Journal of Number Theory 147 (2015) 691–693

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Historical remark on a theorem of Zhang and Yue

Kenneth S. Williams

School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, K1S 5B6, Canada

ARTICLE INFO

Article history:
Received 24 July 2014
Received in revised form 3 August 2014
Accepted 19 August 2014
Available online 7 October 2014
Communicated by David Goss

Keywords:
Theorem of Zhang and Yue
Dirichlet's method
Congruences

ABSTRACT

The purpose of this historical remark is to observe that a slightly stronger form of a recent theorem of Zhang and Yue can be proved more easily using an elementary method given by Dirichlet in 1834.

Let d be a squarefree positive integer such that the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ is odd and its fundamental integral unit $x + y\sqrt{d}(> 1)$ has norm 1. Then it is known that $d = p$, $2p$ or $p_1 p_2$, where p, p_1 and $p_2 (\neq p_1)$ are primes congruent to 3 modulo 4, see for example [1, p. 163]. Zhang and Yue [3] have recently proved some congruences for x and y. These are stated in Theorem 1.

Theorem 1. *(See [3, Theorem 1.1].)*

(1) *If* $d = p$ *with* $p \equiv 3 \pmod 4$ *then* $x \equiv 0 \pmod 2$. *Moreover* $x \equiv 2 \pmod 4$ *if* $p \equiv 3 \pmod 8$ *and* $x \equiv 0 \pmod 4$ *if* $p \equiv 7 \pmod 8$.

E-mail address: kwilliam@connect.carleton.ca.

http://dx.doi.org/10.1016/j.jnt.2014.08.011

(2) *If* $d = 2p$ *with* $p \equiv 3 \pmod 4$ *then* $y \equiv 0 \pmod 2$ *and* $x + y \equiv 3 \pmod 4$.
(3) *If* $d = p_1 p_2$ *with* $p_1 \equiv p_2 \equiv 3 \pmod 4$ *then* $x \equiv 3 \pmod 4$ *and* $y \equiv 0 \pmod 4$.

The purpose of this remark is to point out that a slightly stronger form of Zhang and Yue's theorem can be proved easily using an elementary method given by Dirichlet [2] in 1834, see Theorem 2. This method requires only the fundamental theorem of arithmetic.

Theorem 2.

(1) *If* $d = p$ *with* $p \equiv 3 \pmod 4$ *then* $x \equiv 0 \pmod 2$. *Moreover* $x \equiv 2 \pmod 8$ *if* $p \equiv 3 \pmod 8$ *and* $x \equiv 0 \pmod 8$ *if* $p \equiv 7 \pmod 8$.
(2) *If* $d = 2p$ *with* $p \equiv 3 \pmod 4$ *then* $y \equiv 0 \pmod 2$. *Moreover* $x \equiv 5 \pmod{32}$, $y \equiv 2 \pmod 4$ *if* $p \equiv 3 \pmod 8$ *and* $x \equiv 15 \pmod{16}$, $y \equiv 0 \pmod 4$ *if* $p \equiv 7 \pmod 8$.
(3) *If* $d = p_1 p_2$ *with* $p_1 \equiv p_2 \equiv 3 \pmod 4$ *then* $x \equiv 7 \pmod 8$ *and* $y \equiv 0 \pmod 4$. *Moreover* $x \equiv 7 \pmod{16}$, $y \equiv 4 \pmod 8$ *if* $(p_1, p_2) \equiv (3, 3) \pmod 8$; $x \equiv 15 \pmod{16}$, $y \equiv 0 \pmod 8$ *if* $(p_1, p_2) \equiv (7, 7) \pmod 8$; *and either* $x \equiv 15 \pmod{16}$, $y \equiv 0 \pmod 8$ *or* $x \equiv 7 \pmod{16}$, $y \equiv 4 \pmod 8$ *if* $(p_1, p_2) \equiv (3, 7)$ *or* $(7, 3) \pmod 8$.

Proof. As $x + y\sqrt{d}$ is the fundamental integral unit of $\mathbb{Q}(\sqrt{d})$ of norm 1, x and y are positive integers satisfying $x^2 - dy^2 = 1$ with y the least such integer.

We first use Dirichlet's method to prove (1). Suppose that $x \equiv 1 \pmod 2$. Then $y \equiv 0 \pmod 2$. Thus $\frac{x-1}{2}$, $\frac{x+1}{2}$ and $\frac{y}{2}$ are positive integers satisfying $\frac{x-1}{2} \cdot \frac{x+1}{2} = p(\frac{y}{2})^2$. Hence p divides either $\frac{x-1}{2}$ or $\frac{x+1}{2}$. Let $\epsilon = \pm 1$ be such that p divides $\frac{x-\epsilon}{2}$. Thus $\frac{x-\epsilon}{2p}$ and $\frac{x+\epsilon}{2}$ are positive integers such that $\frac{x-\epsilon}{2p} \cdot \frac{x+\epsilon}{2} = (\frac{y}{2})^2$. As $\frac{x-\epsilon}{2} - \frac{x+\epsilon}{2} = \pm 1$ the integers $\frac{x-\epsilon}{2p}$ and $\frac{x+\epsilon}{2}$ are coprime. Thus there exist coprime positive integers r and s such that

$$\frac{x-\epsilon}{2p} = r^2, \qquad \frac{x+\epsilon}{2} = s^2, \qquad \frac{y}{2} = rs.$$

Hence $s^2 - pr^2 = \epsilon$. As $p \equiv 3 \pmod 4$ we must have $\epsilon = 1$, so $s^2 - pr^2 = 1$. But $r < 2rs = y$, which contradicts the minimality of y. Thus we must have $x \equiv 0 \pmod 2$, and so $y \equiv 1 \pmod 2$. Proceeding as above but now with y odd, we deduce that there are coprime positive odd integers r and s such that

$$x - \epsilon = pr^2, \qquad x + \epsilon = s^2, \qquad y = rs,$$

for some $\epsilon = \pm 1$. Hence $s^2 - pr^2 = 2\epsilon$. If $p \equiv 3 \pmod 8$ then $2\epsilon \equiv 1 - p \equiv -2 \pmod 8$ so $\epsilon = -1$ and $x = pr^2 - 1 \equiv 2 \pmod 8$. If $p \equiv 7 \pmod 8$ then $2\epsilon \equiv 1 - p \equiv 2 \pmod 8$ so $\epsilon = 1$ and $x = pr^2 + 1 \equiv 0 \pmod 8$.

Next we use Dirichlet's method to prove (2). If $y \equiv 1 \pmod 2$ then $x^2 = 2py^2 + 1 \equiv 6y^2 + 1 \equiv 7 \pmod 8$, which is impossible, so $y \equiv 0 \pmod 2$ and $x \equiv 1 \pmod 2$. Applying Dirichlet's method as before, we find that there are positive coprime integers r and s such that

$$x-1=2pr^2, \qquad x+1=4s^2, \qquad y=2rs, \qquad r\equiv 1 \pmod 2, \qquad s\equiv 0 \pmod 2$$

or

$$x-1=4r^2, \qquad x+1=2ps^2, \qquad y=2rs, \qquad r\equiv 1 \pmod 2, \qquad s\equiv 1 \pmod 2.$$

The first possibility gives $2s^2-pr^2=1$ so $p\equiv pr^2\equiv 2s^2-1\equiv 7 \pmod 8$, $x=4s^2-1\equiv 15 \pmod{16}$ and $y=2rs\equiv 0 \pmod 4$. The second possibility gives $ps^2-2r^2=1$ so $p\equiv ps^2\equiv 2r^2+1\equiv 3 \pmod 8$, $x=4r^2+1\equiv 5 \pmod{32}$ and $y=2rs\equiv 2 \pmod 4$.

Finally we use Dirichlet's method to prove (3). If $y\equiv 1 \pmod 2$ then $x^2=p_1p_2y^2+1\equiv 2 \pmod 4$, which is impossible. Hence $y\equiv 0 \pmod 2$ and $x\equiv 1 \pmod 2$. Dirichlet's method shows that there exist coprime positive integers r and s with $r\equiv 1 \pmod 2$ and $s\equiv 0 \pmod 2$ such that

$$x-1=2p_1r^2, \qquad x+1=2p_2s^2, \qquad y=2rs, \qquad p_1r^2-p_2s^2=-1$$

or

$$x-1=2p_2r^2, \qquad x+1=2p_1s^2, \qquad y=2rs, \qquad p_1s^2-p_2r^2=1.$$

Thus $x=1+2(p_1 \text{ or } p_2)r^2\equiv 1+6r^2\equiv 7 \pmod 8$ and $y=2rs\equiv 0 \pmod 4$.

If $(p_1,p_2)\equiv(3,3) \pmod 8$ we have $x=1+2(p_1 \text{ or } p_2)r^2\equiv 1+6\equiv 7 \pmod{16}$. Then $8\equiv x+1=2(p_2 \text{ or } p_1)s^2\equiv 6s^2 \pmod{16}$ so $s\equiv 2 \pmod 4$ and $y=2rs\equiv 4 \pmod 8$.

If $(p_1,p_2)\equiv(7,7) \pmod 8$ we have $x=1+2(p_1 \text{ or } p_2)r^2\equiv 1+14\equiv 15 \pmod{16}$. Then $0\equiv x+1=2(p_2 \text{ or } p_1)s^2\equiv 14s^2 \pmod{16}$ so $s\equiv 0 \pmod 4$ and $y=2rs\equiv 0 \pmod 8$.

If $(p_1,p_2)\equiv(3,7)$ or $(7,3) \pmod 8$, interchanging p_1 and p_2 if necessary, we may suppose without loss of generality that $(p_1,p_2)\equiv(3,7) \pmod 8$. From the first possibility we obtain $x=1+2p_1r^2\equiv 1+6\equiv 7 \pmod{16}$. Then $8\equiv x+1=2p_2s^2\equiv 14s^2 \pmod{16}$ so $s\equiv 2 \pmod 4$ and $y=2rs\equiv 4 \pmod 8$. From the second possibility we deduce $x=1+2p_1r^2\equiv 1+14\equiv 15 \pmod{16}$. Then $0\equiv x+1=2p_1s^2\equiv 6s^2 \pmod{16}$ so $s\equiv 0 \pmod 4$ and $y=2rs\equiv 0 \pmod 8$. □

References

[1] P.E. Conner, J. Hurrelbrink, Class Number Parity, World Sci. Ser. Pure Math., vol. 8, World Scientific, Singapore, 1988.
[2] P.G.L. Dirichlet, Einige neue Sätze über unbestimmte Gleichungen, Abh. Königlich Preussischen Akad. Wiss., 1834, pp. 649–664; Werke, Chelsea Pub. Co., NY, 1969, pp. 219–236.
[3] Zhe Zhang, Qin Yue, Fundamental units of real quadratic fields of odd class number, J. Number Theory 137 (2014) 122–129.