Algebra & Number Theory

Volume 7

2013

No. 8

Differential characterization of Wilson primes for $\mathbb{F}_q[t]$

Dinesh S. Thakur

msp

ALGEBRA AND NUMBER THEORY 7:8 (2013)
dx.doi.org/10.2140/ant.2013.7.1841

Differential characterization of Wilson primes for $\mathbb{F}_q[t]$

Dinesh S. Thakur

Dedicated to Barry Mazur on his 75th birthday

We consider an analog, when $\mathbb{Z}$ is replaced by $\mathbb{F}_q[t]$, of Wilson primes, namely the primes satisfying Wilson's congruence $(p-1)! \equiv -1$ to modulus p^2 rather than the usual prime modulus p. We fully characterize these primes by connecting these or higher power congruences to other fundamental quantities such as higher derivatives and higher difference quotients as well as higher Fermat quotients. For example, in characteristic $p > 2$, we show that a prime $\wp$ of $\mathbb{F}_q[t]$ is a Wilson prime if and only if its second derivative with respect to t is 0 and in this case, further, that the congruence holds automatically modulo $\wp^{p-1}$. For $p = 2$, the power $p-1$ is replaced by $4-1=3$. For every q, we show that there are infinitely many such primes.

1. Introduction

For a prime p, the well-known Wilson congruence says that $(p-1)! \equiv -1 \bmod p$. A prime p is called a Wilson prime if the congruence above holds modulo p^2. Only three such primes are known, and we refer to [Ribenboim 1996, pp. 346 and 350] for history and [Sauerberg et al. 2013] for more references.

Many strong analogies [Goss 1996; Rosen 2002; Thakur 2004] between number fields and function fields over finite fields have been used to benefit the study of both. These analogies are even stronger in the base case $\mathbb{Q}, \mathbb{Z} \leftrightarrow F(t), F[t]$, where F is a finite field. We will study the concept of Wilson prime in this function field context and find interesting differential characterizations for them with the usual and arithmetic derivatives. In [Sauerberg et al. 2013], we exhibited infinitely many of them, at least for many F. Our characterization gives easier alternate proof generalizing to all F.

The author is supported in part by NSA grant H98230-10-1-0200.
MSC2010: primary 11T55; secondary 11A41, 11N05, 11N69, 11A07.
Keywords: Wilson prime, arithmetic derivative, Fermat quotient.

2. Wilson primes

Let us fix some basic notation. We use the standard conventions that empty sums are zero and empty products are one. Further,

q is a power of a prime p,
$A = \mathbb{F}_q[t]$,
$A_d = \{\text{elements of } A \text{ of degree } d\}$,
$[n] = t^{q^n} - t$,
$D_n = \prod_{i=0}^{n-1}(t^{q^n} - t^{q^i}) = \prod [n-i]^{q^i}$,
$L_n = \prod_{i=1}^{n}(t^{q^i} - t) = \prod [i]$,
F_i is the product of all (nonzero) elements of A of degree less than i,
$\mathcal{N}a = q^d$ for $a \in A_d$, i.e., the norm of a and
$\wp$ is a monic irreducible polynomial in A of degree d.

If we interpret the factorial of $n-1$ as the product of nonzero "remainders" when we divide by n, we get F_i as a naïve analog of factorial of $a \in A_i$. Note that it just depends on the degree of a. By the usual group theory argument with pairing of elements with their inverses, we get an analog of Wilson's theorem that $F_d \equiv -1 \bmod \wp$ for $\wp$ a prime of degree d. Though not strictly necessary for this paper, we now introduce a more refined notion of factorial due to Carlitz. For $n \in \mathbb{Z}$ and $n \geq 0$, we define its factorial by

$$n! := \prod D_i^{n_i} \in A \quad \text{for } n = \sum n_i q^i,\ 0 \leq n_i < q.$$

See [Thakur 2004, 4.5–4.8, 4.12 and 4.13; 2012] for its properties such as prime factorization, divisibilities, functional equations, interpolations and arithmetic of special values and congruences, which are analogous to those of the classical factorial. See also [Bhargava 2000], which gives many interesting divisibility properties in great generality.

Carlitz proved D_n is the product of monics of degree n. This gives the connection between the two notions above, that for $a \in A_i$, $(\mathcal{N}a - 1)! = (-1)^i F_i$. (See [Thakur 2012, Theorem 4.1, Section 6] for more on these analogies and some refinements of analogs of Wilson's theorem.) This also implies

$$F_d = (-1)^d \prod_{j=1}^{d-1} [d-j]^{q^j - 1} = (-1)^d D_d / L_d. \tag{1}$$

So let us restate the above well-known analog of Wilson's theorem.

Theorem 2.1. *If $\wp$ is a prime of A of degree d, then*

$$(-1)^d (\mathcal{N}\wp - 1)! = F_d \equiv -1 \bmod \wp.$$

This naturally leads to:

Definition 2.2. A prime $\wp \in A_d$ is a Wilson prime if $F_d \equiv -1 \bmod \wp^2$.

Remarks 2.3. If $d = 1$, then $F_d = -1$. So the primes of degree 1 are Wilson primes. If $\wp(t)$ is Wilson prime, then so are $\wp(t+\theta)$ and $\wp(\mu t)$ for $\theta \in \mathbb{F}_q$ and $\mu \in \mathbb{F}_q^*$ as follows immediately from the formula for F_d.

We introduce some differential, difference and arithmetic differential operators.

Definition 2.4. (1) For $\wp$ as above and $a \in A$, let $Q_\wp(a) := (a^{q^d} - a)/\wp$ be the Fermat quotient. We denote its i-th iteration by $Q_\wp^{(i)}$.

(2) For $a = a(t) \in A$, we denote by $D^{(i)}(a) = a^{(i)}$ its i-th derivative with respect to t. We also use the usual short forms $a' = a^{(1)}$ and $a'' = a^{(2)}$.

(3) We define the higher difference quotients $\Delta^{(i)}(a) = a^{[i]}$ of $a \in A$ (with respect to t and θ to be fixed later) by

$$a^{[0]}(t) = a(t) \quad \text{and} \quad a^{[i+1]}(t) = (a^{[i]}(t) - a^{[i]}(\theta))/(t-\theta).$$

Theorem 2.5. *Let $d := \deg \wp$. If $d = 1$, then $F_d = -1$ and the valuation of $Q_\wp(t)$ at $\wp$ is $q-2$.*

Let $d > 1$ and $k \le q$. Then $F_d \equiv -1 \bmod \wp^k$ if and only if $Q_\wp^{(2)}(t) \equiv 0 \bmod \wp^{k-1}$ if and only if $Q_\wp^{(r)}(t) \equiv 0 \bmod \wp$ for $2 \le r \le k$.

Proof. The $d = 1$ case follows immediately from the definitions. Let $d > 1$. We recall (see, e.g., [Thakur 2004, pp. 7 and 103; 2012, proof of Theorem 7.2]) some facts, which we use below.

(i) The product of elements of $(A/\wp^k)^*$ is -1 unless $q = 2$, $d = 1$, and $k = 2$ or 3, as seen by pairing elements with their inverses and counting order-2 elements.

(ii) The product of all monic elements prime to $\wp$ and of degree i is $D_i/(\wp^r D_{i-d})$, where r is uniquely determined by the condition that the quantity is prime to $\wp$.

(iii) Since the valuation of $[m]$ at $\wp$ is 1 or 0 according to whether d divides m, we have $[i+kd] \equiv [i] \bmod \wp^{q^i}$ and thus $[kd]/\wp \equiv [d]/\wp \bmod \wp^{q^d-1}$ for k a positive integer. In particular, these congruences hold modulo $\wp^q$.

Hence, by (1), we have modulo $\wp^k$ (with s appropriate to make the second quantity below a unit at $\wp$)

$$\begin{aligned}
-1 &\equiv (-1)^d \wp^s \frac{D_{kd} L_{(k-1)d}}{L_{kd} D_{(k-1)d}} \\
&\equiv \bigl((-1)^d [kd-1]^{q-1} \cdots [(k-1)d+1]^{q^{d-1}-1}\bigr) \wp^s [(k-1)d]^{q^d-1} \\
&\qquad \times \bigl([(k-1)d-1]^{q^{d+1}-q} \cdots\bigr) [(k-2)d]^{q^{2d}-q^d} (\cdots) \cdots \\
&\equiv F_d([d]/\wp)^{(q^d-1)+(q^{2d}-q^d)+\cdots} (D_{d-1}^q)^{q^d-1} \bigl(D_{d-1}^{q^{d+1}}\bigr)^{q^d-1} \cdots \\
&\equiv F_d([d]/\wp)^{q^{(k-1)d}-1},
\end{aligned}$$

where we used that, for a prime to $\wp$, we have $a^{q^{id}-1} \equiv 1 \bmod \wp$ and thus $a^{q(q^{id}-1)} \equiv 1 \bmod \wp^q$.

Hence, if $Q_\wp^{(2)}(t)$ is 0 modulo $\wp^{k-1}$, then $([d]/\wp)^{q^d-1} \equiv 1 \bmod \wp^k$, and thus, $F_d \equiv -1 \bmod \wp^k$. Conversely, writing $([d]/\wp)^{q^d-1} = 1 + a\wp$ for some $a \in A$, we see that if $F_d \equiv -1 \bmod \wp^k$, then modulo $\wp^k$, we have

$$1 \equiv (1+a\wp)^{1+q^d+\cdots+q^{(k-2)d}} \equiv 1 + a\wp$$

so that $a\wp \equiv 0$ as desired. The other implications are immediate. □

This generalizes the $k = 2$ case [Sauerberg et al. 2013, Theorem 2.6] with a different manipulation of the quantities even in that case.

Next, we use this to give another criterion for Wilson prime now using the derivative of the Fermat quotient instead of iterated Fermat quotient! For a general study of differential operators in the arithmetic context, their classification and applications, we refer to [Buium 2005] and references there. See also [Ihara 1992].

Theorem 2.6. *Assume $q > 2$ or $d > 1$. The prime $\wp$ is a Wilson prime if and only if $\wp$ divides the derivative of $[d]/\wp$ with respect to t.*

Proof. Let $a = [d]/\wp = \sum a_i t^i$. Then by the binomial theorem, modulo $[d]^2$, we have

$$a^{q^d} - a \equiv \sum a_i t^i \big((t^{q^d-1} - 1 + 1)^i - 1\big) \equiv \sum a_i t^i \binom{i}{1} ([d]/t)^1 \equiv a'[d].$$

(In words, the Frobenius difference quotient $(a^{q^d} - a)/(t^{q^d} - t)$ of $a = Q_\wp(t)$ with respect to t is congruent to the derivative of a with respect to t modulo any prime of degree dividing the degree of $\wp$.) Now since a is square-free and, in particular, not a p-th power, a' is nonzero, and since the valuation of $[d]$ at $\wp$ is 1, the claim follows from Theorem 2.5. □

This reduces computations from dq^d-degree polynomials occurring in F_d to just q^d-degree or from iterates of Fermat quotients to the first one. Also, the derivative kills $1/p$ of the coefficients on average. In fact, we will improve further.

Now we consider $\wp$-adic expansion of t using Teichmüller representatives. Let $A_\wp$ be the completion of A at $\wp$, and let $\mathbb{F}_\wp$ be its residue field. Let $\theta \in \mathbb{F}_\wp$ be the Teichmüller representative of t modulo $\wp$.

Lemma 2.7. *Let $t = \theta + \sum \mu_i \wp^i$ be the $\wp$-adic expansion of t with Teichmüller representatives $\mu_i \in \mathbb{F}_\wp$. Then*

$$\mu_1 = \frac{1}{\wp^{[1]}(\theta)} = \frac{1}{\wp^{(1)}(\theta)} \quad \textit{and} \quad \mu_2 = -\frac{\wp^{[2]}(\theta)}{\wp^{[1]}(\theta)^3}.$$

More generally, if $(t-\theta)^r$ divides $\wp^{[2]}$, then $\mu_i = \wp^{[i]}(\theta) = 0$ for $2 \le i < r$, and for $2 \le i \le r$, we have

$$\mu_i = -\frac{\wp^{[i]}(\theta)}{\wp^{[1]}(\theta)^{i+1}}.$$

Proof. For $d=1$, we have $t=\theta+\wp$, whereas for $d>1$ the expansion is an infinite sum. Noting that $\wp=\prod(t-\theta^{q^i})$, where i runs from 0 to $d-1$, the claim follows inductively on i by starting with the unknown $\wp$-adic expansion and by dividing by $t-\theta$ and then putting $t=\theta$ in each step.

In more detail, in the first step, we have $1=\mu_1\prod_{d>i>0}(t-\theta^{q^i})$ plus terms divisible by $t-\theta$ so that $\mu_1=1/\prod(\theta-\theta^{q^i})=1/\wp^{(1)}(\theta)$. In the next step, we have $-\wp^{[2]}/(\wp^{[1]}(\theta)(\wp^{[1]})^2)=\mu_2+\mu_3(t-\theta)\wp^{[1]}+\cdots$, proving the claim for μ_2. Under the hypothesis of divisibility, the claims are clear inductively on i. □

Remarks 2.8. We record in passing that without any hypothesis as in the second part of Lemma 2.7, a similar manipulation leads to

$$\mu_3=-\frac{\wp^{[3]}(\theta)}{\wp^{[1]}(\theta)^4}+2\frac{\wp^{[2]}(\theta)^2}{\wp^{[1]}(\theta)^5}.$$

Note that the second term vanishes if $\wp^{[2]}(\theta)=0$ (or if $p=2$).

We now use Theorem 2.5 and Lemma 2.7 to get our main theorem, a criterion for Wilson prime in terms of vanishing at θ of the second difference quotient value as well as in terms of the total vanishing of the second derivative of $\wp$ with respect to t:

Theorem 2.9. (i) *A prime $\wp$ is a Wilson prime if and only if $\wp^{[2]}(\theta)=0$.*

(ii) *When $p>2$, $\wp$ is a Wilson prime if and only if $\wp''=d^2\wp/dt^2$ is identically zero. In other words, the Wilson primes are exactly the primes of the form $\sum p_it^i$ with p_i nonzero implying $i\equiv 0, 1 \bmod p$.*

(iii) *When $p>2$, if $\wp$ is a Wilson prime, then the Wilson congruence holds modulo $\wp^{p-1}$. Also, $\wp^{[i]}(\theta)=0$ for $1<i<p$.*

(iv) *When $p=2$, the Wilson primes are exactly the primes of the form $\sum p_it^i$ with p_i nonzero implying $i\equiv 0, 1 \bmod 4$. For such $\wp$, the Wilson congruence holds modulo $\wp^3$, and $\wp^{[i]}(\theta)=0$ for $1<i<4$.*

Proof. We have $Q_\wp(t)=-\mu_1-\mu_2\wp-\cdots-\mu_{q^d-1}\wp^{q^d-2} \bmod \wp^{q^d-1}$ and

$$Q_\wp(Q_\wp(t))=\mu_2+\mu_3\wp+\cdots+\mu_{q^d-1}\wp^{q^d-3} \bmod \wp^{q^d-2}.$$

Hence, (i) follows by Lemma 2.7.

Let $\alpha:=\wp^{(1)}(\theta)$ and $f(t)=\wp(t)-\alpha(t-\theta)$. Then $\wp^{[2]}(\theta)=0$ is equivalent to $(t-\theta)^3$ dividing $f(t)$. This condition implies $f''(\theta)=\wp''(\theta)=0$, but $\wp$ being an irreducible polynomial with θ as a root, this implies that the lower degree second derivative is identically zero. Conversely, $f(\theta)=f'(\theta)=0$ implies, if $d>1$, $f(t)=(t-\theta)^2h(t)$, and $f''(\theta)=0$ then implies that $2h(\theta)=0$ so that if $p>2$, h is divisible by $t-\theta$, implying (ii).

Once the second derivative is identically zero, the higher derivatives are also zero. (Note the $(d+1)$-th derivative or p-th derivative is identically zero anyway for any $\wp$.) The vanishing of first i derivatives implies at least $i+1$ multiplicity for $i<p$, which implies vanishing of higher difference quotients (which decrease in degree by 1 in each step). This implies (iii) by Lemma 2.7 and Theorem 2.5.

Here is an another way to see the last part. If we write $\wp(t)=\sum p_i t^i$, then $\wp(t+\theta)=\sum \alpha_i t^i$ with $\alpha_i=\sum p_k \binom{i}{k}\theta^{k-i}$. Our condition translates to t^3 dividing $f(t+\theta)$ so that $\alpha_2=0$. By Lucas' theorem or directly, if $p=2$, $\binom{i}{2}=0$ implies $\binom{i}{3}=0$ so that $\alpha_3=0$. Similarly, for general p, $\binom{i}{2}=0$ implies $\binom{i}{r}=0$ for $2\le r\le p-1$, implying $\alpha_r=0$ for those r. This also proves (iv). □

Theorem 2.10. *There are infinitely many Wilson primes for* $\mathbb{F}_q[t]$.

Proof. First let q be odd. It is enough to produce infinitely many irreducible elements in A that have powers of t occurring only with exponents that are 0 or 1 modulo p. Let n be a positive integer. Then by consideration of factorization of the cyclotomic polynomial, we see that there are $\phi(q^n-1)/n$ primitive monic polynomials of degree n, where (as usual) we mean by a primitive polynomial of degree n a minimal polynomial over $\mathbb{F}_q$ of a generator of $\mathbb{F}_{q^n}$. For each such irreducible polynomial $P(t)=\sum p_i t^i$, the polynomial $\sum p_i t^{(q^i-1)/(q-1)}$ is of the form we want and is irreducible by a theorem of Ore [1934, Chapter 3, Theorem 1].

The same method works for $q=2^s$ with $s>1$ since the exponents are then 0, 1 mod 4 as we require. The remaining case $q=2$ can not be handled by this method. In this case, applying Serret's theorem [Lidl and Niederreiter 1996, Theorem 3.3.5] (or the special case recalled in [Sauerberg et al. 2013, Theorem 2.8]) to the (Wilson) prime $f(t)=t^4+t+1$ and $s=5^n$, we get infinitely many primes $f(t^{5^n})$, which are Wilson primes by Theorem 2.9(iv). □

Remarks 2.11 (Heuristic counts and exact multiplicity). In the $\mathbb{Z}$ case, the number of Wilson primes less than x grows like $\sum_{p<x} 1/p \sim \log\log(x)$ under the naïve heuristics of $((p-1)!+1)/p$ being randomly distributed modulo p, and we expect at most finitely many primes giving the congruence to power p^3. In [Sauerberg et al. 2013] for some q, we produced families of Wilson primes for A with $\log\log(x)$ growth of the size, but now with Theorem 2.9(ii), we can show that there are many more. In fact, if we let π_d and w_d denote the number of primes and Wilson primes, respectively, of A of degree d, then under the naïve heuristics of randomness of p_i in Theorem 2.9(ii) for primes, we see that as d tends to infinity and $(\log w_d)/(\log \pi_d)$ approaches $2/p$ if p is odd and $1/2$ if $p=2$. It should be possible to prove these asymptotics using Theorem 2.9(ii). In our case, the congruence holds to power $\wp^{p-1}$ for the Wilson primes (to power $\wp^3$ if $p=2$). It is unclear whether this power can be increased for some primes. Though the correspondence of Theorem 2.5 goes up to power $\wp^{q-1}$, the small amount of numerical data calculated by the author's masters student George Todd (for which the author thanks him) showed exactness of the power $\wp^{p-1}$ even for q not prime.

Remarks 2.12. We finish by giving quick sketches of alternate and simplified proofs of earlier results.

(1) We know that for $a \in \mathbb{F}_q$, $\wp = t^p - t - a$ is a prime of A if and only if trace of a to $\mathbb{F}_p$ is nonzero. Assume $\wp$ is a prime and $q = p^m$. Then

$$t^{q^p} = \wp^{p^{mp-1}} + t^{p^{mp-1}} + a^{p^{mp-1}} = \cdots = \wp^{p^{mp-1}} + \wp^{p^{mp-2}} + \cdots + \wp + t$$

so that $Q_\wp(t) = (t^{q^p} - t)/\wp = \wp^{p^{mp-1}-1} + \cdots + \wp^{p-1} + 1$. If $Q_\wp^{(r)}(t)$ denotes the r-th iteration of $Q_\wp$, we see immediately by induction that for $p \geq r > 1$, the valuation at $\wp$ of $Q_\wp^{(r)}(t)$ is $p - r$. Similarly, it is easy to check that $q = 2$ and $\wp = t^4 + t + 1$ satisfies the Wilson congruence modulo $\wp^3$ but not $\wp^4$, and similarly, a calculation as above shows that in this case $Q_\wp^{(3)}(t)$ vanishes modulo $\wp$ but not $Q_\wp^{(4)}(t)$.

This gives another proof of [Thakur 2012, Theorem 7.1], which says that such $\wp$'s are Wilson primes (even to the exact $(p-1)$-th power congruence) if $p > 2$.

(2) Theorem 2.6 allows us to give a simple alternate proof of [Sauerberg et al. 2013, Theorem 2.9]. By the theorem above, $\wp(t)^2$ divides $1 + (t^{q^d} - t)\wp'(t)/\wp(t)$ so that modulo $\wp(t^s)^2$,

$$0 \equiv 1 + \big(t^{s(q^d-1)} - 1\big)t^s\wp'(t^s)/\wp(t^s) \equiv 1 + \big(t^{q^{ds}-1} - 1\big)t\wp'(t^s)st^{s-1}/\wp(t^s),$$

exactly as in the middle part of the proof of [Sauerberg et al. 2013, Theorem 2.9]. This implies by Theorem 2.5 that $\wp(t^s)$ is Wilson prime as desired.

(3) Theorem 2.6 also provides another proof for the reciprocal prime theorem [Sauerberg et al. 2013, Theorem 3.3] when p is odd. If $f(t) = t^d\wp(1/t)$ and $\wp$ is a Wilson prime, then $\wp'' = 0$ and $d(d-1) = 0 \bmod p$ so that taking derivatives with the product and chain rules simplifies to $f'' = -2(d-1)t^{d-3}\wp'(1/t)$, which is 0 if and only if $d \equiv 1 \bmod p$.

Using Theorem 2.9(ii) and (iv), instead of Theorem 2.6, gives even simpler proofs of results in (2) and (3) (and also (1) except for the exactness of the exponent $p-1$ in the modulus). We leave it as a straightforward exercise.

References

[Bhargava 2000] M. Bhargava, "The factorial function and generalizations", *Amer. Math. Monthly* **107**:9 (2000), 783–799. MR 2002d:05002 Zbl 0987.05003

[Buium 2005] A. Buium, *Arithmetic differential equations*, Mathematical Surveys and Monographs **118**, American Mathematical Society, Providence, RI, 2005. MR 2006k:14035 Zbl 1088.14001

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **35**, Springer, Berlin, 1996. MR 97i:11062 Zbl 0874.11004

[Ihara 1992] Y. Ihara, "On Fermat quotients and 'the differentials of numbers"', pp. 324–341 in *Algebraic analysis and number theory* (Kyoto, 1992), edited by T. Kawai, Sūrikaisekikenkyūsho Kōkyūroku **810**, 1992. In Japanese. MR 94m:11136 Zbl 0966.11509

[Lidl and Niederreiter 1996] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1996. MR 97i:11115 Zbl 0866.11069

[Ore 1934] O. Ore, "Contributions to the theory of finite fields", *Trans. Amer. Math. Soc.* **36**:2 (1934), 243–274. MR 1501740 Zbl 0009.10003

[Ribenboim 1996] P. Ribenboim, *The new book of prime number records*, Springer, New York, 1996. MR 96k:11112 Zbl 0856.11001

[Rosen 2002] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **210**, Springer, New York, 2002. MR 2003d:11171 Zbl 1043.11079

[Sauerberg et al. 2013] J. Sauerberg, L. Shu, D. S. Thakur, and G. Todd, "Infinitude of Wilson primes for $\mathbb{F}_q[t]$", *Acta Arith.* **157**:1 (2013), 91–100. Zbl 06113347

[Thakur 2004] D. S. Thakur, *Function field arithmetic*, World Scientific Publishing Co., River Edge, NJ, 2004. MR 2005h:11115 Zbl 1061.11001

[Thakur 2012] D. S. Thakur, "Binomial and factorial congruences for $\mathbb{F}_q[t]$", *Finite Fields Appl.* **18**:2 (2012), 271–282. MR 2890552 Zbl 06017544

Communicated by Andrew Granville
Received 2012-05-09 Revised 2012-09-10 Accepted 2012-10-31

dinesh.thakur@rochester.edu
*1013 Hylan Building, Department of Mathematics,
University of Rochester, RC Box 270138,
Rochester, NY 14627, United States*

Algebra & Number Theory

msp.org/ant

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 7 No. 8 2013