A Cubic Analogue of the Jacobsthal Identity

Heng Huat Chan, Ling Long, and YiFan Yang

Abstract. It is well known that if p is a prime such that $p \equiv 1 \pmod 4$, then p can be expressed as a sum of two squares. Several proofs of this fact are known and one of them, due to E. Jacobsthal, involves the identity $p = x^2 + y^2$, with x and y expressed explicitly in terms of sums involving the Legendre symbol. These sums are now known as the Jacobsthal sums. In this short note, we prove that if $p \equiv 1 \pmod 6$, then $3p = u^2 + uv + v^2$ for some integers u and v using an analogue of Jacobsthal's identity.

1. INTRODUCTION. The following theorem is well known:

Theorem 1.1. *If p is a prime such that $p \equiv 1 \pmod 4$ then*

$$p = x^2 + y^2 \tag{1.1}$$

for some integers x and y.

Theorem 1.1 was first observed independently by A. Girard (1595–1632) and P. de Fermat (1601–1665) (see [**5**, p. 14]). A complete proof of Theorem 1.1 appears to have been first obtained by L. Euler (1707–1783) (see [**3**, pp. 7–12]). Since then, many different proofs of this result have been discovered, one of which is due to E. Jacobsthal.

To describe Jacobsthal's proof, we introduce the Legendre symbol. Let p be an odd prime. An integer a relatively prime to p is said to be a *quadratic residue* modulo p if the congruence $x^2 \equiv a \pmod p$ is solvable in integers; otherwise, it is called a *quadratic nonresidue*. The *Legendre symbol* is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p. \end{cases}$$

Around 1907, E. Jacobsthal (see [**8**]) proved Theorem 1.1 using the identity [**1**]:

$$p = \left\{\frac{1}{2}\sum_{\alpha=1}^{p-1}\left(\frac{\alpha^3+\alpha}{p}\right)\right\}^2 + \left\{\frac{1}{2}\sum_{\alpha=1}^{p-1}\left(\frac{\alpha^3+a\alpha}{p}\right)\right\}^2, \tag{1.2}$$

where the integer a is any quadratic nonresidue modulo p.

The relation (1.1) can be interpreted as the factorization of the number p as a product of elements $(x + iy)$ and $(x - iy)$ in $\mathbf{Z}[i]$, where $i = \sqrt{-1}$. If we replace i and $p \equiv 1 \pmod 4$ by $\omega = e^{\pi i/3}$ and $p \equiv 1 \pmod 6$ respectively, then it is known that p is a product of $(x + \omega y)$ and $(x + \overline{\omega} y)$, where $x, y \in \mathbf{Z}$ and $\overline{\omega}$ denotes the complex conjugate of ω. Equivalently, we have the following theorem.

doi:10.4169/amer.math.monthly.118.04.316

Theorem 1.2. *If p is a prime such that $p \equiv 1 \pmod 6$ then*

$$p = x^2 + xy + y^2 \tag{1.3}$$

for some integers x and y.

Theorem 1.2 is clearly a cubic analogue[1] of Theorem 1.1 and it can be proved using Euler's ideas in his proof of Theorem 1.1. A natural question is to ask for a cubic analogue of (1.2). After several attempts, we were led to a possible generalization of (1.2), which we now describe.

Let $\Delta(A, B, C) = B^2 - 4AC$ be the discriminant of the binary quadratic form

$$f(x, y) = Ax^2 + Bxy + Cy^2.$$

We first observe that (1.2) can be expressed as

$$|\Delta(1, 0, 1)|p = 4p = \left\{\sum_{\alpha=1}^{p}\left(\frac{\alpha^3+\alpha}{p}\right)\right\}^2 + \left\{\sum_{\alpha=1}^{p}\left(\frac{\alpha^3+a\alpha}{p}\right)\right\}^2. \tag{1.4}$$

With this interpretation of (1.2), we have the following analogue:

Theorem 1.3. *Let $p \equiv 1 \pmod 6$. Suppose that a is any integer such that $x^3 \equiv a \pmod p$ is not solvable. Then*

$$|\Delta(1, 1, 1)|p = 3p = x^2 + xy + y^2, \tag{1.5}$$

with

$$x = \sum_{\alpha=1}^{p}\left(\frac{\alpha^3+1}{p}\right) \quad \textit{and} \quad y = \left(\frac{a}{p}\right)\sum_{\alpha=1}^{p}\left(\frac{\alpha^3+a}{p}\right).$$

2. THE GAUSS SUMS.

Let p be a prime number and $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ be the finite field of p elements. In particular, $\mathbf{F}_p^*$, the set of invertible elements in $\mathbf{F}_p$, is a cyclic group of order $p-1$ under multiplication. An integer g is a *primitive root* modulo p if g generates the cyclic group $\mathbf{F}_p^*$. A (multiplicative) character χ of $\mathbf{F}_p^*$ (or modulo p) is a group homomorphism from $\mathbf{F}_p^*$ to $\mathbf{C}^*$, the set of nonzero complex numbers. Namely, for any nonzero elements $\alpha, \beta \in \mathbf{F}_p$, $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$. The image $\chi(\mathbf{F}_p^*)$ is a finite cyclic subgroup of $\mathbf{C}^*$ whose cardinality is called the *order* of the character χ. By convention, $\chi(0) = 0$.

Example 2.1. The assignment $\chi(\alpha) = 1$ for all $\alpha \in \mathbf{F}_p^*$ is an order-1 character, called the *principal character* modulo p.

Example 2.2. The Legendre symbol defined on $\mathbf{Z}$ in Section 1 is periodic with period p and can be viewed as an order-2 character (or a *quadratic character*) on $\mathbf{F}_p^*$ when p is an odd prime. Note that this character is the only character of order 2 on $\mathbf{F}_p^*$ because a character of order 2 must take value -1 at a primitive root g, and the assigment $g \mapsto -1$ completely determines this character.

[1]The word "cubic" refers to the fact that the binary quadratic form $x^2 + xy + y^2$ factors over the field generated by the cube root of unity.

For convenience, we shall adopt the following notation.

Notation 2.1. When we write (α^{-1}/p), we view α^{-1} as the inverse of α in $\mathbf{F}_p^*$. Furthermore, we will replace

$$\sum_{\alpha=1}^{p-1} \quad \text{by} \quad \sum_{\alpha\in\mathbf{F}_p^*} \quad \left(\text{or simply } \sum_{\alpha}{}^{*}\right)$$

and

$$\sum_{\alpha=1}^{p} \quad \text{by} \quad \sum_{\alpha\in\mathbf{F}_p} \quad \left(\text{or simply } \sum_{\alpha}\right).$$

The following well-known lemma about characters will be used later in this article.

Lemma 2.3. *If χ is a nonprincipal character of $\mathbf{F}_p^*$, then*

$$\sum_{\alpha} \chi(\alpha) = 0.$$

Proof. As the character χ is nonprincipal, there exists $\beta \in \mathbf{F}_p^*$ such that $\chi(\beta) \neq 1$. Also, the map that sends $\alpha \mapsto \alpha\beta$ is one-to-one on $\mathbf{F}_p$, and is therefore a bijection since $\mathbf{F}_p$ is finite. Consequently,

$$\sum_{\alpha} \chi(\alpha) = \sum_{\alpha} \chi(\alpha\beta) = \left(\sum_{\alpha} \chi(\alpha)\right) \chi(\beta).$$

This implies $\left(\sum_{\alpha} \chi(\alpha)\right)(1 - \chi(\beta)) = 0$. By our choice of β, $(1 - \chi(\beta)) \neq 0$. Hence, $\sum_{\alpha} \chi(\alpha) = 0$. ■

For any character χ on $\mathbf{F}_p^*$ and $\beta \in \mathbf{F}_p$, we define the Gauss sum

$$G(\beta, \chi) = \sum_{\alpha} \chi(\alpha) e^{2\pi i\alpha\beta/p}.$$

When $\beta = 1$, we write

$$G(\chi) = G(1, \chi).$$

Note that for $\beta \neq 0$,

$$G(\beta, \chi) = \sum_{\alpha} \chi(\alpha) e^{2\pi i\alpha\beta/p} = \chi^{-1}(\beta) \sum_{\alpha} \chi(\alpha\beta) e^{2\pi i\alpha\beta/p} = \chi(\beta^{-1}) G(\chi). \tag{2.1}$$

Another basic property of Gauss sums that we need is the following:

Lemma 2.4 ([2, Theorem 1.1.4(c)]). *Let χ be a nonprincipal character of $\mathbf{F}_p^*$. Then, for $\beta \neq 0$,*

$$|G(\beta, \chi)|^2 = G(\beta, \chi)\overline{G(\beta, \chi)} = p.$$

Proof. By (2.1), we have for $\beta \neq 0$,

$$\chi(\beta^{-1})G(\chi) = G(\beta, \chi) = \sum_{\alpha} \chi(\alpha) e^{2\pi i \alpha\beta/p}. \tag{2.2}$$

Notice that in the case $\beta = 0$, (2.2) still holds in view of Lemma 2.3. Multiplying the two sides of (2.2) by $e^{-2\pi i\beta/p}$ and summing over all β in $\mathbf{F}_p$, we get

$$\overline{G(\chi)}G(\chi) = \sum_{\alpha} \chi(\alpha) \sum_{\beta} e^{2\pi i\beta(\alpha-1)/p}.$$

The inner sum is nonzero only when $\alpha = 1$, in which case the inner sum is equal to p. This implies that $G(\chi)\overline{G(\chi)} = p$. Hence, we conclude that

$$|G(\beta, \chi)|^2 = \left|\chi(\beta^{-1})\right|^2 \cdot |G(\chi)|^2 = 1 \cdot p = p. \qquad \blacksquare$$

3. THE JACOBI SUMS. Let χ and ξ be characters of $\mathbf{F}_p^*$. The Jacobi sum is defined as

$$J(\chi, \xi) = \sum_{\alpha} \chi(\alpha)\xi(1-\alpha).$$

The following lemma gives a relation between the Gauss sum and the Jacobi sum.

Lemma 3.1 ([2, Theorem 2.1.3]). *Let χ and ξ be two characters of $\mathbf{F}_p^*$ such that $\chi\xi$ is nonprincipal. Then*

$$J(\chi, \xi) = \frac{G(\chi)G(\xi)}{G(\chi\xi)}.$$

Proof. We observe that

$$\begin{aligned}
G(\chi)G(\xi) &= \sum_{\alpha}\sum_{\beta} \chi(\alpha)\xi(\beta)e^{2\pi i(\alpha+\beta)/p} = \sum_{\gamma}\sum_{\alpha+\beta=\gamma} \chi(\alpha)\xi(\beta)e^{2\pi i\gamma/p} \\
&= \sum_{\alpha+\beta=0} \chi(\alpha)\xi(\beta) + \sum_{\gamma\neq 0} e^{2\pi i\gamma/p} \sum_{\alpha} \chi(\alpha)\xi(\gamma-\alpha) \\
&= \xi(-1)\sum_{\alpha} \chi\xi(\alpha) + \sum_{\gamma\neq 0} e^{2\pi i\gamma/p} \sum_{\alpha} \chi(\gamma\alpha)\xi(\gamma-\gamma\alpha) \\
&= 0 + \sum_{\gamma\neq 0} \chi\xi(\gamma)e^{2\pi i\gamma/p} J(\chi, \xi) = G(\chi\xi)J(\chi, \xi),
\end{aligned}$$

where we have used Lemma 2.3 in the second-to-last equality. $\blacksquare$

The next lemma is useful in computing Jacobi sums of the type $J(\chi, \rho)$ where ρ is the quadratic character of $\mathbf{F}_p^*$.

Lemma 3.2 ([2, Theorem 2.1.4]). *Let χ be a character of $\mathbf{F}_p^*$, where p is an odd prime, and ρ be the quadratic character of $\mathbf{F}_p^*$. Then*

$$J(\chi, \rho) = \chi(4)J(\chi, \chi).$$

Proof. Let β be a fixed element of $\mathbf{F}_p$. Consider the number of solutions to the equation

$$\alpha(1-\alpha) = \beta.$$

Since 2 is invertible in $\mathbf{F}_p$, the above equation is equivalent to

$$(2\alpha - 1)^2 = 1 - 4\beta,$$

whose number of solutions is given by

$$1 + \rho(1 - 4\beta).$$

Therefore

$$\begin{aligned} J(\chi, \chi) &= \sum_{\alpha} \chi(\alpha(1-\alpha)) = \sum_{\beta} \chi(\beta)(1 + \rho(1 - 4\beta)) \\ &= \frac{1}{\chi(4)} \sum_{\beta} \chi(4\beta)\rho(1-4\beta) = \frac{1}{\chi(4)} J(\chi, \rho). \end{aligned}$$ ∎

Lemma 3.3. *Let $p \equiv 1 \pmod 6$ and χ be a character of order 6 of $\mathbf{F}_p$. Then*

$$J(\chi, \rho) = c + d\sqrt{-3},$$

where $c, d \in \mathbf{Z}$ such that

$$c^2 + 3d^2 = p.$$

Proof. Pairing α with $1 - \alpha$ and noting that $4\alpha(1-\alpha) = 1$ when $\alpha = (p+1)/2$, we find that

$$\begin{aligned} J(\chi, \rho) &= \chi(4) J(\chi, \chi) = \sum_{\alpha} \chi(4\alpha(1-\alpha)) \\ &= 1 + 2 \sum_{m=2}^{(p-1)/2} \chi(4m(1-m)). \end{aligned}$$

Note that $\chi(w)$ is a 6th root of unity since χ has order 6. Therefore,

$$\chi(w) \in \mathbf{Z}\left[\frac{1+\sqrt{-3}}{2}\right],$$

and we conclude that $J(\chi, \rho) = c + d\sqrt{-3}$, with $c, d \in \mathbf{Z}$. Now, by Lemmas 2.4, 3.1, and 3.2,

$$|J(\chi, \rho)|^2 = |J(\chi, \chi)|^2 = \frac{|G^2(\chi)|^2}{|G(\chi^2)|^2} = p.$$

Therefore, the integers c and d satisfy

$$c^2 + 3d^2 = |J(\chi, \rho)|^2 = p.$$ ∎

4. THE JACOBSTHAL SUMS. Let p be a prime. Let a be an integer not divisible by p and k be a positive integer. The Jacobsthal sums $\phi_k(a)$ and $\psi_k(a)$ are defined by

$$\phi_k(a) = \sum_{\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\alpha^k + a}{p}\right)$$

and

$$\psi_k(a) = \sum_{\alpha}{}^{*} \left(\frac{\alpha^k + a}{p}\right) = \sum_{\alpha} \left(\frac{\alpha^k + a}{p}\right) - \left(\frac{a}{p}\right).$$

In this note, we will concentrate on evaluating $\phi_k(a)$ and $\psi_k(a)$ when $k = 3$. To shorten our notation, we let $\phi = \phi_3$ and $\psi = \psi_3$.

Lemma 4.1 ([2, Proposition 6.1.5]). *Let g be a primitive root modulo p. Let n and j be integers. Then*

$$\phi(g^{3n+j}) = \phi(g^j).$$

Proof. We observe that

$$\begin{aligned}
\phi(g^{3n+j}) &= \sum_{\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\alpha^3 + g^{3n+j}}{p}\right) \\
&= \sum_{\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{g^{3n}}{p}\right)\left(\frac{(\alpha g^{-n})^3 + g^j}{p}\right) \\
&= \sum_{\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{g^{-3n}}{p}\right)\left(\frac{(\alpha g^{-n})^3 + g^j}{p}\right) \\
&= \sum_{\alpha} \left(\frac{(\alpha g^{-n})^3}{p}\right)\left(\frac{(\alpha g^{-n})^3 + g^j}{p}\right) = \phi(g^j),
\end{aligned}$$

where we have used $(g^{3n}/p) = (g^{-3n}/p)$ in the third equality and $(\alpha/p) = (\alpha^3/p)$ in the fourth equality. ■

Lemma 4.2 ([2, Proposition 6.1.7]). *Let p be an odd prime and a be an integer not divisible by p. Then*

$$\phi(a) = \left(\frac{a}{p}\right)\psi(a^{-1}).$$

Proof.

$$\begin{aligned}
\phi(a) &= \sum_{\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\alpha^3 + a}{p}\right) = \sum_{\alpha}{}^{*} \left(\frac{\alpha}{p}\right)\left(\frac{\alpha^3 a}{p}\right)\left(\frac{\alpha^{-3} + a^{-1}}{p}\right) \\
&= \left(\frac{a}{p}\right)\sum_{\alpha}{}^{*} \left(\frac{\alpha^{-3} + a^{-1}}{p}\right) = \left(\frac{a}{p}\right)\psi(a^{-1}).
\end{aligned}$$

■

5. THE MAIN LEMMA.

Lemma 5.1 ([2, Proposition 6.2.2]). *Let p be a prime such that $p \equiv 1 \pmod 6$, g be a primitive root $\pmod p$, and a be an integer such that $p \nmid a$. Let χ be the character of order 6 on $\mathbf{F}_p^*$ such that $\chi(g) = e^{2\pi i/6}$. If $a \equiv g^N \pmod p$, then*

$$\phi(a) = \begin{cases} -1 + 2\left(\dfrac{-1}{p}\right) c & \text{if } N \equiv 0 \pmod 3 \\ -1 - \left(\dfrac{-1}{p}\right)(c - 3d) & \text{if } N \equiv 1 \pmod 3 \\ -1 - \left(\dfrac{-1}{p}\right)(c + 3d) & \text{if } N \equiv 2 \pmod 3, \end{cases}$$

where c and d are the integers in Lemma 3.3 such that $J(\chi, \rho) = c + d\sqrt{-3}$ with the property $c^2 + 3d^2 = p$.

Proof. By our assumption, the Legendre symbol can be identified with χ^3. Hence,

$$\phi(a) = \sum_{\alpha} \left(\frac{\alpha}{p}\right)\left(\frac{\alpha^3 + a}{p}\right) = \sum_{\alpha} \chi(\alpha^3)\chi^3(\alpha^3 + a).$$

Now, observe that

$$1 + \chi^2(g^s) + \chi^4(g^s) = \begin{cases} 0 & \text{if } 3 \nmid s, \\ 3 & \text{otherwise.} \end{cases}$$

Therefore, we may write

$$\begin{aligned} \phi(a) &= \sum_{m=0}^{p-1} \chi(g^{3m})\chi^3(g^{3m} + a) \\ &= \sum_{n=0}^{3p-1} \chi(g^n)\chi^3(g^n + a)\frac{1}{3}\sum_{j=0}^{2} \chi^{2j}(g^n) \\ &= \sum_{n=0}^{p-1} \chi(g^n)\chi^3(g^n + a)\sum_{j=0}^{2} \chi^{2j}(g^n). \end{aligned}$$

The last equality follows from the fact that if

$$F(k) = \sum_{n=(k-1)p}^{kp-1} \chi(g^n)\chi^3(g^n + a)\sum_{j=0}^{2} \chi^{2j}(g^n),$$

then for any integer k,

$$F(k+1) = F(k).$$

Therefore, we may rewrite

$$\begin{aligned}
\phi(a) &= \sum_{\alpha} \chi(\alpha)\chi^3(\alpha + a) \sum_{j=0}^{2} \chi^{2j}(\alpha) \\
&= \chi(-1) \sum_{\alpha} \chi(-\alpha)\chi^3((-\alpha)(-1) + a) \sum_{j=0}^{2} \chi^{2j}(-\alpha) \\
&= \chi(-1) \sum_{\alpha} \chi(\alpha)\chi^3(a - \alpha) \sum_{j=0}^{2} \chi^{2j}(\alpha) \\
&= \chi(-1) \sum_{\alpha} \chi(a\alpha)\chi^3(a - a\alpha) \sum_{j=0}^{2} \chi^{2j}(a\alpha) \\
&= \chi(-1)\chi^4(a) \sum_{j=0}^{2} \chi^{2j}(a) J(\chi^{2j+1}, \chi^3).
\end{aligned}$$

Simplifying the above, we conclude that

$$\phi(a) = \left(\frac{-1}{p}\right) \chi^{-2}(a) J(\chi, \chi^3) + \left(\frac{-1}{p}\right) J(\chi^3, \chi^3) + \left(\frac{-1}{p}\right) \chi^2(a) J(\chi^5, \chi^3). \tag{5.1}$$

The middle term of (5.1) is

$$\left(\frac{-1}{p}\right) J(\chi^3, \chi^3) = \left(\frac{-1}{p}\right) \sum_{\alpha} \left(\frac{\alpha(1-\alpha)}{p}\right).$$

Note that

$$\begin{aligned}
\sum_{\alpha} \left(\frac{\alpha(1-\alpha)}{p}\right) &= \sum_{\alpha}{}^{*} \left(\frac{\alpha(1-\alpha)}{p}\right) \\
&= \sum_{\alpha}{}^{*} \left(\frac{\alpha}{p}\right)\left(\frac{\alpha}{p}\right)\left(\frac{\alpha^{-1} - 1}{p}\right) \\
&= \sum_{\alpha}{}^{*} \left(\frac{\alpha - 1}{p}\right) = -\left(\frac{-1}{p}\right)
\end{aligned}$$

by Lemma 2.3. Hence, the middle term of (5.1) is -1.

Therefore, if we write $J(\chi, \chi^3) = c + \sqrt{-3}d$ with $c, d \in \mathbf{Z}$ as in Lemma 3.3, then

$$\phi(a) = -1 + \left(\frac{-1}{p}\right) \left(2\,\mathrm{Re}(\chi^{-2}(a))c - 2\,\mathrm{Im}(\chi^{-2}(a))\sqrt{3}d\right).$$

Now, if $N \equiv 1 \pmod 3$, then by Lemma 4.1, we may set $a = g$ and observe that

$$2\,\mathrm{Re}(\chi^{-2}(g)) = -1 \quad \text{and} \quad 2\,\mathrm{Im}(\chi^{-2}(g)) = -\sqrt{3}.$$

If $N \equiv 2 \pmod 3$, then by Lemma 4.1, we may set $a = g^2$ and observe that

$$2\,\mathrm{Re}(\chi^{-2}(g^2)) = -1 \quad \text{and} \quad 2\,\mathrm{Im}(\chi^{-2}(g^2)) = \sqrt{3}.$$

Finally, when $N \equiv 0 \pmod 3$ then we only need to compute

$$\phi(1) = -1 + 2\left(\frac{-1}{p}\right)c.$$

This completes the proof of the lemma. ■

Completion of the proof of Theorem 1.3. If a is a quadratic residue modulo p and $a \equiv g^N \pmod p$ with $N \equiv 1 \pmod 3$, then

$$\sum_{\alpha}\left(\frac{\alpha^3 + a}{p}\right) - 1 = \psi(a) = \phi(a^{-1}) = -1 - \left(\frac{-1}{p}\right)(c + 3d),$$

since $a^{-1} \equiv g^{-N} \pmod 3$ and $-N \equiv 2 \pmod 3$. This shows that

$$y = \sum_{\alpha}\left(\frac{\alpha^3 + a}{p}\right) = -\left(\frac{-1}{p}\right)(c + 3d).$$

Now,

$$x = \sum_{\alpha}\left(\frac{\alpha^3 + 1}{p}\right) = 2\left(\frac{-1}{p}\right)c.$$

Hence,

$$x^2 + xy + y^2 = 3p.$$

Similarly, we conclude the identity in the case when a is a quadratic residue modulo p such that the integer N in $a \equiv g^N \pmod p$ satisfies $N \equiv 2 \pmod 3$.

The case when a is not a quadratic residue can be treated in a similar way. ■

6. CONCLUDING REMARKS.

1. The proof of Theorem 1.3 given here is a slight modification of the proof due to R. Evans. This result can also be obtained by counting points on elliptic curves over finite fields. For more details, see [**7**, p. 305, Theorem 4].
2. Evans informed us that using the same idea illustrated here, one can obtain similar results for other quadratic forms. For example, from [**2**, Theorem 6.2.3], one can obtain

$$\left(\frac{1}{4}\sum_{\alpha}\left(\frac{\alpha^5 + \alpha}{p}\right)\right)^2 + 2\left(\frac{1}{4}\sum_{\alpha}\left(\frac{\alpha^5 + g\alpha}{p}\right)\right)^2 = p$$

   where $p \equiv 1 \pmod 8$ and g is a primitive root modulo p.
3. There are other proofs of Theorem 1.3 using eigenforms associated with Hecke Grössencharacters. A subset of the authors are working in this direction and they

succeeded in deriving solutions to equations such as

$$|\Delta(1,0,2)|p = 8p = A^2 + 2B^2$$

in terms of analogues of Jacobsthal sums. See [**6**] for more details.

4. Another cubic generalization of the Jacobsthal identity (1.2) was given by D. Zagier in [**4**, p. 92]. There, a solution was given to

$$4p = A^2 + 3B^2$$

when $p \equiv 1 \pmod 6$ as follows: Let χ be an order-6 character of $\mathbf{F}_p^*$ such that $\chi(a)$ is a primitive cubic root of unity and $\chi(b) = \chi(a)^{-1}$. Then one can take

$$A = \sum_{x=0}^{p-1} \left(\frac{x^3+1}{p}\right), \quad B = \frac{1}{3}\sum_{x=0}^{p-1} \left(\frac{x^3+a}{p}\right) - \frac{1}{3}\sum_{x=0}^{p-1} \left(\frac{x^3+b}{p}\right).$$

Zagier mentioned a septic analogue for

$$4p = A^2 + 7B^2$$

and encouraged readers to investigate the solutions of

$$4p = A^2 + dB^2$$

whenever $\mathbf{Q}(\sqrt{-d})$ has class number 1.

ACKNOWLEDGMENTS. It is our great pleasure to thank R. J. Evans for his interest, suggestions, and encouragement during the completion of this article. We also thank the editor of the MONTHLY D. J. Velleman for his excellent job in handling this article and the referees for their fruitful suggestions which have improved this article significantly. The first author would like to thank P. Moree and students J. L. Goh, N. Kayaalp, M. Lang, and L. Sauermann for discovering some misprints in a preliminary version of this article. The authors also thank the National Center for Theoretical Sciences in Hsinchu Taiwan, where the project was started. The first author was supported by NUS Academic Research Grant R-146-000-103-112. The second author was supported by NSA grant H98230-08-1-0076. The third author was supported by Grant 97-2115-M-009-001 of the National Science Council of Taiwan.

REFERENCES

1. G. E. Andrews, *Number Theory*, W. B. Saunders, Philadelphia, 1971.
2. B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, John Wiley, New York, 1998.
3. D. A. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley, New York, 1989.
4. J. H. Bruinier, G. van der Geer, G. Harder, and D. Zagier, *The 1-2-3 of Modular Forms,* Lectures at a Summer School in Nordfjordeid, Norway, K. Ranestad, ed., Springer-Verlag, Berlin, 2008.
5. E. Grosswald, *Representations of Integers as Sums of Squares,* Springer-Verlag, New York, 1984.
6. K. I. Hashimoto, L. Long, and Y. F. Yang, Jacobsthal identity for $\mathbf{Q}(\sqrt{-2})$, *Forum Mathematicum* (to appear).
7. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.
8. E. Jacobsthal, Über die Darstellung der Primzahlen der Form $4n + 1$ als Summe zweier Quadrate, *J. Reine Angew. Math.* **132** (1907) 238–245.

HENG HUAT CHAN received his Ph.D. in 1995 under the supervision of Professor B. C. Berndt and spent nine months at the Institute for Advanced Study after his graduation. He then took up a one-year visiting position at the National Chung Cheng University in Taiwan. In 1997, he returned to Singapore to join the

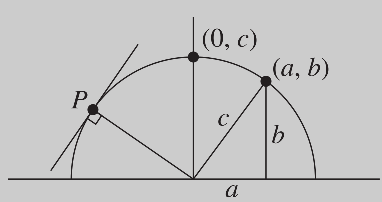
department at the National University of Singapore. When he is not working on mathematical problems, he enjoys spending his time with his wife and three kids, aged 14, 12, and 6.
Department of Mathematics, National University of Singapore, Faculty of Science, Block S17, 10 Lower Kent Ridge Road, Singapore 119076
matchh@nus.edu.sg

LING LONG received her Ph.D. degree from the Pennsylvania State University in 2002. Her research interests lie in number theory and its applications to other areas like combinatorics. In addition, she enjoys teaching to share her enthusiasm for mathematics.
Department of Mathematics, Iowa State University, Ames, IA 50011, USA
linglong@iastate.edu

YIFAN YANG received his B.S. degree from the National Taiwan University in 1992 and his Ph.D. degree from the University of Illinois at Urbana-Champaign in 2000. His research interest is in number theory, especially in areas related to modular forms. He enjoys music and playing bridge when he is not busy with research.
Department of Applied Mathematics, National Chiao Tung University, Hsinchu 300, Taiwan; National Center for Theoretical Sciences, Hsinchu 300, Taiwan
yfyang@math.nctu.edu.tw

A Calculus Proof for the Pythagorean Theorem

Consider a right triangle with legs of length a and b and hypotenuse of length c. Construct a rectangular coordinate system so that the vertices of the triangle have coordinates $(0, 0)$, $(a, 0)$, and (a, b). Draw the semicircle in the upper half-plane centered at the origin with radius c. This semicircle passes through the points (a, b) and $(0, c)$.



Euclid showed in Book III, Proposition 16 that if P is any point on the semicircle, then the line through P that is perpendicular to the radius from the origin to P is tangent to the semicircle, in the sense that it does not intersect the semicircle at any point other than P. We leave it as an exercise for the reader to verify that this line also satisfies the calculus definition of the tangent line to the semicircle at P. It follows that the semicircle must be the graph of a solution to the differential equation $dy/dx = -x/y$. Solving this differential equation, we find that $\int y\,dy = -\int x\,dx$, and therefore $x^2 + y^2 = C$ for some constant C. Since the circle passes through the point $(0, c)$, we must have $C = c^2$. But then since the circle also passes through (a, b), we can conclude that $a^2 + b^2 = c^2$.

—Submitted by John Molokach, North Carolina Virtual Public School
Smithfield-Selma High School, Smithfield, NC