

Let the finite field with $q = p^\nu$ elements be denoted as $\mathbb{F}_q$, where p is an odd prime and $\nu \geq 1$. Given a polynomial $f(X)$ of degree n with coefficients in $\mathbb{F}_q$, we denote the number of distinct values $f(x), x \in \mathbb{F}_q$ as $V(q)$. Without loss of generality we can assume that the polynomial is monic, that is, that its leading coefficient is equal to one.

[1] Richard Kantor: *Über die Anzahl inkongruenter Werte ganzer, rationaler Funktionen*, Monatshefte Für Mathematik, Vol. 26, No. 1, 24 – 39 (1915). [*Translator's note:* Reference corrected.]

[2] Cf. Sarvadaman Chowla: *The Riemann Zeta and Allied Functions*, Bulletin of the American Mathematical Society, 58, p. 301 (1952). We trivially have $W(p) > p/n$.

[*] Original paper Saburô Uchiyama: *Sur le Nombre des Valeurs Distinctes d'un Polynôme à Coefficients dans un Corps Fini*. Proc. Japan Acad. Volume 30, Number 10, 930 – 933 (1954) available at `http://projecteuclid.org/euclid.pja/1195525873`

It is easy to show that:
1. if $n = 2$ and $f(X) = X^2 + aX + b$, with $a, b \in \mathbb{F}_q$ $(p \neq 2)$, we have

$$V(q) = \frac{q+1}{2}$$

and
2. if $n = 3$ and $f(X) = X^3 + aX^2 + bX + c$, with $a, b, c \in \mathbb{F}_q$ $(p \neq 2 \text{ or } 3)$, we have

$$V(q) = \begin{cases} q & a^2 - 3b = 0 \text{ and } q \equiv -1 \pmod 3 \\ \frac{q+2}{3} & a^2 - 3b = 0 \text{ and } q \equiv 1 \pmod 3 \\ \frac{2q-1}{3} & a^2 - 3b \neq 0 \text{ and } q \equiv -1 \pmod 3 \\ \frac{2q+1}{3} & a^2 - 3b \neq 0 \text{ and } q \equiv 1 \pmod 3 \end{cases}$$

2. For the case where $n \geq 4$ we show the following result:

Theorem. *Let $f(X) \in \mathbb{F}_q[x]$ be a polynomial of degree $n \geq 4$ for which the polynomial $f^*(u, v) = \frac{f(u)-f(v)}{u-v}$ is absolutely irreducible*[3]*. Then, we have the inequality*

$$V(q) > \frac{q}{2}$$

for any sufficiently large prime p.

Note 1. If a polynomial $P(u, v)$ with coefficients in an algebraic number field is absolutely irreducible, then it is also absolutely irreducible modulo a prime ideal except for finitely many prime ideals.[4]

Note 2. If we drop the assumption in the theorem that the polynomial $f^*(u, v)$ is absolutely irreducible, we can *not*[†] in general conclude that $V(q) > q/2$ for *any* sufficiently large prime p. Indeed, for $f(X) = X^4 - X^2 + 1$ we have $f^*(u, v) = (u + v)(u^2 + v^2 - 1)$ and there are infinitely many primes p such that $V(q) \leq (q - 1)/2$. There is another more important example. Consider the polynomial $f(X) = X^3 + aX^2 + bX + c$, $(a, b, c \in \mathbb{F}_q)$: we then have

$$f^*(u, v) = u^2 + uv + v^2 + a(u + v) + b$$

A necessary and sufficient condition for $f^*(u, v)$ to be absolutely irreducible is $a^2 - 3b \neq 0$ in $\mathbb{F}_q$. Therefore, if $a^2 - 3b = 0$, the polynomial $f^*(u, v)$ can be reduced to two linear factors and, as we have seen, $V(q) = (q + 2)/3$ for all $q \equiv 1 \pmod 3$.

[3] That is to say, irreducible over the algebraic closure, $\bar{\mathbb{F}}_q$

[4] Alexander Ostrowski: *Zur arithmetischen Theorie der algebraischen Grössen*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch–physikalische Klasse aus dem Jahre 1919, p. 296. Cf. Emmy Noether: *Ein algebraisches Kriterium für absolute Irreduzibilität*, Mathematische Annalen 85, 26 – 33 (1922) [*Translator's note:* References corrected.]

[†] *Translator's note*: Should the original paper read "nous ne pas pourions" here? Google Translate's attempt at this didn't make any sense. Thanks to Will Orton and Andrew Ranta for their French language guidance!

3. We will now briefly sketch a proof for the above theorem; the author's detailed reasoning will appear elsewhere.

Let $q = p^\nu$, a power of an odd prime, and let $f(X) \in \mathbb{F}_q[X]$ be a polynomial of degree $n \geq 4$: let M_r $(1 \leq r \leq n)$ denote the number of $m \in \mathbb{F}_q$ for which the equation $f(x) = m$ has exactly r roots in $\mathbb{F}_q$, then we have by definition

$$V(q) = \sum_{r=1}^{n} M_r \tag{3.1}$$

and

$$q = \sum_{r=1}^{n} rM_r \tag{3.2}$$

If, in addition, N_1 and N_2 are the numbers of solutions (x, y) and (u, v) in $\mathbb{F}_q$ of $f(x) - f(y) = 0$ and $f^*(u, v) = 0$, respectively, then obviously

$$N_1 = \sum_{r=1}^{n} r^2 M_r = q + N_2 + O(1) \tag{3.3}$$

And a theorem of A. Weil[5] gives

$$N_2 = q + O\left(q^{\frac{1}{2}}\right) \tag{3.4}$$

when the polynomial $f^*(u, v)$ is absolutely irreducible. Therefore, we have the inequality

$$2\left(N_1 V(q) - q^2\right) \geq \left(\sum_{r=1}^{n} M_r\right)^2 - \sum_{r=1}^{n} M_r^2 \tag{3.5}$$

We have $\left(\sum M_r\right)^2 - \sum M_r^2 \geq 0$, so it follows immediately that if the polynomial $f^*(u, v)$ is absolutely irreducible, there are two constants c_1 and c_2 (> 0) independent of q such that

$$V(q) > \frac{q}{2} - c_1 q^{\frac{1}{2}} \tag{3.6}$$

for any prime $p > c_2$.

4. We must first provide an auxiliary lemma:

Lemma. *If $V(q) < q/2$ and $p > c_2$, then there is a constant $\delta > 0$ so that $M_2 < \left(\frac{1}{2} - \delta\right) q$, such that δ is independent of q.*

To prove this lemma we use L-functions[6] defined on the finite field $\mathbb{F}_q$.

5. We now conclude the proof of our theorem.

Assume that $V(q) < q/2$ for any sufficiently large prime p. Let

$$M_{r_0} = \max_{1 \leq r \leq u} M_r$$

[5] André Weil: *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités scientifiques et industrielles, 1041, Paris, 1948. See also Halmut Hasse: *Über die Kongruenzzetafunktionen*, Sitzungsberichte Berlin, 1934 §9. [*Translator's note:* First reference corrected; translator cannot find second reference; please contact the translator if you have access to the second reference.]

[6] See Saburô Uchiyama: *Sur les Polynômes Irréductibles dans un Corps Fini. I.* Proceedings of the Japan Academy, Vol. 30, No. 7, 523 – 527 (1954). [*Translator's note:* Reference expanded]

We must distinguish the case of $r_0 \neq 2$ and that of $r_0 = 2$:

i) $r_0 \neq 2$. According to (3.1) and (3.2) we have

$$M_{r_0} < \left(\frac{1}{2} - \frac{1}{2n}\right) q$$

and the inequality (3.5) combined with (3.6) gives us

$$\begin{aligned} 2\left(N_1 V(q) - q^2\right) &\geq \left(\sum M_r\right)^2 - M_{r_0}\left(\sum M_r\right) \\ &> \left(\frac{q}{2} - c_1 q^{\frac{1}{2}}\right)\left(\frac{q}{2n} - c_1 q^{\frac{1}{2}}\right) \end{aligned}$$

for $p > c_2$. But this last inequality leads $V(q) > q/2$ for all sufficiently large p, which contradicts our assumption.

ii) $r_0 = 2$. In this case, under the previous lemma, we will again arrive at a contradiction by similar reasoning as the case $r_0 \neq 2$.

Our theorem is thus proven.