A Factoring Lemma

Iurie Boreico, Roman Teleuca

1 Introduction

The following classical problem was used in the Moldavian Mathematical Olympiad.

Problem 1. *Let a, b, c, d be positive integers with $ab = cd$. Prove that $a + b + c + d$ is composite.*

Solution. Let $N = a + b + c + d$. Then

$$aN = a^2 + ab + ac + ad. \tag{1}$$

Because to $ab = cd$, we can rewrite (1) as

$$aN = a^2 + cd + ac + ad = (a + c)(a + d).$$

Both $a + c$ and $a + d$ are greater than a, so each contributes a factor greater than 1 to N. Thus N is composite. □

This solution relies on a clever algebraic trick. However, there is a more consistent and motivated solution that relies on the Factoring Lemma.

Lemma 1. *Let a, b, c, d be positive integers with $ab = cd$. Then there are positive integers m, n, p, q such that $\gcd(n, p) = 1$ and*

$$a = mn,\ b = pq,\ c = mp,\ d = nq.$$

Proof. The condition $ab = cd$ can be rewritten as

$$\frac{a}{c} = \frac{d}{b}.$$

Both fractions have the same representation $\frac{n}{p}$ in lowest terms

$$m = \frac{a}{n} = \frac{c}{p},\ q = \frac{b}{p} = \frac{d}{n}.$$

It is clear that m and q are integers and m, n, p, q have the desired properties. □

Alternative solution to problem 1. We can find positive integers m, n, p, q satisfying the conditions in Lemma 1. Then

$$a + b + c + d = mn + pq + mp + nq = (m + n)(p + q),$$

which explicitly shows that $a + b + c + d$ is composite. □

Not only does Lemma 1 make problem 1 trivial, but it also appears to be useful in many other problems proposed to national and international mathematical olympiads. The techniques can be applied in solving equations and systems of equations over integers. Interesting results can be obtained when this lemma is used in connection with Euclidean rings other than the integers.

2 Diophantine Equations

The problem of Pythagorean triples can be solved using the Factoring Lemma.

Problem 2. *Pairwise relatively prime integers a, b, c satisfy $a^2 + b^2 = c^2$. If a is odd, then there exist integers u and v such that $a = u^2 - v^2$ and $b = 2uv$.*

Solution. Let us rewrite the given condition as

$$b^2 = (c - a)(c + a).$$

By Lemma 1 there exist m, n, p, q such that $b = mn = pq$, $c - a = mp$, $c + a = nq$. Again, by Lemma 1, there exist x, y, z, w such that $m = xy, n = zw, p = xz, q = yw$. This means that $b = xyzw$ and

$$a = \frac{nq - mp}{2} = \frac{yz}{2}(w^2 - x^2).$$

Because w^2 and x^2 are congruent to either 0 or 1 modulo 4 and a is odd, it follows that $2 \mid yz$. On the other hand, yz divides both b and $2a$, so $yz = 2$. This finishes the proof. □

Problem 3. *Pairwise relatively prime positive integers a, b, c satisfy $a^2 + b^2 = 2c^2$. Prove that there exist integers u and v such that*

$$\begin{aligned} a &= u^2 - v^2 + 2uv \\ b &= v^2 - u^2 + 2uv \\ c &= u^2 + v^2. \end{aligned}$$

Solution. We have

$$(a - c)(a + c) = (c - b)(c + b).$$

From Lemma 1, there exist m, n, p, q such that

$$a - c = mn,\ a + c = pq,\ c - b = mp,\ c + b = nq.$$

We thus have

$$pq - mn = mp + nq,$$

implying

$$p(q - m) = n(q + m).$$

Again, there exist x, y, z, w such that

$$p = xy,\ q - m = zw,\ n = xz,\ q + m = yw.$$

We have

$$a = \frac{1}{2}(mn + pq) = \frac{1}{2}\left(\frac{yw - zw}{2}xz + \frac{zw + yw}{2}xy\right) = \frac{xw}{4}(y^2 + 2zy - z^2)$$

and

$$b = \frac{1}{2}(nq - mp) = \frac{1}{2}\left(\frac{yw + zw}{2}xz - \frac{yw - zw}{2}xy\right) = \frac{xw}{4}(-y^2 + 2zy + z^2).$$

It follows that either $xw = 4$ and one of z and y is odd or $xw = 1$ and both z and y are even. We then set $u = y, v = z$ or $u = \frac{y}{2}, v = \frac{z}{2}$, respectively. □

Problem 4. *Prove that there are no positive integers x, y, z such that*

$$2(x^4 - y^4) = z^2.$$

Solution. Suppose there exist such x, y, z. Then consider such a triple with the minimum possible $x + y + z$. If two of x, y, z are divisible by a prime r, then the third number is also divisible by r. If $x = rx_1$, $y = ry_1$, $z = rz_1$, then

$$2r^2(x_1^4 - y_1^4) = z_1^2.$$

Hence $p \mid z_1$ and $z_1 = pz_2$, so

$$2(x_1^4 - y_1^4) = z_2^2.$$

Then x_1, y_1, z_2 is a smaller triple. Thus x, y, z must be pairwise relatively prime.

We have $\gcd(x^2 - y^2, x^2 + y^2) \mid \gcd(2x^2, 2y^2) = 2$. If it equals 1, then both $x^2 - y^2$ and $x^2 + y^2$ are squares, which is impossible. Therefore $\gcd(x^2 - y^2, x^2 + y^2) = 2$ and both x, y are odd. Thus

$$x^2 - y^2 = 4u^2 \quad x^2 + y^2 = 2v^2 \tag{2}$$

for some integers u and v. By Problem 2, there exist integers a and b such that

$$u = ab,\ y = a^2 - b^2,\ x = a^2 + b^2.$$

We have

$$x^2 = 2u^2 + v^2,\ y^2 = v^2 - 2u^2.$$

Thus $(x - v)(x + v) = 2u^2$ and $(v - y)(v + y) = 2u^2$. There exist integers a, b, c, d with $\{x - v, x + v\} = \{2a^2, 4b^2\}$, and $\{v - y, v + y\} = \{2c^2, 4d^2\}$. Because $u = ab = cd$, there exist $m, n, p, q \in \mathbb{Z}$ with $a = mn$, $b = pq$, $c = mp$, $d = nq$. We have $v = |a^2 - 2b^2| = c^2 + 2d^2$. There are two possible cases:

(a) If $a^2 - 2b^2 = c^2 + 2d^2$, then

$$m^2n^2 = 2p^2q^2 + m^2p^2 + 2n^2q^2, \quad m^2(n^2 - p^2) = 2q^2(n^2 + p^2),$$

implying that $|n|, |p|, |mq|$ form a smaller solution.

(b) If $2b^2 - a^2 = c^2 + 2d^2$, then

$$2p^2q^2 = m^2n^2 + m^2p^2 + 2n^2q^2, \quad 2q^2(p^2 - n^2) = m^2(n^2 + p^2),$$

implying that $|n|, |p|, |mq|$ form a smaller triple.

Because both cases lead to a contradiction, the original equation has no solutions. □

3 Sums of two squares and $\mathbb{Z}[i]$

The following is a well-known fact in Number Theory which also appeared as a problem at the Moldavian IMO team selection tests in 2004.

Problem 5. *Let (a, b) and (c, d) be two different unordered pairs of integers such that $a^2 + b^2 = c^2 + d^2 = k$. Prove that k is composite.*

Solution. Without loss of generality, $a > c$ (for if $a = c$, then $b = d$ and the pairs would be the same). We can rearrange the terms to obtain

$$(a - c)(a + c) = (d - b)(d + b). \tag{3}$$

We immediately see that $d > b$. Then $a+c, a-c, d+b, d-b$ are positive integers and due to (3) and Lemma 1 we can find positive integers m, n, p, q with $\gcd(n, p) = 1$ such that

$$a + c = mn,\ a - c = pq,\ d + b = mp,\ d - b = nq.$$

Then

$$a = \frac{mn + pq}{2},\ b = \frac{nq - mp}{2}$$

and

$$\begin{aligned} 4k = 4(a^2 + b^2) &= (mn + pq)^2 + (nq - mp)^2 \\ &= m^2n^2 + p^2q^2 + n^2q^2 + m^2p^2 = (m^2 + q^2)(n^2 + p^2). \end{aligned} \tag{4}$$

Suppose k is prime. Then from (4), without loss of generality, $k \mid m^2 + q^2$. Hence either $n^2 + p^2 = 4$ or $n^2 + p^2 = 2$. The former is impossible, because 4 cannot be represented as the sum of two positive perfect squares. The latter case yields $n = p = 1$, which implies $a = c$, $b = d$ that is again impossible. Thus our assumption is wrong and k is composite. □

Note that along the way we proved the following simple statement.

Lemma 2. *If $a, b, c, d \in \mathbb{Z}$ and $a^2 + b^2 = c^2 + d^2$, then there exist $m, n, p, q \in \mathbb{Z}$ such that*

$$2a = mn + pq,\ 2b = mp - nq,\ 2c = mp + nq,\ 2d = mn - pq.$$

The Factoring Lemma also holds true in the Euclidean ring $\mathbb{Z}[i]$. One application is the following lemma which leads to many interesting results.

Lemma 3. *If a, b, c, d are positive integers such that $a^2 + b^2 = cd$ then there exist integers x, y, z, w, t such that*

$$c = t(x^2 + y^2),\ d = t(z^2 + w^2),\ a = t(xz - yw),\ b = t(xw + yz).$$

Proof. Let $t = \gcd(a, b, c, d)$, $a = ta_1$, $b = tb_1$, $c = tc_1$, $d = td_1$. Then

$$a_1^2 + b_1^2 = c_1 d_1,$$

which can be rewritten as

$$(a_1 + b_1 i)(a_1 - b_1 i) = c_1 d_1. \tag{5}$$

From Lemma (1), there exist $m, n, p, q \in \mathbb{Z}[i]$ such that

$$a_1 + b_1 i = mn,\ a_1 - b_1 i = pq,\ c_1 = np,\ d_1 = mq. \tag{6}$$

Because np and mq are positive integers, it follows that $n = k\overline{p}$ and $q = l\overline{m}$, for some positive rational numbers k and l. On the other hand, $|mn| = |pq|$ implies $|km\overline{p}| = |lp\overline{m}|$ and $k = l$.

Let u, v be relatively prime positive integers such that $k = \frac{u}{v}$. Then

$$a_1 + b_1 i = \frac{u}{v} m\overline{p},\ a_1 - b_1 i = \frac{u}{v} p\overline{m},\ c_1 = \frac{u}{v} p\overline{p},\ d_1 = \frac{u}{v} m\overline{m}.$$

This means that $u \mid a, b, c, d$ and thus $u = 1$. We also have

$$a_1 + b_1 i = \frac{v}{u} n\overline{q},\ a_1 - b_1 i = \frac{v}{u} q\overline{n},\ c_1 = \frac{v}{u} n\overline{n},\ d_1 = \frac{v}{u} q\overline{q},$$

implying $v \mid a, b, c, d$ and thus $v = 1$. Let $n = x + yi$ and $m = z + wi$, where $x, y, z, w \in \mathbb{Z}$. Then (6) implies

$$a_1 = xz - yw,\ b_1 = xw + yz,\ c_1 = x^2 + y^2,\ d_1 = z^2 + w^2,$$

and thus

$$a = t(xz - yw),\ b = t(xw + yz),\ c = t(x^2 + y^2),\ d = t(z^2 + w^2).$$

□

Corollary 1. *If a, b, c are positive integers such that $ab = c^2 + 1$, then a and b can be represented as sums of two perfect squares.*

Proof. By lemma 3 there exist integers x, y, z, t such that

$$t(x^2 + y^2) = a,\ t(z^2 + w^2) = b,\ t(xz - yw) = c,\ t(xw + yz) = 1.$$

This implies $t = 1$ and $a = x^2 + y^2$, $b = z^2 + w^2$.

□

Corollary 2. *Every prime p of the form $4k + 1$ can be represented as a sum of two integer squares.*

Proof. By Wilson's theorem,

$$\begin{aligned} -1 &\equiv (p-1)! = 1 \cdot 2 \cdots 4k \\ &\equiv 1 \cdot 2 \cdots 2k \cdots (2k+1-p) \cdot (2k+2-p) \cdots (4k-p) \\ &\equiv (-1)^{2k}(2k!)^2 = (2k!)^2 \pmod{p}. \end{aligned} \tag{7}$$

From (7), we have

$$(2k!)^2 + 1 = ap,$$

for some integer a and by Corollary 1, p is a sum of two integer squares. □

4 Exercises

The following problems may help the readers sharpen their skills in applying techniques associated with the Factoring Lemma.

Problem 6. *Find all integer solutions to the equation* $x^2 + 3y^2 = z^2$.

Problem 7. *Find all integer solutions to the equation* $x^2 + y^2 = 5z^2$

Problem 8. *Prove that if* $N = a^2 + 2b^2 = c^2 + 2d^2$ *and* $\{a, b\} \neq \{c, d\}$, *then* N *is composite.*

Problem 9. *Prove that no four perfect squares form a non-constant arithmetic sequence.*

Problem 10. (IMO Shortlist, 1998) *Find all positive integers* n *for which there is an integer* m *with* $2^n - 1 \mid m^2 + 9$.

References

[1] Titu Andreescu, Dorin Andrica, An Introduction to Diophantine Equations, GIL Publishing House, 2003.

[2] Titu Andreescu, Dorin Andrica, Zuming Feng, 104 Number Theory Problems: From the training of USA IMO Team, Birkhauser, 2006.

[3] Laurentiu Panaitopol, Alexandru Gica, O introducere in aritmetica si teoria numerelor, Editura Universitatii din Bucuresti, 2001.