J. Austral. Math. Soc. (Series A) **44** (1988), 287–293

ON A CONVERSE TO THE TSCHEBOTAREV DENSITY THEOREM

C. E. VAN DER PLOEG

(Received 3 April 1986; revised 5 November 1986)

Communicated by J. H. Loxton

Abstract

Using an elementary counting procedure on biquadratic polynomials over $\mathbf{Z}_p$ it is shown that the probability distribution of odd, unramified rational primes according to decomposition type in a fixed dihedral numberfield is identical to the probability distribution of separable quartic polynomials (mod p) whose roots generate numberfields with normal closure having Galois group isomorphic to D_4, as $p \to \infty$. This verifies a conjecture about a converse to the Tschebotarev density theorem. Further evidence in support of this conjecture is provided in quadratic and cubic numberfields.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*): 12 A 30.

Let P be the set of prime ideals in a numberfield F which are unramified in a fixed extension K of F. That is, $\mathbf{p} \in P$ if the ideal $(\mathbf{p})$ generated by $\mathbf{p}$ has no repeated factors in K. The factorization of $(\mathbf{p})$ can be represented by a partition of n, the degree of K over F, in the following way: we write

$$d_K(\mathbf{p}) = (e_1, e_2, \ldots, e_n)$$

if $(\mathbf{p})$ factorizes into a product of e_1 prime ideals of degree one, e_2 prime ideals of degree two, $\ldots$, e_n prime ideals of degree n in K. Clearly

$$\sum_{i=1}^{n} ie_i = n.$$

We may also associate a partition of n with each element of G, the Galois group of the normal closure of K over F: regard G as a permutation group on the roots of the minimal polynomial of K over F, that is, $G \leqslant S_n$. Then for $g \in G$ we

© 1988 Australian Mathematical Society 0263-6115/88 $A2.00 + 0.00

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press

write

$$d_G(g) = (e_1, e_2, \ldots, e_n)$$

if g is a product of e_1 unit cycles, e_2 transpositions, $\ldots$, e_n cycles of length n in lowest terms.

For a given partition d_0 of n let m be the number of permutations in G such that $d_G(g) = d_0$ and let S be the set of prime ideals in P such that $d_K(\mathbf{p}) = d_0$ (that is, with 'decomposition type' d_0). Then the Tschebotarev generalization of the Frobenius density theorem states that

$$\sum_{\mathbf{p} \in S} N(\mathbf{p})^{-t} = \frac{m}{n} \ln\left(\frac{1}{t-1}\right) + g(t)$$

where $N(\mathbf{p})$ denotes the norm of $\mathbf{p}$ in F and $g(t)$ remains bounded when $t \to 1^+$. That is, S has 'Dirichlet density' m/n. See Hasse (1930).

Now suppose that $F = \mathbf{Q}$ and that K is a non-normal quartic field generated by a root of an irreducible biquadratic polynomial

$$x^4 + ax^2 + b, \qquad a, b \in \mathbf{Z}.$$

That is, K is a 'dihedral numberfield', and G is isomorphic to D_4, the dihedral group of order 8. So in this case Tschebotarev's result takes the form

$$\lim_{t \to 1^+} \frac{\sum_{p \in S} p^{-t}}{\ln\left(\frac{1}{t-1}\right)} = \begin{cases} \frac{1}{8} & \text{if } d_0 = (4,0,0,0), \\ \frac{1}{4} & \text{if } d_0 = (2,1,0,0), \\ \frac{3}{8} & \text{if } d_0 = (0,2,0,0), \\ \frac{1}{4} & \text{if } d_0 = (0,0,0,1), \\ 0 & \text{otherwise.} \end{cases}$$

The notion of decomposition type being represented by a partition of n can also be applied to irreducible polynomials of degree n over $\mathbf{Q}$ in the following way: suppose that p is a rational prime which is unramified in the numberfield K and let f be the minimal polynomial of K over Q. Then we write

$$d_p(f) = (e_1, e_2, \ldots, e_n)$$

if f factors (mod p) into e_1 linear factors, e_2 irreducible quadratic factors, and so on.

It is well known that if p is odd then $d_p(t) = d_K(p)$, see Mann (1955). This motivates the following conjecture:

The probability distribution of odd rational primes which are unramified in a fixed numberfield K of degree n over $\mathbf{Q}$ *is identical to the probability distribution of separable polynomials of degree n* (mod p) *whose roots generate numberfields with normal closure having Galois group isomorphic to the Galois group of the normal closure of K over* $\mathbf{Q}$, *as* $p \to \infty$. *In both cases the distribution is classified according to decomposition type.*

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press

The difficulty in proving this result lies with the classification of polynomials which generate numberfields with fixed Galois group. However, it is shown in van der Ploeg (1987) that all quartic fields whose normal closure has Galois group isomorphic to D_4 are generated by roots of irreducible biquadratic polynomials of the form $x^4 + ax^2 + b$, $a, b \in \mathbf{Z}$, and that all polynomials of this type generate fields whose normal closure has Galois group isomorphic to D_4. So in the case that $G \simeq D_4$ the conjecture becomes

THEOREM. *Let K be a fixed dihedral numberfield and consider the probability distribution according to decomposition type of odd rational primes which are unramified in K. Then this is identical to the probability distribution of separable quartic polynomials* (mod p) *whose roots generate numberfields with normal closure having Galois group isomorphic to D_4, as $p \to \infty$.*

PROOF. In view of the remarks preceding the theorem it is sufficient to consider only separable biquadratic polynomials (mod p). In order to prove the theorem we need the following lemma.

LEMMA. *Of the p^2 polynomials of the form*

$$f(x) \equiv x^4 + ax^2 + b \pmod{p}, \quad a, b \in \mathbf{Z},$$

$2p - 1$ are inseparable. The distribution of decomposition types amongst the remaining $(p-1)^2$ separable polynomials is given by:

Number of polynomials	*Decomposition type*
$(p-1)(p-3)/8$	$(4,0,0,0)$
$(p-1)^2/4$	$(2,1,0,0)$
$(p-1)(3p-5)/8$	$(0,2,0,0)$
$(p-1)(p+1)/4$	$(0,0,0,1)$

PROOF. Inseparability occurs when $b \equiv 0 \pmod{p}$ or when $f(x) \equiv (x^2 - c)^2 \pmod{p}$. So there are $2p - 1$ distinct inseparable biquadratic polynomials (mod p). Assuming f to be separable, two cases arise.

Case 1. $f(x) \equiv (x^2 - c)(x^2 - d) \pmod{p}$, $c \not\equiv d$, $c, d \not\equiv 0 \pmod{p}$.

(i) If $(c/p) = (d/p) = 1$ then $d_p(f) = (4,0,0,0)$. Now if $c \equiv r^2 \pmod{p}$ and $d \equiv s^2 \pmod{p}$ we may assume without loss of generality $1 \leqslant r \leqslant (p-1)/2$ and $1 \leqslant s \leqslant (p-1)/2$ (for if $1 \leqslant X \leqslant (p-1)/2$ then $(p+1)/2 \leqslant -X \leqslant p-1$). So the number of distinct f with decomposition type $(4,0,0,0)$ is the number of ways that two different integers can be chosen from the range $[1,(p-1)/2]$.

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press

That is

$$\frac{1}{2}\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}-1\right)=(p-1)(p-3)/8.$$

(ii) If $(c/p)=1$ and $(d/p)=-1$ then $d_p(f)=(2,1,0,0)$. Since c and d may each take $(p-1)/2$ different values there are $(p-1)^2/4$ such polynomials in this case.

(iii) If $(c/p)=(d/p)=-1$ then $d_p(f)=(0,2,0,0)$. The number of such polynomials is the number of ways of choosing two different quadratic non-residues (mod p). That is $(p-1)(p-3)/8$.

Case 2. $f(x)\equiv(x^2+cx+d)(x^2-cx+d) \pmod p$, $c,d\not\equiv 0 \pmod p$. In this case f must have an even number of irreducible factors because the roots of each quadratic factor have the same modulus. So we cannot have decomposition type $(2,1,0,0)$. Furthermore, if f splits completely it has already been counted in Case 1, so it only remains to enumerate the case that f has two irreducible quadratic factors.

Let $g(x)=x^2+cx+d$ and $h(x)=x^2-cx+d$. Denote by A the set of all irreducible quadratic polynomials over $\mathbf{Z}_p$ with non-zero coefficient of x and divide A into two disjoint subsets G and H according as the coefficient of x lies in the ranges $[1,(p-1)/2]$ or $[(p+1)/2,p-1]$ respectively. Since we may assume without loss of generality that $g\in G$ and $h\in H$ and since G and H have the same cardinality, the number of biquadratic polynomials which are the product of two distinct irreducible quadratic factors is exactly one half of the cardinality of A.

Now suppose that $g(x)\equiv(x-x_0)(x-x_1) \pmod p$ where $0\leqslant x_0\leqslant x_1\leqslant p-1$. There are $p(p+1)/2$ quadratics of this form and so there are $p^2-p(p+1)/2=p(p-1)/2$ irreducible quadratics of the form

$$x^2+cx+d \pmod p, \qquad d\not\equiv 0 \pmod p.$$

But this includes those where $c\equiv 0 \pmod p$, which have already been counted in case 1. There are $(p-1)/2$ of these, and so the cardinality of A is $p(p-1)/2-(p-1)/2=(p-1)^2/2$. Hence we have $(p-1)^2/4$ to add to the number in case 1 of biquadratic polynomials with decomposition type $(0,2,0,0)$. Hence there are $(p-1)(p-3)/8+(p-1)^2/4=(p-1)(3p-5)/8$ biquadratic polynomials which split into two distinct irreducible quadratic factors (mod p).

Finally we may calculate the number of irreducible biquadratic polynomials (mod p) by subtraction, as

$$(p-1)^2-(p-1)(p-3)/8-(p-1)^2/4 \\ -(p-1)(3p-5)/8=(p-1)(p+1)/4.$$

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press

Let us now define a probability distribution over the set B_p of separable biquadratic polynomials (mod p) as $p \to \infty$ as

$$P\big(d_p(f) = d_0\big) = \lim_{p\to\infty} \frac{|f \in B_p : d_p(f) = d_0|}{(p-1)^2}$$

where $|\cdot|$ denotes cardinality. Then by the lemma

$$P\big(d_p(f) = d_0\big) = \begin{cases} \frac{1}{8} & \text{if } d_0 = (4,0,0,0), \\ \frac{1}{4} & \text{if } d_0 = (2,1,0,0), \\ \frac{3}{8} & \text{if } d_0 = (0,2,0,0), \\ \frac{1}{4} & \text{if } d_0 = (0,0,0,1), \\ 0 & \text{otherwise.} \end{cases}$$

The proof of the theorem now follows from Tschebotarev's result in dihedral numberfields, on noting that the Dirichlet density may be interpreted as a probability density. That is,

$$\lim_{t\to 1^+} \frac{\sum_{p\in S} p^{-t}}{\ln\left(\frac{1}{t-1}\right)} = P\big(d_K(p) = d_0\big) = \lim_{r\to\infty} \frac{|p \in S : p \leqslant r|}{|p \in I_K : p \leqslant r|}$$

where I_K denotes the set of odd rational primes which are unramified in K, see Lagarias and Odlyzko (1977).

We conclude with a discussion of quadratic and cubic fields, whose Galois groups are readily determined by their minimal polynomials. This provides further evidence in support of the conjecture.

For quadratic fields the minimal polynomial is $f(x) = x^2 + ax + b$ where $D = a^2 - 4b$ is not a square in $\mathbf{Z}$. There are p such polynomials for which $D \equiv 0 \pmod p$ since inseparability occurs only when $f(x) \equiv (x-c)^2 \pmod p$. So consider the factorization of $f(x)$ modulo odd primes p such that $D \not\equiv 0 \pmod p$. Since there are $\frac{1}{2}p(p-1)$ distinct polynomials such that

$$f(x) \equiv (x-c)(x-d) \pmod p$$

for $c \not\equiv d \pmod p$, exactly one half of the separable polynomials are irreducible, and the other half split into two distinct linear factors. Hence

$$P\big(d_p(f) = d_0\big) = \begin{cases} \frac{1}{2} & \text{if } d_0 = (2,0), \\ \frac{1}{2} & \text{if } d_0 = (0,1), \\ 0 & \text{otherwise.} \end{cases}$$

This verifies the conjecture for the quadratic case, since $G \simeq \mathbf{Z}_2$.

For cubic fields the minimal polynomial may be written in reduced form as $f(x) = x^3 + ax + b$ with discriminant $D = -27b^2 - 4a^3$. It is well known that $G \simeq \mathbf{Z}_3$ or S_3 according as D is or is not a square in $\mathbf{Z}$. We verify the conjecture in both cases.

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press

Results on the factorization of this type of polynomial have been known for some time. Skolem (1941) shows that the number of cubics which split into a given decomposition type (mod p) depends on the residue class of p (mod 3). He assumes $a \not\equiv 0 \pmod{p}$ and his results are summarized in the following table:

Table 1	Inseparable	$d_0 = (0,0,1)$	$d_0 = (1,1,0)$	$d_0 = (3,0,0)$
$p \equiv 1 \pmod 3$	$p-1$	$\frac{(p-1)^2}{3}$	$\frac{p(p-1)}{2}$	$\frac{(p-4)(p-1)}{6}$
$p \equiv 2 \pmod 3$	$p-1$	$\frac{(p+1)(p-1)}{3}$	$\frac{(p-2)(p-1)}{2}$	$\frac{(p-2)(p-1)}{6}$

These results provide all the information we need for the distribution of decomposition types of cubics (mod p), except for the case $a \equiv 0 \pmod{p}$. For $p > 3$ there are $p-1$ separable $f(x)$ such that $f(x) \equiv x^3 + b \pmod{p}$. If $p \equiv 2 \pmod 3$ there are $p-1$ cubic residues (mod p), so all separable $f(x)$ of this form split completely. If $p \equiv 1 \pmod 3$ there are $\frac{1}{3}(p-1)$ cubic residues (mod p), so only $\frac{1}{3}$ of these separable cubics split completely. The other $\frac{2}{3}(p-1)$ cubics remain irreducible, since $(D/p) = (-3/p) = 1$ in this case.

Now suppose $G \simeq \mathbf{Z}_3$, so that D is a square in $\mathbf{Z}$. Then $f(x)$ either remains irreducible or splits completely (mod p). By the results above it is clear that the number of separable, normal cubics $x^3 + ax + b$ which fall into each category is given by the following table:

Table 2	$d_0 = (0,0,1)$	$d_0 = (3,0,0)$
$p \equiv 1 \pmod 3$	$\frac{1}{3}(p-1)(p+1)$	$\frac{1}{6}(p-1)(p-2)$
$p \equiv 2 \pmod 3$	$\frac{1}{3}(p-1)(p+1)$	$\frac{1}{6}(p-1)(p+4)$

It follows that

$$P\big(d_p(f) = d_0\big) = \begin{cases} \frac{1}{3} & \text{if } d_0 = (3,0,0), \\ \frac{2}{3} & \text{if } d_0 = (0,0,1), \\ 0 & \text{otherwise,} \end{cases}$$

and the conjecture is verified for the case $G \simeq \mathbf{Z}_3$.

Finally suppose that $G \simeq S_3$. In this case the quadratic character of D can be $+1$ or -1 and all decomposition types of $f(x)$ (mod p) can occur. Combining Table 1 with the results for $a \equiv 0 \pmod{p}$ and defining the distribution in the

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press

usual way yields our final verification of the conjecture, that is

$$P\big(d_p(f) = d_0\big) = \begin{cases} \frac{1}{6} & \text{if } d_0 = (3,0,0), \\ \frac{1}{2} & \text{if } d_0 = (1,1,0), \\ \frac{1}{3} & \text{if } d_0 = (0,0,1), \\ 0 & \text{otherwise.} \end{cases}$$

References

H. Hasse (1930), *Bericht über neuere untersuchungen und probleme aus der theorie der Algebraischen Zahlkörper*, Teil II §24 (Leipzig und Berlin).

S. Lang (1970), *Algebraic number theory* (Addison-Wesley).

J. C. Lagarias and A. M. Odlyzko (1977), 'Effective versions of the Chebotarev density theorem' *Algebraic Number Fields*, ed. A. Frölich, (Academic Press), pp. 409–464.

H. B. Mann (1955), *Introduction to algebraic number theory* (Ohio State University Press).

Th. Skolem (1941), 'Die Anzahl der Wurzeln der Kongruenz $x^3 + ax + b \equiv 0 \pmod{p}$ für die verschiedenen Paare a, b', *Norske. Vid. Selsk. Forh.* (*Trondheim*) **14**, 161–4.

C. E. van der Ploeg (1987), 'Duality in non-normal quartic fields', *Amer. Math. Monthly* **94** (March).

Mathematics Division
University of Sussex
Falmer, Brighton
United Kingdom

https://doi.org/10.1017/S1446788700032109 Published online by Cambridge University Press