Resolving Grosswald's conjecture on GRH

Enrique Treviño

joint work with **Kevin McGown**[1] and **Tim Trudgian**[2]

Carl Pomerance 70th birthday conference
June 11, 2015

LAKE FOREST
COLLEGE

[1] California State University, Chico
[2] Australian National University

Primitive Roots

Let p be a prime number. Then g is a primitive root modulo p if

$$< g >= \{1, 2, 3, \ldots, p-1\},$$

or

$$g^k = 1 \text{ if and only if } (p-1)|k,$$

or

$$\frac{\phi(p-1)}{p-1}\left(1 + \sum_{\substack{d|p-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi \bmod p \\ \chi \text{ has order } d}} \chi(n)\right) = 1.$$

Least primitive root

How big can the least primitive root be?

p	Least primitive root
2	1
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2
31	3
37	2

Primitive Root Champions

p	Least primitive root
3	2
7	3
23	5
41	6
71	7
191	19
409	21
2161	23
5881	31
36721	37
55441	38
71761	44
110881	69
760321	73

Prime Primitive Roots Champions

p	Least primitive root	Least **prime** primitive root
7	3	3
23	5	5
41	6	7
109	6	11
191	19	19
271	6	43
2791	6	53
11971	10	79
31771	10	107

The least primitive root champions happen at the following p:
$7, 23, 41, 109, 191, 271, 2791, 11971, 31771$.
The least **prime** primitive roots happen at the following p:
3, 7, 23, 41, 71, 191, 409, 2161, 5881, 36721, 55441, 71761, 110881, 760321.

Theorems on the least primitive roots mod$p$

Let $g(p)$ be the least primitive root mod$p$.

- Unconditionally, Burgess (1960s) showed

$$g(p) \ll_{\varepsilon} p^{\frac{1}{4}+\varepsilon}.$$

- **Under GRH**, Ankeny (1952) showed

$$g(p) \ll \left(2^{\omega(p-1)} \log p \left(\log\left(2^{\omega(p-1)} \log p\right)\right)\right)^2.$$

- **Under GRH**, Wang (1959) showed

$$g(p) \ll (\omega(p-1))^6 \log^2 p.$$

- **Under GRH**, Shoup (1992) showed

$$g(p) \ll (\omega(p-1))^4 (\log(\omega(p-1)+1))^4 \log^2 p.$$

Grosswald's Conjecture

Conjecture (Grosswald)

For all primes $p > 409$,

$$g(p) < \sqrt{p} - 2.$$

Theorem (Grosswald, 1982)

For $p \geq 1 + e^{e^{24}} \approx 10^{10^{10}}$,

$$g(p) \leq p^{0.499}.$$

Theorem (Cohen, Oliveira e Silva, Trudgian, 2015)

For $409 < p < 2.5 \times 10^{15}$ *or* $p > 3.67 \times 10^{71}$,

$$g(p) < \sqrt{p} - 2.$$

Grosswald under GRH and an explicit upper bound

Theorem (McGown, Trudgian, T.)

Assuming the Generalized Riemann Hypothesis for Dirichlet L functions for all $p \geq 10^{14}$,

$$g(p) < \sqrt{p} - 2.$$

Furthermore if $\hat{g}(p)$ *is the least prime primitive root, then*

$$\hat{g}(p) < \sqrt{p} - 2.$$

Theorem (McGown, Trudgian, T.)

Assuming GRH. For $p \geq 10^9$,

$$\hat{g}(p) \leq \left(\frac{8}{5} 2^{\omega(p-1)} \log p\right)^2.$$

Sketch of Proof

Let $f(n)$ be the characteristic function for a primitive root, i.e.,

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is a primitive root,} \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$f(n) = \frac{\phi(p-1)}{p-1}\left(1 + \sum_{\substack{d|p-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi \bmod p \\ \chi \text{ has order } d}} \chi(n)\right).$$

Proof continued

$$f(n) = \frac{\phi(p-1)}{p-1}\left(1 + \sum_{\substack{d|p-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi \bmod p \\ \chi \text{ has order } d}} \chi(n)\right).$$

Suppose that for all $n \leq x$, n is not a primitive root. Then

$$\frac{p-1}{\phi(p-1)} f(n)\Lambda(n)\left(1 - \frac{n}{x}\right) = 0 \quad \text{for all } n.$$

Then summing over all $n \leq x$ and changing order of summation we get

$$\sum_{n \leq x} \Lambda(n)\left(1 - \frac{n}{x}\right) + \sum_{\substack{d|p-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\substack{\chi \bmod p \\ \chi \text{ has order } d}} \sum_{n \leq x} \chi(n)\Lambda(n)\left(1 - \frac{n}{x}\right) = 0.$$

$$\sum_{n\leq x}\Lambda(n)\left(1-\frac{n}{x}\right)+\sum_{\substack{d|p-1\\ d>1}}\frac{\mu(d)}{\phi(d)}\sum_{\substack{\chi \bmod p\\ \chi \text{ has order } d}}\sum_{n\leq x}\chi(n)\Lambda(n)\left(1-\frac{n}{x}\right)=0.$$

We have

$$\sum_{n\leq x}\Lambda(n)\left(1-\frac{n}{x}\right)\approx\sum_{n\leq x}\left(1-\frac{n}{x}\right)\approx\frac{x}{2},$$

and using GRH

$$\left|\sum_{n\leq x}\chi(n)\Lambda(n)\left(1-\frac{n}{x}\right)\right|=O\left(\sqrt{x}\log p\right).$$

Therefore

$$\frac{x}{2}=O\left((2^{\omega(p-1)}-1)\sqrt{x}\log p\right).$$

It follows that

$$\hat{g}(p)=O\left(\left((2^{\omega(p-1)}-1)\log p\right)^2\right).$$

Sieve

- From this inequality (when made explicit), one can show that for $p \geq 10^{43}$, then $\hat{g}(p) < \sqrt{p} - 2$. An extra idea is needed to cover $2.5 \times 10^{15} < p < 10^{43}$.
- Let e be an even divisor of $p-1$. Let $p_1, p_2, \ldots, p_s$ be the primes dividing $p-1$ that do not divide e. Set

$$\delta = 1 - \sum_{i=1}^{s} \frac{1}{p_i}.$$

Theorem (McGown, Trudgian, T.)

Assume GRH. Then for $p \geq 10^9$, we have

$$\hat{g}(p) \leq \left(\frac{1}{5} + \frac{14}{9} \left(2 + \frac{s-1}{\delta} \right) 2^{n-s} \log p \right)^2.$$

Theorem

Theorem (McGown, Trudgian, T.)

Assuming the Generalized Riemann Hypothesis for Dirichlet L functions. For all $p > 409$,

$$g(p) < \sqrt{p} - 2.$$

Furthermore if $p > 2791$, *then*

$$\hat{g}(p) < \sqrt{p} - 2.$$

Thank you!

Happy 70th Birthday Carl!