# Thoughts on the order of $a$ mod $p$

Paul Pollack, UGA

2020 AMS Southeastern Sectional Meeting

October 2020

# Best laid schemes...

When I signed up to give this talk, my plan was to discuss two recent papers, both of which concern orders of integers mod $p$, where $p$ is prime.

Both papers are joint work, but with different authors, namely ...

# Best laid schemes...

When I signed up to give this talk, my plan was to discuss two recent papers, both of which concern orders of integers mod $p$, where $p$ is prime.

Both papers are joint work, but with different authors, namely ...

Zeb Engberg, Wasatch Academy

Komal Agrawal, UGA

## . . . gang aft agley

When I got around to preparing this talk (later rather than sooner), I realized this plan was too ambitious. So with apologies to Zeb, this talk will concentrate on the work with Komal.

For the curious, the paper with Zeb (to appear in Acta Arith.) can be found at my website:

The reciprocal sum of divisors of Mersenne numbers
*Acta Arith.*, to appear.
`pollack.uga.edu/research.html`

# Out of chaos. . .

Let $a$ be an integer, $a \neq 0, \pm 1$. For each integer $m$ relatively prime to $a$, we define

$$\ell_a(m) = \text{multiplicative order of } a \bmod m.$$

In other words, $\ell_a(m)$ is the least positive integer $\ell$ for which

$$a^\ell \equiv 1 \pmod{m}.$$

Fermat/Euler: $\ell_a(m) \mid \varphi(m)$, and in particular, $\ell_a(p) \mid p - 1$.

# Out of chaos...

Let $a$ be an integer, $a \neq 0, \pm 1$. For each integer $m$ relatively prime to $a$, we define

$$\ell_a(m) = \text{multiplicative order of } a \bmod m.$$

In other words, $\ell_a(m)$ is the least positive integer $\ell$ for which

$$a^\ell \equiv 1 \pmod{m}.$$

Fermat/Euler: $\ell_a(m) \mid \varphi(m)$, and in particular, $\ell_a(p) \mid p - 1$.

We are interested in understanding the distribution of $\ell_a(p)$ as $p$ varies, with $a$ fixed, or $a$ belonging to a finite set.

# Artin's primitive root conjecture

## Conjecture (E. Artin, 1927)

*Fix $a \in \mathbb{Z}$, not a square, and not $\pm 1$. There are infinitely many primes $p$ for which $\ell_a(p) = p - 1$. In fact, the number of primes $p \leq x$ with $\ell(p) = p - 1$ is*

$$\sim C(a)\pi(x),$$

*where $C(a)$ is an explicitly described positive constant.*

# Artin's primitive root conjecture

## Conjecture (E. Artin, 1927)

*Fix $a \in \mathbb{Z}$, not a square, and not $\pm 1$. There are infinitely many primes $p$ for which $\ell_a(p) = p - 1$. In fact, the number of primes $p \le x$ with $\ell(p) = p - 1$ is*

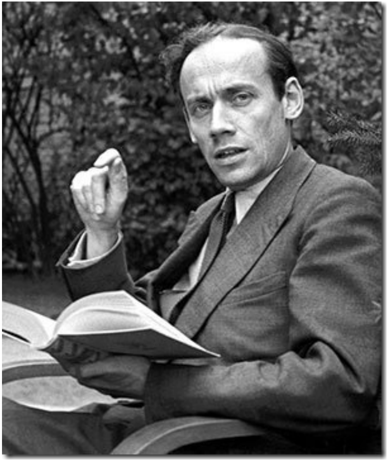
$$\sim C(a)\pi(x),$$

*where $C(a)$ is an explicitly described positive constant.*

When $a = 2$, he predicts

$$C(2) = \prod_p \left(1 - \frac{1}{p(p-1)}\right)$$
$$= 0.3739558...$$

Of the 78498 primes $p \le 10^6$, 29341 have 2 as a primitive root: $29341/78498 = 0.37378\ldots$.



Emil Artin

# So close and yet so far

Hooley (1967): Artin's conjecture is correct … assuming GRH!

Hooley's work implies that (on GRH) $\ell(p)$ is usually fairly close to $p-1$. If $\xi(x) \to \infty$ as $x \to \infty$, no matter how slowly, then almost all primes $p$ satisfy

$$\ell(p) > p/\xi(p).$$

"Almost all": Asymptotically 100%.

Pappalardi and others (e.g., Kurlberg and Pomerance) have quantitative estimates for the size of the exceptional set given $\xi(.)$.

# So close and yet so far

Hooley (1967): Artin's conjecture is correct ... assuming GRH!

Hooley's work implies that (on GRH) $\ell(p)$ is usually fairly close to $p-1$. If $\xi(x) \to \infty$ as $x \to \infty$, no matter how slowly, then almost all primes $p$ satisfy

$$\ell(p) > p/\xi(p).$$

"Almost all": Asymptotically 100%.

Pappalardi and others (e.g., Kurlberg and Pomerance) have quantitative estimates for the size of the exceptional set given $\xi(.)$.

This talk: What can we say unconditionally?

Theorem (Heath-Brown, Gupta–Murty)

*At least one of* $2, 3, 5$ *is a primitive root for infinitely many primes* $p$. *That is, there is some* $a \in \{2, 3, 5\}$ *such that*

$$\ell_a(p) = p - 1$$

*for infinitely many primes* $p$. *Moreover,* $2, 3, 5$ *can be replaced with any three distinct primes.*

Their proofs give: $\gg x/(\log x)^2$ such primes $p \leq x$.

Question

*What kind of lower bound on* $\ell_a(p)$ *can be shown to hold for a positive proportion of primes* $p$*? Or for almost all primes* $p$*?*

Ram Murty

### Theorem (Hooley)

*Fix $\epsilon > 0$. Fix $a \notin \{0, \pm 1\}$. For almost all primes $p$,*

$$\ell_a(p) > p^{1/2-\epsilon}.$$

### Proof.

We give the proof when $a = 2$.

Suppose $p \le x$ and $\ell_2(p) \le p^{1/2-\epsilon} \le x^{1/2-\epsilon} := X$. Then

$$p \mid 2^{\ell_2(p)} - 1 \mid (2^1 - 1)(2^2 - 1) \cdots (2^{\lfloor X \rfloor} - 1).$$

The product is $< 2^{X^2}$ and so has $< X^2 = x^{1-2\epsilon}$ prime factors. And $X^2$ is asymptotically 0% of $\pi(x)$, as $x \to \infty$.

**Theorem (Kurlberg–Pomerance)**

*For each fixed $a \notin \{0, \pm 1\}$, Kurlberg–Pomerance showed that a positive proportion of primes $p$ satisfy*

$$\ell_a(p) > p^{0.677}.$$

Here is their simple proof: By a result of Baker–Harman, a positive proportion of $p$ are such that $p - 1$ has a prime factor $> p^{0.677}$. If $\ell_a(p)$ is divisible by that prime, then $\ell_a(p) > p^{0.677}$ also. If not, then $\ell_a(p) < (p-1)/p^{0.677} < p^{0.323}$, which is very rare (0% of primes, by Hooley).

# Almost all?

Hooley's exponent $\frac{1}{2}$ has resisted improvement for more than 50 years.

The "record" result in this direction is due to Erdős and Murty and replaces $\frac{1}{2} - \epsilon$ with $\frac{1}{2} + \epsilon(p)$: *If* $\epsilon(p)$ *is any function tending to* 0 *as* $p \to \infty$, *then*

$$\ell_a(p) > p^{\frac{1}{2}+\epsilon(p)}$$

*for almost all primes p.*

Komal and I showed that we can break the "$\frac{1}{2}$-barrier" for a slightly different question.

**Theorem (Agrawal and P., 2020)**

*Fix $\epsilon > 0$. For almost all primes $p$, there is an $a \in \{2, 3, 6, 12, 18\}$ with*

$$\ell_a(p) > p^{8/15-\epsilon}.$$

Note that $8/15 = 1/2 + 1/30$.

One can replace 2, 3, 6, 12, 18 with $a, b, ab, a^2b, ab^2$ for multiplicatively independent nonzero integers $a, b$.

To prove the $8/15$ theorem, we look at the prime factorization of the product

$$\ell_2(p)\ell_3(p)\ell_6(p)\ell_{12}(p)\ell_{18}(p).$$

Let $L = \mathrm{lcm}[\ell_2(p), \ell_3(p)]$. We show that for almost all primes $p$,

$$L^4 \mid F\ell_2(p)\ell_3(p)\ell_6(p)\ell_{12}(p)\ell_{18}(p),$$

where $F$ is a small integer, meaning $F < p^{\epsilon}$.
Hence,

$$\ell_2(p)\ell_3(p)\ell_6(p)\ell_{12}(p)\ell_{18}(p) > L^4 p^{-\epsilon}.$$

A result of Matthews gives $L > p^{2/3-\epsilon}$, almost always.
Hence,

$$\ell_2(p)\ell_3(p)\ell_6(p)\ell_{12}(p)\ell_{18}(p) > p^{8/3-5\epsilon}.$$

Now take fifth roots and view LHS as a geometric mean.

## A remark

One can get exponents larger than $8/15$ but working with larger sets.

### Theorem

*For each $\epsilon > 0$, there is a finite set $\mathcal{A}$ such that, for almost all primes $p$, some $a \in \mathcal{A}$ satisfies*

$$\ell_a(p) > p^{1-\epsilon}.$$

## A remark

One can get exponents larger than $8/15$ but working with larger sets.

**Theorem**

*For each $\epsilon > 0$, there is a finite set $\mathcal{A}$ such that, for almost all primes $p$, some $a \in \mathcal{A}$ satisfies*

$$\ell_a(p) > p^{1-\epsilon}.$$

*Consequently (Pigeonhole Principle), there is a (fixed) $a \in \mathcal{A}$ such that*

$$\ell_a(p) > p^{1-\epsilon}$$

*on a set of primes $p$ of upper density at least $1/|\mathcal{A}| > 0$.*

For example, there is a positive integer $a$ such that, on a set of primes $p$ of positive upper density,

$$\ell_a(p) > p^{0.999}.$$

One can also get this going for composite numbers.

Let $\ell_a^*(n)$ be the length of the period of the sequence $a, a^2, a^3, \ldots$ modulo $n$. Then for almost all $n$, there is an $a \in \{2, 3, 6, 12, 18\}$ with

$$\ell_a^*(n) > n^{8/15-\epsilon}.$$

Again this goes through for $a, b, ab, a^2b, ab^2$ if $a, b$ are multiplicatively independent.

One can also incorporate the $+\epsilon(p)$ improvement of Erdős–Murty. As an example, if $\epsilon(p) \to 0$, then for almost all primes $p$, there is an $a \in \{2, 3, 6, 12, 18\}$ with

$$\ell_a(p) > p^{8/15+\epsilon(p)}.$$

THANK YOU YOUR ATTENTION!