Equality of Polynomial and Field Discriminants

Avner Ash, Jos Brakenhoff, and Theodore Zarrabi

CONTENTS

We give a conjecture concerning when the discriminant of an irreducible monic integral polynomial equals the discriminant of the field defined by adjoining one of its roots to $\mathbb{Q}$. We discuss computational evidence for it. An appendix by the second author gives a conjecture concerning when the discriminant of an irreducible monic integral polynomial is square-free and some computational evidence for it.

1. INTRODUCTION

This paper arose out of a search for S_5-extensions of $\mathbb{Q}$ with small discriminant, performed by the first and third authors. Using `PARI`, they made lists of irreducible monic integral quintic polynomials f and computed both the polynomial discriminant $D_{\mathrm{pol}}(f)$ and the absolute discriminant of the splitting field $D_{\mathrm{field}}(f)$. They noticed that these two discriminants were equal far more often than expected.

Call an irreducible monic integral polynomial f *essential* if $D_{\mathrm{pol}}(f) = D_{\mathrm{field}}(f)$. It is well known that this implies that the ring of integers of the splitting field of f is monogenic.

In reply to an inquiry, Hendrik Lenstra suggested the following:

Conjecture 1.1. *Let $n \geq 2$. The probability that a random irreducible monic integral polynomial of degree n and height $\leq X$ is essential should tend to $6/\pi^2$ as $X \to \infty$.*

For any irreducible monic integral polynomial f, $D_{\mathrm{pol}}(f)/D_{\mathrm{field}}(f)$ is a square integer. Hence, f is essential if $D_{\mathrm{pol}}(f)$ is square-free. However, this square-freeness does not account for 100% of essential polynomials, probabilistically speaking.

In Section 3, we present a heuristic argument for Conjecture 1.1 due to Lenstra, who kindly communicated it to us via email in October 2004. In Section 4, we ask, when does a random polynomial have square-free discriminant? A conjecture of Bjorn Poonen suggests that

2000 AMS Subject Classification: Primary 11R29; Secondary 11C08

Keywords: Discriminant, polynomial, number field, monogenic, square-free, Dedekind's criterion

1058-6458/2007 $0.50 per page

for a fixed degree, there should be an asymptotic probability for this. In the appendix (Section 6), the second author gives a precise conjecture for the value of this probability. Unlike Conjecture 1.1, this probability depends on the degree of the polynomial.

In Section 5 and the appendix we present our experimental evidence, gathered using PARI and MAGMA, where we studied polynomials whose degrees ranged from 2 to 7. This evidence supports our conjectures.

2. PROBABILITY

In this paper we deal with two kinds of probability that are easily related. First, let n, N be positive integers and let $\mathbb{Z}/N\mathbb{Z}[x]_n$ denote the set of all monic polynomials in $\mathbb{Z}/N\mathbb{Z}[x]$ of degree n.

Suppose $Q(f)$ is a predicate of a monic polynomial f of degree n in $\mathbb{Z}/N\mathbb{Z}[x]$. For example, Q might be the property that f is irreducible.

Define the probability that f possesses Q to be

$$\frac{\#\{\ f \in \mathbb{Z}/N\mathbb{Z}[x]_n \mid f \text{ has } Q\ \}}{\#\mathbb{Z}/N\mathbb{Z}[x]_n}.$$

Now let $R(T)$ be a predicate of an irreducible monic polynomial T of degree n in $\mathbb{Z}[x]$. Define the height $h(T)$ to be the maximum of the absolute values of the coefficients of T. Let $B_n(X)$ be the set of all monic, irreducible T of degree n with $h(T) \le X$. Then we define the probability that T has R to be

$$\lim_{X\to\infty} \frac{\#\{\ T \in B_n(X)\ \mid T \text{ has } R\ \}}{\#B_n(X)}.$$

We make a similar definition for all polynomials (not necessarily irreducible) in a similar way.

We have the following lemma:

Lemma 2.1. *Let n, N be positive integers and Q, R predicates as above. Suppose $R(T) = Q(T \bmod N)$. Then the probability that $T \bmod N$ has Q equals the probability that T has R.*

Proof: Easy, given the fact that the probability that a monic integral polynomial of degree n is irreducible equals 1 [van der Waerden 34]. □

3. LENSTRA'S HEURISTIC ARGUMENT

Let p be a prime number, K a number field, and A a sublattice of finite index of the ring of integers $\mathcal{O}_K$ of K. We say that A is *p-maximal* if p does not divide the index of A in $\mathcal{O}_K$.

Let $T \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with root θ and $K = \mathbb{Q}[\theta]$. It is well known that the polynomial discriminant of T equals the field discriminant of K if and only if $\mathbb{Z}[\theta]$ is p-maximal for every prime p. (See, for example, [Lang 70, Proposition 16 and Remark 1, Section 3.3].) We call such a T *essential*. Of course, if T is essential, $\mathcal{O}_K$ is monogenic, i.e., $\mathcal{O}_K$ is generated as a ring over $\mathbb{Z}$ by a single element.

We wish to determine the probability (as defined in Section 2.1) that an irreducible monic T of degree n is essential. Obviously, if $n = 1$ this probability is 1. It will turn out that for $n \ge 2$, the probability we conjecture is independent of n. Start with Dedekind's criterion, as found, for example, in [Cohen 95, Section 6.1.2], as part (2) of Theorem 6.1.4.

Denote reduction modulo p by an overbar.

Lemma 3.1. (Dedekind's criterion.) *Let $T \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with root θ and $K = \mathbb{Q}[\theta]$. Let p be a prime number. Let*

$$\bar{T} = \prod \bar{t}_i^{e_i}$$

be the factorization of $\bar{T}$ into monic irreducible polynomials in $\mathbb{F}_p[x]$, where the $t_i \in \mathbb{Z}[x]$ are arbitrary monic lifts of the $\bar{t}_i$. Let

$$g = \prod t_i, \quad h = \prod t_i^{e_i - 1},$$

so that $h \in \mathbb{Z}[x]$ is a monic lift of $\bar{T}/\bar{g}$. Set $f = (gh - T)/p \in \mathbb{Z}[x]$. Then $\mathbb{Z}[\theta]$ is p-maximal if and only if

$$(\bar{f}, \bar{g}, \bar{h}) = 1$$

in $\mathbb{F}_p[x]$.

From this we can derive the following corollary:

Corollary 3.2. *With notation as above, $\mathbb{Z}[\theta]$ is p-maximal if and only if ($\star$) there does not exist a monic polynomial $u \in \mathbb{Z}[x]$ such that $\bar{u}$ is irreducible in $\mathbb{F}_p[x]$ and $T \in (p^2, pu, u^2) \subset \mathbb{Z}[x]$.*

Proof: First suppose that $\mathbb{Z}[\theta]$ is not p-maximal. Then $\bar{f}, \bar{g}, \bar{h}$ have a common factor, which without loss of generality is $\bar{t}_1$. Therefore $e_1 > 1$. Set $u = t_1$. Then $T = gh - pf = \prod t_i^{e_i} - pf$. Since $\bar{u}$ divides $\bar{f}$, we have $au = f + pb$ for some integral polynomials a, b. Hence $pf \in (p^2, pu)$ and $T \in (p^2, pu, u^2)$. Conversely, let u be

as in the statement of the corollary. Then $\bar{T} \in (\bar{u}^2)$. Without loss of generality, $u = t_1$ and $e_1 > 1$. Then $\bar{u}$ divides $\bar{g}$ and $\bar{h}$. Now there are integral polynomials a, b, c such that $T = p^2a + pub + u^2c$. Therefore, $f = (gh - T)/p = -pa - ub + u^2(\frac{g}{u}\frac{h}{u} - c)/p$. By Gauss's lemma, p must divide $\left(\frac{g}{u}\frac{h}{u} - c\right)$. It follows that $\bar{u}$ also divides $\bar{f}$. □

Continuing with the heuristic, we note that the probability that a monic integral polynomial T satisfies $(\star)$ is independent of whether T is irreducible. This is because the probability that T is irreducible is 1 [van der Waerden 34]. We can then compute that probability as follows: First note that $(\star)$ depends on T only modulo p^2. Let $R = (\mathbb{Z}/p^2\mathbb{Z})[x]$. For each positive integer i, let R_i denote the set of polynomials in R of degree $\leq i$ and let R_i^{monic} be the subset of monic polynomials of degree i. For any $g \in R$ denote by I_g the ideal (g^2, pg), $I_{g,n} = I_g \cap R_n$, and $I_{g,n}^{\text{monic}} = I_g \cap R_n^{\text{monic}}$. Note that each of these sets depends only on $\bar{g}$.

Lemma 3.3. *Let g, h be monic polynomials in R of degrees d, e respectively such that $\bar{g}$ and $\bar{h}$ are both square-free and relatively prime. Then $I_{g,n} \cap I_{h,n} = I_{gh,n}$.*

Proof: If $f \in I_{g,n} \cap I_{h,n}$, then $f = ag^2 + pbg$ and $f = Ah^2 + pBh$ for some polynomials a, b, A, B. Then $\bar{f} = \bar{a}\bar{g}^2 = \bar{A}\bar{h}^2$, and hence $\bar{f}$ is equal to $\bar{C}\overline{(gh)}^2$ for some polynomial C.

Therefore $f - C(gh)^2 = pk$ for some polynomial k. Then

$$k = \frac{ag^2 + pbg - Cg^2h^2}{p} = \frac{(a - Ch^2)g^2}{p} + bg.$$

Since g is monic, this implies that p divides $a - Ch^2$ and thus that $\bar{k}$ is divisible by $\bar{g}$. Similarly, $\bar{k}$ is divisible by $\bar{h}$. It follows that $f = C(gh)^2 + pD(gh)$ for some polynomial D, and so $f \in I_{gh,n}$. The converse is obvious. □

Proposition 3.4. *Let $g_1, \ldots, g_k$ be monic polynomials in R such that the $\bar{g}_i$ are all irreducible and distinct. Let d be the sum of their degrees. Let $f \in R_n^{\text{monic}}$ be randomly chosen. Then the probability $P(g_1, \ldots, g_k)$ that $f \in I_{g_1,n}^{\text{monic}} \cap \cdots \cap I_{g_k,n}^{\text{monic}}$ is 0 if $2d > n$ and p^{-3d} otherwise.*

Proof: Let $g = g_1 \cdots g_k$. Then $I_{g_1,n}^{\text{monic}} \cap \cdots \cap I_{g_k,n}^{\text{monic}} = I_{g_1,n} \cap \cdots \cap I_{g_k,n} \cap R_n^{\text{monic}} = I_{g,n}^{\text{monic}}$, since by Lemma 3.3 we have that $I_{g_1,n} \cap \cdots \cap I_{g_k,n} = I_{g,n}$.

We must show that the cardinality of $I_{g,n}^{\text{monic}}$ is 0 if $2d > n$ and p^{2n-3d} otherwise. If $f = ag^2 + pbg$ for some a, b, since f and g are monic, looking modulo p we see that $2d \leq n$. So we may assume from now on that $2d \leq n$.

Define a map of sets

$$\phi : \bar{R}_{n-2d}^{\text{monic}} \times \bar{R}_{n-d-1} \to I_{g,n}^{\text{monic}}$$

as follows: For each $\alpha \in \bar{R}_{n-2d}^{\text{monic}}$ fix a lift $a(\alpha) \in R_{n-2d}^{\text{monic}}$ and for each $\beta \in \bar{R}_{n-d-1}$ fix a lift $b(\beta) \in R_{n-d-1}$. Set $\phi(\alpha, \beta) = a(\alpha)g^2 + pb(\beta)g$. We will show that ϕ is bijective.

1. ϕ is injective: If $a(\alpha)g^2 + pb(\beta)g = a(\alpha')g^2 + pb(\beta')g$, then $\bar{a}(\alpha) = \bar{a}(\alpha')$, which means that $\alpha = \alpha'$. Then $pb(\beta)g = pb(\beta')g$ so $b(\beta)g = b(\beta')g + pk$ for some polynomial k, and hence $\bar{b}(\beta) = \bar{b}(\beta')$, which means that $\beta = \beta'$.

2. ϕ is surjective: Let $f = ag^2 + pbg$ for some a, b, where f is monic. Since $\bar{a}$ must be monic of degree $n-2d$, we may write $a = a' + pb'$, where a' is itself monic of degree $n - 2d$. By adding $b'g$ to b we may thus assume that a is already monic of degree $n - 2d$ and (since we can add p times any polynomial we like to b) that the degree of b is $n - d$ or less.

Let b_* be the coefficient of x^{n-d} in b. Then $f = ag^2 + pb_*x^{n-d}g + p(b - b_*x^{n-d})g$. Now $p(b - b_*x^{n-d})g$ has degree less than n, so that $ag^2 + pb_*x^{n-d}g$ must be monic of degree n. Then $\bar{a}$ is monic of degree $n - 2d$, so that $a = a(\alpha) + pk$ for some α and some polynomial k of degree $n - 2d$ or less. Therefore $f = a(\alpha)g^2 + p(b + kg)g$.

Since $f, g, a(\alpha)$ are all monic, the coefficient of x^{n-d} in $b + kg$ (which has degree $n - d$ or less) must be divisible by p. Therefore $\overline{(b + kg)} = \beta$ for some β in $\bar{R}_{n-d-1}$ and $p(b + kg) = pb(\beta)$. Therefore $f = a(\alpha)g^2 + pb(\beta)g$ is in the image of ϕ. It now follows easily that $P(g_1, \ldots, g_k) = p^{-3d}$ if $2d \leq n$. □

Proposition 3.5. *Let P_n denote the probability that an element of R_n^{monic} is not in $I_{g,n}$ for any $g \in R$ such that $\bar{g}$ is irreducible. Then if $n \geq 2$, $P_n = 1 - p^{-2}$.*

Proof: Let $H(t) = \sum_{n \geq 0} P_n t^n$. To evaluate this using our previous results, consider

$$K(t) = (1 - t)^{-1} \prod_{\gamma} \left(1 - \frac{t^{2d(\gamma)}}{p^{3d(\gamma)}}\right),$$

where the product runs over all irreducible monic γ in $\bar{R}$ and $d(\gamma)$ denotes the degree of γ. The coefficient of t^n in $K(t)$ is

$$\sum_{k \geq 0} \sum_{\gamma_1, \ldots, \gamma_k} (-1)^k p^{-3d},$$

where the inner sum runs over k-tuples of γ's such that $2d = 2d(\gamma_1) + \cdots + 2d(\gamma_k) \leq n$.

By Proposition 3.4, using the usual inclusion–exclusion rule for independent events, we see that the double sum equals P_n. So $H(t) = K(t)$.

On the other hand, let $Z(u) = \frac{1}{1-pu}$ be the zeta function of $Y = \mathrm{Spec}\mathbb{F}_p[x]$. Defining s by the equation $u = p^{-s}$, the Euler product for the zeta function gives

$$Z(u) = \prod_y (1 - N(y)^{-s})^{-1},$$

where the product is taken over all the closed points y of Y. If y corresponds to the irreducible polynomial γ of degree $d(\gamma)$, its norm is given by $N(y) = p^{d(\gamma)}$. Thus

$$Z(u) = \prod_\gamma \left(1 - p^{-d(\gamma)s}\right)^{-1} = \prod_\gamma \left(1 - u^{d(\gamma)}\right)^{-1}.$$

Hence as formal power series, we have

$$1 - pu = \prod_\gamma \left(1 - u^{d(\gamma)}\right).$$

Setting $u = t^2/p^3$ we obtain

$$1 - \frac{t^2}{p^2} = \prod_\gamma \left(1 - \frac{t^{2d(\gamma)}}{p^{3d(\gamma)}}\right).$$

Thus

$$H(t) = (1-t)^{-1}\left(1 - \frac{t^2}{p^2}\right)$$

and the coefficient P_n of t^n is $1 - p^{-2}$ if $n \geq 2$. □

Finally, we assume that the probabilities that $\mathbb{Z}[\theta]$ is p-maximal, for varying p's, are independent. Applying this assumption to Corollary 3.2 and Proposition 3.5, we obtain our Conjecture 1.1, which we can restate as follows:

Conjecture *The probability that an irreducible monic integral polynomial T of degree $n \geq 2$ with root θ has its polynomial discriminant equal to the discriminant of the number field $\mathbb{Q}(\theta)$ exists and equals $\prod_p (1 - p^{-2}) = 6/\pi^2$.*

4. SQUARE-FREENESS OF POLYNOMIAL DISCRIMINANTS

It might be thought that the reason Conjecture 1.1 should be true is that almost all polynomials might have square-free discriminant, since the probability that a random integer is square-free is known to be $6/\pi^2$. For if the irreducible, monic, integral polynomial $T(x)$ has discriminant $D(T)$ and the field discriminant of $\mathbb{Q}[x]/(T)$ is D, then it is well known that $D(T)/D$ is an integral square. (See, for example, [Lang 70, Section 3.3].)

Section 6 presents a conjecture and numerical evidence for the value of the probability that a random polynomial of fixed degree has square-free discriminant. This result denies the "thought" of the previous paragraph.

We remark that the existence of such a probability is consistent with general results of Bjorn Poonen, where the abc conjecture implies that there is a well-defined density P_n for the set of integral, monic polynomials T of fixed degree n with square-free discriminant. The formula for the density is given by [Poonen 03, Theorem 3.2], applied to the discriminant viewed as a polynomial in the coefficients of T. Of course, there is no easy way to evaluate Poonen's formula directly.

5. EXPERIMENTAL EVIDENCE

The data in Table 1 below were generated (using `PARI`) from random samples of one million polynomials per degree, chosen uniformly from a box of prescribed coefficient height 10,000. The polynomials were first checked for reducibility, and then the irreducible polynomials had their fields and polynomial discriminants compared. The last column shows the experimental value minus the expected value $6/\pi^2 \approx 0.6079271$ divided by the standard deviation. (The standard deviation σ is computed in the usual way for a binomial distribution with N trials assuming $p = 6/\pi^2$. That is, $\sigma = \sqrt{p(1-p)/N}$, which in our case is ≈ 0.00049.)

Degree	Percent Coincidence	Error/Standard Deviation
2	0.608356	0.8797
3	0.608551	1.2777
4	0.607761	−0.3391
5	0.607229	−1.4289
6	0.607297	−1.2908
7	0.607995	0.0443

TABLE 1.

6. APPENDIX: SQUARE-FREE DISCRIMINANTS

Let p be a prime and let I be the set of monic irreducible elements of $\mathbb{Z}/p\mathbb{Z}[X]$. If $f \in \mathbb{Z}_p[X]$ is a monic polynomial, then we can write $f \bmod p = \prod_{g\in I} g^{e_g}$. Using Hensel's lemma [Weiss 63, 2.2.1] we can write $f = \prod_{g\in I} f_g$, where $f_g \in \mathbb{Z}_p[X]$ is monic and satisfies $f_g = g^{e_g} \bmod p$. Recall that we let D_{pol} denote the polynomial discriminant and we denote reduction modulo p by an overbar.

Denote by $R(f,g)$ the resultant of f and g.

Lemma 6.1. *Let $f, g \in \mathbb{Z}_p[X]$, with f monic. If $\gcd(\bar{f}, \bar{g}) = 1$, then $\mathrm{ord}_p R(f,g) = 0$.*

Proof: Write $\bar{f} = (X-t_1)\cdots\cdots(X-t_n)$, with the t_i in some algebraic closure of $\mathbb{F}_p$. From the proof of [Lang 93, Section IV.8, Proposition 8.3] we have $R(\bar{f},\bar{g}) = \prod_{i=1}^{n} \bar{g}(t_i)$. Now $p \mid R(f,g)$ if and only if $R(\bar{f},\bar{g}) = 0$, so $\bar{g}(t_i) = 0$ for some t_i, i.e., if t_i is a zero of $\bar{g}$. □

Corollary 6.2. *Let $f, g \in \mathbb{Z}_p[X]$ be monic. If $\gcd(\bar{f},\bar{g}) = 1$, then $\operatorname{ord}_p(D_{\mathrm{pol}}(fg)) = \operatorname{ord}_p(D_{\mathrm{pol}}(f)) + \operatorname{ord}_p(D_{\mathrm{pol}}(g))$.*

Proof: This follows from

$$D_{\mathrm{pol}}(fg) = D_{\mathrm{pol}}(f) D_{\mathrm{pol}}(g) R(f,g)^2$$

and Lemma 6.1. □

Corollary 6.3. *Let $f \in \mathbb{Z}_p[X]$ be monic. If $\bar{f}$ is irreducible, then $\operatorname{ord}_p(D_{\mathrm{pol}}(f)) = 0$.*

Proof: This follows from using Lemma 6.1 with $g = f'$ and from [Lang 93, Section IV.8, Proposition 8.5]. □

Proposition 6.4. *Let $P_{n,0}$ denote the probability that a monic polynomial $f \in \mathbb{Z}_p[X]$ of degree n satisfies $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 0$. If $n \le 1$, then $P_{n,0} = 1$ and if $n \ge 2$, then $P_{n,0} = 1 - p^{-1}$.*

Proof: Let $H(t) = \sum_{n\ge 0} P_{n,0} t^n$. From Lemma 6.1 and its corollaries, we see that whether the polynomial f satisfies $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 0$ depends only on f modulo p. We have $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 0$ if and only if for all $g \in I$ we have $e_g = 0$ or 1, i.e., if and only if $\bar{f}$ is square-free.

Denote by M the set of monic polynomials in $\mathbb{Z}/p\mathbb{Z}[X]$. From unique factorization in $\mathbb{Z}/p\mathbb{Z}[X]$ we have the following formula:

$$\sum_{f\in M} u^{\deg f} = \prod_{g\in I} \sum_{k\ge 0} u^{k \deg g}.$$

Taking square-free parts left and right and replacing u by t/p, we obtain

$$H(t) = \prod_{g\in I} \left(1 + \left(\frac{t}{p}\right)^{\deg g}\right).$$

Now,

$$\begin{aligned}\frac{1}{1-t} = \sum t^n &= \prod_g \sum_{i\ge 0} \left(\frac{t}{p}\right)^{i \deg g}, \\ &= \prod_g \frac{1}{1-(t/p)^{\deg g}} = \prod_g \frac{1+(t/p)^{\deg g}}{1-(t^2/p^2)^{\deg g}}, \\ &= H(t)\frac{1}{1-t^2/p}.\end{aligned}$$

So $H(t) = (1-t)^{-1}\left(1-\frac{t^2}{p}\right)$. The coefficient $P_{n,0}$ of t^n is 1 if $n \le 1$ and $1-p^{-1}$ otherwise. □

Lemma 6.5. *Let R be a ring and $r \in R[X]$ a monic polynomial. Denote by $\Omega_{(R[X]/(r))/R}$ the module of Kähler differentials of $R[X]/r$ over R. Then $\Omega_{(R[X]/r)/R} \cong R[X]/(r, r')$.*

Proof: Follows from [Matsumura 70, Section 10.26] □

Write $l(L)$ for the length of a finite-length $\mathbb{Z}_p$-module L, and set $e(\psi, L) = l(\operatorname{cok}(\psi)) - l(\ker(\psi))$ for a $\mathbb{Z}_p$-module endomorphism $\psi : L \to L$.

Lemma 6.6. *Let $f \in \mathbb{Z}_p[X]$ be monic and $h \in I$. Then $\operatorname{ord}_p D_{\mathrm{pol}}(f_h) \ge (e_h - 1)\deg h$. If also $p \mid e_h$, then*

$$\operatorname{ord}_p D_{\mathrm{pol}}(f_h) \ge e_h \deg h.$$

Proof: Let

$$\begin{aligned}\phi : \mathbb{Z}_p[X]/f_h &\to \mathbb{Z}_p[X]/f_h, \\ x &\mapsto f_h' x,\end{aligned}$$

be multiplication by f_h'. Then

$$\operatorname{cok}(\phi) = \mathbb{Z}_p[X]/(f_h, f_h') = \Omega_{(Z_p[X]/f_h)/Z_p}$$

(Lemma 6.5).

From [Fulton 70, Lemma A.2.6] we get that

$$e(\phi, \mathbb{Z}_p[X]/f_h) = e(\det(\phi), \mathbb{Z}_p),$$

and from [Fulton 70, Example A.2.1], we get

$$\det(\phi) = R(f_h, f_h') = D_{\mathrm{pol}}(f_h).$$

We have

$$p^{\operatorname{ord}_p D_{\mathrm{pol}}(f_h)} = p^{e(\det(\phi),\mathbb{Z}_p)} \ge \#\Omega_{(\mathbb{Z}_p[X]/f_h)/\mathbb{Z}_p}.$$

The map

$$\begin{aligned}\Omega_{(\mathbb{Z}_p[X]/(f_h))/\mathbb{Z}_p} &\to \Omega_{(\mathbb{F}_p[X]/(f_h))/\mathbb{F}_p}, \\ dg &\mapsto d\bar{g},\end{aligned}$$

is surjective, so

$$\begin{aligned}\#\Omega_{(\mathbb{Z}_p[X]/f_h)/\mathbb{Z}_p} &\ge \#\Omega_{(\mathbb{F}_p[X]/(f_h))/\mathbb{F}_p} \\ &= \#\mathbb{F}_p[X]/(f_h, f_h') \\ &= \begin{cases} \#\mathbb{F}_p[X]/(h^{e_h}) = p^{e_h \deg(h)} & \text{if } p \mid e_h, \\ \#\mathbb{F}_p[X]/(h^{e_h-1}) = p^{(e_h-1)\deg(h)} & \text{otherwise,}\end{cases}\end{aligned}$$

which completes the proof. □

Proposition 6.7. *A monic polynomial $f \in \mathbb{Z}_p[X]$ satisfies $\operatorname{ord}_p D_{\mathrm{pol}}(f) = 1$ if and only if the following conditions are met:*

(i) $p \neq 2$;

(ii) *there is a unique $h \in I$ for which $e_h \geq 2$;*

(iii) *for this h we have $\deg h = 1$ and $e_h = 2$;*

(iv) *if $h = X - \widetilde{\alpha}$ and α is any lift of $\widetilde{\alpha}$ to $\mathbb{Z}_p$, then $f_h(\alpha) \not\equiv 0 \bmod p^2$.*

Proof: Let I' be the set of all $g \in I$ with $e_g \geq 2$. From Lemma 6.1, its corollaries, and Lemma 6.6, we see that

$$\operatorname{ord}_p(D_{\mathrm{pol}}(f)) = \sum_{g \in I'} \operatorname{ord}_p(D_{\mathrm{pol}}(f_g)) \geq \sum_{g \in I'} (e_g - 1) \deg g.$$

This can equal 1 only if $\#I' = 1$ and the only $h \in I'$ satisfies $\deg h = 1$ and $e_h = 2$. Furthermore, if $p = 2$, then $\operatorname{ord}_p(D_{\mathrm{pol}}(f)) \geq e_h \deg h = 2$. So $p \neq 2$.

If f satisfies conditions (i)–(iii), then there are $b, c \in p\mathbb{Z}_p$ such that $f_h = (X - \alpha)^2 + b(X - \alpha) + c$ and $\operatorname{ord}_p(D_{\mathrm{pol}}(f_h)) = \operatorname{ord}_p(b^2 - 4c)$, which is 1 if and only if $\operatorname{ord}_p(c) = 1$, independently of the choice of the lift α. □

Theorem 6.8. *Let $P_{n,1}$ denote the probability that a monic polynomial $f \in \mathbb{Z}_p[X]$ of degree n satisfies $\operatorname{ord}_p(D_{\mathrm{pol}}(f)) = 1$. The following table gives $P_{n,1}$ for various n and p.*

	$p = 2$	$p \neq 2$
$n = 2$	0	$p^{-1} - p^{-2}$
$n = 3$	0	$p^{-1} - 2p^{-2} + p^{-3}$
$n \geq 4$	0	$(p-1)^2(1 - (-p)^{-n})/(p^2(p+1))$

Proof: From Proposition 6.7 we see that whether f satisfies $\operatorname{ord}_p(D_{\mathrm{pol}}(f)) = 1$ depends only on f modulo p^2. So we have

$$P_{n,1} = \frac{1}{p^{2n}} \#\{f \in \mathbb{Z}/p^2\mathbb{Z}[X] : f \text{ monic}, \ \deg f = n, \ \operatorname{ord}_p(D_{\mathrm{pol}}(f)) = 1\}.$$

If $p = 2$, then Proposition 6.7 tells us that the discriminant being square-free is the same as it being a unit, so $P_{n,1} = 0$.

Now let $p \neq 2$ and let $H(t) = \sum_{n \geq 0} P_{n,1} t^n$. Let $N = \{f \in \mathbb{Z}/p^2\mathbb{Z}[X] : f \text{ monic}\}$ and $N' = \{f \in N : \operatorname{ord}_p(D_{\mathrm{pol}}(f)) = 1\}$. For $h \in I$ linear, let

$$N_h = \{f \in N : \operatorname{ord}_p D_{\mathrm{pol}}(f_h) = 1\},$$
$$N_{h,1} = \{f \in N : h^2 = \bar{f}, \ f(\alpha) \neq 0\},$$
$$N_{h,2} = \{f \in N : \operatorname{ord}_p D_{\mathrm{pol}}(f) = 0, \ h \nmid \bar{f}\}.$$

Then $N' = \cup_{h \in I, \deg h = 1} N_h$, and for all h we have a bijection

$$N_h \to N_{h,1} \times N_{h,2},$$
$$f \mapsto (f_h, f/f_h).$$

So we have the following generating function:

$$\begin{aligned}
&\sum_{n \geq 0} P_{n,1} p^{2n} u^n \\
&\quad = \sum_{f \in N'} u^{\deg f} = \sum_{h \in I, \deg h = 1} \sum_{f \in N_h} u^{\deg f} \\
&\quad = \sum_{h \in I, \deg h = 1} \Big(\Big(\sum_{f \in N_{h,1}} u^{\deg f} \Big) \Big(\sum_{f \in N_{h,2}} u^{\deg f} \Big) \Big) \\
&\quad = \sum_{h \in I, \deg h = 1} p\,(p-1)\,u^2 \prod_{g \in I, g \neq h} \left(1 + (pu)^{\deg g}\right),
\end{aligned}$$

where we have used Proposition 6.7 and the proof of Proposition 6.4 for the last step.

Setting $u = t/p^2$, we obtain

$$H(t) = \sum_{h \in I, \deg h = 1} t^2 \Big(\frac{p-1}{p^3}\Big) \prod_{g \in I, g \neq h} \left(1 + \Big(\frac{t}{p}\Big)^{\deg g}\right).$$

By rewriting this formula and using Proposition 6.4 we obtain

$$\begin{aligned}
H(t) &= pt^2 \left(\frac{p-1}{p^3}\right) \left(1 + \frac{t}{p}\right)^{-1} \prod_{g \in I} \left(1 + \left(\frac{t}{p}\right)^{\deg g}\right) \\
&= t^2 \left(\frac{p-1}{p^2}\right) \left(1 + \frac{t}{p}\right)^{-1} (1-t)^{-1} \left(1 - \frac{t^2}{p}\right) \\
&= t^2 \frac{p-1}{p^2(p+1)} \left(\frac{p - t^2}{1-t} + \frac{1 - \frac{t^2}{p}}{1 + \frac{t}{p}}\right),
\end{aligned}$$

and the coefficient of t^n is given by

$$P_{n,1} = \begin{cases} \frac{p-1}{p^2(p+1)}(p+1), & n = 2, \\ \frac{p-1}{p^2(p+1)}(p - \frac{1}{p}), & n = 3, \\ \frac{p-1}{p^2(p+1)} \left(p - 1 + \left(\frac{-1}{p}\right)^{n-2} + (\frac{-1}{p})^{n-3}\right), & n \geq 4. \end{cases}$$

□

By combining Proposition 6.4 and Theorem 6.8, we obtain the probability that $\operatorname{ord}_p D_{\mathrm{pol}}(f) \leq 1$:

	$p = 2$	$p \neq 2$
$n = 2$	$\frac{1}{2}$	$1 - \frac{1}{p^2}$
$n = 3$	$\frac{1}{2}$	$1 - \frac{2}{p^2} + \frac{1}{p^3}$
$n \geq 4$	$\frac{1}{2}$	$(1 - \frac{1}{p}) + \frac{(p-1)^2(1-(-p)^{-n+2})}{(p^2(p+1))}$

If we assume that all these probabilities are independent, then we obtain a heuristic for the probability that

degree	heuristic value	experimental value	error/s.d.
2	0.4052847	0.404588	−1.4191
3	0.3425997	0.342442	−0.3323
4	0.2997226	0.299933	0.4593
5	0.3090905	0.309574	1.0463
6	0.3064416	0.305986	−0.9883
7	0.3072498	0.307041	−0.4526

TABLE 2.

a polynomial $f \in \mathbb{Z}[X]$ has square-free discriminant, by taking the product over all p.

For $2 \le n \le 7$, Table 2 gives approximations for the heuristic probability. It is obtained by calculating the product for primes up to one million. It also gives experimental values, which were obtained as the fraction of polynomials with square-free discriminant out of a random set of one million polynomials of height at most 10,000. In the last column the experimental value is compared to the heuristic value and then divided by the standard deviation.

For $n = 2$ we can calculate the heuristic probability exactly. It is

$$\frac{1}{2}\prod_{p\neq 2}\left(1-\frac{1}{p^2}\right) = \frac{2}{3}\prod_{p}\left(1-\frac{1}{p^2}\right) = \frac{4}{\pi^2}.$$

The following theorem proves that this value is in fact correct.

Theorem 6.9. *The probability that a random monic polynomial in $\mathbb{Z}[X]$ of degree 2 has square-free discriminant is $4/\pi^2$. More exactly,*

$$\begin{aligned}\lim_{x\to\infty} &\#\{(b,c) \in ([-x,x]\times[-x,x]) \cap (\mathbb{Z}\times\mathbb{Z}) : \\ &\qquad D_{\mathrm{pol}}(X^2+bX+c) \text{ is square-free}\} \\ &= \frac{4}{\pi^2}(2x)^2 + O(x^{7/4}).\end{aligned}$$

Proof: Write

$$\begin{aligned}P(x) = \#\{(b,c) \in ([-x,x]\times[-x,x]) \cap (\mathbb{Z}\times\mathbb{Z}) : \\ D_{\mathrm{pol}}(X^2+bX+c) \text{ is square-free}\}.\end{aligned}$$

If b is even, then $D_{\mathrm{pol}}(X^2+bX+c) = b^2-4c = 0 \bmod 4$, so we need to consider only odd b. Since $D_{\mathrm{pol}}(X^2+bX+c)$ is square-free if and only if $D_{\mathrm{pol}}(X^2-bX+c)$ is square-free, it suffices to count the case in which $b > 0$ twice. So we have

$$\begin{aligned}P(x) = 2\#\{(d,c) \in ([0,(x-1)/2]\times[-x,x]) \cap (\mathbb{Z}\times\mathbb{Z}) : \\ (2d+1)^2 - 4c \text{ is square-free}\}.\end{aligned}$$

Now we can use inclusion–exclusion. Since $|(2d+1)^2 - 4c| \le x^2+4x < (x+2)^2$, it suffices to do the inclusion–exclusion up to $x+2$. We have already dealt with the even n, so the inclusion–exclusion needs to be done only over the odd n. Let $\mu(n)$ denote the Möbius function. Then we have

$$P(x) = 2\sum_{\substack{n=1\\ n \text{ odd}}}^{x+2} \mu(n)A(n),$$

where

$$\begin{aligned}A(n) = \#\{(d,c) \in ([0,(x-1)/2]\times[-x,x]) \cap (\mathbb{Z}\times\mathbb{Z}) : \\ (2d+1)^2 - 4c = 0 \bmod n^2\}.\end{aligned}$$

We split this sum into two parts:

$$Q_1(x) = 2\sum_{\substack{n=1\\ n \text{ odd}}}^{x^{3/4}} \mu(n)A(n)$$

and

$$Q_2(x) = 2\sum_{\substack{n=x^{3/4}\\ n \text{ odd}}}^{x+2} \mu(n)A(n).$$

For the first part we observe that we have an element in the set only if $c = 4^{-1}(2d+1)^2 \bmod n^2$. So the number of c is $\left\lfloor \frac{2x+1}{n^2} \right\rfloor$ or this number plus 1. Then we sum over all d to get

$$Q_1(x) = 2\sum_{\substack{n=1\\ n \text{ odd}}}^{x^{3/4}} \mu(n)\left\lfloor \frac{x+1}{2} \right\rfloor \left(\frac{2x+1}{n^2} + B(n)\right),$$

where $|B(n)| \le 1$. Now, $\left\lfloor \frac{x+1}{2} \right\rfloor \left(\frac{2x+1}{n^2}\right) = \frac{x^2}{n^2} + O(x)$.

Furthermore,

$$\sum_{\substack{n=1\\ n \text{ odd}}}^{x^{3/4}} |\mu(n)\left\lfloor \frac{x+1}{2} \right\rfloor B(n)| < \sum_{\substack{n=1\\ n \text{ odd}}}^{x^{3/4}} \left\lfloor \frac{x+1}{2} \right\rfloor = O(x^{7/4}).$$

So

$$Q_1(x) = 2\sum_{\substack{n=1\\ n \text{ odd}}}^{x^{3/4}} \mu(n)\frac{x^2}{n^2} + O(x^{7/4}).$$

To count $Q_2(x)$, we observe that since $(2d+1)^2 - 4c \neq 0$, we need $(2d+1)^2 \ge n^2 + 4c \ge x^{6/4} - 4x$, which can

happen only if $d \geq \frac{1}{2}x^{3/4} - x^{1/4} - 1$. So when d is large enough to get a solution, the difference between $(2(d+1)+1)^2$ and $(2d+1)^2$ is at least $4x^{3/4} - 8x^{1/4}$, which is greater than $x^{3/4}$, for x sufficiently large. Around every multiple of n^2 we have an interval of length $8x$ in which $(2d+1)^2$ must lie for solutions to occur. The number of d that can lie in such an interval is at most $8x/x^{3/4} + 1 = 8x^{1/4} + 1$, and the number of intervals is at most $x^2/n^2 + 1 \leq x^{2/4} + 1$. So per n, the number of solutions is at most $8x^{3/4} + O(x^{2/4})$. So

$$\begin{aligned} Q_2(x) &\leq 2 \sum_{\substack{n=x^{3/4} \\ n \text{ odd}}}^{x+2} (8x^{3/4} + O(x^{2/4})) < 16x^{7/4} + O(x^{6/4}) \\ &= O(x^{7/4}). \end{aligned}$$

Now we have

$$P(x) = 2 \sum_{\substack{n=1 \\ n \text{ odd}}}^{x^{3/4}} \mu(n) \frac{x^2}{n^2} + O(x^{7/4}).$$

We use that

$$\sum_{\substack{n=x^{3/4} \\ n \text{ odd}}}^{\infty} x^2 \frac{\mu(n)}{n^2} \leq \int_{x^{3/4}-1}^{\infty} \frac{x^2}{t^2} dt = \frac{x^2}{(x^{3/4}-1)} = O(x^{5/4})$$

to conclude that

$$P(x) = 2x^2 \sum_{\substack{n=1 \\ n \text{ odd}}}^{\infty} \frac{\mu(n)}{n^2} + O(x^{7/4}).$$

Since

$$\sum_{\substack{n=1 \\ n \text{ even}}}^{\infty} \frac{\mu(n)}{n^2} = \sum_{m=1}^{\infty} \frac{\mu(2m)}{(2m)^2} = -\frac{1}{4} \sum_{\substack{m=1 \\ n \text{ odd}}}^{\infty} \frac{\mu(m)}{m^2}$$

and

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2},$$

we obtain

$$P(x) = 4x^2 \frac{4}{\pi^2} + O(x^{7/4}),$$

and the proof is complete. □

ACKNOWLEDGMENTS

We wish to thank the following individuals whom we consulted when we were at the beginning of this project: Manjul Bhargava, Henri Cohen, Keith Conrad, Darrin Doud, William Duke, Farshid Hajir, Roger Heath-Brown, John Jones, Hugh Montgomery, David Rohrlich, and Jean-Pierre Serre. Special thanks to Hendrik Lenstra for explaining his heuristic argument to us.

Many thanks to the first referee, who noted in an earlier version that some of our experimental results differed from the heuristic results by several standard deviations. This led us to discover a slight error in our formulas and to report the standard deviations, which are now within respectable limits. Thanks also to the second referee for very helpful suggestions.

The first and third authors wish to thank the National Science Foundation for support of this research through NSF grant number DMS-0139287.

REFERENCES

[Cohen 95] Henri Cohen. *A Course in Computational Algebraic Number Theory*, second corrected printing. New York: Springer, 1993.

[Fulton 70] W. Fulton. *Intersection Theory*. Berlin: Springer, 1997.

[Lang 70] S. Lang. *Algebraic Number Theory*. Reading, MA: Addison-Wesley, 1970.

[Lang 93] S. Lang. *Algebra*, 3rd edition. Reading, MA: Addison-Wesley, 1993.

[Matsumura 70] H. Matsumura. *Commutative Algebra*. New York: Benjamin, 1970.

[Poonen 03] Bjorn Poonen. "Squarefree Values of Multivariable Polynomials." *Duke Math. J.* 118 (2003), 353–373.

[van der Waerden 34] B. L. van der Waerden. "Die Seltenheit der Gleichungen mit Affekt." *Math. Ann.* 109 (1934), 13–16.

[Weiss 63] Edwin Weiss. *Algebraic Number Theory*. New York: McGraw-Hill, 1963

Avner Ash, Boston College, Chestnut Hill, MA 02445 (Avner.Ash@bc.edu)

Jos Brakenhoff, Universiteit Leiden, Leiden, the Netherlands (jbrakenh@math.leidenuniv.nl)

Theodore Zarrabi, Boston College, Chestnut Hill, MA 02445 (Ted.Zarrabi@risk.sungard.com)

Received December 2, 2005; accepted in revised form February 1, 2007.