Journal of Mathematical Sciences, Vol. 140, No. 5, 2007

A COMBINATORIAL PROOF OF EULER–FERMAT'S THEOREM ON THE REPRESENTATION OF THE PRIMES p=8k+3 BY THE QUADRATIC FORM x^2+2y^2

A. I. Generalov* UDC 512.5

An elementary and extremely short proof of the theorem on the representation of the primes $p = 8k + 3$ by the quadratic form $x^2 + 2y^2$ with integers x and y. Bibliography: 1 title.

In [1], D. Zagier gave an extremely short and elegant proof of Fermat's theorem on the representation of primes of the form $p = 4k + 1$ as a sum of two squares of integers: he defined actions of two involutions on a suitable finite set Ω; one of these involutions has a unique the fixed point, whence it follows that the cardinality $|\Omega|$ is odd, and then fixed points of the second involution provide the desired representation of a given prime. In the present paper, we use a similar approach to prove the following theorem.

Theorem 1. *Let p be a prime that is congruent to* 3 *modulo* 8*. Then p is represented in the form $p = x^2 + 2y^2$, where x and y are natural numbers.*

Proof. Put

$$\Omega = \{(x, y, z) \in \mathbb{N}^3 \mid p = x^2 + 2yz\}. \tag{1}$$

We observe that the set Ω is finite (if $(x, y, z) \in \Omega$, then $x, y, z < p/2$) and nonempty (since the point $\omega_0 = (1, 1, (p-1)/2)$ belongs to Ω). We also note that x, y, and z are odd for any $(x, y, z) \in \Omega$. Moreover, since $p = x^2 + 2y^2 + 2y(z - y)$ and $x^2 \equiv y^2 \equiv 1 (\bmod 8)$, we see that $2y(z - y)$ is divisible by 8, and thus $z - y$ is divisible by 4.

The set Ω is a disjoint union of the following sets:

$$\begin{aligned}
\Omega_0 &= \left\{(x, y, z) \in \Omega \mid y - \frac{z}{2} < x < 2y\right\}, \\
\Omega_1 &= \{(x, y, z) \in \Omega \mid x > 2y\}, \\
\Omega_2 &= \left\{(x, y, z) \in \Omega \mid x < \frac{y}{2} - z\right\}, \\
\Omega_3 &= \left\{(x, y, z) \in \Omega \mid \frac{y}{2} - z < x < \frac{2}{3}(y - z)\right\}, \\
\Omega_4 &= \left\{(x, y, z) \in \Omega \mid \frac{2}{3}(y - z) < x < y - \frac{z}{2}\right\}.
\end{aligned}$$

Indeed, if $(x, y, z) \in \Omega$, then $y - \frac{z}{2} \neq x \neq \frac{y}{2} - z$ (because y and z are odd) and $2y \neq x \neq \frac{2}{3}(y - z)$ (because x is odd). We define a map $\Phi : \Omega \to \Omega$ by the formula

$$\Phi(x, y, z) = \begin{cases}
(2y - x,\ y,\ z + 2x - 2y) & \text{if } (x, y, z) \in \Omega_0, \\
(x - 2y,\ z + 2x - 2y,\ y) & \text{if } (x, y, z) \in \Omega_1, \\
(x + 2z,\ z,\ y - 2x - 2z) & \text{if } (x, y, z) \in \Omega_2, \\
(-3x + 2y - 2z, -2x + 2y - z, 2x - y + 2z) & \text{if } (x, y, z) \in \Omega_3, \\
(3x - 2y + 2z, 2x - y + 2z, -2x + 2y - z) & \text{if } (x, y, z) \in \Omega_4.
\end{cases} \tag{2}$$

We can directly verify that

$$\left.\begin{aligned}
\Phi(\Omega_0) \subset \Omega_0, \Phi(\Omega_1) \subset \Omega_2, \Phi(\Omega_2) \subset \Omega_1, \\
\Phi(\Omega_3) \subset \Omega_3, \Phi(\Omega_4) \subset \Omega_4,
\end{aligned}\right\} \tag{3}$$

and then we conclude that $\Phi \circ \Phi = \mathrm{id}_\Omega$. In particular, this implies that all the inclusions in (3) can be replaced by equalities.

*St.Petersburg State University, St.Petersburg, Russia, e-mail:general@pdmi.ras.ru.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 330, 2006, pp. 155–157. Original article submitted December 10, 2005.

 1072-3374/07/1405-0690

It is easily seen that ω_0 is a unique fixed point of the involution Φ. Consequently, the cardinality $|\Omega|$ is odd. Now, we consider another involution on the set Ω:

$$\Psi\colon \Omega \to \Omega, \quad (x, y, z) \mapsto (x, z, y).$$

This involution must have a fixed point $(x_0, y_0, y_0) \in \Omega$, whence we obtain $p = x_0^2 + 2y_0^2$. $\square$

Remark 2. Assume that a prime p is congruent to 1 modulo 8. We again consider the set Ω in (1) and the involution defined in (2). If $(x, y, z) \in \Omega$, it is easily seen that x is odd and yz is divisible by 4, and, as in the situation of Theorem 1, we have $\Omega = \bigcup_{i=0}^{4} \Omega_i$. But now, in addition to the point ω_0, the involution Φ has two further fixed points: one point in each of the sets Ω_3 and Ω_4 (in this case, the arguments in the proof of Theorem 1 are applied again). The uniqueness of a fixed point in the set Ω_4 (respectively, in Ω_3) is established by using the arithmetic of the ring $\mathbb{Z}[i]$ of integer Gaussian numbers (respectively, in the ring of integers of the field $\mathbb{Q}(\sqrt{2})$), and so on. But, in this case, to prove the existence (and uniqueness) of the representation $p = x^2 + 2y^2$ it is much simpler to use directly the arithmetic of the ring of integers of the field $\mathbb{Q}(\sqrt{-2})$.

Translated by A. I. Generalov.

REFERENCES

1. D. Zagier, "A one-sentence proof that every prime $p \equiv 1 (\bmod 4)$ is a sum of two squares," *Amer. Math. Monthly*, **97**, 144 (1990).