Notes

101.01 Fermat's last theorem for $n = 3$ revisited

In the 17th century, Fermat discovered the insolvability in non-zero integers of the equation $x^3 + y^3 = z^3$ (but his proof has been lost). In 1770, Euler gave a proof (see [1, pp. 39-42]), followed by Gauss (see [1, pp. 42-45]) and Legendre (see [2, pp. 357-360]). Various proofs were obtained by Lamé, Tait, Günther, Gambioli, Krey, Thue, Carmichael and by many other mathematicians. A proof in Euler's style is based on a crucial lemma, followed by an infinite descent that is divided in *two* main cases (according as to whether the g.c.d. of $x + y$ and $x^2 - xy + y^2$ is 1 or 3). In the present version, the crucial lemma receives a short proof and an additional observation allows elimination of one of the two main cases.

General properties of the ring of units of a quadratic field (needed here) can be found in [3].

Notations: $\mathbb{Z}^*$ stands for $\mathbb{Z} - \{0\}$ and $\mathbb{N}^*$ for $\mathbb{N} - \{0\}$. Throughout, a, b lie in $\mathbb{Z}^*$ and (a, b) denotes the g.c.d. of a and b.

Introduction

Recall that every prime $p = 6k + 1$ of $\mathbb{N}$ has a unique representation as $p = r^2 + 3s^2$, $r, s \in \mathbb{N}^*$. Set $\omega = \dfrac{-1 + \sqrt{-3}}{2}$,

$$A = \mathbb{Z}(\omega) = \left\{ \frac{m + n\sqrt{-3}}{2},\ m, n \in \mathbb{Z},\ m + n \text{ even} \right\} \supset \mathbb{Z}\left(\sqrt{-3}\right).$$

The units of A are ± 1, $\pm\omega$, $\pm\omega^2$. A is a euclidean (hence factorial) ring for the norm $N\left(\alpha + \beta\sqrt{-3}\right) = \alpha^2 + 3\beta^2$. Define the *atoms* of A, *all lying* in $\mathbb{Z}\left(\sqrt{-3}\right)$, as the elements: 2, $p = 6k - 1$ prime of $\mathbb{N}$, $\sqrt{-3}$, $r + s\sqrt{-3}$ and $r - s\sqrt{-3}$ for each prime $p = 6k + 1$ of $\mathbb{N}$, $p = r^2 + 3s^2$, $r, s \in \mathbb{N}^*$. The atoms of A, pairwise coprime, represent (up to units) *all* the irreducible (or prime) elements of A. For example, the six prime elements ± 5, $\pm 5\omega$, $\pm 5\omega^2$ are all represented by the single atom 5. Let $z \in A - \{0\}$; z not a unit. Then z has a unique *atomic* decomposition as $z = \varepsilon \times \pi$, where ε is a unit of A and $\pi \in \mathbb{Z}\left(\sqrt{-3}\right)$ is a product of atoms in a *unique* way (up to order). For example, $70\left(\dfrac{3 + \sqrt{-3}}{2}\right) = (-\omega) \times 2 \times 5 \times \sqrt{-3} \times \left(2 + \sqrt{-3}\right) \times \left(2 - \sqrt{-3}\right)$. Every atom of z corresponds to *one* prime factor (or its square) of $N(z)$: 2 to 2^2, $p = 6 - 1$ to p^2, $\sqrt{-3}$ to 3, $r + s\sqrt{-3}$, respectively $r - s\sqrt{-3}$, to $p\left(= 6k + 1\right) = r^2 + 3s^2$.

The following properties are trivial:

(R1) If $a + b$ is odd, then the atom 2 does not divide $a + b\sqrt{-3}$ in A.

(R2) If $(a, b) = 1$, then the atom $p = 6k - 1$ does not divide $a + b\sqrt{-3}$ in A.

(R3) If $(a, b) = 1$, then the square of the atom $\sqrt{-3}$ does not divide $a + b\sqrt{-3}$ in A.

https://doi.org/10.1017/mag.2017.9 Published online by Cambridge University Press

In particular we have:

(P1) If $a + b$ is odd and $(a, b) = 1$, then $N(a + b\sqrt{-3}) = a^2 + 3b^2$ has neither factor 2, nor $p = 6k - 1$, nor 3^2.

Proof of F.L.T. in the case $n = 3$

Notice the following properties:

(P2) If $(a, b) = 1$ and $p = 6k + 1 = r^2 + 3s^2$ is a prime of $\mathbb{N}$, then the product of the atoms $\lambda = r + s\sqrt{-3}$ and $\bar{\lambda} = r - s\sqrt{-3}$ does not divide $z = a + b\sqrt{-3}$ in A.

Proof: Otherwise, for some $m, n \in \mathbb{Z}$:

$$a + b\sqrt{-3} = \lambda\bar{\lambda}\left(\frac{m + n\sqrt{-3}}{2}\right) = p\left(\frac{m + n\sqrt{-3}}{2}\right).$$

Then $2a = pm$, $2b = pn$. Hence, $p \mid a$ and $p \mid b$, a contradiction.

(P3) Let $a + b$ be odd and $(a, b) = 1$. Suppose that $a^2 + 3b^2 = c^3$, $c \in \mathbb{N}^*$. Then $z = a + b\sqrt{-3}$ is a cube in $\mathbb{Z}(\sqrt{-3})$.

Proof: Let $z = \varepsilon \times \pi$ be the atomic decomposition. As $N(z) = c^3$, by P1, c has only prime factors $p = 6k + 1$: for *each* such p, $p \times p \times p$ divides $N(z)$. By P2, *no two* of the three corresponding atoms of z can be *conjugate*. Hence these three atoms are equal. This argument shows that π is a cube in $\mathbb{Z}(\sqrt{-3})$. Hence $z = \varepsilon \times \gamma^3$, $\gamma \in \mathbb{Z}(\sqrt{-3})$. Then $\varepsilon^{-1}z = \gamma^3 \in \mathbb{Z}(\sqrt{-3})$. But, since $a + b$ is odd, $\pm\omega z, \pm\omega^2 z \notin \mathbb{Z}(\sqrt{-3})$. Hence $\varepsilon^{-1} = \pm 1$, so $z = (\pm\gamma)^3$.

Lemma: Let $a + b$ be odd and $(a, b) = 1$. Suppose that $a^2 + 3b^2 = c^3$, $c \in \mathbb{N}^*$. Then

(i) 3 divides b,

(ii) for some $e, f \in \mathbb{Z}^* : a = e(e^2 - 9f^2)$ and $b = 3f(e^2 - f^2)$.

Proof: By P3, for some $e + f\sqrt{-3} \in \mathbb{Z}(\sqrt{-3})$, $a + b\sqrt{-3} = (e + f\sqrt{-3})^3$. By expanding we get (ii). (i) follows.

(P4) Let $p + q$ be odd and $(p, q) = 1$. Suppose that $2p(p^2 + 3q^2) = \theta^3$, $\theta \in \mathbb{Z}^*$. Then, q is odd and $9 \mid p$. In particular, $3 \mid \theta$ and $3 \nmid q$.

Proof:

$8 \mid \theta^3$ so $4 \mid p(p^2 + 3q^2)$. Because $p^2 + 3q^2$ is odd, then $4 \mid p$. Hence q is odd. If $3 \nmid p$, then $3 \nmid \theta$, so $\theta^3 \equiv \pm 1 \pmod 9$ and $2p^3 \equiv \pm 2 \pmod 9$. Now, $(2p, p^2 + 3q^2) = 1$ so $p^2 + 3q^2$ is a cube in $\mathbb{N}^*$. By the lemma, $3 \mid q$, so $2p(p^2 + 3q^2) \equiv 2p^3 \equiv \pm 2 \pmod 9$, a contradiction.

Hence $3 \mid p$, so $3 \mid \theta$ and $3 \nmid q$. Now $27 \mid p(p^2 + 3q^2)$ and $9 \nmid (p^2 + 3q^2)$ so that $9 \mid p$.

https://doi.org/10.1017/mag.2017.9 Published online by Cambridge University Press

Theorem: The equation

$$2p\left(p^2 + 3q^2\right) = \theta^3 \tag{1}$$

with $p + q$ odd and $(p, q) = 1$ is insolvable in $\mathbb{Z}^*$.

Proof (*by descent*): Consider a solution of (1) with $|\theta|$ minimum. By P4, q is odd, $9 \mid p$, $3 \mid \theta$, $3 \nmid q$. We may write

$$\left(\frac{2p}{9}\right)\left(\frac{p^2 + 3q^2}{3}\right) = \left(\frac{\theta}{3}\right)^3 \tag{2}$$

As $3 \nmid \dfrac{p^2 + 3q^2}{3}$, clearly $\left(\dfrac{2p}{9}, \dfrac{p^2 + 3q^2}{3}\right) = 1$. Hence,

$$\frac{2p}{9} = u^3, \tag{3}$$

$$\frac{p^2 + 3q^2}{3} = v^3, \tag{4}$$

$$uv = \frac{\theta}{3} \qquad \left(\text{and } u, v \in \mathbb{Z}^*\right).$$

From (4), $q^2 + 3\left(\dfrac{p}{3}\right)^2 = v^3$ and with the lemma, we get

$$q = e\left(e^2 - 9f^2\right), \tag{5}$$

$$\frac{p}{3} = 3f\left(e^2 - f^2\right). \tag{6}$$

Since $\left(q, \frac{p}{3}\right) = 1$, by (5) and (6), $(e, f) = 1$. As q is odd, by (5), e is odd and f even. By (6) and (3) we have $\dfrac{2p}{9} = (e + f)(e - f)(2f) = u^3$, where the three factors are pairwise coprime. Hence, $e + f = r^3$, $e - f = s^3$, $2f = t^3$, $rst = u$, r and s both odd, $(r, s) = 1$. Set $\alpha = \dfrac{r - s}{2}$, $\beta = \dfrac{r + s}{2}$. Then $\alpha + \beta$ is odd and $(\alpha, \beta) = 1$. Rewrite $r^3 - s^3 = t^3$ as

$$2\alpha\left(\alpha^2 + 3\beta^2\right) = t^3$$

where $|t| < |\theta|$ since $rstv = uv = \dfrac{\theta}{3}$.

Corollary: The cubic Fermat's equation $x^3 + y^3 + z^3 = 0$ is insolvable in $\mathbb{Z}^*$.

Proof: Otherwise, pick a primitive solution with x, y odd. Putting $p = \dfrac{x + y}{2}$ and $q = \dfrac{x - y}{2}$ yields $2p\left(p^2 + 3q^2\right) = (-z)^3$, where $p + q$ is odd and $(p, q) = 1$.

https://doi.org/10.1017/mag.2017.9 Published online by Cambridge University Press

References

1. P. Ribenboim, *13 lectures on Fermat's last theorem*, Springer-Verlag, (1999).
2. A. M. Legendre, *Théorie des nombres*, vol. 2, reprint, Blanchard, Paris (1955).
3. H. M. Edwards, *Fermat's last theorem: a genetic introduction to algebraic number theory*, New York: Springer-Verlag (1977).

10.1017/mag.2017.9

ROY BARBARA

Lebanese University, Faculty of Science II, Fanar Campus. P.O.Box 90656, Jdeidet El Metn, Lebanon

e-mail: *roybarbara.math@gmail.com*

101.02 A (doubly) elementary formula for prime numbers

In [1, p. 5], the problem of giving a formula for the nth prime number was raised. Using a characterisation of prime numbers by Wilson's theorem, Willans gave such a formula [2]. In [3], new formulas were given. They were obtained using the definition of prime numbers, say that they possess only trivial factorisations. In [4], another such formula was obtained using a clever encoding of Eratosthenes's sieve. In [5], Regimbal gave an explicit formula for the nth prime number using only a primality definition. Recently Ruiz and Sondow [6] also exhibited such constructions.

The formulas in [2, 4, 6] make use of transcendental functions such as log or cos. The other works make use only of the four elementary operations $+, -, \times, /$, the floor function $\lfloor \cdot \rfloor$ and powers. With the exception of [4], formulas require an upper bound for the nth prime number. In most cases, this bound is obtained with the help of Bertrand's postulate. Alternatively, in [6], theorems of Rosser and Schoenfeld are used for this purpose. These results, although classical, are not accessible to audiences below first degree level. In this paper, we present two new formulas involving elementary operations. Moreover, only elementary results of number theory are required for the proofs so that the title of this note is justified.

Let $\pi(x)$ denote the prime counting function and let p_n denote the nth prime number. We will prove the two following formulas.

$$\pi(x) = \sum_{i=2}^{\lfloor x \rfloor} \left\lfloor \frac{1}{\sum_{j=1}^{i} \left\lfloor \frac{1}{i+1-j\left\lfloor \frac{i}{j} \right\rfloor} \right\rfloor - 1} \right\rfloor \tag{1}$$

$$p_n = \sum_{k=2}^{2^{2n}} k \left\lfloor \frac{1}{1 + (\pi(k) + \pi(k-1) - 2n + 1)^2} \right\rfloor \tag{2}$$

Let $r, s \in \mathbb{R}$. If we suppose that $r \geqslant 0$, we have

$$r = 0 \Rightarrow \left\lfloor \frac{1}{1+r} \right\rfloor = 1 \text{ and } r > 0 \Rightarrow \left\lfloor \frac{1}{1+r} \right\rfloor = 0. \tag{3}$$

https://doi.org/10.1017/mag.2017.9 Published online by Cambridge University Press