Multiplicative orders mod p

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

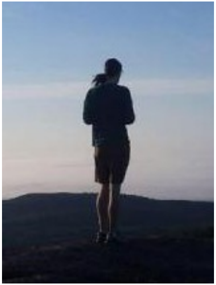
Kansas State NTS

March 2021

Today I'll be discussing several problems connected with multiplicative orders of integers modulo p, where p is a prime number. Much of what I will say concerns work done by others (shoulders of giants). The new results are joint with two UGA graduate students.

Today I'll be discussing several problems connected with multiplicative orders of integers modulo p, where p is a prime number. Much of what I will say concerns work done by others (shoulders of giants). The new results are joint with two UGA graduate students.

Komal Agrawal



Matthew Just

Out of chaos...

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

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

In other words, $o(a \bmod m)$ is the least positive integer ℓ for which

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

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

Out of chaos...

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

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

In other words, $o(a \bmod m)$ is the least positive integer ℓ for which

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

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

We are interested in understanding the distribution of $o(a \bmod p)$ as p varies.

A warm up

Fix an integer a. We will assume $a \notin \{0, \pm 1\}$.
For all primes $p \nmid a$, we know that $o(a \bmod p) = (p-1)/l$ for some integer l.

Question: Are there primes p for which $o(a \bmod p)/(p-1)$ can be as small as we like? Equivalently, can l be arbitrarily large?

A warm up

Fix an integer a. We will assume $a \notin \{0, \pm 1\}$.
For all primes $p \nmid a$, we know that $o(a \bmod p) = (p-1)/l$ for some integer l.

Question: Are there primes p for which $o(a \bmod p)/(p-1)$ can be as small as we like? Equivalently, can l be arbitrarily large?

Yes: Look at primes $p \equiv 1 \pmod{k}$ for which a is a kth power modulo p. Then $a^{(p-1)/k} \equiv 1 \pmod{p}$, so that $l \geq k$.

Is there always such a prime p? Yes! It is enough to take a prime p that splits completely in $\mathbb{Q}(\zeta_k, \sqrt[k]{a})$. There are infinitely many of these.

We have just seen that if $o(a \bmod p) = (p-1)/l$, then l can be arbitrarily large.

Question: Must l be arbitrarily large?
Less cheekily: Is there a infinite sequence of p along which l is bounded? That is, along which $o(a \bmod p) \gg p$?

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

Let's take $a = 2$.

There are 78498 primes $p \leq 10^6$. And $o(2 \bmod p)$ is defined for 78497 of these.

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

Let's take $a = 2$.

There are 78498 primes $p \leq 10^6$. And $o(2 \bmod p)$ is defined for 78497 of these.

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

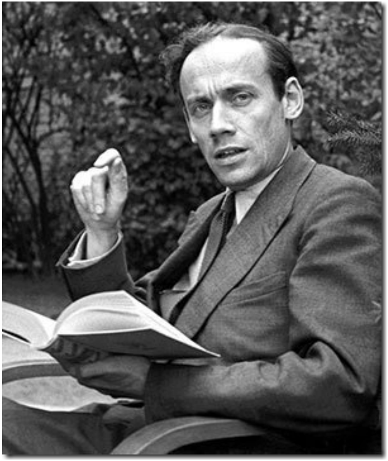
There is nothing like looking, if you want to find something. – J.R.R. Tolkien

Let's take $a = 2$.

There are 78498 primes $p \leq 10^6$. And $o(2 \bmod p)$ is defined for 78497 of these.

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

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



Emil Artin

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 $o(a \bmod p) = p - 1$. In fact, the number of primes $p \leq x$ with $o(a \bmod p) = p - 1$ 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 $o(a \bmod p) = p - 1$. In fact, the number of primes $p \leq x$ with $o(a \bmod p) = p - 1$ is

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

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

When $a = 2$, he predicts

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

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

So close and yet so far

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

Hooley's work implies that (on GRH) $o(a \bmod p)$ 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

$$I = \frac{p-1}{o(a \bmod p)} < \xi(p).$$

"Almost all": Asymptotically 100%.

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

Even on GRH, important questions remain.

Problem. Determine $\mathcal{L}$, the set of all limit points of ratios

$$\frac{\log(o(a \bmod p))}{\log p}.$$

Even on GRH, important questions remain.

Problem. Determine $\mathcal{L}$, the set of all limit points of ratios

$$\frac{\log(o(a \bmod p))}{\log p}.$$

I would be happy to know even a modest amount about $\mathcal{L}$. Under GRH, we know $1 \in \mathcal{L}$, and that there is a limit point $\leq 3/4$. (Run the argument for large values of l at the start of the talk, using a quantitative form of the Chebotarev density theorem to take k large.)

Problem. Show that $\mathcal{L}$ contains an interval $[1-\delta, 1]$.

Large values of $o(a \bmod p)$, unconditionally?

As far as I know, there is no single value of a for which we can prove that $o(a \bmod p) \gg p$ infinitely often.

The word *single* is important here!

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 $o(a \bmod p) = p - 1$ for infinitely many primes p. Moreover, $2, 3, 5$ can be replaced with any three distinct primes.

One 'defect' of the argument is that one only produces $\gg x/(\log x)^2$ primes of this kind, whereas one 'should' get a positive proportion.

Ram Murty

Recall that if $\xi(p) \to \infty$, no matter how slowly, it should be the case that

$$o(a \bmod p) > p/\xi(p)$$

almost always (asymptotically 100% of the time).

What lower bounds on $o(a \bmod p)$ can we prove, unconditionally, to hold almost always?

Hooley: $o(a \bmod p) > p^{1/2-\delta}$ almost always.

We give the proof for $a = 2$.

If $p \le x$ and $o(2 \bmod p) \le p^{1/2-\delta}$, then p divides one of

$$2^1 - 1, \quad 2^2 - 1, \quad \dots, \quad 2^N - 1$$

where $N = \lfloor x^{1/2-\delta} \rfloor$. Size considerations show that $2^n - 1$ has $< n$ prime factors. So there are $< 1 + 2 + \cdots + N < N^2 < x^{1-\delta}$ primes of this kind, which is $o(\pi(x))$ as $x \to \infty$.

Matthews: Let a, b be multiplicatively independent integers. For almost all primes p, the subgroup of $\mathbb{F}_p^\times$ generated by a, b mod p has size $> p^{2/3-\delta}$. With k multiplicatively independent integers, one gets order $> p^{\frac{k}{k+1}-\delta}$ almost always.

Agrawal–P.: Let a, b be multiplicatively independent integers. For almost all primes p, at least one of a, b, ab, ab^2, a^2b has order $> p^{8/15-\delta}$. The exponent $8/15$ can be pushed arbitrarily close to 1 by starting with more multiplicatively independent bases.

The proof compares the factorization of the product of the orders of a, b, ab, ab^2, a^2b with the factorization of the lcm of the orders of a, b.

PART II: Comparative order theory

Theme: Let a, b be integers, not 0 or ± 1. How does $o(a \bmod p)$ compare to $o(b \mod p)$, as p varies?

Erdős's support problem

Question (Erdős, 1988): For which pairs a and b do we have that

$$o(a \bmod p) = o(b \mod p)$$

for all primes p? Equivalently, what conclusion can be drawn about a, b if, for every positive integer n,

$$\mathrm{Supp}(a^n - 1) = \mathrm{Supp}(b^n - 1) \quad ?$$

Here "Supp" means the set of prime divisors.

Erdős's support problem

Question (Erdős, 1988): For which pairs a and b do we have that

$$o(a \bmod p) = o(b \mod p)$$

for all primes p? Equivalently, what conclusion can be drawn about a, b if, for every positive integer n,

$$\mathrm{Supp}(a^n - 1) = \mathrm{Supp}(b^n - 1) \quad ?$$

Here "Supp" means the set of prime divisors.

Answer (Schinzel, 1960): $a = b \quad !$
The same conclusion can be drawn if "all primes p" is replaced with "all but finitely many" or "almost all" (in the sense of Dirichlet density).

Paul Erdős

Andrzej Schinzel

Proof sketch [finitely many exceptions version]

Let k be a positive integer. Then, for each prime $p \equiv 1 \pmod{k}$ (up to a finite set of exceptions),

$$a^{(p-1)/k} \equiv 1 \pmod{p} \Longleftrightarrow b^{(p-1)/k} \equiv 1 \pmod{p}.$$

It follows that the primes which split completely in $\mathbb{Q}(\zeta_k, \sqrt[k]{a})$ coincide, up to a finite set of exceptions, with those that split in $\mathbb{Q}(\zeta_k, \sqrt[k]{b})$. By class field theory, Galois number fields are determined by their set of split primes, and so $\mathbb{Q}(\zeta_k, \sqrt[k]{a}) = \mathbb{Q}(\zeta_k, \sqrt[k]{b})$.

At this point, we know that for each positive integer k,

$$\mathbb{Q}(\zeta_k, \sqrt[k]{a}) = \mathbb{Q}(\zeta_k, \sqrt[k]{b}).$$

By Kummer theory, $a = b^d$ in $K^\times/(K^\times)^k$ for some integer d coprime to k, where $K = \mathbb{Q}(\zeta_k)$. One can show that when k is odd, this implies that $a = b^d$ already in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^k$. Knowing that this holds for *all* odd k is enough to prove a, b are multiplicatively dependent. And from here it's easy to wrap up, using facts about primitive prime factors of numbers in sequences $A^n - 1$ (Bang–Zsigmondy–Birkhoff–Vandiver–. . .).

Remark. A variant of the proof will show that if $o(a \bmod p)$ *divides* $o(b \mod p)$ for all primes p, up to a density zero set of exceptions, then a is a power of b (Schinzel, 1960).

What if we only ask that $o(a \bmod p) = o(b \mod p)$ for infinitely many primes p?

One would guess this happens quite often. For example, for suitably generic a and b, it seems we should have

$$o(a \bmod p) = o(b \mod p) = p - 1$$

for infinitely many primes p. This can indeed be shown on GRH.

What if we don't assume GRH?

Equality infinitely often

Theorem (Schinzel–Wójcik)

Let a, b be any integers, not 0 or ± 1. Then there are infinitely many primes p for which $o(a \bmod p) = o(b \mod p)$.

Let's see how the proof goes with $a = 2, b = 3$.

We look at primes dividing $2^\ell - 3$, as the prime ℓ varies. Notice that modulo ℓ,

$$2^\ell - 3 \equiv 2 - 3 \equiv -1 \pmod{\ell}.$$

So as long as ℓ is an odd prime, so that $1 \not\equiv -1$, there must be a prime p dividing $2^\ell - 3$ with $p \not\equiv 1 \pmod{\ell}$.

Then $2^\ell \equiv 3 \pmod{p}$. Since $\ell \nmid p-1$, the ℓth power map is an automorphism of $\mathbb{F}_p^\times$, and so

$$o(2 \bmod p) = o(2^\ell \bmod p) = o(3 \bmod p).$$

We need to show that infinitely many primes p arise from different choices of ℓ.

Idea: Use primes ℓ so that the numbers $\ell - 1$ become "more and more divisible", in the sense that $\ell \to 1$ in $\hat{\mathbb{Z}}$. For instance, choose the nth prime ℓ in the sequence congruent to 1 modulo $n!$.

It's enough to argue that any prime we discover as a divisor of $2^\ell - 3$ is only discovered finitely many times (meaning, for finitely many ℓ).

Let p be a fixed odd prime. (All primes discovered in our process are odd!) Then for all large ℓ in our sequence, we have that $p - 1 \mid \ell - 1$, and so

$$2^\ell - 3 \equiv 2 \cdot 2^{\ell-1} - 3 \equiv 2 \cdot 1 - 3 \equiv -1 \pmod{p},$$

so p will not divide $2^\ell - 3$.

Order-dominance

What about $o(a \bmod p) > o(b \mod p)$? Call the pair a, b **order-dominant** if this inequality holds for infinitely many p.

When a, b are multiplicatively independent, Järviniemi has shown under GRH that $o(a \bmod p)/o(b \mod p)$ can be arbitrarily large. The multiplicatively dependent case is not so hard (again, using classical results on primitive prime divisors), and one gets the following theorem.

Theorem

Assume GRH. Then a, b is order dominant unless a is a power of b.

Order-dominance

What about $o(a \bmod p) > o(b \mod p)$? Call the pair a, b **order-dominant** if this inequality holds for infinitely many p.

When a, b are multiplicatively independent, Järviniemi has shown under GRH that $o(a \bmod p)/o(b \mod p)$ can be arbitrarily large. The multiplicatively dependent case is not so hard (again, using classical results on primitive prime divisors), and one gets the following theorem.

Theorem

Assume GRH. Then a, b is order dominant unless a is a power of b.

Unconditionally???

Let's prove that $2, 3$ is an order dominant pair.

Look at p dividing $2^{n!} - 3$. As long as $n \geq 3$, we have $2^{n!} - 3 \equiv -3 \pmod 8$, and so the Jacobi symbol $\left(\frac{2}{2^{n!}-3}\right) = -1$. Hence, there is a p dividing $2^{n!} - 3$ with $\left(\frac{2}{p}\right) = -1$.

Since $2^{n!} \equiv 3 \pmod p$, we see that 3 lies in the subgroup generated by 2, mod p. Since $n!$ is even, 3 is a square mod p. But 2 is not a square mod p, and so the subgroup generated by 3 cannot coincide with the subgroup generated by 2. Hence, $o(3 \bmod p) < o(2 \bmod p)$.

That infinitely many different p arise is proved as before. A given odd prime p can divide only finitely many of the numbers $2^{n!} - 3$.

This argument (due to Banaszak in another context) is promising, but it doesn't generalize as far as one would like.

This proof required finding p with 2 a nonsquare mod p. So if A is a square in $\mathbb{Z}$, there is no hope of establishing the order dominance of pairs A, B this way.

This argument (due to Banaszak in another context) is promising, but it doesn't generalize as far as one would like.

This proof required finding p with 2 a nonsquare mod p. So if A is a square in $\mathbb{Z}$, there is no hope of establishing the order dominance of pairs A, B this way.

One of the first things Matt and I do is try to write down a fairly general class of cases for which this argument can be made to work.

Theorem (Just–P.)

(a) *Let A, B be odd positive integers. Then A, B is order-dominant if either*

$$\left(\frac{B(B-1)}{A}\right) = -1 \quad \textit{or} \quad \left(\frac{-(B-1)}{A}\right) = -1.$$

(b) *The pair $2, B$ is order-dominant for every odd positive integer B.*

(c) *The pair $A, 2$ is order-dominant for every odd positive integer $A \not\equiv 1 \pmod 8$.*

(d) *Let A, B be coprime positive integers with $B > A^4$. Then $-A, B$ is order-dominant.*

These methods are enough to prove that A, B is order dominant for distinct A, B from the list $2, 3, 5, 7$.

There is a somewhat surprising (to me) obstruction that appears in these generalizations. To illustrate, consider the problem of showing that $17, 2$ is order-dominant.

It is straightforward to verify, by quadratic reciprocity for the Jacobi symbol, that

$$\frac{2 \cdot 17^{6k+4} - 1}{7}$$

always has a prime divisor p with $\left(\frac{17}{p}\right) = -1$. Arguing as in the last slide, one gets that $o(17 \bmod p) > o(2 \bmod p)$. But I do not know how to show that infinitely many different p will appear as k varies in a suitable family!

Quadratic reciprocity is not the only game in town.

One might hope to use higher reciprocity laws to establish the order-dominance of further pairs.

Theorem (Just–P.)

Let A be an integer coprime to 3 with $A^2 \not\equiv 1 \pmod{9}$. Then $A, -3$ and $A, 3$ are order-dominant.

The proof uses cubic reciprocity. The ± 3 appearing in the second component of the pair corresponds to cubic reciprocity's natural habitat being $\mathbb{Q}(\sqrt{-3})$.

So far analytic number theory has not made its presence felt in this talk!

Theorem (Just–P.)

The pair $A, 2$ is order-dominant for almost all positive integers A.

The proof uses Fermat numbers $F_n = 2^{2^n} + 1$. It is well-known that the F_n are coprime and easy to see that if $p \mid F_n$, then $o(2 \bmod p) = 2^{n+1}$. If $n \geq 2$, this implies that

$$8 \mid 2^{n+1} = o(2 \bmod p) \mid p - 1,$$

and hence 2 is a square mod p. But then $2^{n+1} = o(2 \bmod p) \mid \frac{p-1}{2}$, and

$$p \equiv 1 \pmod{2^{n+2}}.$$

Suppose there are infinitely many Fermat numbers n with $\left(\frac{A}{F_n}\right) = -1$.

Choose $p \mid F_n$ with $\left(\frac{A}{p}\right) = -1$. Then $o(A \bmod p)$ has to be divisible by the full power of 2 in $p - 1$. So,

$$2^{n+2} \mid o(A \bmod p).$$

On the other hand, $o(2 \bmod p) = 2^{n+1}$. So $A, 2$ is order-dominant.

Using ideas of Křížek, M.–Luca–Somer, we show that this condition holds for all but $O(x/(\log x)^{1-\epsilon})$ values of $A \leq x$. The proof uses character sums and the Brun–Titchmarsh inequality.

Much remains to be done!

Problem. Prove $17, 2$ is order-dominant.

Ideas welcome!

Thank you!