

BIỂU DIỄN MỘT SỐ NGUYÊN DƯỚI DẠNG $x^2 + Dy^2$

Lê Thị Hà

Khoa Toán - Tin, Trường Đại học Sư phạm Hà Nội

Tóm tắt. Trong bài báo này tác giả đưa ra điều kiện cần để một số nguyên tố lẻ hay số đối của nó có thể biểu diễn được dưới dạng toàn phương nhị phân $x^2 + Dy^2$, với các số nguyên D mà $-D$ là số nguyên tố trong khoảng $[5; 23]$. Từ đó tác giả đưa ra điều kiện cần và đủ để một số nguyên có thể biểu diễn dưới dạng này.

Từ khóa: Dạng toàn phương, số nguyên tố, kí hiệu Legendre, thặng dư bậc 2.

1. Mở đầu

Một dạng toàn phương nhị phân là một đa thức hai biến

$$q(x, y) = ax^2 + bxy + cy^2,$$

với a, b, c là những số nguyên. Vấn đề biểu diễn các số nguyên dưới dạng toàn phương nhị phân từ lâu đã được rất nhiều nhà Toán học quan tâm. Chúng ta có thể tìm thấy nhiều kết quả đề cập đến vấn đề biểu diễn một số nguyên tố dưới dạng toàn phương nhị phân đặc biệt

$$x^2 + Dy^2, \tag{1.1}$$

với D là một số nguyên khác 0 không có nhân tử nào là số chính phương khác 1. Với $D = 1$, Fermat đã chỉ ra rằng một số nguyên tố p biểu diễn được duy nhất dưới dạng tổng hai số chính phương nếu và chỉ nếu nó có dạng $4n + 1$. Người ta cũng có thể tìm thấy trong các công trình của ông các kết quả với $D = 2, D = 3$. Cụ thể nếu p là một số nguyên tố lẻ thì:

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \iff p \equiv 1, 3 \pmod{8},$$

$$p = x^2 + 3y^2, x, y \in \mathbb{Z} \iff p = 3 \text{ hoặc } p \equiv 1 \pmod{3}.$$

Trong [1], Cox đã giải quyết hoàn toàn vấn đề biểu diễn một số nguyên tố dưới dạng (1.1), nhưng với D là số nguyên dương. Để giải quyết các trường hợp tổng quát, ông đã sử dụng các kiến thức liên quan đến lý thuyết lớp trường. Tuy nhiên Cox đã không đề cập đến biểu diễn một số nguyên bất kì dưới dạng đó. Cùng giải quyết vấn đề với nhiều giá trị nguyên dương D , nhưng trong [2], Hagedorn đã có cách tiếp cận sơ cấp bằng việc sử dụng định lí lỗi Minkowski.

Ngày nhận bài: 13/3/2020. Ngày sửa bài: 26/3/2020. Ngày nhận đăng: 31/3/2020.

Tác giả liên hệ: Lê Thị Hà. Địa chỉ e-mail: lethiha@gmail.com

Năm 1966, trong bài báo của mình [3], Mordell đã sử dụng định lý Minkowski về các dạng tuyến tính, đồng thời cũng sử dụng kí hiệu Legendre để giải quyết vấn đề với một số trường hợp D là số nguyên âm và D là số nguyên dương. Chúng ta cũng có thể tìm thấy các kết quả đó trong [4]. Cụ thể, cùng xét các số nguyên tố lẻ p thoả mãn $\left(\frac{-D}{p}\right) = 1$, thì với các giá trị $D = -2; -5; -13; -17$, p biểu diễn được dưới dạng (1.1); Với các giá trị $D = -3; -6; -7; -11; -14; -15; -19$, thì hoặc p hoặc $-p$ đều biểu diễn được dưới dạng $x^2 + Dy^2$; Riêng với $D = -10$ thì hoặc p hoặc $-p$ hoặc $2p$ có thể biểu diễn được dưới dạng (1.1). Mordell chỉ chứng minh chi tiết cho trường hợp $D = -19$ và đối với các giá trị D ở trên, ông cũng không đưa ra điều kiện cần và đủ để một số nguyên có thể biểu diễn được dưới dạng (1.1).

Trong [5], Clark đã sử dụng Bổ đề Thue (đó là một kết quả về đồng dư thức), kí hiệu Legendre và luật thuận nghịch về thặng dư bậc 2 để đưa ra điều kiện cần cho một số nguyên tố biểu diễn được dưới dạng toàn phương nhị phân đặc biệt với nhiều giá trị nguyên D . Từ đó Clark đưa ra điều kiện cần và đủ để một số nguyên biểu diễn được dưới dạng đó. Tuy nhiên Clark chủ yếu chỉ giải quyết vấn đề với những số nguyên dương, còn đối với D là số nguyên âm, Clark chỉ xét $D = -2$ và $D = -3$. Phương pháp của Clark không áp dụng được cho $D = -5$.

Trong bài báo này, tác giả sẽ sử dụng các kết quả của Mordell cùng với các kiến thức cơ bản về lý thuyết số để giải quyết vấn đề biểu diễn một số nguyên dưới dạng (1.1) với các giá trị cụ thể của D mà $-D$ là số nguyên tố trong khoảng [5; 23].

2. Nội dung nghiên cứu

2.1. Cơ sở lý thuyết

2.1.1. Thặng dư bậc hai

Định nghĩa 2.1. Cho một số nguyên tố lẻ p và một số nguyên a nguyên tố cùng nhau với p . Số nguyên a được gọi là một thặng dư bậc hai modulo p nếu phương trình đồng dư $x^2 \equiv a \pmod{p}$ có nghiệm; a được gọi là một bất thặng dư bậc hai modulo p nếu phương trình đồng dư $x^2 \equiv a \pmod{p}$ vô nghiệm.

Định nghĩa 2.2. Cho một số nguyên tố lẻ p và một số nguyên a nguyên tố cùng nhau với p . Kí hiệu Legendre $\left(\frac{a}{p}\right)$ được xác định như sau:

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{nếu } a \text{ là một thặng dư bậc hai modulo } p \\ -1 & \text{nếu } a \text{ là một bất thặng dư bậc hai modulo } p. \end{cases}$$

Định lý 2.1. Cho một số nguyên tố lẻ p và một số nguyên a nguyên tố cùng nhau với p . Khi đó:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Định lý 2.2. Với p là một số nguyên tố lẻ. Ta có:

$$i) \left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Biểu diễn một số nguyên dưới dạng $x^2 + Dy^2$

$$ii) \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Định lí 2.3 (Luật thuận nghịch). Cho hai số nguyên tố lẻ phân biệt p và q . Khi đó ta có:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right),$$

hay

$$\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Các chứng minh của các kết quả trên có thể được tìm thấy trong [6].

2.1.2. Dạng toàn phương nhị phân

Định nghĩa 2.3. Một dạng toàn phương nhị phân $q(x, y) = ax^2 + bxy + cy^2$ được gọi là nguyên thủy nếu $(a, b, c) = 1$ và được gọi là bất đẳng hướng (anisotropic) nếu từ $q(x, y) = 0$ với $x, y \in \mathbb{Z}$ suy ra $x = y = 0$.

Dạng toàn phương $q(x, y)$ được gọi là xác định dương nếu với mọi $x, y \in \mathbb{R}$, $q(x, y) \geq 0$ và dấu bằng xảy ra khi và chỉ khi $(x, y) = (0, 0)$. Nếu tồn tại $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ sao cho $q(x_1, y_1) > 0, q(x_2, y_2) < 0$ thì $q(x, y)$ được gọi là không xác định.

Biệt thức của $q(x, y)$ được xác định bởi $\Delta = b^2 - 4ac$.

Bằng tính toán trực tiếp chúng ta nhận được kết quả sau:

Mệnh đề 2.1. Với các số nguyên D, x_1, x_2, y_1, y_2 ta có:

$$(x_1^2 + Dy_1^2)(x_2^2 + Dy_2^2) = (x_1x_2 - Dy_1y_2)^2 + D(x_1y_2 + x_2y_1)^2.$$

Nhận xét 2.1. Từ mệnh đề trên ta suy ra rằng tập các số nguyên được biểu diễn dưới dạng (1.1) là đóng với phép nhân.

Định lí 2.4. Giả sử $q(x, y) = ax^2 + bxy + cy^2$ là một dạng toàn phương nguyên thủy bất đẳng hướng với biệt thức Δ và p là một số nguyên tố lẻ sao cho $\left(\frac{\Delta}{p}\right) = -1$. Khi đó

i) Nếu có $x, y \in \mathbb{Z}$ sao cho $p \mid q(x, y)$ thì $p \mid x$ và $p \mid y$.

ii) Với mọi $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, $\text{ord}_p(q(x, y))$ là số chẵn.

Ở đó kí hiệu $\text{ord}_p(n)$ là số mũ của p trong phân tích tiêu chuẩn của số nguyên n .

Để chứng minh Định lí 2.4 người ta đã sử dụng kiến thức về Toán Cao cấp như miền nguyên, vành nhân tử hoá duy nhất, ideal nguyên tố,... Chúng ta có thể tham khảo chứng minh định lí trong [5].

2.2. Bổ đề Thue

Bổ đề Thue là một kết quả rất sơ cấp về đồng dư thức, nhưng lại có nhiều ứng dụng trong Lí thuyết số, được phát biểu bởi nhà Toán học Axel Thue người Na Uy vào năm 1902.

Bổ đề 2.1. (Bổ đề Thue)

Cho n là một số nguyên dương và c là một số nguyên dương nguyên tố cùng nhau với n . Khi đó tồn tại các số nguyên x và y sao cho:

$$i) \ 0 < |x|, |y| \leq \sqrt{n}.$$

$$ii) \ x \equiv cy \pmod{n}.$$

Chứng minh: Xem trong [5].

Áp dụng Bổ đề Thue, Clark đã chứng minh một kết quả sau đây:

Định lí 2.5. Cho $q(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ là một dạng toàn phương bất đẳng hướng với biệt thức $\Delta = b^2 - 4ac$. Giả sử n là một số nguyên dương không là số chính phương sao cho $(n, 2C) = 1$ và Δ là một bình phương modulo n . Khi đó:

$$i) \ \text{Tồn tại các số nguyên } k, x, y \text{ với } 0 < |x|, |y| \leq \sqrt{n}, \ 0 < |k| < |a| + |b| + |c| \text{ sao cho}$$

$$q(x, y) = kn.$$

$$ii) \ \text{Nếu } q \text{ xác định dương thì } k > 0.$$

$$iii) \ \text{Nếu } a > 0, b = 0, c < 0 \text{ thì } c < k < a.$$

$$iv) \ \text{Nếu } ac < 0 \text{ thì } |k| < \max(|a| + |b|, |c| + |b|).$$

Nhận xét 2.2.

i) Áp dụng Định lí 2.5 trên với trường hợp đặc biệt $a = 1, b = 0$, kết hợp với Định lí 2.4, Clark đã đưa ra điều kiện cần và đủ để một số nguyên khác 0 có thể biểu diễn dưới dạng (1.1) đối với một số giá trị D nguyên dương và $D = -2; -3$. Xem chi tiết trong [5].

ii) Với việc sử dụng Định lí 2.5, Clark không thể giải quyết được vấn đề với $D = -5$. Thật vậy, áp dụng Định lí 2.5.iii với $a = 1, b = 0, c = D = -5$, và $n = p$ là số nguyên tố lẻ thoả mãn $\left(\frac{5}{p}\right) = 1$, tức là $p \equiv 1, 4 \pmod{5}$, ta suy ra tồn tại các số nguyên k, x, y sao cho $x^2 - 5y^2 = kp$ với $-5 < k < 1$ và $k \neq 0$. Như vậy k có thể nhận các giá trị $-4, -3, -2, -1$. Vì $-4 = 1^2 - 5 \cdot 1^2$ nên nếu p có dạng $x^2 - 5y^2$ thì ta không loại trừ được $-4p$ có dạng này (theo Nhận xét 2.1). Mặt khác biểu diễn một số có dạng $4A$ dưới dạng $x^2 - 5y^2$ chưa chắc suy ra được A cũng có dạng đó nếu x, y cùng là lẻ. Như vậy ta chưa thể loại các trường hợp $k = -4, -3, -2$ để kết luận chỉ có trường hợp $k = -1$, như điều chúng ta mong muốn.

Biểu diễn một số nguyên dưới dạng $x^2 + Dy^2$

2.3. Định lí Minkowski về dạng tuyến tính

Định lí 2.6. (Định lí Minkowski)

Cho $L_i = \sum_{j=1}^n a_{ij}x_j, i = 1, \dots, n$ là n dạng tuyến tính với hệ số thực và định thức $\Delta = \|a_{ij}\| \neq 0$. Giả sử $l_1, l_2, \dots, l_n$ là n số thực sao cho $l_1 l_2 \dots l_n \geq |\Delta|$. Khi đó tồn tại $(x_1, x_2, \dots, x_n) \in \mathbb{Z}^n$, khác 0 sao cho $|L_i| \leq l_i$ với mọi $i = 1, \dots, n$, trong đó chỉ có một bất đẳng thức xảy ra dấu bằng.

Sử dụng Định lí Minkowski với $n = 2$, Mordell đã chứng minh được định lí sau đây:

Định lí 2.7. Cho m là một số nguyên dương và a, b là hai số nguyên sao cho $(ab, m) = 1$. Nếu tồn tại số nguyên k sao cho

$$ak^2 + b \equiv 0 \pmod{m},$$

thì tồn tại hai số nguyên x, y khác 0 sao cho

$$ax^2 + by^2 = km,$$

với số nguyên k nào đó thoả mãn

i) $k < 2\sqrt{ab}$ nếu $a > 0, b > 0$,

ii) $|k| < \sqrt{|ab|}$ nếu $ab < 0$.

Bạn đọc có thể tìm thấy chứng minh của hai định lí trên trong [4].

Áp dụng Định lí 2.7 với $a = 1$ và m là số nguyên tố lẻ. Giả sử có số nguyên k sao cho $k^2 + D \equiv 0 \pmod{m}$ tức là $-D$ là một thặng dư bậc 2 modulo m . Chúng ta thu được hệ quả sau:

Hệ quả 2.1. Cho p là một số nguyên tố lẻ và D là một số nguyên, nguyên tố cùng nhau với p thoả mãn $\left(\frac{-D}{p}\right) = 1$. Khi đó tồn tại hai số nguyên x, y khác 0 sao cho

$$x^2 + Dy^2 = kp$$

với số nguyên k nào đó thoả mãn

i) $k < 2\sqrt{D}$ nếu $D > 0$,

ii) $|k| < \sqrt{|D|}$ nếu $D < 0$.

2.4. Một số kết quả

Trước hết chúng ta phát biểu Định lí 2.4 cho dạng toàn phương nhị phân đặc biệt (1.1) và đưa ra cách chứng minh sơ cấp bằng cách sử dụng kí hiệu Legendre và kiến thức về quan hệ chia hết. Rõ ràng nếu D là một số nguyên khác 0 không có nhân tử là số chính phương khác 1 thì dạng (1.1) là một dạng toàn phương nguyên thuỷ bất đẳng hướng.

Định lí 2.8. Giả sử $q(x, y) = x^2 + Dy^2$ với D là một số nguyên khác 0 không có nhân tử là số chính phương nào khác 1 và p là một số nguyên tố lẻ nguyên tố cùng nhau với D sao cho $\left(\frac{-D}{p}\right) = -1$. Khi đó

i) Nếu có $x, y \in \mathbb{Z}$ sao cho $p \mid q(x, y)$ thì $p \mid x$ và $p \mid y$.

ii) Với mọi $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$, $\text{ord}_p(q(x, y))$ là số chẵn.

Chứng minh. Giả sử có hai số $x, y \in \mathbb{Z}$ để $p \mid q(x, y)$, tức là $x^2 + Dy^2 \equiv 0 \pmod{p}$. Nếu $p \nmid x$ thì $(x, p) = 1$. Khi đó $\left(\frac{-Dy^2}{p}\right) = 1$ hay $\left(\frac{-D}{p}\right) = 1$, mâu thuẫn với giả thiết. Vậy $p \mid x$. Suy ra $p \mid (Dy^2)$. Mặt khác do $(D, p) = 1$ nên $p \mid y$. Vậy i) được chứng minh. $\square$

Chứng minh. Giả sử ngược lại $\text{ord}_p(q(x, y))$ có dạng $2k + 1$. Theo i) ta có $\frac{q(x, y)}{p^{2k}}$ vẫn có dạng $X^2 + DY^2$. Mặt khác tiếp tục lí luận như trong i), do $\frac{q(x, y)}{p^{2k}}$ chia hết cho p nên $p \mid X$ và $p \mid Y$. Từ đó suy ra $\frac{q(x, y)}{p^{2k}}$ chia hết cho p^2 . Điều này không xảy ra vì $\text{ord}_p(q(x, y)) = 2k + 1$. Vậy ii) được chứng minh. $\square$

Bây giờ chúng ta sẽ tìm điều kiện cần và đủ để một số nguyên có thể biểu diễn dưới dạng (1.1) với một số giá trị D nguyên âm. Theo Nhận xét 2.2, trường hợp $D = -2; -3$ đã được Clark giải quyết triệt để. Nhưng phương pháp mà ông đưa ra không áp dụng được cho trường hợp $D = -5$ và dường như đòi hỏi nhiều tính toán hơn, thậm chí không thu được kết quả như mong muốn đối với các giá trị D càng nhỏ (tức là $-D$ càng lớn), vì khi đó k lấy giá trị trong khoảng càng lớn. Chúng ta sẽ sử dụng Hệ quả 2.1 để xét các giá trị D mà $-D$ là các số nguyên tố thuộc khoảng $[5; 23]$. Ta bắt đầu với $D = -5$.

Định lí 2.9. Cho p là một số nguyên tố lẻ và $p \equiv \pm 1 \pmod{5}$. Khi đó p có thể viết được dưới dạng $p = x^2 - 5y^2$.

Chứng minh. Để chứng minh định lí này, ta áp dụng Hệ quả 2.1 với $D = -5$. Vì $p \equiv \pm 1 \pmod{5}$ nên

$$\left(\frac{-D}{p}\right) = \left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2} \frac{p-1}{2}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = 1.$$

Khi đó tồn tại các số nguyên k, x, y sao cho $x^2 - 5y^2 = kp$, với $|k| < \sqrt{5}$. Hiển nhiên $k \neq 0$. Suy ra $k = \pm 1, \pm 2$.

- + Nếu $k = \pm 2$, tức là tồn tại các số nguyên x_0, y_0 khác 0 sao cho $x_0^2 - 5y_0^2 = \pm 2p$. Suy ra $2 \mid (x_0^2 - y_0^2)$. Do đó x và y cùng tính chẵn lẻ. Điều này dẫn đến $x_0^2 - y_0^2$ chia hết cho 4 hay $2p$ chia hết cho 4. Điều này không thể xảy ra vì p là số nguyên tố lẻ.
- + Nếu $k = -1$, tức là tồn tại các số nguyên x_1, y_1 sao cho $x_1^2 - 5y_1^2 = -p$. Mặt khác do $-1 = 2^2 - 5 \cdot 1^2$ và theo Nhận xét 2.1 ta suy ra p biểu diễn được dưới dạng $x^2 - 5y^2$. Nghĩa là trường hợp $k = -1$ có thể dẫn tới trường hợp $k = 1$.

□

Nhận xét 2.3. Nếu d là số nguyên tố lẻ có dạng $4m + 1$ thì phương trình Pell $x^2 - dy^2 = -1$ có nghiệm. Vì thế chứng minh định lí trên (với trường hợp $-D = 5$) có thể áp dụng cho số nguyên tố $-D$ bất kì có dạng $4m + 1$ trong trường hợp $k = -1$ và cả trong trường hợp $k = \pm 2$.

Tương tự, chúng ta có kết quả với $D = -13$ và $D = -17$ như sau:

Định lí 2.10. Cho p là một số nguyên tố lẻ và $\left(\frac{p}{13}\right) = 1$. Khi đó p có thể viết được dưới dạng $p = x^2 - 13y^2$.

Chứng minh. Áp dụng Hệ quả 2.1 với $D = -13$. Ta có

$$\left(\frac{-D}{p}\right) = \left(\frac{13}{p}\right) = (-1)^{\frac{13-1}{2} \frac{p-1}{2}} \left(\frac{p}{13}\right) = \left(\frac{p}{13}\right) = 1.$$

Khi đó tồn tại các số nguyên k, x, y sao cho $x^2 - 13y^2 = kp$, với $|k| < \sqrt{13}$. Hiển nhiên $k \neq 0$. Suy ra $k = \pm 1, \pm 2, \pm 3$.

Theo Nhận xét 2.3, các trường hợp $k = -1, \pm 2$ được chứng minh hoàn toàn tương tự như trong Định lí 2.9. Trường hợp $k = -3$ có thể đưa được về trường hợp $k = 3$ vì phương trình $-1 = x^2 - 13y^2$ có nghiệm. Như vậy ta chỉ cần chứng minh trường hợp $k = 3$ có thể đưa về trường hợp $k = 1$ và ngược lại. Thật vậy, giả sử có $x, y \in \mathbb{Z}$ sao cho $x^2 - 13y^2 = p$. Do $4^2 - 13 \cdot 1^2 = 3$ nên theo Nhận xét 2.1 ta có $A^2 - 13B^2 = 3p$ với

$$A = 4x + 13y, B = x + 4y.$$

Khi đó $3x = 4A - 13B$, $3y = -A + 4B$. Từ đó ta cũng suy ra rằng, nếu có hai số nguyên A, B sao cho $A^2 - 13B^2 = 3p$ thì $A^2 \equiv B^2 \pmod{3}$ và ta có thể lấy A, B sao cho $A \equiv B \pmod{3}$. Như vậy ta có thể tìm được x, y thỏa mãn $x^2 - 13y^2 = p$. Vậy định lí được chứng minh. □

Định lí 2.11. Cho p là một số nguyên tố lẻ và $\left(\frac{p}{17}\right) = 1$. Khi đó p có thể viết được dưới dạng $p = x^2 - 17y^2$.

Chứng minh. Áp dụng Hệ quả 2.1 với $D = -17$. Ta có

$$\left(\frac{-D}{p}\right) = \left(\frac{17}{p}\right) = (-1)^{\frac{17-1}{2} \frac{p-1}{2}} \left(\frac{p}{17}\right) = \left(\frac{p}{17}\right) = 1.$$

Khi đó tồn tại các số nguyên k, x, y sao cho $x^2 - 17y^2 = kp$, với $|k| < \sqrt{17}$. Hiển nhiên $k \neq 0$. Suy ra $k = \pm 1, \pm 2, \pm 3, \pm 4$.

- + Nếu $k = -1$ hoặc $k = \pm 2$, chứng minh hoàn toàn tương tự như trong Định lí 2.9.
- + Nếu $k = \pm 3$, tức là tồn tại các số nguyên x, y sao cho $x^2 - 17y^2 = \pm 3p$. Suy ra $3 \mid (x^2 + y^2)$. Từ đó suy ra $3 \mid x$ và $3 \mid y$. Dẫn đến $3 \mid p$. Điều này không xảy ra do $\left(\frac{p}{17}\right) = 1$, tức $p \neq 3$.

- + Nếu $k = \pm 4$, tức là tồn tại các số nguyên x, y sao cho $x^2 - 17y^2 = \pm 4p$. Suy ra $4 \mid (x^2 - y^2)$, tức là x, y cùng tính chẵn lẻ. Nếu x, y cùng lẻ, ta suy ra p là số chẵn (không thỏa mãn giả thiết). Nếu x, y cùng chẵn thì trường hợp này sẽ dẫn đến trường hợp $k = \pm 1$ và dẫn đến $k = 1$.

Vậy định lí được chứng minh. $\square$

Tiếp theo ta đưa ra điều kiện cần và đủ để một số nguyên khác 0 biểu diễn được dưới dạng (1.1) với $D = -5$. Các trường hợp $D = -13, -17$ được lập luận tương tự.

Định lí 2.12. Một số nguyên n khác 0 biểu diễn được dưới dạng $x^2 - 5y^2$ nếu và chỉ nếu đối với các số nguyên tố lẻ $p \equiv \pm 2 \pmod{5}$, $\text{ord}_p(n)$ là chẵn và $\text{ord}_2(n)$ là chẵn.

Chứng minh. +) Điều kiện đủ: Ta có $-1 = 2^2 - 5 \cdot 1^2$ và $5 = 5^2 - 5 \cdot 2^2$. Mặt khác một số chính phương bao giờ cũng viết được dưới dạng $x^2 - 5y^2$. Hơn nữa theo Định lí 2.9, các số nguyên tố $p \equiv \pm 1 \pmod{5}$ đều biểu diễn được dưới dạng $x^2 - 5y^2$. Cuối cùng theo Nhận xét 2.1 ta suy ra điều kiện đủ được chứng minh. $\square$

+) Điều kiện cần: Giả sử n có dạng $x^2 - 5y^2$. Nếu $p \equiv \pm 2 \pmod{5}$ thì $\left(\frac{5}{p}\right) = -1$. Theo

Định lí 2.8 ta suy ra $\text{ord}_p(n)$ là số chẵn.

Ta viết $n = x^2 - 5y^2 = 5^a A$, với $(A, 5) = 1$. Suy ra $5 \mid x$. Đặt $x = 5X$ thay vào n ta được: $5X^2 - y^2 = 5^{a-1}A$. Nếu $a > 1$ thì $5 \mid y$ và đặt $y = 5Y$. Khi đó $X^2 - 5Y^2 = 5^{a-2}A$. Cứ tiếp tục quá trình này ta thấy nếu a chẵn (tương ứng a lẻ) thì n có dạng $x^2 - 5y^2$ khi và chỉ khi A (tương ứng $-A$) có dạng này. Nhưng do -1 cũng có dạng này nên theo Nhận xét 2.1 ta suy ra n có dạng $x^2 - 5y^2$ khi và chỉ khi A có dạng đó với mọi a . Bây giờ ta giả sử $\text{ord}_2(n)$ là lẻ, tức là $\text{ord}_2(A)$ là lẻ, có dạng $2k + 1$. Theo chứng minh ở trên ta cũng có $\text{ord}_p(A)$ là chẵn với $p \equiv \pm 2 \pmod{5}$. Do đó $A \equiv \pm 2^{2k+1} \pmod{5}$ hay $A \equiv \pm 2 \pmod{5}$. Mặt khác A có dạng $x^2 - 5y^2$ nên $A \equiv \pm 1 \pmod{5}$, mâu thuẫn. Vậy điều giả sử là sai, tức là $\text{ord}_2(A) = \text{ord}_2(n)$ là số chẵn.

Bây giờ ta sẽ xét các giá trị D mà $-D$ là số nguyên tố dạng $4m + 3$ và không vượt quá 23. Trước hết xét $D = -23$, ta có kết quả sau:

Định lí 2.13. Cho p là số nguyên tố lẻ thỏa mãn $\left(\frac{23}{p}\right) = 1$. Khi đó tồn tại các số nguyên x, y sao cho $x^2 - 23y^2 = (-1)^{\frac{p-1}{2}} p$.

Chứng minh. Áp dụng Hệ quả 2.1 với $D = -23$, khi đó tồn tại các số nguyên k, x, y sao cho $x^2 - 23y^2 = kp$, với $|k| < \sqrt{23}$. Suy ra $k = \pm 1, \pm 2, \pm 3, \pm 4$. Bây giờ ta sẽ xét từng trường hợp.

- + Nếu $k = \pm 4$, tức là tồn tại hai số nguyên x, y sao cho $x^2 - 23y^2 = \pm 4p$. Suy ra $4 \mid (x^2 - 23y^2)$. Dẫn đến $4 \mid (x^2 + y^2)$. Vì một số chính phương chia cho 4 chỉ có thể dư 0 hoặc 1 nên suy ra x, y là những số chẵn. Đặt $x = 2X, y = 2Y$, ta được $X^2 - 23Y^2 = \pm p$. Như vậy trường hợp này được đưa về trường hợp $k = \pm 1$.
- + Nếu $k = \pm 3$, tức là tồn tại hai số nguyên x, y sao cho $x^2 - 23y^2 = \pm 3p$. Suy ra $3 \mid (x^2 + y^2)$. Vì một số chính phương chia cho 3 chỉ có thể dư 0 hoặc 1 nên suy ra x và y đều chia hết

Biểu diễn một số nguyên dưới dạng $x^2 + Dy^2$

cho 3. Từ đó $9 \mid (x^2 - 23y^2)$. Điều này không thể xảy ra vì $p \neq 3$ (do giả thiết $\left(\frac{23}{p}\right) = 1$).

Vậy trường hợp này không xảy ra.

- + Nếu $k = \pm 2$, tức là tồn tại hai số nguyên x, y sao cho $x^2 - 23y^2 = \pm 2p$. Do $2 = 5^2 - 23 \cdot 1^2$ nên theo Nhận xét 2.1, trường hợp này được đưa về trường hợp $k = \pm 4$ và đưa tiếp về trường hợp $k = \pm 1$.

Như vậy tồn tại hai số nguyên x, y để hoặc $x^2 - 23y^2 = p$ hoặc $x^2 - 23y^2 = -p$. Ta có $\left(\frac{23}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{23}\right) = 1$. Nếu p có dạng $4m+1$ thì $k = 1$. Vì ngược lại, nếu $k = -1$, tức là $x^2 - 23y^2 = -p = -4m-1$, tức là $x^2 - 23y^2 \equiv -1 \pmod{4}$ hay $x^2 + y^2 \equiv -1 \pmod{4}$, điều này không xảy ra. Tương tự ta cũng có nếu p có dạng $4m+3$ thì $k = -1$. Từ đó định lí được chứng minh. $\square$

Ta có thể lấy ví dụ với $p = 7$, $\left(\frac{23}{7}\right) = 1$ và $-7 = 4^2 - 23 \cdot 1^2$. Với $p = 13$, $\left(\frac{23}{13}\right) = 1$ và $13 = 6^2 - 23 \cdot 1^2$.

Nhận xét 2.4.

- + Trong chứng minh định lí trên ta đã biết rằng 2 là số nguyên biểu diễn được dưới dạng $x^2 - 23y^2$.
- + Ta viết một số nguyên n dưới dạng $n = 23^a A$, với $(23, A) = 1$ và giả sử n có dạng $x^2 - 23y^2$. Khi đó bằng cách lập luận như trong chứng minh Định lí 2.12, ta suy ra rằng nếu a chẵn thì n có dạng $x^2 - 23y^2$ khi và chỉ khi A có dạng này, còn nếu a lẻ thì n có dạng $x^2 - 23y^2$ khi và chỉ khi $-A$ có dạng này.

Định lí 2.14. Cho n là một số nguyên khác 0.

a) Nếu $\text{ord}_{23}(n)$ là số chẵn thì n có dạng $x^2 - 23y^2$ nếu và chỉ nếu có hai khẳng định sau:

- Mọi số nguyên tố lẻ p thoả mãn $\left(\frac{23}{p}\right) = -1$, ta có $\text{ord}_p(n)$ là chẵn.
- n là số nguyên dương khi và chỉ khi số các ước nguyên tố lẻ p của n (kể cả bội) thoả mãn $\left(\frac{p}{23}\right) = -1$, là một số chẵn.

b) Nếu $\text{ord}_{23}(n)$ là số lẻ thì n có dạng $x^2 - 23y^2$ nếu và chỉ nếu có hai khẳng định sau:

- Mọi số nguyên tố lẻ p thoả mãn $\left(\frac{23}{p}\right) = -1$, ta có $\text{ord}_p(n)$ là chẵn.
- n là số nguyên dương khi và chỉ khi số các ước nguyên tố lẻ p của n (kể cả bội) thoả mãn $\left(\frac{p}{23}\right) = -1$, là một số lẻ.

Chứng minh. a) Theo Nhận xét 2.4 ta chỉ cần tìm điều kiện cần và đủ cho một số nguyên lẻ n nguyên tố cùng nhau với 23 viết được dưới dạng $x^2 - 23y^2$.

Nếu n có dạng $x^2 - 23y^2$, áp dụng Định lí 2.8 ta suy ra i). Ta cũng suy ra rằng tích của các số nguyên tố thoả mãn điều kiện i) chia cho 4 dư 1.

Để chứng minh *ii*) ta chỉ cần kể đến các số nguyên tố lẻ p thỏa mãn $\left(\frac{23}{p}\right) = 1$. Ta có

$$\left(\frac{23}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{23}\right).$$

Suy ra nếu $\left(\frac{p}{23}\right) = -1$ thì $(-1)^{\frac{p-1}{2}} = -1$, tức là $p \equiv 3 \pmod{4}$. Khi đó theo Định lí 2.13, ta có $-p$ biểu diễn được dưới dạng $X^2 - 23Y^2$. Từ đó ta suy ra khẳng định *ii*).

Giả sử ngược lại ta có khẳng định *i*) và *ii*). Nhận thấy rằng một số chính phương bao giờ cũng viết được dưới dạng $x^2 - 23y^2$ và theo Định lí 2.13, với mọi số nguyên tố p thỏa mãn $\left(\frac{23}{p}\right) = 1$ thì $\pm p$ có dạng $x^2 - 23y^2$. Do đó $\pm n$ có dạng $x^2 - 23y^2$. Mặt khác từ $x^2 - 23y^2 = x^2 + y^2 - 24y^2$, ta suy ra $x^2 - 23y^2 \equiv 0; 1; 2 \pmod{4}$. Kết hợp với khẳng định *ii*) ta suy ra n có dạng $x^2 - 23y^2$.

Tương tự ta chứng minh được ý *b*). Vậy định lí được chứng minh. $\square$

Cuối cùng ta xét các trường hợp $D = -19; -11; -7$.

Định lí 2.15. Cho p là số nguyên tố lẻ thỏa mãn $\left(\frac{19}{p}\right) = 1$. Khi đó tồn tại các số nguyên x, y sao cho $x^2 - 19y^2 = (-1)^{\frac{p-1}{2}} p$.

Chứng minh. Xem [4], trang 168 – 169. $\square$

Định lí 2.16. Cho p là số nguyên tố lẻ thỏa mãn $\left(\frac{11}{p}\right) = 1$. Khi đó tồn tại các số nguyên x, y sao cho $x^2 - 11y^2 = (-1)^{\frac{p-1}{2}} p$.

Chứng minh. Áp dụng Hệ quả 2.1 với $D = -11$, khi đó tồn tại các số nguyên k, x, y sao cho $x^2 - 11y^2 = kp$, với $|k| < \sqrt{11}$. Suy ra $k = \pm 1, \pm 2, \pm 3$. Bây giờ ta sẽ xét từng trường hợp.

- + Nếu $k = \pm 3$, tức là tồn tại hai số nguyên x, y sao cho $x^2 - 11y^2 = \pm 3p$. Suy ra $3 \mid (x^2 + y^2)$. Chứng minh tương tự như trong chứng minh Định lí 2.13 ta cũng suy ra trường hợp này không thể xảy ra.
- + Nếu $k = \pm 2$, tức là tồn tại hai số nguyên x, y sao cho $x^2 - 11y^2 = \pm 2p$. Do $-2 = 3^2 - 11 \cdot 1^2$ nên theo Nhận xét 2.1 trường hợp này được đưa về trường hợp $k = \pm 4$ và đưa tiếp về trường hợp $k = \pm 1$ (lí luận hoàn toàn tương tự như trong chứng minh Định lí 2.13).

Như vậy tồn tại hai số nguyên x, y để hoặc $x^2 - 11y^2 = p$ hoặc $x^2 - 11y^2 = -p$. Cũng tương tự như trong chứng minh Định lí 2.13 ta suy ra $x^2 - 11y^2 = (-1)^{\frac{p-1}{2}} p$. Vậy định lí được chứng minh. $\square$

Định lí 2.17. Cho p là số nguyên tố lẻ thỏa mãn $\left(\frac{7}{p}\right) = 1$. Khi đó tồn tại các số nguyên x, y sao cho $x^2 - 7y^2 = (-1)^{\frac{p-1}{2}} p$.

Chứng minh. Áp dụng Hệ quả 2.1 với $D = -7$, khi đó tồn tại các số nguyên k, x, y sao cho $x^2 - 7y^2 = kp$, với $|k| < \sqrt{7}$. Suy ra $k = \pm 1, \pm 2$. Nếu $k = \pm 2$, tức là tồn tại hai số nguyên x, y sao cho $x^2 - 7y^2 = \pm 2p$. Do $2 = 3^2 - 7 \cdot 1^2$ nên theo Nhận xét 2.1 trường hợp này cũng được

đưa về trường hợp $k = \pm 4$ và đưa tiếp về trường hợp $k = \pm 1$ (lí luận hoàn toàn tương tự như trong chứng minh Định lí 2.13). Như vậy tồn tại hai số nguyên x, y để hoặc $x^2 - 7y^2 = p$ hoặc $x^2 - 7y^2 = -p$. Cũng tương tự như trong chứng minh Định lí 2.13, ta suy ra $x^2 - 7y^2 = (-1)^{\frac{p-1}{2}}p$. Vậy định lí được chứng minh. $\square$

3. Kết luận

Trong bài báo này, tác giả đã đưa ra chứng minh Định lí 2.8 (là trường hợp đặc biệt của Định lí 2.4) bằng phương pháp sơ cấp, dễ tiếp cận với nhiều đối tượng bạn đọc. Từ các kết quả của Mordell tác giả đưa ra điều kiện cần và đủ để một số nguyên có thể biểu diễn được dưới dạng $x^2 + Dy^2$ với một số giá trị D mà $-D$ là số nguyên tố trong khoảng $[5; 23]$. Tác giả hy vọng phương pháp lập luận đưa ra có thể áp dụng cho nhiều số nguyên âm D khác mà $-D$ là một số nguyên tố.

TÀI LIỆU THAM KHẢO

- [1] D. A. Cox, 2013. *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Pure and Applied Mathematics, John Wiley and Sons Inc, New York, second edition.
- [2] T. Hagedorn, 2010. *Primes of the Form $x^2 + ny^2$ and the geometry of convenient numbers*, preprint.
- [3] L. J. Mordell, 1966. Solvability of the equation $ax^2 + by^2 = p$. *Journal of the London Mathematical Society*, Volume s1-41, Issue 1, pages 517–522.
- [4] L. J. Mordell, 1969. *Diophantine Equations*, Pure and Applied Mathematics, Academic Press; British, first edition.
- [5] P. L. Clark, 2010. *Thue's lemma and idoneal quadratic forms*, preprint.
- [6] Dương Quốc Việt, Đàm Văn Nhĩ, 2008. *Cơ sở lý thuyết số và đa thức*, NXB Đại học Sư phạm, Hà Nội.

ABSTRACT

Representation of an integer by $x^2 + Dy^2$

Le Thi Ha

Faculty of Mathematics, Hanoi National University of Education

In this paper we give the necessary conditions for a old prime number or its opposite number to be of a binary quadratic form $x^2 + Dy^2$ with the intergers D where $-D$ is prime number in the interval $[5; 23]$. Then we give the necessary and sufficient conditions for an integer to be represented by this form.

Keywords: Quadratic form, prime number, Legendre symbol, quadratic residue.