A Classification of Integral Apollonian Circle Packings

Tabes Bridges
Warren Tai
Advised by: Karol Koziol

25 July 2011

Abstract

We review the basic notions related to Apollonian circle packings, in particular focusing on root quadruples. After considering several examples of infinite families of such quadruples, we show that all primitive root quadruples take on a particularly simple form, and can be easily parametrized by suitable integers k and α. We then classify all possible families with $k = p^j$, p a prime, and combine these families using an analog of the Chinese Remainder Theorem to give an exhaustive classification of all such families. As a final note, we examine a congruence property mod 12 of the families $\mathcal{P}_{k,\alpha}$ for $gcd(k, 12) = 1$.

1 Introduction

Apollonian circle packing is rooted in the following theorem of Euclidean geometry, known as Apollonius' Theorem: given any three mutually tangent circles in the plane, there are exactly two circles tangent to the first three. By starting with a configuration of four mutually tangent circles, with one containing the other three, this theorem can be exploited to fill in the lunes between circles, as each lune is bounded by three circles. Continuing in this fashion ad infinitum gives an Apollonian circle packing. The curvatures (a, b, c, d) of any set of four mutually tangent circles satisfy the **Descartes equation**

$$(a + b + c + d)^2 = 2(a^2 + b^2 + c^2 + d^2) \tag{1.1}$$

and are called a **Descartes quadruple**. We are primarily concerned with **primitive integral root quadruples**, which are Descartes quadruples of the form $(a, b, c, d) \in \mathbb{Z}^4$ such that $gcd(a, b, c, d) = 1$, $a + b + c + d > 0$, $a \leq 0 \leq b \leq c \leq d$, and $a + b + c \geq d$. A root quadruple represents the curvatures of the four largest circles in a packing, with $a \leq 0$ representing the negative orientation of the circle which contains the other three. The case $a = 0$ refers to the case of an unbounded strip packing, which contains circles of infinite radius and is of no particular concern to us, so we shall henceforth omit it from our discussion.

We note that starting with an integral root quadruple will result in a packing that has all integral curvatures. This follows from the formula for d', the curvature of the circle tangent to the three circles of curvature a, b, and c, and unequal to the circle of curvature d:

$$d' = 2a + 2b + 2c - d, \tag{1.2}$$

which itself follows from a consequence of the Descartes equation,

$$d,\, d' = a + b + c \pm 2\sqrt{ab + bc + ac}. \tag{1.3}$$

The paper [GLMWY] gives the following theorem:

Theorem 1. *For a solution $(a, b, c, d) \in \mathbb{Z}^4$ to the Descartes Equation (1.1) we define the* ***simplified quadruple*** *$(x, d_1, d_2, m) \in \mathbb{Z}^4$ by*

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 1 & 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ d_1 \\ d_2 \\ m \end{pmatrix} = \begin{pmatrix} x \\ d_1 - x \\ d_2 - x \\ -2m + d_1 + d_2 - x \end{pmatrix}, \tag{1.4}$$

which satisfies

$$x^2 + m^2 = d_1 d_2. \tag{1.5}$$

The transformation can, of course, be reversed, giving a bijection between integral solutions to the equations (1.1) and (1.5). Furthermore,

(i) the Descartes quadruple (a, b, c, d) is primitive if and only if $gcd(x, d_1, d_2) = 1$,

and

(ii) the Descartes quadruple (a, b, c, d) with $a+b+c+d > 0$ and $a \neq 0$ is a root quadruple if and only if $x < 0 \leq 2m \leq d_1 \leq d_2$.

Notation. Let A denote the 4×4 matrix in (1.4). Its inverse, by which we can transform from Descartes quadruples to simplified quadruples, is

$$A^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}. \tag{1.6}$$

2 Finding Infinite Families

We can use the much simpler (1.5) in lieu of (1.1) to calculate formulae in terms of a variable $n \in \mathbb{N}$, which may be free or constrained to certain equivalence classes; in any case, such a formula will have infinitely many solutions. We start by examining several examples in an ad hoc fashion; we will later proceed systematically.

Example 1. *[GLMWY] The quadruple $(-n, n + 1, n^2 + n, n^2 + n + 1)$ is a primitive root quadruple for all $n \in \mathbb{N}$.*

Let $m = 0$ and $x = -n$ in (1.5), giving

$$n^2 = d_1 d_2. \tag{2.1}$$

In order to satisfy condition (i), let $d_1 = 1$ and $d_2 = n^2$. Then we have a simplified quadruple $\mathbf{x} = (-n, 1, n^2, 0)^T$. We can transform $\mathbf{x}$ to a Descartes quadruple by multiplying on the left by A, which gives $A\mathbf{x} = (-n, n+1, n^2+n, n^2+n+1)^T$.

Letting $m = 1$ and $x = -n$ results in a similar computation which yields the Descartes quadruple for all $n \equiv 1 \pmod 2$, $n > 1$

$$\left(-n, n+2, \frac{(n+1)^2}{2}, \frac{(n+1)^2}{2}\right). \tag{2.2}$$

Example 2. *The quadruple* $\left(-n, n+8, \dfrac{n^2+8n+4}{8}, \dfrac{n^2+8n+36}{8}\right)$ *is a root quadruple for all* $n \equiv 2 \pmod 4$, $n > 6$.

Letting $m = 2$ and $x = -n$ in (1.5) gives

$$n^2 + 4 = d_1 d_2. \tag{2.3}$$

Pick $n = 2k$, giving $4(k^2+1) = d_1 d_2$. Choosing k odd gives us $k^2 \equiv 1 \pmod 4$, so that $k^2 + 1 \equiv 2 \pmod 4$, and $\frac{k^2+1}{2} \equiv 1 \pmod 2$. Now let $d_1 = 8$, so that $d_2 = \frac{n^2+4}{8}$ is odd (and hence relatively prime to 8). We now have the simplified quadruple $\mathbf{x} = (-n, 8, \frac{n^2+4}{8}, 2)^T$. Computing $A\mathbf{x}$ gives the desired Descartes quadruple.

Example 3. *The quadruple* $\left(-n, n+4, \dfrac{n^2+4n}{4}, \dfrac{n^2+4n+16}{4}\right)$ *is a root quadruple for all* $n \equiv 2 \pmod 4, n > 2$.

Letting $d_1 = 4$ and $x = -n$ in (1.5) gives

$$n^2 + m^2 = 4d_2. \tag{2.4}$$

Taking $n \equiv 2 \pmod 4$, we can set $n = 4k + 2$, which gives

$$16k^2 + 16k + 4 + m^2 = 4d_2. \tag{2.5}$$

We see that m must be even, so we set $m = 2j$, which gives

$$4(4k^2 + 4k + 1 + j^2) = 4d_2 \quad \Leftrightarrow \quad 4k^2 + 4k + 1 + j^2 = d_2. \tag{2.6}$$

We are assured condition (i) by setting j even. By condition (ii), we in fact have $j = 0$, which implies $m = 0$, which in turn implies $d_2 = 4k^2 + 4k + 1$. We thus get the quadruple $\mathbf{x} = (-n, 4, \frac{n^2}{4}, 0)^T$. Computing $A\mathbf{x}$ gives the desired Descartes quadruple.

A similar computation yields the Descartes quadruple for all $n \equiv 0 \pmod 4$, $n > 12$

$$\left(-n, n+4, \frac{n^2+4n+4}{4}, \frac{n^2+4n+4}{4}\right). \tag{2.7}$$

Example 4. *Without belabouring computations, we note the following two families of quadruples:*

$$\left(-n, n+5, \frac{n^2+5n+1}{5}, \frac{n^2+5n+16}{5}\right), \quad n \equiv \pm 2 \pmod 5, n > 3 \tag{2.8}$$

$$\left(-n, n+5, \frac{n^2+5n+4}{5}, \frac{n^2+5n+9}{5}\right), \quad n \equiv \pm 1 \pmod 5, n > 4. \tag{2.9}$$

3 An Infinite Family of Infinite Families

For the remainder of this paper, we will denote by δ a number which squares to -1 modulo some positive integer k. If δ does not exist in a particular ring $\mathbb{Z}/k\mathbb{Z}$, it may still be used hypothetically for the sake of argument. In particular, it is well-known that δ exists in $\mathbb{Z}/p\mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$ or $p = 2$.

Theorem 2. *For each prime $p \equiv 1 \pmod 4$, the following is a primitive root quadruple for suitable natural numbers n, α, and β.*

$$\mathbf{x} := \left(-n, n+p, \frac{n^2+pn+\alpha^2}{p}, \frac{n^2+pn+\beta^2}{p}\right)^T. \tag{3.1}$$

More precisely, we must have $0 < \alpha < \frac{p}{2}$ and $\beta = p - \alpha$. This condition implies that $\alpha < \beta$. The given quadruple is a primitive root quadruple for all $n \equiv \pm\delta\alpha \pmod p$ such that $p^2 - \alpha^2 \leq n^2$. Note that there are infinitely many such $n \in \mathbb{N}$. In fact, this covers all possible families of the form $(-n, n+p, ...)$.

Proof. Applying (1.5) to

$$A^{-1}\mathbf{x} = \left(-n, p, \frac{n^2+\alpha^2}{p}, \frac{p^2+(\alpha^2-\beta^2)}{2p}\right)^T \tag{3.2}$$

we get that $\alpha = \left(\frac{p^2+(\alpha^2-\beta^2)}{2p}\right)$. Clearing denominators and collecting terms we get

$$\beta^2 = \alpha^2 + p^2 - 2p\alpha \quad \Leftrightarrow \quad \beta = \sqrt{\alpha^2+p^2-2p\alpha} = \sqrt{(p-\alpha)^2} = p - \alpha. \tag{3.3}$$

To ensure that $\alpha < \beta$, we require $\alpha < \frac{p}{2}$. In addition, we require $\alpha > 0$, since $\alpha = 0$ would give $gcd(n, p, \frac{n^2+\alpha^2}{p}) > 1$.

We need to ensure that $\dfrac{n^2+pn+\alpha^2}{p}$ and $\dfrac{n^2+pn+\beta^2}{p}$ are integers, meaning find n such that $n^2+\alpha^2$ and $n^2+\beta^2$ are congruent to $0 \pmod p$. Since $\alpha^2 \equiv \beta^2 \pmod p$, it suffices to check for the former. Since $\alpha \not\equiv 0 \pmod p$, we have

$$n^2 \equiv -\alpha^2 \pmod p \quad \Leftrightarrow \quad n \equiv \pm\delta\alpha \pmod p. \tag{3.4}$$

We need to find $\delta \in \mathbb{Z}/p\mathbb{Z}$ such that $\delta^2 \equiv -1 \pmod p$. As noted above, it is well know that δ can be found for all $p \equiv 1 \pmod 4$ (for example, Wilson's Theorem implies that $\delta \equiv \pm\left(\frac{p-1}{2}\right)! \pmod p$). Therefore, the quadruple will be integral for $p \equiv 1 \pmod 4$.

In [GLMWY], it is demonstrated that for a simplified quadruple to transform to a primitive root quadruple, it must satisfy two conditions:

(i) $gcd(x, d_1, d_2) = 1$, and

(ii) $x < 0 \leq 2m \leq d_1 \leq d_2$. We will refer to these four inequalities as I, II, III, and IV, listed left to right.

Every quadruple in our family satisfies (i), since $n \not\equiv 0 \pmod{p}$ so that $gcd(n, p) = 1$. For (ii), we move left to right:

I. Clear by positivity of n.

II. We need $p^2 \geq (\beta^2 - \alpha^2) = p^2 - 2p\alpha$, which implies $2p\alpha \geq 0$. This is satisfied by our hypothesis.

III. We need $p^2 + (\alpha^2 - \beta^2) \leq p^2$. This holds by $\beta \geq \alpha$.

IV. We need $p^2 \leq n^2 + \alpha^2$. We simply give this inequality as a lower bound for n.

To prove that we have covered all such families, note that we have proven that α must be in $\left(0, \frac{p}{2}\right] \cap \mathbb{Z}$. Since all other parameters are tied to α, and are exhaustive, it must be the case that these conditions exhaust families of the form $(-n, n + p, ...)$. ■

Remark. The quadruple (3.1) does not give an infinite family of integral root quadruples for any $p \equiv 3 \pmod{4}$, because the number δ does not exist in $\mathbb{Z}/p\mathbb{Z}$ for any $p \equiv 3 \pmod{4}$.

4 The Form of a Root Quadruple

It is no coincidence that all of the families we have looked at take a form like that in Theorem 2. We will prove that, in fact, all primitive root quadruples take this form, and we will henceforth write them in the form given in Theorem 3.

Theorem 3. *Each primitive root quadruple can be written in the form*

$$\mathbf{x} := \left(-n, n + k, \frac{n^2 + kn + \alpha^2}{k}, \frac{n^2 + kn + (k - \alpha)^2}{k}\right)^T, \tag{4.1}$$

where n, k, and α are integers such that $\frac{n^2+\alpha^2}{k} \in \mathbb{N}$, $gcd(n, k, \frac{n^2+\alpha^2}{k}) = 1$, $n, k > 0$, and $0 \leq \alpha \leq (k - \alpha)$.

Proof. Let (a, b, c, d) be a primitive root quadruple. In particular, this implies that the quantity $\sqrt{ab + ac + bc}$ is an integer, and that $d = a + b + c - 2\sqrt{ab + ac + bc}$, since we must have $d' \geq d$. Define $n = -a$, $k = a + b$, and $\alpha = \sqrt{ab + ac + bc}$. The positivity of k follows from Lemma 3.1(i) of [GLMWY]. Plugging these values into (4.1) yields the quadruple (a, b, c, d). Note also that the root condition implies $(k - \alpha)^2 = ab + bd + ad$. Since (a, b, c, d) is a root quadruple,

$$\begin{aligned} c \leq d &\Leftrightarrow ca + cb \leq da + db \\ &\Leftrightarrow ab + ca + cb \leq ab + da + db \\ &\Leftrightarrow \alpha^2 \leq (k - \alpha)^2 = k^2 - 2k\alpha + \alpha^2. \end{aligned} \tag{4.2}$$

From this we know that

$$0 \leq k(k-2\alpha) \Leftrightarrow 0 \leq k-2\alpha \\ \Leftrightarrow \alpha \leq k-\alpha. \tag{4.3}$$

The coprimality of n, k and $\frac{n^2+\alpha^2}{k}$ follows from that of a, b, and c, since $gcd(a,b,c) = gcd(a,b,c,d)$ (note that d is determined by a, b, and c).

Conversely, any quadruple of the form (4.1) satisfying the divisibility conditions and inequalities is a primitive root quadruple. ■

With this theorem in hand, we proceed to classify all possible root quadruples of the form (4.1) with $k = p^j$, for p a prime.

5 Powers of 2

Theorem 4. *Let j be a positive even integer. The following is a primitive root quadruple:*

$$\mathbf{x} := \left(-n, n+2^j, \frac{n^2+2^j n+\alpha^2}{2^j}, \frac{n^2+2^j n+(2^j-\alpha)^2}{2^j}\right)^T, \tag{5.1}$$

where $\alpha \leq 2^{j-1}$, $\alpha = q2^{j/2}$, $n = \ell 2^{j/2}$, and $n^2 \geq 2^{2j} - \alpha^2$, and where $q, \ell \in \mathbb{N}$ have opposite parity. More succinctly, we may write $n \equiv 2^{j/2} + \alpha \pmod{2^{j/2+1}}$. As there is no upper bound on j or n, this gives an infinite set of infinite families of primitive root quadruples. The given parameters are the only such that guarantee primitivity.

Proof. One easily verifies that

$$A^{-1}\mathbf{x} = \left(-n, 2^j, \frac{n^2+\alpha^2}{2^j}, \frac{2^{2j}+(2^{j+1}\alpha - 2^{2j})}{2^{j+1}}\right)^T \tag{5.2}$$

satisfies (1.5). Because $q^2+\ell^2 \equiv 1 \pmod 2$, $A^{-1}\mathbf{x}$ satisfies condition (i). Simple computations analogous to those done in the proof of Theorem 2 show that (5.2) satisfies condition (ii):

I. Clear.

II. $2^{2j} + (2^{j+1}\alpha - 2^{2j}) = 2^{j+1}\alpha \geq 0$.

III. $2^{2j} \geq 2^{j+1}\alpha \quad \Leftrightarrow \quad 2^{j-1} \geq \alpha$, which is part of our hypothesis.

IV. This is our given lower bound for n^2.

We must now show that our choices of α and n are the only ones that generate primitive quadruples. Assuming first that α is odd, the equation $n^2 + \alpha^2 \equiv 0 \pmod{2^j}$ implies that n must also be odd. In particular, n and α are units in the ring $\mathbb{Z}/2^j\mathbb{Z}$, satisfying the equation $\left(\frac{n}{\alpha}\right)^2 \equiv -1 \pmod{2^j}$. This is a contradiction, as the equation $y^2 + 1 \equiv 0 \pmod{2^j}$ has no solution for $j > 1$. Assume now that $\alpha = q2^e$, with $e < j/2$ and $gcd(q, 2^j) = 1$. Reducing the equation $n^2 + \alpha^2 \equiv 0 \pmod{2^j}$ modulo 2^{2e} shows that $n^2 \equiv 0 \pmod{2^{2e}}$, which implies in turn that $n \equiv 0 \pmod{2^e}$. Writing $n = \ell 2^e$ yields the equation $\ell^2 + q^2 \equiv 0 \pmod{2^{j-2e}}$, which gives a contradiction by a completely analogous argument to the one previously considered. ■

Theorem 5. *Let j be a positive odd integer. The quadruple* (5.1) *is a primitive root quadruple if we take $\alpha = q2^{(j-1)/2}$ and $n = \ell 2^{(j-1)/2}$, where q and ℓ are both odd. More succinctly, this condition is equivalent to $n \equiv \alpha \equiv 2^{(j-1)/2} \pmod{2^{(j+1)/2}}$.*

Proof. Verifying that condition (ii) is satisfied is identical to the case for j even. We verify the primitivity condition. Suppose first that q is even. We can then set $q = 2q'$, so $\dfrac{n^2+\alpha^2}{2^j} = \dfrac{q^2+\ell^2}{2} = \dfrac{4q'^2+\ell^2}{2}$, which is only an integer for ℓ even. In this case, condition (i) is not satisfied.

Suppose now q is odd and set $q = 2q'+1$, so $\dfrac{n^2+\alpha^2}{2^j} = \dfrac{q^2+\ell^2}{2} = \dfrac{4q'^2+4q'+1+\ell^2}{2}$, which is only an integer for ℓ odd. Writing $\ell = 2\ell'+1$ shows that this fraction is an odd integer, meaning that condition (i) is satisfied.

Verifying that these are the only such parameters that yield primitive root quadruples follows exactly as in the case for j even. We need only consider the cases where α is odd, or $\alpha = q2^e$ with $gcd(q, 2^j) = 1$ and $e < (j-1)/2$. ■

6 Powers of Odd Primes

Theorem 6. *Let p be a prime equivalent to* $1 \pmod 4$*, and let j be a positive even integer. The following is a primitive root quadruple for suitable natural numbers n and α.*

$$\mathbf{x} := \left(-n, n+p^j, \frac{n^2+p^jn+\alpha^2}{p^j}, \frac{n^2+p^jn+(p^j-\alpha)^2}{p^j}\right)^T. \tag{6.1}$$

More precisely, let $\alpha = qp^e$, with $gcd(q, p^j) = 1$, and $\alpha \le p^j/2$. Let δ denote a square root of -1 in $\mathbb{Z}/p^j\mathbb{Z}$. If $e < j/2$, then we may take $n \equiv \pm\delta\alpha \pmod{p^{j-e}}$ (with a slight restriction, explained in the proof). If $e = j/2$, then $n = \ell p^{j/2}$, with $\ell \not\equiv \pm\delta q \pmod p$. If $e > j/2$, then $n = \ell p^{j/2}$, with $\ell \not\equiv 0 \pmod p$. In each of these cases, we take $n^2 \ge p^{2j} - \alpha^2$. There are infinitely many n satisfying each of these conditions. The given conditions are the only such that guarantee primitivity.

Proof. We easily verify that

$$A^{-1}\mathbf{x} = \left(-n, p^j, \frac{n^2+\alpha^2}{p^j}, \frac{p^{2j}+(2p^j\alpha - p^{2j})}{2p^j}\right)^T \tag{6.2}$$

satisfies (1.5). We first verify condition (ii):

I. Clear.

II. $p^{2j} + (2p^j\alpha - p^{2j}) = 2p^j\alpha \ge 0$.

III. $p^{2j} \ge 2p^j\alpha \quad \Leftrightarrow \quad p^j/2 \ge \alpha$, which is part of our hypothesis.

IV. This is our given lower bound for n^2.

We now proceed systematically and verify the remaining claims in the theorem. Note that, by Hensel's Lemma, the existence of δ in $\mathbb{Z}/p\mathbb{Z}$ guarantees its existence in $\mathbb{Z}/p^j\mathbb{Z}$. Moreover, reducing δ modulo p^e with $0 < e < j$ yields an element in $\mathbb{Z}/p^e\mathbb{Z}$ which squares to -1. Writing $\alpha = qp^e$, with $gcd(q, p^j) = 1$, and substituting into the equation $n^2 + \alpha^2 \equiv 0$

$(\text{mod } p^j)$ gives $n^2 + q^2p^{2e} \equiv 0 \pmod{p^j}$. If $e < j/2$, we proceed as in the characteristic 2 case, and find that $n = \ell p^e$. This gives the equation $\ell^2 + q^2 \equiv 0 \pmod{p^{j-2e}}$, which is equivalent to $\ell \equiv \pm\delta q \pmod{p^{j-2e}}$. Multiplying through by p^e gives $n \equiv \pm\delta\alpha \pmod{p^{j-e}}$. If $e \neq 0$, we write $n \equiv \pm\delta\alpha + fp^{j-e} \pmod{p^j}$, where $f \in \mathbb{Z}/p^e\mathbb{Z}$. Expanding the equation $\dfrac{(\pm\delta\alpha + fp^{j-e})^2 + \alpha^2}{p^j}$ shows exactly which values of f will yield integers relatively prime to p, thereby guaranteeing primitivity.

If $e = j/2$, then we arrive at the equation $\dfrac{n^2 + \alpha^2}{p^j} = \ell^2 + q^2$. If ℓ is congruent to $\pm\delta q \pmod{p}$, then evidently $\ell^2 + q^2 \equiv 0 \pmod{p}$, and the quadruple will not be primitive.

If $e > j/2$, then we are left with the equation $\dfrac{n^2 + \alpha^2}{p^j} \equiv \dfrac{n}{p^j} \pmod{p}$, in which case we must have $n = \ell p^{j/2}$ with $gcd(\ell, p) = 1$.

These three subcases exhaust all possible choices for α. ■

Theorem 7. *Let j be a positive odd integer. The quadruple* (6.1) *is a primitive root quadruple for suitable α and n. More precisely, let $\alpha = qp^e$, with $gcd(q, p^j) = 1$, and $\alpha \leq p^j/2$. If $e < j/2$, then we may take $n \equiv \pm\delta\alpha \pmod{p^{j-e}}$ (with a suitable restriction, explained in the proof). These are the only parameters for α that yield primitive root quadruples.*

Proof. Verifying that the given α and n (subject to the same restriction as previously discussed) satisfy conditions (i) and (ii) is identical to the proof for the case of j even. We prove that these are the only admissible choices for α. Assuming that $\alpha = qp^e$ with $e > j/2$ gives $\dfrac{n^2 + \alpha^2}{p^j} \equiv \dfrac{n^2}{p^j} \pmod{p}$. This implies that n must be of the form $\ell p^{(j+1)/2}$, with ℓ an arbitrary integer. This gives $\dfrac{n^2}{p^j} \equiv \ell^2 p \equiv 0 \pmod{p}$, and therefore such an α cannot yield a primitive quadruple. ■

We now deal with primes $p \equiv 3 \pmod 4$. For such primes, there does not exist a square root δ of -1 in $\mathbb{Z}/p^j\mathbb{Z}$, because such a δ would imply the existence of δ in $\mathbb{Z}/p\mathbb{Z}$, which we know to be false.

Lemma 1. *There never exists an infinite family of primitive root quadruples in the form $(n, n + k, ...)$ when $k = p^j$ for $p \equiv 3 \pmod 4$ and j an odd positive integer.*

Proof. We assume such a family exists and work by cases depending on the nature of a hypothetical α.

Case 1. $gcd(\alpha, p) = 1$. This implies that α is a unit in $\mathbb{Z}/p^j\mathbb{Z}$, so

$$n^2 + \alpha^2 \equiv 0 \pmod{p^j} \quad \Leftrightarrow \quad \left(\frac{n}{\alpha}\right)^2 \equiv -1 \pmod{p^j}, \tag{6.3}$$

but $\delta \notin \mathbb{Z}/p^j\mathbb{Z}$, a contradiction.

Case 2. $gcd(\alpha, p) > 1$. Let $\alpha = qp^e$, where $gcd(q, p) = 1$ and $e > 0$. Then

$$n^2 + \alpha^2 \equiv 0 \pmod{p^j} \quad \Leftrightarrow \quad n^2 + q^2p^{2e} \equiv 0 \pmod{p^j}. \tag{6.4}$$

Subcase 1. $e < j/2$. We can then take

$$\left(\frac{n}{p^e}\right)^2 \equiv -q^2 \pmod{p^{j-2e}} \quad \Leftrightarrow \quad \left(\frac{n}{qp^e}\right)^2 \equiv -1 \pmod{p^{j-2e}}, \tag{6.5}$$

which is again a contradiction.
Subcase 2. $e > j/2$. In this case, $n^2 \equiv 0 \pmod{p^j}$, which implies that $n \equiv 0 \pmod{p^{(j+1)/2}}$. Let $n = \ell p^{(j+1)/2}$, so that $n^2 = \ell^2 p^{j+1}$. We then have

$$\frac{n^2+\alpha^2}{p^j} = \frac{\ell^2 p^{j+1} + q^2 p^{2e}}{p^j} = \ell^2 p + q^2 p^{2e-j}, \tag{6.6}$$

which gives $gcd(x, d_1, d_2) > 1$, a contradiction. ■

Theorem 8. *Let j be a positive even integer. The following is a primitive root quadruple for $p \equiv 3 \pmod 4$:*

$$\left(-n, n+p^j, \frac{n^2+p^j n+\alpha^2}{p^j}, \frac{n^2+p^j n+(p^j-\alpha)^2}{p^j}\right), \tag{6.7}$$

where $\alpha = qp^{j/2}$, $\alpha \le p^j/2$, $n = \ell p^{j/2}$, and $n^2 \ge p^{2j} - \alpha^2$. If $q \equiv 0 \pmod p$, ℓ must be relatively prime to p. If $q \not\equiv 0 \pmod p$, ℓ may be any positive integer large enough to satisfy the lower bound on n. These are the only parameters that yield primitive root quadruples.

Proof. The simplified quadruple

$$\left(-n, p^j, \frac{n^2+\alpha^2}{p^j}, \frac{p^{2j} + (2p^j\alpha - p^{2j})}{2p^j}\right) \tag{6.8}$$

is easily seen to satisfy (1.5).

To satisfy condition (i), we need $\ell^2 + q^2 \not\equiv 0 \pmod p$. By similar computations to those used in the proof of Lemma 1, α must be a multiple of $p^{j/2}$. For $q \equiv 0 \pmod p$, we obviously need $\ell \not\equiv 0 \pmod p$. For $q \not\equiv 0 \pmod p$, we get

$$\ell^2 + q^2 \not\equiv 0 \pmod p \quad \Leftrightarrow \quad \ell^2 \not\equiv -q^2 \pmod p, \tag{6.9}$$

which is always satisfied, since $\delta \notin \mathbb{Z}/p^{2j}\mathbb{Z}$.

We show that condition (ii) is satisfied by the usual computations:
I. Clear.
II. $p^{2j} + (2p^j\alpha - p^{2j}) = 2p^j\alpha \ge 0$.
III. $p^{2j} \ge 2p^j\alpha \quad \Leftrightarrow \quad p^j/2 \ge \alpha \quad \Leftrightarrow \quad p^{j/2}/2 \ge q$, which is part of our hypothesis.
IV. This is our given lower bound for n^2.

We now show that our choices of α and n are the only possibilities. Assume that $\alpha = qp^e$, with $e < j/2$ and $gcd(q, p^j) = 1$. The equation $n^2 + \alpha^2 \equiv 0 \pmod{p^j}$ is then equivalent to the equation $\left(\frac{n}{qp^e}\right)^2 \equiv -1 \pmod{p^{j-2e}}$, which we know to be a contradiction. Hence, α must be divisible by $p^{j/2}$. ■

7 Composite Numbers

Theorem 9. *Given two infinite families of primitive root quadruples of the form*

$$\mathcal{P}_{k,\alpha_k} := \left(-n, n+k, \frac{n^2+kn+\alpha_k^2}{k}, \frac{n^2+kn+(k-\alpha_k)^2}{k}\right) \text{ where } n \equiv n_k \pmod{k} \quad (7.1)$$

and

$$\mathcal{P}_{k',\alpha_{k'}} := \left(-n, n+k', \frac{n^2+k'n+\alpha_{k'}^2}{k'}, \frac{n^2+k'n+(k'-\alpha_{k'})^2}{k'}\right) \text{ where } n \equiv n_{k'} \pmod{k'}, \quad (7.2)$$

where k and k' are relatively prime, we can generate an associated composition:

$$\mathcal{P}_{k,\alpha_k} \odot \mathcal{P}_{k',\alpha_{k'}} := \left(-n, n+kk', \frac{n^2+kk'n+\alpha_{kk'}^2}{kk'}, \frac{n^2+kk'n+(kk'-\alpha_{kk'})^2}{kk'}\right). \quad (7.3)$$

Here $n \equiv n_{kk'} \equiv n_k k'\tau_{k'} + n_{k'} k\tau_k \pmod{kk'}$, $0 \le \alpha_{kk'} \le kk'/2$ with $\alpha_{kk'} \equiv \pm(\alpha_k k'\tau_{k'} + \alpha_{k'} k\tau_k) \pmod{kk'}$, and τ_k denotes the multiplicative inverse of $k \pmod{k'}$ and vice versa. The composition $\mathcal{P}_{k,\alpha_k} \odot \mathcal{P}_{k',\alpha_{k'}}$ is primitive, and a root quadruple for $n^2 \ge k^2k'^2 - \alpha_{kk'}^2$.

Proof. By the Chinese Remainder Theorem, $n_{kk'} \equiv n_k k'\tau_{k'} + n_{k'} k\tau_k \pmod{kk'}$. We know that $n_k^2 \equiv -\alpha_k^2 \pmod{k}$ and $n_{k'}^2 \equiv -\alpha_{k'}^2 \pmod{k'}$. Defining $\alpha_{kk'}$ as in the statement of the theorem, we have $\alpha_{kk'}^2 \equiv \alpha_k^2 k'^2 \tau_{k'}^2 + \alpha_{k'}^2 k^2 \tau_k^2 \pmod{kk'}$. There are no cross terms due to reduction modulo kk'. We will show that this $\alpha_{kk'}$ satisfies the necessary conditions. Note that

$$n_{kk'}^2 + \alpha_{kk'}^2 = n_k^2 k'^2 \tau_{k'}^2 + n_{k'}^2 k^2 \tau_k^2 + \alpha_k^2 k'^2 \tau_{k'}^2 + \alpha_{k'}^2 k^2 \tau_k^2. \quad (7.4)$$

Again by the Chinese Remainder Theorem, the right hand side is 0 modulo both k and k', therefore $n_{kk'}^2 + \alpha_{kk'}^2 \equiv 0 \pmod{kk'}$.

To ensure that the quadruple is ordered correctly, we need to verify that $\alpha_{kk'} \le \frac{kk'}{2}$. If that is the case upon computation, we are done. If the computed α is greater than $\frac{kk'}{2}$, replace it with $kk' - \alpha < kk' - \frac{kk'}{2} = \frac{kk'}{2}$.

We need only to verify that $gcd(n, kk', \frac{n^2+\alpha_{kk'}^2}{kk'}, \frac{n^2+(kk'-\alpha_{kk'})^2}{kk'}) = 1$, assuming

$$gcd\left(n, k, \frac{n^2+\alpha_k^2}{k}, \frac{n^2+(k-\alpha_k)^2}{k}\right) = gcd\left(n, k', \frac{n^2+\alpha_{k'}^2}{k'}, \frac{n^2+(k'-\alpha_{k'})^2}{k'}\right) = 1.$$

Note that, by coprimality of k and k', we have the following chain of equalities:

$$\begin{aligned}
gcd\left(n, kk', \frac{n^2+\alpha_{kk'}^2}{kk'}, \frac{n^2+(kk'-\alpha_{kk'})^2}{kk'}\right) &= gcd\left(n, kk', \frac{n^2+\alpha_{kk'}^2}{kk'}, \frac{n^2+\alpha_{kk'}^2}{kk'} + kk' - 2\alpha_{kk'}\right) \\
&= gcd\left(n, kk', \frac{n^2+\alpha_{kk'}^2}{kk'}, 2\alpha_{kk'}\right) \\
&= gcd\left(gcd(n, kk'), \frac{n^2+\alpha_{kk'}^2}{kk'}, 2\alpha_{kk'}\right) \\
&= gcd\left(gcd(n,k)gcd(n,k'), \frac{n^2+\alpha_{kk'}^2}{kk'}, 2\alpha_{kk'}\right)
\end{aligned}$$

$$
\begin{aligned}
&= gcd\left(gcd(n,k), \frac{n^2+\alpha_{kk'}^2}{kk'}, 2\alpha_{kk'}\right) \\
&\quad \times gcd\left(gcd(n,k'), \frac{n^2+\alpha_{kk'}^2}{kk'}, 2\alpha_{kk'}\right) \\
&\overset{\star}{=} gcd\left(gcd(n,k), \frac{n^2+\alpha_{kk'}^2}{k}, 2\alpha_{kk'}\right) \\
&\quad \times gcd\left(gcd(n,k'), \frac{n^2+\alpha_{kk'}^2}{k'}, 2\alpha_{kk'}\right).
\end{aligned}
$$

The equality $(\star)$ follows from the following fact: if a divides bc, and $gcd(a,b) = d$, then a/d divides c. Let $a = gcd(gcd(n,k,2\alpha_{kk'}), \frac{n^2+\alpha_{kk'}^2}{k}), b = k'$, and $c = \frac{n^2+\alpha_{kk'}^2}{kk'}$. Then the since $gcd(a,b) = 1$, the claim says that a divides c, and a divides $gcd(n,k,2\alpha_{kk'})$ by definition. Therefore, a divides $gcd(gcd(n,k,2\alpha_{kk'}), \frac{n^2+\alpha_{kk'}^2}{kk'})$, and therefore must be less than or equal to this quantity. We have a priori that $gcd(gcd(n,k,2\alpha_{kk'}), \frac{n^2+\alpha_{kk'}^2}{kk'})$ is less than or equal to a, and therefore the result follows.

Since $\alpha_{kk'} \equiv \alpha_k (\text{mod } k)$ we have

$$
\frac{n^2+\alpha_{kk'}^2}{k} = \frac{n^2+(\alpha_k+\ell k)^2}{k} = \frac{n^2+\alpha_k^2}{k} + 2\alpha_k\ell + k\ell^2,
$$

with $\alpha_{kk'} = \alpha_k + \ell k$ for some ℓ (likewise for k'). Additionally, by construction, we must have $gcd(k, \alpha_{kk'}) = gcd(k, \alpha_k)$ (and likewise for k'). Continuing in the chain of equalities gives

$$
\begin{aligned}
gcd\left(n, kk', \frac{n^2+\alpha_{kk'}^2}{kk'}, \frac{n^2+(kk'-\alpha_{kk'})^2}{kk'}\right) &= gcd\left(gcd(n,k), \frac{n^2+\alpha_{kk'}^2}{k}, 2\alpha_{kk'}\right) \\
&\quad \times gcd\left(gcd(n,k'), \frac{n^2+\alpha_{kk'}^2}{k'}, 2\alpha_{kk'}\right) \\
&= gcd\left(n, k, \frac{n^2+\alpha_k^2}{k} + 2\alpha_k\ell, 2\alpha_k\right) \\
&\quad \times gcd\left(n, k', \frac{n^2+\alpha_{k'}^2}{k'} + 2\alpha_{k'}\ell', 2\alpha_{k'}\right) \\
&= gcd\left(n, k, \frac{n^2+\alpha_k^2}{k}, 2\alpha_k\right) \\
&\quad \times gcd\left(n, k', \frac{n^2+\alpha_{k'}^2}{k'}, 2\alpha_{k'}\right) \\
&= 1.
\end{aligned}
$$

The last equality follows from primitivity of the families $\mathcal{P}_{k,\alpha_k}, \mathcal{P}_{k',\alpha_{k'}}$. ■

This theorem gives us a way to generate all families of primitive integral root quadruples. For any choice of k (except those containing odd powers of primes congruent to 3 (mod 4)), one can find a family for the appropriate power of each prime factor of k, then compose these families using Theorem 9. Using reduction of n modulo these prime powers, one can determine which family to lift. Together with Theorem 3 and the classification of families corresponding

to $k = p^j$, this shows how to generate all primitive integral root quadruples. Moreover, this theorem implies the following claim: given a primitive root quadruple (a, b, c, d) with $a + b + c + d > 0$, the integer $a + b = k$ is a sum of two squares.

8 Congruence Relations

In this section we investigate a curious congruence relation satisfied by certain families $\mathcal{P}_{k,\alpha}$. We first recall the following result from [GLMWY]:

Theorem 10. *In any primitive integral Apollonian packing, the Descartes quadruples (mod 12) all fall in exactly one of four possible orbits. The first orbit $Y = Y_1$ (mod 12) consists of all permutations of*

$$\{(0, 0, 1, 1), \quad (0, 1, 1, 4), \quad (0, 1, 4, 9), \quad (1, 4, 4, 9), \quad (4, 4, 9, 9)\} \quad (mod\ 12).$$

The other three orbits are $Y_2 := (3, 3, 3, 3) - Y, Y_3 := (6, 6, 6, 6) + Y$, and $Y_4 := (9, 9, 9, 9) - Y (mod\ 12)$.

We note that by writing out all the elements in each orbit, we may determine in which orbit a given Descartes quadruple lies simply by checking any two entries of the quadruple (that is, any two entries of a Descartes quadruple determine the orbit in which it lies). With this, we may prove the following theorem.

Theorem 11. *Let $\mathcal{P}_{k,\alpha}$ denote any primitive family corresponding to the parameter k, with arbitrary admissible α, and assume that k and 12 are relatively prime. Then the family $\mathcal{P}_{k,\alpha}$ contains root quadruples in every orbit $Y_i, i = 1, 2, 3, 4$.*

Proof. Let $\mathcal{P}_{k,\alpha}$ be given by quadruples

$$\mathbf{x}_n = \left(-n, n + k, \frac{n^2 + kn + \alpha^2}{k}, \frac{n^2 + kn + (k - \alpha)^2}{k}\right)^T, \quad n \equiv n_k \pmod{k}.$$

Since the entries are given by polynomials in n, we have $\mathbf{x}_{n+12} \equiv \mathbf{x}_n \pmod{12}$. Since $n \equiv n_k \pmod{k}$, we have that n is of the form $n = km + n_k$, with $m \in \mathbb{Z}$. By coprimality of k and 12, as m ranges over $\mathbb{Z}$ (or, more precisely, as m ranges over $\mathbb{Z}/12\mathbb{Z}$), n will range over $\mathbb{Z}/12\mathbb{Z}$. Therefore, after rearranging quadruples mod 12, the elements of $\mathcal{P}_{k,\alpha}$ fall into the following congruence classes:

$$\begin{array}{l} (0, k, \ldots) \\ (11, k + 1, \ldots) \\ (10, k + 2, \ldots) \\ \vdots \\ (1, k + 11, \ldots) \end{array}$$

Since we may determine in which orbit a quadruple lies with only two entries, this information suffices.

Now, since k is relatively prime to 12, it must be congruent to $1, 5, 7$, or 11 (mod 12). Since we know that k must be a sum of two squares, it cannot be congruent to 3 (mod 4), and therefore the only congruence classes we need consider are $k \equiv 1 \pmod{12}$ and $k \equiv 5 \pmod{12}$. In each case, we have:

$$\begin{array}{ll} (0,1,\ldots) \in Y_1, & (0,5,\ldots) \in Y_4 \\ (11,2,\ldots) \in Y_2, & (11,6,\ldots) \in Y_2 \\ (10,3,\ldots) \in Y_3, & (10,7,\ldots) \in Y_3 \\ (8,5,\ldots) \in Y_4, & (4,1,\ldots) \in Y_1. \end{array}$$

Therefore, we see that if k and 12 are relatively prime, the family $\mathcal{P}_{k,\alpha}$ will contain at least one (indeed, infinitely many) elements in each orbit Y_i. ■

9 Acknowledgements

The results summarized in this paper were obtained during an REU at Columbia University during July 2011, which was funded by a grant in number theory held jointly by Columbia, NYU, and CUNY. The authors wish to thank Professor Dorian Goldfeld for sponsoring the project, as well as our graduate mentors Tim Heath, Karol Koziol, and Ian Whitehead for their generous dispensations of advice and knowledge.

References

[GLMWY] R.L. Graham, J.C. Lagarias, C.L. Mallows, A. Wilks, and C. Yan, "Apollonian Circle Packings: Number Theory," *J. Number Theory* **100** (2003), 1-45.