Class numbers in cyclotomic $\mathbb{Z}_p$-extensions

John Miller

Rutgers University

ANTS XI - Rump Session
August 10, 2014

Cyclotomic $\mathbb{Z}_p$-extensions

Let $\mathbb{B}_{p^n}$ denote the nth layer of the cyclotomic $\mathbb{Z}_p$-extension of the rationals, i.e. the unique real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{p^{n+2}})$ that has degree p^n over $\mathbb{Q}$.

$\mathbb{B}_{p^\infty} = \bigcup_{n\geq 1} \mathbb{B}_{p^n}$ is called the **cyclotomic $\mathbb{Z}_p$-extension of** $\mathbb{Q}$. Its Galois group over $\mathbb{Q}$ is isomorphic to the p-adic integers $\mathbb{Z}_p$.

Hence the name.

A Big Question

Let h_{p^n} denote the class number of $\mathbb{B}_{p^n}$.

A Big Question: Is h_{p^n} ever not equal to 1? Does it have any prime divisors?

Let's consider the evidence...

The Evidence: no prime divisors of h_{p^n} so far...

(Weber, 1886) h_{2^n} odd for all n.

(Fukuda-Komatsu, 2011) h_{2^n} has no prime divisors less than 10^9, for all n.

(Fukuda-Komatsu-Morisawa, 2014) h_{3^n} has no prime divisors less than 10^9, for all n.

(Iwasawa, 1956) h_{p^n} not divisible by p, for all n.

(Ichimura-Nakajima, 2010) h_{p^n} is odd, for all n and primes $p < 500$.

The few h_{p^n} that are known all have class number 1.

$\mathbb{B}_{p,n}$	Class number	
$\mathbb{B}_{2^6}$	1	M. (2013)
$\mathbb{B}_{2^7}$	1 (under GRH)	M. (2013)
$\mathbb{B}_{3^3}$	1	Masley (1978)
$\mathbb{B}_{3^4}$	1 (under GRH)	van der Linden (1982)
$\mathbb{B}_{5^2}$	1	M. (2014)
$\mathbb{B}_{7^1}$	1	Bauer (1969)
$\mathbb{B}_{11^1}$	1	M. (2014)
$\mathbb{B}_{13^1}$	1	M. (2014)
$\mathbb{B}_{17^1}$	1	M. (2014)
$\mathbb{B}_{19^1}$	1	M. (2014)
$\mathbb{B}_{23^1}$	1 (under GRH)	Pari via SageMathCloud
$\mathbb{B}_{29^1}$	1 (under GRH)	Pari via SageMathCloud
$\mathbb{B}_{31^1}$	1 (under GRH)	Pari via SageMathCloud

What do the Cohen-Lenstra heuristics suggest?

$$P_T = \prod_{p \text{ prime}} \prod_{\substack{q \text{ prime} \\ q \neq p}} \prod_{j \geq 2} \prod_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f}$$

is the "probability" (in the Bayesian sense) that $h_{p^n} = 1$ for all p and n. Here f is the order of q modulo p^j.

We can think of

$$-\log P_T = -\sum_{p \text{ prime}} \sum_{\substack{q \text{ prime} \\ q \neq p}} \sum_{j \geq 2} \sum_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f}$$

as the number of expected exceptions to $h_{p^n} = h_{p^{n-1}}$.

What about that quadruple sum?

Buhler, Pomerance and Robertson (2003) proved that the sum is finite,

$$-\log P_T = -\sum_{p \text{ prime}} \sum_{\substack{q \text{ prime} \\ q \neq p}} \sum_{j \geq 2} \sum_{k \geq 2} (1 - q^{-fk})^{\phi(p^j)/f} < \infty,$$

and conjectured that the number of expected exceptions to $h_{p^n} = h_{p^{n-1}}$ is finite.

What's new?

Using an explicit sieve result of Siebert (1976) and refining our sum by excluding terms the correspond to primes that we already know do now divide h_{p^n}, we can prove that

$$-\log P_T = -\sum_{p \text{ prime}} \sum_{\substack{q \text{ prime} \\ \text{excluding terms where the} \\ q\text{-part of the class group} \\ \text{is known to be trivial}}} \sum_{j=1}^{\infty} \sum_{k \geq 2} \frac{\phi(p^j)}{f} \log(1 - q^{-fk}) < 0.33$$

and so

$$P_T > 72\%$$

The Conjecture

This suggests the following conjecture:

For **any** prime p and positive integer n,

$$h_{p^n} = 1.$$