# Primes in a prescribed arithmetic progression dividing the sequence $\{a^k + b^k\}_{k=1}^{\infty}$

P. Moree and B. Sury

**Abstract**

Given positive integers $a, b, c$ and $d$ such that $c$ and $d$ are coprime we show that the primes $p \equiv c (\mathrm{mod}\ d)$ dividing $a^k + b^k$ for some $k \geq 1$ have a natural density and explicitly compute this density. We demonstrate our results by considering some claims of Fermat that he made in a 1641 letter to Mersenne.

*Mathematics Subject Classification (2001).* 11N37, 11R45.

## 1 Introduction

If $S$ is a sequence of integers, then we say that an integer $m$ divides the sequence if it divides at least one term of the sequence. The sequence $\{a^k + b^k\}_{k=1}^{\infty}$ we will denote by $S_{a,b}$. Several authors studied the problem of characterising (prime) divisors of the sequence $S_{a,b}$. Hasse [5] seems to have been the first to consider the Dirichlet density of prime divisors of such sequences. Later authors, e.g., Odoni [13] and Wiertelak strengthened the analytic aspects of his work, with the strongest result being due to Wiertelak [18]. In particular, Theorem 2 of Wiertelak [18], in the formulation of [11], yields the following corollary (recall that $\mathrm{Li}(x) = \int_2^x dt/\log t$ denotes the logarithmic integral):

**Theorem 1** *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 $\lambda$ 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 $\delta(r)$

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

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 prime divisors of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$ has a positive natural density.

In this paper we will establish, inspired by a letter from Fermat (see next section), a related result.

**Theorem 2** *Let $a, b, c, d$ be positive integers with $(c, d) = 1$ and assume that $a \neq b$. Let $r$ and $\lambda$ be as in the previous theorem. Let*

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

*Then, for*

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

*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.*

We have $0 \le \delta_{a,b}(c, d) \le 1/\varphi(d)$ 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 $S_{a,b}$. For a more precise statement we refer to Theorem 4.

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 $m$.

**Notations:**
As the tables for the density depend on some auxiliary parameters computed from $a, b, c, d$, some notations are needed to read them. We introduce these notations here and they will be maintained throughout this article. Given $a, b$ and the modulus $d$, there is a unique table among the 6 from which one reads off the density. Put $r = a/b = r_0^h$, where $r_0$ is not a proper power of a rational number. Write $h = 2^{\lambda}h', d = 2^{\delta}d'$, with $h', d'$ odd. Put $v_2(c-1) = \gamma$, where it is understood that $\gamma$ is larger than any number when $c = 1$. We denote the discriminant of the quadratic field $\mathbb{Q}(\sqrt{t})$ by $D(t)$ and we put $D(r_0) = 2^{\delta_0}D'$. We also write $r_0 = u/v$ and $t = -r_0$ or $\prod_{i=1}^{k}(\frac{-1}{p_i})p_i$ according as to whether $uv$ is odd or $uv = 2\prod_{i=1}^{k} p_i$. By $d^{\infty}$ we denote the supernatural (Steinitz) number $\prod_{p|d} p^{\infty}$. For each positive integer $j \ge 1$, 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 $\zeta_l$ for any $l$, denotes any fixed primitive $l$-th root of unity. Finally, for $j \ge 1$, 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.

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

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

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

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

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

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

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

| $\lambda$ | $\delta$ | $\gamma$ | $\phi(d)\delta_{a,b}(c,d)$ |
|---|---|---|---|
| 0 | $\leq 1$ | $\geq \delta$ | 17/24 |
| 0 | 2 | $\geq \delta$ | 11/12 |
| 0 | 2 | 1 | 1/2 |
| 1 | 2 | 1 | 0 |
| 1 | $\leq 1$ | $\geq \delta$ | 5/12 |
| 1 | 2 | $\geq \delta$ | 5/6 |
| $\geq 2$ | $\leq 1$ | $\geq \delta$ | $2^{-\lambda}/3$ |
| $\geq 2$ | 2 | $\geq \delta$ | $2^{1-\lambda}/3$ |
| $\geq 2$ | 2 | 1 | 0 |

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

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

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

| $\gamma$ | $c(\text{mod } 8)$ | $\phi(d)\delta_{a,b}(c,d)$ |
|---|---|---|
| $\geq \delta$ | 1 | $1 - \frac{2^{2-\delta}}{3}$ |
| $\leq 2$ | $\pm 1$ | 0 |
| $\leq 2$ | $\pm 3$ | 1 |
| $\geq 3, < \delta$ | 1 | $1 - 2^{1-\gamma}$ |

In the next section we reconsider a letter from Fermat and papers by 3 authors [1, 2, 17] in the light of Theorem 2. In Section 3 we prove Theorem 2, except for the fact that an expression for $\delta_{a,b}(c,d)$ in terms of data from algebraic number theory appears. In Sections 4-7 we evaluate this expression for $\delta_{a,b}(c,d)$. The outcome is recorded in Tables 1-6. This then completes the proof of Theorem 2. In Section 8 we determine the cases in which $\delta_{a,b}(c,d) = 0$, respectively $\delta_{a,b}(c,d) = 1/\varphi(d)$. In the final section we produce the results of some numerical experiments and show that they match well with what can be read from our tables.

## 2 On a letter of Fermat to Mersenne

Fermat [4, p. 220], cf. Dickson [3, p. 267], in a letter to Mersenne dated 15 June 1641 stated that ($p$ will always be used to denote primes):

**Conjecture 1** (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* $p \not\equiv +1 (\mathrm{mod}\ 10)$.

Pur $r = a/b$. For $p \nmid ab$ there exists a smallest positive integer $k$ such that $r^k \equiv 1 (\mathrm{mod}\ p)$; this is $\mathrm{ord}_p(r)$, the multiplicative order of $r (\mathrm{mod}\ p)$. It is not difficult to see that if $p \nmid ab$, then $p|S_{a,b}$ if and only if $\mathrm{ord}_p(r)$ is even. If $p|ab$ and $p \nmid (a,b)$, then clearly $p \nmid S_{a,b}$. (With $(a,b)$ and $[a,b]$ we denote the greatest common divisor, respectively lowest common multiple of $a$ and $b$.) Using this observation and the law of quadratic reciprocity it is easy to see that the following holds:

**Proposition 1** *Conjecture 1.1 of Fermat holds true.*

*Proof.* For $p > 3$ by the law of quadratic reciprocity we have $(\frac{3}{p})(\frac{p}{3}) = (-1)^{\frac{p-1}{2}}$. Suppose that $p \equiv -1 (\mathrm{mod}\ 12)$. It then follows that $(\frac{3}{p}) = 1$. By Euler's identity we then have $3^{\frac{p-1}{2}} \equiv (\frac{3}{p}) = 1 (\mathrm{mod}\ p)$. Since $(p-1)/2$ is the largest odd divisor of $p-1$ it follows that $\mathrm{ord}_p(3)$ is odd. This implies that $p \nmid S_{3,1}$. □

However, a computeralgebra computation learns that the remaining conjectures are all false. Counterexamples (in ascending order) are listed below :
Counterexamples to:

Conjecture 1.2: 37, 61, 73, 97, 157, 193, 241, 337, 349, 373, 397, 409, 457, $\cdots$
Conjecture 1.3: 41, 61, 241, 281, 421, 521, 601, 641, 661, 701, 761, 821, 881,$\cdots$
Conjecture 1.4: 29, 89, 229, 349, 449, 509, 709, 769, 809, 929, 1009, 1049, $\cdots$

Sierpiński suggested that Conjecture 1.2 is false for infinitely many primes. This was proved by Schinzel [16], who in the same paper showed that also Conjecture 1.3 and Conjecture 1.4 are false for infinitely many primes. Theorem 2 implies that there is even a positive density of primes for which the conclusions of these three conjectures are false:

**Corollary 1** *We have*

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

*Furthermore, we have*

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

*In particular, the relative density of the primes for which the conclusion in Conjectures 1.1-1.4 fail are, respectively,*

$$\frac{\delta_{3,1}(11,12)}{\delta(3)}=0,\ \frac{\delta_{3,1}(1,12)}{\delta(3)}=\frac{1}{4},\ \frac{\delta_{5,1}(9,10)}{\delta(5)}=\frac{1}{8},\ \frac{\delta_{5,1}(1,10)}{\delta(5)}=\frac{1}{8}.$$

After Fermat various authors considered primes in arithmetic progressions dividing $S_{a,b}$. Thus Sierpiński [17] proved that every prime $p\equiv\pm 3(\text{mod }8)$ divides $S_{2,1}$ and, furthermore, that no prime $p\equiv 7(\text{mod }8)$ divides $S_{2,1}$. This result easily follows on using that $(\frac{2}{p})=(-1)^{(p^2-1)/8}$. Sierpiński states that M.A. Makowski has proved that infinitely many primes $p\equiv 1(\text{mod }8)$ divide $S_{2,1}$ (namely Makowski notices that the prime factors of the numbers of the form $2^{2^n}+1$ with $n\ge 3$ have the required property) and ends his paper with stating the problem of whether there are infinitely many primes $p\equiv 1(\text{mod }8)$ not dividing $S_{2,1}$. Subsequently, using results on the biquadratic and octavic residue character of 2, this problem has been independently resolved by A. Aigner [1] and A. Brauer [2]. Brauer shows for example that the infinitely many primes $p\equiv 9(\text{mod }16)$ which can be represented as $65x^2+256xy+256y^2$ all do not divide $S_{2,1}$ (the number of such primes $\le x$ is of order $O(x/\sqrt{\log x})$ by a result of G. Pall [14], and thus this set has natural density zero). Using the first entry of Table 6 we infer that there many more primes not dividing $S_{2,1}$: 1/6th of all primes $p\equiv 1(\text{mod }8)$ do not divide $S_{2,1}$.

# 3 The density written as infinite sum

In order to evaluate $\delta_{a,b}(c,d)$ we will make use of the following result.

**Theorem 3** *Let $a,b,c,d$ be positive integers with $c\ge 1$ and $d\ge 1$ coprime. Let $\sigma_c$ 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 $p\equiv c(\text{mod }d)$ such that $p|S_{a,b}$ exists and satisfies*

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

*where*

$$\tau(j)=\begin{cases}1 & \textit{if } \sigma_c|_{K_j}=id.;\\ 0 & \textit{otherwise,}\end{cases}\ \text{ and, similarly, }\ \tau'(j)=\begin{cases}1 & \textit{if } \sigma_c|_{K'_j}=id.;\\ 0 & \textit{otherwise.}\end{cases}$$

*Furthermore, Theorem 2 holds true with $\delta_{a,b}(c,d)$ as given by (1).*

*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 $j\ge 1$ 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 proceeding as in the proof of Lemma 8 of [15] it is then found that for $ab \le \log^{2/3} x$ and $[d, 2^j] \le y := \log^{1/6} x / \log\log x$, and any number $A > 0$, we have

$$Q_j(x) = \delta(Q_j)\text{Li}(x) + O_A\Big(\frac{x}{\log^A x}\Big). \tag{2}$$

Thus

$$N_{a,b}(c, d)(x) = \sum_{j\ge1} Q_j(x) = \sum_{[d,2^j]\le y} Q_j(x) + O(\sum_{[d,2^j]>y} \pi(x; [2^j, d], c_j)),$$

where $\pi(x; m, n)$ denotes the number of primes $p \le x$ such that $p \equiv n (\text{mod } m)$ and $c_j$ is any integer such that $c_j \equiv c (\text{mod } d)$ and $c_j \equiv 1 (\text{mod } 2^j)$ if such an integer exists and 1 otherwise. A minor modification of the proof of Lemma 2 of [7] then yields that

$$N_{a,b}(c, d)(x) = \sum_{[d,2^j]\le y} Q_j(x) + O\Big(\frac{x \log\log x}{\log^{7/6} x}\Big). \tag{3}$$

Using Lemma 2 we find that

$$\sum_{[d,2^j]>y}^{\infty} \delta(Q_j) = O\Big(2^\lambda \sum_{[d,2^j]>y} \frac{1}{[d, 2^j]2^j}\Big) = O(\frac{2^\lambda}{y}). \tag{4}$$

On combining (2), (3) and (4), the result is then obtained with $\delta_{a,b}(c, d) = \sum_{j=1}^{\infty} \delta(Q_j)$. $\square$

`Remark 1`. The algebraic side of the approach above (originating in Moree [7]) is not the traditional one to study the divisiblity of sequences $S_{a,b}$, but is chosen since it turns out to be easier to explicitly work out. The traditional approach rests on the observation that if $p \equiv 1+2^j (\text{mod } 2^{j+1})$ for some $j$ (which is uniquely determined), then $\text{ord}_p(r)$ is odd if and only if $r^{(p-1)/2^j} \equiv 1 (\text{mod } p)$, that is if and only if $p$ splits completely in $\mathbb{Q}(\zeta_{2^j}, r^{1/2^j})$, see e.g. [12] for a sketch of the traditional approach. Note that $(p-1)/2^j$ is the largest odd divisor of $p-1$ and so $\text{ord}_p(r)$ is odd if and only if $\text{ord}_p(r)$ divides $(p-1)/2^j$.

`Remark 2`. On GRH the existence of $\delta_{a,b}(c, d)$ was established by Moree [9, Theorem 1]. He showed under GRH that the set of primes $p$ such that $p \equiv a_1 (\text{mod } d_1)$

and $\mathrm{ord}_p(r) \equiv a_2 (\mathrm{mod}\ d_2)$ has a density $\delta_r(a_1, d_1; a_2; d_2)$ and gave an expression for it in terms of field degrees and Galois intersection coefficients ($\tau(j)$ and $\tau'(j)$ in Theorem 3 are examples of such coefficients). Since $\delta_{a,b}(c,d) = \delta_r(c,d;0,2)$, where $r = a/b$, it follows that $\delta_{a,b}(c,d)$ exists under GRH.

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

**Proposition 2** *The density $\delta_{a,b}(c,d)$ is always a rational number.*

*Proof.* We show that the sum in (1) 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 2 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 (1) 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. □

# 4 Preliminaries on field degrees and field intersections

The following facts from elementary algebraic number theory, for further details we refer to e.g. Moree [9], will be used freely in the sequel:
1) a quadratic field $K \subseteq \mathbb{Q}(\zeta_n)$ iff the discriminant of $K$ divides $n$.
2) Let $\mathbb{Q}(\sqrt{\Delta}) \subseteq \mathbb{Q}(\zeta_n)$ be a quadratic fields of discriminant $\Delta$ and $b$ be an integer with $(b,n) = 1$. Then $\sigma_b|_{\mathbb{Q}(\sqrt{\Delta}}$ = id. iff $(\frac{\Delta}{b}) = 1$, with $(\frac{\cdot}{\cdot})$ the Krnecker symbol.

In order to use Theorem 3 to compute $\delta_{a,b}(c,d)$, we first compute the degrees of the fields $N_j, N'_j$ for $j \geq 1$. This can be done directly or by using the general formula from Lemma 1 of [8] quoted below:

**Lemma 1** *Put $n_t = [2^{v_2(ht)+1}, D(r_0)]$. We have*

$$[\mathbb{Q}(\zeta_{kt}, r^{1/k}) : \mathbb{Q}] = \frac{\phi(kt)k}{\epsilon(kt,k)(k,h)}, \quad \text{where } \epsilon(kt,k) = \begin{cases} 2 & \text{if } n_t | kt; \\ 1 & \text{if } n_t \nmid kt. \end{cases}$$

Using the lemma or otherwise, we compute the degrees of

$$\begin{cases} N_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}, \zeta_d) = \mathbb{Q}(\zeta_{2^{\max(j,\delta)}d'}, r^{1/2^{j-1}}); \\ N'_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}, \zeta_d) = \mathbb{Q}(\zeta_{2^{\max(j,\delta)}d'}, r^{1/2^j}), \end{cases}$$

to be as given in Lemma 2. The degrees turn out to be dependent on the following property which we call $C_j$ :

*The property $(C_j)$ holds if and only if $D'|d', \delta_0 \leq \max(j,\delta)$.*

Note that if $D'|d'$, then $(C_j)$ can fail only for finitely many $j$'s.

**Lemma 2** *The degrees of* $N_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}, \zeta_d)$ *and* $N'_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}, \zeta_d)$ *over* $\mathbb{Q}$ *are given by:*

$$\frac{1}{\varphi(d)}[N_j : \mathbb{Q}] = \begin{cases} 2^{\max(j,\delta)-1} & \textit{if } j \le \lambda+1; \\ 2^{\max(j,\delta)+j-\lambda-3} & \textit{if } j > \lambda+1 \textit{ and } (C_j) \textit{ holds;} \\ 2^{\max(j,\delta)+j-\lambda-2} & \textit{if } j > \lambda+1, \textit{ and } (C_j) \textit{ fails,} \end{cases}$$

$$\frac{1}{\varphi(d')}[N'_j : \mathbb{Q}] = \begin{cases} 2^{\max(j,\delta)-1} & \textit{if } j \le \lambda; \\ 2^{\max(j,\delta)+j-\lambda-2} & \textit{if } j > \lambda \textit{ and } (C_j) \textit{ holds;} \\ 2^{\max(j,\delta)+j-\lambda-1} & \textit{if } j > \lambda \textit{ and } (C_j) \textit{ fails.} \end{cases}$$

`Remark 3`. *Equivalent form of* $(C_j)$.
It will also be convenient to use the following version of $(C_j)$ later.

Property $(C_j)$ *holds if and only if, either* $D(r_0)|d$ *or* $D(r_0)|2^l d, D(r_0) \nmid 2^{l-1}d$ *for some* $l \ge 1$ *and* $j \ge l+\delta$.
*Equivalently, property* $(C_j)$ *fails if, and only if, either* $D(r_0) \nmid 2^l d$ $\forall l \ge 0$ *or* $D(r_0)|2^l d, D(r_0) \nmid 2^{l-1}d$ *for some* $l \ge 1$ *and* $j < l+\delta$.

In the remainder of this section we assume that $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2})$. The case $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2})$ requires modification due to the ramification of 2 in cyclotomic extensions generated by large 2-power roots of unity and is discussed in Sections 7 and 8.

We need to determine precisely the set of all $j \ge 1$ for which $\tau(j) = 1$ and those for which $\tau'(j) = 1$. To this end we first determine the degrees of $K_j, K'_j$ over $\mathbb{Q}$.

**Lemma 3** *When* $\delta > 0$, *the degrees of* $K_j, K'_j$ *are given by the expressions :*

$$[K_j : \mathbb{Q}] = \begin{cases} 2^{\min(j,\delta)} & \textit{if } j \le \lambda+1; \\ 2^{\min(j,\delta)} & \textit{if } j > \lambda+1 \textit{ and } (C_j) \textit{ holds;} \\ 2^{\min(j,\delta)-1} & \textit{if } j > \lambda+1 \textit{ and } (C_j) \textit{ does not hold,} \end{cases}$$

$$[K'_j : \mathbb{Q}] = \begin{cases} 2^{\min(j,\delta)} & \textit{if } j \le \lambda; \\ 2^{\min(j,\delta)} & \textit{if } j > \lambda \textit{ and } (C_j) \textit{ holds;} \\ 2^{\min(j,\delta)-1} & \textit{if } j > \lambda \textit{ and } (C_j) \textit{ does not hold.} \end{cases}$$

*Proof.* When $j \le \lambda+1$, clearly $r^{1/2^{j-1}}$ is rational and, therefore, $K_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$. Similarly, $K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ if $j \le \lambda$. Further, note that $K_j \subseteq K'_j$ for all $j$. Writing $L_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}})$, and $L'_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j})$, we have $N_j = L_j\mathbb{Q}(\zeta_d)$ and $K_j = L_j \cap \mathbb{Q}(\zeta_d)$. Therefore,

$$[K_j : \mathbb{Q}] = \frac{[L_j : \mathbb{Q}][\mathbb{Q}(\zeta_d) : \mathbb{Q}]}{[N_j : \mathbb{Q}]}.$$

Similarly, $N'_j = L'_j\mathbb{Q}(\zeta_d)$ and $K'_j = L'_j \cap \mathbb{Q}(\zeta_d)$. So,

$$[K'_j : \mathbb{Q}] = \frac{[L'_j : \mathbb{Q}][\mathbb{Q}(\zeta_d) : \mathbb{Q}]}{[N'_j : \mathbb{Q}]}.$$

Using the above degree computations for $N_j, N_j'$ etc., we obtain the asserted expressions.

For $\delta = 0$, the above formula has to be modified as we have used $\phi(2^\delta) = 2^{\delta-1}$. In this case, we get :

**Lemma 4** *When $\delta = 0$, we have*

$$[K_j : \mathbb{Q}] = \begin{cases} 2 & \text{if } j > \lambda + 1 \text{ and } (C_j) \text{ holds;} \\ 1 & \text{if either } j \leq \lambda + 1 \text{ or } j > \lambda + 1 \text{ and } (C_j) \text{ fails,} \end{cases}$$

*and*

$$[K_j' : \mathbb{Q}] = \begin{cases} 2 & \text{if } j > \lambda \text{ and } (C_j) \text{ holds;} \\ 1 & \text{if either } j \leq \lambda \text{ or } j > \lambda \text{ and } (C_j) \text{ fails.} \end{cases}$$

`Remark 4.` Since $K_j$ is a subfield of $K_j'$, it follows from the above degree computation that $K_j = K_j'$ in all cases except possibly when $j = \lambda + 1$. For $j = \lambda + 1$, we have $\mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}}) = K_{\lambda+1}$ and the degree of $K_{\lambda+1}'$ over $K_{\lambda+1}$ is 2 if $D'|d'$ and $\delta_0 \leq \max(\lambda + 1, \delta)$. If this latter condition $(C_{\lambda+1})$ does not hold, then $K_{\lambda+1} = K_{\lambda+1}'$. In other words, we have the following property :

$$K_j = K_j', \quad \tau(j) = \tau'(j) \quad \forall \quad j \neq \lambda + 1.$$

We would like to actually write the fields $K_j, K_j'$ in a convenient form so that we can determine how the automorphism $\zeta_d \mapsto \zeta_d^c$ acts on them. Note that clearly the field $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ is always contained in $K_j, K_j'$ and its degree is either the whole or half of that of $K_j, K_j'$ . We look for a subfield of the form $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ or $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{v})$ which has the full degree and will, therefore, have to be the whole field.

**Lemma 5** *For $j \leq \lambda$, $K_j = K_j' = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$.*
*Furthermore, $K_{\lambda+1} = \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}})$.*
*For $j > \lambda + 1$, $K_j = K_j'$.*
*For $j \geq \lambda + 1$, $K_j'$ is :*
(a) $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ *if either $D' \nmid d'$ or if $\delta_0 > \max(j, \delta)$ ;*
(b) $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{r_0})$ *if $D(r_0)|d$ ;*
(c) $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{-r_0})$ *if $D'|d', \delta < \delta_0 \leq \max(j, \delta)$, where $r_0 = u/v$ and $2 \nmid uv$;*
(d) $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{\prod_{i=1}^{k} (\frac{-1}{p_i}) p_i})$ *if $D'|d', \delta < \delta_0 \leq \max(j, \delta)$, where $r_0 = u/v$ with $uv = 2 \prod_{i=1}^{k} p_i$ and $p_i > 2$ for $i = 1, \ldots, k$.*

*Proof.* We know that $K_j = K_j' = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ if either $j \leq \lambda$ or $j > \lambda + 1$ and $(C_j)$ fails. Also, $K_{\lambda+1} = \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}}) = K_{\lambda+1}'$ unless $(C_{\lambda+1})$ fails. In other words, we have to determine $K_j'$ only for those $j > \lambda$ for which $(C_j)$ holds.
Recall that the truth of $(C_j)$ is equivalent to the property :
either $D(r_0)|d$ or $D(r_0)|2^l d, D(r_0) \nmid 2^{l-1} d$ for some $1 \leq l \leq 3$ and $j \geq l + \delta$.
We examine each case separately.

When $D(r_0)|d$, we have $\sqrt{r_0} \in \mathbb{Q}(\zeta_d)$ and so, $\sqrt{r_0} \in K_j'$.
Moreover, if $\delta \geq 1$, then $[\mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{r_0}) : \mathbb{Q}] = 2^{\min(j,\delta)} = [K_j : \mathbb{Q}]$, except in

the case when $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{2})$ which we have excluded in this section. Also, when $\delta = 0$, $[\mathbb{Q}(\sqrt{r_0}) : \mathbb{Q}] = 2 = [K'_j : \mathbb{Q}]$. Therefore $K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{r_0})$ if $D(r_0)|d$.

When $D(r_0)|2^l d, D(r_0) \nmid 2^{l-1}d$ for some $1 \leq l \leq 3$ and $j \geq l + \delta$, it means that $D'|d'$, $\delta_0 = \delta + l$. If $r_0 = u/v$, note that $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{uv})$. Now, if $uv$ is odd, it has to be $\equiv 3 (\bmod\ 4)$ since otherwise $D(r_0) = uv$ which cannot divide $2^l d$ without dividing $d$. Also then $D(r_0) = 4uv = 4D'$, $D'|d'$, $\delta_0 = 2 = \delta + l$ means that $l = 1 = \delta$ or $l = 2, \delta = 0$. In case $uv \equiv 3 (\bmod\ 4)$, we have $\sqrt{-r_0} \in \mathbb{Q}(\sqrt{d})$ as the discriminant of $\mathbb{Q}(\sqrt{-r_0}) = -uv = D'$ which divides $d'$ and hence divides $d$. Therefore $K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{-r_0})$, when $D(r_0)|2^l d, D(r_0) \nmid 2^{l-1}d$ for some $1 \leq l \leq 3$ and $j \geq l + \delta$ and $r_0 = u/v$ with $uv$ odd. Here, we have used the fact that since $j \geq \delta_0 = 2$, $\zeta_4$ (and hence $\sqrt{-r_0}$) belongs to $L'_j$.

When $uv = 2s_0$ with $s_0 > 1$ odd, then $D(r_0) = 4uv = 8s_0, \delta_0 = 3, D' = s_0$. Also $\delta = \delta_0 - l = 3 - l$ and $s_0 = D'|d'$. Thus, if $s_0 = \prod_{i=1}^k p_i$, then $\sqrt{t} \in \mathbb{Q}(\zeta_{p_1 \cdots p_k}) \subseteq \mathbb{Q}(\zeta_d)$, where $t := \prod_{i=1}^k (\frac{-1}{p_i}) p_i$. We have used the fact that $\sqrt{2}, i \in \mathbb{Q}(\zeta_8)$ and that $j \geq \delta_0 = 3$. Hence $K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{t})$ when $uv$ is even and $D(r_0)|2^l d, D(r_0) \nmid 2^{l-1}d$ for some $1 \leq l \leq 3$ and $j \geq l + \delta$. □

An immediate consequence of the previous lemma is the following result on the values of $\tau(j)$ and $\tau'(j)$.

**Lemma 6** *If $j \leq \lambda + 1$, then $\tau(j) = 1 \Leftrightarrow \min(j, \delta) \leq \gamma$.*
*If $j > \lambda+1$ and if either $D' \nmid d'$ or $\delta_0 > \max(j, \delta)$, then $\tau(j) = 1 \Leftrightarrow \min(j, \delta) \leq \gamma$.*
*If $j > \lambda + 1$ and $D(r_0)|d$, then $\tau(j) = 1 \Leftrightarrow \min(j, \delta) \leq \gamma$ and $(\frac{D(r_0)}{c}) = 1$.*
*If $j > \lambda + 1$ and $D'|d', \delta < \delta_0 \leq j$ with $uv$ odd where $r_0 = u/v$, then $\tau(j) = 1 \Leftrightarrow \min(j, \delta) \leq \gamma$ and $(\frac{D(-r_0)}{c}) = 1$.*
*If $j > \lambda + 1$ and $D'|d', \delta < \delta_0 \leq j$ with $uv = 2\prod_{i=1}^k p_i$ where $r_0 = u/v$ and $p_i$'s odd primes, then $\tau(j) = 1 \Leftrightarrow \min(j, \delta) \leq \gamma$ and $(\frac{D(\prod_{i=1}^k (\frac{-1}{p_i}) p_i)}{c}) = 1$.*
*We have $\tau'(j) = \tau(j)$ for $j \neq \lambda + 1$.*
*If either $D' \nmid d'$ or $\delta_0 > \max(\lambda + 1, \delta)$, then $\tau'(\lambda + 1) = 1 \Leftrightarrow \min(\lambda + 1, \delta) \leq \gamma$.*
*If $D(r_0)|d$, then $\tau'(\lambda + 1) = 1 \Leftrightarrow \min(\lambda + 1, \delta) \leq \gamma$ and $(\frac{D(r_0)}{c}) = 1$.*
*If $D'|d', \delta < \delta_0 \leq \lambda + 1$ with $uv$ odd where $r_0 = u/v$, then $\tau'(\lambda + 1) = 1 \Leftrightarrow \min(\lambda + 1, \delta) \leq \gamma$ and $(\frac{D(-r_0)}{c}) = 1$.*
*If $D'|d', \delta < \delta_0 \leq \lambda+1$ with $uv = 2\prod_{i=1}^k p_i$ where $r_0 = u/v$, then $\tau'(\lambda+1) = 1 \Leftrightarrow \min(\lambda + 1, \delta) \leq \gamma$ and $(\frac{D(\prod_{i=1}^k (\frac{-1}{p_i}) p_i)}{c}) = 1$.*

# 5 Tables for the density $\delta_{a,b}(c, d)$ when $\mathbb{Q}(\sqrt{r_0}) \neq \mathbb{Q}(\sqrt{2})$

Recall that the density $\delta_{a,b}(c, d)$ is given by (1). Since the primes considered are in $\phi(d)$ residue classes, it is more natural to compute the sum

$$S := \phi(d)\delta_{a,b}(c, d) = \phi(d) \sum_{j \geq 1} \Big( \frac{\tau(j)}{[N_j : \mathbb{Q}]} - \frac{\tau'(j)}{[N'_j : \mathbb{Q}]} \Big). \tag{5}$$

Note that $S$ gives the relative density of divisibility of $S_{a,b}$, that is

$$S = \lim_{x\to\infty} \frac{\#\{p \le x : p \equiv c(\text{mod } d),\ p|S_{a,b}\}}{\#\{p \le x : p \equiv c(\text{mod } d)\}}.$$

Putting in the degrees of $N_j, N_j'$ we can simplify the sum in (5) as follows.

Since $[N_j : \mathbb{Q}] = [N_j' : \mathbb{Q}]$ and $\tau(j) = \tau'(j)$ for $j \le \lambda$, the terms corresponding to $j \le \lambda$ do not contribute. Also $\tau(j) = \tau'(j)$ for $j > \lambda{+}1$, but $\tau(\lambda + 1)$ and $\tau'(\lambda + 1)$ may be different (only) when $(C_{\lambda+1})$ holds. Therefore, we have :

$$\begin{aligned}\tfrac{S}{\phi(2^\delta)} &= \tau(\lambda+1)2^{1-\max(\lambda+1,\delta)} - \tau'(\lambda+1)2^{1-\max(\lambda+1,\delta)} \\ &+ 2^{\lambda+1}\textstyle\sum_{j>\lambda+1,(C_j)\text{ fails}}\tau(j)2^{-\max(j,\delta)-j} && \text{if } (C_{\lambda+1}) \text{ holds} \\ &+ 2^{\lambda+2}\textstyle\sum_{j>\lambda+1,(C_j)\text{ holds}}\tau(j)2^{-\max(j,\delta)-j}\end{aligned}$$

$$\begin{aligned}\tfrac{S}{\phi(2^\delta)} &= \tau(\lambda+1)2^{1-\max(\lambda+1,\delta)} - \tau(\lambda+1)2^{-\max(\lambda+1,\delta)} \\ &+ 2^{\lambda+1}\textstyle\sum_{j>\lambda+1,(C_j)\text{ fails}}\tau(j)2^{-\max(j,\delta)-j} && \text{if } (C_{\lambda+1}) \text{ fails} \\ &+ 2^{\lambda+2}\textstyle\sum_{j>\lambda+1,(C_j)\text{ holds}}\tau(j)2^{-\max(j,\delta)-j}\end{aligned}$$

As the degrees of the fields $N_j, N_j'$ and the values of $\tau(j), \tau'(j)$'s depend on the following three conditions, is convenient to have 3 tables depending on them. The three conditions are :
(A) $D' \nmid d'$;
(B) $D'|d', \delta_0 \le \delta$;
(C) $D'|d', \delta_0 > \delta$.

Let us first work out the expression for $S$ in case A.

**Case A:** $D' \nmid d'$

Here, every $(C_j)$ fails. In particular,

$$\frac{S}{\phi(2^\delta)} = \tau(\lambda+1)2^{-\max(\lambda+1,\delta)} + 2^{\lambda+1}\sum_{j>\lambda+1}\tau(j)2^{-\max(j,\delta)-j}.$$

Moreover, since $K_j = K_j' = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ for all $j \ge \lambda + 1$, we have :
For all $j \ge \lambda+1$, $\tau(j) = \tau'(j)$ and this is 1 if and only if $\min(j,\delta) \le \gamma$.
Thus, $S = \phi(2^\delta)2^{\lambda+1}\sum_{j>\lambda,\min(j,\delta)\le\gamma} 2^{-\max(j,\delta)-j} = \phi(2^\delta)2^{\lambda+1}(S_1 + S_2)$,
where $S_1$ is the sum over $j \le \delta$ and $S_2$ is the sum over $j \ge \delta + 1$.
We get

$$S_1 = \sum_{\lambda+1\le j\le\min(\gamma,\delta)} 2^{-\delta-j} \text{ and } S_2 = \begin{cases}\sum_{j\ge\max(\lambda+1,\delta+1)} 4^{-j} & \text{if } \delta \le \gamma; \\ 0 & \text{otherwise.}\end{cases}$$

From this, it is easy to obtain Table 1.

**Case B :** $D'|d'$**,** $\delta_0 \le \delta$

Note that $(C_j)$ holds for all $j$.
Here $K_{\lambda+1} = \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}})$ and $K'_{\lambda+1} = \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}}, \sqrt{r_0})$.

For all $j > \lambda+1$, we have $K_j = K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{r_0})$.
Therefore, $\tau(\lambda+1) = 1$ if and only if $\min(\lambda+1,\delta) \leq \gamma$;
$\tau'(\lambda+1) = 1$ if and only if $\min(\lambda+1,\delta) \leq \gamma$ and $(\frac{D(r_0)}{c}) = 1$.
Moreover, for $j > \lambda+1$, we have
$\tau(j) = \tau'(j)$ which is 1 if and only if $\min(j,\delta) \leq \gamma$ and $(\frac{D(r_0)}{c}) = 1$.
Hence, we have

$$\begin{aligned}\frac{S}{\phi(2^\delta)} &= \tau(\lambda+1)2^{1-\max(\lambda+1,\delta)} - \tau'(\lambda+1)2^{1-\max(\lambda+1,\delta)} \\ &+ 2^{\lambda+2}\sum_{j>\lambda+1} \tau(j)2^{-\max(j,\delta)-j},\end{aligned}$$

which can be written down more explicitly as $S = \phi(2^\delta)(t_1 + t_2 + S_0)$, where

$$t_1 = \begin{cases} 2^{1-\max(\lambda+1,\delta)} & \text{if } \min(\lambda+1,\delta) \leq \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

$$t_2 = \begin{cases} -2^{1-\max(\lambda+1,\delta)} & \text{if } \min(\lambda+1,\delta) \leq \gamma \text{ and } (\frac{D(r_0)}{c}) = 1; \\ 0 & \text{otherwise,} \end{cases}$$

$$S_0 = \begin{cases} 2^{\lambda+2}\sum_{j>\lambda+1, \min(j,\delta)\leq\gamma} 2^{-\max(j,\delta)-j} & \text{if } (\frac{D(r_0)}{c}) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Further, $S_0 = S_{01} + S_{02}$, where $S_{01}$ is the subsum where $j$ varies over $j \leq \delta$ and $S_{02}$ is the subsum where $j$ varies over $j > \delta$. We find

$$S_{01} = \begin{cases} 2^{\lambda+2-\delta}(2^{-1-\lambda} - 2^{-\min(\gamma,\delta)}) & \text{if } (\frac{D(r_0)}{c}) = 1 \text{ and } \lambda+2 \leq \min(\delta,\gamma); \\ 0 & \text{otherwise,} \end{cases}$$

and that

$$S_{02} = \begin{cases} 2^{\lambda+2-2\max(\lambda+1,\delta)}/3 & \text{if } (\frac{D(r_0)}{c}) = 1 \text{ and } \delta \leq \gamma; \\ 0 & \text{otherwise.} \end{cases}$$

From this, we obtain Table 2.

Finally, we work out the expression for $S$ in case C. We write $r_0 = u/v$ and $t = -r_0$ or $\prod_{i=1}^k (\frac{-1}{p_i})p_i$ according as to whether $uv$ is odd or $uv = 2\prod_{i=1}^k p_i$. We also write $D(t)$ for the discriminant of the quadratic field $\mathbb{Q}(\sqrt{t})$.

**Case C :** $D'|d'$, $\delta_0 > \delta$

Notice that there are finitely many $j$'s for which the property $(C_j)$ may fail in this case. Now

$$K_{\lambda+1} = \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}}),\ K'_{\lambda+1} = \begin{cases} \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}}) & \text{if } \lambda+1 < \delta_0; \\ \mathbb{Q}(\zeta_{2^{\min(\lambda+1,\delta)}}, \sqrt{t}) & \text{otherwise.} \end{cases}$$

For all $j > \lambda+1$, we have

$$K_j = K'_j = \begin{cases} \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}) & \text{if } j < \delta_0; \\ \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{t}) & \text{otherwise.} \end{cases}$$

So, we have $\tau(\lambda+1) = 1$ if and only if $\min(\lambda+1,\delta) \leq \gamma$ and furthermore we have

$$\tau'(\lambda+1) = 1 \iff \begin{cases} \min(\lambda+1,\delta) \leq \gamma,\ \lambda+1 < \delta_0; \\ \min(\lambda+1,\delta) \leq \gamma,\ \lambda+1 \geq \delta_0,\ \text{and } (\frac{D(t)}{c}) = 1. \end{cases}$$

Moreover, for $j > \lambda+1$ with $j < \delta_0$, we have $\tau(j) = \tau'(j)$ which is 1 if and only if $\min(j,\delta) \le \gamma$.On the other hand, for $j > \lambda+1$ with $j \ge \delta_0$, we have $\tau(j) = \tau'(j)$ which is 1 if and only if $\min(j,\delta) \le \gamma$ and $(\frac{D(t)}{c}) = 1$.
Therefore, we get $S = \phi(2^\delta)(t_1 + t_2 + S_1 + S_2)$, where

$$t_1 = \tau(\lambda+1)2^{1-\max(\lambda+1,\delta)};$$

$$t_2 = \begin{cases} -\tau'(\lambda+1)2^{1-\max(\lambda+1,\delta)} & \text{if } \lambda+1 \ge \delta_0; \\ -\tau(\lambda+1)2^{-\max(\lambda+1,\delta)} & \text{if } \lambda+1 < \delta_0; \end{cases}$$

$S_1 = 2^{\lambda+1} \sum\{2^{-\max(j,\delta)-j} : j > \lambda+1,\ j\delta_0, \min(j,\delta) \le \gamma\}$;
$S_2 = 2^{\lambda+2} \sum\{2^{-\max(j,\delta)-j} : j > \lambda+1, j \ge \delta_0, \min(j,\delta) \le \gamma\}$ if $(\frac{D(t)}{c}) = 1$ and, is 0, otherwise.

Putting in the values of $\tau(\lambda+1)$ and $\tau'(\lambda+1)$, we obtain

$$t_1 = \begin{cases} 2^{1-\max(\lambda+1,\delta)} & \text{if } \min(\lambda+1,\delta) \le \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

$$t_2 = \begin{cases} -2^{1-\max(\lambda+1,\delta)} & \text{if } \lambda+1 \ge \delta_0, \min(\lambda+1,\delta) \le \gamma, (\frac{D(t)}{c}) = 1; \\ -2^{-\max(\lambda+1,\delta)} & \text{if } \lambda+1 < \delta_0, \min(\lambda+1,\delta) \le \gamma; \\ 0 & \text{otherwise.} \end{cases}$$

Finally, as before, we break up each of $S_1$ and $S_2$ into two subsums over $j \le \delta$, respectively, over $j > \delta$. So, we have $S_1 = S_{11} + S_{12}$, where

$$S_{11} = 2^{\lambda+1-\delta} \sum\{2^{-j} : \min(\gamma,\delta) \ge j > \lambda+1\};$$

$$S_{12} = \begin{cases} 2^{\lambda+1} \sum\{4^{-j} : \delta_0 > j \ge \max(\lambda+2, \delta+1)\} & \text{if } \delta \le \gamma; \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, we have $S_2 = S_{21} + S_{22}$,where

$$S_{21} = 0,\ S_{22} = \begin{cases} 2^{\lambda+2} \sum\{4^{-j} : j \ge \max(\lambda+2, \delta_0)\} & \text{if } \delta \le \gamma \text{ and } (\frac{D(t)}{c}) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

On evaluating these expressions further we obtain Table 3.

# 6 The intersection fields when $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{2})$

Next we consider the case where $r_0 = 2$ or $1/2$. Note that the discriminant of $\mathbb{Q}(\sqrt{2})$ is 8 and that $\sqrt{2}$ belongs to the cyclotomic field $\mathbb{Q}(\zeta_8)$ (indeed $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$). Also note that $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$ (we have $\zeta_8 = (i+1)/\sqrt{2}$). For $j \ge 1$ we consider as before the degrees of the fields $N_j, N_j'$. The earlier expressions in Lemma 2 are valid and, in fact, simplify to give:

**Lemma 7** *The degrees of $N_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}, \zeta_d)$ and $N_j' = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}, \zeta_d)$ over $\mathbb{Q}$ are given by :*

$$\frac{1}{\phi(d')}[N_j : \mathbb{Q}] = \begin{cases} 2^{\max(j,\delta)-1} & \textit{if } j \le \lambda+1; \\ 2^{\max(j,\delta)+j-\lambda-3} & \textit{if } j > \lambda+1 \textit{ and } 3 \le \max(j,\delta); \\ 2^{\max(j,\delta)+j-\lambda-2} & \textit{if } j > \lambda+1 \textit{ and } 3 > \max(j,\delta), \end{cases}$$

$$\frac{1}{\phi(d')}[N'_j:\mathbb{Q}] = \begin{cases} 2^{\max(j,\delta)-1} & \text{if } j \leq \lambda; \\ 2^{\max(j,\delta)+j-\lambda-2} & \text{if } j > \lambda \text{ and } 3 \leq \max(j,\delta); \\ 2^{\max(j,\delta)+j-\lambda-1} & \text{if } j > \lambda \text{ and } 3 > \max(j,\delta). \end{cases}$$

The fields $K_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^{j-1}}) \cap \mathbb{Q}(\zeta_d)$ and $K'_j = \mathbb{Q}(\zeta_{2^j}, r^{1/2^j}) \cap \mathbb{Q}(\zeta_d)$ are to be determined. This is where the computation gives different values from Lemma 3. However, the method of evaluation is the same and the degrees turn out to be :

For $j > \lambda + 1$,

$$[K_j:\mathbb{Q}] = \begin{cases} 2^2 & \text{if } j \leq 2, \delta \geq 3; \\ 2^{\min(j,\delta)-1} & \text{if either } j \geq 3,\ \delta \geq 1 \text{ or } j < 3,\ 1 \leq \delta \leq 2; \\ 1 & \text{if } \delta = 0. \end{cases}$$

For $j > \lambda$,

$$[K'_j:\mathbb{Q}] = \begin{cases} 2^j & \text{if } j \leq 2, \delta \geq 3; \\ 2^{\min(j,\delta)-1} & \text{if either } j \geq 3,\ \delta \geq 1 \text{ or } j < 3,\ 1 \leq \delta \leq 2; \\ 1 & \text{if } \delta = 0. \end{cases}$$

As we have evidently, $K_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ for $j \leq \lambda+1$ and for every $j$, $\mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ is a subfield of $K_j$, we have the following result :

**Lemma 8** *We have $K_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ for all $j$ unless $\lambda = 0, j = 2, \delta \geq 3$.*
*In the exceptional cases $\lambda = 0, j = 2, \delta \geq 3$, we have $K_2 = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{2}) = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$.*

*Further, we have $K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ for all $j$ unless $\lambda < j \leq 2, \delta \geq 3$. The exceptional cases here are : either $\lambda = 0, j = 1, \delta \geq 3$ or $\lambda \leq 1, j = 2, \delta \geq 3$. We find the following intersection fields:*

$$\begin{cases} \lambda = 0, j = 1, \delta \geq 3, & K'_1 = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{2}) = \mathbb{Q}(\sqrt{2}); \\ \lambda \leq 1, j = 2, \delta \geq 3, & K'_2 = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}}, \sqrt{2}) = \mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8). \end{cases}$$

# 7 Tables for the density when $\mathbb{Q}(\sqrt{r_0}) = \mathbb{Q}(\sqrt{2})$

Let $S$ be defined as in (5). We divide its computation into four cases :
(A) $\delta < 3$;
(B) $\delta \geq 3$ and $\lambda \geq 2$,
(C) $\delta \geq 3$ and $\lambda = 1$, and
(D) $\delta \geq 3$ and $\lambda = 0$.

**Case A :** $\delta < 3$

Then $K_j = K'_j = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ for all $j$. Thus $\tau(j) = \tau'(j)$ for all $j$ and, this is 1 if and only if $\min(j,\delta) \leq \gamma$. It turns out that $S = \phi(2^\delta)(t_1 + t_2 + t_3)$, with

$$t_1 = \begin{cases} 2^{-\max(\lambda+1,\delta)} & \text{if } \lambda \leq 1, \min(\lambda+1,\delta) \leq \gamma; \\ 0 & \text{otherwise,} \end{cases}, \quad t_2 = \begin{cases} 1/8 & \text{if } \lambda = 0, \delta \leq \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

$$t_3 = \begin{cases} 2^{\lambda+2-2\max(\lambda+1,2)}/3 & \text{if } \delta \leq \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

where $t_1, t_2, t_3$ correspond, respectively, to the terms in (5) with $j = \lambda + 1$, $\lambda + 2 \le j \le 3$, $j \ge \max(3, \lambda + 2)$ and $j \ge \max(3, \delta + 1)$. From this, we obtain Table 4.

**Case B :** $\delta \ge 3$, $\lambda \ge 2$

Once again, $K_j = K_j' = \mathbb{Q}(\zeta_{2^{\min(j,\delta)}})$ for all $j$. Note that $(C_j)$ always holds true. We obtain

$$S = \varphi(d) \sum_{\substack{j \ge \lambda+2 \\ \min(j,\delta) \le \gamma}} \Big( \frac{1}{[N_j : \mathbb{Q}]} - \frac{1}{[N_j' : \mathbb{Q}]} \Big) = \phi(2^\delta)(t_1 + t_2),$$

where

$$t_1 = \begin{cases} 2^{1-\delta} - 2^{\lambda+2-\delta-\min(\gamma,\delta)} & \text{if } \lambda + 2 \le \min(\gamma, \delta); \\ 0 & \text{otherwise,} \end{cases}$$

$$t_2 = \begin{cases} 2^{\lambda+2-2\max(\lambda+1,\delta)}/3 & \text{if } \delta \le \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

with $\varphi(2^\delta)t_1$, $\varphi(2^\delta)t_2$ the subsum over $j \le \delta$, respectively $j > \delta$.

**Case C :** $\delta \ge 3$, $\lambda = 1$

Here, we need to observe that when $8|d$, the Galois automorphism $\zeta_d \mapsto \zeta_d^c$ of $\mathbb{Q}(\zeta_d)$ fixes $\sqrt{2}$ if and only if $c \equiv \pm 1 (\mathrm{mod}\ 8)$. We obtain

$$\frac{S}{\varphi(2^\delta)} = \frac{\tau(\lambda+1)}{2^{\delta-1}} - \frac{\tau'(\lambda+1)}{2^{\delta-1}} + 2^{\lambda+2} \sum_{3 \le j \le \delta} \frac{\tau(j)}{2^{\max(j,\delta)+j}} + 2^{\lambda+2} \sum_{j > \max(2,\delta)} \frac{\tau(j)}{2^{\max(j,\delta)+j}},$$

which can be written as $t_1 + t_2 + t_3 + t_4$ say, where further evaluation yields that

$$t_1 = \begin{cases} 2^{1-\delta} & \text{if } 2 \le \gamma; \\ 0 & \text{otherwise;} \end{cases}, \quad t_2 = \begin{cases} -2^{1-\delta} & \text{if } 3 \le \gamma; \\ 0 & \text{otherwise;} \end{cases}$$

$$t_3 = \begin{cases} 2^{1-\delta} - 2^{3-\delta-\min(\gamma,\delta)} & \text{if } 3 \le \gamma; \\ 0 & \text{otherwise;} \end{cases}, \text{ and } t_4 = \begin{cases} 2^{3-2\delta}/3 & \text{if } \delta \le \gamma; \\ 0 & \text{otherwise.} \end{cases}$$

Table 5 is obtained from cases B and C.

**Case D :** $\delta \ge 3$, $\lambda = 0$

As in the previous case, we need the fact that when $8|d$, the Galois automorphism $\zeta_d \mapsto \zeta_d^c$ of $\mathbb{Q}(\zeta_d)$ fixes $\sqrt{2}$ if and only if $c \equiv \pm 1 (\mathrm{mod}\ 8)$.
We find that $S = \phi(2^\delta)(t_1 + t_2 + t_3 + t_4)$, where

$$t_1 = \begin{cases} 2^{1-\delta} & \text{if } c \equiv \pm 3 (\mathrm{mod}\ 8); \\ 0 & \text{otherwise,} \end{cases}, \quad t_2 = \begin{cases} 2^{-\delta} & \text{if } 3 \le \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

$$t_3 = \begin{cases} 2^{-\delta} - 2^{2-\delta-\min(\gamma,\delta)} & \text{if } 3 \le \min(\gamma, \delta); \\ 0 & \text{otherwise,} \end{cases}, \text{ and } t_4 = \begin{cases} 2^{2-2\delta}/3 & \text{if } \delta \le \gamma; \\ 0 & \text{otherwise,} \end{cases}$$

where $t_1, t_2, t_3, t_4$ correspond, respectively, to the terms in (5) with $j = 1$, $j = 2$, $3 \le j \le \delta$ and $j \ge \max(3, \delta + 1)$. This yields us Table 6.

# 8 Extremal densities

We have $0 \le \varphi(d)\delta_{a,b}(c,d) \le 1$. In this section we are interested when $\delta_{a,b}(c,d) = 0$ and when $\delta_{a,b}(c,d) = 1/\varphi(d)$. The following elementary result shows that if $c \not\equiv 1(\text{mod } (d, 2^{\lambda+1}))$, then $\delta_{a,b}(c,d) = 0$.

**Lemma 9** *If $p \nmid (a,b)$ and $p|S_{a,b}$, then $p \equiv 1(\text{mod } 2^{\lambda+1})$.*

*Proof.* For a prime $p$ put $\tau(p) = (p-1)/(p-1,h)$. If $p \nmid (a,b)$ and $p|ab$, then $p \nmid S_{a,b}$, so we may assume that $p \nmid ab$. Since $r^{\tau(p)} = (r_0^h)^{\tau(p)} \equiv 1(\text{mod } p)$ by Fermat's little theorem, it follows that $\text{ord}_p(r)|\tau(p)$. If $p$ is to divide $S_{a,b}$, then $\tau(p)$ must be even and so $\nu_2(p-1) \ge \lambda + 1$. □

**Theorem 4** a) *Suppose that $\delta_{a,b}(c,d) = 0$. This happens if and only if*
*i) $\lambda \ge \gamma$ and $\delta > \gamma$;*
*or*
*ii) $\lambda = \gamma - 1$, $\delta > \gamma$, $D(r_0)|d$ and $(\frac{D(r_0)}{c}) = 1$.*
*Moreover, if $\delta_{a,b}(c,d) = 0$, then there are at most finitely primes $p \equiv c(\text{mod } d)$ dividing the sequence $S_{a,b}$.*
b) *Suppose that $\delta_{a,b}(c,d) = 1/\varphi(d)$. This happens if and only if*
*i) $\lambda = 0$, $\delta = 0$, $D(r_0)|d$ and $(\frac{D(r_0)}{c}) = -1$;*
*or*
*ii) $\min(\gamma, \delta) > \lambda$, $D(r_0)|d$ and $(\frac{D(r_0)}{c}) = -1$.*
*Moreover, if $\delta_{a,b}(c,d) = 1/\varphi(d)$, then there are at most finitely primes $p \equiv c(\text{mod } d)$ not dividing the sequence $S_{a,b}$.*

*Proof.* For a prime $p$ put $\tau(p) = (p-1)/(p-1,h)$. The first parts of both (a) and (b) follow on inspection of the Tables. Let us prove the second part of (a) now. If $\lambda \ge \gamma$ and $\delta > \gamma$, we claim that $\tau(p)$ is odd. Indeed, writing $p = c + qd$, and $c - 1 = 2^\gamma c_0$ with $c_0$ odd, we have $p - 1 = 2^\gamma c_0 + 2^\delta qd'$. Therefore, $v_2(p-1) = \gamma$ since $\delta > \gamma$. Now, $(p-1,h) = (p-1, 2^\lambda h')$ which has 2-adic valuation $\gamma$ since $\lambda \ge \gamma$. Therefore $\tau(p)$ is odd in the case (i) of (a) of the theorem. Since clearly $\text{ord}_p(r)|\tau(p)$, it then follows that $p \nmid S_{a,b}$. Finally suppose we are in case ii. Suppose that $p > 2$ is a prime satisfying $p \equiv c(\text{mod } d)$ and such that $p$ does not divide $ab$. Then, by the properties of the Kronecker symbol,

$$(\frac{\overline{r_0}}{p}) = \Big(\frac{D(r_0)}{p}\Big) = \Big(\frac{D(r_0)}{c}\Big) = 1,$$

where the first symbol is the Legendre symbol and $\overline{r_0}$ denotes the reduction of $r_0$ modulo $p$. It follows that

$$r_0^{\frac{h(p-1)}{2(p-1,h)}} \equiv 1(\text{mod } p),$$

and so $\text{ord}_p(r)|\tau(p)/2$. We claim that $\tau(p)/2$ is odd. Now $p - 1 = 2^\gamma c_0 + 2^\delta qd'$ which has 2-adic valuation $\gamma$ because $\delta > \gamma$. On the other hand, $2(p-1,h) = 2(p-1, 2^\lambda h') = 2(p-1, 2^{\gamma-1}h')$ which has 2-adic valuation $1 + (\gamma - 1) = \gamma$. Thus, $\tau(p)/2$ is odd and so $p \nmid S_{a,b}$.
b) The proof is similar; let us consider (i) first.

As $\delta = \lambda = 0$, we have $h$ is odd and $r = r_0^h$. If $p > 2$ is a prime not dividing $ab$, then

$$(\frac{\overline{r_0}}{p}) = \Big(\frac{D(r_0)}{p}\Big) = \Big(\frac{D(r_0)}{c}\Big) = -1$$

by assumption. Thus, $r_0^{(p-1)/2} \equiv -1(\text{mod`}p)$, which implies that $r^{(p-1)/2} \equiv -1(\text{mod } p)$ and therefore, that $p|S_{a,b}$. Finally suppose we are in case ii. Writing $p = c + qd$, and $c - 1 = 2^\gamma c_0$ with $c_0$ odd, we have $p - 1 = 2^\gamma c_0 + 2^\delta qd'$. Therefore, $v_2(p-1) \ge \min(\delta, \gamma)$. Now, $v_2(p-1, h) = v_2(p-1, 2^\lambda h') = \lambda$, since $v_2(p-1) \ge \min(\gamma, \delta) > \lambda$. Therefore, we have that $\frac{h}{(p-1,h)}$ is odd while $\tau(p)$ is even; that is, $\frac{p-1}{2(p-1,h)}$ is a positive integer. Once again, we have for each prime not dividing $2ab$ that

$$(\frac{\overline{r_0}}{p}) = \Big(\frac{D(r_0)}{p}\Big) = \Big(\frac{D(r_0)}{c}\Big) = -1.$$

Thus, $(r_0^{(p-1)/2})^{\frac{h}{(p-1,h)}} \equiv -1(\text{mod } p)$. But then $r^{\frac{p-1}{2(p-1,h)}} = (r_0^{(p-1)/2})^{\frac{h}{(p-1,h)}} \equiv -1(\text{mod } p)$, which means that $p|S_{a,b}$. $\square$

`Example`. 1) By case ii of (a) we infer that $\delta_{3,1}(11, 12) = 0$ (cf. Conjecture 1.1 of Fermat).
2) By case ii of (b) we infer that $\varphi(8)\delta_{2,1}(\pm 3, 8) = 1$ (easily proved using $(2/p) = (-1)^{(p^2-1)/8}$), cf. the paper by Sierpiński [17].

Perhaps a more illuminating phrasing of the above theorem is the following.

**Theorem 5** *For a prime $p$ put $\tau(p) = (p-1)/(p-1, h)$.*
a) *We have $\delta_{a,b}(c, d) = 0$ if and only if $\tau(p)$ is odd or $2||\tau(p)$ and $(\frac{r_0}{p}) = 1$, for all but finitely many primes $p \equiv c(\text{mod } d)$.*
b) *We have $\delta_{a,b}(c, d) = 1/\varphi(d)$ if and only if for all but finitely many primes $p \equiv c(\text{mod } d)$ we have that $\tau(p)$ is even and $(\frac{r_0}{p}) = -1$.*

`Conclusion`: if the density is extremal, then 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.

`Remark 5` (*uniform distribution*). It is generally not true that the primes dividing $S_{a,b}$ are uniformly distributed over the residue classes modulo $d$. However, there are some cases where we have uniform distribution. For example, if $d$ is odd and $D(r_0) \nmid d$, then the primes in any residue class mod $d$ which divide $S_{a,b}$ have the same density.

# 9 Some numerical experiments

For each entry in Tables 1-6 an example with parameters $a$ and $b = 1$ was choosen and below we give the value of $\delta_{a,1}(c, d)$ according to the tables on the one hand, and an approximation to this that consists of the first six decimals of the ratio

$$\frac{\#\{p \le p_m : p \equiv c(\text{mod } d),\ p|S_{a,1}\}}{\#\{p \le p_m : p \equiv c(\text{mod } d)\}},$$

where $p_m$ denotes the $m$th prime and $m = 2097152000 \approx 2 \cdot 10^9$. As a rule of thumb an approximation of $\delta_{a,1}(c,d)$ obtained in this way by looking for prime divisors amongs the primes should have an accuracy of about $\pi(p_m; d, c)^{-1/2}$. We clearly observed in our experiments that for larger $d$ the accuracy tends to be less (and the same holds for the run time).

**Test cases for Table 1**

| Residue class | $a$ | $\phi(d)\delta_{a,1}(c,d)$ | Experimental value |
|---|---|---|---|
| 17 mod 56 | $3^2$ | 5/6 | $0.833200\cdots$ |
| 17 mod 56 | $3^8$ | 1/3 | $0.333317\cdots$ |
| 1 mod 21 | 5 | 2/3 | $0.666592\cdots$ |
| 7 mod 20 | $3^4$ | 0 | 0 |
| 7 mod 20 | $3^3$ | 1/2 | $0.500015\cdots$ |

**Test cases for Table 2**

| Residue class | $a$ | $\phi(d)\delta_{a,1}(c,d)$ | Experimental value |
|---|---|---|---|
| 9 mod 28 | $7^2$ | 1/3 | $0.333312\cdots$ |
| 5 mod 12 | $3^2$ | 1 | 1 |
| 1 mod 15 | 5 | 1/3 | $0.333257\cdots$ |
| 7 mod 15 | 5 | 1 | 1 |
| 1 mod 12 | 3 | 2/3 | $0.666657\cdots$ |
| 5 mod 12 | 3 | 1 | 1 |
| 11 mod 20 | $5^4$ | 0 | 0 |
| 13 mod 24 | 3 | 1/2 | $0.500006\cdots$ |
| 13 mod 56 | 7 | 1 | 1 |
| 7 mod 20 | $5^2$ | 0 | 0 |

**Test cases for Table 3**

| Residue class | $a$ | $\phi(d)\delta_{a,1}(c,d)$ | Experimental value |
|---|---|---|---|
| 1 mod 12 | 6 | 11/12 | $0.916693\cdots$ |
| 5 mod 12 | 6 | 3/4 | $0.749989\cdots$ |
| 1 mod 12 | $6^2$ | 5/6 | $0.833362\cdots$ |
| 5 mod 12 | $6^2$ | 1/2 | $0.499996\cdots$ |
| 7 mod 12 | 6 | 1/2 | $0.500038\cdots$ |
| 11 mod 28 | $14^2$ | 0 | 0 |
| 7 mod 12 | $6^4$ | 0 | 0 |
| 7 mod 30 | $6^2$ | 5/12 | $0.416679\cdots$ |
| 11 mod 30 | $6^2$ | 1/4 | $0.250055\cdots$ |
| 7 mod 30 | $6^4$ | 1/12 | $0.083321\cdots$ |
| 11 mod 30 | $6^4$ | 1/4 | $0.250055\cdots$ |
| 7 mod 15 | 6 | 17/24 | $0.708336\cdots$ |
| 11 mod 15 | 6 | 5/8 | $0.624999\cdots$ |
| 7 mod 15 | $6^4$ | 1/12 | $0.083321\cdots$ |
| 11 mod 15 | $6^4$ | 1/4 | $0.250055\cdots$ |

**Test cases for Table 4**

| Residue class | $a$ | $\phi(d)\delta_{a,1}(c,d)$ | Experimental value |
|---|---|---|---|
| 5 mod 14 | 2 | 17/24 | $0.708327\cdots$ |
| 5 mod 12 | 2 | 11/12 | $0.916652\cdots$ |
| 7 mod 12 | 2 | 1/2 | $0.499961\cdots$ |
| 7 mod 12 | $2^2$ | 0 | 0 |
| 5 mod 6 | $2^2$ | 5/12 | $0.416673\cdots$ |
| 5 mod 12 | $2^2$ | 5/6 | $0.833331\cdots$ |
| 5 mod 6 | $2^8$ | 1/24 | $0.041672\cdots$ |
| 5 mod 12 | $2^4$ | 1/6 | $0.166685\cdots$ |
| 7 mod 12 | $2^4$ | 0 | 0 |

**Test cases for Table 5**

| Residue class | $a$ | $\phi(d)\delta_{a,1}(c,d)$ | Experimental value |
|---|---|---|---|
| 5 mod 24 | $2^4$ | 0 | 0 |
| 17 mod 24 | $2^4$ | 1/3 | $0.333372\cdots$ |
| 17 mod 48 | $2^4$ | 2/3 | $0.666740\cdots$ |
| 17 mod 96 | $2^4$ | 1/2 | $0.500145\cdots$ |
| 41 mod 48 | $2^4$ | 0 | 0 |
| 17 mod 24 | $2^2$ | 2/3 | $0.666659\cdots$ |
| 7 mod 24 | $2^2$ | 0 | 0 |
| 5 mod 24 | $2^2$ | 1 | 1 |
| 17 mod 32 | $2^2$ | 3/4 | $0.750049\cdots$ |

**Test cases for Table 6**

| Residue class | $a$ | $\phi(d)\delta_{a,1}(c,d)$ | Experimental value |
|---|---|---|---|
| 9 mod 40 | 2 | 5/6 | $0.833411\cdots$ |
| 7 mod 8 | 2 | 0 | 0 |
| 5 mod 8 | 2 | 1 | 1 |
| 9 mod 16 | 2 | 3/4 | $0.749983\cdots$ |

`Acknowledgement`. This paper was written during a stay February-March 2007 of the second author at the Max-Planck-Institut für Mathematik. The authors have the pleasure in thanking that institute for providing excellent hospitality and a wonderful work atmosphere. In addition they thank Yves Gallot for kindly writing a Visual $C^{++}$ program that was used to create the data in the test case tables.

# References


[1] A. Aigner, Bemerkung und Lösung zum Problem Nr. 29. Unendlich viele Primzahlen der Form $8n+1$ mit geraden und ungeraden Exponenten für 2, *Elem. Math.* **15** (1960), 66-67.

[2] A. Brauer, A note on a number theoretical paper of Sierpinski, *Proc. Amer. Math. Soc.* **11** (1960), 406–409.

[3] L.E. Dickson, History of the theory of numbers, Vol. I: Divisibility and primality, Chelsea Publishing Co., New York 1966.

[4] P. de Fermat, Oeuvres de Fermat publiés par les soins de MM. Paul Tannery et Charles Henry, Tome deuxième, Correspondance, Gauthier-Villars et Fils, Paris, 1894.

[5] H. Hasse, Über die Dichte der Primzahlen $p$, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod. $p$ ist, *Math. Ann.* **166** (1966), 19–23.

[6] P. Moree, On the divisors of $a^k + b^k$, *Acta Arith.* **80** (1997), 197–212.

[7] P. Moree, On primes $p$ for which $d$ divides $\mathrm{ord}_p(g)$, *Funct. Approx. Comment. Math.* **33** (2005), 85–95.

[8] P. Moree, On the distribution of the order and index of $g(\mathrm{mod}\ p)$ over residue classes I, *J. Number Theory* **114** (2005), 238–271.

[9] P. Moree, On the distribution of the order and index of $g(\mathrm{mod}\ p)$ over residue classes. II, *J. Number Theory* **117** (2006), 330–354.

[10] P. Moree, On the distribution of the order and index of $g(\mathrm{mod}\ p)$ over residue classes. III, *J. Number Theory* **120** (2006), 132–160.

[11] P. Moree, Asymptotically exact heuristics for prime divisors of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$, *J. Integer Seq.* **9** (2006), no. 2, Article 06.2.8, 15 pp.

[12] P. Moree, Artin's primitive root conjecture -a survey -, arXiv:math.NT/0412262.

[13] R.W.K. Odoni, A conjecture of Krishnamurthy on decimal periods and some allied problems, *J. Number Theory* **13** (1981), 303–319.

[14] G. Pall, The distribution of integers represented by binary quadratic forms, *Bull. Amer. Math. Soc.* **49** (1943), 447–449.

[15] C. Pomerance and I.E. Shparlinski, Rank statistics for a family of elliptic curves over a function field, preprint (see e.g. homepage of Pomerance).

[16] A. Schinzel, Sur quelques propositions fausses de P. Fermat, *C. R. Acad. Sci. Paris* **249** (1959), 1604–1605.

[17] W. Sierpiński, Sur une décomposition des nombres premiers en deux classes, *Collect. Math.* **10** (1958), 81–83.

[18] K. Wiertelak, On the density of some sets of primes. IV, *Acta Arith.* **43** (1984), 177–190.

Max-Planck-Institut für Mathematik,
Vivatsgasse 7, D-53111 Bonn, Germany.
e-mail: moree@mpim-bonn.mpg.de

Statistics & Mathematics Unit, Indian Statistical Institute,
8th Mile Mysore Road, Bangalore 560059, India.
email : sury@isibang.ac.in