Vol. 87, No. 1 DUKE MATHEMATICAL JOURNAL © 1997

THE GENERIC IRREDUCIBILITY OF THE NUMERATOR OF THE ZETA FUNCTION IN A FAMILY OF CURVES WITH LARGE MONODROMY

NICK CHAVDAROV

1. Introduction. The article is essentially my Ph.D. thesis at Princeton University. It is devoted to proving the following conjecture of N. Katz.

CONJECTURE. *Let $U/\mathbf{F}_q$ be an open subset of the affine line $A^1_{\mathbf{F}_q}$. Let $\psi: X \to U$ be a proper smooth family of curves of genus g. Assume that the family has "large" monodromy. Let p_n = fraction of points $u \in U(\mathbf{F}_{q^n})$, such that the polynomial $P(T)$ = the numerator of $Z(X_u/\mathbf{F}_{q^n}, T)$ is irreducible over* $\mathbf{Q}$. *Then* $\lim_{n\to\infty} p_n = 1$.

First, let us consider an elementary case where we prove that "most" polynomials are irreducible.

PROPOSITION 1.1. *Fix a positive integer d. Let M_R be the set of degree-d monic polynomials whose coefficients are integers between 1 and R, where R is a positive integer. Then*

$$\lim_{R\to\infty} \frac{\#\{\text{irreducible polynomials in } M_R\}}{\# M_R} = 1.$$

Proof. We will prove the following stronger statement:

$$\lim_{R\to\infty} \frac{\#\{\text{polynomials in } M_R \text{ which are reducible mod } l, \text{ for some prime } l\}}{\# M_R} = 0.$$

It is known that approximately $1 - 1/d$ of the degree-d monic polynomials in $\mathbf{F}_l[T]$ are reducible. We will reduce polynomials modulo several prime numbers $l_1, l_2, \ldots, l_r$. The Chinese remainder theorem shows that if R is divisible by the product of the l_i's, then the values of the reductions of polynomials in M_R modulo l_i for $i = 1, \ldots, r$ are independent random variables. Then the events that a polynomial is reducible modulo l_i for $i = 1, \ldots, r$ are independent. Thus, the probability that a polynomial is reducible modulo all l_i for $i = 1, \ldots, r$ is approximately $(1 - 1/d)^r$, which can be made arbitrarily small by choosing $r \gg 0$.

Our main idea is that one can apply the above argument to prove Katz's conjecture if one knows that the mod-l monodromy of the family of curves is

Received 14 June 1996.
Author's research was sponsored by Princeton University.