p-ADIC QUOTIENT SETS

STEPHAN RAMON GARCIA, YU XUAN HONG, FLORIAN LUCA, ELENA PINSKER, EVAN SCHECHTER, AND ADAM STARR

Abstract. For $A \subseteq \mathbb{N}$, the question of when $R(A) = \{a/a' : a, a' \in A\}$ is dense in the positive real numbers $\mathbb{R}_+$ has been examined by many authors over the years. In contrast, the p-adic setting is largely unexplored. We investigate conditions under which $R(A)$ is dense in the p-adic numbers. Techniques from elementary, algebraic, and analytic number theory are employed in this endeavor. We also pose many open questions that should be of general interest.

1. Introduction

For $A \subseteq \mathbb{N} = \{1, 2, \ldots\}$ let $R(A) = \{a/a' : a, a' \in A\}$ denote the corresponding *ratio set* (or *quotient set*). The question of when $R(A)$ is dense in the positive real numbers $\mathbb{R}_+$ has been examined by many authors over the years [3–7, 14, 20, 21, 24, 26, 27, 29, 32, 33, 36–38]. Analogues in the Gaussian integers [12] and, more generally, in imaginary quadratic number fields [34] have been considered.

Since $R(A)$ is a subset of the rational numbers $\mathbb{Q}$, there are other important metrics that can be considered. Fix a prime number p and observe that each nonzero rational number has a unique representation of the form $r = \pm p^k a/b$, in which $k \in \mathbb{Z}$, $a, b \in \mathbb{N}$ and $(a, p) = (b, p) = (a, b) = 1$. The *$p$-adic valuation* of such an r is $\nu_p(r) = k$ and its *p-adic absolute value* is $\|r\|_p = p^{-k}$. By convention, $\nu_p(0) = \infty$ and $\|0\|_p = 0$. The *p-adic metric* on $\mathbb{Q}$ is $d(x, y) = \|x - y\|_p$. The field $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to the p-adic metric. Further information can be found in [15, 22].

The first and third authors recently proved that the set of quotients of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all p [13]. Other than this isolated result, the study of quotient sets in the p-adic setting appears largely neglected. We seek here to initiate the general study of p-adic quotient sets. Techniques from elementary, algebraic, and analytic number theory are employed in this endeavor. We also pose many open questions that should be of general interest.

Section 2 introduces several simple, but effective, lemmas. In Section 3, we compare and contrast the p-adic setting with the "real setting." The potential p-adic analogues (or lack thereof) of known results from the real setting are discussed.

Sums of powers are studied in Section 4. Theorem 4.1 completely describes for which m and primes p the ratio set of $\{x_1^2 + \cdots + x_m^2 : x_i \geqslant 0\}$ is dense in $\mathbb{Q}_p$. Cubes are considerably trickier; the somewhat surprising answer is given by Theorem 4.2.

In Section 5 we consider sets whose elements are generated by a second-order recurrence. Theorem 5.2 provides an essentially complete answer for recurrences of the form $a_{n+2} = ra_{n+1} + sa_n$ with $a_0 = 0$ and $a_1 = 1$. Examples are given that demonstrate the sharpness of our result. The proof of Theorem 5.2 involves the

First author partially supported by NSF grant DMS-1265973.

arithmetic of quadratic number fields and relies upon a few interesting techniques that arise again in Section 6 and 7.

Section 6 concerns sets of the form $A = \{b^n + 1 : n \geqslant 0\}$. Theorem 6.3 completely describes the situation: $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 2$ and p divides some element of A. If b is squarefree, a result of Hasse ensures that $R(A)$ is dense in $\mathbb{Q}_p$ for infinitely many p [18].

Fibonacci and Lucas numbers are considered in Section 7. Corollary 7.1 recovers the main result of [13]: the set of quotients of Fibonacci numbers is dense in each $\mathbb{Q}_p$. The situation for Lucas numbers is strikingly different. Theorem 7.2 asserts that the set of quotients of Lucas numbers is dense in $\mathbb{Q}_p$ if and only if $p \neq 2, 5$ divides a Lucas number.

In Section 8 we examine certain unions of arithmetic progressions. For instance, the ratio set of $A = \{5^j : j \geqslant 0\} \cup \{7^j : j \geqslant 0\}$ is dense in $\mathbb{Q}_7$ but not $\mathbb{Q}_5$. This sort of asymmetry is not unusual. Section 9 is devoted to the proof of Theorem 8.3, which asserts that there are infinitely many pairs of primes (p, q) such that p is not a primitive root modulo q while q is a primitive root modulo p^2. The proof is somewhat technical and involves a sieve lemma due to Heath-Brown, along with a little heavy machinery in the form of the Brun-Titchmarsh and Bombieri-Vinogradov theorems. The upshot of Theorem 8.3 is that there are infinitely many pairs of primes (p, q) so that the ratio set of $\{p^j : j \geqslant 0\} \cup \{q^k : k \geqslant 0\}$ is dense in $\mathbb{Q}_p$ but not in $\mathbb{Q}_q$. A number of related questions are posed at the end of Section 8.

2. Preliminaries

We collect here a few preliminary observations and lemmas that will be fruitful in what follows. Although these observations are all elementary, we state them here explicitly as lemmas since we will refer to them frequently.

Lemma 2.1. *If S is dense in $\mathbb{Q}_p$, then for each finite value of the p-adic valuation, there is an element of S with that valuation.*

Proof. If $q \in \mathbb{Q}_p^\times$ can be arbitrarily well approximated with elements of S, then there is a sequence $s_n \in S$ so that $|p^{-\nu_p(s_n)} - p^{-\nu_p(q)}| = |\|s_n\|_p - \|q\|_p| \leqslant \|s_n - q\|_p \to 0$. On $\mathbb{Q}^\times$, the p-adic valuation assumes only integral values, so $\nu_p(s_n)$ eventually equals $\nu_p(q)$. $\square$

The converse of the preceding lemma is false as $S = \{p^k : k \in \mathbb{Z}\}$ demonstrates. More generally, we have the following lemma.

Lemma 2.2. *If A is a geometric progression in $\mathbb{Z}$, then $R(A)$ is not dense in any $\mathbb{Q}_p$.*

Proof. If $A = \{cr^n : n \geqslant 0\}$, in which c and r are nonzero integers, then $R(A) = \{r^n : n \in \mathbb{Z}\}$. Let p be a prime. If $p \nmid r$, then $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1. If $p|r$, then $r^k \equiv -1 \pmod{p^2}$ is impossible since -1 is a unit modulo p. Thus, $R(A)$ is bounded away from -1 in $\mathbb{Q}_p$. $\square$

To simplify our arguments, we frequently appeal to the "transitivity of density." That is, if X is dense in Y and Y is dense in Z, then X is dense in Z. This observation is used in conjunction with the following lemma.

Lemma 2.3. *Let $A \subseteq \mathbb{N}$.*

(a) If A is p-adically dense in $\mathbb{N}$, then $R(A)$ is dense in $\mathbb{Q}_p$.

(b) If $R(A)$ is p-adically dense in $\mathbb{N}$, then $R(A)$ is dense in $\mathbb{Q}_p$.

Proof. (a) If A is p-adically dense in $\mathbb{N}$, it is p-adically dense in $\mathbb{Z}$. Inversion is continuous on $\mathbb{Q}_p^\times$, so $R(A)$ is p-adically dense in $\mathbb{Q}$, which is dense in $\mathbb{Q}_p$.
(b) Suppose that $R(A)$ is p-adically dense in $\mathbb{N}$. Since inversion is continuous on $\mathbb{Q}_p^\times$, the result follows from the fact that $\mathbb{N}$ is p-adically dense in $\{x \in \mathbb{Q} : \nu_p(x) \geqslant 0\}$. $\square$

Although the hypothesis of (a) implies the hypothesis of (b), we have stated them separately. We prefer to use (a) whenever possible. We turn to (b) when confronted with problems that do not succumb easily to (a). This can occur since the hypothesis of (a) is not necessary for $R(A)$ to be dense in $\mathbb{Q}_p$. If A is the set of even numbers, then $R(A) = \mathbb{Q}$ is dense in $\mathbb{Q}_p$ for all p, but A is not 2-adically dense in $\mathbb{N}$. The following lemma concerns more general arithmetic progressions.

Lemma 2.4. *Let $A = \{an + b : n \geqslant 0\}$.*

(a) If $p \nmid a$, then $R(A)$ is dense in $\mathbb{Q}_p$.

(b) If $p | a$ and $p \nmid b$, then $R(A)$ is not dense in $\mathbb{Q}_p$.

Proof. (a) Let $p \nmid a$ and let $n \in \mathbb{N}$ be arbitrary. If $r \geqslant 1$, let $i \equiv a^{-1}(n-b) \pmod{p^r}$ so that $ai + b \equiv n \pmod{p^r}$. Then A is p-adically dense in $\mathbb{N}$, so $R(A)$ is dense in $\mathbb{Q}_p$ by Lemma 2.3.
(b) If $p|a$ and $p \nmid b$, then $\nu_p(an+b) = 0$ for all n. Thus, $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1. $\square$

3. Real versus p-adic setting

A large amount of work has been dedicated to studying the behavior of quotient sets in the "real setting." By this, we refer to work focused on determining conditions upon A which ensure that $R(A)$ is dense in $\mathbb{R}_+$. It is therefore appropriate to begin our investigations by examining the extent to which known results in the real setting remain valid in the p-adic setting.

3.1. **Independence from the real case.** The behavior of a quotient set in the p-adic setting is essentially independent from its behavior in the real setting. To be more specific, a concrete example exists for each of the four statements of the form "$R(A)$ is (dense/not dense) in every $\mathbb{Q}_p$ and (dense/not dense) dense in $\mathbb{R}_+$."

(a) Let $A = \mathbb{N}$. Then $R(A)$ is dense in every $\mathbb{Q}_p$ and dense in $\mathbb{R}_+$.

(b) Let $F = \{1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots\}$ denote the set of Fibonacci numbers. Then $R(F)$ is dense in each $\mathbb{Q}_p$ [13]; see Theorem 5.2 for a more general result. On the other hand, Binet's formula ensures that $R(F)$ accumulates only at integral powers of the Golden ratio, so $R(F)$ is not dense in $\mathbb{R}_+$.

(c) Let $A = \{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ denote the set of prime numbers. The p-adic valuation of a quotient of primes belong to $\{-1, 0, 1\}$, so Lemma 2.1 ensures that $R(A)$ is not dense in any $\mathbb{Q}_p$. The density of $R(A)$ in $\mathbb{R}_+$ is well known consequence of the Prime Number Theorem; see [10, Ex. 218], [11, Ex. 4.19], [14, Cor. 4], [21, Thm. 4], [30, Ex. 7, p. 107], [31, Thm. 4], [36, Cor. 2] (this result dates back at least to Sierpiński, who attributed it to Schinzel [29]).

(d) Let $A = \{2, 6, 30, 210, \ldots\}$ denote the set of *primorials*; the nth primorial is the product of the first n prime numbers. The p-adic valuation of a quotient of primorials belongs to $\{-1, 0, 1\}$, so Lemma 2.1 ensures that $R(A)$ is not dense in any $\mathbb{Q}_p$. Moreover, $R(A) \cap [1, \infty) \subseteq \mathbb{N}$, so $R(A)$ is not dense in $\mathbb{R}_+$.

3.2. **Independence across primes.** Not only is the behavior of a quotient set in the p-adic setting unrelated to its behavior in the real setting, the density of a quotient set in one p-adic number system is completely independent, in a very strong sense, from its density in another.

Theorem 3.1. *For each set P of prime numbers, there is an $A \subseteq \mathbb{N}$ so that $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \in P$.*

Proof. Let P be a set of prime numbers, let Q be the set of prime numbers not in P, and let $A = \{a \in \mathbb{N} : \nu_q(a) \leqslant 1 \ \forall q \in Q\}$. Lemma 2.1 ensures that $R(A)$ is not dense in $\mathbb{Q}_q$ for any $q \in Q$. Fix $p \in P$, let $\ell \geqslant 0$, and let $n = p^k m \in \mathbb{N}$ with $p \nmid m$. Dirichlet's theorem on primes in arithmetic progressions provides a prime of the form $r = p^\ell j + m$. Then $p^k r \in A$ and $p^k r \equiv p^k(p^\ell j + m) \equiv p^k m \equiv n \pmod{p^\ell}$. Since n was arbitrary, Lemma 2.3 ensures that $R(A)$ is dense in $\mathbb{Q}_p$. □

3.3. **Arithmetic progressions.** There exists a set $A \subseteq \mathbb{N}$ which contains arbitrarily long arithmetic progressions and so that $R(A)$ is not dense in $\mathbb{R}_+$ [3, Prop. 1]. On the other hand, there exists a set A that contains no arithmetic progressions of length three and so that $R(A)$ is dense in $\mathbb{R}_+$ [3, Prop. 6]. The same results hold, with different examples, in the p-adic setting.

Example 3.2 (Arbitrarily long arithmetic progressions)**.** The celebrated Green-Tao theorem asserts that the set of primes contains arbitrarily long arithmetic progressions [16]. However, its ratio set is dense in no $\mathbb{Q}_p$; see (c) in Section 3.

A set without long arithmetic progressions can have a quotient set that is dense in some $\mathbb{Q}_p$. Consider the set $A = \{2^n : n \geqslant 0\} \cup \{3^n : n \geqslant 0\}$, which contains no arithmetic progressions of length three [3]. The upcoming Theorem 8.1 implies that $R(A)$ is dense in $\mathbb{Q}_3$. One can confirm that $R(A)$ is bounded away from 5 in $\mathbb{Q}_2$, so $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p = 3$. However, we can do much better.

Theorem 3.3. *There is a set $A \subseteq \mathbb{N}$ that contains no arithmetic progression of length three and which is dense in each $\mathbb{Q}_p$.*

Proof. Fix an enumeration (q_n, r_n) of the set of all pairs (q, r), in which q is a prime power and $0 \leqslant r < q$; observe that each of the the pairs $(q, 0), (q, 1), \ldots, (q, q-1)$ appears exactly once in this enumeration. Construct A, initially empty, according to the following procedure. Include the first natural number a_1 for which $a_1 \equiv r_1 \pmod{q_1}$, then include the first a_2 so that $a_2 > a_1$ and $a_2 \equiv r_2 \pmod{q_2}$. Next, select $a_3 > a_2$ so that $a_3 \equiv r_3 \pmod{q_3}$ and so that a_1, a_2, a_3 is not an arithmetic progression of length three. Continue in this manner, so that a natural number $a_n > a_{n-1}$ is produced in the nth stage so that $a_n \equiv r_n \pmod{q_n}$ and $a_1, a_2, \ldots, a_n$ contains no arithmetic progression of length three. Since $A = \{a_n : n \geqslant 1\}$ contains a complete set of residues modulo each prime power, it is p-adically dense in $\mathbb{N}$ for each prime p. Thus, $R(A)$ is dense in each $\mathbb{Q}_p$ by Lemma 2.3. By construction, A contains no arithmetic progression of length three. □

3.4. **Asymptotic density.** For $A \subseteq \mathbb{N}$, define $A(x) = A \cap [1, x]$. Then $|A(x)|$ denotes the number of elements in A that are at most x. The *lower asymptotic density* of A is

$$\underline{d}(A) = \liminf_{n\to\infty} \frac{|A(n)|}{n}$$

and the *upper asymptotic density* of A is

$$\overline{d}(A) = \limsup_{n\to\infty} \frac{|A(n)|}{n}.$$

If $\underline{d}(A) = \overline{d}(A)$, then their common value is denoted $d(A)$ and called the *asymptotic density* (or *natural density*) of A. In this case, $d(A) = \lim_{n\to\infty} |A(n)|/n$. Clearly $0 \leqslant \underline{d}(A) \leqslant \overline{d}(A) \leqslant 1$.

A striking result of Strauch and Tóth is that if $\underline{d}(A) \geqslant \frac{1}{2}$, then $R(A)$ is dense in $\mathbb{R}_+$ [37]; see also [3] for a detailed exposition. That is, $\frac{1}{2}$ is a critical threshold in the sense that any subset of $\mathbb{N}$ that contains at least half of the natural numbers has a quotient set that is dense in $\mathbb{R}_+$. On the other hand, the critical threshold in the p-adic setting is 1.

Theorem 3.4.

(a) If $\overline{d}(A) = 1$, then $R(A)$ is dense in each $\mathbb{Q}_p$.

(b) For each $\alpha \in [0, 1)$, there is an $A \subseteq \mathbb{N}$ so that $R(A)$ is dense in no $\mathbb{Q}_p$ and $\underline{d}(A) \geqslant \alpha$.

Proof. (a) Suppose that $\overline{d}(A) = 1$. If A contained no representative from some congruence class modulo a prime power p^r, then $\overline{d}(A) \leqslant 1 - 1/p^r < 1$, a contradiction. Thus, A contains a representative from every congruence class modulo each prime power p^r. Let $n, r \in \mathbb{N}$ and select $a, b \in A$ so that $a \equiv n \pmod{p^r}$ and $b \equiv 1 \pmod{p^r}$. Then $a \equiv bn \pmod{p^r}$ and hence $\nu_p(a/b - n) = \nu_p(a - bn) \geqslant r$. Thus, $R(A)$ is dense in $\mathbb{Q}_p$ by Lemma 2.3.

(b) Let $\alpha \in (0, 1)$, let p_n denote the nth prime number, and let r_n be so large that $2^n \leqslant (1 - \alpha)p_n^{r_n}$ for $n \geqslant 1$. If

$$A = \{a \in \mathbb{N} : \nu_{p_n}(a) \leqslant r_n \ \forall n\},$$

then $R(A)$ is dense in no $\mathbb{Q}_p$ by Lemma 2.1. Since A omits every multiple of $p_n^{r_n}$,

$$\underline{d}(A) \geqslant 1 - \sum_{n=1}^{\infty} \frac{1}{p_n^{r_n}} \geqslant 1 - \sum_{n=1}^{\infty} \frac{(1-\alpha)}{2^n} = \alpha. \qquad \square$$

It is also known that if $\underline{d}(A) + \overline{d}(A) \geqslant 1$, then $R(A)$ is dense in $\mathbb{R}_+$ [37, p. 71]. The p-adic analogue is false: for $\alpha \geqslant \frac{1}{2}$, the set A from Theorem 3.4 satisfies $\underline{d}(A) + \overline{d}(A) \geqslant 1$ and is dense in no $\mathbb{Q}_p$. On the other extreme, we have the following theorem.

Theorem 3.5. *There is an $A \subseteq \mathbb{N}$ with $d(A) = 0$ for which $R(A)$ dense in every $\mathbb{Q}_p$.*

Proof. Let q_n denote the increasing sequence $2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, \ldots$ of prime powers. Construct A according to the following procedure. Add the first q_1 numbers to A (that is, $1, 2 \in A$) and skip the next $q_1!$ numbers (that is, $3, 4, \notin A$). Then add the next q_2 numbers to A (that is, $5, 6, 7 \in A$) and skip the next $q_2!$ numbers (that is $8, 9, 10, 11, 12, 13 \notin A$). The rapidly increasing sizes of the gaps between successive blocks of elements of A ensures that $d(A) = 0$. Since A contains arbitrarily long blocks of consecutive integers, it contains a complete set of residues modulo each q_n. Thus, A is p-adically dense in $\mathbb{N}$ for each prime p and hence $R(A)$ is dense in each $\mathbb{Q}_p$ by Lemma 2.3. $\square$

3.5. **Partitions of $\mathbb{N}$.** If $\mathbb{N} = A \sqcup B$, then at least one of $R(A)$ or $R(B)$ is dense in $\mathbb{R}_+$ [5]; this is sharp in the sense that there exists a partition $\mathbb{N} = A \sqcup B \sqcup C$ so that none of $R(A)$, $R(B)$, and $R(C)$ is dense in $\mathbb{R}_+$. See [3] for a detailed exposition of these results. Things are different in the p-adic setting.

Example 3.6. Fix a prime p and let

$$A = \{p^j n \in \mathbb{N} : j \text{ even}, (n,p) = 1\} \quad \text{and} \quad B = \{p^j n \in \mathbb{N} : j \text{ odd}, (n,p) = 1\}.$$

Then $A \cap B = \varnothing$, but neither $R(A)$ nor $R(B)$ is dense in $\mathbb{Q}_p$ by Lemma 2.1.

Problem. Is there a partition $\mathbb{N} = A \sqcup B$ so that A and B are dense in no $\mathbb{Q}_p$?

4. Sums of powers

The representation of integers as the sum of squares dates back to antiquity, although this study only truly flowered with the work of Fermat, Lagrange, and Legendre. Later authors studied more general quadratic forms and also representations of integers as sums of higher powers. From this perspective, it is natural to consider the following family of problems. Let

$$A = \{a \in \mathbb{N} : a = x_1^n + x_2^n + \cdots + x_m^n,\ x_i \geqslant 0\}.$$

For what m, n, and p is $R(A)$ dense in $\mathbb{Q}_p$? For squares and cubes, Theorems 4.1 and 4.2 provide complete answers.

Theorem 4.1. *Let $S_n = \{a \in \mathbb{N} : a$ is the sum of n squares, with 0 permitted$\}$.*

(a) $R(S_1)$ is not dense in any $\mathbb{Q}_p$.

(b) $R(S_2)$ is dense in $\mathbb{Q}_p$ if and only if $p \equiv 1 \pmod 4$.

(c) $R(S_n)$ is dense in $\mathbb{Q}_p$ for all p whenever $n \geqslant 3$.

Proof. (a) Let p be a prime. Then $2|\nu_p(s)$ for all $s \in S_1$ and hence $R(S_1)$ is dense in no $\mathbb{Q}_p$ by Lemma 2.1.

(b) There are three cases: (b1) $p = 2$; (b2) $p \equiv 1 \pmod 4$; (b3) $p \equiv 3 \pmod 4$.

(b1) Since $\nu_2(3) = 0$ any element $a/b \in R(S_2)$ that is sufficiently close in $\mathbb{Q}_2$ to 3 must have $\nu_2(a) = \nu_2(b)$. Without loss of generality, we may assume that a and b are odd. Then $a \equiv b \equiv 1 \pmod 4$ since $a, b \in S_2$, so $a \equiv 3b \pmod 4$ is impossible. Thus, $R(S_2)$ is bounded away from 3 in $\mathbb{Q}_2$.

(b2) Let $p \equiv 1 \pmod 4$. By Lemma 2.3, it suffices to show that for each $n \geqslant 0$ and $r \geqslant 1$, the congruence $x^2 + y^2 \equiv n \pmod{p^r}$ has a solution with $p \nmid x$. We proceed by induction on r. Since there are precisely $(p+1)/2$ quadratic residues modulo p, the sets $\{x^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ and $\{n - y^2 : y \in \mathbb{Z}/p\mathbb{Z}\}$ have a nonempty intersection. Thus, $x^2 + y^2 \equiv n \pmod p$ has a solution. If $p \nmid n$, then p cannot divide both x and y; in this case we may assume that $p \nmid x$. If $p | n$, let $x = 1$ and $y^2 \equiv -1 \pmod p$; such a y exists since $p \equiv 1 \pmod 4$. This establishes the base case $r = 1$.

Suppose that $x^2+y^2 \equiv n \pmod{p^r}$ and $p\nmid x$. Then $x^2+y^2 = n+mp^r$ for some $m \in \mathbb{Z}$. Let $i \equiv -2^{-1}x^{-1}m \pmod{p}$ so that $p|(2ix+m)$. Then

$$\begin{aligned}(x+ip^r)^2+y^2 &= x^2+2ixp^r+i^2p^{2r}+y^2\\ &\equiv n+(2ix+m)p^r \pmod{p^{r+1}}\\ &\equiv n \pmod{p^{r+1}}.\end{aligned}$$

This completes the induction.

(b3) Let $p \equiv 3 \pmod 4$. If $a,b \in S_2$, then a theorem of Fermat ensures that $\nu_p(a)$ and $\nu_p(b)$ are both even. Then $\nu_p(a)-\nu_p(b) = \nu_p(a/b) \neq 1 = \nu_p(p)$ for all $a,b \in S_2$. Thus, S_2 is bounded away from p in $\mathbb{Q}_p$.

(c) Lagrange's four-square theorem asserts that $S_n = \mathbb{N}$ for $n \geqslant 4$, so $R(S_n) = \mathbb{Q}$ is dense in $\mathbb{Q}_p$ for $n \geqslant 4$. Thus, we consider only $n = 3$. There are three cases to consider: (c1) $p = 2$; (c2) $p \equiv 1 \pmod 4$; (c3) $p \equiv 3 \pmod 4$.

(c1) Recall that Legendre's three square theorem asserts that a natural number is in S_3 if and only if it is not of the form $4^i(8j+7)$ for some $i,j \geqslant 0$. Consequently, if the 2-adic order of a natural number is odd, then it is the sum of three squares. Let $n \in \mathbb{N}$ be odd and let $k \in \mathbb{N}$. If k is odd, let $a = 2^k n$ and $b = 1$; if k is even, let $a = 2^{k+1}n$ and $b = 2$. Then $a = 2^k nb$ and $a,b \in S_3$ since $\nu_2(a)$ is odd. Consequently, $a \equiv 2^k nb \pmod{2^r}$ for all $r \in \mathbb{N}$, so $R(S_3)$ is 2-adically dense in $\mathbb{N}$. Lemma 2.3 ensures that $R(S_3)$ is dense in $\mathbb{Q}_2$.

(c2) If $p \equiv 1 \pmod 4$, then $R(S_3)$ contains $R(S_2)$, which is dense in $\mathbb{Q}_p$ by (b2).

(c3) Let $p \equiv 3 \pmod 4$. Since $4^j(8k+7)$ is congruent to either 0, 4, or 7 modulo 8, it follows that S_3 contains the infinite arithmetic progression $A = \{8k+1 : k \geqslant 0\}$. Lemma 2.4 ensures that $R(A)$ is dense in $\mathbb{Q}_p$, so $R(S_3)$ is dense in $\mathbb{Q}_p$ too. $\square$

Theorem 4.2. *Let $C_n = \{a \in \mathbb{N} : a$ is the sum of n cubes, with 0 permitted$\}$.*

(a) $R(C_1)$ is not dense in any $\mathbb{Q}_p$.

(b) $R(C_2)$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 3$.

(c) $R(C_n)$ is dense in all $\mathbb{Q}_p$ for all p whenever $n \geqslant 3$.

Proof. (a) Let p be a prime. Then $3|\nu_p(c)$ for all $c \in C_1$, so Lemma 2.1 ensures that $R(C_1)$ is dense in no $\mathbb{Q}_p$.

(b) There are three cases: (b1) $p \neq 3,7$; (b2) $p = 3$; and (b3) $p = 7$.

(b1) The congruence $x^3+y^3 \equiv n \pmod{m}$ has a solution for each n if and only if $7\nmid m$ or $9\nmid m$ [2, Thm. 3.3]. Consequently, C_2 is p-adically dense in $\mathbb{N}$ if $p \neq 3,7$, so $R(C_2)$ is dense in $\mathbb{Q}_p$ for $p \neq 3,7$ by Lemma 2.3.

(b2) If $x/y \in R(C_2)$ is sufficiently close to 3 in $\mathbb{Q}_3$, then $\nu_3(x) = \nu_3(y)+1$. Without loss of generality, we may suppose that $\nu_3(x) = 1$ and $\nu_3(y) = 0$. A sum of two cubes modulo 9 must be among $0,1,2,7,8$, so $\nu_3(x) = 1$ is impossible for $x \in C_2$. Thus, $R(C_2)$ is not dense in $\mathbb{Q}_3$.

(b3) Let $p = 7$. For each integer m congruent to $0,1,2,5$ or 6 modulo 7 and each $r \geqslant 1$, we use induction on r to show that $x^3+y^3 \equiv m \pmod{7^r}$ has a solution with $7\nmid x$. The cubes modulo 7 are $0,1$ and 6 and hence each of the residue classes $0,1,2,5,6$ is a sum of two cubes modulo 7, at least one of which is nonzero. This is the base of the induction. Suppose that n congruent to $0,1,2,5$ or 6 modulo 7 and that $x^3+y^3 \equiv m \pmod{7^r}$, in which $7 \nmid x$. Then $x^3+y^3 = m + 7^r\ell$ for some $\ell \in \mathbb{Z}$. Let $i \equiv -5\ell x^{-2} \pmod 7$, so that $7|(3ix^2+\ell)$. Then

$$\begin{aligned}(x+7^r i)^3 + y^3 &\equiv x^3+y^3+3x^2\cdot 7^r i \pmod{7^{r+1}}\\ &\equiv m + 7^r(3ix^2+\ell) \pmod{7^{r+1}}\\ &\equiv m \pmod{7^{r+1}}.\end{aligned}$$

Since $7\nmid x$, we have $7 \nmid (x+7^r i)$. This completes the induction.

The inverses of $1,2,5$ and 6 modulo 7 are $1,4,3$ and 6, respectively. Consequently, for each m congruent to $1,3,4$ or 6 modulo 7, the congruence $(x^3+y^3)^{-1} \equiv m \pmod{7^r}$ has a solution with $7\nmid x$.

Each residue class modulo 7 is a product of an element in $\{0,1,2,5,6\}$ with an element in $\{1,3,4,6\}$. Given a natural number n and $r \geqslant 0$, write $n \equiv m_1 m_2 \pmod{7^r}$, in which m_1 modulo 7 is in $\{0,1,2,5,6\}$ and m_2 modulo 7 is in $\{1,3,4,6\}$. Then there are $c_1, c_2 \in C_2$ so that $c_1 c_2^{-1} \equiv m_1 m_2 \equiv n \pmod{7^r}$. Lemma 2.3 ensures that $R(C_2)$ is dense in $\mathbb{Q}_7$.

(c) There are two cases to consider: (c1) $n \geqslant 4$; (c2) $n = 3$ and $p = 3$.

(c1) Almost every natural number, in the sense of natural density, is the sum of four cubes [9]. For each prime power p^r and each $n \in \mathbb{N}$, the congruence $x \equiv n \pmod{p^r}$ must have a solution with $x \in C_4$ since otherwise the natural density of C_4 would be at most $1 - 1/p^r$. Lemma 2.3 ensures that $R(C_4)$ is dense in $\mathbb{Q}_p$.

(c2) Modulo 9, the set of cubes is $\{0,1,8\}$; modulo 9, the set of sums of three cubes is $\{0,1,2,3,6,7,8\}$. Since $4\cdot 7 \equiv 5 \cdot 2 \equiv 1 \pmod 9$, each element of $\{1,4,5,8\}$ is the inverse, modulo 9, of a residue class that is the sum of three cubes.

A lifting argument similar to that used in the proof of (b3) confirms that whenever $m \equiv 0,1,2,3,6,7,8 \pmod 9$, the congruence $x^3+y^3+z^3 \equiv m \pmod{3^r}$ has a solution with $3 \nmid x$ for all $r \geqslant 2$. Thus, whenever $m \equiv 1,4,5,8 \pmod 9$, the congruence $(x^3+y^3+z^3)^{-1} \equiv m \pmod{3^r}$ has a solution with $3\nmid x$ for all $r \geqslant 2$.

Each residue class modulo 9 is the product of an element in $\{0,1,2,3,6,7,8\}$ and an element of $\{1,4,5,8\}$. Given a natural number n and $r \geqslant 2$, write $n \equiv m_1 m_2 \pmod{3^r}$, in which m_1 modulo 9 is in $\{0,1,2,3,6,7,8\}$ and m_2 modulo 9 is in $\{1,4,5,8\}$. Then there are $c_1, c_2 \in C_3$ so that $c_1 c_2^{-1} \equiv m_1 m_2 \equiv n \pmod{3^r}$. Lemma 2.3 ensures that $R(C_2)$ is dense in $\mathbb{Q}_3$. $\square$

We close this section with a couple open problems. In light of Theorems 4.1 and 4.2, the following question is the next logical step.

Problem. What about sums of fourth powers? Fifth powers?

Turning in a different direction, instead of sums of squares one might consider quadratic forms. Cubic and biquadratic forms might also eventually be considered.

Problem. Let Q be a quadratic form and let $A = \{a \in \mathbb{N} : Q \text{ represents } a\}$. For which primes p is $R(A)$ dense in $\mathbb{Q}_p$?

5. Second-order recurrences

The main result of [13] is that the set of quotients of Fibonacci numbers is dense in $\mathbb{Q}_p$ for all p. The proof employed a small amount of algebraic number theory and some relatively obscure results about Fibonacci numbers. The primes $p = 2$ and $p = 5$ required separate treatment. In this section, we establish a result for certain second-order recurrences that includes the Fibonacci result as a special case. We unapologetically use the language of algebraic number theory.

We require Euler's theorem for ideals. Let $\mathbb{K}$ be a number field with ring of integers $\mathcal{O}_{\mathbb{K}}$. If $\mathfrak{i}$ is a nonzero ideal in $\mathcal{O}_{\mathbb{K}}$ and $\alpha \in \mathcal{O}_{\mathbb{K}}$ is relatively prime to $\mathfrak{i}$, then

$$\alpha^{\Phi(\mathfrak{i})} \equiv 1 \pmod{\mathfrak{i}}, \tag{5.1}$$

in which

$$\Phi(\mathfrak{i}) = N(\mathfrak{i}) \prod_{\mathfrak{q}|\mathfrak{i}} \Big(1 - \frac{1}{N(\mathfrak{q})}\Big)$$

is the Euler totient function for ideals. In the preceding, $N(\cdot)$ denotes the norm of an ideals; the product runs over all distinct prime ideals $\mathfrak{q}$ that divide $\mathfrak{i}$.

Theorem 5.2. *Let r and s be nonzero integers with*

$$r^2 \notin \{-s, -2s, -3s, -4s\}, \tag{5.3}$$

let $(a_n)_{n\geqslant 0}$ be defined by[1]

$$a_0 = 0, \qquad a_1 = 1, \qquad a_{n+2} = ra_{n+1} + sa_n, \tag{5.4}$$

and let $A = \{a_n : n \geqslant 1\}$.

(a) If $p|s$ and $p\nmid r$, then $R(A)$ is not dense in $\mathbb{Q}_p$.[2]

(b) If $p\nmid s$, then $R(A)$ is dense in $\mathbb{Q}_p$.

Proof. (a) If $p|s$ and $p\nmid r$, then induction confirms that $a_n \equiv r^{n-1} \pmod{p}$ so that $\nu_p(a_n) = 0$ for $n \geqslant 0$. Thus, $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1.

(b) Suppose that $p \nmid s$. The characteristic polynomial of the recurrence (5.4) is $x^2 - rx - s$. It is monic and has integer coefficients, so its roots

$$\alpha = \frac{r + \sqrt{r^2+4s}}{2} \quad \text{and} \quad \beta = \frac{r - \sqrt{r^2+4s}}{2} \tag{5.5}$$

are algebraic integers. They satisfy

$$\alpha + \beta = r \quad \text{and} \quad \alpha\beta = -s. \tag{5.6}$$

Since $s \neq 0$, both α and β are nonzero; since $r^2+4s \neq 0$, they are distinct. Regard α and β as elements of the ring $\mathcal{O}_{\mathbb{K}}$ of algebraic integers in the field $\mathbb{K} = \mathbb{Q}(\sqrt{r^2+4s})$, in which it is understood that $\mathbb{K} = \mathbb{Q}$ and $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}$ if r^2+4s is a perfect square. The initial conditions (5.4) and the integrality of r and s ensure that

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{5.7}$$

and that a_n is an integer for $n \geqslant 0$.

We claim that $a_n \neq 0$ for all $n \geqslant 1$. In light of (5.7), it suffices to show that α/β is not a root of unity. Suppose toward a contradiction that

$$\frac{\alpha}{\beta} = \frac{r + \sqrt{r^2+4s}}{r - \sqrt{r^2+4s}} = \frac{r^2 + 2s + r\sqrt{r^2+4s}}{-2s} \tag{5.8}$$

is a primitive nth root of unity. Then the degree of α/β is $\Phi(n)$, in which Φ denotes the Euler totient function; this is the degree of the nth cyclotomic polynomial Φ_n.

---

[1]The condition (5.3) ultimately ensures that $a_n \neq 0$ for $n \geqslant 1$. There is no loss of generality in assuming that $r, s \neq 0$. If $r = 0$, we obtain the sequence $0, 1, 0, s, 0, s^2, \ldots$. Even if we disregard the 0 terms, Lemma 2.2 ensures that $R(A)$ is dense in no $\mathbb{Q}_p$. If $s = 0$, then (5.4) is inconsistent.

[2]If $p|s$ and $p|r$, then anything can happen. See the remarks after the proof.

Since $\alpha/\beta \in \mathbb{K}$, which is either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$, we have $\Phi(n) \leqslant 2$. Consequently, $n \in \{1, 2, 3, 4, 6\}$. We show that each case leads to a contradiction.

(a) If $n = 1$, then $\alpha = \beta$ and (5.5) implies that $r^2 = -4s$, in violation of (5.3).

(b) If $n = 2$, then $\alpha = -\beta$ and (5.6) implies that $r = 0$, a contradiction.

(c) If $n = 3$, then α/β is a root of $\Phi_3(x) = x^2 + x + 1$; these are $(-1 \pm i\sqrt{3})/2$. Then (5.8) and a computation ensure that $r^2 = -s$, which contradicts (5.3).

(d) If $n = 4$, then α/β is a root of $\Phi_4(x) = x^2 + 1$; these are $\pm i$. Then (5.8) and a computation ensure that $r^2 = -2s$, which contradicts (5.3).

(e) If $n = 6$, then α/β is a root of $\Phi_6(x) = x^2 - x + 1$; these are $(1 \pm i\sqrt{3})/2$. Then (5.8) and a computation ensure that $r^2 = -3s$, which contradicts (5.3).

Recall that p is a rational prime that does not divide $s = -\alpha\beta$. If $\mathfrak{p} = p\mathcal{O}_{\mathbb{K}}$ denotes the ideal in $\mathcal{O}_{\mathbb{K}}$ generated by p, then $\alpha, \beta \notin \mathfrak{p}$; that is, α and β are relatively prime to $\mathfrak{p}$. Let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}_{\mathbb{K}}$ that divides $\mathfrak{p}$. Then $\mathfrak{q}^2$ might divide $\mathfrak{p}$, but higher powers of $\mathfrak{q}$ cannot since $\mathbb{K}$ is at worst a quadratic extension of $\mathbb{Q}$. Euler's theorem for ideals ensures that

$$\alpha^{\Phi(\mathfrak{p}^{2j})} \equiv \beta^{\Phi(\mathfrak{p}^{2j})} \equiv 1 \pmod{\mathfrak{p}^{2j}}$$

for all $j \geqslant 1$ and hence

$$\alpha^{\Phi(\mathfrak{p}^{2j})} \equiv \beta^{\Phi(\mathfrak{p}^{2j})} \equiv 1 \pmod{\mathfrak{q}^{2j}}.$$

Since a_n is nonzero for $n \neq 0$, for each $m \in \mathbb{N}$ we have

$$\begin{aligned} \frac{a_{\Phi(\mathfrak{p}^{2j})m}}{a_{\Phi(\mathfrak{p}^{2j})}} &= \frac{\alpha^{\Phi(\mathfrak{p}^{2j})m} - \beta^{\Phi(\mathfrak{p}^{2j})m}}{\alpha^{\Phi(\mathfrak{p}^{2j})} - \beta^{\Phi(\mathfrak{p}^{2j})}} \\ &= (\alpha^{\Phi(\mathfrak{p}^{2j})})^{m-1} + (\alpha^{\Phi(\mathfrak{p}^{2j})})^{m-2}(\beta^{\Phi(\mathfrak{p}^{2j})}) + \cdots + (\beta^{\Phi(\mathfrak{p}^{2j})})^{m-1} \\ &\equiv m \pmod{\mathfrak{q}^{2j}} \end{aligned} \tag{5.9}$$

and hence

$$\frac{a_{\Phi(\mathfrak{p}^{2j})m}}{a_{\Phi(\mathfrak{p}^{2j})}} \equiv m \pmod{\mathfrak{p}^{j}}. \tag{5.10}$$

Since the rational number $a_{\Phi(\mathfrak{p}^{2j})m}/a_{\Phi(\mathfrak{p}^{2j})}$ belongs to $\mathcal{O}_{\mathbb{K}}$ by (5.9) it is a rational integer. Then (5.10) tells us that the rational number $(a_{\Phi(\mathfrak{p}^{2j})m}/a_{\Phi(\mathfrak{p}^{2j})} - m)/p^j$ is an algebraic integer and hence a rational integer. Thus,

$$\frac{a_{\Phi(\mathfrak{p}^{2j})m}}{a_{\Phi(\mathfrak{p}^{2j})}} \equiv m \pmod{p^{j}}. \tag{5.11}$$

Since $m \in \mathbb{N}$ was arbitrary, Lemma 2.3 ensures that $R(A)$ is dense in $\mathbb{Q}_p$. $\square$

The preceding theorem is sharp in the following sense: if $p|s$ and $p|r$, then $R(A)$ may or may not be dense in $\mathbb{Q}_p$. Consider the following examples.

Example 5.12. Let $p = 3$, $r = 15$, and $s = -54$; note that $p|s$ and $p|r$. Then $\alpha = 9$ and $\beta = 6$, so

$$a_n = \frac{9^n - 6^n}{9 - 6} = 3^{n-1}(3^n - 2^n).$$

We claim that $R(A)$ is not dense in $\mathbb{Q}_3$. Since $\nu_3(3) = 1$ and $\nu_3(a_m/a_n) = (m - 1) - (n - 1) = m - n$ for $m, n \geqslant 0$, any element of $R(A)$ that is sufficiently close to

3 in $\mathbb{Q}_3$ must be of the form a_{n+1}/a_n for some $n \geqslant 1$. However,

$$\begin{aligned}
\nu_3\Big(\frac{a_{n+1}}{a_n} - 3\Big) &= \nu_3\Big(\frac{3^n(3^{n+1}-2^{n+1})}{3^{n-1}(3^n-2^n)} - 3\Big) = 1 + \nu_3\Big(\frac{3^{n+1}-2^{n+1}}{3^n-2^n} - 1\Big)\\
&= 1 + \nu_3(3^{n+1} - 2^{n+1} - 3^n + 2^n) = 1 + \nu_3\Big(3^n(3-1) - 2^n(2-1)\Big)\\
&= 1 + \nu_3\Big(2\cdot 3^n - 2^n\Big) = 1 + \nu_3\Big(3^n - 2^{n-1}\Big) = 1,
\end{aligned}$$

so $R(A)$ is bounded away from 3 in $\mathbb{Q}_3$.

Example 5.13. Let $p=5$, $r=20$, and $s=-75$; note that $p|s$ and $p|r$. Then $\alpha = 15$ and $\beta = 5$, so

$$a_n = \frac{15^n - 5^n}{15-5} = 5^{n-1}\frac{3^n-1}{2}.$$

We claim that $R(A)$ is dense in $\mathbb{Q}_5$. Let $N \in \mathbb{N}$ be given and write $N = 5^t N_0$, in which $5\nmid N_0$. Let $r \geqslant t$ be large and so that $r \not\equiv t-1 \pmod 4$. Since $\phi(5^{r+1}) = 4\cdot 5^r$, Euler's theorem permits us to write

$$3^{4\cdot 5^r} - 1 = 5^{r+1}\ell, \qquad 5\nmid \ell. \tag{5.14}$$

Let $m \geqslant 1$ satisfy

$$m \equiv \ell^{-1}N_0(3^{r-t+1}-1) \pmod{5^{r+1}}; \tag{5.15}$$

Euler's theorem ensures that $5\nmid m$ since $4\nmid(r-t+1)$. If $n = 4\cdot 5^r m$, then

$$\begin{aligned}
&(3^{n+r-t+1}-1)\frac{a_n}{a_{n+r-t+1}}\\
&\quad = 5^{n-1}\Big(\frac{3^n-1}{2}\Big)\Big(\frac{2}{5^{n+r-t}}\Big)\\
&\quad = 5^{-r+t-1}(3^{4\cdot 5^r m}-1)\\
&\quad = 5^t\Big(\frac{3^{4\cdot 5^r m}-1}{3^{4\cdot 5^r}-1}\Big)\Big(\frac{3^{4\cdot 5^r}-1}{5^{r+1}}\Big)\\
&\quad = 5^t\Big(\frac{(3^{4\cdot 5^r})^m-1}{3^{4\cdot 5^r}-1}\Big)\ell && \text{(by (5.14))}\\
&\quad = 5^t\big((3^{4\cdot 5^r})^{m-1} + (3^{4\cdot 5^r})^{m-2} + \cdots + 1\big)\ell\\
&\quad \equiv 5^t m\ell \pmod{5^{r+1}} && \text{(since } \phi(5^{r+1}) = 4\cdot 5^r)\\
&\quad \equiv 5^t N_0(3^{r-t+1}-1) \pmod{5^{r+1}} && \text{(by (5.15))}\\
&\quad \equiv N(3^{r-t+1}-1) \pmod{5^{r+1}} && \text{(since } N = 5^t N_0)\\
&\quad \equiv N(3^{n+r-t+1}-1) \pmod{5^{r+1}} && \text{(since } \phi(5^{r+1})|n).
\end{aligned}$$

Since $4|n$ and $4\nmid(r-t+1)$, it follows that $5\nmid(3^{n+r-t+1}-1)$ and hence

$$\nu_5\Big(\frac{a_n}{a_{n+r-t+1}} - N\Big) \geqslant r+1.$$

Thus, $R(A)$ is 5-adically dense in $\mathbb{N}$, so it is dense in $\mathbb{Q}_5$ by Lemma 2.3.

Where do the preceding two examples leave us? Suppose that $p|s$ and $p|r$. Then $d = (r,s)$ is divisible by p. Induction confirms that $d^{\lfloor n/2\rfloor}$ divides a_n for $n \geqslant 0$. To be more specific,

$$a_n = \sum_{k=0}^{n-1}\binom{n-1-k}{k} r^{\max\{n-1-2k,0\}} s^{\max\{\lfloor\frac{2k+1}{2}\rfloor,0\}}$$

and hence it is difficult to precisely evaluate $\nu_p(a_n)$. Consequently, we are unable at this time to completely characterize when $R(A)$ is dense in $\mathbb{Q}_p$ if $p|s$ and $p|r$. However, in most instances, ad hoc arguments can handle these situations. Consider the following examples.

Example 5.16. The integer sequence

$$0,\ 1,\ 2,\ -1,\ -12,\ -19,\ 22,\ 139,\ 168,\ -359,\ -1558,\ -1321,\ 5148,\ldots$$

is generated by the recurrence

$$a_0 = 0, \qquad a_1 = 1, \qquad a_{n+2} = 2a_{n+1} - 5a_n, \quad n \geqslant 0.$$

In this case, $\alpha = 1 + 2i$ and $\beta = 1 - 2i$ are nonreal. Let $A = \{a_n : n \geqslant 1\}$ and confirm by induction that $5 \nmid a_n$ for all $n \geqslant 1$. Apply Lemma 2.1 and Theorem 5.2 to see that $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 5$.

Example 5.17. Let b be an integer not equal to ± 1 and consider the sequence $a_n = b^n - 1$, which is generated by

$$a_0 = 0, \qquad a_1 = b - 1, \qquad a_{n+2} = (b + 1)a_{n+1} - ba_n.$$

Apply Theorem 5.2 with $r = b + 1$ and $s = -b$ to the set $A = \{a_n : n \geqslant 1\}$ andconclude that $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p \nmid b$. For instance, the set $\{1, 3, 7, 15, 31, \ldots\}$ is dense in $\mathbb{Q}_p$ if and only if $p \neq 2$.

6. Sequences of the form $b^n + 1$

The preceding example prompts an immediate follow-up question. Suppose that $b \neq \pm 1$ and consider the set $A = \{b^n + 1 : n \geqslant 0\}$. For which p is $R(A)$ dense in $\mathbb{Q}_p$? Unfortunately, Theorem 5.2 does not apply here since the sequence $1, b+1, b^2+1, \ldots$ which defines A does not satisfy the initial conditions in (5.4). This is indeed a difficulty since the initial conditions guarantee that the sequences considered in Theorem 5.2 enjoy the special representation (5.7). Fortunately, the main idea used in the second half of the proof of Theorem 5.2 still applies. It is the setup that requires a totally different approach. We require a "lifting the exponent" lemma, familiar to mathematics contest participants.

Lemma 6.1. *Let x, y be nonzero integers with $x + y \neq 0$, let n be odd, let p be an odd prime such that $p|(x + y)$, $p \nmid x$, and $p \nmid y$. Then*

$$\nu_p(x^n + y^n) = \nu_p(x + y) + \nu_p(n). \tag{6.2}$$

We omit the proof of the lemma since it is well known and can be found on many websites devoted to problem solving. Although one can find countless proofs and applications of this lemma by conducting a web search for "lifting the exponent", we are strangely unable to locate a proof in a standard number theory textbook.

Theorem 6.3. *Let $b \neq \pm 1$, let $A = \{b^n + 1 : n \geqslant 0\}$, and let p be an odd prime.*

(a) $R(A)$ is not dense in $\mathbb{Q}_2$.

(b) $R(A)$ is dense in $\mathbb{Q}_p$ if and only if $p|(b^n + 1)$ for some n.

Proof. (a) If b is even, then $\nu_2(b^n + 1) = 0$ for $n \geqslant 0$ so $R(A)$ is not dense in $\mathbb{Q}_2$ by Lemma 2.1. If $b \equiv 1 \pmod 4$, then $b^n + 1 \equiv 2 \pmod 4$ for $n \geqslant 0$. Since

$\nu_2(b^n+1)=1$ for $n \geqslant 0$, Lemma 2.1 ensures that $R(A)$ is not dense in $\mathbb{Q}_2$. If $b \equiv 3 \pmod 4$, then

$$\nu_2(b^n+1) \equiv \begin{cases} 1 \text{ or } 2 \pmod 4 & \text{if } b \equiv 3, 11 \pmod{16}, \\ 1 \text{ or } 3 \pmod 4 & \text{if } b \equiv 7 \pmod{16}, \\ 0 \text{ or } 1 \pmod 4 & \text{if } b \equiv 15 \pmod{16}, \end{cases}$$

for $n \geqslant 0$. This implies that for $i,j \geqslant 0$,

$$\nu_2\Big(\frac{b^i+1}{b^j+1}\Big) = \nu_2(b^i+1) - \nu_2(b^j+1) \equiv \begin{cases} 0,1,3 \pmod 4 & \text{if } b \equiv 3, 11, 15 \pmod{16}, \\ 0,2 \pmod 4 & \text{if } b \equiv 7 \pmod{16}. \end{cases}$$

Thus, $R(A)$ is not dense in $\mathbb{Q}_2$ by Lemma 2.1.

(b) ($\Rightarrow$) We prove the contrapositive. If $p \nmid (b^n+1)$ for all n, then $\nu_p(b^n+1)=0$ for all n. Then $R(A)$ is not dense in $\mathbb{Q}_p$ by Lemma 2.1.

($\Leftarrow$) Suppose that p is an odd prime that divides b^k+1 for some $k \geqslant 1$. For odd m, let $r \geqslant 1$, $x=b^k$, $y=1$, and $n=mp^r$ in Lemma 6.2 and obtain

$$\nu_p(b^{mkp^r}+1) = \nu_p(b^k+1) + \nu_p(mp^r) \geqslant r.$$

Consequently, $b^{mkp^r} \equiv -1 \pmod{p^r}$ for $r \geqslant 1$ and hence

$$\begin{aligned} \frac{b^{mkp^r}+1}{b^{kp^r}+1} &= \frac{b^{mkp^r}-(-1)^{mkp^r}}{b^{kp^r}-(-1)^{kp^r}} \\ &= \frac{(b^{kp^r})^m - ((-1)^{kp^r})^m}{b^{kp^r}-(-1)^{kp^r}} \\ &= (b^{kp^r})^{m-1} - (b^{kp^r})^{m-2} + \cdots + ((-1)^{kp^r})^{m-1} \\ &\equiv (-1)^{m-1} - (-1)^{m-2} - \cdots (-1)^{m-1} \pmod{p^r} \\ &\equiv m \pmod{p^r} \end{aligned}$$

since m is odd. As m runs over the odd numbers, it produces a complete set of residue classes modulo p^r. Thus, $R(A)$ is p-adically dense in $\mathbb{N}$; Lemma 2.3 ensures that $R(A)$ is dense in $\mathbb{Q}_p$. $\square$

If $b \geqslant 3$ is squarefree, then the set of primes p for which $p|(b^n+1)$ for some $n \geqslant 0$ has relative density $2/3$ as a subset of the primes [18]. That is,

$$\lim_{x\to\infty} \frac{|\{p \leqslant x : p \text{ is prime and } p|(b^n+1) \text{ for some } n \geqslant 0\}|}{2x/3\log x} = 1.$$

If $b=2$, then relative density is $17/24$ instead [18]. In all of these cases, the set $\{b^n+1 : n \geqslant 0\}$ is dense in $\mathbb{Q}_p$ for infinitely many p.

7. Fibonacci and Lucas numbers

The Fibonacci numbers $0,1,1,2,3,5,8,13,21,\ldots$ are generated by the recurrence

$$F_0 = 0, \qquad F_1 = 1, \qquad F_{n+2} = F_{n+1} + F_n, \quad n \geqslant 0.$$

Apply Theorem 5.2 with $r=s=1$ to the set $F=\{F_n : n \geqslant 1\}$ and conclude that $R(F)$ is dense in $\mathbb{Q}_p$ for all p. This is the main result of [13]:[3]

[3] On a related note, a *Fibonacci integer* is an integer that is a ratio of products of Fibonacci numbers. For every $\epsilon > 0$, the counting function for the Fibonacci integers is $\exp(c(\log x)^{1/2} + O((\log x)^{1/6}+\epsilon))$, in which c is explicit constant [25].

Corollary 7.1. *The set of quotients of Fibonacci numbers is dense in each* $\mathbb{Q}_p$.

A simpler proof is available if $p = 3$ or $p = 5$. It is known that the Fibonacci numbers modulo m produce a complete system of residues modulo if and only if m has one of the following forms:

$$5^k, \quad 2 \cdot 5^k, \quad 4 \cdot 5^k, \quad 3^j \cdot 5^k, \quad 6 \cdot 5^k, \quad 7 \cdot 5^k, \quad 14 \cdot 5^k, \quad j \geqslant 1,\, k \geqslant 0;$$

see [8]. As a consequence, $R(F)$ is dense in $\mathbb{Q}_3$ and $\mathbb{Q}_5$. In particular, the density of $R(F)$ in $\mathbb{Q}_p$ for $p \neq 3, 5$ is not simply due to the p-adic density of F in $\mathbb{N}$.

The Lucas numbers $2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, \ldots$ obey the same recurrence as the Fibonacci numbers, but with different initial conditions:

$$L_0 = 2, \qquad L_1 = 1, \qquad L_{n+2} = L_{n+1} + L_n, \quad n \geqslant 0.$$

Since the initial term is nonzero, Theorem 5.2 no longer applies. Modulo m, the Lucas numbers contain a complete system of residues if and only if m is one of the following numbers:

$$2, \quad 4, \quad 6, \quad 7, \quad 14, \quad 3^j, \quad j \geqslant 1;$$

see [35]. Consequently, the set of quotients of Lucas numbers is dense in $\mathbb{Q}_3$. We can do better by suitably adapting the proof of Theorem 6.3.

Theorem 7.2. *Let* $L = \{L_n : n \geqslant 0\}$ *denote the set of Lucas numbers and let* $p \neq 5$ *be an odd prime.*

(a) $R(L)$ *is not dense in* $\mathbb{Q}_2$ *and* $\mathbb{Q}_5$.

(b) $R(L)$ *is dense in* $\mathbb{Q}_p$ *if and only if* $p | L_n$ *for some* $n \geqslant 0$.

Proof. (a) If $F_n \geqslant 5$, then no Lucas number is divisible by F_n [39]. Since $F_5 = 5$ and $F_6 = 8$, we conclude that $\nu_5(L_n) = 0$ and $\nu_2(L_n) \leqslant 3$ for all n. Thus, $R(L)$ is not dense in $\mathbb{Q}_2$ or $\mathbb{Q}_5$.

(b) ($\Rightarrow$) We prove the contrapositive. If $p \nmid L_n$ for all $n \geqslant 0$, then $\nu_p(L_n) = 0$ for all $n \geqslant 0$. Thus, $R(L)$ is not dense in $\mathbb{Q}_p$.

($\Leftarrow$) Suppose that $p \neq 5$ is an odd rational prime that divides L_n for some $n \geqslant 0$. Then $L_n = \alpha^n + \beta^n$, in which $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$ are units in the ring $\mathcal{O}_{\mathbb{K}}$ of algebraic integers in $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Let $\mathfrak{p} = p\mathcal{O}_{\mathbb{K}}$ denote the ideal in $\mathcal{O}_{\mathbb{K}}$ generated by p. Since $p | L_n$ in $\mathbb{Z}$, we have $\alpha^n = -\beta^n \pmod{\mathfrak{p}}$. Since $\mathbb{K}$ is a unique factorization domain, a straightforward generalization of Lemma 6.1 applies and

$$\nu_{\mathfrak{q}}(\alpha^{np^r} + \beta^{np^r}) = \nu_{\mathfrak{q}}(\alpha^n + \beta^n) + \nu_{\mathfrak{q}}(p^r) \geqslant r$$

for each prime $\mathfrak{q}$ in $\mathcal{O}_{\mathbb{K}}$ that divides $\mathfrak{p}$. The discriminant of $\mathbb{K}$ is 5, so the only rational prime in $\mathcal{O}_{\mathbb{K}}$ that ramifies is 5. Thus, $\mathfrak{p}$ is either inert or the product of two distinct prime ideals. Consequently,

$$\alpha^{np^r} \equiv -\beta^{np^r} \pmod{\mathfrak{p}^r} \tag{7.3}$$

and hence

$$\alpha^{4np^r} = (\alpha^{np^r})^2 (\alpha^{np^r})^2 \equiv (\alpha^{np^r})^2 (-\beta^{np^r})^2 \equiv (\alpha\beta)^{2np^r} \equiv 1 \pmod{\mathfrak{p}^r} \tag{7.4}$$

because $\alpha\beta = -1$. Given $m \in \mathbb{N}$ and $r \geqslant 1$, the Chinese Remainder Theorem provides a natural number ℓ so that $\ell \equiv m \pmod{p^r}$ and $\ell \equiv 1 \pmod{4}$. Since ℓ is odd and congruent to 1 modulo 4, we conclude from (7.3) and (7.4) that

$$\frac{L_{\ell np^r}}{L_{np^r}} = \frac{\alpha^{\ell np^r} + \beta^{\ell np^r}}{\alpha^{np^r} + \beta^{np^r}} = \frac{(\alpha^{np^r})^\ell - (-\beta^{np^r})^\ell}{\alpha^{np^r} - (-\beta^{np^r})} \tag{7.5}$$

$$
\begin{aligned}
&= (\alpha^{np^r})^{\ell-1} + (\alpha^{np^r})^{\ell-2}(-\beta^{np^r}) + \cdots + (-\beta^{np^r})^{\ell-1} \qquad (7.6)\\
&\equiv \ell(\alpha^{np^r})^{\ell-1} \pmod{\mathfrak{p}^r}\\
&\equiv \ell \pmod{\mathfrak{p}^r}.
\end{aligned}
$$

The rational number $L_{\ell np^r}/L_{np^r}$ is an algebraic integer by (7.6), so it is an integer. Since it is congruent to the natural number ℓ modulo $\mathfrak{p}^r$, we have

$$\frac{L_{\ell np^r}}{L_{np^r}} \equiv \ell \pmod{p^r} \equiv m \pmod{p^r}.$$

Since m was arbitrarily, Lemma 2.3 ensures that $R(L)$ is dense in $\mathbb{Q}_p$. □

The set of primes that divide some a Lucas number L_n has relative density $2/3$ as a subset of the primes [23]; see [1] for more information about these types of results. In particular, $R(L)$ is dense in $\mathbb{Q}_p$ more often than not.

It is worth remarking on the modifications involved in the proof of Theorem 7.2. Euler's theorem for ideals ensures that $\alpha^{\Phi(\mathfrak{p})} \equiv \beta^{\Phi(\mathfrak{p})} \equiv 1 \pmod{\mathfrak{p}}$ since α and β are units in $\mathcal{O}_{\mathbb{K}}$. If $\mathfrak{p}$ is inert, then $\Phi(\mathfrak{p}) = p^2 - 1$; if $\mathfrak{p}$ is the product of two distinct prime ideals, then $\Phi(\mathfrak{p}) = p - 1$. In both cases, $\Phi(\mathfrak{p})$ is even. This prevents the proof of Theorem 5.2 from going through in this case since (7.5) requires an odd exponent. Instead, we used the relation $\alpha\beta = -1$ in to obtain a viable replacement (7.4) for Euler's theorem. Because the exponent in (7.4) is even, we required the Chinese Remainer Theorem to replace it with a suitable odd exponent.

8. Unions of geometric progressions

The ratio set of $A = \{2^n : n \in \mathbb{N}\} \cup \{3^n : n \in \mathbb{N}\}$ is dense in $\mathbb{R}_+$ [3, Prop. 6]. The argument relies upon the irrationality of $\log_2 3$ and the inhomogeneous form of Kronecker's approximation theorem [17, Thm. 440]. We consider such sets in the p-adic setting, restricting our attention to prime bases. The reader should have no difficulty stating the appropriate generalizations if they are desired.

An integer g is called a *primitive root modulo m* if g is a generator of the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$. Gauss proved that primitive roots exist only for the moduli 2, 4, p^k, and $2p^k$, in which p is an odd prime [28, Thm. 2.41]. Consequently, our arguments here tend to focus on odd primes.

Theorem 8.1. *Let p be an odd prime, let b be a nonzero integer, and let*

$$A = \{p^j : j \geqslant 0\} \cup \{b^j : j \geqslant 0\}.$$

Then $R(A)$ is dense in $\mathbb{Q}_p$ if and only if b is a primitive root modulo p^2.

Proof. ($\Rightarrow$) Suppose that $R(A)$ is dense in $\mathbb{Q}_p$. We first claim that b is a primitive root modulo p. If not, then there is an $m \in \{2, 3, \ldots, p-1\}$ so that $b^j \not\equiv m \pmod{p}$ for all $j \in \mathbb{Z}$. Then $R(A)$ is bounded away from m in $\mathbb{Q}_p$, a contradiction. Thus, b must be a primitive root modulo p.

Suppose toward a contradiction that b is not a primitive root modulo p^2. Since b is a primitive root modulo p, the order of b modulo p^2 is at least $p-1$. On the other hand, the order must divide $\Phi(p^2) = p(p-1)$. Since p is prime, it follows that the order of b modulo p^2 must be exactly $p-1$. Thus, $b^{p-1} \equiv 1 \pmod{p^2}$.

If $b^n \equiv p+1 \pmod{p^2}$, then $b^n \equiv 1 \pmod{p}$ and hence n is a multiple of $p-1$. Then $b^n \equiv 1 \pmod{p^2}$, a contradiction. Thus, $R(A)$ is bounded away from $p+1$ in $\mathbb{Q}_p$. This contradiction shows that b must be a primitive root modulo p^2.

($\Leftarrow$) Let $r \geqslant 1$ and let $n = p^k m \in \mathbb{N}$, in which $p \nmid m$. Since b is a primitive root modulo p^2 it is a primitive root modulo $p^3, p^4, \ldots$ [28, Thm. 2.40], so there is a j such that $b^j m \equiv 1 \pmod{p^r}$. Thus,

$$\nu_p\Big(n - \frac{p^k}{b^j}\Big) = k + \nu_p\Big(m - \frac{1}{b^j}\Big) \geqslant \nu_p(b^j m - 1) \geqslant r,$$

so $R(A)$ is dense in $\mathbb{Q}_p$ by Lemma 2.3. □

A primitive root modulo p is not necessarily a primitive root modulo p^2. For instance, 1 is a primitive root modulo 2, but not modulo 4. A less trivial example is furnished by $p = 29$, for which 14 is a primitive root modulo p, but not modulo p^2. Similarly, if $p = 37$, then 18 is a primitive root modulo p, but not modulo p^2.

Example 8.2. Consider $p = 5$ and $q = 7$; note that 5 is a primitive root modulo 7 and vice versa. However, 5 is a primitive root modulo 7^2 but 7 is not a primitive root modulo 5^2. Let

$$A = \{5, 7, 25, 49, 125, 343, 625, 2401, 3125, \ldots\} = \{5^j : j \geqslant 0\} \cup \{7^j : j \geqslant 0\}.$$

Then Theorem 8.1 ensures that $R(A)$ is dense in $\mathbb{Q}_7$ but not in $\mathbb{Q}_5$.

This sort of asymmetry is not unusual. The following theorem tells us that infinitely many such pairs of primes exist. The proof is considerably more difficult than the preceding material and it requires a different collection of tools (e.g., a sieve lemma of Heath-Brown, the Brun-Titchmarsh theorem, and the Bombieri-Vinogradov theorem). Consequently, the proof of Theorem 8.3 is deferred until Section 9.

Theorem 8.3. *There exist infinitely many pairs of primes (p, q) such that p is not a primitive root modulo q and q is a primitive root modulo p^2.*

Corollary 8.4. *There are infinitely many pairs of primes (p, q) so that the ratio set of $\{p^j : j \geqslant 0\} \cup \{q^k : k \geqslant 0\}$ is dense in $\mathbb{Q}_p$ but not in $\mathbb{Q}_q$.*

Let $a \prec b$ denote "p is a primitive root modulo b." The following table shows some of the various logical possibilities (bear in mind that a primitive root modulo p^2 is automatically a primitive root modulo p).

p	q	$p \prec q$	$q \prec p$	$p \prec q^2$	$q \prec p^2$
3	5	T	T	T	T
5	7	T	T	T	F
3	7	T	F	T	F
5	11	F	F	F	F
7	19	F	T	F	F

Despite an extensive computer search, we were unable to find a pair (p, q) of primes for which $p \prec q$ and $q \prec p$, but $p \not\prec q^2$ and $q \not\prec p^2$. We hope to revisit this question in later work. For now we are content to pose the following question.

Problem. Is there a pair (p, q) of primes for which $p \prec q$ and $q \prec p$, but $p \not\prec q^2$ and $q \not\prec p^2$

On the other hand, numerical evidence and heuristic arguments suggests that there are infinitely many pairs (p, q) of primes for which $p \prec q^2$ and $q \prec p^2$. Although we have given the proof of the closely related Theorem 8.3, we feel that attempting to address more questions of this nature would draw us too far afield. Consequently, we postpone this venture until another day.

Problem. Prove that there infinitely many pairs of primes (p,q) for which $p \prec q^2$ and $q \prec p^2$?

9. Proof of Theorem 8.3

Step 1: We start with a sieve lemma due to Heath-Brown. It is a weaker version of [19, Lem. 3]. In what follows, p always denotes an odd prime. We write $(\frac{a}{p})$ for the Legendre symbol of a with respect to p and write $x \prec y$ to indicate that x is a primitive root modulo y.

Lemma 9.1 (Heath-Brown)**.** *Let q, r, s be three primes, let $k \in \{1,2,3\}$, and let u, v be positive integers such that*

(a) $16|v$,

(b) $2^k|(u-1)$,

(c) $(\frac{u-1}{2^k}, v) = 1$,

(d) if $p \equiv u \pmod{v}$, then

$$\left(\frac{-3}{p}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{s}{p}\right) = -1.$$

Then for large x, the set of primes

$$\mathcal{P}(x;u,v) = \big\{p \leqslant x \,:\, p \equiv u \pmod{v},\ (p-1)/2^k \textit{ is prime or a product of two primes, and one of } q,r,s \textit{ is primitive root modulo } p\big\}$$

has cardinality satisfying

$$|\mathcal{P}(x;u,v)| \gg \frac{x}{(\log x)^2}.$$

Consider the primes $q=7$, $r=11$, and $s=19$. Let

$$v = 70{,}224 = 16 \times 3 \times 7 \times 11 \times 19$$

and observe that $16|v$, so (a) is satisfied. Let $u = 2{,}951$ so that

$$u - 1 = 2{,}950 = 2 \times 5^2 \times 59,$$

so that (b) is satisfied with $k=1$. Then (c) is satisfied since $u-1$ and v have no common factors. If $p \equiv u \pmod{v}$, then

$$p \equiv 3 \pmod{4}, \qquad p \equiv 2 \pmod{3}, \quad \text{and} \quad p \equiv 25 \pmod{qrs}. \tag{9.2}$$

Since $q \equiv r \equiv s \equiv 3 \pmod{4}$, quadratic reciprocity ensures that q,r,s are quadratic nonresidues modulo p. For instance,

$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) = -\left(\frac{25}{p}\right) = -1 \tag{9.3}$$

and similarity if q is replaced with r or s. In addition,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$$

by (9.2) and quadratic reciprocity. Thus, (d) is satisfied.

Step 2: With $u = 2{,}951$, $v = 70{,}224$, $q = 7$, $r = 11$, and $s = 19$ as above, let

$$\mathcal{P} = \{p \equiv u \pmod{v} \,:\, \text{one of } q, r, s \text{ is a primitive root modulo } p\}$$

and let $\mathcal{P}(x) = \mathcal{P} \cap [1, x]$. Since $\mathcal{P}(x; u, v) \subseteq \mathcal{P}(x)$, Lemma 9.1 ensures that

$$|\mathcal{P}(x)| \geqslant \frac{x}{(\log x)^2}.$$

If $p \in \mathcal{P}$, then $(\frac{p}{q}) = 1$ by (9.3), so p is a quadratic residue modulo q and hence it fails to be a primitive root modulo q. Since (9.3) holds with q replaced with r or s, we conclude that p is not a primitive root modulo q, r, or s.

Step 3: The definition of $\mathcal{P}(x)$ ensures that one of the primes q, r, s is a primitive root for at least $\frac{1}{3}|\mathcal{P}(x)|$ primes $p \leqslant x$. Without loss of generality, we may assume that this prime is q since the specific numerical values of q, r, s are irrelevant in what follows (save that they are all congruent to 3 modulo 4). Let

$$\mathcal{P}_1(x) = \left\{ \frac{x}{(\log x)^2} < p \leqslant x \,:\, p \equiv u \pmod{v} \text{ and } q \prec p \right\}$$

and let $\pi(x)$ denote the number of primes at most x. Then the prime number theorem implies that

$$\begin{aligned}
|\mathcal{P}_1(x)| &\geqslant \tfrac{1}{3}|\mathcal{P}(x)| - \pi\left(\frac{x}{(\log x)^2}\right) \\
&\gg \frac{x}{(\log x)^2} - O\left(\frac{x}{(\log x)^3}\right) \\
&\gg \frac{x}{(\log x)^2}.
\end{aligned}$$

Step 4: Let $\mathcal{P}_2(x)$ be the set of $p \in \mathcal{P}_1(x)$ for which $q \prec p^2$; let $\mathcal{P}_3(x) = \mathcal{P}_1(x) \backslash \mathcal{P}_2(x)$ be the subset for which $q \not\prec p^2$. One of these two possibilities must occur at least half the time. This leads to two cases.

Step 4.a: If

$$|\mathcal{P}_2(x)| \geqslant \tfrac{1}{2}|\mathcal{P}_1(x)|, \tag{9.4}$$

then there are at least $\gg x/(\log x)^2$ pairs of primes (p, q) with $p \leqslant x$ for which $q \prec p^2$ and $p \not\prec q$.

Step 4.b: Suppose that

$$|\mathcal{P}_3(x)| \geqslant \tfrac{1}{2}|\mathcal{P}_1(x)|. \tag{9.5}$$

For $p \in \mathcal{P}_3(x)$ consider primes of the form

$$\ell = q + 4hp, \qquad h \in [1, x^{3/2} - 1] \cap \mathbb{Z}, \tag{9.6}$$

first observing that $\ell \ll x^{5/2}$. The prime number theorem for arithmetic progressions asserts that the number of such primes is $\pi(4x^{3/2}p; 4p, q) + O(1)$, in which $\pi(x; m, a)$ denotes the number of primes at most x that are congruent to $a \pmod{m}$. For such a prime ℓ, quadratic reciprocity and (9.3) ensure that

$$\left(\frac{p}{\ell}\right) = -\left(\frac{\ell}{p}\right) = -\left(\frac{q + 4hp}{p}\right) = -\left(\frac{q}{p}\right) = 1$$

since $p, q \equiv 3 \pmod{4}$. Consequently, $p \not\prec \ell$. Since

$$\begin{aligned}
\ell^{p-1} &= (q + 4hp)^{p-1} \\
&\equiv q^{p-1} + 4h(p-1)q^{p-2}p \pmod{p^2}
\end{aligned}$$

$$\equiv 1 + 4h(p-1)q^{p-2}p \pmod{p^2},$$

we see that ℓ is a primitive root modulo p^2 whenever $p \nmid h$. The Brun-Titchmarsh theorem ensures that the number of primes ℓ of the form (9.6) for which $p|h$ is

$$\pi(4x^{3/2}p; 4p^2, q) + O(1) \ll \frac{x^{3/2}p}{p^2 \log(x^{3/2}p)} \ll \frac{x^{3/2}}{p \log x}.$$

Thus, for each $p \in \mathcal{P}_3(x)$, there are

$$\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q) + O(1)$$

primes $\ell \leqslant x^{5/2}$ for which $p \not\prec \ell$ and $\ell \prec p^2$.

Step 5: Let $\mathcal{P}_4(x)$ be the subset of $\mathcal{P}_3(x)$ such that

$$\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q) \geqslant \frac{x^{3/2}}{(\log x)^2}, \tag{9.7}$$

and let $\mathcal{P}_5(x) = \mathcal{P}_3(x) \backslash \mathcal{P}_4(x)$. We intend to show that $|\mathcal{P}_5(x)|$ is small and hence that (9.7) holds for most $p \in \mathcal{P}_3(x)$. Suppose that $p \in \mathcal{P}_5(x)$; that is,

$$\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q) < \frac{x^{3/2}}{(\log x)^2}.$$

Then

$$\begin{aligned}
&\left|\pi(4x^{3/2}p; 4p; q) - \frac{\pi(4x^{3/2}p)}{\phi(4p)}\right| \\
&\qquad \geqslant \frac{\pi(4x^{3/2}p)}{\phi(4p)} - \left|\pi(4x^{3/2}p; 4p, q) - \pi(4x^{3/2}p; 4p^2, q)\right| - \pi(4x^{3/2}p; 4p^2, q) \\
&\qquad \gg \frac{x^{3/2}}{\log x} + O\left(\frac{x^{3/2}}{(\log x)^2} + \frac{x^{3/2}}{p \log x}\right) \\
&\qquad \gg \frac{x^{3/2}}{\log x}
\end{aligned}$$

because $p \geqslant x/(\log x)^2$ by the definition of $\mathcal{P}_1(x)$. Thus,

$$\max_{\substack{1 \leqslant a \leqslant 4p \\ (a,4p)=1 \\ 1 \leqslant y \leqslant 4x^{5/2}}} \left|\pi(y; 4p, a) - \frac{\pi(y)}{\phi(4p)}\right| \geqslant \left|\pi(4x^{3/2}p; 4p, q) - \frac{\pi(4x^{3/2}p)}{\phi(4p)}\right| \gg \frac{x^{3/2}}{\log x}.$$

Summing up the above inequality over all $p \in \mathcal{P}_5(x)$ and appealing to the Bombieri-Vinogradov theorem, for large x we obtain

$$\begin{aligned}
\left(\frac{x^{3/2}}{\log x}\right) |\mathcal{P}_5(x)| &\ll \sum_{p \in \mathcal{P}_5(x)} \max_{\substack{1 \leqslant a \leqslant 4p \\ (a,4p)=1 \\ 1 \leqslant y \leqslant 4x^{5/2}}} \left|\pi(y; 4p, a) - \frac{\pi(y)}{\phi(4p)}\right| \\
&\ll \sum_{m \leqslant 4x} \max_{\substack{1 \leqslant a \leqslant m: \\ (a,m)=1 \\ y \leqslant x^{5/2}}} \left|\pi(y; m, a) - \frac{\pi(y)}{\phi(m)}\right| \\
&\ll x^{5/2}/(\log x)^4.
\end{aligned}$$

Thus,

$$|\mathcal{P}_5(x)| \ll \frac{x}{(\log x)^3}$$

and hence

$$|\mathcal{P}_4(x)| = |\mathcal{P}_3(x)| - |\mathcal{P}_5(x)| \geqslant \tfrac{1}{2}|\mathcal{P}_3(x)| \gg \frac{x}{(\log x)^2}$$

when (9.5) holds and x is sufficiently large. Comparing this with (9.7), we conclude that the number of pairs (p,ℓ) with $p \not\prec \ell$ and $\ell \prec p^2$ and $p < \ell \leqslant 4x^{5/2}$ is

$$\gg \left(\frac{x^{3/2}}{(\log x)^2}\right)\left(\frac{x}{(\log x)^2}\right) \gg \frac{x^{5/2}}{(\log x)^4}. \tag{9.8}$$

Step 6. If (9.4) holds, then the number of pairs (p,q) for which $p \in \mathcal{P}_1(x)$, $q \prec p^2$, and $p \not\prec q$ is $\gg x/(\log x)^2$, which is dominated by (9.8) for large x. For such p we have $\max\{p,q\} \leqslant x < 4x^{5/2}$. If $y = 4x^{5/2}$ is sufficiently large, then the number of pairs of primes (p,q) with $\max\{p,q\} \leqslant y$ and for which $p \not\prec q$ and $q \prec p^2$ is

$$\gg \frac{x}{(\log x)^2} \gg \frac{y^{2/5}}{(\log y)^2}.$$

This completes the proof of Theorem 8.3. □

Remark. A more careful application of the Bombieri-Vinogradov theorem shows that this count can be improved to $y^{1/2-\varepsilon}$ for any $\varepsilon > 0$ fixed (just replace the range for h in (9.6) $x^{3/2}$ by $x^{1+\varepsilon}$), or even to $y^{1/2}/(\log y)^A$ for some constant $A > 0$, but we do not get into such details.

References

1. Christian Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, viii+102. MR 1257079
2. Kevin A. Broughan, *Characterizing the sum of two cubes*, J. Integer Seq. **6** (2003), no. 4, Article 03.4.6, 7. MR 2051960
3. Bryan Brown, Michael Dairyko, Stephan Ramon Garcia, Bob Lutz, and Michael Someck, *Four quotient set gems*, Amer. Math. Monthly **121** (2014), no. 7, 590–599. MR 3229105
4. J. Bukor, P. Erdős, T. Šalát, and J. T. Tóth, *Remarks on the (R)-density of sets of numbers. II*, Math. Slovaca **47** (1997), no. 5, 517–526. MR 1635220 (99e:11013)
5. Jozef Bukor, Tibor Šalát, and János T. Tóth, *Remarks on R-density of sets of numbers*, Tatra Mt. Math. Publ. **11** (1997), 159–165, Number theory (Liptovský Ján, 1995). MR 1475512 (98e:11012)
6. József Bukor and Peter Csiba, *On estimations of dispersion of ratio block sequences*, Math. Slovaca **59** (2009), no. 3, 283–290. MR 2505807
7. József Bukor and János T. Tóth, *On accumulation points of ratio sets of positive integers*, Amer. Math. Monthly **103** (1996), no. 6, 502–504. MR 1390582 (97c:11009)
8. S. A. Burr, *On moduli for which the Fibonacci sequence contains a complete system of residues*, Fibonacci Quart. **9** (1971), no. 5, 497–504, 526. MR 0294238 (45 #3307)
9. H. Davenport, *On Waring's problem for cubes*, Acta Math. **71** (1939), 123–143. MR 0000026
10. Jean-Marie De Koninck and Armel Mercier, *1001 problems in classical number theory*, American Mathematical Society, Providence, RI, 2007. MR MR2302879 (2007m:11001)
11. Benjamin Fine and Gerhard Rosenberger, *Number theory: An introduction via the distribution of primes*, Birkhäuser, Boston, 2007. MR MR2261276 (2007i:11001)
12. Stephan Ramon Garcia, *Quotients of Gaussian Primes*, Amer. Math. Monthly **120** (2013), no. 9, 851–853. MR 3115449
13. Stephan Ramon Garcia and Florian Luca, *Quotients of Fibonacci numbers*, Amer. Math. Monthly, in press.
14. Stephan Ramon Garcia, Vincent Selhorst-Jones, Daniel E. Poore, and Noah Simon, *Quotient sets and Diophantine equations*, Amer. Math. Monthly **118** (2011), no. 8, 704–711. MR 2843990 (2012h:11008)
15. Fernando Q. Gouvêa, *p-adic numbers*, second ed., Universitext, Springer-Verlag, Berlin, 1997, An introduction. MR 1488696 (98h:11155)

16. Ben Green and Terence Tao, *The primes contain arbitrarily long arithmetic progressions*, Ann. of Math. (2) **167** (2008), no. 2, 481–547. MR 2415379
17. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008. MR MR2445243 (2009i:11001)
18. Helmut 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. MR 0205975
19. D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38. MR 830627 (88a:11004)
20. Shawn Hedman and David Rose, *Light subsets of $\mathbb{N}$ with dense quotient sets*, Amer. Math. Monthly **116** (2009), no. 7, 635–641. MR MR2549381
21. David Hobby and D. M. Silberger, *Quotients of primes*, Amer. Math. Monthly **100** (1993), no. 1, 50–52. MR MR1197643 (94a:11007)
22. Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR 754003 (86c:11086)
23. J. C. Lagarias, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), no. 2, 449–461. MR 789184
24. Florian Luca, Carl Pomerance, and Štefan Porubský, *Sets with prescribed arithmetic densities*, Unif. Distrib. Theory **3** (2008), no. 2, 67–80. MR 2480233
25. Florian Luca, Carl Pomerance, and Stephan Wagner, *Fibonacci integers*, J. Number Theory **131** (2011), no. 3, 440–457. MR 2739045 (2011k:11131)
26. Ace Micholson, *Quotients of primes in arithmetic progressions*, Notes Number Theory Disc. Math. **18** (2012), no. 2, 56–57.
27. Ladislav Mišik, *Sets of positive integers with prescribed values of densities*, Math. Slovaca **52** (2002), no. 3, 289–296. MR 1936334
28. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, *An introduction to the theory of numbers*, fifth ed., John Wiley & Sons, Inc., New York, 1991. MR 1083765 (91i:11001)
29. Andrzej Nowicki, *Editor's endnotes*, Amer. Math. Monthly **117** (2010), no. 8, 755–756.
30. Paul Pollack, *Not always buried deep: A second course in elementary number theory*, American Mathematical Society, Providence, RI, 2009. MR 2555430 (2010i:11003)
31. Paulo Ribenboim, *Classical theory of algebraic numbers*, Universitext, Springer-Verlag, New York, 2001. MR 1821363 (2002e:11001)
32. T. Šalát, *On ratio sets of sets of natural numbers*, Acta Arith. **15** (1968/1969), 273–278. MR 0242756 (39 #4083)
33. ———, *Corrigendum to the paper "On ratio sets of sets of natural numbers".*, Acta Arith. **16** (1969/1970), 103. MR 0248107 (40 #1361)
34. Brian D. Sittinger, *Quotients of primes in an imaginary quadratic number ring*, preprint.
35. Jeremiah T. Southwick, *The Lucas numbers and other Gibonacci qequences mod m*, `http://arxiv.org/abs/1402.0598`.
36. Paolo Starni, *Answers to two questions concerning quotients of primes*, Amer. Math. Monthly **102** (1995), no. 4, 347–349. MR MR1328019 (97a:11025)
37. Oto Strauch and János T. Tóth, *Asymptotic density of $A \subset \mathbf{N}$ and density of the ratio set $R(A)$*, Acta Arith. **87** (1998), no. 1, 67–78. MR 1659159 (99k:11020)
38. ———, *Corrigendum to Theorem 5 of the paper: "Asymptotic density of $A \subset \mathbb{N}$ and density of the ratio set $R(A)$" [Acta Arith.* **87** *(1998), no. 1, 67–78; MR1659159 (99k:11020)]*, Acta Arith. **103** (2002), no. 2, 191–200. MR 1904872 (2003f:11015)
39. S. Vajda, *Fibonacci & Lucas numbers, and the golden section*, Ellis Horwood Series: Mathematics and its Applications, Ellis Horwood Ltd., Chichester; Halsted Press [John Wiley & Sons, Inc.], New York, 1989, Theory and applications, With chapter XII by B. W. Conolly. MR 1015938 (90h:11014)

Department of Mathematics, Pomona College, 610 N. College Ave., Claremont, CA 91711
E-mail address: stephan.garcia@pomona.edu
URL: http://pages.pomona.edu/~sg064747

School of Mathematics, University of the Witwatersrand, Private Bag 3, Wits 2050, Johannesburg, South Africa
E-mail address: Florian.Luca@wits.ac.za