(Primes and) Squares modulo p

Paul Pollack

The City *of* SAN DIEGO

MAA Invited Paper Session
on Accessible Problems in
Modern Number Theory

January 13, 2018

Question

Consider the infinite arithmetic progression

$$2, 5, 8, 11, 14, \ldots.$$

Does it contain any squares?

Question

Consider the infinite arithmetic progression

$$2, 5, 8, 11, 14, \ldots.$$

Does it contain any squares?

Answer

No. If $n = \square$, then also $n \equiv \square \pmod{m}$ for any choice of modulus m. We take $m = 3$. Every square modulo 3 is

$$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad \text{or} \quad 2^2 \equiv 1.$$

But the numbers in our list are congruent to 2 modulo 3.

For the rest of this talk, p denotes an odd prime.

As on the last slide, we will be mostly concerned with the set of **reduced** squares modulo p, by which we mean the squares mod p in $[0, p-1]$. E.g., when $p = 5$, the reduced squares are

$$0, 1, 4.$$

Many cheerful facts

Let p be an odd prime.

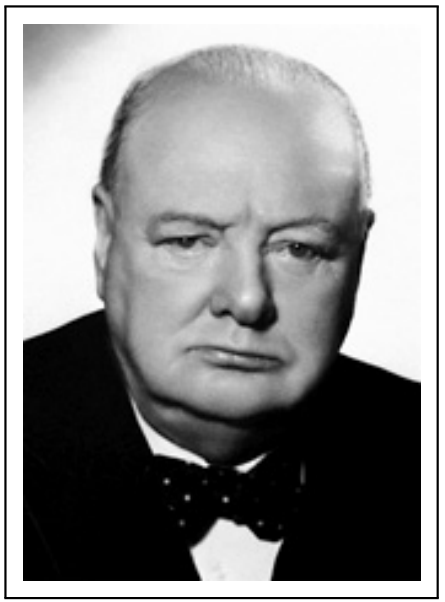
- There are $\frac{p-1}{2}$ nonzero reduced squares modulo p.
- The Legendre symbol $\left(\frac{\cdot}{p}\right)$ is multiplicative.
- For each integer a, one can characterize those primes p for which a is congruent to a square modulo p (via Quadratic Reciprocity).

Many cheerful facts

Let p be an odd prime.

- There are $\frac{p-1}{2}$ nonzero reduced squares modulo p.
- The Legendre symbol $\left(\frac{\cdot}{p}\right)$ is multiplicative.
- For each integer a, one can characterize those primes p for which a is congruent to a square modulo p (via Quadratic Reciprocity).

Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.



Primes make everything more interesting

Take $p = 13$. Then the reduced squares modulo p are

$$0, 1, 3, 4, 9, 10, 12$$

while the reduced nonsquares are

$$2, 5, 6, 7, 8, 11.$$

Primes make everything more interesting

Take $p = 13$. Then the reduced squares modulo p are

$$0, 1, 3, 4, 9, 10, 12$$

while the reduced nonsquares are

$$2, 5, 6, 7, 8, 11.$$

Question

Assume $p \geq 7$. Is there always a prime reduced square modulo p? a prime reduced nonsquare?

Answer

YES for nonsquares: Start with any n in the list of reduced nonsquares. Then $n \geq 2$, so n factors as a (nonempty) product of primes. Not every prime factor can be a square, else n would be a square.

Answer

YES for squares: To start with, suppose $p \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 8$, then 2 is in the list of squares. Otherwise, since $p > 5$, we know that $p - 1$ is not a power of 2. So there is an odd prime q dividing $p - 1$. Then

$$p \equiv 1 \pmod q,$$

so p is on the list of squares modulo q. Since $p \equiv 1 \pmod 4$, QR puts q on the list of squares modulo p.

Now suppose $p \equiv 3 \pmod 4$. A similar argument works with q a prime dividing $\frac{p+1}{4}$. (Exercise!) ■

Many directions one could try to push this. For example, one could ask.

Question

What is the size of the smallest prime nonsquare modulo p?

Answer

For each $\epsilon > 0$, the smallest prime nonsquare is

$$< p^{\frac{1}{4\sqrt{e}}+\epsilon}$$

for all large enough p (Burgess, 1963).

Many directions one could try to push this. For example, one could ask.

Question

What is the size of the smallest prime square modulo p?

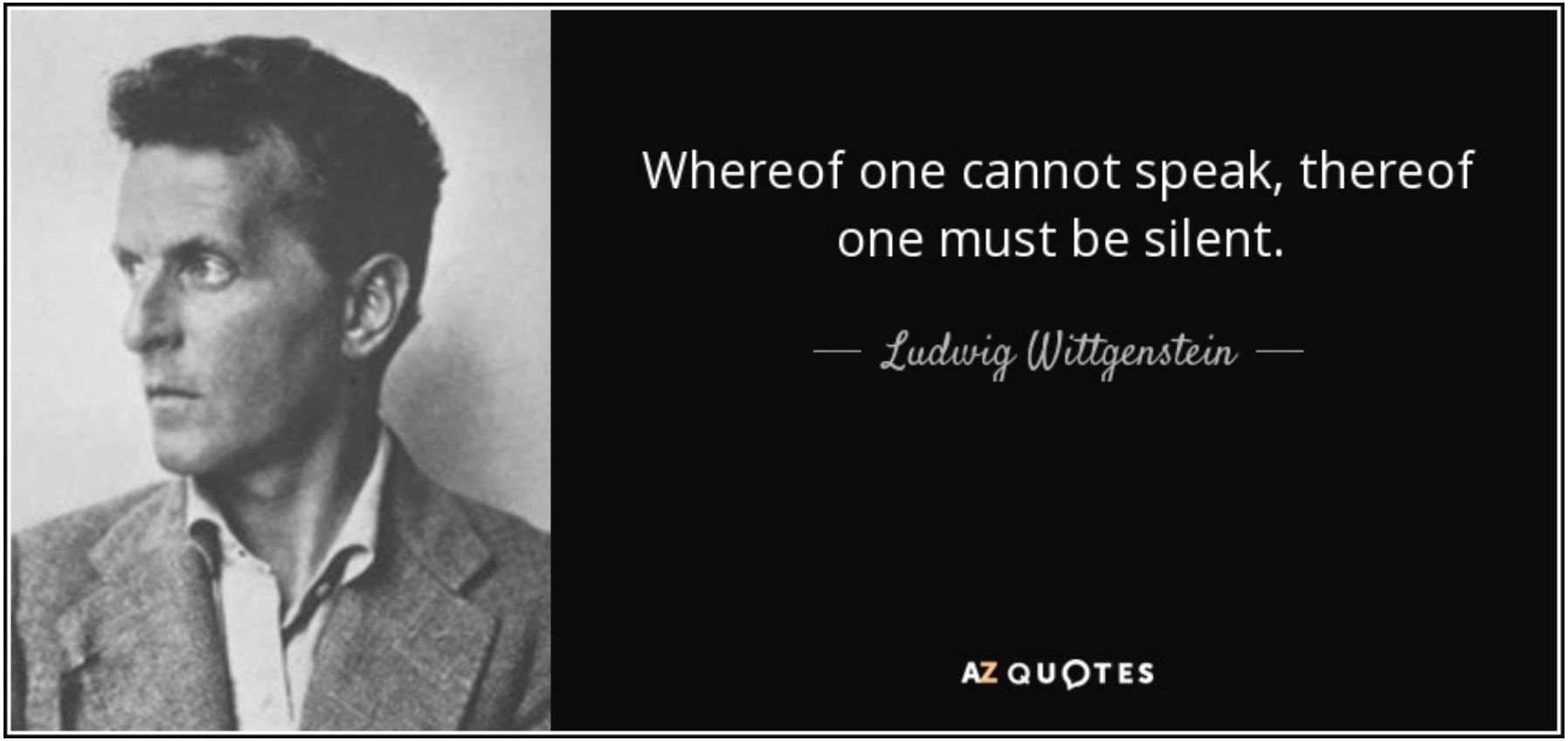
Answer

For each $\epsilon > 0$, the smallest prime square is

$$< p^{\frac{1}{4}+\epsilon}$$

for all large enough p (Linnik and A. I. Vinogradov, 1966).

Surely, the truth is that p^{ϵ} works as an upper bound in both problems. But the Burgess and Linnik–Vinogradov results have seen no substantial improvement in more than 50 years.


Whereof one cannot speak, thereof one must be silent.
— Ludwig Wittgenstein —
AZ QUOTES

Question

How many primes appear in the list of reduced squares modulo p?
How many primes appear in the list of reduced nonsquares?

All the primes up to $p-1$ appear in one of the two lists.
Conjecturally, each list should contain about half, so $\approx \frac{1}{2}p/\log p$.

What we can prove (unconditionally) are lower bounds of a small power of p.

Theorem (P., 2017)

Fix $\epsilon > 0$. There is an $\eta = \eta(\epsilon) > 0$ such that, for all large primes p, there are more than p^{η} primes not exceeding $p^{\frac{1}{4\sqrt{e}}+\epsilon}$ that are nonsquares modulo p.

Theorem (Benli and P., 2017)

Fix $\epsilon > 0$. There is an $\eta = \eta(\epsilon) > 0$ such that, for all large primes p, there are more than p^{η} primes not exceeding $p^{\frac{1}{2}+\epsilon}$ that are squares modulo p.

In work in progress, Benli expects to replace the exponent $\frac{1}{2}$ in the theorem with $\frac{1}{4}$, matching the exponent in the theorem of Linnik–Vinogradov.

In a different direction, one could look for primes in a prescribed residue class, a la Dirichlet.

Theorem (Gica, 2006)

If $p \geq 41$, both the residue classes 1 mod 4 and 3 mod 4 contain a prime in the list of reduced squares mod p.

Theorem (P., 2017)

If $p \geq 13$, both the residue classes 1 mod 4 and 3 mod 4 contain a prime in the list of reduced nonsquares mod p.

It does not appear easy to replace the modulus 4 here with other integers!

The proofs often involve results from the classical theory of binary quadratic forms.

To give the flavor, let's prove the following special case of Gica's theorem.

Theorem

If $p \equiv 5 \pmod 8$ *and* $p > 37$, *then there is a prime* 1 *modulo* 4 *on the list of reduced squares modulo* p.

Theorem

If $p \equiv 5 \pmod 8$ *and* $p > 37$, *then there is a prime* 1 *modulo* 4 *on the list of reduced squares modulo* p.

Theorem (Gauss, 1801)

If n *is odd, then* n *is a sum of three squares unless* $n \equiv 7 \pmod 8$.

Theorem (Grosswald, Calloway, Calloway, 1959)

If n *is odd, then* n *is a sum of three positive squares unless* $n \equiv 7 \pmod 8$ *or* $n = \{1, 5, 13, 25, 37, 85\}$.

So we can write $p = x^2 + y^2 + z^2$ with $x, y, z > 0$.

Write $p = x^2 + y^2 + z^2$. Then $x^2 + y^2 = p - z^2 < p$.

We also have $x \neq y$: otherwise $p = 2x^2 + z^2$, and one gets a contradiction reducing modulo 8.

A sum of unequal squares of positive integers always has a prime factor 1 modulo 4. (Exercise!) So we can choose a prime $q \equiv 1 \pmod 4$ with $q \mid x^2 + y^2$. Since $x^2 + y^2 < p$, we have

$$q < p.$$

Also,

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{x^2 + y^2 + z^2}{q}\right) = \left(\frac{z^2}{q}\right) = 1.$$

Thank you!