Density of primes in progressions dividing certain sequences

B.Sury
Indian Statistical Institute
Bangalore, India
sury@isibang.ac.in

23rd May 2011
St.Petersburg, Russia

Primes and polynomials

Start with the simple-looking question:
Are there infinitely many prime numbers of the form n^2+1?

Answer : Unknown!

Easier question : *Which primes can DIVIDE a number of the form* n^2+1*?*
Equivalently, what are the primes for which the polynomial x^2+1 has a root modulo p?

The answer is easy because we are looking for p such that -1 is a square modulo p.
Apart from $p=2$, these are all the primes of the form $4k+1$.
Thus, roughly half of the prime numbers divide some n^2+1 and half do not.

In general, consider any irreducible integral polynomial f of degree > 1.
We show:

Lemma. *There must be infinitely many primes p such that not divide any of the integers $f(n)$; that is, such that f does not have roots modulo p.*

More generally, ask:
If f is an irreducible integral polynomial, is it necessarily irreducible modulo some prime (infinitely many primes?)?

The answer to this is 'yes and no' !
It is yes if the degree is prime and no if it is composite!
In a few minutes, we show how such questions are attacked and how the earlier lemma is proved.

There exist irreducible, integer polynomials of any composite degree which are reducible modulo evert prime p but Hilbert was the first to find examples in degree 4.
One such is the polynomial $x^4 - 10x^2 + 1$.

More generally, the following ones in degree 4 are all examples:
Let p, q be odd prime numbers such that $(\frac{p}{q}) = (\frac{q}{p}) = 1$ and $p \equiv 1 \ mod \, 8$. Then, the polynomial $P(X) = (X^2 - p - q)^2 - 4pq$ is irreducible whereas it is reducible modulo any integer.

Here is a quick proof using the quadratic reciprocity law.

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X-\sqrt{p}-\sqrt{q})(X+\sqrt{p}+\sqrt{q})(X-\sqrt{p}+\sqrt{q})(X+\sqrt{p}-\sqrt{q}). \end{aligned}$$

Since $\sqrt{p}, \sqrt{q}, \sqrt{p} \pm \sqrt{q}, \sqrt{pq}$ are all irrational, none of the linear or quadratic factors of $P(X)$ are in $\mathbf{Z}[X]$ i.e. $P(X)$ is irreducible.

Note that it is enough to show that a factorization of P exists modulo any prime power as we can use Chinese reminder theorem to get a factorization modulo a general integer.

Now, $P(X)$ can be written in the following ways:

$$\begin{aligned} P(X) &= X^4 - 2(p+q)X^2 + (p-q)^2 \\ &= (X^2 + p - q)^2 - 4pX^2 \\ &= (X^2 - p + q)^2 - 4qX^2 \\ &= (X^2 - p - q)^2 - 4pq. \end{aligned}$$

The second and third equalities above show that $P(X)$ is reducible modulo any q^n and any p^n respectively.
Also since $p \equiv 1 \bmod 8, p$ is a quadratic residue modulo 2 and, therefore, modulo any 2^n; the second equality above again shows that $P(X)$ is the difference of two squares modulo 2^n, and hence reducible mod 2^n.

If ℓ is a prime $\neq 2, p, q$, at least one of $(\frac{p}{\ell}), (\frac{q}{\ell})$ and $(\frac{pq}{\ell})$ is 1 by the product formula $(\frac{p}{\ell}) \cdot (\frac{q}{\ell}) \cdot (\frac{pq}{\ell}) = 1$.

According as $(\frac{p}{\ell}), (\frac{q}{\ell})$ or $(\frac{pq}{\ell}) = 1$, the second, third or fourth equality shows that $P(X)$ is reducible mod ℓ^n for any n.

To make precise statements about infinite sets of primes, it is useful to have a notion of density such as:

A set S of prime numbers is said to have density δ if $\frac{\sum_{p \in S} 1/p^s}{\sum_{all \ \ p} 1/p^s} \to \delta$ as $s \to 1^+$.
Note that any finite set of primes has density 0.

To use this in our situation, recall basic facts from Galois theory.
If f is an irreducible, integral polynomial of degree n, its Galois group is a subgroup of the permutation group S_n.
It permutes the roots transitively and acts as automorphisms of the smallest subfield of $\mathbf{C}$ containing all the roots of f.

Frobenius density theorem

Let f be a monic integral, irreducible polynomial. The set of prime numbers p such that the polynomial f modulo p decomposes as a product of irreducible polynomials of degrees $n_1, n_2, \cdots, n_r$, has a well-defined density. This density equals $N/O(Gal(f))$ where N is the number of elements σ in Gal(f) which have a cycle pattern $n_1, n_2, \cdots, n_r$.

This easily implies our earlier lemma that if f is an irreducible integral polynomial which has roots modulo all but finitely many primes, then it has degree 1.
In other words, for an irreducible integral polynomial f of degree > 1, there are infinitely many primes which do not divide any of the values $f(n)$.

Here is the proof.
The theorem shows that **each** σ in $\mathrm{Gal}(f)$ has a cycle pattern of the form $1, n_2, n_3, \cdots$

This means that each element of $\mathrm{Gal}(f)$ fixes a root of f.

Since the roots of f are transitively moved around by $\mathrm{Gal}(f)$, this Galois group would be the union of the conjugates of its subgroup H consisting of elements which fix a particular root of f.

However, it is an elementary exercise that a finite group cannot be the union of conjugates of a proper subgroup. Thus, in our case $H = \mathrm{Gal}(f)$. This means that $\mathrm{Gal}(f)$ fixes each root and is, therefore, identity. That is, f is linear.

An amusing application is the solution of a problem which appeared in a recent International Mathematical Olympiad:

If p is a prime number, show that there is another prime number q such that $n^p - p$ is not a multiple of q for any natural number n.

Applying our statement above to the polynomial $x^p - p$, we get a conceptually better, proof of a stronger assertion (as it produces infinitely many primes q).

Strong as the above theorem of Frobenius is, there is an even stronger result due to Chebotarev.

To state Chebotarev's theorem, we recall one or two facts from basic algebraic number theory.

The key fact is that given any prime number p not dividing the discriminant of f, there is a conjugacy class defined in Gal(f), called the Frobenius conjugacy class $[Frob_p]$ which comes about as follows.

- If K is the splitting field of f, the ideal generated by p in the ring O_K of integers of K, decomposes uniquely as a product $P_1 P_2 \cdots P_g$ of distinct prime ideals of O_K.

- These prime ideals are said to lie over p; they are permuted transitively by Gal(f).

- Each O_K/P_i is a finite field of p^r elements for some r (and $rg = deg(f)$).

- The stabilizer subgroup $G_{P_i} := \{\sigma \in Gal(f) : \sigma(P_i) = P_i\}$ which is called the decomposition group at P_i maps isomorphically onto the Galois group of the finite field extension $(O_K/P_i)/(Z/pZ)$.

In particular, there is an element $Frob_{P_i}$ of $Gal(f)$ which generates G_{P_i}. For the different i's they are conjugate giving a conjugacy class $[Frob_p]$ in Gal(f).

The Frobenius conjugacy class is trivial if and only if the prime p splits completely into $deg(f)$ prime ideals.

In general, the primes which split completely in an extension field is an important set as it essentially determines the abelian extensions.
We shall soon see how this is of use for us.

For instance, the prime numbers which split completely in the field corresponding to $f(x) = x^n - 1$ are the primes $p \equiv 1 \bmod n$.

In Frobenius's density theorem, one cannot distinguish between two primes p, q which define different conjugacy classes $C(x)$ and $C(y)$ which are such that some power of x and y are conjugate.

For instance, for the polynomial $X^{10} - 1$, the decomposition type modulo primes congruent to $1, 3, 7, 9$ mod 10 are, respectively,
$1, 1, 1, 1, 1, 1, 1, 1, 1, 1;$
$1, 1, 4, 4;$
$1, 1, 4, 4;$
$1, 1, 2, 2, 2, 2.$

Frobenius's theorem cannot distinguish between primes which are 3 mod 10 and those which are 7 mod 10 which define different conjugacy classes in $\mathrm{Gal}(X^{10} - 1)$. Thus, it would imply that the number of primes $\equiv 3$ or 7 mod 10 is infinite but does not say whether each congruence class contains infinitely many primes. This is what Chebotarev's theorem asserts.

Chebotarev's density theorem.
Let f be a monic, irreducible, integral polynomial. Let C be a conjugacy class of Gal(f). Then, the set of primes p not dividing disc (f) for which $\sigma_p \in C$, has a well-defined density which equals $\frac{|C|}{|G|}$.

This theorem implies in particular Dirichlet's theorem that for each a co-prime to n, the set of primes in the congruence class a mod n has density $\frac{1}{\phi(n)}$.

Dirichlet's theorem (in the above form) implies Frobenius's theorem for the polynomial $f(X) = X^n - 1$. The converse conclusion cannot quite be made.

Chebotarev's idea of proving this has been described by two prominent mathematicians as " a spark from heaven".

In fact, this theorem was proved in 1922 ("*while carrying water from the lower part of town to the higher part, or buckets of cabbages to the market, which my mother sold to feed the entire family*")!

Emil Artin wrote to Helmut Hasse in 1925:
"Did you read Chebotarev's paper? ... If it is correct, then one surely has the general abelian reciprocity laws in one's pocket..."
Artin found the proof of the general reciprocity law in 1927 using Chebotarev's technique (he had already boldly published the reciprocity law in 1923 but admitted that he had no proof).
Nowadays, Artin's reciprocity law is proved in some other way and Chebotarev's theorem is deduced from it !

Before moving on, we show how to approach the earlier question we asked:

If f is an irreducible integral polynomial, is it necessarily irreducible modulo some prime?

The answer lies in knowing whether or not $Gal(f)$ has an element of order n, where $\deg(f) = n$.

Indeed, if f is irreducible modulo p, the (mutually conjugate) decomposition groups G_{P_i} for prime ideals P_i lying over p, are cyclic groups of order equal to n.
Therefore, $\mathrm{Gal}(f)$ has elements of order n.

Therefore, if Gal(f) does not contain an element of order n, then f is reducible modulo every prime !

Conversely, if Gal(f) has an element of order n, the Chebotarev density theorem guarantees the existence of an infinite number of primes p whose Frobenius has order n; that is, the polynomial f is irreducible modulo p for such p.

Now, Gal(f) is a transitive subgroup of S_n and, hence, its order is a multiple of n.
If n is a prime, then evidently $Gal(f)$ must contain an element of order p (!)
If n is composite, Gal(f) may or may not contain an element of order n. For Hilbert's example of degree 4, the Galois group is isomorphic to Klein's four group.

Fermat's letter on June 15th, 1641

Now, we come to a specific theorem on primes dividing sequences. Our motivation is a letter written by Fermat to Mersenne on 15th June 1641. For positive integers a, b, let us denote the sequence $\{a^n + b^n\}_{n=1}^{\infty}$ by $S_{a,b}$ and we write $p|S_{a,b}$ if p divides at least one member of $S_{a,b}$. Fermat stated :

Conjecture

(Fermat, 1641)
1) *If* $p|S_{3,1}$, *then* $p \not\equiv -1 (\mathrm{mod}\ 12)$.
2) *If* $p|S_{3,1}$, *then* $p \not\equiv +1 (\mathrm{mod}\ 12)$.
3) *If* $p|S_{5,1}$, *then* $p \not\equiv -1 (\mathrm{mod}\ 10)$.
4) *If* $p|S_{5,1}$, *then* $p \not\equiv +1 (\mathrm{mod}\ 10)$.

The quadratic reciprocity law is easily seen to imply that Conjecture 1 holds true. However, the remaining three conjectures are all false for infinitely many primes!

We completely determine explicitly in terms of a, b, c, d the natural density of primes in the residue class c mod d which divide $S_{a,b}$. It implies, in particular, that there is even a positive density of primes for which each of the conclusions of these three conjectures is false!
For instance, denoting by $\delta_{a,b}(c,d)$ the density of primes in the residue class c mod d which divides $S_{a,b}$, our theorem has the following bearing on the above conjectures :

Corollary

$$\delta_{3,1}(1,12) = 1/6,\ \delta_{3,1}(5,12) = 1/4,\ \delta_{3,1}(7,12) = 1/4 \text{ and } \delta_{3,1}(11,12) = 0.$$

Furthermore, we have

$$\delta_{5,1}(1,10) = 1/12,\ \delta_{5,1}(3,10) = 1/4,\ \delta_{5,1}(7,10) = 1/4 \text{ and } \delta_{5,1}(9,10) = 1/12.$$

The problem of primes dividing sequences arises naturally in the context of the famous unsolved conjecture of Artin on primitive roots.

Gauss considers in articles 315-317 of his Disquisitiones Arithmeticae (1801) the decimal expansion of numbers of the form $\frac{1}{p}$ with p prime. For example, $1/7 = 0.\overline{142857}$, $1/11 = 0.\overline{09}$.

Note that the decimal expansion of $1/p$ is periodic for $p \neq 2, 5$ and the period is $p - 1$ if and only if 10 is a primitive root modulo p.

Artin's primitive root conjecture (1927)

Let $g \in \mathbf{Q} \setminus \{-1,0,1\}$. For a prime p not dividing neither the numerator nor the denominator, one can look at the subgroup of $\mathbf{F}_p^*$ generated by g and call g a primitive root modulo p if this is the whole group.
That is, the order of g modulo p is $p-1$.

Denote by $P(g)$ the set of prime numbers for which g is a primitive root.
Qualitative form of Artin's primitive root conjecture:
The set $P(g)$ is infinite if g is not a square of a rational number.
Quantitative form:
Let h be the largest integer such that $g = g_0^h$ with $g_0 \in \mathbf{Q}$. We have, as x tends to infinity,

$$P(g)(x) := \sum_{p \in P(g), p \leq x} 1 = \prod_{p \nmid h}(1 - \frac{1}{p(p-1)}) \prod_{p | h}(1 - \frac{1}{p-1}) \frac{x}{\log x} + o(x/\log x)$$

Recall the Prime Number Theorem in the form $\pi(x) := \#\{p \leq x\} \sim \mathrm{Li}(x)$ as x tends to infinity (i.e. the quotient of the r.h.s. and l.h.s. tends to 1 as x tends to infinity), where The *logarithmic integral* $\mathrm{Li}(x)$ is defined as $\int_2^x dt/\log t$.

The theorem suggests that the 'probability that a number n is prime' is $1/\log n$.

The prime number theorem is useful especially when used with an error term.
For instance, we shall prove statements like the following:
The number of prime numbers $p \leq x$ dividing some term of the sequence $a^n + b^n$ equals $\delta(a,b)Li(x) + O(E(x))$ where $\delta(a,b)$ is a positive real number and $E(x)/Li(x) \to 0$ as $x \to \infty$.

The starting point to analyse Artin's primitive root conjecture is the following observation :

$$p \in P(g) \iff g^{\frac{p-1}{q}} \not\equiv 1(\mod p) \text{ for every prime } q \text{ dividing } p-1. \tag{1}$$

"$\Longrightarrow$" Obvious.
"$\Longleftarrow$" Suppose $p \notin \mathcal{P}(g)$.
Then $g^{\frac{p-1}{k}} \equiv 1(\mod p)$ for some $k|p-1$, $k > 1$.
But this implies that $g^{\frac{p-1}{d}} \equiv 1(\mod p)$ for some prime divisor d of k.
This is a contradiction.

Thus, associated with a prime p we have conditions for various q. Interchanging the roles of p and q, that is for a *fixed* q we can consider the set of primes p such that $p \equiv 1(\mod q)$ and $g^{\frac{p-1}{q}} \not\equiv 1(\mod p)$.

Fix any prime q and let us try to compute the density of primes p such that both $p \equiv 1(\mod q)$ and $g^{\frac{p-1}{q}} \equiv 1(\mod p)$.

The main observation is that the above two conditions can be interpreted as the prime p splitting completely in a certain field extension and, Chebotarev density theorem determines the density of such primes in terms of the field degree.

For instance, $p \equiv 1(\mod q)$ is true for primes p with density $1/\varphi(q) = 1/(q-1)$.

About the other condition $g^{\frac{p-1}{q}} \equiv 1(\mod p)$, using Fermat's little theorem, we infer (in case $p \nmid g$) that $g^{\frac{p-1}{q}}$ is a solution of $x^q \equiv 1(\mod p)$.

We expect there to be q solutions and we want a solution to be 1 modulo q.
Thus we expect to be successful with probability $\frac{1}{q}$, except when $q|h$.

Then $g^{\frac{p-1}{q}} = g_0^{h\frac{p-1}{q}} \equiv 1 (\mod p)$, trivially.

If we assume that these events are independent then the probability that both events occur is $\frac{1}{q(q-1)}$ if $q \nmid h$ and $\frac{1}{q-1}$ otherwise.

The above events should not occur for any q in order to ensure that $p \in \mathcal{P}(g)$.
This suggests a natural density of

$$\prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q|h} \left(1 - \frac{1}{q-1}\right)$$

for such primes and hence we expect the analytic formulation of Artin's conjecture to hold true.

Artin conjecture as splitting conditions

In Artin's conjecture, a number r divides the index $[\mathbf{F}_p^* :< g \ mod \ p >]$ if, and only if, $r|(p-1)$ and the order of g divides $(p-1)/r$.

This is just the condition that p splits completely in the splitting field $\mathbf{Q}(\zeta_r, g^{1/r})$ of the polynomial $X^r - g$ over $\mathbf{Q}$.
In particular, if $v_2(p-1) = v_2(r)$, then this is equivalent to g having odd order modulo p.

This, in turn, is characterized by the property that $p \equiv 1 + 2^k \mod 2^{k+1}$ and splits completely in the field extension $K_k := \mathbf{Q}(\zeta_{2^k}, g^{1/2^k})$.
So, g is a primitive root modulo p if and only if p does not split completely in *any* of the fields K_k for $k > 1$.

Primes dividing sequences as splitting conditions

Now, we interpret the statement that, for given positive integers a, b, a prime p divides some term of $S_{a,b} := \{a^n + b^n\}$ as statements about splitting of primes in field extensions.

Leaving out primes dividing b, a prime p divides some $a^n + b^n$ if and only if, $g := a/b$ has odd order in $\mathbf{F}_p^*$.
We already know this as splitting conditions in the fields
$K_k := \mathbf{Q}(\zeta_{2^k}, g^{1/2^k})$.

If we have additional conditions on the prime (like $p \equiv c \mod d$) as we have here, we need to 'count' the primes splitting completely in fields obtained by intersecting fields like K_k's above with $\mathbf{Q}(\zeta_d)$ etc. and with a given Frobenius conjugacy class.

Hasse was the first one to raise the question of existence of density for primes dividing sequences.
For instance, he showed that the density exists, and equals $17/24$, for the primes dividing the sequence $2^n + 1$.

The method can be adapted to sequences which satisfy second order linear recurrences like the Lucas sequence $2, 1, 3, 4, 7, 11, \cdots$ for which the density turns out to be $2/3$.

Theorem

Let a and b be positive integers with $a \neq b$. Let $N_{a,b}(x)$ count the number of primes $p \leq x$ that divide $S_{a,b}$. Put $r = a/b$. Let λ be the largest integer such that $r = u^{2^{\lambda}}$, with u a rational number. Let $L = \mathbb{Q}(\sqrt{u})$. We have

$$N_{a,b}(x) = \delta(r)\mathrm{Li}(x) + O\left(\frac{x(\log\log x)^4}{\log^3 x}\right),$$

where the implied constant may depend on a and b, and $\delta(r)$ is a positive rational number that is given in Table 0.

Table 0: The value of $\delta(r)$

L	λ	$\delta(r)$
$L \neq \mathbb{Q}(\sqrt{2})$	$\lambda \geq 0$	$2^{1-\lambda}/3$
$L = \mathbb{Q}(\sqrt{2})$	$\lambda = 0$	$17/24$
$L = \mathbb{Q}(\sqrt{2})$	$\lambda = 1$	$5/12$
$L = \mathbb{Q}(\sqrt{2})$	$\lambda \geq 2$	$2^{-\lambda}/3$

Note that the above table gives, for instance, that the density of primes dividing $10^n + 1$ is $2/3$.
In other words, for two-thirds of the prime numbers p, the decimal expansion of $1/p$ has even period!

Let us indicate how the table is obtained.
For simplicity, take $a \neq 2$ to be a positive integer which is not a proper power.
We are interested in finding the density of primes dividing $a^n + 1$; that is, a has even order modulo p.
The earlier discussion shows that a has odd order modulo p if:
p splits completely in $\mathbf{Q}(\zeta_{2^k}, a^{1/2^k})$ but not in $\mathbf{Q}(\zeta_{2^{k+1}}, a^{1/2^k})$ where $p - 1 \equiv 2^k$ modulo 2^{k+1}.
The Chebotarev density theorem gives the density to be

$$\frac{1}{\mathbf{Q}(\zeta_{2^k}, a^{1/2^k})} - \frac{1}{\mathbf{Q}(\zeta_{2^{k+1}}, a^{1/2^k})} = 1/4^k.$$

Therefore, the density of primes NOT dividing $a^n + 1$ (that is, for which a has odd order) is $\sum_{k \geq 1} 1/4^k = 1/3$.

Theorem 1 implies that if a and b are positive integers such that $a \neq b$, then asymptotically $N_{a,b}(x) \sim \delta(r)x/\log x$ with $\delta(r) > 0$. In particular, the set of all prime divisors of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$ has a positive natural density.

Now, we explicitly determine the densities of primes dividing $S_{a,b}$ lying in the progression c mod d. These can be read off from the tables below knowing the values of a, b, c, d.
However, obtaining these tables is much more complicated.

Theorem

Let a, b, c, d be positive integers with $(c, d) = 1$ and assume that $a \neq b$. Let r and λ be as in the previous theorem. Let

$$N_{a,b}(c,d)(x) := \#\{p \leq x : \; p | S_{a,b}, \; p \equiv c (\mathrm{mod}\ d)\}.$$

Then, for

$$ab \leq \log^{2/3} x \text{ and } d \leq \frac{\log^{1/6} x}{\log\log x},$$

we have

$$N_{a,b}(c,d)(x) = \delta_{a,b}(c,d)\mathrm{Li}(x) + O\left(\frac{2^\lambda x \log\log x}{\log^{7/6} x}\right),$$

where $\delta_{a,b}(c,d)$ is a rational number that is given in Tables 1 to 6 and the implied constant is absolute.

Inspection of the tables shows that we can always write $\varphi(d)\delta_{a,b}(c,d) = \frac{c}{2^m \cdot 3}$, for some non-negative integers c and m.

We have $0 \leq \delta_{a,b}(c,d) \leq 1/\varphi(d)$ by the prime number theorem for arithmetic progressions. In case $\delta_{a,b}(c,d) = 0$ there could potentially be infinitely many primes $p \equiv c (\mathrm{mod}\ d)$ dividing $S_{a,b}$. However, using elementary arguments not going beyond quadratic reciprocity, one can show that there are at most finitely many primes p dividing $S_{a,b}$ in this case. Likewise if $\delta_{a,b} = 1/\varphi(d)$, using elementary arguments not going beyond quadratic reciprocity, one can show that in each case there are at most finitely many primes $p \equiv c (\mathrm{mod}\ d)$ not dividing $S_{a,b}$.

Our results are *unconditional* and we use a version of the Chebotarev density theorem due to Lagarias & Odlyzko.

More precisely, combining such a version with a bound due to Stark for a possible Siegel zero, Pomerance & Shparlinski showed :
Lemma (C.Pomerance & I.E.Shparlinski)
Let $L/\mathbf{Q}$ be a finite, Galois extension. Let $\mathcal{C}$ be a union of conjugacy classes in $G :=$Gal($L/\mathbf{Q}$) and let $\pi_{\mathcal{C}}(L; x)$ denote the number of primes $p \leq x$ which are unramified in L and whose Frobenius class belongs to $\mathcal{C}$. Then, there exist constants $A_1, A_2 > 0$ so that whenever $\log(x) \geq 10[L : \mathbf{Q}](\log|disc(L)|)^2$, we have

$$|\pi_{\mathcal{C}}(L; x) - \frac{|\mathcal{C}|}{|G|}Li(x)| << \frac{|\mathcal{C}|}{|G|}Li(x^{\beta}) + mx\ exp(-A_1\sqrt{\log(x)/[L : \mathbf{Q}]})$$

for some $\beta < 1 - \frac{A_2}{max(|disc(L)|^{1/[L:\mathbf{Q}]}, \log|disc(L)|)}$ where m is the number of conjugacy classes in $\mathcal{C}$.

Although we need to deal only with primes splitting completely, this lemma has an explicit convenient form for our purpose.

As the tables for the density depend on some auxiliary parameters computed from a, b, c, d, some notations are needed to read them.
Given a, b and the modulus d, there is a unique table among the 6 and a unique row of it from which one reads off the density.

- Compute r_0, h from $a/b = r_0^h$, where r_0 is not a proper power of a rational number.
- Find $\lambda = v_2(h)$.
- Find δ, d' in $d = 2^\delta d'$, with $\delta = v_2(d)$.
- Get $\gamma = v_2(c-1)$.
- Write the discriminant $D(r_0)$ of the quadratic field $\mathbb{Q}(\sqrt{r_0})$ as $D(r_0) = 2^{\delta_0} D'$.
- Writing $r_0 = u/v$, let $t = -r_0$ if u, v are odd and, $t = \prod_{i=1}^{k} (\frac{-1}{p_i}) p_i$ if $uv = 2\prod_{i=1}^{k} p_i$.

Table 1 : $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2}), D' \nmid d'$

λ	δ	$\phi(d)\delta_{a,b}(c,d)$
$< \delta$	$\leq \gamma$	$1 - \frac{2^{\lambda+1-\delta}}{3}$
$*$	$> 0, \leq \min(\lambda, \gamma)$	$\frac{2^{\delta-\lambda}}{3}$
$*$	0	$\frac{2^{1-\lambda}}{3}$
$\geq \gamma$	$> \gamma$	0
$< \gamma$	$> \gamma$	$1 - 2^{\lambda-\gamma}$

Table 2 : $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2}), D'|d', \delta_0 \leq \delta$

λ	δ	$(\frac{D(r_0)}{c})$	$\phi(d)\delta_{a,b}(c,d)$
$\geq \delta - 1$	$> 0, \leq \gamma$	1 -1	$\frac{2^{\delta-1-\lambda}}{3}$ $2^{\delta-1-\lambda}$
$*$	0	1 -1	$\frac{2^{-\lambda}}{3}$ $2^{-\lambda}$
$< \delta - 1$	$\leq \gamma$	1 -1	$1 - \frac{2^{\lambda+2-\delta}}{3}$ 1
$\geq \delta$	$> \gamma$	$*$	0
$\leq \gamma - 1$	$> \gamma$	1 -1	$1 - 2^{\lambda+1-\gamma}$ 1
$\geq \gamma$	$> \lambda$	$*$	0

Table 3 : $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2}), D'|d'$ **and** $\delta_0 > \delta$

λ	δ	$(\frac{D(t)}{c})$	$\phi(d)\delta_{a,b}(c,d)$
$< \delta - 1$	$\leq \gamma$	1	$1 - \frac{2^{\lambda+1-\delta}}{3} + \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$< \delta - 1$	$\leq \gamma$	-1	$1 - \frac{2^{\lambda+1-\delta}}{3} - \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$= \delta - 1$	$\leq \gamma$	1	$\frac{2}{3} + \frac{2^{2\delta+1-2\delta_0}}{3}$
$= \delta - 1$	$\leq \gamma$	-1	$\frac{2}{3} - \frac{2^{2\delta+1-2\delta_0}}{3}$
$\leq \gamma - 1$	$> \gamma$	$*$	$1 - 2^{\lambda-\gamma}$
$\geq \gamma$	$> \lambda$	$*$	0
$\geq \delta$	$> \gamma$	$*$	0
$\leq \delta_0 - 2$	$> 0, \leq \min(\gamma, \lambda)$	1	$\frac{2^{\delta-\lambda}}{3} + \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$\leq \delta_0 - 2$	$> 0, \leq \min(\gamma, \lambda)$	-1	$\frac{2^{\delta-\lambda}}{3} - \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$\geq \delta_0 - 1$	$> 0, \leq \gamma$	1	$\frac{2^{\delta-1-\lambda}}{3}$
$\geq \delta_0 - 1$	$> 0, \leq \gamma$	-1	$2^{\delta-\lambda-1}$
$\leq \delta_0 - 2$	0	1	$\frac{2^{1-\lambda}}{3} + \frac{2^{\lambda+3-2\delta_0}}{3}$
$\leq \delta_0 - 2$	0	-1	$\frac{2^{1-\lambda}}{3} - \frac{2^{\lambda+3-2\delta_0}}{3}$
$\geq \delta_0 - 1$	0	1	$\frac{2^{-\lambda}}{3}$
$\geq \delta_0 - 1$	0	-1	$2^{-\lambda}$

Table 4 : $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{2}), \delta \leq 2$

λ	δ	γ	$\phi(d)\delta_{a,b}(c,d)$
0	≤ 1	$\geq \delta$	$17/24$
0	2	$\geq \delta$	$11/12$
0	2	1	$1/2$
1	2	1	0
1	≤ 1	$\geq \delta$	$5/12$
1	2	$\geq \delta$	$5/6$
≥ 2	≤ 1	$\geq \delta$	$2^{-\lambda}/3$
≥ 2	2	$\geq \delta$	$2^{1-\lambda}/3$
≥ 2	2	1	0

Table 5 : $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{2}), \delta \geq 3, \lambda > 0$

λ	δ	γ	$\phi(d)\delta_{a,b}(c,d)$
≥ 2	3	$< \delta$	0
$\geq \delta - 1$	≥ 3	$\geq \delta$	$\frac{2^{\delta-1-\lambda}}{3}$
$\geq 2, < \delta - 1$	≥ 4	$\geq \delta$	$1 - \frac{2^{\lambda+2-\delta}}{3}$
$\geq 2, \leq \gamma - 2$	≥ 4	$< \delta$	$1 - 2^{\lambda+1-\gamma}$
$\geq \max(2, \gamma - 1)$	≥ 4	$< \delta$	0
1	≥ 3	$\geq \delta$	$1 - \frac{2^{3-\delta}}{3}$
1	≥ 3	1	0
1	≥ 3	2	1
1	≥ 3	$\geq 3, < \delta$	$1 - 2^{2-\gamma}$

Table 6 : $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{2}), \delta \geq 3, \lambda = 0$

γ	$c \pmod 8$	$\phi(d)\delta_{a,b}(c,d)$
$\geq \delta$	1	$1 - \frac{2^{2-\delta}}{3}$
≤ 2	± 1	0
≤ 2	± 3	1
$\geq 3, < \delta$	1	$1 - 2^{1-\gamma}$

Table 3 : $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2}), D'|d'$ and $\delta_0 > \delta$

λ	δ	$(\frac{D(t)}{c})$	$\phi(d)\delta_{a,b}(c,d)$
$< \delta - 1$	$\leq \gamma$	1	$1 - \frac{2^{\lambda+1-\delta}}{3} + \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$< \delta - 1$	$\leq \gamma$	-1	$1 - \frac{2^{\lambda+1-\delta}}{3} - \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$= \delta - 1$	$\leq \gamma$	1	$\frac{2}{3} + \frac{2^{2\delta+1-2\delta_0}}{3}$
$= \delta - 1$	$\leq \gamma$	-1	$\frac{2}{3} - \frac{2^{2\delta+1-2\delta_0}}{3}$
$\leq \gamma - 1$	$> \gamma$	$*$	$1 - 2^{\lambda-\gamma}$
$\geq \gamma$	$> \lambda$	$*$	0
$\geq \delta$	$> \gamma$	$*$	0
$\leq \delta_0 - 2$	$> 0, \leq \min(\gamma, \lambda)$	1	$\frac{2^{\delta-\lambda}}{3} + \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$\leq \delta_0 - 2$	$> 0, \leq \min(\gamma, \lambda)$	-1	$\frac{2^{\delta-\lambda}}{3} - \frac{2^{\lambda+2+\delta-2\delta_0}}{3}$
$\geq \delta_0 - 1$	$> 0, \leq \gamma$	1	$\frac{2^{\delta-1-\lambda}}{3}$
$\geq \delta_0 - 1$	$> 0, \leq \gamma$	-1	$2^{\delta-\lambda-1}$
$\leq \delta_0 - 2$	0	1	$\frac{2^{1-\lambda}}{3} + \frac{2^{\lambda+3-2\delta_0}}{3}$
$\leq \delta_0 - 2$	0	-1	$\frac{2^{1-\lambda}}{3} - \frac{2^{\lambda+3-2\delta_0}}{3}$
$\geq \delta_0 - 1$	0	1	$\frac{2^{-\lambda}}{3}$
$\geq \delta_0 - 1$	0	-1	$2^{-\lambda}$

Illustration : $a = 36, b = 1, c = 7, d = 30$

We argue that we must took at row 8.
Indeed $a = 36, b = 1, c = 7, d = 30$ gives $a/b = 36 = 6^2$.
So $r_0 = 6, h = 2, \lambda = v_2(h) = 1$.
As $d = 30$, we get $\delta = 1, d' = 15$ and $\gamma = v_2(c-1) = v_2(6) = 1$.
As $r_0 = 6$, discriminant $D(r_0) = 24 = 2^{\delta_0}D'$ gives $\delta_0 = 3, D' = 3$.
So, $t = -3$ and so $\left(\frac{D(t)}{c}\right) = \left(\frac{-3}{7}\right) = 1$.
As $3 = D'|d' = 15$, we need to look at table 2 or 3.
As $\delta_0 = 3 > \delta = 1$, we look at table 3.
$\lambda = 1 = \delta = \gamma$, so first column means not in first 5 rows.
The 6th and 7th rows are ruled out by looking at the second column.
Last 4 rows ruled out by 2nd column as $\delta \neq 0$; we have rows 8 to 11.
As $\delta_0 = 3$, the first column rules out rows 10 and 11.
Finally, row 9 is ruled out by the 3rd column.
Hence, the density of primes congruent to 7 mod 30 which divide the sequence $36^n + 1$ equals $5/96$.

For $j \geq 1$, the intersection fields $K_j := \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}) \cap \mathbb{Q}(\zeta_d)$ and $K'_j := \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}) \cap \mathbb{Q}(\zeta_d)$ will occur throughout our discussion.

The intersection of $\mathbb{Q}(\sqrt{r_0})$ with cyclotomic fields is different for the case $r_0 = 2$ (due to the ramification of 2 in cyclotomic extensions generated by large 2-power roots).
Thus, although there are esssentially 3 tables, the case of $\mathbb{Q}(\sqrt{2})$ requires separate tables.

Extremal densities

We have $0 \leq \varphi(d)\delta_{a,b}(c,d) \leq 1$. In this section we are interested in the extremal cases when $\delta_{a,b}(c,d) = 0$ and when $\delta_{a,b}(c,d) = 1/\varphi(d)$. If the density is extremal, then it turns out that this can always be explained by elementary arguments not using more than quadratic reciprocity and, furthermore, the associated set of exceptional primes is at most finite.

The sequence $a^n + b^n$ when $ab < 0$.

If we consider the sequence $a^n + (-b)^n$ for positive integers $a > b$, the corresponding density of primes $\equiv c \bmod d$ dividing the sequence can be deduced from our computations for the positive cases - although it is not sufficient to consider only the positive case $a^n + b^n$!

Now, $p|(a^n + (-b)^n)$ for some n if and only if $p|(a^{2m} + b^{2m})$ or $p|(a^{2m-1} - b^{2m-1})$ for some m.
Leaving out the primes dividing b (a set of density zero), the first statement on the right hand side is equivalent to a^2/b^2 having even order modulo p and, the second statement is equivalent to a/b having odd order modulo p.

Therefore, the density for the sequence $a^n + (-b)^n$ satisfies :

$$\delta_{a,-b}(c,d) = \delta_{a^2,b^2}(c,d) + \frac{1}{\phi(d)} - \delta_{a,b}(c,d).$$

In the same notations as used for the earlier tables, we may work out the density values for the sequence $S_{a,-b}$ as tables.

For instance, the tables (which are below) show that the relative density of primes which are 17 mod 56 and divide $3^{8n} + (-1)^n$ is $5/6$ while it is $1/3$ for primes in this progression for the sequence $3^{8n} + 1$.

The relative density for primes 7 mod 15 dividing $6^{4n} + (-1)^n$ is $23/24$ while it is $1/12$ for $6^{4n} + 1$.

A problem by Schinzel & Wójcik

We recall an interesting problem which can be approached similarly to the above one.

In 1976, K.R.Matthews proved under the Generalized Riemann Hypothesis, a simultaneous primitive roots theorem. He proved :

Given non-zero integers $a_1, \cdots, a_r$, there is a constant $c(a_1, \cdots, a_r) \geq 0$ such that if GRH holds, then

$$|\{p \leq x :< a_i \ mod \ p >= \mathbf{Z}_p^* \forall i\}| = c(a_1, \cdots, a_r) Li(x) + O\left(\frac{x(\log\log x)^{2^r - 1}}{(\log x)^2}\right).$$

This has bearing on the following problem studied by Pappalardi, Schinzel, Susa, Wójcik etc. Schinzel & Wójcik posed the following problem :

Given $a, b, c \in \mathbf{Q} \setminus \{0, \pm 1\}$, do there exist infinitely many primes p such that a, b, c have equal orders modulo p ?

More generally, the same problem can be posed for r rational numbers as above instead of three.

It is interesting to note that there are a, b, c which have no odd prime with the desired property !
Indeed, if $b = a^2 = -c$, then the order of $b = a^2$ mod p for any odd prime p, must divide $\frac{ord_p(a)}{2}$.
So, it is very interesting to determine all the possible triples for which the question has an affirmative answer.

Matthews's theorem can be used to deduce an affirmative answer for any $a_1, \cdots, a_r$ with $c(a_1, \cdots, a_r) \neq 0$, provided we assume GRH.
For instance, the triple $2, 3, -6$ provides an affirmative answer as $c(2, 3, -6) \neq 0$.
However, the case $4, 3, -12$ is still open, for instance.
In fact, Wójcik proved under a conjecture known as Schinzel's hypothesis H, that whenever $a_1, \cdots, a_r \neq 0, 1$ are in some number field K and generate a torsion-free subgroup of K^*, then Schinzel's hypothesis H implies that there are infinitely many prime ideals P of degree 1 in K such that all the a_i's have the same order modulo P.

The case $4, 3, -12$ is thus unsolved even if we assume GRH and Schinzel's hypothesis !

The density written as infinite sum

In order to evaluate $\delta_{a,b}(c,d)$ we will make use of the following result. To state it, we need the following notations.
For each positive integer $j \geq 1$, we put $N_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}, \zeta_d)$ and $N'_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}, \zeta_d)$, where $r = a/b$ and, ζ_l for any l, denotes a fixed primitive l-th root of unity. Finally, for $j \geq 1$, the intersection fields $K_j := \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}) \cap \mathbb{Q}(\zeta_d)$ and $K'_j := \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}) \cap \mathbb{Q}(\zeta_d)$ will occur throughout our discussion. As usual, the intersection of $\mathbb{Q}(\sqrt{r_0})$ with cyclotomic fields is different for the case $r_0 = 2$ (due to the ramification of 2 in cyclotomic extensions generated by large 2-power roots). Thus, although there are esssentially 3 tables, the case of $\mathbb{Q}(\sqrt{2})$ requires separate tables.

Theorem

Let a, b, c, d be positive integers with c and d coprime. Let σ_c denote the automorphism of $\mathbb{Q}(\zeta_d)$ determined by $\sigma_c(\zeta_d) = \zeta_d^c$. The density $\delta_{a,b}(c,d)$ of primes $p \equiv c \pmod{d}$ such that $p | S_{a,b}$ exists and satisfies

$$\delta_{a,b}(c,d) = \sum_{j=1}^{\infty} \Big(\frac{\tau(j)}{[N_j : \mathbb{Q}]} - \frac{\tau'(j)}{[N'_j : \mathbb{Q}]} \Big), \tag{2}$$

where
$\tau(j) = 1$ if $\sigma_c|_{K_j} =$id. and 0 if not; and
similarly, $\tau'(j) = 1$ if $\sigma_c|_{K'_j} =$id. and 0 if not.
Furthermore, Theorem 2 holds true with $\delta_{a,b}(c,d)$ as given by (2).

Proof. In case $\text{ord}_p(r)$ is defined we can define the *index*, $i_p(r)$, as $(p-1)/\text{ord}_p(r)$. Note that it equals $[\mathbb{F}_p^* : \langle r \rangle]$. There is a unique $j \geq 1$ such that $2^{j-1} || i_p(r)$. Let P_j denote the set of primes p such that $2^{j-1} || i_p(r)$. Note that $\cup_{j=1}^{\infty} P_j$ equals, with finitely many exceptions, the set of all primes and that the P_i are disjoint sets. Now note that for a prime p in P_j we have that $\text{ord}_p(r)$ is even if and only if $p \equiv 1 (\text{mod } 2^j)$. Thus, except for finitely many primes, the set of prime divisors of $S_{a,b}$ satisfying $p \equiv c (\text{mod } d)$ is of the form $\cup_{j=1}^{\infty} Q_j$, where

$$Q_j := \{p : p \equiv c (\text{mod } d), p \equiv 1 (\text{mod } 2^j),\ p \in P_j\}.$$

It is an easy observation that $n | i_p(r)$ if and only if p splits completely in $\mathbb{Q}(\zeta_n, r^{1/n})$. Using this observation and writing 's.c.' below to mean that the prime is split completely, we infer that

$$Q_j = \{p : p \equiv c (\text{mod } d), p \, \text{s.c.in } \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}), \text{but not s.c.in } \mathbb{Q}(\zeta_{2^j}, r^{1/2^j})\}.$$

On invoking the Chebotarev density theorem, it is then found that the set Q_j has a natural density that is given by

$$\delta(Q_j) = \frac{\tau(j)}{[N_j : \mathbb{Q}]} - \frac{\tau'(j)}{[N_j' : \mathbb{Q}]}.$$

On using the lemma of Pomerance-Shparlinski mentioned earlier, we find that for $ab \leq \log^{2/3} x$ and $[d, 2^j] \leq y := \log^{1/6} x / \log\log x$, and any number $A > 0$, we have

$$Q_j(x) = \delta(Q_j)\mathrm{Li}(x) + O_A\Big(\frac{x}{\log^A x}\Big). \tag{3}$$

Thus

$$N_{a,b}(c,d)(x) = \sum_{j \geq 1} Q_j(x) = \sum_{[d,2^j] \leq y} Q_j(x) + O(\sum_{[d,2^j] > y} \pi(x; [2^j, d], c_j)),$$

where $\pi(x; m, n)$ denotes the number of primes $p \leq x$ such that $p \equiv n (\mathrm{mod}\ m)$ and c_j is any integer such that $c_j \equiv c (\mathrm{mod}\ d)$ and $c_j \equiv 1 (\mathrm{mod}\ 2^j)$ if such an integer exists and 1 otherwise. Using this, one can show

$$N_{a,b}(c,d)(x) = \sum_{[d,2^j] \leq y} Q_j(x) + O\Big(\frac{x \log\log x}{\log^{7/6} x}\Big). \tag{4}$$

Using simple lower bounds for the degrees of $N_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}, \zeta_d)$ and $N_j' = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}, \zeta_d)$, (see lemma below for a more precise computation needed later), we get

$$\sum^{\infty} \delta(Q_j) = O\Big(2^\lambda \sum \frac{1}{[d,2^j]2^j}\Big) = O\Big(\frac{2^\lambda}{}\Big). \tag{5}$$

Remark. The algebraic side of the approach above is not the traditional one, but is chosen since it turns out to be easier to explicitly work out. The traditional approach rests on the observation that if $p \equiv 1 + 2^j \pmod{2^{j+1}}$ for some j (which is uniquely determined), then $\mathrm{ord}_p(r)$ is odd if and only if $r^{(p-1)/2^j} \equiv 1 \pmod{p}$, that is if and only if p splits completely in $\mathbb{Q}(\zeta_{2^j}, r^{1/2^j})$. Note that $(p-1)/2^j$ is the largest odd divisor of $p-1$ and so $\mathrm{ord}_p(r)$ is odd if and only if $\mathrm{ord}_p(r)$ divides $(p-1)/2^j$.

From our tables it is seen that $\delta_{a,b}(c,d)$ is always rational. Below a conceptual explanation for this is given.

Proposition

The density $\delta_{a,b}(c,d)$ is always a rational number.

Proof. We show that the sum in (2) always yields a rational number. Note that $K_j \subseteq K_{j+1}$ and $K'_j \subseteq K'_{j+1}$ and hence the fields $\lim_{j\to\infty} K_j$, $\lim_{j\to\infty} K'_j$ exist. Denote these limits by K, K'. Note that $K = K'$. It follows that there exists j_0 such that $\tau(j) = \tau'(j)$ and $K_j = K'_j = K = K'$ for every $j \geq j_0$. By Lemma **??** below, it follows that there exist constants c_1 and c_2 such that $[N_j : \mathbb{Q}] = c_1 4^j$ and $[N'_j : \mathbb{Q}] = c_2 4^j$ for every j large enough. It follows that the terms with j large enough in (2) are in geometric progression and sum to a rational number. The terms are all rational and so $\delta_{a,b}(c,d)$ is itself rational. □