Thoughts on the order of a mod p

Paul Pollack, University of Georgia, Athens, GA, USA

Luxembourg NTS

October 2020

My plan in this talk to discuss two recent papers, both on the theme of multiplicative orders modulo p. Both papers are joint work, but with different authors, namely ...

My plan in this talk to discuss two recent papers, both on the theme of multiplicative orders modulo p. Both papers are joint work, but with different authors, namely ...

Komal Agrawal, UGA

Zeb Engberg, Wasatch Academy

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 ℓ 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 ℓ 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, either with a fixed, or a belonging to a finite set.

There is nothing like looking, if you want to find something. – J.R.R. Tolkien

Fix $a = 2$ and write $\ell(p)$ rather than $\ell_2(p)$.

There are 78498 primes $p \leq 10^6$. And $\ell(p)$ is defined for 78497 of these.

There is nothing like looking, if you want to find something. – J.R.R. Tolkien

Fix $a = 2$ and write $\ell(p)$ rather than $\ell_2(p)$.

There are 78498 primes $p \leq 10^6$. And $\ell(p)$ is defined for 78497 of these.

For 29341 of these, have $\ell(p) = p - 1$.
For 22092 of these, have $\ell(p) = (p-1)/2$.
For 5233 of these, have $\ell(p) = (p-1)/3$.
For 3655 of these, have $\ell(p) = (p-1)/4$.
For 1477 of these, have $\ell(p) = (p-1)/5$.

There is nothing like looking, if you want to find something. – J.R.R. Tolkien

Fix $a = 2$ and write $\ell(p)$ rather than $\ell_2(p)$.

There are 78498 primes $p \le 10^6$. And $\ell(p)$ is defined for 78497 of these.

For 29341 of these, have $\ell(p) = p - 1$.
For 22092 of these, have $\ell(p) = (p-1)/2$.
For 5233 of these, have $\ell(p) = (p-1)/3$.
For 3655 of these, have $\ell(p) = (p-1)/4$.
For 1477 of these, have $\ell(p) = (p-1)/5$.

These cases account for about 79% of the primes $p \le 10^6$.

Artin's primitive root conjecture

Conjecture (E. Artin, 1927)

Fix $a \in \mathbb{Z}$, not a square, and not ± 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 ± 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

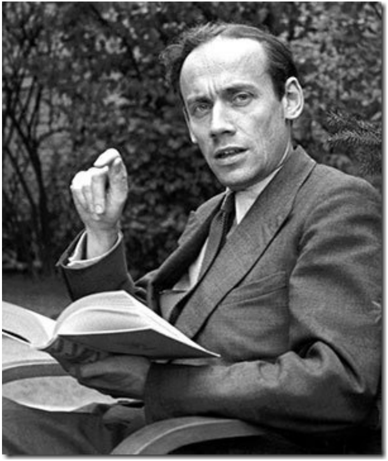
$$\sim C(a)\pi(x),$$

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

When $a = 2$, he predicts

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

Of the 78498 primes $p \leq 10^6$, 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

$$\frac{p-1}{\ell(p)} < \xi(p).$$

"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

$$\frac{p-1}{\ell(p)} < \xi(p).$$

"Almost all": Asymptotically 100%.

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

First half of 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 $x \to \infty$.

This observation was extended by Matthews.

Theorem (Matthews)

Fix $\epsilon > 0$ and fix a positive integer k.
Suppose $a_1, \ldots, a_k$ are multiplicatively independent nonzero integers. Then for almost all primes p, the order of the subgroup mod p generated by $a_1, \ldots, a_k$ is at least

$$p^{\frac{k}{k+1}-\epsilon}.$$

The proof is similar: With $a_1, \ldots, a_k$ as above, one shows there are few primes "dividing" the rational numbers

$$a_1^{n_1} \cdots a_k^{n_k} - 1,$$

for nonzero tuples $(n_1, \ldots, n_k) \in \mathbb{Z}^k$ of small height, meaning $\max|n_i| \leq n^{(1-\epsilon)/(k+1)}$.

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.

Our proof uses the results of Hooley and Matthews, along with the following undergraduate-level exercise, applied to the multiplicative group mod p.

Proposition

Let G be a cyclic group of order M whose order is divisible by p but not p^2, with generator g. Let $\log_g \colon G \to \mathbb{Z}/M\mathbb{Z}$ be the "discrete log" base g. Then for each $a \in G$,

$$p \mid \text{order of } a \iff p \nmid \log_g(a).$$

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 $L = \mathrm{lcm}[\ell_2(p), \ell_3(p)]$.

Observe that each of $2, 3, 6, 12, 18$ has order dividing L. Hence, every prime dividing our 5-fold product divides L.

Using the elementary group theoretic fact described above, we show that "typically" a prime dividing L divides at least four of the five terms in the product.

What is it we really show about $L = \mathrm{lcm}[\ell_2(p), \ell_3(p)]$?

Let $F = \lfloor \log\log p \rfloor !$. We show that for almost all primes p,

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

Note that F is small: in particular, $F < p^{\epsilon}$.

Hence,

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

The 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

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

Part II: Mersenne numbers

We would like to understand arithmetic properties of Mersenne numbers $2^n - 1$.

As an example of a natural question, it would be good to understand the average order of the arithmetic function

$$\omega(2^n - 1) = \sum_{p \mid 2^n - 1} 1.$$

We have only very weak results on this problem: with $\ell(p) = \ell_2(p)$, it comes down to estimating $\sum_{p \leq x} \frac{1}{\ell(p)}$, which appears very difficult.

The situation gets easier if we replace the summand 1 with a weight that dampens the sensitivity to small values of $\ell(p)$. With this in mind, we let

$$f(n) = \sum_{p \mid 2^n - 1} \frac{1}{p}.$$

Then the average order problem becomes tractable:

$$\begin{aligned}\sum_{n \le x} f(n) &= \sum_{n \le x} \sum_{p \mid 2^n - 1} \frac{1}{p} \\ &= \sum_{p > 2} \frac{1}{p} \sum_{\substack{n \le x \\ \ell(p) \mid n}} 1 \approx x \sum_{p > 2} \frac{1}{p\ell(p)}.\end{aligned}$$

It is not hard to prove that the sum converges and that the approximation is justified: $\frac{1}{x} \sum_{n \le x} f(n) \to \sum_{p > 2} \frac{1}{p\ell(p)}$.

The function $f(n)$ was introduced by Erdős, who was interested in large values of $f(n)$.

One way of constructing large values of $f(n)$ is to make n divisible by all of the small numbers. Choose $z = \frac{1}{2}\log x$, and let n be the lcm of all positive integers $\leq z$. Then $n \leq x$ (for large x). Moreover,

$$f(n) = \sum_{p \mid 2^n - 1} \frac{1}{p} = \sum_{\ell(p) \mid n} \frac{1}{p}$$

$$\geq \sum_{2 < p \leq z} \frac{1}{p}.$$

By a theorem of Mertens, for a certain constant $C_0 = 0.261\ldots$,

$$\sum_{p \leq z} \frac{1}{p} = \log\log z + C_0 + o(1)$$

$$= \log\log\log x + C_0 + o(1).$$

So we know that for all large x, there are values of $n \le x$ with

$$f(n) \ge \log\log\log x - \frac{1}{2} + C_0 + o(1).$$

In 1971, Erdős proved the remarkable result that this inequality is sharp up to the constant addend: For some constant C, all large real numbers x, and all $n \le x$,

$$f(n) \le \log\log\log x + C.$$

Paul Erdős

Theorem (Engberg, 2014)

Assume the GRH and the Elliott–Halberstam Conjecture. There is a constant $C_1 \approx 0.522$ *such that the following holds: For all large* x*, there are values of* $n \leq x$ *for which*

$$f(n) \geq \log\log\log x - \frac{1}{2} + C_0 + C_1 + o(1).$$

This is sharp, in the sense that the reverse inequality holds for all $n \leq x$*, as* $x \to \infty$*.*

Here $C_1 = \int_1^\infty \rho(u)u^{-1}\,du$, where $\rho(u)$ is Dickman's rho-function (stay tuned).

In the interests of time, I will focus on the lower bound implicit in the theorem.

Once again, take n the lcm of the positive integers not exceeding $z := \frac{1}{2}\log x$, so that $n \le x$. Then

$$f(n) \ge \sum_{2<p\le z} \frac{1}{p} \qquad\qquad .$$

In the interests of time, I will focus on the lower bound implicit in the theorem.

Once again, take n the lcm of the positive integers not exceeding $z := \frac{1}{2}\log x$, so that $n \le x$. Then

$$f(n) \ge \sum_{2<p\le z} \frac{1}{p} + \sum_{\substack{p>z \\ \ell(p)|n}} \frac{1}{p}.$$

Since $\ell(p) \mid p-1$, we can bound the remaining contribution from below:

$$\sum_{\substack{p>z \\ \ell(p)|n}} \frac{1}{p} \ge \sum_{\substack{p>z \\ p-1|n}} \frac{1}{p}.$$

Since $\ell(p) \mid p-1$, we can bound the remaining contribution from below:

$$\sum_{\substack{p>z \\ \ell(p)|n}} \frac{1}{p} \geq \sum_{\substack{p>z \\ p-1|n}} \frac{1}{p}.$$

If $p-1 \mid n$, then $P(p-1) \leq z$. We argue that

$$\sum_{\substack{p>z \\ p-1|n}} \frac{1}{p} = \sum_{\substack{p>z \\ P(p-1)\leq z}} \frac{1}{p} + o(1).$$

To understand this last sum, we need to understand the frequency with which shifted primes $p-1$ have only small prime factors.

Dickman: For each fixed $u \geq 0$, the limiting proportion of $n \leq x$ with $P(n) \leq x^{1/u}$ exists. We call this $\rho(u)$; that is,

$$\rho(u) = \lim_{x\to\infty} \frac{1}{x} \#\{n \leq x : P(n) \leq x^{1/u}\}.$$

The function $\rho(u)$ is positive but decays rapidly as $u \to \infty$, roughly like u^{-u}.

Granville: Assume the Elliott–Halberstam Conjecture. For each fixed $u \geq 0$, the limiting proportion of $p-1 \leq x$ with $P(p-1) \leq x^{1/u}$ is also given by $\rho(u)$.

Using Granville's theorem, we prove (under EHC) that the function of z given by

$$\sum_{\substack{p>z \\ P(p-1)\leq z}} \frac{1}{p}$$

converges as $z \to \infty$ to

$$\int_1^\infty \rho(u)u^{-1}\,du =: C_1.$$

Collecting estimates shows (under EHC) that for all large x, there is an integer $n \leq x$ with

$$f(n) \geq \log\log\log x - \frac{1}{2} + C_0 + C_1 + o(1).$$

In fact, we can take n as the lcm of the numbers $\leq \frac{1}{2}\log x$.

We prove that this is sharp by establishing that the same expression serves as an upper bound, valid for *all* $n \leq x$. How? Overarching arguments are similar, but now need GRH.

Why? We replaced $\ell(p)$ with $p-1$ above. GRH is used to show that this doesn't make much difference, since the ratio $(p-1)/\ell(p)$ is usually small.

The method also allows us to handle certain relatives of $f(n)$. For example, let

$$g(n) = \sum_{d|2^n-1} \frac{1}{d}.$$

Note that this is equal to

$$\sigma(2^n-1)/(2^n-1),$$

where σ is the usual sum-of-divisors function.

Assuming GRH and EHC, Zeb and I prove that as $x \to \infty$,

$$\max_{n \le x} g(n) \sim \frac{1}{2} e^{\gamma + C_1} \log\log x.$$

Thank you your attention!