Solving number theory problems with cyclic and symmetric variables

Huy Nguyen, Tam Nguyen

Le Hong Phong High School - July 11, 2013

Abstract

The beauty of many algebraic problems (solving system of equations, proving inequality, ...) comes from the symmetric / cyclic properties of its variables. These properties also exist in a class of number theory problems, but require a different approach to utilize, as the variables in this context are often natural numbers or integers, instead of real numbers. In this article we mention two directions that can be taken into account to solve a variety of cyclic problems. The reader is encouraged to gain familiarity with the technique of Vieta jumping and the concept of p-adic order $\nu_p(n)$, both of which are employed throughout this writing.

1 Turning cyclicity into symmetry

This method is often used in divisibility problems with cyclic conditions

$$a \mid f(b),\ b \mid f(a).$$

If $\gcd(a, b) = 1$, we can construct two functions $g : \mathbb{Z} \to \mathbb{Z}$ and $h : \mathbb{Z}^2 \to \mathbb{Z}$ such that:

- $x \mid g(x)$ for all $x \in \mathbb{Z}$.
- $h(a, b) = f(a) + g(b) = f(b) + g(a)$ is symmetric w.r.t a and b.

It then follows that

$$a \mid h(a, b),\ b \mid h(a, b) \Rightarrow ab \mid h(a, b) \Rightarrow h(a, b) = k \cdot ab, \tag{1}$$

for some $k \in \mathbb{Z}$. (1) is a two-variable equation in terms of a and b. If $\deg h = 1$ we can use inequalities to restrict the domain of a and b to a finite subset of $\mathbb{Z}$. If $\deg h = 2$ we can use Vieta jumping to solve (1).

Without $\gcd(a, b) = 1$, we still have $ab \mid f(a)f(b)$. We can then expand the RHS and remove all multiples of ab, essentially ending up with an equation similar to (1).

Example 1.1

Find prime numbers $p \geq q$ such that

$$q - 1 \mid 3p - 1,\ p - 1 \mid 3q - 1.$$

Solution. Let $a = p - 1,\ b = q - 1$ then $a \geq b \geq 1$ and

$$a \mid 3(b + 1) - 1,\ b \mid 3(a + 1) - 1,$$

which implies

$$ab \mid (3a + 2)(3b + 2) \Leftrightarrow ab \mid 6a + 6b + 4.$$

As a, b are positive integers, divisibility implies that

$$6a + 6b + 4 \geq ab \Rightarrow \frac{6}{a} + \frac{6}{b} + \frac{4}{ab} \geq 1.$$

On the other hand, because $a \geq b$,

$$\frac{12}{b} + \frac{4}{b^2} \geq \frac{6}{a} + \frac{6}{b} + \frac{4}{ab}.$$

We now get a one-variable inequality,

$$\frac{12}{b} + \frac{4}{b^2} \geq 1 \Leftrightarrow b^2 - 12b - 4 \leq 0 \Leftrightarrow 1 \leq b \leq 12.$$

Note that $b + 1 = q$ is prime so $b \in \{1, 2, 4, 6, 10, 12\}$. Knowing b, we can easily infer a:

b	Condition for a	Values of a
1	$a \mid 6a + 6 + 4$	$\{1, 2, 10\}$
2	$2a \mid 6a + 12 + 4$	$\{2, 4\}$
4	$4a \mid 6a + 24 + 4$	$\{6, 10\}$
6	$6a \mid 6a + 36 + 4$	$\emptyset$
10	$10a \mid 6a + 60 + 4$	$\{16\}$
12	$12a \mid 6a + 72 + 4$	$\emptyset$

Hence all possible values of (p, q) are $(2, 2); (3, 3); (5, 3); (7, 5); (17, 11)$. □

Example 1.2

Find the number of tuples (a, b, c) where $a < b < c$ are positive and pairwise coprime integers satisfying

$$a \mid bc - 31,\ b \mid ca - 31,\ c \mid ab - 31.$$

Solution. As $a \mid bc - 31$ and $a \mid a(b + c)$ we have

$$a \mid ab + bc + ca - 31.$$

Similar arguments apply to b and c. Since a, b, c are pairwise coprime,

$$abc \mid ab + bc + ca - 31. \tag{2}$$

Now consider the following cases:

- $a \geq 3$. Then $b \geq 4$ and $c \geq 5$, so $ab + bc + ca > 31$. It also follows that

  $$abc \geq 3bc > ab + bc + ca > ab + bc + ca - 31,$$

  which contradicts (2). Hence this case does not yield any solution.

- $a = 2$. Then $b \mid 2c - 31$ and $c \mid 2b - 31$. It follows that

  $$bc \mid 2b + 2c - 31.$$

  By similar arguments, we get $b = 3$ and $c = 5$.

- $a = 1$. Then $b \mid c - 31$ and $c \mid b - 31$. Note that $b + c = 31$ satisfies both conditions, and there are a total of 14 tuples (a, b, c) satisfying

  $$\begin{cases} a = 1 \\ b + c = 31 \\ a < b < c \end{cases}$$

  If $b + c \neq 31$, we prove that $1 < b, c < 31$. Assume otherwise,

  - If $b > 31$ then $c > b > b - 31 > 0$ so $c \nmid b - 31$, which is false.
  - If $b = 31$ then $31 \mid c - 31$ so $31 \mid c$. But then $\gcd(b, c) = 31 > 1$, which is false.

– If $b < 31 < c$ then $|c| > |b - 31| > 0$ so $c \nmid b - 31$, which is false.

Hence $1 < b < c < 31$. Combining with $b \mid c - 31$ and $c \mid b - 31$, we get

$$bc \mid 31 - b - c.$$

Further consider the following cases:

– If $b \geq 5$ then $c \geq 6$ so $bc \geq 30 > 31 - (b + c)$, which is false.

– If $b = 4$ then $4 \mid c - 31$ and $c \mid 27$, so $c = 27$. However, this is false since we are assuming $b + c \neq 31$.

– If $b = 3$ then $3 \mid c - 31$ and $c \mid 28$, so $c \in \{4, 7\}$.

To sum up, the case $a = 1$ yields 16 possible values of (b, c).

Hence we conclude that there are in total 17 possible tuples (a, b, c). □

Remark 1. In the previous two examples, we try to arrive at a condition of the form

$$xy \mid \alpha x + \beta y + \gamma.$$

We can then use algebraic manipulations to restrict $|x|$ and $|y|$, since if $|x|$ and $|y|$ gets too large, $|xy|$ will quickly outgrow $|\alpha x+\beta y+\gamma|$, which means the divisibility condition cannot be satisfied. This illustrates our initial point that if $\deg h = 1$ we can use inequalities. In case $\deg h > 1$, however, pure algebraic manipulations are no longer effective. Instead, an effective way to tackle higher degree polynomials is Vieta jumping.

Example 1.3

Find all primes $p < q < 1000$ satisfying

$$q \mid p^3 - 1,\ p \mid q^3 - 1.$$

Solution. From

$$q \mid p^3 - 1 = (p - 1)(q^2 + q + 1)$$

and $q > p > p - 1$ we have $q \mid p^2 + p + 1$.

Also $p \mid q^3 - 1 = (q - 1)(q^2 + q + 1)$, so either $p \mid q - 1$ or $p \mid q^2 + q + 1$.

- If $p \mid q-1$ then let $p^2+p+1 = nq$ where $n \in \mathbb{N}^*$. Note that in mod p, $q \equiv 1$ and $p^2+p+1 \equiv 1$ so $n \equiv 1$. Since $q \geq p+1$, we also have

$$n = \frac{p^2+p+1}{q} \leq \left\lfloor \frac{p^2+p+1}{p+1} \right\rfloor = \left\lfloor p + \frac{1}{p+1} \right\rfloor = p,$$

Hence $n = 1$ and $q = p^2+p+1$ so $p^2+p+1 < 1000$. This implies $p \leq 31$, since $37^2+37+1 > 1000$.

We can then brute force to find all values of p and then q. These are

$$(2,7); (3,13); (5,31); (17,307).$$

- If $p \mid q^2+q+1$ then

$$p \mid (q^2+q+1) + (p^2+p), \text{ and}$$
$$q \mid (p^2+p+1) + (q^2+q),$$

so

$$pq \mid p^2+q^2+p+q+1.$$

In other words, for some $m \in \mathbb{N}^*$ we need to find a, b satisfying

$$a^2+b^2+a+b+1 = mab. \tag{3}$$

Rewrite (3) as

$$a^2 + (1-mb)\cdot a + (b^2+b+1) = 0.$$

Let S be the set of all pairs (a,b) satisfying (3). Consider $(a_0, b_0) \in S$ where a_0+b_0 is smallest. WLOG assume $a_0 \geq b_0$.

According to Vieta's theorem, (3) also has another solution (a', b_0) where a' satisfies

$$a_0 + a' = mb_0 - 1, \tag{4}$$
$$a_0 a' = b_0^2 + b_0 + 1. \tag{5}$$

(4) implies that $a' \in \mathbb{Z}$, while (5) implies $a' > 0$. Hence $(a', b_0) \in S$. By the definition of (a_0, b_0), we then have

$$a_0 + b_0 \leq a' + b_0 \Rightarrow a_0 \leq a' = \frac{b_0^2+b_0+1}{a_0} \Rightarrow b_0^2+b_0+1 \geq a_0.$$

If $a_0 > b_0$ then $a_0 \geq b_0+1$, so $a_0^2 > (b_0+1)^2 > b_0^2+b_0+1$, which is false. Hence $a_0 = b_0$, so

$$a_0^2 + (1-a_0)\cdot a_0 + (a_0^2+a_0+1) = 0,$$

which means $a_0 \mid 1 \Rightarrow a_0 = b_0 = 1$. This leads to $m = 5$. (3) then becomes

$$a^2 + b^2 + a + b + 1 = 5ab. \tag{6}$$

As we proved earlier, if (a_0, b_0) is a solution then so is $(5a_0 - b_0 - 1, a_0)$. Hence from one solution $(1, 1)$ we get $(3, 1)$, and then $(13, 3)$, ... We can in fact prove that all solutions of (6) are $(a_i, b_i) = (x_{i+1}, x_i)$ where x_is come from the sequence

$$(x_n) : \begin{cases} x_0 = x_1 = 1 \\ x_{n+1} = 5x_n - x_{n-1} - 1 \text{ for } n \geq 1 \end{cases}$$

The proof for this statement is very similar to that of VMO 2012 P6. All that's left is to find the pairs (x_{i+1}, x_i) from the above sequence such that x_i and x_{i+1} are primes smaller than 1000. It's easy to observe that $i \leq 4$ because $x_6 > 1000$. We then find $(p, q) \in \{(3, 13); (13, 61)\}$.

In conclusion, all possible values of p and q are $(2, 7); (3, 13); (5, 31); (13, 61); (17, 307)$. □

2 Imposing orders on the variables

If the variables are symmetric, we can sort them in ascending or descending order. If the variables are cyclic, we can point out one variable with some maximum / minimum property.

Example 2.1

Consider arbitrary positive numbers a, b, c. Denote (a, b) and $[a, b]$ as the greatest common divisors and lowest common multiples of a and b respectively. Prove that

$$\frac{(a, b) \cdot (b, c) \cdot (c, a)}{(a, b, c)^2} = \frac{[a, b] \cdot [b, c] \cdot [c, a]}{[a, b, c]^2}.$$

Solution. Let L and R denote the LHS and RHS of the equality repspectively. Consider an arbitrary prime p. If $p \nmid [a, b, c]$ then it's obvious that $\nu_p(L) = \nu_p(R) = 0$. On the other hand, if $p \mid [a, b, c]$ then either $p \mid a$ or $p \mid b$ or $p \mid c$. Let $x = \nu_p(a),\ y = \nu_p(b),\ z = \nu_p(c)$. As a, b, c are symmetric, WLOG assume $x \geq y \geq z$, then

$$\nu_p(L) = y + z + z - 2z = y$$

$$\nu_p(R) = x + y + x - 2x = y$$

Hence $\nu_p(L) = \nu_p(R)$ as well. In other words, for any prime p, $\nu_p(L) = \nu_p(R)$, so L and R have the same prime factorization. By the fundamental theorem of arithmetic, $L = R$. □

Example 2.2

Find prime numbers p, q satisfying

$$pq \mid (5^p - 2^p)(5^q - 2^q).$$

Solution. WLOG assume $p \leq q$. Consider the following cases:

- If $p = 3$ then

  $$3q \mid 117(5^q - 2^q) \Rightarrow q \mid 39(5^q - 2^q).$$

  According to Fermat's theorem, $5^q - 2^q \equiv 5 - 2 \equiv 3 \pmod{q}$, so it must be the case that $q \mid 39 \Rightarrow q \in \{3, 13\}$.

- If $5 < p < q$ then, following similar arguments, we have

  $$5^p - 2^p \equiv 5 - 2 \equiv 3 \pmod{p}$$

  so $p \mid 5^q - 2^q$. Further note that $5^{p-1} \equiv 2^{p-1} \equiv 1 \pmod{p}$ so $p \mid 5^{p-1} - 2^{p-1}$.
  As $q > p > p - 1, \gcd(q, p - 1) = 1$, so there exist $m, n \in \mathbb{N}^*$ such that

  $$m \cdot q - n \cdot (p - 1) = 1 \text{ or } m \cdot (p - 1) - n \cdot q = 1. \tag{7}$$

  Consider the following equivalences in mod p:

  $$\begin{cases} 5^{p-1} & \equiv 2^{p-1} \\ 5^q & \equiv 2^q \end{cases} \Rightarrow \begin{cases} 5^{n(p-1)} & \equiv 2^{n(p-1)} \\ 5^{mq} & \equiv 2^{mq} \end{cases}$$

  which yields

  $$5^{n(p-1)}.2^{mq} \equiv 2^{n(p-1)}.5^{mq},$$

  which, combining with (7), implies that $5 \equiv 2 \pmod{p}$ and therefore $p = 3$ (rejected since we are assuming $p > 5$).

In conclusion, all possible values of (p, q) are $(3, 3); (3, 13); (13, 3)$. □

Example 2.3

Find prime numbers p, q satisfying

$$pq \mid 2^p + 2^q.$$

Solution. First note that for any $x \in \mathbb{Z}, \gcd(x-1, x+1) = \gcd(2, x+1) \leq 2$.

WLOG assume $p \geq q$. If $p = q$ then $p^2 \mid 2^{p+1} \Rightarrow p = q = 2$. If $p > q$:

- If $q = 2$ then $2p \mid 2^2 + 2^p$ or $p \mid 2 + 2^{p-1}$ so $p \in \{2, 3\}$.
- If $q > 2$, we have $q \mid 2^p + 2^q = 2^q(2^{p-1} + 1)$ so

$$q \mid 2^{p+1} - 1 \Rightarrow 2^{2(p-q)} \equiv 1 \pmod{p}. \tag{8}$$

  Let a be the smallest positive integer satisfying $2^a \equiv 1 \pmod{q}$ (i.e., a is the order of 2 in $\mathbb{Z}_q$). By the property of order,

$$a \mid q - 1 \text{ and } a \mid 2(p - q).$$

  Let $p - q = 2^k \cdot m, q - 1 = 2^l \cdot n, a = 2^r \cdot s$ where $k + 1 \geq r, l \geq r, s \mid m, s \mid n$ and m, n, s are odd. Consider two cases:

  – If $r = k + 1$ then $l \geq k + 1$, so

$$2(p - q) = 2^{k+1} \cdot m,$$
$$q - 1 = 2^l \cdot n$$

  would imply

$$2(p - q)s = am$$
$$(q - 1)m = (p - q) \cdot n \cdot 2^{l-k-1}.$$

  It then follows that

$$\frac{n \cdot 2^{l-k-1}}{2s} = \frac{(q-1) \cdot m}{2s(p-q)} = \frac{q-1}{a} = \frac{2^l \cdot n}{2^r \cdot s},$$

  which results in

$$2^{l-k-2} = 2^{l-r} \Rightarrow r = k + 2,$$

  which is false. Hence this case does not yield any solution.

– If $r \leq k$ then

$$a \mid p-q \Rightarrow q \mid 2^a - 1 \mid 2^{p-q} - 1. \tag{9}$$

From (8) and (9) we see that $q \mid (2^{p-q} - 1, 2^{p-q} + 1)$. On the other hand, $\gcd(2^{p-q} - 1, 2^{p-q} + 1) \leq 2$ as remarked earlier, so it follows that $q = 2$. However, this is false since we are assuming $q > 2$.

In conclusion, all values of (p, q) are $(2, 2); (2; 3), (3; 2)$.

□

Example 2.4

Consider positive integers x, y, z where $(xy + 1)(yz + 1)(zx + 1)$ is a square. Prove that each of $xy + 1, yz + 1$ and $zx + 1$ is also a square.

Solution. Let $S = \{(x, y, z) \mid (xy + 1)(yz + 1)(zx + 1)$ is square$\}$. Consider the tuple $(x, y, z) \in S$ where $x + y + z$ is smallest. WLOG assume $z = \max\{x, y, z\}$.
Let t be a root of the equation.

$$t^2 + x^2 + y^2 + z^2 - 2(xy + yz + zt + tx + zx + ty) - 4xyzt - 4 = 0.$$

which is equivalent to

$$t^2 - 2t(x + y + z + 2xyz) + x^2 + y^2 + z^2 - 2(xy + yz + zx) - 4 = 0. \tag{10}$$

Note that (10) is equivalent to the following three equations:

$$(x + y - z - t)^2 = 4(xy + 1)(zt + 1) \tag{11}$$

$$(x + z - y - t)^2 = 4(xz + 1)(yt + 1) \tag{12}$$

$$(x + t - y - z)^2 = 4(xt + 1)(yz + 1) \tag{13}$$

and that $t \in \mathbb{Z}$ because (10) has two integer solutions

$$t_{1,2} = x + y + z + 2xyz \pm 2\sqrt{(xy + 1)(yz + 1)(zx + 1)}.$$

Multiplying the LHSs and RHSs of (11), (12), (13) together yields

$$[(x + y + z - t)(x + z - y - t)(x + t - y - z)]^2$$
$$= [8(xy + 1)(yz + 1)(zx + 1)]^2 \cdot [(xt + 1)(yt + 1)(zt + 1)],$$

so $(xt+1)(yt+1)(zt+1)$ is a square. We also have $xt+1, yt+1, zt+1 \geq 0$ and $\max\{x,y,z\} > 1$ because $x=y=z=1$ isn't valid. Hence

$$t > \frac{-1}{\max\{x,y,z\}} > -1.$$

Now consider two cases:

- If $t=0$ then (10) yields

$$(x+y+z)^2 = 4(xy+yz+zx+1) \Leftrightarrow (x+y-z)^2 = 4(xy+1)$$

  so $xy+1$ is a square. By similar arguments, $yz+1$ and $zx+1$ are also squares.

- If $t>0$ then $(x,y,t) \in S$. By the definition of (x,y,z), we see that $t \geq z$, so $t_1 \geq z$ and $t_2 \geq z$. On the other hand, we have

$$\begin{aligned} t_1 t_2 &= x^2+y^2+z^2-2(xy+yz+zx)-4 \\ &\leq z^2 - x(2z-x) - y(2z-y) \\ &< z^2, \end{aligned}$$

  which is false. Hence this case does cannot happen.

In conclusion, each of $xy+1, yz+1$ and $zx+1$ is a square. □

Example 2.5

Find all integers a, b, c satisfying

$$\begin{cases} a^2 - bc = 91 \\ b^2 - ca = 91 \\ c^2 - ab = 91 \end{cases}$$

Solution. WLOG assume $a \leq b \leq c$. As 91 is not a square, we have $a, b, c \neq 0$.

If $a \geq 0$ and $b, c \geq 0$ so $a^2 - bc < 0 < 91$, which is false. Hence $a < 0$.

Also observe that if (a,b,c) satisfies the system of equations then so does $(-a,-b,-c)$.

Hence we only need to consider the tuples (a,b,c) where $c > 0$.

Now if $b = c$ then

$$a^2 - b^2 = 91 = b^2 - ab \Rightarrow a^2 + ab - 2b^2 = (a-b)(a+2b) = 0$$

which implies either $a = b$ or $a = -2b$. If $a = b$ then $a = b = c$ so $a^2 - bc = 0$, which is false. If $a = -2b$ then $5b^2 = 91$, which is also false. Hence it must be the case that $b \neq c$. By similar arguments, $a \neq b$. Now consider two cases:

- If $b > 0$, then we have

$$\begin{aligned} & 91b = b(b^2 - ac),\ 91c = c(c^2 - ab) \\ \Rightarrow\ & 91b - 91c = b^3 - c^3 \\ \Rightarrow\ & 91 = b^2 + bc + c^2 \geq 3b^2 \\ \Rightarrow\ & b \in \{1; 2; 3; 4; 5\}. \end{aligned}$$

  From b it's easy to find a and c. The solutions this case yields are $(-10, 1, 9)$ and $(-11, 5, 6)$.

- If $b < 0$ then

$$\begin{aligned} & 91b = b(b^2 - ac),\ 91a = a(a^2 - bc) \\ \Rightarrow\ & 91(b - a) = b^3 - a^3 \\ \Rightarrow\ & 91 = a^2 + ab + b^2 \geq 3b^2 \\ \Rightarrow\ & b \in \{-1; -2; -3; -4; -5\}. \end{aligned}$$

  The solutions this case yields are $(-9; -1; 10)$ and $(-6; -5; 11)$.

In conclusion, all possible values of (a, b, c) are $(-10, 1, 9)$, $(10, -1, -9)$, $(-11, 5, 6)$, $(11, -5, -6)$, $(-9, -1, 10)$, $(9, 1, -10)$, $(-6, -5, 11)$, and their permutations. □

3 Further practices

Practice 1 (APMO 2002)**.** Find all positive integers a, b satisfying

$$b^2 - a \mid a^2 + b,\ a^2 - b \mid b^2 + a.$$

Practice 2. Prove that there are infinitely many positive integers a, b, c such that

$$ab + 1, bc + 1 \text{ and } ca + 1$$

are all squares.

Practice 3. Find positive and pairwise coprime integers x, y, z satisfying

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \in \mathbb{N}^*.$$

Practice 4. Find integers $2 \leq x \leq y \leq z$ satisfying

$$z \mid xy - 1,\ y \mid zx - 1,\ x \mid yz - 1.$$

Practice 5. Find all positive and pairwise distinct integers $a, b, c > 1$ satisfying

$$(a-1)(b-1)(c-1) \mid abc - 1.$$

Practice 6. Prove that for any positive integers a, b, n, we have

$$(36a + b)(36b + a) \neq 2^n.$$

Practice 7 (VMO 2012)**.** Find all positive odd integers a, b satisfying

$$a \mid b^2 + 2,\ b \mid a^2 + 2.$$

Practice 8 (VMO 2013)**.** Find all positive integers $a, b, c, a', b', c' \in \{0, 1, \ldots, 14\}$ satisfying

$$\begin{aligned} ab + a'b' &\equiv 1 \pmod{15} \\ bc + b'c' &\equiv 1 \pmod{15} \\ ca + c'a' &\equiv 1 \pmod{15} \end{aligned}$$