DOES $XY^2 = Z^2$ IMPLY X IS A SQUARE?

JACK S. CALCUT

1. Introduction

Ordinary integers have the property that if the product of a number and a square is a square, then the number itself is a square. That is, if

$$XY^2 = Z^2 \neq 0 \tag{1}$$

where $X, Y, Z \in \mathbb{Z}$, then $X = W^2$ for some $W \in \mathbb{Z}$. This property is at the heart of the age old question: *is $\sqrt{2}$ a rational number?* If so, then $2q^2 = p^2$ for some nonzero integers p and q. The property now implies that 2 is a square in $\mathbb{Z}$, a contradiction. A similar argument shows that only the square integers have rational square roots.

The aforementioned property of positive integers $\mathbb{Z}^+$ was known to Euclid. Proposition 22 in book VIII of Euclid's Elements [2, p. 379] states that *if three numbers be in continued proportion, and the first be a square, the third will also be a square.* That is, if $a, b, c \in \mathbb{Z}^+$, $a : b : c$ and $a = d^2$ for some $d \in \mathbb{Z}^+$, then $c = e^2$ for some $e \in \mathbb{Z}^+$. The continued proportion $a : b : c$ means $a/b = b/c$ or $ca = b^2$. Therefore, Euclid's Proposition 22 is equivalent to: if $c, d, b \in \mathbb{Z}^+$ and $cd^2 = b^2$, then $c = e^2$ for some $e \in \mathbb{Z}^+$.

This note explores the above property in general rings. Let R be a ring. A *square* in R is an element $X \in R$ such that $X = W^2$ for some $W \in R$. An *apparent square* in R is an element $X \in R$ such that equation (1) holds for some $Y, Z \in R$. Therefore, in $\mathbb{Z}$ every apparent square is a square (we prove this fact below). Note that we naturally require $Z^2 \neq 0$ in equation (1) as otherwise every element in R is trivially an apparent square with $Y = Z = 0$.

This note investigates the following potential properties of a fixed ring R or multiplicative group G.

Property I. *If $a, b, c \in R$ and $a \cdot b^2 = c^2 \neq 0$, then there exists an element $d \in R$ such that $a = d^2$.*

Property II. *If $a, b, c \in G$ and $a \cdot b^2 = c^2$, then there exists an element $d \in G$ such that $a = d^2$.*

One may further require that the choice of d is natural and not arbitrary. We will say more about this below.

Date: May 12, 2008.

The author was led in [1] to consider Property I for rings of integers in certain quadratic extension fields of $\mathbb{Q}$. The general question of which rings and groups possess Properties I and II then suggested itself.

A key point is that the ring R or group G is fixed and the square root d of a is required to lie in R or G respectively. Solutions to an equation depend heavily on domain assumptions. For example, take the equation $x^2+1=0$ and consider the different solution sets when $x \in \mathbb{R}$, $x \in \mathbb{C}$ and $x \in \mathbb{H}$ (the real quaternions).

2. Property I

We begin with a positive class of examples that includes $\mathbb{Z}$ and many polynomial rings.

Proposition 1. *Each unique factorization domain R possesses Property I.*

Recall that an *integral domain* R is a commutative ring with $1_R \neq 0_R$ and without zero divisors. A *unique factorization domain* (UFD) is an integral domain R such that every nonzero nonunit of R is the product of finitely many irreducibles of R and, moreover, this product is unique up to order and multiplication by units (i.e. invertible elements). In a UFD, primes and irreducibles coincide.

Proof. Suppose that $a \cdot b^2 = c^2 \neq 0$. Plainly $a, b, c \neq 0$. If b is a unit, then $a = \left(cb^{-1}\right)^2$. Otherwise, b and c are nonzero nonunits. Let $b = p_1 p_2 \cdots p_k$ and $c = q_1 q_2 \cdots q_l$ be factorizations into irreducibles. We have

$$a \cdot (p_1 p_2 \cdots p_k)^2 = (q_1 q_2 \cdots q_l)^2 .$$

By uniqueness of factorizations into irreducibles, p_1 is a unit multiple of some q_i. Reindex so that $p_1 = u_1 q_1$ for some unit u_1. We have

$$a \cdot p_1^2 (p_2 p_3 \cdots p_k)^2 = (u_1 q_1)^2 \left(u_1^{-1} q_2 q_3 \cdots q_l\right)^2$$

and so by cancellation (which holds in any integral domain)

$$a \cdot (p_2 p_3 \cdots p_k)^2 = \left(u_1^{-1} q_2 q_3 \cdots q_l\right)^2 .$$

Repeat this process (informal induction on k) to obtain

$$a = \left(u_1^{-1} u_2^{-1} \cdots u_k^{-1} q_{k+1} q_{k+2} \cdots q_l\right)^2$$

as desired. □

The previous result is natural since in the field of fractions of R we have

$$u_1^{-1} u_2^{-1} \cdots u_k^{-1} q_{k+1} q_{k+2} \cdots q_l = \frac{c}{b}.$$

Another positive class of examples is as follows. A *number field* K is a subfield of $\mathbb{C}$ that is a finite dimensional field extension of $\mathbb{Q}$. If K is a number field, then the *ring of integers* of K is the set $\mathcal{O}_K$ of all roots in K of monic polynomials in $\mathbb{Z}[x]$. Any such ring of integers is an integral domain since it is a subring of $\mathbb{C}$ (see [6, §2.3]). For example, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ which explains the terminology 'rational integers' for $\mathbb{Z}$. The following was proved in [1].

Proposition 2. *If K is a number field, then $\mathcal{O}_K$ possesses Property I.*

Proof. Suppose that $a, b, c \in \mathcal{O}_K$ are nonzero and $a \cdot b^2 = c^2$. The polynomial $x^2 - a \in \mathcal{O}_K[x]$ has the root $c/b \in K$. Therefore c/b is integral over $\mathcal{O}_K$. The ring of integers $\mathcal{O}_K$ is integrally closed (see [1]) and so $c/b \in \mathcal{O}_K$. Hence $a = c^2/b^2 = (c/b)^2$ where $c/b \in \mathcal{O}_K$. □

The previous proposition is natural as well since c/b was a square root. This proposition applies to the Gaussian integers $\mathbb{Z}[i]$ since they are the ring of integers for $K = \mathbb{Q}(i)$. However, this is not very interesting since the Gaussian integers are a UFD. More interesting is the application with $K = \mathbb{Q}\left(\sqrt{D}\right)$ where, say, $D = -5, -6, 10, 15$ since $\mathcal{O}_K$ lacks unique factorization for these and many other values of D [6, §4.4].

Recall that a *division ring* R is a ring with $1_R \neq 0_R$ such that every nonzero element is a unit. A *field* is a commutative division ring. Every field has Property I naturally since $a \cdot b^2 = c^2 \neq 0$ implies that $a = \left(cb^{-1}\right)^2$. By Wedderburn's theorem, every finite division ring is a field and hence has Property I. A trivial observation is that if R is a ring in which every element has a square root in R, then R has Property I. However, Property I is not equivalent to the existence in R of a square root for each element of R as shown by the Gaussian integers.

Corollary 1. *The noncommutative division ring $\mathbb{H}$ of real quaternions has Property I.*

Proof. We show that every quaternion has a square root in $\mathbb{H}$. Given $A + Bi + Cj + Dk \in \mathbb{H}$, we solve

$$A + Bi + Cj + Dk = (a + bi + cj + dk)^2 = a^2 - b^2 - c^2 - d^2 + 2abi + 2acj + 2adk$$

for $a, b, c, d \in \mathbb{R}$. This is a system of four equations

$$\begin{aligned} A &= a^2 - b^2 - c^2 - d^2, \\ B &= 2ab, \\ C &= 2ac \quad \text{and} \\ D &= 2ad. \end{aligned}$$

The reader may show that this system always has one or more real solutions. □

The reasoning in the previous proof using the trivial observation above is not natural since the square root is chosen arbitrarily. For example, in $\mathbb{H}$ we have

$$(-1)\left(\frac{i}{\sqrt{2}} + \frac{j}{\sqrt{2}}\right)^2 = (-1)^2. \tag{2}$$

The trivial observation concludes that -1 is a square in $\mathbb{H}$ but only since -1 is known to have a square root in $\mathbb{H}$ which one could take to be $(i + j + k)/\sqrt{3}$ for instance. However, equation (2) is naturally suggesting that the square root of -1 be $(i + j)/\sqrt{2}$ since

$$-1 = \frac{(-1)(-1)}{\left(i/\sqrt{2} + j/\sqrt{2}\right)\left(i/\sqrt{2} + j/\sqrt{2}\right)} = \left(\frac{i + j}{\sqrt{2}}\right)^2. \tag{3}$$

In this example, the -1 on the right hand side of equation (2) was chosen to lie in the center of $\mathbb{H}$ so that equation (2) could be manipulated as in equation (3). In general, we argue that there is not always a natural choice of square root of a as

follows. In $\mathbb{H}$ we have $1 \cdot i^2 = j^2$. On one hand $1 \cdot (-1) = -1$ implies $1 = (-1)^2$ and so -1 suggests itself as a square root of 1. On the other hand j and $-i$ anticommute so

$$1 = jji^{-1}i^{-1} = jj\,(-i)\,(-i) = -\,(-ji)\,(-ji) = -kk = -k^2$$

and the minus sign prevents a natural choice of a square root of 1.

Let $\mathbb{H}_{\mathbb{Q}}$ denote the division ring of quaternions with rational coefficients.

Proposition 3. *The division ring $\mathbb{H}_{\mathbb{Q}}$ does not possess Property I.*

Proof. Notice that $2 \cdot i^2 = (i+j)^2$. However, 2 has no square root in $\mathbb{H}_{\mathbb{Q}}$ as is easily shown using the system of four equations in the proof of Corollary 1. □

It is easy to produce lots of finite rings R that do not have Property I. Let $R = \mathbb{Z}/2n\mathbb{Z}$ where $n > 1$ is odd. The reader may verify that $[n]^2 = [n]$ and that $[2n-1] \cdot [n]^2 = [n]^2$. So, if $2n-1$ is not a quadratic residue modulo $2n$, then $\mathbb{Z}/2n\mathbb{Z}$ does not have Property I. This occurs for many values of n including $n = 3, 7, 9, 11, 15, 19, 21$ and so forth.

Another negative example is the integral domain $\mathbb{Z}[2i]$. Here we have $-1 \cdot 2^2 = (2i)^2$, however -1 is not a square in $\mathbb{Z}[2i]$. This is caused by the fact that $\mathbb{Z}[2i]$ is not integrally closed and is 'missing' some integers such as i.

3. Property II

If R is a ring, then let $R^* = R - \{0_R\}$. If R is a division ring, then R^* is a multiplicative group. Therefore, all of the results concerning division rings in the previous section yield analogous results for groups and Property II. For instance, if $p > 0$ is prime, then $\mathbb{Z}_p^*$ has Property II. As inverses exist in a group, any abelian group G has Property II naturally in the same way that a field has Property I. The more interesting cases concern nonabelian groups.

Proposition 4. *The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ has Property II.*

Proof. The only squares in Q_8 are ± 1, so $a \cdot b^2 = c^2$ implies $a = \pm 1$ and $a = 1^2$ or $a = i^2$. □

As with $\mathbb{H}$ in the previous section, Q_8 has Property II but the choice of square root is not always natural.

Proposition 5. *The free group $F_2 = \langle x, y \rangle$ of rank 2 does not have Property II.*

Proof. We have $(xyyx)(y)^2 = (xyy)^2$ and we will show that $xyyx$ is not a square in F_2. Suppose by way of contradiction that $xyyx = w^2$ for some freely reduced word $w \in F_2$. Then ww freely reduces to $xyyx$. Free reduction in ww is only possible directly in the middle. Therefore w begins and ends with x. But then ww is already freely reduced and contains xx, whereas $xyyx$ does not. This contradicts uniqueness of freely reduced form. □

The same proof shows that a free group of rank 2 or greater does not have Property II.

Here is another proof of the previous proposition. Felix Klein's ping-pong lemma may be used to prove that

$$X = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ and } Y = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

generate a free subgroup $\langle X, Y \rangle$ of rank 2 in $\mathrm{SL}_2(\mathbb{Z})$ (see [5]). In other words $\varphi : F_2 \to \mathrm{SL}_2(\mathbb{Z})$ given by $\varphi(x) = X$ and $\varphi(y) = Y$ is an injective homomorphism. We have $(XYYX)(Y)^2 = (XYY)^2$ and

$$XYYX = \begin{bmatrix} 9 & 20 \\ 4 & 9 \end{bmatrix}.$$

It is easy to solve directly for $a, b, c, d \in \mathbb{Z}$ in the four equations coming from

$$\begin{bmatrix} 9 & 20 \\ 4 & 9 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^2$$

and obtain the only square roots of $XYYX$ in $\mathrm{GL}_2(\mathbb{Z})$, namely

$$\pm D = \pm \begin{bmatrix} 2 & 5 \\ 1 & 2 \end{bmatrix}.$$

However, $\det(\pm D) = -1$ and $\pm D \notin \langle X, Y \rangle \subset \mathrm{SL}_2(\mathbb{Z})$. Therefore, $XYYX$ has no square root in $\langle X, Y \rangle$ as desired. This approach shows that an element g of a group G may not have a square root in G but there may exist an injective homomorphism $\varphi : G \to H$ such that $\varphi(g)$ does have a square root in H. In fact, there is a quite general procedure due to B. H. Neumann for the adjunction of roots to a group [4, pp. 49-50, 189].

References

[1] Jack S. Calcut, *Grade School Triangles,* preprint, 2008.

[2] Euclid, *The Thirteen Books of The Elements, Vol. 2 (Books III–IX),* Dover Publications, Inc., New York, translated by Sir Thomas L. Heath, 1956.

[3] Thomas W. Hungerford, *Algebra,* Springer-Verlag, New York, 1974.

[4] Roger C. Lyndon and Paul E. Schupp, *Combinatorial Group Theory,* Springer-Verlag, Berlin, 1977.

[5] D. S. Passman, *Free Subgroups in Linear Groups and Group Rings,* Contemporary Math., to appear.

[6] Ian Stewart and David Tall, *Algebraic Number Theory and Fermat's Last Theorem, Third Edition,* A K Peters, Ltd., Natick, MA, 2002.

4201 Great Plains Drive, Austin, TX 78735-6005

E-mail address: jack@math.utexas.edu

URL: http://www.ma.utexas.edu/users/jack/