Glasgow Math. J. **50** (2008) 27–32. © 2008 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089507003977. Printed in the United Kingdom

INFINITE HILBERT CLASS FIELD TOWERS OVER CYCLOTOMIC FIELDS

IGOR E. SHPARLINSKI
Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
e-mail: igor@ics.mq.edu.au

(Received 2 June, 2006; revised 8 June, 2007; accepted 24 June, 2007)

Abstract. We use a result of Y. Furuta to show that for almost all positive integers m, the cyclotomic field $\mathbb{Q}(\exp(2\pi i/m))$ has an infinite Hilbert p-class field tower with high rank Galois groups at each step, simultaneously for all primes p of size up to about $(\log\log m)^{1+o(1)}$. We also use a recent result of B. Schmidt to show that for infinitely many m there is an infinite Hilbert p-class field tower over $\mathbb{Q}(\exp(2\pi i/m))$ for some $p \geq m^{0.3385+o(1)}$. These results have immediate applications to the divisibility properties of the class number of $\mathbb{Q}(\exp(2\pi i/m))$.

2000 *Mathematics Subject Classification.* 11N25, 11R17, 11R37.

1. Introduction. For any integer m we let $\zeta_m = \exp(2\pi i/m)$ and consider the cyclotomic field $\mathbb{K}_m = \mathbb{Q}(\zeta_m)$.

In a number of works, see [**3**, **5**, **6**, **7**, **10**, **13**, **14**, **15**] and references therein, one can find various conditions which guarantee that, for a prime p, cyclotomic fields (and also some other fields) contain an infinite *Hilbert p-class field tower*, see [**4**] for terminology. For example, it follows from a result of [**8**], that under some mild conditions on a field $\mathbb{L}$ that the p-rank of the Galois groups in any tower of unramified p-extensions of $\mathbb{L}$ tends to infinity.

Here, we show that a sufficient condition for the existence of such a tower over $\mathbb{K}_m$, given by Y. Furuta [**5**], combined with a result of K. K. Norton [**11**], implies that for almost all positive integers m, $\mathbb{K}_m$ has an infinite Hilbert p-class field tower for every prime p of size up to about $(\log\log m)^{1+o(1)}$. Moreover, for each of these primes p, the Galois group at each step is of p-rank at least $(\log\log m)^{1+o(1)}$. Thus in the case of $\mathbb{K}_m$ this complements a result of [**8**] which applies to sufficiently large steps.

This also implies that for almost all m the class number h_m of $\mathbb{K}_m$ is divisible by all primes p of size up to about $(\log\log m)^{1+o(1)}$.

We also combine a certain characterisation of B. Schmidt [**13**] of cyclotomic fields having infinite Hilbert p-class field towers with a result of R. C. Baker and G. Harman [**1**] about shifted primes with a large prime divisor, to show that for infinitely many m, the field $\mathbb{K}_m$ has an infinite Hilbert p-class field tower for a rather large p. Moreover, a different construction (based on a combination of [**2**] and [**5**]) allows us to control the p-rank of the corresponding Galois groups.

Throughout this paper, for any real number $x > 0$ and any integer $\nu \geq 1$, we write $\log_\nu x$ for the function defined inductively by $\log_1 x = \max\{\log x,\ 1\}$ (where $\log x$ is the natural logarithm of x), and $\log_\nu x = \max\{\log(\log_{\nu-1} x),\ 1\}$ for $\nu > 1$. When $\nu = 1$, we omit the subscript in order to simplify the notation; however, we continue to assume that $\log x \geq 1$ for any $x > 0$.

In what follows, we use the Landau symbol O, as well as the Vinogradov symbols $\ll$, $\gg$ and $\asymp$ with their usual meanings, where all implied constants are *absolute*. We recall that the notations $A \ll B$, $B \gg A$ and $A = O(B)$ are equivalent, and that $A \asymp B$ is equivalent to $A \ll B \ll A$. We always use the letters ℓ, p and q to denote prime numbers, while m and n always denote positive integers.

2. Results.

We start with establishing a result for almost all m.

THEOREM 1. *Let x be a sufficiently large real number. Them for all $m \leq x$ except possibly $O(x(\log_2 x)^{-0.08})$ of them, $\mathbb{K}_m$ has an infinite Hilbert p-class field tower, such that the Galois group at each step is of p-rank at least*

$$s_p = \left\lceil \frac{(\log_2 x)^2}{9(p-1)^2} \right\rceil$$

for all primes

$$p \leq \frac{\log_2 x}{10 \log_3 x}.$$

Proof. For a prime p and an integer $m \geq 1$, we denote by $\omega_p(m)$ the number of distinct prime factors q of m such that $q \equiv 1 \pmod p$. It follows immediately from Theorem 6.27 of [**11**] (applied with $L = \{1\}$ and $\alpha = 1/2$) that for $p = o(\log_2 x)$, the set $\mathcal{E}_p(x)$ of $m \leq x$ with

$$\omega_p(m) \leq \frac{\log_2 x}{2(p-1)}$$

is of cardinality at most

$$\#\mathcal{E}_p(x) \leq x \exp\left(-(\vartheta + o(1))\frac{\log_2 x}{p-1}\right),$$

where

$$\vartheta = \frac{3}{2}\log\frac{3}{2} - \frac{1}{2} = 0.10819\ldots.$$

On the other hand, by Theorem 4 of [**5**], we have that if

$$\omega_p(x) \geq \left\lceil 4 + 2\sqrt{s+4} \right\rceil$$

then $\mathbb{K}_m$ has an infinite Hilbert p-class field tower, such that the Galois group at each step is of p-rank at least s. Thus for every $p = o(\log_2 x)$ and $m \leq x$ which is not in $\mathcal{E}_p(x)$, we see that $\mathbb{K}_m$ satisfies the required property with $s = s_p$, provided that x is large enough.

It remains to note that for

$$y = \frac{\log_2 x}{10 \log_3 x}$$

we have

$$\sum_{p\le \log_2 x/10\log_3 x} \#\mathcal{E}_p(x) \le x \sum_{p\le \log_2 x/10\log_3 x} \exp\left(-(\vartheta+o(1))\frac{\log_2 x}{p-1}\right)$$
$$\le x(\log_2 x)^{-10(\vartheta+o(1))}\pi(\log_2 x/10\log_3 x)$$
$$\le x(\log_2 x)^{-0.08}.$$

where we used the trivial bound $\pi(y) \le y$ on the number of primes $p \le y$. □

Since for a sufficiently large x we always have $s_p \ge 9$, as in Theorem 4 of [**5**], we derive the following statement about divisibility of the class number h_m of $\mathbb{K}_m$.

COROLLARY 2. *Let x be a sufficiently large real number. Them for all $m \le x$ except possibly $O(x(\log_2 x)^{-0.08})$ of them, h_m is divisible by all primes*

$$p \le \frac{\log_2 x}{10\log_3 x}.$$

In particular

$$\omega(h_m) \gg \frac{\log_2 x}{(\log_3 x)^2}$$

for almost all $m \le x$, where $\omega(k)$ denotes the number of distinct prime divisors of $k \ge 1$.

We now consider extremal values.

THEOREM 3. *There are infinitely many m such that $\mathbb{K}_m$ has an infinite Hilbert p-class field tower for some prime*

$$p \ge m^{0.3385+o(1)}.$$

Proof. For two integers r and s with $\gcd(r, s) = 1$ we denote by $\mathrm{ord}_r s$ the multiplicative order s modulo r.

It is shown in Corollary 5.9 of [**13**] that if $m = kq$ where k is an integer and q is a prime with

$$q \equiv 1 \pmod p, \qquad \gcd(k, q) = 1, \qquad q^n \not\equiv -1 \pmod k, \tag{1}$$

for $n = 1, 2, \dots$ (that is, -1 is not a power of q modulo k), and also such that

$$\frac{\varphi(k)}{\mathrm{ord}_k q} \ge 8p + 12, \tag{2}$$

where $\varphi(k)$ is the Euler function, then $\mathbb{K}_m$ has an infinite Hilbert p-class field tower.

We now show that there are infinitely many pairs (m, p) which satisfy (1) and are (2) and are such that $p \ge m^{0.3385+o(1)}$.

Let $P(k)$ denotes the largest prime divisor of $k \ge 1$ (with $P(1) = 1$). By [**1**] we see that for any $y > 1$ we have $P(q-1) \ge q^{0.677}$ for at least $A(y) \gg y/\log y$ primes $q \le y$.

On the other hand, by the Brun sieve (see Theorem 2.2 in [**9**]) the number of $q \le y$ for which $q-1$ does not have an odd prime divisor ℓ in the interval $\log_2 y \le \ell \le \log y$

is

$$B(y) \ll \frac{y}{\log y} \prod_{\log_2 y \le \ell \le \log y} \left(1 - \frac{1}{\ell}\right) \ll \frac{y \log_3 y}{\log y \log_2 y},$$

by the Mertens formula (see Theorem 3.1 of Chapter 1 in [**12**]). Therefore, $B(y) = o(A(y))$ and there are infinitely many primes q such that $P(q-1) \ge q^{0.677}$ and $q \equiv 1 \pmod{\ell}$ for some prime $\log_2 q \le \ell \le \log q$.

Put $p = P(q-1)$ and $m = kq$ where $k = \ell(q+1)$. Since $q \equiv 1 \pmod{\ell}$, we obviously have (1). To verify (2), we note that $\mathrm{ord}_k q = 2$. Then

$$\frac{\varphi(k)}{\mathrm{ord}_k q} \ge \frac{\varphi(\ell(q+1))}{2} = \frac{(\ell-1)\varphi(q+1)}{2} \gg \frac{\ell q}{\log_2 q},$$

by the well-known lower bound on the Euler function (see Theorem 5.1 in Chapter 1 of [**12**]).

Since $p \le (q-1)/\ell$ and $\ell \ge \log_2 q$ we see that (2) holds as well.

It remains to note that

$$p \gg q^{0.677} \ge (m/\ell(q+1))^{0.677} = m^{0.3385+o(1)}$$

since $q = m^{1/2+o(1)}$. □

We now immediately obtain the following conclusion about the largest prime divisor $P(h_m)$ of the class number h_m of $\mathbb{K}_m$.

COROLLARY 4. *There are infinitely many m such that $P(h_m) \ge m^{0.3385+o(1)}$.*

Finally, we show an analogue of Theorem 3 for towers of a prescribed p-rank of their Galois groups.

THEOREM 5. *For any integer s, there are infinitely many m such that $\mathbb{K}_m$ has an infinite Hilbert p-class field tower such that the Galois group at each step is of p-rank at least s for some prime*

$$p \ge m^{\alpha_s + o(1)},$$

where

$$\alpha_s = \frac{17}{128 + 64\sqrt{3+s}}.$$

Proof. Let

$$t = \left\lfloor 4 + 2\sqrt{3+s} \right\rfloor.$$

By Theorem 4 of [**5**] it is enough to construct a square free m with $\omega_p(m) \ge t$, for some prime satisfying the inequality of the theorem, where, as before, $\omega_p(m)$ denotes the number of distinct prime factors q of m such that $q \equiv 1 \pmod{p}$.

Also, as before, we use $P(k)$ to denote the largest prime divisor of $k \ge 1$ (with $P(1) = 1$). Given two positive constant η and c, we consider the set of primes

$$\mathcal{P}_{a,\eta,c}(z) = \{p \le z \ : \ p = P(q-a) \text{ for some prime } q \text{ with } p^\eta < q < c\,p^\eta\}.$$

By Theorem 1 of [**2**] for any η with $32/17 < \eta < (4+3\sqrt{2})/4$, there is a constant c_η such that

$$\#\mathcal{P}_{a,\eta,c_\eta}(z) = (1+o(1))\pi(z)$$

as $z \to \infty$. Let us fix some $\varepsilon > 0$. Then we see that for any η in the interval $32/17 < \eta < (4+3\sqrt{2})/4$ and sufficiently small $\varepsilon > 0$ (to satisfy $\eta + (t-1)\varepsilon < (4+3\sqrt{2})/4$) and sufficiently large z, there is a prime p such that $z/2 \le p \le z$ and

$$p \in \bigcap_{\nu=0}^{t-1} \mathcal{P}_{a,\eta+\nu\varepsilon,c_{\eta+\nu\varepsilon}}(z).$$

Thus there are t distinct primes $q_\nu \equiv 1 \pmod p$ with $q_\nu \ll p^{\eta+\nu\varepsilon} \le p^{\eta+\nu\varepsilon}$, $\nu = 0,\dots,t-1$. Then for $m = q_1 \dots q_t$ we clearly have $\omega_p(m) \ge t$. On the other hand

$$m \le p^{t\eta + t^2\varepsilon}$$

and since $\eta > 32/17$ and $\varepsilon > 0$ are arbitrary, the result follows. □

3. Concluding Remarks. It would be interesting to find some arithmetic conditions on m which imply that $\mathbb{K}_m$ does not have an infinite Hilbert p-class field tower, and thus try to get some lower bounds on the size of the exceptional set of Theorem 1.

It is clear that any refinement of Theorem 3 is possible only if a result of [**1**] is improved. However, Theorem 5 in the case $s = 1$ does not give Theorem 3 and thus there could be some more realistic opportunities for further improvement.

Finally, one can probably find some other parametric families algebraic number fields having an infinite Hilbert p-class field tower provided the corresponding parameters satisfy certain concise arithmetic conditions. This may potentially lead to some interesting number theoretic problems.

ACKNOWLEDGEMENTS. The author is grateful to Florian Luca and Bernhard Schmidt for several very useful discussions and helpful comments. This work was done during a pleasant visit by the author to the Nanyang Technological University, Singapore, whose support and hospitality are gratefully acknowledged. During the preparation of this paper, the author was also supported in part by ARC grant DP0556431.

REFERENCES

1. R. C. Baker and G. Harman, Shifted primes without large prime factors, *Acta Arith.* **83** (1998), 331–361.

2. W. D. Banks and I. E. Shparlinski, On values taken by the largest prime factor of shifted primes, *J. Aust. Math. Soc.* **82** (2007), 133–147.

3. A. Brumer, Ramification and class towers of number fields, *Michigan Math. J.* **12** (1965), 129–131.

4. J. W. S. Cassels and A. Froehlich, *Algebraic number theory* (Academic Press, London 1967).

https://doi.org/10.1017/S0017089507003977 Published online by Cambridge University Press

5. Y. Furuta, On class field towers and the rank of ideal class groups, *Nagoya Math. J.* **48** (1972), 147–157.

6. F. Gerth III, On cyclic fields of odd prime degree p with infinite Hilbert p-class field towers, *Canad. Math. Bull.* **45** (2002), 86–88.

7. F. Gerth III, A density result for some imaginary quadratic fields with infinite Hilbert 2-class field towers, *Arch. Math.* (*Basel*) **82** (2004), 23–27.

8. F. Hajir, On the growth of p-class groups in p-class field towers, *J. Algebra* **188** (1997), 256–271.

9. H. Halberstam and H.-E. Richert, *Sieve methods* (Academic Press, London, 1974).

10. F. Lemmermeyer, Ideal class groups of cyclotomic number fields, II, *Acta Arith.* **84** (1998), 59–70.

11. K. K. Norton, On the number of restricted prime factors of an integer, I, *Illinois J. Math.* **20** (1976), 681–705.

12. K. Prachar, *Primzahlverteilung* (Springer-Verlag, 1957).

13. B. Schmidt, The field descent and class groups of CM-fields, *Acta Arith.* **119** (2005), 291–306.

14. R. Schoof, Infinite class field towers of quadratic fields, *J. Reine Angew. Math.* **372** (1986), 209–220.

15. T. Takeuchi, Notes on the class field towers of cyclic fields of degree l, *Tôhoku Math. J.* **31** (1979), 301–307.