Irish Math. Soc. Bulletin
Number 77, Summer 2016, 45–49
ISSN 0791-5578

A PROBLEM OF DIOPHANTUS MODULO A PRIME

JOSHUA HARRINGTON AND LENNY JONES

Abstract. A set S of $k \geq 2$ positive rational numbers is called a *rational Diophantine k-tuple* if the product of any two elements of S increased by 1 is a perfect square. Around the third century A.D., Diophantus found infinitely many rational Diophantine triples, and very recently, Dujella, Kazalicki, Mikić and Sziksza have proven the existence of infinitely many rational Diophantine sextuples. It is still unknown whether there exist any rational Diophantine septuples. In this note, we investigate this problem in $\mathbb{Z}_p$, the field of integers modulo a prime p, where the situation is quite different. We show, given any set S of $k \geq 2$ positive integers, that there exist infinitely many primes p such that all elements of S are nonzero squares modulo p, and furthermore, that the product of any t elements of S, where $1 \leq t \leq k$, increased by 1 is also a nonzero square modulo p.

1. Introduction

In Problem 19 of Book IV of the Arithmetica [7], Diophantus asked:

> *To find three numbers indeterminately such that the product of any two increased by 1 is a square.*

He provided the solution

$$\{x, \quad x+2, \quad 4x+4\}, \tag{1}$$

and he outlined a procedure using (1) to construct 4-element sets of positive rational numbers such that the product of any two increased by 1 is a square. As an example, he gave

$$\left\{\frac{1}{16}, \quad \frac{33}{16}, \quad \frac{17}{4}, \quad \frac{105}{16}\right\}.$$

In the literature, k-element sets S of positive rational numbers, such that the product of any two increased by 1 is a square, are generally

2010 *Mathematics Subject Classification.* 11A07, 11A15.
Key words and phrases. Diophantus, congruence, quadratic reciprocity.
Received on 12-12-2015.

referred to as *rational Diophantine k-tuples*, or simply *Diophantine k-tuples* if all the elements of S are integers. Since the time of Diophantus, many mathematicians have searched for rational Diophantine k-tuples and Diophantine k-tuples, where $k \geq 5$. Very recently, Dujella, Kazalicki, Mikić and Sziksza [4] have proven that there exist infinitely many rational Diophantine sextuples, but it is still unknown whether any rational Diophantine septuples exist. If a certain conjecture of Lang [1] is true, then there exists an upper bound on k for the existence of a rational Diophantine k-tuple. Along these lines, Dujella [3] has shown unconditionally that no Diophantine sextuple exists, and that there are at most finitely many Diophantine quintuples. Although it is still unknown as to whether a single Diophantine quintuple exists, more recent work [5, 6, 10] suggests that the answer is most likely negative. In this note, we investigate this problem in the finite field of integers modulo a prime p, which we denote as $\mathbb{Z}_p$. We see that the situation is quite different in this setting. More precisely, we prove the following theorem.

Theorem 1.1. *Let $k \geq 2$ be a fixed integer, and let S be any set of k positive integers. Then there exist infinitely many primes p for which each element of S is a nonzero square modulo p, and furthermore, that 1 plus the product of any t elements of S, where $1 \leq t \leq k$, is also a nonzero square modulo p.*

Throughout this note, we say that a set S *has property* $\mathcal{D}$ if S satisfies the conditions in the statement of Theorem 1.1.

2. Preliminary Material

To help establish Theorem 1.1, we recall some ideas from number theory. A *quadratic residue* modulo the prime p is a nonzero element $a \in \mathbb{Z}_p$ such that there exists $x \in \mathbb{Z}_p$ with $x^2 \equiv a \pmod{p}$. In other words, a quadratic residue is a nonzero square in $\mathbb{Z}_p$. For any integer a and any prime p, we define the *Legendre symbol* as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo the prime } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo the prime } p \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases} \tag{2}$$

It is easy to see from (2) that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right), \tag{3}$$

for any integers a and b. Although there are many celebrated theorems concerning the Legendre symbol, we require only two of the more well-known results, which we state without proof.

Proposition 2.1. [8] *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = 1 \quad \textit{if and only if} \quad p \equiv \pm 1 \pmod 8.$$

The next remarkable theorem is due to Gauss [8].

Theorem 2.2 (Law of Quadratic Reciprocity)**.** *Let p and q be odd primes. Then*

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{(p-1)(q-1)/4}.$$

Finally, we need a theorem due to Dirichlet [8].

Theorem 2.3 (Dirichlet's Theorem of Primes in an Arithmetic Progression)**.** *Let r and m be positive integers with* $\gcd(r, m) = 1$*. Then there exist infinitely many positive integers n such that $mn + r$ is prime.*

Remark 2.4. In other words, according to Theorem 2.3, if $\gcd(r, m) = 1$, then there are infinitely many primes p such that $p \equiv r \pmod m$.

3. Proof of Theorem 1.1

We are now in a position to give a proof of Theorem 1.1.

Proof of Theorem 1.1. Let L be the largest element of S, and let $m = 8\prod_{q_i \in Q} q_i$, where Q is the set of all odd primes $q_i \leq L! + 1$. By Theorem 2.3, there exist infinitely many primes $p \equiv 1 \pmod m$. Since $p \equiv 1 \pmod 8$, it follows from Proposition 2.1 and Theorem 2.2 that $\left(\frac{q_i}{p}\right) = 1$ for each $q_i \in Q$. Let t be any integer with $1 \leq t \leq k$, and let s be the product of any t elements from S. Since $s < L! + 1$, all prime factors of s and $s + 1$ are contained in Q. In particular, no element of S is divisible by p. Hence, by (3), it follows that $\left(\frac{s}{p}\right) = \left(\frac{s+1}{p}\right) = 1$. Therefore, the set S has property $\mathcal{D}$, and the proof is complete. □

4. An Example and Some Open Questions

As an illustration of Theorem 1.1, we provide the following example.

Example 4.1. Let $k = 4$. Recall the sequence of Fibonacci numbers (F_n) defined as

$$F_0 = 0, \quad F_1 = 1, \quad \text{and} \quad F_n = F_{n-1} + F_{n-2} \quad \text{for } n \geq 2.$$

Let $S = \{F_2, F_3, F_4, F_5\} = \{1, 2, 3, 5\}$. According to the method described in the proof of Theorem 1.1, we get in this situation that

$$Q = \{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, \\ 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113\},$$

$$m = 126440218561670431152580825166174649973098747960,$$

and the smallest prime $p \equiv 1 \pmod{m}$ is

$$p = 10115217484933634492206466013293971997847899836 81.$$

Then S has property $\mathcal{D}$ since all elements of the set

$$\{1, 2, \ldots, 121 = F_5! + 1\}$$

are quadratic residues modulo p.

Remark 4.2. Call a Diophantine t-tuple $\mathcal{T}$ a *Fibonacci Diophantine t-tuple* if all elements of $\mathcal{T}$ are Fibonacci numbers. It is easy to show that the only Fibonacci Diophantine triple $\mathcal{T}$ containing $F_1 = F_2 = 1$ is $\mathcal{T} = \{1, 3, 8\}$ [9]. If the smallest index in $\mathcal{T}$ is larger than 1, then it is conjectured that all such Fibonacci Diophantine triples are of the form $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$. Dujella [2] has shown that if $\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$ is a Diophantine 4-tuple, where $k \geq 1$, then d cannot be a Fibonacci number. This fact, combined with the truth of the aforementioned conjecture, would establish that no Fibonacci Diophantine 4-tuples exist.

To conclude, we raise a couple of questions.

Question 1. *For each $k \geq 2$, what is the smallest prime p such that a set S with exactly k elements exists with property $\mathcal{D}$?*

The answer to Question 1 for $k = 4$ is $p = 41$, which is achieved using $S = \{1, 4, 8, 9\}$.

Question 2. *For each $k \geq 2$, does there exist a natural number N_k such that for all primes $p > N_k$, there exists a set S with k elements that has property $\mathcal{D}$?*

References

[1] D. Abramovich, J. Felipe, *Lang's conjectures, fibered powers, and uniformity*, New York J. Math. **2** (1996), 20–34, electronic.

[2] A. Dujella, *A proof of the Hoggatt-Bergum conjecture*, Proc. Amer. Math. Soc. **127** (1999), 1999–2005.

[3] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[4] A. Dujella, M. Kazalicki, M. Mikić and M. Sziksza, *There are infinitely many rational Diophantine sextuples*, arXiv:1507.00569.

[5] C. Elsholtz, A. Filipin and Y. Fujita, *On Diophantine quintuples and D(-1)-quadruples*, Monatsh. Math. **175** (2014), no. 2, 227–239.

[6] A. Filipin and Y. Fujita, *The number of Diophantine quintuples II*, Publ. Math. Debrecen **82** (2013), no. 2, 293–308.

[7] T. L. Heath, *Diophantus of Alexandria: A study in the history of Greek algebra, Second edition*, With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler, Dover Publications, Inc., New York (1964) viii+387 pp.

[8] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Math., vol. 84, 2nd ed., Springer, New York, 1990.

[9] N. Robbins, *Fibonacci and Lucas numbers of the forms $w^2 1$, $w^3 1$*, Fibonacci Quart. **19** (1981), no. 4, 369–373.

[10] W. Wu and B. He, *On Diophantine quintuple conjecture*, Proc. Japan Acad. Ser. A Math. Sci. **90** (2014), no. 6, 84–86.

Joshua Harrington is currently a professor of mathematics at Cedar Crest College. His research interests include number theory and combinatorics. He is especially interested in problems involving the irreducibility of polynomials as well as covering systems of the integers.

Lenny Jones is currently a professor of mathematics at Shippensburg University. His research interests include algebra, number theory and combinatorics, and especially problems that simultaneously involve all three of these areas.

(Joshua Harrington) Department of Mathematics, Cedar Crest College, Pennsylvania USA

(Lenny Jones) Department of Mathematics, Shippensburg University, Pennsylvania USA

E-mail address: Joshua.Harrington@cedarcrest.edu, lkjone@ship.edu