(Primes and) Squares modulo p

Paul Pollack

Tufts Algebra, Geometry, and Number Theory Seminar

May 3, 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

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

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

$$0, 1, 4.$$

Question

How many squares modulo p are there?

Too easy: Infinitely many! But what about reduced squares?

Theorem

The number of reduced squares modulo p is $1 + \frac{p-1}{2} = \frac{p+1}{2}$.

Proof.

Over any field in which $2 \neq 0$, the map $x \mapsto x^2$ is 2-to-1 on nonzero elements. The integers modulo p form a field with $p - 1$ nonzero elements, so there are $\frac{p-1}{2}$ nonzero squares there. ∎

$\therefore$ Precisely half of the numbers in $[1, p-1]$ are squares modulo p.

OK... New question: which half?

Following Legendre, for each integer a and odd prime p, define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p}, \\ 1 & \text{if } a \equiv \text{nonzero square mod } p, \\ -1 & \text{if } a \equiv \text{nonsquare mod } p. \end{cases}$$

Using that the subgroup of squares has index 2 in the unit group of the integers mod p, one can show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Proposition (Euler)

$\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}$. Also,

$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$.

Law of quadratic reciprocity (Gauss)

If p, q are distinct odd primes, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

In other words, for distinct odd primes p and q,

$$p \equiv \square \pmod q \iff q \equiv \square \mod p,$$

except when $p \equiv q \equiv 3 \pmod 4$, in which case

$$p \equiv \square \pmod q \iff q \not\equiv \square \mod p.$$

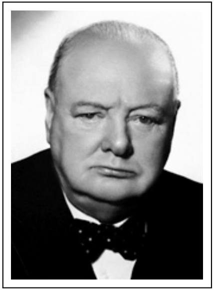
Using the results of Gauss and Euler, for any given integer a, one can completely characterize those primes p for which a shows up in the list of squares modulo p. As an example,

$$10 \text{ is a square mod } p \iff \\ p = 5 \text{ or } p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}.$$

Using the results of Gauss and Euler, for any given integer a, one can completely characterize those primes p for which a shows up in the list of squares modulo p. As an example,

$$10 \text{ is a square mod } p \iff \\ p = 5 \text{ or } p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \pmod{40}.$$

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.

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.

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.

Quite recently, Benli has managed 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!

Part II: (More) Proofs

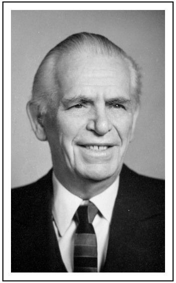
Earlier, I mentioned the theorem of Burgess that for large enough primes p, there is a prime nonsquare mod p smaller than about $p^{1/4\sqrt{e}}$.

I want to present for you a proof of a somewhat weaker result. The beautiful argument — which in my opinion deserves to be better known — is due to Lắszlő Rẽdei.

Theorem (Rẽdei, 1950)

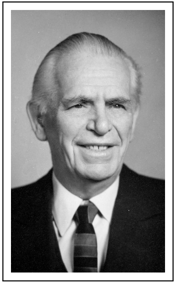
For all large enough primes p, the smallest prime nonsquare mod p is

$$< p^{1/2}.$$



Earlier, I mentioned the theorem of Burgess that for large enough primes p, there is a prime nonsquare mod p smaller than about $p^{1/4\sqrt{e}}$.

I want to present for you a proof of a somewhat weaker result. The beautiful argument — which in my opinion deserves to be better known — is due to Lắszlő Rĕdei.



Theorem (Rĕdei, 1950)

For all large enough primes p, the smallest prime nonsquare mod p is

$$< p^{1/2}.$$

It's enough to produce *any* nonsquare $< p^{1/2}$.

Lemma (Dirichlet, 1849)

The "probability" that two positive integers are relatively prime is $\left(\sum_{n=1}^{\infty} \frac{1}{n^2}\right)^{-1}$, *and so* $(\text{Euler}) = \frac{6}{\pi^2}$.

Here's a heuristic argument for the theorem.

Let's call the probability in question P.

Let P_d be the probability that two positive integers have gcd d, so that $P_1 = P$. It is easy to express P_d in terms of P. Indeed, for x and y to have gcd d, it is necessary and sufficient that $d \mid x$, that $d \mid y$, and that $x/d, y/d$ are relatively prime.

All of this happens with probability

$$\frac{1}{d} \cdot \frac{1}{d} \cdot P = \frac{P}{d^2}.$$

All of this happens with probability

$$\frac{1}{d} \cdot \frac{1}{d} \cdot P = \frac{p}{d^2}.$$

So

$$P_d = \frac{P}{d^2}.$$

But every pair of positive integers has *some* gcd, and so

$$1 = \sum_{d=1}^{\infty} P_d = P \sum_{d=1}^{\infty} \frac{1}{d^2}.$$

Solving for P gives the stated result.

A precise version of the lemma is as follows.

Lemma

As $x \to \infty$, the number of ordered pairs of integers (a, b) with $1 \leq a, b \leq x$ and $\gcd(a, b) = 1$ is

$$\sim \frac{6}{\pi^2} x^2.$$

A precise version of the lemma is as follows.

Lemma

As $x \to \infty$, the number of ordered pairs of integers (a, b) with $1 \le a, b \le x$ and $\gcd(a, b) = 1$ is

$$\sim \frac{6}{\pi^2} x^2.$$

Great, but ... what does this have to do with squares mod p?

Let's suppose for a contradiction that all integers $1 \le a \le \sqrt{p}$ are squares mod p. Then so is every fraction

$$\frac{a}{b}, \quad \text{where} \quad 1 \le a, b \le \sqrt{p},$$

where the fractions are viewed as elements of $\mathbb{F}_p$.

So if all $a \leq \sqrt{p}$ are squares mod p, so are all

$$\frac{a}{b}, \quad \text{where} \quad 1 \leq a, b \leq \sqrt{p}.$$

Claim: The **reduced** fractions in the above list represent distinct elements of $\mathbb{F}_p$.

Indeed, suppose $a/b = c/d$, where $1 \leq a, b, c, d \leq \sqrt{p}$ and $\gcd(a, b) = \gcd(c, d) = 1$. Then

$$0 = ad - bc \qquad \text{in } \mathbb{F}_p.$$

But $|ad - bc| < p$, so $ad - bc = 0$, so $a/b = c/d$ in $\mathbb{Q}$. By uniqueness of lowest-terms representations in $\mathbb{Q}$, we have $a = c$ and $b = d$.

But how many reduced fractions do we have?

This is precisely the number of pairs $1 \leq a, b \leq \sqrt{p}$ with $\gcd(a, b) = 1$, which is

$$\sim \frac{6}{\pi^2}(\sqrt{p})^2 \sim \frac{6}{\pi^2} p.$$

So if all $a \leq \sqrt{p}$ are squares, then the number of squares is at least $\sim \frac{6}{\pi^2} p$. But $\frac{6}{\pi^2} > 0.6$, so there would be $> 0.6p$ squares mod p. But the number of nonzero squares mod p is $< \frac{1}{2} p$. So we get a contradiction for large p.

Working a bit harder, one sees $p = 23$ is the last exception.

Nonsquares in progressions mod 4

Theorem (P.)

If $p \geq 5$, then there is a prime $q < p$ with $q \equiv 3 \pmod 4$ in the list of reduced nonsquares modulo p.

Example ($p = 41$)

3, 6, 7, 11, 12, 13, 14, 15, 17, 19, 22, 24, 26, 27, 28, 29, 30, 34, 35, 38

Theorem (P.)

If $p \geq 13$, then there is a prime $q < p$ with $q \equiv 1 \pmod 4$ in the list of reduced nonsquares modulo p.

Example ($p = 41$)

3, 6, 7, 11, 12, 13, 14, 15, 17, 19, 22, 24, 26, 27, 28, 29, 30, 34, 35, 38

Let's talk first about finding nonsquares congruent to 1 modulo 4.

Theorem (P.)

If $p \geq 13$, then there is a prime $q < p$ with $q \equiv 1 \pmod 4$ in the list of reduced nonsquares modulo p.

Right now I don't have an *elegant* argument for this that works in general — the proof uses analytic arguments that work for $p \geq 3 \cdot 10^{11}$, and then a computer checks the rest.

In some sense this theorem is the easier of the two, since it was already known from work of Friedlander that the conclusion held for all p larger than a certain effectively computable constant. The work is getting the constant down to $3 \cdot 10^{11}$.

Theorem (P.)

If $p \geq 13$, then there is a prime $q < p$ with $q \equiv 1 \pmod 4$ in the list of nonsquares modulo p.

It would be interesting to know if there's a proof that doesn't rely on extensive computer calculation.

There are proofs for certain special classes of primes p. For example, suppose $p \equiv 5 \pmod 8$. In this case, a theorem of Ramanujan–Dickson guarantees one can write $p = x^2 + y^2 + 2z^2$ in integers x, y, z.

Exercise: Show that (a) there is a prime $q \equiv 5 \pmod 8$ dividing $x^2 + y^2$, (b) any such prime satisfies $q < p$ and $\left(\frac{q}{p}\right) = -1$.

Theorem (P.)

If $p \geq 5$, then there is a prime $q < p$ with $q \equiv 3 \pmod 4$ in the list of nonsquares modulo p.

The case of the theorem when $p \equiv 3 \pmod 4$ case is fairly easy.

Proof.

We first treat the case when $p \equiv 3 \pmod 4$. Then $p \geq 7$, so $p - 4 \geq 3$ and $p - 4 \equiv 3 \pmod 4$. Take a prime

$$q \mid p - 4 \quad \text{with} \quad q \equiv 3 \pmod 4.$$

Since $p \equiv 4 \equiv 2^2 \pmod q$, we know p is on the list of squares modulo q. Since $p, q \equiv 3 \pmod 4$, q is **not** on the list of squares mod p. ∎

Theorem (P.)

If $p \geq 5$, then there is a prime $q < p$ with $q \equiv 3 \pmod 4$ in the list of nonsquares modulo p.

Now suppose that $p \equiv 1 \pmod 4$. The classical theory of binary quadratic forms (as developed by Gauss) implies the existence of integers A, B, C with $\gcd(A, B, C) = 1$ such that the two-variable quadratic polynomial

$$F(x, y) := Ax^2 + Bxy + Cy^2$$

has the following properties:

1. $B^2 - 4AC = -4p$,
2. $|B| \leq A \leq C$,
3. if $n = F(x, y)$ for some $x, y \in \mathbb{Z}$ and $\gcd(n, 4p) = 1$, then $n \equiv 3 \pmod 4$ and $\left(\frac{n}{p}\right) = -1$.

$F(x, y) = Ax^2 + Bxy + Cy^2$ has the following properties:

1. $B^2 - 4AC = -4p$,
2. $|B| \leq A \leq C$,
3. if $n = F(x, y)$ for some $x, y \in \mathbb{Z}$ and $\gcd(n, 4p) = 1$, then $n \equiv 3 \pmod{4}$ and $\left(\frac{n}{p}\right) = -1$.

From this we see that

(i) B is even,

(ii) at least one of A, C is odd [since $\gcd(A, B, C) = 1$]

(iii) $A > 1$ [otherwise $1 = F(1, 0)$ violates 3.],

(iv) $1 < A, C \leq \frac{p+1}{2}$,

By (iv), A and C are coprime to p. By (ii), at least one of these is odd, so coprime to $4p$.

$F(x, y) = Ax^2 + Bxy + Cy^2$ has the following properties:

(i) B is even,

(ii) at least one of A, C is odd [since $\gcd(A, B, C) = 1$]

(iii) $A > 1$ [otherwise $1 = F(1, 0)$ violates 3.],

(iv) $1 < A, C \leq \frac{p+1}{2}$,

By (iv), A and C are coprime to p. By (ii), at least one of these is odd, and hence coprime to $4p$. Both A, C are represented by F:

$$A = F(1, 0), \quad \text{while} \quad C = F(0, 1).$$

Now using (3.), we can choose $n \in \{A, C\}$ with

$$\left(\frac{n}{p}\right) = -1 \quad \text{and} \quad n \equiv 3 \pmod 4.$$

Recall: $F(x, y) = Ax^2 + Bxy + Cy^2$, where $B^2 - 4AC = -4p$ and $1 < A, C \leq \frac{p+1}{2}$. Also, $n \in \{A, C\}$ satisfies $n \equiv 3 \pmod 4$.

Take a prime $q \mid n$ with $q \equiv 3 \pmod 4$. Clearly,

$$q \leq n \leq \frac{p+1}{2}.$$

Finally,

$$-4p = B^2 - 4AC \equiv B^2 \pmod q,$$

so that

$$1 = \left(\frac{-4p}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{4}{q}\right)\left(\frac{p}{q}\right) = (-1)(1)\left(\frac{q}{p}\right),$$

so that $\left(\frac{q}{p}\right) = -1$, as desired. ■

Thank you!