Wolstenholme and Vandiver primes

Shehzad Hathi
UNSW Canberra at ADFA

Joint work with Michael Mossinghoff (CCR Princeton) & Tim Trudgian (UNSW Canberra)

October 8, 2020

Contents

1. Introduction
2. Search for new Wolstenholme and Vandiver primes
3. Future work

Irregular primes

A prime p is said to be *irregular* if p divides the class number of the cyclotomic field $\mathbb{Q}(\zeta_p)$, where $\zeta_p = e^{2\pi i/p}$.

Equivalently, p is irregular if p divides the numerator of any of the Bernoulli numbers B_{2k} with $0 < 2k \leq p - 3$ where B_k is the coefficient in the series expansion

$$\frac{z}{e^z - 1} = \sum_{k \geq 0} B_k \frac{z^k}{k!}.$$

Wolstenholme prime

We have the following result due to Wolstenholme for every odd prime p

$$\sum_{0<k<p} \frac{1}{k^2} \equiv 0 \mod p, \ \sum_{0<k<p} \frac{1}{k} \equiv 0 \mod p^2, \ \binom{2p-1}{p-1} \equiv 1 \mod p^3.$$

A *Wolstenholme prime* is an odd prime p such that

$$\binom{2p-1}{p-1} \equiv 1 \mod p^4.$$

Glaisher's congruence

Due to Glaisher, we know that

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}p^3 B_{p-3} \mod p^4.$$

Thus, p is a Wolstenholme prime if and only if p divides the numerator of the Bernoulli number B_{p-3}.

Only two Wolstenholme primes (16843 and 2124679) are known.

Vandiver primes

The Euler numbers E_k are coefficients in the series expansion

$$\sec(z) = \sum_{k \geq 0} E_k \frac{z^k}{k!}.$$

A prime p is *E-irregular* if p divides any of the Euler numbers E_{2k} with $0 < 2k \leq p - 3$.

A prime p is called a *Vandiver prime* if it divides the Euler number E_{p-3}.

Stafford and Vandiver congruence

In 1930, Stafford and Vandiver established that

$$\frac{3^{p-2k}+4^{p-2k}-6^{p-2k}-1}{4k}B_{2k} \equiv \sum_{p/6<s<p/4} s^{2k-1} \mod p$$

For $2k = p - 3$, this becomes

$$B_{p-3} \equiv \frac{1}{27} \sum_{p/6<s<p/4} \frac{1}{s^3} \mod p.$$

Notation for congruences

For real numbers $x < y$ in $[0,1]$, let

$$S_\ell(x,y) = \sum_{xp<s<yp} s^\ell \mod p,$$

and let

$$C_k(a,b,c) = \frac{a^{p-2k} + b^{p-2k} - c^{p-2k} - 1}{4k}.$$

With the above notation, Stafford and Vandiver's congruence becomes

$$C_k(3,4,6)B_{2k} \equiv S_{2k-1}\left(\frac{1}{6},\frac{1}{4}\right) \mod p.$$

Tanner and Wagstaff congruences

In 1987, Tanner and Wagstaff developed a family of congruences:

$$C_k(2, b, b+1)B_{2k} \equiv \sum_{m=1}^{\lfloor b/2 \rfloor} S_{2k-1}\left(\frac{m}{b+1}, \frac{m}{b}\right) \mod p$$

which has cost $\frac{\lfloor b/2 \rfloor(\lfloor b/2 \rfloor + 1)}{2b(b+1)}p$, so asymptotically $p/8$.

The special case $b = 5$ was proved by Vandiver in 1937:

$$C_k(2, 5, 6)B_{2k} \equiv S_{2k-1}\left(\frac{1}{6}, \frac{1}{5}\right) + S_{2k-1}\left(\frac{1}{3}, \frac{2}{5}\right) \mod p.$$

Congruence transformations

(a) Separation (σ_f):

$$S_\ell(x,y) = S_\ell\left(x, x + f \cdot (y - x)\right) + S_\ell\left(x + f \cdot (y-x), y\right).$$

(b) Reflection (ρ):

$$S_\ell(x,y) \equiv (-1)^\ell S_\ell(1-y, 1-x) \mod p.$$

(c) Subdivision (τ_d): If d is a positive integer and $p \nmid d$, then

$$S_\ell(x,y) \equiv d^\ell \sum_{i=0}^{d-1} S_\ell\left(\frac{x+i}{d}, \frac{y+i}{d}\right) \mod p.$$

Derived congruence

Using the transformations, one can convert Vandiver's congruence

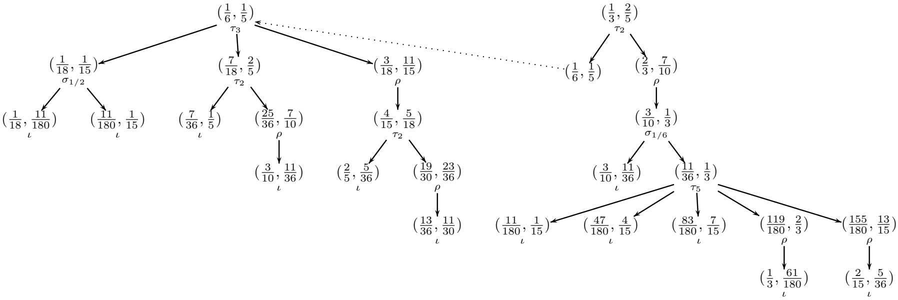
$$C_k(2,5,6)B_{2k} \equiv S_{2k-1}\left(\frac{1}{6},\frac{1}{5}\right) + S_{2k-1}\left(\frac{1}{3},\frac{2}{5}\right) \mod p.$$

to this nine-term congruence with cost $p/20$:

$$\begin{aligned} C_k(2,5,6)B_{2k} \equiv &(3^t+6^t)S_t(\tfrac{1}{18},\tfrac{11}{180}) + (3^t+6^t-10^t)S_t(\tfrac{11}{180},\tfrac{1}{15}) \\ &-(6^t-10^t+12^t)S_t(\tfrac{2}{15},\tfrac{5}{36}) + (6^t+12^t)S_t(\tfrac{7}{36},\tfrac{1}{5}) \\ &-10^tS_t(\tfrac{47}{180},\tfrac{4}{15}) - (2^t+6^t+12^t)S_t(\tfrac{3}{10},\tfrac{11}{36}) + 10^tS_t(\tfrac{1}{3},\tfrac{61}{180}) \\ &+(6^t+12^t)S_t(\tfrac{13}{36},\tfrac{11}{30}) - 10^tS_t(\tfrac{83}{180},\tfrac{7}{15}) \mod p, \end{aligned}$$

where $t = 2k-1$.

Transformation graph



Near misses for Wolstenholme primes

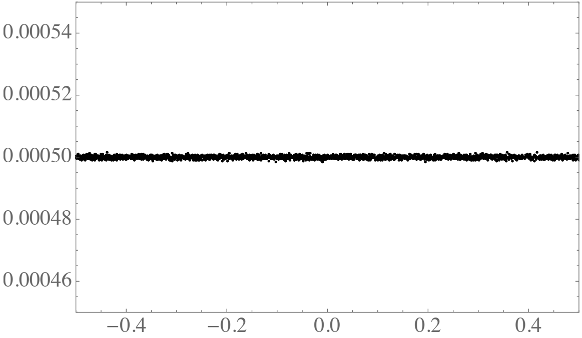
Table: Primes $p \in (10^9, 5 \cdot 10^{10})$ for which $|\langle B_{p-3} \rangle_p| < 50$.

p	$\langle B_{p-3} \rangle_p$
1025793739	-9
1029113299	-7
1939582759	-19
2139716869	2
3803691517	13
8208762073	24
9267199079	-22
13581221947	40
14211360143	-41

p	$\langle B_{p-3} \rangle_p$
15744104053	-2
16425136499	7
21861395221	-11
22855335949	33
23345427659	-27
23543635009	-21
27827984099	34
40306537633	42
44718258259	-6

Histogram for Bernoulli numbers

Figure: Histogram for $\langle B_{p-3} \rangle_p / p$ for $p < 5 \cdot 10^{10}$.



Near misses for Vandiver primes

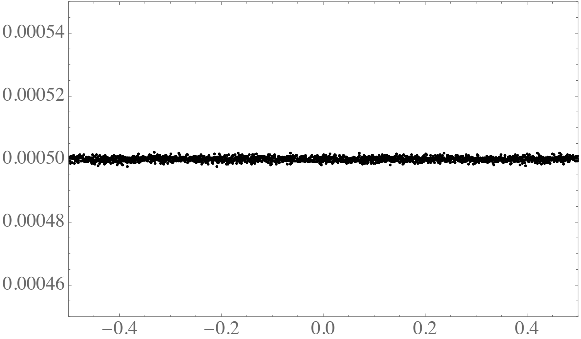
Table: Primes $p \in (10^9, 2.5 \cdot 10^{10})$ for which $|\langle E_{p-3} \rangle_p| < 50$.

p	$\langle E_{p-3} \rangle_p$
1062232319	0
1348936931	17
1352698411	-17
1836806681	-15
2114780851	2
2161739347	-32
2264214119	38
2978890751	35

p	$\langle E_{p-3} \rangle_p$
3700821251	23
10158743171	-49
10179358499	-12
14884379297	-40
17380814081	5
18642203467	34
18044797027	-10
23177794127	-48

Histogram for Euler numbers

Figure: Histogram for $\langle E_{p-3} \rangle_p / p$ for $p < 2.5 \cdot 10^{10}$.



Further questions

How small can the cost of a congruence be?

Starting from Vandiver's congruence again, we can find a 546 term congruence with cost $p/40.5$.

What is the optimal number of terms for a congruence with a certain cost?