#A3 INTEGERS 24A (2024)

COMPUTING FOUR-TERM ARITHMETIC PROGRESSIONS OF POWERFUL NUMBERS

Michael A. Bennett[1]
Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada
bennett@math.ubc.ca

P.G. Walsh
Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada
gwalsh@uottawa.ca

Received: 8/8/23, Accepted: 3/3/24, Published: 5/27/24

Abstract

We describe our search for the smallest four-tuple of distinct relatively prime powerful numbers in arithmetic progression, which leads to the current "record" example involving integers with 111 decimal digits.

1. Introduction

In [2], Erdős asked "Are there infinitely many quadruples of relatively prime powerful numbers which form an arithmetic progression?". Here, a powerful number is a positive integer n with the property that if a prime $p \mid n$, then necessarily $p^2 \mid n$. Erdős' question was perhaps somewhat motivated by the fact that no four consecutive powerful numbers exist (and, indeed, it is conjectured that there are not even three consecutive powerful numbers). Recently, Bajpai, the first author and Chan [1] answered Erdős' question in the affirmative, describing an algorithm which produces infinitely many four-tuples of coprime integers in arithmetic progression. In particular, if we represent such a four-tuple as $\{N, N+d, N+2d, N+3d\}$, let

$$N = \alpha^3 x^2, \ N+d = \beta^3 y^2, \ N+2d = \gamma^3 z^2, \ N+3d = \delta^3 w^2, \tag{1.1}$$

be their representations as powerful numbers, with $\alpha, \beta, \gamma, \delta \in \mathbb{N}$, and call the sequence $[\alpha, \beta, \gamma, \delta]$ the *signature* of the four-tuple, one finds in [1] a method for constructing infinitely many four-tuples of signature $[1, 1, 1, 73]$, the smallest with 190 and 191 decimal digits for N and d, respectively.

DOI: 10.5281/zenodo.11352598

[1]Supported in part by a grant from NSERC

It is a natural question then to ask for the smallest example of a four-term arithmetic progression of coprime powerful numbers (which can theoretically be found through an exhaustive if impractically large search). In this paper, we will look for smaller examples, providing details of an analogous method which produces such solutions for other signatures. As the most essential ingredient in our approach is the group structure of an elliptic curve, it is not surprising that the examples found are strikingly large, and moreover, for this type of problem, finding larger solutions is relatively easy compared to finding smaller solutions. To this end, the computation we will describe has been successful in finding a solution with signature $[1, 3, 5, 7]$ having 111 digits, which is currently the smallest known example.

2. An Overview of the Computation

We begin with noting that the first three equations in (1.1) are equivalent to solving

$$\alpha^3 x^2 + \gamma^3 z^2 = 2\beta^3 y^2, \tag{1.2}$$

for a fixed triple of integers (α, β, γ). The complete set of integer solutions to such an equation is described in Theorem 4 of Chapter 7 of Mordell [3], which leads to explicit representations of (x, y, z) as values of quadratic forms

$$x = F_1(u, v),\ y = F_2(u, v),\ \text{ and }\ z = F_3(u, v),$$

where (F_1, F_2, F_3) range over a finite set of triples of forms in $\mathbb{Z}[u, v]$.

In order to achieve a powerful value for the fourth term in the arithmetic progression, one can exploit the relation $N + 3d = (N + 2d) + (N + d) - N$ together with the forms F_1, F_2, F_3. Defining

$$F(u, v) = \gamma^3 F_3(u, v)^2 + \beta^3 F_2(u, v)^2 - \alpha^3 F_1(u, v)^2,$$

the problem thus becomes one of solving

$$\delta^3 w^2 = F(u, v),$$

or equivalently

$$(\delta^2 w)^2 = \delta F(u, v). \tag{1.3}$$

The curve $Y^2 = \delta F(u, v)$ is a hyperelliptic curve of genus one, which we will refer to as H. If an integer solution (u_0, v_0) to $F(u_0, v_0) = \delta$ exists, one can use the point $P = (u_0, v_0)$ as a base point of the hyperelliptic curve in order to transform it into an elliptic curve, say E, given by a Weierstrass equation, along with explicit birational maps between H and E. The reader may wish to consult Section 5.3 of

[1] for an elucidation of this process. Otherwise, one can defer to the Magma code available at https://mysite.science.uottawa.ca/gwalsh/pwflprog.txt.

The problem remaining then is to find an integer point (Y, u, v) on H for which δ^2 divides Y. We will make heavy use of the arithmetic of E to carry this out. In particular, given E, the problem then turns to computing generators of either the full Mordell-Weil group of E over $\mathbb{Q}$, or a subgroup that will be sufficient in producing a point (Y, u, v) on H with δ^2 dividing Y. Once such generators are found, linear combinations of them are mapped to H and tested for the desired property.

3. Details of the Computation

Let us briefly explain some implementation issues that arise, and how we chose to deal with them. Firstly, a loop over (α, β, γ) involves only odd and squarefree positive integers α, β, and γ, as the powerful numbers in the arithmetic progression are necessarily odd, and squared factors can be subsumed in x, y, and z, respectively. Next, we remark that the issue of common factors among the values of F_1, F_2, and F_3 becomes an issue when solving (1.2), so instead, we simply solve the corresponding equation with $\alpha^3, \beta^3, \gamma^3$ replaced by α, β, γ, and make up for it at the end of the algorithm by looking for solutions (u, v) to $Y^2 = F(u, v)$ which give rise to x, y, z satisfying $\alpha \mid x$, $\beta \mid y$, and $\gamma \mid z$.

We then compute F from F_1, F_2, F_3 and loop over small values of $|u|$ and $|v|$ to produce a suitably small value δ, along with (u_0, v_0), for which $F(u_0, v_0) = \delta$. One needs to keep in mind that the final phase of the calculation will require δ^2 to divide Y, as mentioned above, thus δ should not be too large or else the computation will likely require going too far into the Mordell-Weil group, yielding a very large solution to the problem.

Once a suitable δ is computed, and thus a hyperelliptic curve H, and an elliptic curve E, one needs generators of E to work with. This is by far the most cumbersome aspect of our computation (and the one aspect that prevents it from being an actual algorithm.) Performing a descent on E is a useful tool for this, however anything beyond a two-descent does not offer any gain for various reasons. Moreover, a two-descent actually just means searching for points on H, as it is the cover of E which is pertinent to the situation at hand.

We therefore simply fix a reasonable height bound, search on H for rational points up to that bound, map those points to E, and proceed to computing linear combinations of those points, despite the fact that these image points will most often only generate a proper subgroup of $E(\mathbb{Q})$. The linear combinations are mapped back to H as triples (u, Y, v), and the testing of $\delta^2 \mid Y$, $\alpha \mid x$, $\beta \mid y$, $\gamma \mid z$, with

$x = F_1(u, v)$, $y = F_2(u, v)$, and $z = F_3(u, v)$, then determines if the method has found a solution or not.

4. Results of Our Search

We ran the above computation with a certain measure of success, although it became abundantly clear that finding generators for $E(\mathbb{Q})$, or a suitable subgroup thereof, stood in the way of solving the problem for most triples (α, β, γ), and even when generators for a suitable subgroup of $E(\mathbb{Q})$ were found, the condition of having δ^2 to divide the coordinate Y of a point (u, Y, v) on H was indeed quite difficult to satisfy. In the end, the algorithm was successful in finding quadruples of coprime powerful numbers of signature $[1, 1, 1, \delta]$ for $\delta \in \{73, 193, 241, 409, 601, 1081\}$, and also of signature $[1, 3, 5, 7]$. Despite this rather disappointing outcome, we can report that the smallest quadruple with signature $[1, 3, 5, 7]$ has integers with only 111 digits, a considerable improvement on the previous record of 190 digits. Specifically, the quadruple is given by N and common difference d with

$N = 146027586840764992443268586116964792396346300745498996983761221282$8
$540606013909295321624865120723200734824296$41
and
$d = 702453477383069580332301713710563864348279545538648197419441572715$64
$3523112871409665830011383050794330313832$42.

5. Near Misses

It is not especially difficult to find examples of four-term arithmetic progressions that almost possess the properties we desire. Indeed, if we relax the constraint that the terms be coprime, then four-term progressions of powerful numbers are relatively abundant. If we assume that N and $N + d$ are powerful, it follows that $\gcd(d, N)$ is also powerful and so the smallest such common factor exceeding 1 corresponds to $\gcd(d, N) = 4$. The smallest example of a four-term arithmetic progression of powerful numbers $\{N, N + d, N + 2d, N + 3d\}$ with $\gcd(d, N) = 4$ is given by $N = 2704 = 2^4 \cdot 13^2$ and $d = 36284$. In Table 1, we list *primitive* examples of four term progressions with $\gcd(d, N) < 100$ and $N + 3d < 10^9$. We call a four-tuple $\{N, N + d, N + 2d, N + 3d\}$ *primitive* if there does not exist an integer $t > 1$ with the property that each of $N/t, (N + d)/t, (N + 2d)/t$ and $(N + 3d)/t$ is a powerful positive integer.

d	N	$\gcd(d,N)$
36	$2^2 \cdot 3^2$	36
5782	7^3	49
828	$2^2 \cdot 3^3 \cdot 5^2$	36
36284	$2^4 \cdot 13^2$	4
330732	$2^4 \cdot 311^2$	4
22744836	$2^2 \cdot 3^2 \cdot 5^3 \cdot 47^2$	36
923045724	$2^2 \cdot 3^3 \cdot 23^2 \cdot 73^2$	36

Table 1: Primitive examples with small gcd

In a different direction, if we slightly relax the assumption that all four of our terms in progression are powerful, we can find, by way of example, a 43-digit example of a four term arithmetic progression of coprime integers which are all powerful except only that one of the four numbers is properly divisible by 2. This example is determined as above by N and d, whose values are

$$N = 1074491897493407528245506048484101277342291 \quad \text{and}$$
$$d = 2619517172625777613796518738959883071 1169167.$$

Here, we have
$$N = 11^2 \cdot 19^3 \cdot 777309457^2 \cdot 1463809409^2$$
$$N + d = 2 \cdot 1302292723^2 \cdot 2835412690499^2$$
$$N + 2d = 3^4 \cdot 5^4 \cdot 431^2 \cdot 232451447^2 \cdot 324371041^2$$
$$N + 3d = 2^{10} \cdot 7^3 \cdot 157^2 \cdot 229^2 \cdot 5647^2 \cdot 8167^2 \cdot 9082547^2.$$

6. Concluding Remarks

It is entirely possible that the example corresponding to signature $[1, 3, 5, 7]$, given at the end of Section 4, is actually the minimal one for this problem. To prove this would require careful analysis of the quadratic forms arising from a given signature $[\alpha, \beta, \gamma, \delta]$, and generators for corresponding elliptic curves E.

References

[1] P. Bajpai, M.A. Bennett, and T.H. Chan, Arithmetic progressions in squarefull numbers. *Int. J. Number Theory* **20** (2024), 19–45.

[2] P. Erdős, Problems and results on number theoretic properties of consecutive integers and related questions, *Proceedings of the Fifth Manitoba Conference on Numerical Mathematics* (Univ. Manitoba, Winnipeg, Man., 1975), Congress. Numer. XVI , *Utilitas Math.*, (1976), 25–44.

[3] L.J. Mordell, *Diophantine Equations*, Academic Press, London, 1969.