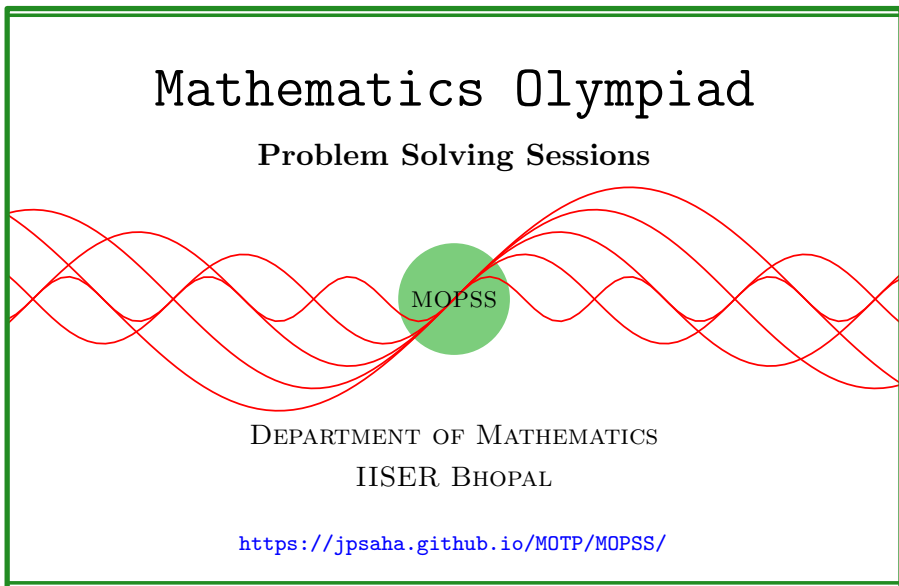


Chinese remainder theorem

MOPSS

6 May 2025



Suggested readings

- Evan Chen's advice [On reading solutions](https://blog.evanchen.cc/2017/03/06/on-reading-solutions/), available at <https://blog.evanchen.cc/2017/03/06/on-reading-solutions/>.
- Evan Chen's [Advice for writing proofs/Remarks on English](https://web.evanchen.cc/handouts/english/english.pdf), available at <https://web.evanchen.cc/handouts/english/english.pdf>.
- [Notes on proofs](#) by Evan Chen from [OTIS Excerpts](#) [[Che25](#), Chapter 1].
- [Tips for writing up solutions](https://www.math.utoronto.ca/barbeau/writingup.pdf) by Edward Barbeau, available at <https://www.math.utoronto.ca/barbeau/writingup.pdf>.
- Evan Chen discusses why [math olympiads are a valuable experience for high schoolers](#) in the post on [Lessons from math olympiads](#), available at <https://blog.evanchen.cc/2018/01/05/lessons-from-math-olympiads/>.

List of problems and examples

1.1	Example (Canada CMO 1991 P1)	2
1.2	Example	2
1.3	Example	3
1.4	Example (India RMO 2015a P3, Canada CMO 1991 P1 Example 1.1)	3
1.5	Example (India RMO 2018b P3)	5

§1 Chinese remainder theorem

Example 1.1 (Canada CMO 1991 P1). Show that the equation $x^2 + y^5 = z^3$ has infinitely many solutions in integers x, y, z for which $xyz \neq 0$.

Walkthrough — Note that

$$2^{10} + 2^{10} = 2^{11}$$

holds. But this does not seem to be of any help! What about $2^{20} + 2^{20}$? Also note that if (x, y, z) is a solution, then another solution can be obtained by multiplying $x^2 + y^5 = z^3$ by k^{30} , namely, $(k^{15}x, k^6y, k^{10}z)$ is also a solution.

Solution 1. Note that

$$(k^{15}2^{10})^2 + (k^62^4)^5 = k^{30}2^{21} = (k^{10}2^7)^3$$

holds for any positive integer k . ■

Example 1.2. Show that there are infinitely many triples (x, y, z) of positive integers such that $x^2 + y = z^7$.

Walkthrough — Does $2^6 + 2^6 = 2^7$ help?

Solution 2. Note that $2^6 + 2^6 = 2^7$ holds. It shows that $(2^3k^7, 2^6k^{14}, 2k^2)$ is a solution to the given equation. This proves the result. ■

Here is another solution to the above problem.

Solution 3. Note that if x, y, z are positive integers satisfying $y = 2x + 1$ and $x^2 + y = z^7$, then $(x + 1)^2 = y^7$ holds, which shows that

$$x = a^7 - 1, z = a^2$$

for some positive integer a . Observe that for any integer $a \geq 2$, the triple $(a^7 - 1, 2(a^7 - 1) + 1, a^2)$ of positive integers satisfy the given equation. Thus the result follows. ■

Example 1.3. There are infinitely many triples (x, y, z) of positive integers such that $x^2 + y^3 = z^7$.

Walkthrough — Note that $2^6 + 2^6 = 2^7$

$$(2^3)^2 + (2^2)^3 = 2^7$$

holds. This shows that $(2^3 k^{3 \cdot 7}, 2^2 k^{2 \cdot 7}, 2k^{2 \cdot 3})$ is a solution to the above equation for any positive integer k .

Here is another argument from [Beu12].

Solution 4. Take three positive integers a, b, c satisfying $a + b = c$. Multiplying it by $a^{21}b^{14}c^6$, we obtain

$$(a^{11}b^7c^3)^2 + (a^7b^5c^2)^3 = (a^3b^2c)^7.$$

■

Remark. The following is a result due to Poonen–Schaefer–Stoll [PSS07], determining the primitive solutions to $x^2 + y^3 = z^7$, that is, the triples of integers having prime factor in common and satisfying this equation. Its proof uses techniques from **Arithmetic Geometry**, and lies beyond the scope of this modest notes, for obvious reasons! The **only purpose** of stating the following result is to indicate that finding all solutions of prescribed nature to some equation (say, the primitive solutions to the above equation) often turns out to be a problem of considerable interest, and may require modern techniques to solve them.

Theorem 1 (Poonen, Schaefer, Stoll)

The primitive solutions to $x^2 + y^3 = z^7$ are the 16 tuples

$$\begin{aligned} &(\pm 1, -1, 0), (\pm 1, 0, 1), \pm(0, 1, 1), (\pm 3, -2, 1), (\pm 71, -17, 2), \\ &(\pm 2213459, 1414, 65), (\pm 15312283, 9262, 113), (\pm 21063928, -76271, 17). \end{aligned}$$

Example 1.4 (India RMO 2015a P3, Canada CMO 1991 P1 Example 1.1). Show that there are infinitely many triples (x, y, z) of integers, such that $x^3 + y^4 = z^{31}$.

Walkthrough —

(a) Note that

$$2^{12k} + 2^{12k} = 2^{12k+1}$$

holds.

(b) It suffices to find an positive integer k such that $12k + 1 = 31\ell$ holds

for some positive integer ℓ . This shows that any such integer ℓ satisfies $\ell \equiv 1 \pmod{3}$, and $\ell \equiv -1 \pmod{4}$, which implies that $\ell \equiv 7 \pmod{12}$. Moreover, if ℓ is congruent to 7 modulo 12, then

$$31\ell - 1 \equiv 31 \cdot 7 - 1 \pmod{12} \equiv 7^2 - 1 \pmod{12} \equiv 0 \pmod{12}$$

holds, or equivalently, there exists an integer k_ℓ such that

$$12k_\ell + 1 = 31\ell$$

holds.

(c) Note that

$$(2^{4k_\ell}, 2^{3k_\ell}, 2^\ell)$$

satisfies the given equation, for any positive integer $\ell \equiv 7 \pmod{12}$.

Remark. Alternatively, one may argue as follows, motivated by the solution of Example 1.3.

Solution 5. Let a, b, c be integers such that $a + b = c$. Multiplying by $a^p b^q c^r$, we get

$$a^{p+1} b^q c^r + a^p b^{q+1} c^r = a^p b^q c^{r+1}.$$

Note that $a^{p+1} b^q c^r, a^p b^{q+1} c^r, a^p b^q c^{r+1}$ are a 3rd, 4th, and a 31st power respectively if 3 divides $p+1, q, r$, 4 divides $p, q+1, r$, 31 divides $p, q, r+1$, which holds if there are positive integers P, Q, R such that

$$p = 4 \cdot 31 \cdot P, q = 3 \cdot 31 \cdot Q, r = 3 \cdot 4 \cdot R$$

holds, and 3 divides $4 \cdot 31 \cdot P + 1$, 4 divides $3 \cdot 31 \cdot Q + 1$, 31 divides $3 \cdot 4 \cdot R + 1$. Since the integers 3, 4, 31 are pairwise coprime, it follows that each of them is coprime to the product of the remaining two integers, and hence, by the division algorithm, there are positive integers P, Q, R such that 3 divides $4 \cdot 31 \cdot P + 1$, 4 divides $3 \cdot 31 \cdot Q + 1$, 31 divides $3 \cdot 4 \cdot R + 1$, or equivalently,

$$P \equiv 2 \pmod{3}, Q \equiv 3 \pmod{4}, R \equiv 18 \pmod{31}$$

holds. In the above, the last congruence is obtained using $(3 \cdot 4) \cdot (6 \cdot 3) \equiv -1 \pmod{31}$, which follows from $3 \cdot 4 \cdot 6 \equiv 10 \pmod{31}$ and $10 \cdot 3 \equiv -1 \pmod{31}$.

This shows that for any positive integers P, Q, R satisfying the above congruence conditions (for instance, $P = 2, Q = 3, R = 18$), and for any positive integers a, b, c satisfying $a + b = c$, the triple

$$((a^{p+1} b^q c^r)^{\frac{1}{3}}, (a^p b^{q+1} c^r)^{\frac{1}{4}}, (a^p b^q c^{r+1})^{\frac{1}{31}})$$

satisfies the given equation, where $p = 124P, q = 93Q, r = 12R$. Hence the given equation has infinitely many solution in integers. \blacksquare

Example 1.5 (India RMO 2018b P3). Show that there are infinitely many tuples (a, b, c, d) of natural numbers such that $a^3 + b^4 + c^5 = d^7$.

Remark. All of the above examples (which excludes Theorem 1!) admit solutions using the Chinese remainder theorem.

References

- [Beu12] FRITS BEUKERS. “The generalized Fermat equation”. In: *Explicit methods in number theory*. Vol. 36. Panor. Synthèses. Soc. Math. France, Paris, 2012, pp. 119–149 (cited p. 3)
- [Che25] EVAN CHEN. *The OTIS Excerpts*. Available at <https://web.evanchen.cc/excerpts.html>. 2025, pp. vi+289 (cited p. 1)
- [PSS07] BJORN POONEN, EDWARD F. SCHAEFER, and MICHAEL STOLL. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. In: *Duke Math. J.*, **137**:1 (2007), pp. 103–158. ISSN: 0012-7094. DOI: [10.1215/S0012-7094-07-13714-1](https://doi.org/10.1215/S0012-7094-07-13714-1). URL: <http://dx.doi.org/10.1215/S0012-7094-07-13714-1> (cited p. 3)