Solutions of the Congrunces $x^3 + y^3 \equiv 0 (mod\ p)$, $x^3 - y^3 \equiv 0 (mod\ p)$, and $x^6 - y^6 \equiv 0 (mod\ p)$ for a prime number p

Ali Astaneh,PD(Lon), Vancouver BC, Canada

As in the previous Article 6, this article might also have been entitled "Solutions of the Diophantine equations $x^3 + y^3 = pz$ and $x^3 - y^3 = pz$ for prime number p", simply because the two statements are equivalent; if (x, y) is a possible pair of integers satisfying the any of the equations for a given integer z, then the pair (x, y) satisfies the corresponding congruency. However, it would be more common stick to the terminology in the title, as to find the solutions to the congruences we will be using are a couple facts for congruency of integers. In this regard we recall if p is an odd prime number, then the set $\mathbb{Z}$ of integers is partitioned into p disjoint classes integers as $\mathbb{Z} = [0] \cup,[1] \cup \ldots \cup [p-1]$, where for each $i = 1, 2, \ldots, (p-1)$ the class $[i]$ consists of all integers $[i] = \{i + kp : k \in \mathbb{Z}\}$. Therefore, as expected, here all solutions of the congruences $x^3 + y^3 \equiv 0\ (mod\ p)$ and $x^3 - y^3 \equiv 0\ (mod\ p)$ will be obtained in terms of "class solutions" $(x, y) = ([u], [v]), u, v \in \mathbb{Z}$.
We will first deal with the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$. As we will shortly see, in general, depending on the prime number p, the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$ will have only *trivial* class solutions of the form $(x, y) = ([u], [-u]), u \in \mathbb{Z}$, or else apart from the *trivial* solutions the congruency also has a further $2(p-1)$ infinitely more "sequences" of class solutions as described in Theorem 1 of the article.
Note that the *trivial* solution classes in particular include the class solution $([0], [0])$, meaning all ordered pairs of the $(up, vp), u, v \in \mathbb{Z}$.

In providing description of the *non-trivial* class solutions of the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$ we need to recall the following Lemma (proved as Lemma 2 in Article 6), keeping in mind that any odd prime number is either of the form $p = 3k - 1$, or else $p = 3k + 1, , k = 1, 2, \ldots$.

Lemma : Give an odd prime number p the integer -3 is a quadratic residue $(mod\ p)$ if and only if p is of the form $p = 3k + 1$.

Indeed, since the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$ is equivalent to

$$(x + y)(x^2 - xy + y^2) \equiv 0\ (mod\ p),$$

and since the option $(x + y) \equiv 0\ (mod\ p)$ only leads to the *trivial* class solutions described earlier, we only need to deal with the potential class solutions of the second option $(x^2 - xy + y^2) \equiv 0\ (mod\ p)$. To this end, we can assume without loss of generality that y is even, say $y = 2n$, otherwise we set $X = P - x$, $Y = P - y$ and deal with the congruency $X^3 + Y^3 \equiv 0\ (mod\ p)$ where Y is even.
Assuming $y = 2n$, the congruency $(x^2 - xy + y^2) \equiv 0\ (mod\ p)$ can be expressed as

$$(x - n)^2 \equiv -3\, n^2 (mod\ p). \quad (1)$$

Now we bring the Theorem describing all class solutions of the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$. Not that for part **(b)** of the Theorem 1 bellow we use the above Lemma, and assume that when $p = 3k + 1$ there exists an integer $1 \leq r \leq \frac{p-1}{2}$ for which the congruency $r^2 \equiv -3\ (mod\ p)$ holds.

Theorem 1(Astaneh) Let p be an odd prime number, and consider the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$, then;

(a) If $p = 3k - 1, k = 1, 2, \ldots$; then the only class solutions of the congruency are the *trivial* ones of the form $([u], [-u])$, $u \in \mathbb{Z}$. Note that *trivial* class solutions $([0], [0]) = \{(up. vp): u, v \in \mathbb{Z}\}$ is included here.

(b) If $p = 3k + 1, k = 1, 2, \ldots$, then apart from the *trivial* class solutions $([u], [-u])$, the congruency has a remaining $2(p-1)$ "sequences" of class solutions defined in terms of the specific integers $1 \leq r \leq \frac{p-1}{2}$, where r is the quadratic root $(mod\ p)$ of the -3, that is $r^2 \equiv -3\ (mod\ p)$. As for class solutions (x, y) in which y is even, say $y = 2n$, we have class solutions are given by,

(i) $(X, Y) = ([kp + (r+1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

(ii) $(X, Y) = ([kp - (r-1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

And for class solutions (x, y) with odd integer y, the solutions are given by,

(iii) $(X, Y) = ([kp + (r+1)n]\ , [p - 2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

(iv) $(X, Y) = ([kp - (r-1)n]\ , [p - 2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

As observed here, class solutions (i)-(iv) above produce a total of $2(p-1)$ "sequences" of *non-trivial* class solutions for the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$.

Note: Since the congruency $x^3 + y^3 \equiv 0\ (mod\ p)$ is symmetric in terms of x and y, from number theoretic point of view it only makes sense not to distinguish between solutions (x, y) and (y, x). Keeping this convention in mind, Theorem 1 describes all existing solutions of the congruency under the discussion.

Proof: **(a)** When $p = 3k - 1, k = 1, 2, \ldots$ the congruency (1) preceding Theorem,

$$(x - n)^2 \equiv -3\ n^2 (mod\ p)$$

has no solution, because by Lemma 2, the integer -3 isn't a quadratic residue $(mod\ p)$. Therefore, the congruency $X^3 + Y^3 \equiv 0\ (mod\ p)$ can only have the *trivial* class solutions.

(b) When $p = 3k - 1, k = 1, 2, \ldots$, first assuming that in the congruency $(x^2 - xy + y^2) \equiv 0\ (mod\ p)$ the integer y is even, $y = 2n$, and considering that any solution belongs to a class solution since any solution $([x], [y])$ with $1 \leq y \leq p - 1$, the integer n can only take values $n = 1, 2, \ldots, \frac{p-1}{2}$. Now since there is an integer $1 \leq r \leq \frac{p-1}{2}$ satisfying $r^2 \equiv -3\ (mod\ p)$, the congruency (1) implies

$(x - n)^2 \equiv -3\ n^2 (mod\ p) => (x - n)^2 \equiv (rn)^2 (mod\ p) =>$
$[(x - n)^2 - (rn)^2] \equiv 0 (mod\ p) => [x - (r+1)n][x + (r-1)n] \equiv 0 (mod\ p).$
Therefore either $x - (r+1)n \equiv 0 (mod\ p)$, implying $x = kp + (r+1)n, k \in \mathbb{Z}$, or $x + (r-1)n \equiv 0 (mod\ p)$, implying $x = kp - (r-1)n, k \in \mathbb{Z}$. Now considering $y = 2n$, the first case produces class solutions

(i) $(x, y) = ([kp + (r+1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z},$

and the second case produces class solutions

(ii) $(x, y) = ([kp - (r-1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$.

Now, if y is odd, then $p - y$ is even, and substituting this in (i) and (ii) above we get the rest of the class solutions as

(iii) $(x, y) = ([kp + (r + 1)n], [p - 2n]), n = 1, 2, ..., \frac{p-1}{2}; k \in \mathbb{Z}$

(iv) $(x, y) = ([kp - (r - 1)n], [p - 2n]), n = 1, 2, ..., \frac{p-1}{2}; k \in \mathbb{Z}$.

And the proof of the Theorem is complete.
Here are three examples, first one regarding part (a) and the last two for part (b).

Example 1 For the congruency $x^3 + y^3 \equiv 0\ (mod\ 11)$, since $p = 11 = 4 \times 3 - 1$, by part **(a)** of the Theorem the only class solutions of the congruency are the *trivial* ones $([u], [-u])$, $u \in \mathbb{Z}$.

Example 2 For the congruency $x^3 + y^3 \equiv 0\ (mod\ 7)$, since $p = 2 \times 3 + 1$, by part **(**b) of the Theorem apart from *trivial* class solutions $([u], [-u])$, $u \in \mathbb{Z}$, we also have $2(p - 1) = 12$ sequences of class solutions, each involving the quadratic root r of the integer $-3\ (mod\ 7)$ which happens to be $r = 2$, as $2^2 \equiv -3\ (mod\ 7)$. By part (b) of the Theorem the remaining class solutions are as follows,

(i) $(x, y) = ([7k + 3n], [2n]), n = 1, 2, 3; k \in \mathbb{Z}$,
(ii) $(x, y) = ([7k - n], [2n]), n = 1, 2, 3\ ; k \in \mathbb{Z}$.
(iii) $(x, y) = ([7k + 3n], [7 - 2n]), n = 1, 2, 3\ ; k \in \mathbb{Z}$
(iv) $(x, y) = ([7k - n], [7 - 2n]), n = 1, 2, 3\ ; k \in \mathbb{Z}$.

Example 3 For the congruency $x^3 + y^3 \equiv 0\ (mod\ 13)$, since $p = 4 \times 3 + 1$, again by part (b) of the Theorem apart from *trivial* class solutions $([u], [-u])$, $u \in \mathbb{Z}$, we also have $2(p - 1) = 24$ sequences of class solutions, each involving the quadratic root r of the integer $-3\ (mod\ 13)$ which happens to $r = 6$, as $6^2 \equiv -3\ (mod\ 13)$. Again, by part (b) of the Theorem the remaining class solutions are as follows,

(i) $(x, y) = ([13k + 7n], [2n]), n = 1, 2, 3, 4, 5, 6; k \in \mathbb{Z}$,
(ii) $(x, y) = ([13k - 5n], [2n]), n = 1, 2, 3, 4, 5, 6\ ; k \in \mathbb{Z}$.
(iii) $(x, y) = ([13k + 7n], [13 - 2n]), n = 1, 2, 3, 4, 5, 6\ ; k \in \mathbb{Z}$
(iv) $(x, y) = ([13k - 5n], [13 - 2n]), n = 1, 2, 3, 4, 5, 6\ ; k \in \mathbb{Z}$.

Now we deal with the similar congruency $x^3 - y^3 \equiv 0\ (mod\ p)$ in the title of the article. As one might expect, we will again make use Lemma prior to Theorem 1 to find the "sequences" of class solutions of this congruency as well. More precisely keeping in mind that in part **(b)** of the following Theorem 2 the integer -3 is a quadratic residue $(mod\ p)$, we first note that and the congruency $x^3 - y^3 \equiv 0\ (mod\ p)$ is equivalent to

$$(x - y)(x^2 + xy + y^2) \equiv 0\ (mod\ p),$$

and the option $(x - y) \equiv 0\ (mod\ p)$ only produces *trivial* class solutions $([u], [u])$, $u \in \mathbb{Z}$. Again to find solutions for the second option $(x^2 + xy + y^2) \equiv 0\ (mod\ p)$, without loss of generality we can assume that $1 \leq y \leq p - 1$ is even, say $y = 2n$, otherwise we set $X = P - x$, $Y = P - y$ and deal with the congruency $X^2 + XY + Y^2 \equiv 0\ (mod\ p)$ where Y is even. Now, assuming that $y = 2n$, the congruency $(x^2 + xy + y^2) \equiv 0\ (mod\ p)$ can be expressed as

$$(x + n)^2 \equiv -3\, n^2 (mod\ p). \quad (2)$$

Again, when -3 is a quadratic residue $(mod\ p)$, all class solutions of the congruency $(x^2 + xy + y^2) \equiv 0\ (mod\ p)$ will be expressed in terms of the integer $1 \leq r \leq \frac{p-1}{2}$ satisfying $r^2 \equiv -3\ (mod\ p)$, as (2) implies $x = rn - n$ or $x = -rn - n$.

As observed here, class solutions (i)-(iv) above produce a total of $2(p-1)$ "sequences" of *non-trivial* class solutions for the congruency $x^3 - y^3 \equiv 0 \ (mod\ p)$.

Again note since a pair of integers (x, y) is a solution of the congruency $x^3 - y^3 \equiv 0 \ (mod\ p)$ if and only if (y, x) is, we distinguish between solutions (x, y) and (y, x). Keeping this convention in mind, ow bring the second Theorem.

Theorem 2 (Astaneh) Let p bean odd prime number, and consider the congruency $x^3 - y^3 \equiv 0 \ (mod\ p)$, then;

(a) If $p = 3k - 1, k = 1, 2, \ldots$; then the only class solutions of the congruency are the *trivial* ones of the form $([u], [u])$, $u \in \mathbb{Z}$. Note that class solutions $([0], [0]) = \{(up. vp): u, v \in \mathbb{Z}\}$ is included here.

(b) If $p = 3k + 1, k = 1, 2, \ldots$, then apart from the *trivial* class solutions $([u], [u])$, the congruency has a remaining $2(p-1)$ sequences of class solutions defined in terms of the integer $1 \leq r \leq \frac{p-1}{2}$ where r is the quadratic root $(mod\ p)$ of the -3, that is $r^2 \equiv -3 \ (mod\ p)$. First, for class solutions (x, y) in which y is even, say $y = 2n$, class solutions are given by

(i) $(X, Y) = ([kp + (r-1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

(ii) $(X, Y) = ([kp - (r+1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

Secondly, class solutions (x, y) for which y is odd are given by

(iii) $(X, Y) = ([kp + (r-1)n]\ , [p - 2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

(iv) $(X, Y) = ([kp - (r+1)n]\ , [p - 2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z}$

Again we observe that (i)-(iv) above produce a total of $2(p-1)$ "sequences" of *non-trivial* class solutions for the congruency $x^3 - y^3 \equiv 0 \ (mod\ p)$.

Note: Since the congruency $x^3 + y^3 \equiv 0 \ (mod\ p)$ is symmetric in terms of x and y it only makes sense not to distinguish between solutions (x, y) and (y, x). Keeping this in mind the above Theorem 2 describes all existing solutions of the congruency.

Proof: **(a)** When $p = 3k - 1, k = 1, 2, \ldots$ the congruency (1) preceding Theorem,

$$(x + n)^2 \equiv -3\ n^2 (mod\ p)$$

has no solution, because by Lemma 2, the integer -3 isn't a quadratic residue $(mod\ p)$. Therefore, the congruency $X^3 + Y^3 \equiv 0 \ (mod\ p)$ can only have the *trivial* class solutions.

(b) When $p = 3k + 1, k = 1, 2, \ldots$, first assuming that in the congruency $(x^2 + xy + y^2) \equiv 0 \ (mod\ p)$ the integer y is even, $y = 2n$, we first try to find clss solutions of the form $([x], [2n])$ where $n = 1, 2, \ldots, \frac{p-1}{2}$. Now since there is an integer $1 \leq r \leq \frac{p-1}{2}$ satisfying $r^2 \equiv -3 \ (mod\ p)$, the congruency (1) implies

$(x + n)^2 \equiv -3\ n^2 (mod\ p) \Rightarrow (x + n)^2 \equiv (rn)^2 (mod\ p) \Rightarrow$
$[(x + n)^2 - (rn)^2] \equiv 0 (mod\ p) \Rightarrow [x - (r-1)n][x + (r+1)n] \equiv 0 (mod\ p)$.
Therefore either $x - (r-1)n \equiv 0 (mod\ p)$, implying $x = kp + (r-1)n, k \in \mathbb{Z}$, or else $x + (r+1)n \equiv 0 (mod\ p)$, implying $x = kp - (r+1)n, k \in \mathbb{Z}$. Now considering $y = 2n$, the first case produces class solutions

(i) $(x, y) = ([kp + (r-1)n]\ , [2n]), n = 1, 2, \ldots, \frac{p-1}{2}; k \in \mathbb{Z},$

and the second case produces class solutions

(ii) $(x,y) = ([kp-(r+1)n]\,,[2n]), n = 1,2,\ldots,\frac{p-1}{2}; k \in \mathbb{Z}$.

Now, if y is odd, then $p-y$ is even, and substituting this in (i) and (ii) above we get the rest of the class solutions as

(iii) $(x,y) = ([kp+(r-1)n]\,,[p-2n]), n = 1,2,\ldots,\frac{p-1}{2}; k \in \mathbb{Z}$

(iv) $(x,y) = ([kp-(r+1)n]\,,[p-2n]), n = 1,2,\ldots,\frac{p-1}{2}; k \in \mathbb{Z}$.

And the proof of the Theorem is complete.
Here are three examples, first one regarding part (a) and the last two for part (b).

Example 1 For the congruency $x^3 - y^3 \equiv 0\ (mod\ 11)$, since $p = 11 = 4\times 3 - 1$, by part **(a)** of the Theorem 2 the only class solutions of the congruency are the *trivial* ones $([u],[u]), u \in \mathbb{Z}$.

Example 2 For the congruency $x^3 - y^3 \equiv 0\ (mod\ 7)$, since $p = 2\times 3 + 1$, by part **(b)** of the Theorem 2 apart from *trivial* class solutions $([u],[u]), u \in \mathbb{Z}$, we also have $2(p-1) = 12$ sequences of class solutions, each involving the quadratic root r of the integer $-3\ (mod\ 7)$ which happens to be $r = 2$, as $2^2 \equiv -3\ (mod\ 7)$. By part (b) of the Theorem the remaining class solutions are as follows,

(i) $(x,y) = ([7k+n]\,,[2n]), n = 1,2,3; k \in \mathbb{Z}$,
(ii) $(x,y) = ([7k-3n]\,,[2n]), n = 1,2,3\ ; k \in \mathbb{Z}$.
(iii) $(x,y) = ([7k+n]\,,[7-2n]), n = 1,2,3\ ; k \in \mathbb{Z}$
(iv) $(x,y) = ([7k-3n]\,,[7-2n]), n = 1,2,3\ ; k \in \mathbb{Z}$.

Example 3 For the congruency $x^3 - y^3 \equiv 0\ (mod\ 13)$, since $p = 4\times 3 + 1$, again by part **(b)** of the Theorem 2 apart from *trivial* class solutions $([u],[u]), u \in \mathbb{Z}$, we also have $2(p-1) = 24$ sequences of class solutions, each involving the quadratic root r of the integer $-3\ (mod\ 13)$ which happens to $r = 6$, as $6^2 \equiv -3\ (mod\ 13)$. Again, by part (b) of the Theorem the remaining class solutions are as follows,

(i) $(x,y) = ([13k+5n]\,,[2n]), n = 1,2,3,4,5,6; k \in \mathbb{Z}$,
(ii) $(x,y) = ([13k-7n]\,,[2n]), n = 1,2,3,4,5,6\ ; k \in \mathbb{Z}$.
(iii) $(x,y) = ([13k+5n]\,,[13-2n]), n = 1,2,3,4,5,6\ ; k \in \mathbb{Z}$
(iv) $(x,y) = ([13k-7n]\,,[13-2n]), n = 1,2,3,4,5,6\ ; k \in \mathbb{Z}$.

The last theorem of the article describes class solutions for the last congruency $x^6 - y^6 \equiv 0\ (mod\ p)$ in the title.

Theorem 3 (Astaneh) Let p bean odd prime number, and consider the congruency $x^6 - y^6 \equiv 0\ (mod\ p)$, then;

(a) If $p = 3k-1, k = 1,2,\ldots$; then the only class solutions of the congruency are the *trivial* ones of the form $([u],[u]), u \in \mathbb{Z}$ $([u],[-u]), u \in \mathbb{Z}$.

(b) If $p = 3k+1, k = 1,2,\ldots$, then apart from the *trivial* class solutions of the form $([u],[u]), u \in \mathbb{Z}$ $([u],[-u]), u \in \mathbb{Z}$, the remaining class solutions of the congruency are all class solutions listed as (i)-(iv) in part **(b)** of Theorem 1 plus all class solutions listed as (i)-(iv) in part **(b)** of Theorem 2.

Proof: **(a)** Simply because the congruency $x^6 - y^6 \equiv 0\ (mod\ p)$ is equivalent to the system of congruences consisting of the two congruences $x^3 + y^3 \equiv 0\ (mod\ p)$ and $x^3 - y^3 \equiv 0\ (mod\ p)$.

(b) Fe reason as in the proof of part **(a)** .