Canad. Math. Bull. Vol. 34 (2), 1991 pp. 229–235

JACOBI SUMS, IRREDUCIBLE ZETA-POLYNOMIALS, AND CRYPTOGRAPHY

NEAL KOBLITZ

ABSTRACT. We find conditions under which the numerator of the zeta-function of the curve $y^2+y=x^d$ over $\mathbf{F}_p$, where $d=2g+1$ is a prime, $d\not\equiv p$, is irreducible over $\mathbf{Q}$. This leads to the generalized Mersenne problem of "almost primality" of the number of points on the jacobian of such a curve over an extension of $\mathbf{F}_p$, which has application to public key cryptography.

1. **Introduction.** Suppose one has a large abelian group G such that (i) $\#G$ is either prime, or "almost prime" (i.e., equal to a large prime number times a small factor), and (ii) the group law does not seem to permit a feasible solution of the discrete logarithm problem in G. One can then use G to construct secure Diffie-Hellman type cryptosystems and cryptographic protocols. This was explained in [3], where we argued that the jacobians of hyperelliptic curves defined over a finite field $\mathbf{F}_q$ have the property (ii). In order for $\#G$ to be "almost prime," a necessary condition is that the numerator of the zeta-function of the curve be irreducible over $\mathbf{Q}$. In that case, if α is a reciprocal root of that numerator, then the group of F_q-points on the jacobian has order $N_1=\mathbf{N}(\alpha-1)$ (where $\mathbf{N}$ denotes the absolute norm of an algebraic number). Moreover, the group of $\mathbf{F}_{q^s}$-points on the jacobian has order

$$N_s=\mathbf{N}(\alpha^s-1)=N_1\cdot\mathbf{N}\left(\frac{\alpha^s-1}{\alpha-1}\right), \tag{1}$$

in which the large second factor on the right might possibly be prime for prime s (not for composite $s=s_1s_2$, since then N_s is divisible by N_{s_1}). The question of primality of the second factor on the right in (1) is a natural generalization of the Mersenne problem (the case $\alpha=2$).

The purpose of this paper is to give conditions for irreducibility of the numerator of the zeta-function in the case of the special family of hyperelliptic curves $y^2+y=x^d$ defined over the prime finite field $\mathbf{F}_p$. Roughly speaking, we have irreducibility most of the time when the multiplicative order f of p modulo d is odd, and almost never when f is even. An important special case occurs when p generates the quadratic residues modulo $d\equiv 3 \pmod 4$, in which case the condition for irreducibility is that $d\not\equiv 19 \pmod{24}$ and f be relatively prime to the class number of $\mathbf{Q}(\sqrt{-d})$.

Received by the editors April 25, 1989 and, in revised form, January 16, 1990.
AMS subject classification: 11L05, 11G20, 11G25, 11T71, 12E05.

We conclude with examples showing reducibility when the conditions of the theorem fail and an example of a "twisted" curve for which the number of $\mathbf{F}_2$-points on its jacobian is 3 times a 58-digit prime.

2. **Number of points.** For each positive integer g (the *genus*) we set $d = 2g + 1$ and consider the hyperelliptic curve $C_d : y^2 + y = x^d$ defined over the field $\mathbf{F}_p$ of p elements, where p is a prime not dividing d. If $p \neq 2$, the equation can alternately be written in the form $y^2 = x^d + \frac{1}{4}$. We also consider the *twisted curve* $\tilde{C}_d$ with equation $y^2 + y = x^d + 1$ for $p = 2$ and $\beta y^2 = x^d + \frac{1}{4}$ for $p \neq 2$, where β is a quadratic nonresidue modulo p. Let $C_d(\mathbf{F}_{p^s})$ denote the set of points on C_d with coordinates in the extension field $\mathbf{F}_{p^s}$ (including the point at infinity), and let $M_s = \#C_d(\mathbf{F}_{p^s})$ (for fixed d and p, and $s = 1, 2, \ldots$). Let $\mathbf{J}_d(\mathbf{F}_{p^s})$ denote the abelian group of $\mathbf{F}_{p^s}$-points on the jacobian variety of C_d, and let $N_s = \#\mathbf{J}_d(\mathbf{F}_{p^s})$. (For an explicit description of the elements and group law in $\mathbf{J}_d$, see [3] or [4].) We analogously define $\tilde{C}_d(\mathbf{F}_{p^s}), \tilde{M}_s, \tilde{\mathbf{J}}_d(\mathbf{F}_{p^s}), \tilde{N}_s$.

The *zeta-polynomial* $Z_d(T)$ is the polynomial whose reciprocal polynomial $Zj_d(T) = T^{2g}Z(1/T)$ is the numerator of the zeta-function of C_d. It can be defined by the power series identity

$$\log\,(Zj_d(T)) = \sum_{s=1}^{\infty} \frac{M_s - q^s - 1}{s}\, T^s,$$

or, equivalently,

$$Z_d(T) = \prod_{j=1}^{2g} (T - \alpha_j), \quad \text{where} \quad M_s = q^2 + 1 - \sum_{j=1}^{2g} \alpha_j^s.$$

By Weil's theorem, the roots α_j have absolute value $\sqrt{p}$ in any complex imbedding, and they occur in complex conjugate pairs. We shall index them so that $\alpha_{j+g} = \bar{\alpha}_j, j = 1, \ldots, g$. Once $Z_d(T)$ is known, N_s is determined by the formula

$$N_s = \prod_{j=1}^{g} |1 - \alpha_j^s|^2. \tag{2}$$

The zeta-polynomial $\tilde{Z}_d(T)$ of the twisted curve $\tilde{C}_d$ is related to $Z_d(T)$ in a very simple way:

$$\tilde{Z}_d(T) = Z_d(-T) = \prod_{j=1}^{2g} (T + \alpha_j); \tag{3}$$

this follows from the observation that $\tilde{M}_s = M_s$ for s even and $\tilde{M}_s = 2q + 2 - M_s$ for s odd.

The zeta-polynomial of the curve C_d or $\tilde{C}_d$ can be expressed in terms of Jacobi sums. We shall be interested only in the case when d is prime. (If d is composite, then $Z_d(T)$ is always reducible.) Let $\zeta_d = e^{2\pi i/d}$, and $K_d = \mathbf{Q}(\zeta_d)$. Given d and p, let $\mathfrak{p}$ be a fixed prime ideal of K_d lying over p, and let f be the residue degree of $\mathfrak{p}$ (the smallest positive integer such that $d|p^f - 1$), so that $O_{K_d}/\,\mathfrak{p} \cong \mathbf{F}_{p^f}$. Let χ be the d-th power residue symbol modulo $\mathfrak{p}$, i.e., χ is the character on $(O_{K_d}/\mathfrak{p})j$ with values in the d-th roots of unity for which

$$\chi(a \bmod \mathfrak{p}) \equiv a^{(p^f-1)/d} \pmod{\mathfrak{p}} \quad \text{for} \quad a \in O_{K_d}.$$

For $j = 1, \ldots, d-1$ we define the Jacobi sum $J_j \in K_d$ as follows:

$$J_j = \sum_{a \in O_{K_d}/\mathfrak{p}, a \neq 0,1} \chi^j(a)\chi^j(1-a). \tag{4}$$

We list some elementary properties of the J_j. If we let $\langle \nu \rangle$ denote the representative between 0 and $d-1$ of an integer ν modulo d, then we have

$$J_{\langle p^i j \rangle} = J_j, \quad i = 0, \ldots, f-1. \tag{5}$$

In addition, if $\sigma_\nu, \nu = 1, \ldots, d-1$, denotes the automorphism of K_d for which $\sigma_\nu(\zeta_d) = \zeta_d^{\,\nu}$, then clearly

$$\sigma_\nu(J_j) = J_{\langle \nu j \rangle}. \tag{6}$$

Finally, J_j has absolute value $p^{f/2}$ in any complex embedding.

We shall also need the Stickelberger relation, which in this situation says that the prime ideal decomposition of J_j in K_d is

$$(J_j) = \mathfrak{p}^{\Theta_j}, \quad \text{where} \quad \Theta_j = \sum_{\nu=1}^{d-1} \left(\frac{\langle 2\nu j \rangle + 2\langle -\nu j \rangle}{d} - 1 \right) \sigma_\nu^{-1}. \tag{7}$$

(This just says that the coefficient of σ_ν^{-1} is equal to 0 if $\langle -\nu j \rangle < d/2$ and to 1 if $\langle -\nu j \rangle > d/2$.)

Let $k = (d-1)/f = 2g/f$ be the order of the quotient group of $(\mathbf{Z}/d\mathbf{Z})^*$ by the subgroup generated by p. Let $j_\nu \in \mathbf{Z}/d\mathbf{Z}, \nu = 1, \ldots, k$, be representatives of this quotient group.

The zeta-polynomial $Z_d(T)$ is then given by the formula (see [9])

$$Z_d(T) = \prod_{\nu=1}^{k} (T^f + J_{j_\nu}). \tag{8}$$

3. **Irreducibility theorem.**

THEOREM. *Let $Z_d(T)$ be the zeta-polynomial of $y^2+y = x^d$ over $\mathbf{F}_p$, where $d = 2g+1$ is prime, $d \neq p$, and let f be the multiplicative order of p modulo d.*

(A) *If f is even, then $Z_d(T)$ is irreducible over $\mathbf{Q}$ if and only if either $d = 3$ or else $d \geqq 5$ is a Fermat prime, $p \neq 2$, and $f = 2g$.*

(B) *If f is odd, then $Z_d(T)$ is irreducible over $\mathbf{Q}$ unless one of the following two conditions holds:*

(i) *$3|f$ and -2 is a power of p modulo d;*

(ii) *f is not prime to the minus part of the class number of the decomposition field of p (the fixed field of $\sigma_p \in$ Gal $(K_d/\mathbf{Q})$).*

PROOF. If $d = 3$, then the zeta-polynomial is quadratic, and so is irreducible because it cannot have a rational root (the roots have absolute value $\sqrt{p}$). In what follows suppose $d \geqq 5$.

First suppose that f is even, i.e., that -1 is a power of p modulo d. By Lemma 1.1 of [2] we then have $Z_d(T) = (T^f + p^{f/2})^k$, where $k = 2g/f$. Hence, $Z_d(T)$ is reducible if $f < 2g$. Now let $f = 2g$, in which case $Z_d(T) = T^{2g} + p^g$. If d is not a Fermat prime, then g is divisible by an odd number $\nu > 1$, and so $T^{2g/\nu} + p^{g/\nu}$ is a factor of $Z_d(T)$. If d is a Fermat prime and $p = 2$, then $d = 5$ (otherwise 2 would not be a primitive root modulo d), in which case $Z_d(T) = T^4 + 4 = (T^2 + 2T + 2)(T^2 - 2T + 2)$. Thus, $Z_d(T)$ is reducible unless the conditions in (A) hold. Under the conditions in (A), $Z_d(T)$ has the factorization

$$\prod_{0<j<4g,\, j \text{ odd}} (T - \zeta^j \sqrt{p}),$$

where ζ is a primitive $4g$-th root of unity. Since $p \neq 2$, the fields $\mathbf{Q}(\sqrt{p})$ and $\mathbf{Q}(\zeta)$ are linearly disjoint. Since the different primitive $4g$-th roots of unity ζ^j (j odd) are permuted by Gal $(\mathbf{Q}(\zeta)/\mathbf{Q})$ (here we are using the fact that $d = 2g+1$ is a Fermat prime), it follows that the roots of $Z_d(T)$ are distinct conjugates of $\zeta\sqrt{p}$, i.e., $Z_d(T)$ is irreducible.

Next suppose that f is odd.

LEMMA. *If f is odd, then the J_{j_ν} are distinct, $\nu = 1, \ldots, k$.*

PROOF. (compare with § 2 of [5] and Lemma 1.6 of [2]). Suppose that $J_j = J_{j'}$. We must show that $j, j' \in (\mathbf{Z}/d\mathbf{Z})^*$ are in the same coset of the subgroup P of powers of p. For $\nu \in (\mathbf{Z}/d\mathbf{Z})^*$, let τ_ν denote the projection of σ_ν onto the quotient G of Gal $(K_d/\mathbf{Q})$ by the decomposition group of $\mathfrak{p}$, i.e., $\tau_{p^i\nu} = \tau_\nu, i = 0, \ldots, f-1$. We shall identify G with $(\mathbf{Z}/d\mathbf{Z})^*/P$. Since $J_j = J_{j'}$, then by (7) we must have the following relation in the group algebra $\mathbf{Z}[G]$:

$$\text{(9)} \qquad \sum_{\nu=1}^{d-1} \left(\frac{\langle 2\nu j \rangle + 2\langle -\nu j \rangle}{d} - 1 \right) \tau_\nu^{-1} = \sum_{\nu=1}^{d-1} \left(\frac{\langle 2\nu j' \rangle + 2\langle -\nu j' \rangle}{d} - 1 \right) \tau_\nu^{-1}.$$

We recall the definition of the first Bernoulli polynomial $B_1(x) = x - \frac{1}{2}$ and the generalized Bernoulli number (for χ a character of $(\mathbf{Z}/d\mathbf{Z})^*$)

$$\text{(10)} \qquad B_{1,\chi} = \sum_{\nu=1}^{d-1} B_1(\nu/d)\chi(\nu).$$

It is well known that $B_{1,\chi} \neq 0$ if χ is an *odd* character.

Now let χ be any odd character which is trivial on the subgroup P, i.e., such that $\chi(p) = 1$. Because f is odd — which is equivalent to $-1 \notin P$ — such χ exist (there are $k/2 = g/f$ of them). Applying χ to the identity (9) and using (10), we obtain

$$\chi(2j)B_{1,\bar{\chi}} + 2\chi(-j)B_{1,\bar{\chi}} = \chi(2j')B_{1,\bar{\chi}} + 2\chi(-j')B_{1,\bar{\chi}}.$$

Dividing by $B_{1,\bar{\chi}}$ gives

$$\chi(2j) + 2\chi(-j) = (\chi(2j) + 2\chi(-j))\chi(j'/j).$$

Since $\chi(2j)+2\chi(-j)\neq 0$, it follows that $\chi(j'/j)=1$.

But then also $\chi'(j'/j)=1$ for any even character χ' which is trivial on P, since we can take an arbitrary odd character χ and express χ' as the ratio of the two odd characters $\chi'\chi$ and χ. We conclude that $\chi(j'/j)=1$ for all characters of $(\mathbf{Z}/d\mathbf{Z})^*/P$, and hence $j'/j\in P$, as desired.

We now return to the proof of the theorem. It follows from (6) and the lemma that the $J_{j\nu}$ in (8) are a set of distinct conjugates over $\mathbf{Q}$. Let $K_{d,p}\subset K_d$ denote the decomposition field of p, i.e., the fixed field of $\sigma_p\in$ Gal $(K_d/\mathbf{Q})$. According to the theory of Kummer extensions (see, e.g., Theorem 9.1 of [6]) $Z_d(T)$ is irreducible if and only if for any prime $l|f$ none of the J_j is an l-th power in $K_{d,p}$. It is obviously enough to verify this for J_1, and for this it suffices to show that, if neither of the conditions (i), (ii) in the theorem holds, then for any $l|f$ the element

$$\Theta=\sum_{\nu=1}^{d-1}\left(\frac{\langle 2\nu\rangle+2\langle-\nu\rangle}{d}-1\right)\tau_\nu^{-1} \tag{11}$$

is not divisible by l in the group algebra $\mathbf{Z}[\text{Gal }(K_{d,p}/\mathbf{Q})]$. Suppose l divided this element. We proceed as in the proof of the lemma, letting χ be an arbitrary odd character of Gal $(K_{d,p}/\mathbf{Q})\approx(\mathbf{Z}/d\mathbf{Z})^*/P$. Applying χ to (11), we find that l divides $(2+\chi(-2))B_{1,\bar\chi}$ in the ring $\mathbf{Z}[\chi]$. If condition (i) does not hold, then for some χ we have $l\nmid(2+\chi(-2))$, and so l is not prime to $B_{1,\bar\chi}$. However, up to a power of 2 (and a factor of d if $f=1$) the minus part h^- of the class number of $K_{d,p}$ is equal to the product of the $|B_{1,\chi}|$ over the g/f odd characters χ of Gal $(K_{d,p}/\mathbf{Q})$ (see [7], p. 80). Hence $l|h^-$, and the theorem is proved. ∎

COROLLARY 1. *Suppose that $d=2g+1$ is a prime $\equiv 3$ (mod 4), and p has order g modulo d. Let h_d denote the class number of $\mathbf{Q}(\sqrt{-d})$, and let $\epsilon_d=2-(\frac{2}{d})$. Then $Z_d(T)$ is given by*

$$Z_d(T)=(T^g-p^{(g-\epsilon_dh_d)/2}(a+b\sqrt{-d}))(T^g-p^{(g-\epsilon_dh_d)/2}(a-b\sqrt{-d})),$$

where $a\pm b\sqrt{-d}$ is the unique integer of $\mathbf{Q}(\sqrt{-d})$ such that $a^2+b^2d=p^{\epsilon_dh_d}$, $p\nmid a$, $p^{(g-\epsilon_dh_d)/2}a\equiv 1$ (mod d). In this case $Z_d(T)$ is irreducible over $\mathbf{Q}$ unless either (i) $d\equiv 19$ (mod 24), or else (ii) g.c.d.$(g,h_d)>1$.

This corollary follows from the theorem if we use Stickelberger's relation and the formula $\sum_{\nu=1}^{(d-1)/2}(\frac{\nu}{d})=(2-(\frac{2}{d}))h_d$ (see, e.g., [1], p. 346).

REMARK. Part (2) of the theorem stated without proof in §4 of [4] is incorrect; it is corrected in Corollary 1 above.

COROLLARY 2. *For any fixed prime $d\geqq 3$ there are infinitely many primes p such that the zeta-polynomial of $y^2+y=x^d$ over $\mathbf{F}_p$ is irreducible over $\mathbf{Q}$.*

In fact, it suffices to take $p\equiv 1$ (mod d).

CONJECTURE. *For any fixed prime p there are infinitely many primes d such that the zeta-polynomial of $y^2 + y = x^d$ over $\mathbf{F}_p$ is irreducible over* $\mathbf{Q}$.

REMARK. This conjecture would follow from the following variant of a classical conjecture (see §*I*. 12 of [8]): *There are infinitely many primes $d = 2g + 1$ such that g is prime and such that $d \equiv 7 \pmod 8$ in the case $p = 2$, $(\frac{p}{d}) = (\frac{-d}{p}) = 1$ in the case $p \neq 2$.* Namely, if d satisfies these conditions, then for J_1 to be a g-th power in $\mathbf{Q}(\sqrt{-d})$ there would have to be an integer of $\mathbf{Q}(\sqrt{-d})$ of norm p, and this is impossible for $d > 4p$.

COROLLARY 3. *The theorem and Corollaries 1 and 2 hold with $C_d : \ y^2 + y = x^d$ replaced by the twisted curve $\tilde{C}_d$.*

This follows immediately from (3).

4. Examples.

1. Let $d = 19, p = 5$. Then Corollary 1 applies, $h_{19} = 1$, and condition (i) holds. In this case $J_1 = (5(\frac{1+\sqrt{-19}}{2}))^3$, and $Z_{19}(T)$ is reducible.

2. Let $d = 71, p = 107$. Then condition (ii) of Corollary 1 holds (in fact, $h_{71} = 7$). In this case $J_1 = (107^2(-6+\sqrt{-71}))^7$, and $Z_{71}(T)$ is reducible. However, if we take $p = 2$, which is also a generator of the quadratic residues modulo 71, we obtain an irreducible zeta-polynomial, because there is no integer of $\mathbf{Q}(\sqrt{-71})$ of norm 2.

3. Let $p = 2$. Here is a list of all $d < 200$ for which $Z_d(T)$ is irreducible: 3, 7, 23, 31, 47, 71, 73, 79, 89, 103, 127, 151, 167, 191, 199. In fact, in this range $Z_d(T)$ is irreducible in all cases when 2 has odd order modulo d.

4. Let $p = 2, d = 7$. Then $Z_7(T) = T^6 - 2T^3 + 8$ is irreducible, and for prime s the number $N_s = \#(\mathbf{J}_7(\mathbf{F}_{2^s}))$ may possibly equal $N_1 = 7$ times a large prime. For example,

$$N_{47} = 7 \cdot 39\,82275\,92830\,90398\,46698\,24190\,47946\,07809\,61207.$$

Thus, the jacobian of the curve $y^2 + y = x^7$ over $\mathbf{F}_{2^{47}}$ may be useful in cryptographic applications. One could generalize the Mersenne problem by conjecturing that N_s / N_1 is prime infinitely often (see (1)).

5. The number of $\mathbf{F}_p$-points on the jacobian of C_d is always divisible by d; however, the number of points on the jacobian of the twisted curve $\tilde{C}_d$ is not. Thus, for d large it is *a priori* possible for the number of $\mathbf{F}_p$-points on the latter jacobian to be a prime number or a small factor times a large prime. For example, if we take $p = 2, d = 383$, then we have:

$$g = 191, \quad h_{383} = h(\mathbf{Q}(\sqrt{-383})) = 17, \quad J_1 = 2^{87}\left(\frac{711 + 7\sqrt{-383}}{2}\right),$$

$$\#(\tilde{\mathbf{J}}_{383}(\mathbf{F}_2)) = 3P,$$

where P is a 58-digit prime (its primality, and also the primality of the 42-digit factor of N_{47} in example 4, were kindly verified for me by A. Odlyzko). Explicitly,

$$P = ((1 - 711 \cdot 2^{86})^2 + 49 \cdot 383 \cdot 2^{172})/3 =$$

$$= 104\,61836\,22564\,44679\,39726\,31570\,49793\,70956\,86563\,18343\,34525\,30347.$$

Thus, the jacobian of the curve $v^2 + v = u^{383} + 1$ over $\mathbf{F}_2$ might be suitable for discrete log cryptosystems.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

2. B. H. Gross and D. E. Rohrlich, *Some results on the Mordell-Weil group of the jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201–224.

3. N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150.

4. N. Koblitz, *A family of jacobians suitable for discrete log cryptosystems*, to appear in Proc. Crypto '88.

5. N. Koblitz and D. E. Rohrlich, *Simple factors in the jacobian of a Fermat curve*, Can. J. Math. **30** (1978), 1183–1205.

6. S. Lang, *Algebra*, 2nd ed. Addison-Wesley, Reading MA, 1984.

7. S. Lang, *Cyclotomic Fields*, Springer-Verlag, New York, 1978.

8. D. Shanks, *Solved and Unsolved Problems in Number Theory*, 3rd ed., Chelsea, New York, 1985.

9. A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

Dept. of Mathematics GN-50
Univ. of Washington
Seattle, WA 98195 USA