

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

NGUYỄN HÀ TRANG

SỐ FROBENIUS BÌNH PHƯƠNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

Nghệ An - 2021

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC VINH

NGUYỄN HÀ TRANG

SỐ FROBENIUS BÌNH PHƯƠNG

Chuyên ngành: ĐẠI SỐ VÀ LÝ THUYẾT SỐ
Mã số: 846 01 04

LUẬN VĂN THẠC SĨ TOÁN HỌC

Người hướng dẫn khoa học
PGS. TS. NGUYỄN THỊ HỒNG LOAN

Nghệ An - 2021

MỤC LỤC

Mục lục	2
Mở đầu	3
1 Kiến thức chuẩn bị về nửa nhóm số	6
1.1. Nửa nhóm số	6
1.2. Số Frobenius của nửa nhóm số	8
2 Số Frobenius bình phương	14
2.1. Chặn trên của số Frobenius bình phương của nửa nhóm số sinh bởi một cặp số cộng	15
2.2. Số Frobenius bình phương của nửa nhóm số $\langle a, a + d \rangle$ với d bé . .	24
2.3. Số Frobenius bình phương của nửa nhóm số $S = \langle a, a + d \rangle$ với $d = 1, 2$	31
Kết luận	36
Tài liệu tham khảo	37

MỞ ĐẦU

Vào cuối thế kỷ 19 và đầu thế kỷ 20, nhà toán học Frobenius (1849-1917) đã đưa ra trong các bài giảng của mình, vấn đề tìm công thức xác định số nguyên lớn nhất không biểu thị tuyến tính được qua một tập các số nguyên dương có ước chung lớn nhất bằng 1, với các hệ số nguyên không âm. Điều đặc biệt là những vấn đề này, Ông chỉ đưa ra trong các bài giảng của mình mà không hề xuất bản dưới bất kỳ hình thức nào. Vấn đề Frobenius có thể được diễn đạt như sau: Cho $s_1, s_2, \dots, s_n$ là các số nguyên dương có ước chung lớn nhất bằng 1, xác định số nguyên lớn nhất không biểu thị tuyến tính được qua $s_1, s_2, \dots, s_n$ với các hệ số là các số nguyên không âm. Số nguyên lớn nhất đó được gọi là *số Frobenius* của tập $\{s_1, s_2, \dots, s_n\}$. Vấn đề Frobenius cũng thường được biết đến với tên gọi *Bài toán đôi tiền Frobenius* (Frobenius Coin Problem) vì số Frobenius của tập $\{s_1, s_2, \dots, s_n\}$ chính là số tiền lớn nhất không thể trả được bằng các mệnh giá tiền $s_1, s_2, \dots, s_n$ cho trước. Vấn đề Frobenius có nhiều ứng dụng trong lý thuyết số, lý thuyết tự động (automata theory), thuật toán phân loại (sorting algorithm),

Sử dụng thuật ngữ nửa nhóm số thì vấn đề Frobenius được phát biểu dưới dạng: Cho trước một nửa nhóm số S , xác định số nguyên lớn nhất không thuộc S . Trường hợp chiều nhúng của S bằng 2, vấn đề Frobenius đã được giải quyết bởi Sylvester [7]. Vấn đề này là một bài toán khó, tồn tại một thời gian dài. Đến nay, người ta vẫn chưa tìm được một công thức tổng quát để tính số Frobenius cho nửa nhóm số có chiều nhúng lớn hơn hoặc bằng 3. Tuy

nhien, trong trường hợp chiều nhúng của S bằng 3, đã có một số nhà toán học đưa ra lời giải cho một số trường hợp đặc biệt. Chẳng hạn, ta có các thuật toán Rødseth, thuật toán Greenberg để tính số Frobenius trong trường hợp chiều nhúng của S bằng 3.

Cho S là một nửa nhóm số. Với một tính chất P cho trước, người ta xét các hàm P -kiểu như sau:

$${}^P R(S) := \text{số nguyên lớn nhất có tính chất } P \text{ không thuộc } S$$

$${}_{Pr}(S) := \text{số nguyên nhỏ nhất có tính chất } P \text{ không thuộc } S.$$

Các hàm P -kiểu đã được giới thiệu và nghiên cứu trong một số công trình của Joge Luis Ramírez Alfonsín.

Trong [4], một bài báo đang ở dạng tiền ấn phẩm của hai nhà toán học Jonathan Chappelon và Joge Luis Ramírez Alfonsín trên arXiv ngày 25 tháng 6 năm 2020, họ đã nghiên cứu biến k -lũy thừa sau đây của số Frobenius $g(S)$ của nửa nhóm số S . Cho k là một số nguyên, $k \geq 2$, số nguyên ký hiệu ${}^k g(S)$ và được xác định bởi

$${}^k g(S) := \text{số nguyên lũy thừa } k \text{ lớn nhất không thuộc } S$$

được gọi là *số Frobenius k -lũy thừa* của S . Trong bài báo này, các tác giả tập trung nghiên cứu số Frobenius 2-lũy thừa và gọi là *số Frobenius bình phương*. Họ đã đưa ra một chặn trên cho ${}^2 g(S_A)$, trong đó S_A là một nửa nhóm số sinh bởi một cặp số cộng. Ngoài ra, họ cũng đưa ra công thức tính ${}^2 g(S)$ trong trường hợp $S = \langle a, a + d \rangle$ với a là một số nguyên thỏa mãn tính chất nào đó và $d = 1, 2, 3, 4$.

Nội dung của luận văn là trình bày lại các kết quả của bài báo [4], cụ thể là chúng tôi sẽ trình bày chi tiết các kết quả đã nói trên đây.

Ngoài phần mở đầu, kết luận và danh mục tài liệu tham khảo, nội dung của luận văn được viết thành hai chương. Chương 1 trình bày các kiến thức

chuẩn bị về nửa nhóm số có liên quan đến Chương 2, nhằm làm cơ sở cho việc trình bày Chương 2. Chương 2 là nội dung chính của luận văn. Trong chương này, chúng tôi trình bày lại một cách chi tiết toàn bộ các kết quả của bài báo [4] mà nội dung chính của nó như đã tóm lược ở trên.

Luận văn này được hoàn thành dưới sự hướng dẫn của PGS. TS. Nguyễn Thị Hồng Loan. Tác giả xin được bày tỏ lòng biết ơn sâu sắc tới Cô-người đã giảng dạy, hướng dẫn, chỉ bảo tận tình và chu đáo trong quá trình tác giả học tập và thực hiện luận văn. Tác giả cũng xin được gửi lời cảm ơn tới các thầy cô Ngành Toán - Viện Sư phạm Tự nhiên, Phòng Đào tạo Sau đại học, Trường Đại học Vinh về những sự hỗ trợ cần thiết và quý báu trong quá trình tác giả học tập tại trường. Cuối cùng, tác giả xin được gửi lời cảm ơn tới Ban giám hiệu Trường THPT Đô Lương 2, các đồng nghiệp, gia đình và người thân đã luôn quan tâm giúp đỡ và tạo mọi điều kiện thuận lợi để tác giả có thể học tập, nghiên cứu và hoàn thành luận văn.

Nghệ An, tháng 6 năm 2021

Tác giả

CHƯƠNG 1

KIẾN THỨC CHUẨN BỊ VỀ NỬA NHÓM SỐ

Trong chương này, chúng tôi trình bày các kiến thức chuẩn bị về nửa nhóm số có liên quan đến Chương 2, nhằm làm cơ sở cho việc trình bày nội dung chính của luận văn ở Chương 2. Các kết quả trong chương này được tham khảo chủ yếu từ các tài liệu [1], [2], [3] và [6].

1.1 Nửa nhóm số

1.1.1 Định nghĩa. Một *nửa nhóm số* S là một vị nhóm con của vị nhóm cộng các số tự nhiên $\mathbb{N}$ sao cho phần bù của S trong $\mathbb{N}$ là hữu hạn.

Như vậy, S là một nửa nhóm số nếu S là một tập con của $\mathbb{N}$, chứa 0, đóng kín đối với phép cộng và $\mathbb{N} \setminus S$ là tập hữu hạn.

Cho A là một tập con (có thể vô hạn) của tập hợp các số tự nhiên $\mathbb{N}$. Ký hiệu

$$\langle A \rangle = \{ \lambda_1 a_1 + \cdots + \lambda_n a_n \mid n \in \mathbb{N}^*, a_i \in A, \lambda_i \in \mathbb{N}, \forall i = 1, \dots, n \}.$$

Khi đó $\langle A \rangle$ là nửa nhóm con bé nhất (theo quan hệ bao hàm) của $\mathbb{N}$ chứa A . Do đó, $\langle A \rangle$ là nửa nhóm con sinh bởi A . Nếu $\langle A \rangle = S$ thì A là một *hệ sinh của nửa nhóm số* S .

Ta nói ước chung lớn nhất của A bằng 1, ký hiệu $\gcd(A) = 1$ nếu ước chung lớn nhất của mọi tập con hữu hạn của A đều bằng 1.

1.1.2 Mệnh đề. Cho A là một tập con khác rỗng của $\mathbb{N} \setminus \{0\}$. Khi đó $\langle A \rangle$ là một nửa nhóm số khi và chỉ khi $\gcd(A) = 1$.

Chứng minh. Đặt $d = \gcd(A)$. Rõ ràng nếu $s \in \langle A \rangle$ thì $d \mid s$. Do $\langle A \rangle$ là một nửa nhóm số nên $\mathbb{N} \setminus \langle A \rangle$ là tập hữu hạn và vì vậy tồn tại số nguyên dương x sao cho $d \mid x$ và $d \mid (x + 1)$. Vậy $d = 1$.

Ngược lại, ta cần chứng minh $\mathbb{N} \setminus \langle A \rangle$ là tập hữu hạn. Thật vậy, do $\gcd(A) = 1$ nên tồn tại các số nguyên $z_1, z_2, \dots, z_n$ và $a_1, a_2, \dots, a_n \in A$ sao cho

$$z_1 a_1 + z_2 a_2 + \dots + z_n a_n = 1.$$

Bằng cách chuyển z_i sang vế phải, ta có thể tìm được $i_1, \dots, i_k, j_1, \dots, j_l \in \{1, \dots, n\}$ sao cho

$$z_{i_1} a_{i_1} + \dots + z_{i_k} a_{i_k} = 1 - z_{j_1} a_{j_1} - \dots - z_{j_l} a_{j_l}.$$

Do đó tồn tại $s \in \langle A \rangle$ sao cho $s + 1$ cũng thuộc $\langle A \rangle$. Ta chứng minh nếu $n \geq (s - 1)s + (s - 1)$ thì $n \in \langle A \rangle$. Thật vậy, lấy q và r là các số nguyên sao cho $n = qs + r$ với $0 \leq r < s$. Do $n \geq (s - 1)s + (s - 1)$ ta suy ra $q \geq s - 1 \geq r$. Vì vậy

$$n = (rs + r) + (q - r)s = r(s + 1) + (q - r)s \in \langle A \rangle.$$

Mệnh đề được chứng minh. □

Chú ý rằng, mỗi nửa nhóm số có thể có nhiều hệ sinh. Tuy nhiên, kết quả sau đây chỉ ra rằng mỗi nửa nhóm số chỉ có duy nhất một hệ sinh hữu hạn.

1.1.3 Mệnh đề. *Mỗi nửa nhóm số đều có duy nhất một hệ sinh hữu hạn.*

Như vậy, mỗi nửa nhóm số S là một tập con của tập hợp các số tự nhiên $\mathbb{N}$, gồm các tổ hợp tuyến tính trên $\mathbb{N}$ của một tập hữu hạn các số nguyên dương nguyên tố cùng nhau cho trước.

Cho $s_1, \dots, s_n$ là các số nguyên dương nguyên tố cùng nhau. Khi đó, nửa nhóm số sinh bởi $s_1, \dots, s_n$ là

$$S = \langle s_1, \dots, s_n \rangle = \{ \lambda_1 s_1 + \dots + \lambda_n s_n \mid \lambda_i \in \mathbb{N}, \forall i = 1, \dots, n \}.$$

Mệnh đề 1.1.3 dẫn đến khái niệm sau đây.

1.1.4 Định nghĩa. Số phần tử của một hệ sinh hữu hạn của nửa nhóm số S được gọi là *chiều nhúng* của S .

Trong luận văn này, chúng ta sẽ nghiên cứu các nửa nhóm số S_A sinh bởi một cặp số cộng, nghĩa là hệ sinh của nửa nhóm số này là một dãy các số nguyên tố cùng nhau có dạng: $a, a + d, \dots, a + kd$ trong đó a, d, k là các số nguyên dương. Do điều kiện các phần tử của hệ sinh là nguyên tố cùng nhau nên ta dễ dàng suy ra được $\gcd(a, d) = 1$. Sau đây là tính chất của nửa nhóm số sinh bởi một cặp số cộng.

1.1.5 Mệnh đề. Điều kiện cần và đủ để $M \in \langle a, a + d, \dots, a + kd \rangle$ là tồn tại các số tự nhiên x, y sao cho $M = ax + dy$ với $0 \leq y \leq kx$.

Chứng minh. Ta có $M \in \langle a, a + d, \dots, a + kd \rangle$ khi và chỉ khi tồn tại các số tự nhiên $x_1, x_2, \dots, x_{k+1}$ sao cho

$$M = ax_1 + (a + d)x_2 + \dots + (a + kd)x_{k+1}.$$

Điều này tương đương với

$$M = a(x_1 + x_2 + \dots + x_{k+1}) + d(x_2 + \dots + kx_{k+1}).$$

Đặt $x = x_1 + x_2 + \dots + x_{k+1}$; $y = x_2 + \dots + kx_{k+1}$. Khi đó

$$0 \leq y = x_2 + \dots + kx_{k+1} \leq k(x_1 + x_2 + \dots + x_{k+1}) = kx.$$

Như vậy, ta đã chứng minh được điều kiện cần và đủ để $M \in \langle a, a + d, \dots, a + kd \rangle$ là tồn tại các số tự nhiên x, y sao cho $M = ax + dy$ với $0 \leq y \leq kx$. $\square$

1.2 Số Frobenius của nửa nhóm số

Việc nghiên cứu các nghiệm nguyên không âm của một hệ phương trình tuyến tính thuần nhất với các hệ số nguyên dương là một vấn đề cổ điển

trong Đại số, mà dưới ngôn ngữ của Toán học hiện đại, đồng nghĩa với việc nghiên cứu một nửa nhóm số. Đã có nhiều nhà toán học quan tâm đến vấn đề này, trong đó đặc biệt là hai nhà toán học Frobenius và Sylverster đã có nhiều kết quả quan trọng. Vấn đề này đã được nhiều nhà toán học quan tâm bởi người ta tìm thấy những ứng dụng của nó trong Hình học Đại số và Đại số giao hoán. Chính nhờ những nghiên cứu này mà nhiều khái niệm về các bất biến trong nửa nhóm số được đưa ra như: *bội, chiều nhúng, bậc kỳ dị, conductor, tập Apéry, số giả Frobenius, kiểu,...*

Trong số các bất biến của nửa nhóm số, có một bất biến quan trọng và có nhiều ứng dụng là *số Frobenius*. Nói một cách đơn giản, *số Frobenius* của một nửa nhóm số S là số nguyên lớn nhất mà không thuộc S , ký hiệu bởi $g(S)$ hoặc $g(\langle s_1, \dots, s_n \rangle)$ nếu muốn chỉ rõ hệ sinh. Hiện nay, chưa có công thức cụ thể nào để tính số Frobenius của một nửa nhóm số bất kỳ. Trong mục này, chúng tôi trình bày các kết quả về công thức tính số Frobenius trong trường hợp cụ thể.

Trước tiên, ta tìm hiểu một trong những công cụ tốt nhất để nghiên cứu về nửa nhóm số, đó là tập Apéry. Tập Apéry được định nghĩa như sau.

1.2.1 Định nghĩa. Cho S là một nửa nhóm số và $n \in S \setminus \{0\}$. Tập hợp được xác định bởi

$$\text{Ap}(S, n) = \{h \in S \mid h - n \notin S\}$$

được gọi là *tập Apéry của n trong S* .

Kết quả sau đây được suy ra ngay từ định nghĩa của tập Apéry.

1.2.2 Bổ đề. *Giả sử S là một nửa nhóm số và n là một số nguyên dương thuộc S . Nếu $x, y \in S$ sao cho $x + y \in \text{Ap}(S, n)$ thì $\{x, y\} \subseteq \text{Ap}(S, n)$.*

Mệnh đề sau đây cho ta cách tìm tập Apéry của một nửa nhóm số.

1.2.3 Mệnh đề. Cho S là một nửa nhóm số và $n \in S \setminus \{0\}$. Khi đó ta có

$$\text{Ap}(S, n) = \{0 = w(0), w(1), \dots, w(n-1)\},$$

trong đó $w(i)$ là số nhỏ nhất của S sao cho

$$w(i) \equiv i \pmod{n}, \forall i \in \{0, 1, \dots, n-1\}.$$

Chứng minh. Rõ ràng, với mỗi $i \in \{1, 2, \dots, n-1\}$ thì tập hợp

$$\{i + kn \mid k \in \mathbb{N}\}$$

các số tự nhiên đồng dư với i theo môđun n là tập hợp vô hạn. Vì tập hợp $\mathbb{N} \setminus S$ là hữu hạn nên tồn tại $k \in \mathbb{N}$ sao cho $i + kn \in S$. Gọi $w(i)$ là số nhỏ nhất thuộc S có dạng $i + kn$, nghĩa là $w(i)$ là số nhỏ nhất thuộc S đồng dư với i theo môđun n . Khi đó rõ ràng $w(i) - n \notin S$ vì $w(i) - n = i + kn - n = i + (k-1)n < w(i)$. Vậy $w(i) \in \text{Ap}(S, n)$ với mọi $i \in \{1, 2, \dots, n-1\}$. Do đó

$$\text{Ap}(S, n) \supseteq \{0 = w(0), w(1), \dots, w(n-1)\}.$$

Ngược lại, giả sử $x \in \text{Ap}(S, n)$. Khi đó $x \in S$ và $x - n \notin S$. Do đó

$$x \in \{0 = w(0), w(1), \dots, w(n-1)\}.$$

Suy ra

$$\text{Ap}(S, n) \subseteq \{0 = w(0), w(1), \dots, w(n-1)\}.$$

Vì vậy

$$\text{Ap}(S, n) = \{0 = w(0), w(1), \dots, w(n-1)\}.$$

□

Từ Mệnh đề 1.2.3, ta thấy $\text{Ap}(S, n)$ là một hệ thặng dư đầy đủ mod n . Từ mỗi lớp thặng dư mod n ta trích ra số nguyên nhỏ nhất trong đó thuộc S , ta được một hệ thặng dư đầy đủ môđun n và đó chính là tập $\text{Ap}(S, n)$. Như vậy tập Apéry của phần tử n trong nửa nhóm số S có n phần tử.

1.2.4 Ví dụ. Cho nửa nhóm số

$$S = \langle 5, 7, 9 \rangle = \{0, 5, 7, 9, 10, 12, 14 \rightarrow\}$$

(trong đó ký hiệu $14 \rightarrow$ nghĩa là các số tự nhiên liên tiếp bắt đầu từ 14). Ta tính được

$$\text{Ap}(S, 5) = \{0, 7, 9, 16, 18\},$$

$$\text{Ap}(S, 7) = \{0, 5, 9, 10, 15, 18, 20\}.$$

1.2.5 Định nghĩa. Cho S là một nửa nhóm số.

(1) Số nguyên lớn nhất không thuộc S được gọi là *số Frobenius của S* và được ký hiệu là $g(S)$.

(2) Số chính phương lớn nhất không thuộc S được gọi là *số Frobenius bình phương* và ký hiệu là ${}^2g(S)$.

Ký hiệu $\mathbb{Z}$ là tập hợp số nguyên. Từ định nghĩa trên ta có

$$g(S) = \max(\mathbb{Z} \setminus S),$$

$${}^2g(S) \leq g(S).$$

1.2.6 Ví dụ. 1) Cho nửa nhóm số

$$S = \langle 4, 7 \rangle = \{0, 4, 7, 8, 11, 12, 14, 15, 16, 18 \rightarrow\}.$$

Khi đó ta tính được $g(S) = 17$ và ${}^2g(S) = 9$.

2) Cho nửa nhóm số

$$S = \langle 5, 7, 9 \rangle = \{0, 5, 7, 9, 10, 12, 14 \rightarrow\}.$$

Khi đó ta tính được $g(S) = 13$ và ${}^2g(S) = 4$.

Mệnh đề sau đây cho ta một công thức tính số Frobenius của một nửa nhóm số thông qua tập Apéry.

1.2.7 Mệnh đề. Cho nửa nhóm số S và $0 < n \in S$. Khi đó

$$g(S) = \max \text{Ap}(S, n) - n.$$

Chứng minh. Giả sử $\text{Ap}(S, n) = \{0 = w_0, w_1, \dots, w_{n-1}\}$, trong đó $0 = w_0 < w_1 < \dots < w_{n-1}$. Ta có

$$\max \text{Ap}(S, n) = w_{n-1}.$$

Theo định nghĩa của tập hợp Apéry thì $w_{n-1} - n \notin S$. Ta đặt

$$w_i = k_i n + r_i, \quad i \in \{0, 1, \dots, n-1\}, \quad 0 \leq r_i \leq n-1.$$

Khi đó

$$k_0 < k_1 < \dots < k_{n-1}.$$

Vì thế

$$w_{n-1} - n + 1 = (k_{n-1} - 1)n + r_{n-1} + 1 \in S.$$

Từ những chứng minh trên ta thấy ngay $g(S) = \max \text{Ap}(S, n) - n$.

□

Trong trường hợp nửa nhóm số sinh bởi hai phần tử thì từ mệnh đề trên ta có công thức tính số Frobenius như sau. Kết quả này được đưa ra bởi Sylvester [7].

1.2.8 Hệ quả. Cho nửa nhóm số $S = \langle a, b \rangle$, trong đó a, b là các số nguyên dương sao cho $\gcd(a, b) = 1$. Khi đó số Frobenius của nửa nhóm số S được xác định như sau:

$$g(S) = ab - a - b.$$

Chứng minh. Vì $\gcd(a, b) = 1$ nên $\text{Ap}(S, a) = \{0, b, \dots, (a-1)b\}$. Do đó, theo Mệnh đề 1.2.7, ta có

$$g(S) = \max \text{Ap}(S, a) - a = (a-1)b - a = ab - a - b.$$

□

Mệnh đề sau đây cho ta công thức tính số Frobenius của nửa nhóm số sinh bởi một cấp số cộng (xem [5]).

1.2.9 Mệnh đề. *Cho nửa nhóm số S_A sinh bởi cấp số cộng $a, a + d, \dots, a + kd$ trong đó a, d, k là các số nguyên dương. Khi đó*

$$g(S_A) = \left(\left\lfloor \frac{a-2}{k} \right\rfloor + 1 \right) a + (d-1)(a-1) - 1.$$

Ở đây ký hiệu $\lfloor \dots \rfloor$ để chỉ phần nguyên.

CHƯƠNG 2

SỐ FROBENIUS BÌNH PHƯƠNG

Số Frobenius bình phương, hay còn được gọi số Frobenius lũy thừa 2 có thể diễn đạt một cách sơ cấp như sau: Cho $s_1, s_2, \dots, s_n$ là các số nguyên dương có ước chung lớn nhất bằng 1, xác định số chính phương lớn nhất không biểu diễn tuyến tính được qua $s_1, s_2, \dots, s_n$ với các hệ số nguyên không âm. Số chính phương lớn nhất đó được gọi là *số Frobenius bình phương* của tập $\{s_1, s_2, \dots, s_n\}$. Các số Frobenius lũy thừa k với $k \geq 2$ được định nghĩa hoàn toàn tương tự. Hiển nhiên, ta luôn có một chặn trên của số Frobenius bình phương đó chính là số Frobenius. Tuy nhiên, cũng giống như tìm công thức tính số Frobenius, công thức tính số Frobenius bình phương là không đơn giản.

Sử dụng thuật ngữ nửa nhóm số thì vấn đề số Frobenius bình phương được phát biểu dưới dạng: Cho trước một nửa nhóm số S , xác định số chính phương lớn nhất không thuộc S . Trong trường hợp nửa nhóm số sinh bởi một cấp số cộng, trong [4] đã cho ra một số kết quả thú vị. Trong bài báo này, các tác giả đã đưa ra một chặn trên cho ${}^2g(S_A)$, trong đó S_A là một nửa nhóm số sinh bởi một cấp số cộng. Ngoài ra, họ cũng đưa ra công thức tính ${}^2g(S)$ trong trường hợp $S = \langle a, a + d \rangle$ với a là một số nguyên thỏa mãn tính chất nào đó và $d = 1, 2, 3, 4, 5$.

Trong chương này, chúng tôi trình bày toàn bộ các kết quả trong bài báo [4] của Jonathan Chappelon và Joge Luis Ramírez Alfonsín đã nói trên đây.

2.1 Chặn trên của số Frobenius bình phương của nửa nhóm số sinh bởi một cặp số cộng

Xét nửa nhóm số S_A sinh bởi một cặp số cộng, nghĩa là hệ sinh của nửa nhóm số là một dãy các số nguyên tố cùng nhau có dạng: $a, a + d, \dots, a + kd$ trong đó a, d, k là các số nguyên dương. Do điều kiện các phần tử của hệ sinh là nguyên tố cùng nhau nên ta dễ dàng suy ra được $\gcd(a, d) = 1$. Mục đích chính của mục này là chứng minh Định lý 2.1.5 đưa ra một chặn trên của số Frobenius bình phương nửa nhóm số S_A . Để thống nhất, ta ký hiệu số Frobenius bình phương của nửa nhóm số S_A là ${}^2g(S_A)$ hoặc ${}^2g(\langle a, a + d, \dots, a + kd \rangle)$.

Liên quan đến vấn đề chính của luận văn, mệnh đề dưới đây cho ta một điều kiện cần và đủ để một số chính phương có dạng cho trước thuộc vào nửa nhóm số S_A .

2.1.1 Mệnh đề. *Cho i là một số nguyên và λ_i là số tự nhiên sao cho $0 \leq \lambda_i \leq d - 1$ và $\lambda_i a + i^2 \equiv 0 \pmod{d}$. Khi đó,*

$$(a - i)^2 \in S_A \Leftrightarrow (i + kd)^2 \leq \left(\left(\left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor + k \right) d - \lambda_i \right) (a + kd).$$

Chứng minh. Chứng minh mệnh đề này hoàn toàn dựa vào kiến thức phần nguyên và các phép biến đổi sơ cấp. Cụ thể, ta có:

$$\begin{aligned} (a - i)^2 &= (a - 2i)a + i^2 \\ &= (a - 2i - \lambda_i)a + \frac{i^2 + \lambda_i a}{d}d \\ &= \left(a - 2i - \lambda_i + \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor d \right) a + \left(\frac{i^2 + \lambda_i a}{d} - \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor a \right) d. \end{aligned}$$

Kết hợp với Mệnh đề 1.1.5, ta suy ra $(a - i)^2 \in S_A$ khi và chỉ khi:

$$\begin{aligned}
& \frac{i^2 + \lambda_i a}{d} - \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor a \leq k \left(a - 2i - \lambda_i + \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor d \right) \\
& \Leftrightarrow \frac{i^2 + \lambda_i a}{d} \leq k(a - 2i - \lambda_i) + \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor (a + kd) \\
& \Leftrightarrow i^2 + \lambda_i a \leq kd(a - 2i - \lambda_i) + \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor d(a + kd) \\
& \Leftrightarrow i^2 + 2ikd \leq kda - \lambda_i(a + kd) + \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor d(a + kd) \\
& \Leftrightarrow i^2 + 2ikd + k^2 + d^2 \leq kd(a + kd) - \lambda_i(a + kd) + \left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor d(a + kd) \\
& \Leftrightarrow (i + kd)^2 \leq \left(\left(\left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor + k \right) d - \lambda_i \right) (a + kd).
\end{aligned}$$

□

Từ mệnh đề trên, để trình bày kết quả chính ở Định lý 2.1.5 ta cần một số ký hiệu sau đây.

2.1.2 Định nghĩa. Cho a và $d \geq 3$ là các số nguyên dương nguyên tố cùng nhau.

- Gọi λ^* là số nguyên λ_i lớn nhất thỏa mãn giả thiết Mệnh đề 2.1.1, nghĩa là

$$\lambda^* = \max_{0 \leq i \leq d-1} \{ \lambda_i \in \{0, 1, \dots, d-1\} \mid \lambda_i a + i^2 \equiv 0 \pmod{d} \}.$$

- Ký hiệu $\{\alpha_1, \dots, \alpha_n\}$ là tập con của $\{0, 1, \dots, d-1\}$ sao cho $\lambda_{\alpha_j} = \lambda^*$ và đặt $\alpha_{n+1} = d + \alpha_1$.
- Gọi $1 \leq j \leq n$ là chỉ số duy nhất sao cho

$$(\mu d + \alpha_j)^2 \leq (kd - \lambda^*)(a + kd) < (\mu d + \alpha_{j+1})^2,$$

với số tự nhiên μ nào đó.

- Ta định nghĩa hàm số nguyên $h(a, d, k)$ xác định như sau:

$$h(a, d, k) := (a - ((\mu - k)d + \alpha_{j+1}))^2.$$

Để chứng minh Định lý 2.1.5, ta cần bổ đề sau đây.

2.1.3 Bổ đề. *Cho a và d là các số nguyên dương nguyên tố cùng nhau với $d \geq 3$. Nếu $a + kd > 4k\lambda^*d^3$ thì*

$$2d^2(\mu + 1) \leq a + kd.$$

Chứng minh. **Trường hợp 1.** $j \in \{1, \dots, n-1\}$.

Từ Định nghĩa 2.1.2 ta có

$$(\mu d + \alpha_j)^2 \leq (kd - \lambda^*)(a + kd) < (\mu d + \alpha_{j+1})^2.$$

Kết hợp với $0 < \alpha_j < d$ và $\alpha_{j+1} \leq \alpha_n < d$, ta suy ra

$$\mu = \left\lfloor \frac{\sqrt{(kd - \lambda^*)(a + kd)}}{d} \right\rfloor.$$

Theo giả thiết $a + kd > 4k\lambda^*d^3$ nên ta có $a + kd > 4(kd - \lambda^*)d^2$. Từ đó suy ra

$$\mu \geq 2(kd - \lambda^*). \quad (2.1)$$

Do đó

$$\begin{aligned} (kd - \lambda^*)(a + kd) &\geq (\mu d + \alpha_j)^2 \\ &> \mu^2 d^2 \\ &> (\mu^2 - 1)d^2 \\ &= (\mu - 1)(\mu + 1)d^2 \\ &\geq 2(kd - \lambda^*)(\mu + 1)d^2. \end{aligned}$$

Vì vậy

$$(kd - \lambda^*)(a + kd) > 2(kd - \lambda^*)(\mu + 1)d^2$$

hay $a + kd > 2(\mu + 1)d^2$ với mọi $j \in \{1, \dots, n - 1\}$.

Trường hợp 2. $j = n$.

Do $\alpha_j = \alpha_n = d - \alpha_1$ và $\alpha_{j+1} = \alpha_{n+1} = d + \alpha_1$ nên ta có

$$\left\lfloor \frac{\sqrt{(kd - \lambda^*)(a + kd)}}{d} \right\rfloor \in \{\mu, \mu + 1\}.$$

Mặt khác,

$$(\mu d + \alpha_j)^2 \leq (kd - \lambda^*)(a + kd) < (\mu d + \alpha_{j+1})^2,$$

nên ta có

$$((\mu - 1)d - \alpha_1)^2 \leq (kd - \lambda^*)(a + kd) < ((\mu + 1)d + \alpha_1)^2.$$

Do đó $\mu + 1 \geq 2(kd - \lambda^*)$. Suy ra

$$\begin{aligned} (kd - \lambda^*)(a + kd) &\geq ((\mu + 1)d - \alpha_1)^2 \\ &\geq \left((\mu + 1)d - \frac{d}{2}\right)^2 \\ &= \left(\mu^2 + \mu + \frac{1}{4}\right)d^2 \\ &> \mu(\mu + 1)d^2 \\ &\geq 2(kd - \lambda^*)(\mu + 1)d^2. \end{aligned}$$

Do đó $a + kd > 2(\mu + 1)d^2$. Vậy bổ đề đã được chứng minh. $\square$

2.1.4 Nhận xét. 1). Chứng minh của Bổ đề 2.1.3 đã chỉ ra công thức tính số μ trong hàm $h(a, d, k)$ như sau:

$$\mu = \left\lfloor \frac{\sqrt{(kd - \lambda^*)(a + kd)}}{d} \right\rfloor \text{ với } 1 \leq j \leq n - 1$$

và

$$\left\lfloor \frac{\sqrt{(kd - \lambda^*)(a + kd)}}{d} \right\rfloor \in \{\mu, \mu + 1\} \text{ với } j = n.$$

2) Ta có các nhận xét sau đây về các ký hiệu trong Định nghĩa 2.1.2.

- $\lambda_0 = 0, \lambda_1 \neq 0$ do đó $\lambda^* = \lambda_{\alpha_j} \geq 1, \alpha_j \geq 1$.
- $0 \leq \alpha_1 < \alpha_2 < \dots < \alpha_n < d$
- Với $j = n$ thì $\alpha_j = d - \alpha_1$ và $\alpha_{j+1} = d + \alpha_1 < d + \alpha_j$. Do đó $\alpha_1 \leq \frac{d}{2}$.

3). Giả thiết $a + kd > 4k\lambda^*d^3$ có thể được thay thế bởi giả thiết $a + kd > 4(kd - \lambda^*)d^2$.

4). Sau đây, chúng tôi trình bày một chứng minh của Bổ đề 2.1.3 gọn hơn so với trình bày trong bài báo như sau.

Ta có

$$(\mu d + \alpha_{j+1})^2 > (kd - \lambda^*)(a + kd) > 4d^2(kd - \lambda^*)^2,$$

có nghĩa là $\mu > 2(kd - \lambda^*) - \frac{\alpha_{j+1}}{d}$ với $1 \leq j \leq n$. Từ đây có hai khả năng xảy ra. Khả năng thứ nhất, nếu $\mu \geq 2(kd - \lambda^*)$ thì

$$\begin{aligned} (kd - \lambda^*)(a + kd) &\geq (\mu d + \alpha_j)^2 \\ &> \mu^2 d^2 \\ &> (\mu^2 - 1)d^2 \\ &= (\mu - 1)(\mu + 1)d^2 \geq 2(kd - \lambda^*)(\mu + 1)d^2. \end{aligned}$$

Do đó $(kd - \lambda^*)(a + kd) > 2(kd - \lambda^*)(\mu + 1)d^2$ hay $a + kd > 2(\mu + 1)d^2$. Khả năng thứ hai, nếu $\mu + 1 = 2(kd - \lambda^*)$ thì từ giả thiết ta suy ra

$$a + kd > 4d^2(kd - \lambda^*) = 2d^2(kd - \lambda^*).$$

Định lý sau đây cho ta một chặn trên của ${}^2g(S_A)$.

2.1.5 Định lý. Cho a và d là các số nguyên dương nguyên tố cùng nhau với $d \geq 3$. Nếu $a + kd > 4k\lambda^*d^3$ thì

$${}^2g(S_A) \leq h(a, d, k).$$

Chứng minh. Trước hết, theo Mệnh đề 1.2.9 ta có

$$g(S_A) = \left(\left\lfloor \frac{a-2}{k} \right\rfloor + 1 \right) a + (d-1)(a-1) - 1.$$

Vì $a^2 > \left(\left\lfloor \frac{a-2}{k} \right\rfloor + 1 \right) a$, $2akd > (d-1)(a-1)$ và $(kd)^2 > 0$ nên

$$g(S_A) < a^2 + 2kad + (kd)^2 = (a - (-kd))^2.$$

Vì ${}^2g(S_A) \leq g(S_A)$ nên định lý sẽ được chứng minh nếu ta chỉ ra được $(a-i)^2 \in S_A$ với mọi $-kd \leq i < (\mu-k)d + \alpha_{j+1}$. Ta xét hai trường hợp như sau.

Trường hợp 1. $-kd \leq i \leq (\mu-k)d + \alpha_j$.

Vì $i \leq (\mu-k)d + \alpha_j$, theo Định nghĩa 2.1.2 thì $\lambda^* \geq \lambda_i$ và $\left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor > 0$ nên ta có

$$\begin{aligned} (i+kd)^2 &\leq (\mu d + \alpha_j)^2 \\ &\leq (kd - \lambda^*)(a + kd) \\ &\leq \left(\left(\left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor + k \right) d - \lambda_i \right) (a + kd). \end{aligned}$$

Theo Mệnh đề 2.1.1, ta có $(a-i)^2 \in S_A$.

Trường hợp 2. $(\mu-k)d + \alpha_j < i < (\mu-k)d + \alpha_{j+1}$.

Dựa vào Mệnh đề 2.1.1, vấn đề sẽ được giải quyết nếu ta chứng minh được

$$(i+kd)^2 \leq (kd - \lambda_i)(a + kd).$$

Trong trường hợp này ta có $\alpha_j < i - (\mu-k)d \leq \alpha_{j+1}$ và theo định nghĩa của λ^* như trong Định nghĩa 2.1.2 ta suy ra $\lambda_i \leq \lambda^* - 1$ và do đó

$$(kd - \lambda_i)(a + kd) \geq (kd - \lambda^*)(a + kd) + (a + kd). \quad (2.2)$$

Mặt khác,

$$\begin{aligned} (i+kd)^2 &\leq (\mu d + \alpha_{j+1})^2 \\ &= ((\mu d + \alpha_j) + \alpha_{j+1} - \alpha_j)^2 \\ &= (\mu d + \alpha_j)^2 + (\alpha_{j+1} - \alpha_j)(2(\mu d + \alpha_j) + (\alpha_{j+1} - \alpha_j)) \end{aligned}$$

$$= (\mu d + \alpha_j)^2 + (\alpha_{j+1} - \alpha_j)(2\mu d + \alpha_j + \alpha_{j+1}). \quad (2.3)$$

Do $\lambda_{\alpha_j} = \lambda^*$ nên $\alpha_j > 0$. Với mọi chỉ số $j \in \{1, \dots, n-1\}$ ta có

$$\alpha_{j+1} - \alpha_j < \alpha_{j+1} \leq \alpha_n < d \text{ và } \alpha_j + \alpha_{j+1} < 2\alpha_n < 2d, \quad (2.4)$$

còn với $j = n$ thì $\alpha_j = \alpha_n = d - \alpha_1$ và $\alpha_{j+1} = \alpha_{n+1} = d + \alpha_1$, do đó

$$\alpha_{j+1} - \alpha_j = 2\alpha_1 \leq d \text{ và } \alpha_j + \alpha_{j+1} = 2d. \quad (2.5)$$

Từ 2.2, 2.3 và 2.4 ta suy ra

$$(i + kd)^2 < (\mu d + \alpha_j)^2 + d(2\mu d + 2d) = (\mu d + \alpha_j)^2 + 2d^2(\mu + 1) \quad (2.6)$$

với mọi $j \in \{1, \dots, n\}$. Từ 2.2 và Định nghĩa 2.1.2 ta có

$$(\mu d + \alpha_j)^2 \leq (kd - \lambda^*)(a + kd) \leq (kd - \lambda_i)(a + kd) - (a + kd).$$

Suy ra

$$(i + kd)^2 < (kd - \lambda_i)(a + kd) - (a + kd) + 2d^2(\mu + 1). \quad (2.7)$$

Áp dụng Bổ đề 2.1.3 ta có

$$\begin{aligned} (i + kd)^2 &< (kd - \lambda_i)(a + kd) + 2d^2(\mu + 1) - (a + kd) \leq (kd - \lambda_i)(a + kd) \\ &\leq \left(\left(\left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor + k \right) d - \lambda_i \right) (a + kd). \end{aligned}$$

Như vậy, theo Mệnh đề 2.1.1, Định lý được chứng minh. $\square$

Ta dự đoán rằng, chặn trên của ${}^2g(S_A)$ trong Định lý 2.1.5 sẽ trở thành chặn trên đúng, nghĩa là nó sẽ là công thức tính ${}^2g(S_A)$ với một số nửa nhóm S_A nào đó. Hệ quả dưới đây cho ta một sự khẳng định chắc chắn cho dự đoán trên với những nửa nhóm số chỉ sinh bởi hai phần tử (tức $k = 1$).

2.1.6 Hệ quả. *Cho a và $d \geq 3$ là các số nguyên dương nguyên tố cùng nhau. Nếu $a + d > 4\lambda^*d^3$ thì*

$${}^2g(\langle a, a + d \rangle) = h(a, d, 1).$$

Chứng minh. Từ Định lý 2.1.5 ta có

$$^2g(\langle a, a + d \rangle) \leq (a - ((\mu - 1)d + \alpha_{j+1}))^2.$$

Đặt $i = (\mu - 1)d + \alpha_{j+1}$ (khi đó $\lambda_i = \lambda^*$). Dựa vào Mệnh đề 2.1.1 và giả thiết $(i + d)^2 = (\mu d + \alpha_j + 1)^2 > (d - \lambda^*)(a + d)$, hệ quả sẽ được chứng minh nếu ta chỉ ra được

$$(a - i)^2 \notin \langle a, a + d \rangle.$$

Điều này tương đương với

$$(i + d)^2 > \left(\left(\left\lfloor \frac{i^2 + \lambda_i a}{ad} \right\rfloor + 1 \right) d - \lambda_i \right) (a + d)$$

hay

$$(d - \lambda^*)(a + d) > \left(\left(\left\lfloor \frac{i^2 + \lambda^* a}{ad} \right\rfloor + 1 \right) d - \lambda^* \right) (a + d).$$

Do đó ta cần chứng minh $\left\lfloor \frac{i^2 + \lambda^* a}{ad} \right\rfloor = 0$ hay nói cách khác $\frac{i^2 + \lambda^* a}{ad} < 1$. Thật vậy, ta có

$$\begin{aligned} i^2 &= ((\mu - 1)d + \alpha_j + 1)^2 \\ &= ((\mu d + \alpha_j) - (d + \alpha_j - \alpha_j + 1))^2 \\ &= (\mu d + \alpha_j)^2 - (d + \alpha_j - \alpha_j + 1)((2\mu - 1)d + \alpha_j + \alpha_j + 1). \end{aligned}$$

Ta có các nhận xét sau.

- $d + \alpha_j - \alpha_{j+1} = d - 1 - \alpha_{j+1} + 1 + \alpha_j \geq 2$.
- $(2\mu - 1)d + \alpha_j + \alpha_{j+1} > (2\mu - 1)d$.
- $a + d > 4\lambda^* d^3 \Rightarrow a + d > (d - \lambda^*)d^2$.
- Từ chứng minh Định lý 2.1.5, ta suy ra $\mu \geq 2(d - \lambda^*) - 1 \geq 1$, do đó

$$d - \lambda^* < \frac{1}{2}(\mu + 1) < 2(2\mu - 1).$$

Từ những nhận xét trên, ta có

$$\begin{aligned} i^2 &< (\mu d + \alpha_j)^2 - 2(2\mu - 1)d \\ &\leq (d - \lambda^*)(a + d) - 2(2\mu - 1)d \\ &< (d - \lambda^*)(a + d) - (d - \lambda^*)d = (d - \lambda^*)a. \end{aligned}$$

Từ đó suy ra $\frac{i^2 + \lambda^* a}{ad} < \frac{(d - \lambda^*)a + \lambda^* a}{ad} = 1$ và Hệ quả đã được chứng minh. $\square$

Điều kiện $a + d > 4\lambda^* d^3$ trong Hệ quả 2.1.6 là cần thiết không thể bỏ đi được. Sau đây, chúng tôi chỉ ra ví dụ chứng tỏ điều này.

2.1.7 Ví dụ. Chẳng hạn với $a = 2$, $d = 5$, $k = 1$ thay số kiểm tra thấy điều kiện $a + d > 4\lambda^* d^3$ không được thỏa mãn. Nửa nhóm số trong trường hợp này sẽ có dạng

$$S = \langle 2, 7 \rangle = \{0, 2, 4, 6, 7 \rightarrow\}.$$

Do đó ${}^2g(S) = {}^2g(\langle 2, 7 \rangle) = 1$.

Từ Định nghĩa 2.1.2 ta xác định được các $\lambda_i \in \{0, 1, 2, 3, 4\}$ thỏa mãn $2\lambda_i + i^2 \equiv 0 \pmod{5}$ với mọi $i \in \{0, 1, 2, 3, 4\}$ như sau

$$\lambda_0 = 0; \lambda_1 = 2; \lambda_2 = \lambda_3 = 3; \lambda_4 = 2$$

Do đó $\lambda^* = \lambda_{\alpha_j} = \lambda_2 = \lambda_3 = 3$ nên $\alpha_j = 2$ hoặc $\alpha_j = 3$. Ta xét điều kiện sau với j là chỉ số duy nhất thỏa mãn và μ là số tự nhiên nào đó

$$(5\mu + \alpha_j)^2 \leq (1.5 - 3)(2 + 1.5) < (5\mu + \alpha_{j+1})^2,$$

tương đương với

$$(5\mu + \alpha_j)^2 \leq 14 < (5\mu + \alpha_{j+1})^2.$$

Với $\alpha_j = 2$ hoặc $\alpha_j = 3$ và $(5\mu + \alpha_j)^2 \leq 14$ ta suy ra $\mu = 0$. Từ đó dẫn đến $\alpha_{j+1}^2 > 14$ hay $\alpha_{j+1} \geq 4$.

Xét hai trường hợp.

Trường hợp 1. $j < n$.

Ta có $4 \leq \alpha_{j+1} \leq \alpha_n \leq 4$ từ đó suy ra $\alpha_{j+1} = \alpha_n = 4$.

Với $\alpha_j = 2$ hoặc $\alpha_j = 3$ thì ta đều có $\alpha_j < \alpha_{j+1}$ do đó j không là chỉ số duy nhất thỏa mãn điều kiện. Vậy trường hợp $j < n$ loại.

Trường hợp 2 $j = n$.

Trong trường hợp này ta có

$$\alpha_j = d - \alpha_1$$

và

$$\alpha_{j+1} = d + \alpha_1.$$

Nếu $\alpha_j = 2$ thì $\alpha_1 = 3$ mâu thuẫn với $\alpha_1 < \alpha_j$ với $1 \leq j \leq n$. Vậy $\alpha_j = 3$ dẫn đến $\alpha_1 = 2$ và $\alpha_{j+1} = 5 + 2 = 7$. Từ đó ta tính được

$$h(2, 5, 1) = (2 - ((0 - 1).5 + 7))^2 = 0.$$

Nhận thấy ${}^2g(\langle 2, 7 \rangle) \neq h(2, 5, 1)$, tức là đẳng thức trong Hệ quả 2.1.6 không thỏa mãn. Tuy nhiên, các kết quả tiếp theo ở những mục sau, chúng ta sẽ thấy rằng số các giá trị của a không thỏa mãn đẳng thức ${}^2g(\langle a, a + d \rangle) = h(a, d, 1)$ là hữu hạn đối với mỗi giá trị xác định của d .

2.2 Số Frobenius bình phương của nửa nhóm số $\langle a, a + d \rangle$ với d bé

Trong mục này chúng ta trình bày công thức tính ${}^2g(\langle a, a + d \rangle)$ trong trường hợp $d = 3, 4, 5$.

Đầu tiên, nếu ${}^2g(\langle a, a + d \rangle) \neq h(a, d, 1)$ thì từ Hệ quả 2.1.6 ta suy ra $a + d \leq 4\lambda^*d^3$. Nếu d là số nguyên dương bất kỳ thỏa mãn $d \geq 3$ và với tính chất $\lambda^* \leq d - 1$ thì ta suy ra được

$$2 \leq a \leq 4(d - 1)d^3 - d.$$

Vì ta đang quan tâm đến những giá trị của a không thỏa mãn đẳng thức ở Hệ quả 2.1.6 nên thật tự nhiên ta có định nghĩa sau đây.

2.2.1 Định nghĩa. Cho d là một số nguyên dương bất kỳ thỏa mãn $d \geq 3$ và $\gcd(a, d) = 1$. Ký hiệu tập $E(d)$ là tập các số tự nhiên a không thỏa mãn đẳng thức ở Hệ quả 2.1.6, nghĩa là:

$$E(d) := \{a \in \mathbb{N} \setminus \{0, 1\} \mid \gcd(a, d) = 1; {}^2g(\langle a, a + d \rangle) \neq h(a, d, 1)\}.$$

Dễ thấy rằng $E(d) \subset [2, 4(d-1)d^3 - d] \cap \mathbb{N}$. Với những giá trị d nhỏ, $3 \leq d \leq 12$, [4] đã xác định được $E(d)$ như bảng sau đây nhờ vào việc tính toán trên các phần mềm máy tính

d	$ E(d) $	$E(d)$
3	0	$\emptyset$
4	0	$\emptyset$
5	5	$\{2, 4, 13, 27, 32\}$
6	0	$\emptyset$
7	10	$\{2, 3, 4, 9, 16, 18, 19, 23, 30, 114\}$
8	5	$\{5, 9, 21, 45, 77\}$
9	5	$\{2, 4, 7, 8, 16\}$
10	14	$\{3, 9, 13, 23, 27, 33, 43, 123, 133, 143, 153, 163, 333, 343\}$
11	14	$\{2, 3, 4, 5, 7, 8, 9, 14, 16, 18, 25, 36, 38, 47\}$
12	9	$\{13, 19, 25, 31, 67, 79, 139, 151, 235\}$

Với những giá trị nhỏ của d như đã nói ở trên, giá trị chính xác của ${}^2g(\langle a, a + d \rangle)$ khi $a \in E(d)$ được tính toán nhờ vào các phần mềm mà [4] đã đưa ra cho ở bảng dưới đây.

d	a	${}^2g(\langle a, a+d \rangle)$	$d(a, d, 1)$	d	a	${}^2g(\langle a, a+d \rangle)$	$d(a, d, 1)$
5	2	1	0	10	43	40^2	39^2
5	4	1	2^2	10	123	110^2	109^2
5	13	10^2	9	10	133	120^2	119^2
5	27	21^2	20^2	10	143	130^2	129^2
5	32	26^2	25^2	10	153	140^2	139^2
7	2	1	5^2	10	163	150^2	149^2
7	3	2^2	0	10	333	310^2	309^2
7	4	5^2	6^2	10	343	320^2	319^2
7	9	7^2	6^2	11	2	3^2	4^2
7	16	14^2	13^2	11	3	5^2	9^2
7	18	17^2	16^2	11	4	5^2	6^2
7	19	14^2	13^2	11	5	7^2	9^2
7	23	21^2	20^2	11	7	4^2	2^2
7	30	28^2	27^2	11	8	7^2	12^2
7	114	105^2	104^2	11	9	8^2	12^2
8	5	4^2	3^2	11	14	13^2	19^2
8	9	10^2	12^2	11	16	14^2	20^2
8	21	16^2	15^2	11	18	15^2	13^2
8	45	36^2	35^2	11	25	22^2	20^2
8	77	64^2	63^2	11	36	33^2	31^2
9	2	3^2	4^2	11	38	36^2	34^2
9	4	3^2	6^2	11	47	44^2	42^2
9	7	6^2	11^2	12	13	14^2	18^2
9	8	6^2	4^2	12	19	17^2	16^2
9	16	9^2	12^2	12	25	26^2	30^2
10	3	2^2	7^2	12	31	29^2	28^2
10	9	7^2	12^2	12	67	59^2	58^2
10	13	10^2	9^2	12	79	71^2	70^2
10	23	20^2	19^2	12	139	125^2	124^2
10	27	26^2	25^2	12	151	137^2	136^2
10	33	30^2	29^2	12	235	215^2	214^2

Với mỗi giá trị $d \in \{3, \dots, 12\}$, ta có thể thiết lập công thức để tính ${}^2g(\langle a, a+d \rangle)$ ngoài những giá trị cho trong bảng trên. Ngoài ra trong bảng trên ta nhận thấy khi $d = 3, 4, 5$ thì tập $E(d) = \emptyset$, có nghĩa là ta có thể thiết lập công thức tính ${}^2g(\langle a, a+d \rangle)$ với mọi số nguyên a .

Dựa vào các phương pháp chứng minh ở Định lý 2.1.5 và Hệ quả 2.1.6 ta

có kết quả sau về công thức tính ${}^2g(\langle a, a+d \rangle)$ trong trường hợp $d = 3$.

2.2.2 Định lý. Cho $a \geq 3$ là số nguyên dương không chia hết cho 3 và $S = \langle a, a+3 \rangle$. Khi đó,

$${}^2g(S) = \begin{cases} (a - (3b - 1))^2 \text{ nếu hoặc } (3b + 1)^2 \leq a + 3 < (3b + 2)^2 \text{ và } a \equiv 1 \pmod{3} \\ \text{hoặc } (3b + 1)^2 \leq 2(a + 3) < (3b + 2)^2 \text{ và } a \equiv 2 \pmod{3}, \\ (a - (3b + 1))^2 \text{ nếu hoặc } (3b + 2)^2 \leq a + 3 < (3b + 4)^2 \text{ và } a \equiv 1 \pmod{3} \\ \text{hoặc } (3b + 2)^2 \leq 2(a + 3) < (3b + 4)^2 \text{ và } a \equiv 2 \pmod{3}. \end{cases}$$

Chứng minh. Vì $g(S) = (a - 1)(a + 2) - 1 = a^2 + a - 3 < (a + 1)^2$ nên

$${}^2g(S) \leq (a - 1)^2.$$

Theo Mệnh đề 2.1.1, ta có

$$(a - i)^2 \in S \Leftrightarrow (i + 3)^2 \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i \right) (a + 3). \quad (2.8)$$

với $i \in \mathbb{Z}, \lambda_i \in \{0, 1, 2\}$ sao cho $a\lambda_i + i^2 \equiv 0 \pmod{3}$, nghĩa là

$$\lambda_i = \begin{cases} 0 \text{ nếu } i \equiv 0 \pmod{3} \text{ và } a \equiv 1, 2 \pmod{3}, \\ 1 \text{ nếu } i \equiv 1, 2 \pmod{3} \text{ và } a \equiv 2 \pmod{3}, \\ 2 \text{ nếu } i \equiv 1, 2 \pmod{3} \text{ và } a \equiv 1 \pmod{3}. \end{cases}$$

Ta xét 4 trường hợp sau đây.

Trường hợp 1. Giả sử $a \equiv 1 \pmod{3}$ và $(3b + 1)^2 \leq a + 3 < (3b + 2)^2$.

Nếu $i \leq 3b - 2$ thì

$$(i + 3)^2 \leq (3b + 1)^2 \leq a + 3 \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i \right) (a + 3).$$

Do đó, từ đẳng thức 2.8 ta suy ra $(a - i)^2 \in S$.

Nếu $i = 3b - 1$, do $b \geq 1$ ta có

$$i^2 = (3b - 1)^2 = 9b^2 - 6b + 1 < 9b^2 + 6b - 2 = (3b + 1)^2 - 3 \leq a.$$

Vì $3b - 1 \equiv 2 \pmod{3}$ nên ta có

$$0 \leq \frac{i^2 + \lambda_i a}{3a} = \frac{i^2 + 2a}{3a} < 1.$$

Do đó

$$\left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor = 0.$$

Hơn nữa, vì

$$\left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i \right) (a + 3) = a + 3 < (3b + 2)^2 = (i + 3)^2,$$

nên từ đẳng thức 2.8, ta suy ra $(a - i)^2 \notin S$.

Trường hợp 2. Giả sử $a \equiv 1 \pmod{3}$ và $(3b + 2)^2 \leq a + 3 < (3b + 4)^2$.

Nếu $i \leq 3b - 1$ thì

$$(i + 3)^2 = (3b + 2)^2 \leq a + 3 \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i \right) (a + 3).$$

Do đó, theo 2.8, ta có $(a - i)^2 \in S$.

Nếu $i = 3b$ thì

$$(i + 3)^2 = (3b + 3)^2 \leq 3(3b + 2)^2 \leq 3(a + 3) \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i \right) (a + 3).$$

Do đó, theo 2.8, ta có $(a - i)^2 \in S$.

Nếu $i = 3b + 1$, do $b \geq 1$ nên ta có

$$i^2 = (3b + 1)^2 = 9b^2 + 6b + 1 < 9b^2 + 12b + 1 = (3b + 2)^2 - 3 \leq a.$$

Vì $3b + 1 \equiv 1 \pmod{3}$ ta suy ra

$$0 \leq \frac{i^2 + \lambda_i a}{3a} = \frac{i^2 + 2a}{3a} < 1$$

và do đó

$$\left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor = 0.$$

Hơn nữa, vì

$$\left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i\right) (a + 3) = a + 3 < (3b + 4)^2 = (i + 3)^2,$$

nên theo đẳng thức 2.8, ta có $(a - i)^2 \notin S$.

Trường hợp 3. Giả sử rằng $a \equiv 2 \pmod{3}$ và $(3b + 1)^2 \leq 2(a + 3) < (3b + 2)^2$.

Nếu $i \leq 3b - 2$ thì

$$(i + 3)^2 = (3b + 1)^2 \leq 2(a + 3) \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i\right) (a + 3).$$

Do đó, từ đẳng thức 2.8 ta suy ra $(a - i)^2 \in S$.

Nếu $i = 3b - 1$, do $b \geq 1$ nên

$$i^2 = (3b - 1)^2 = 9b^2 - 6b + 1 < 9b^2 + 6b - 5 = (3b + 1)^2 - 6 \leq 2a.$$

Vì $3b - 1 \equiv 2 \pmod{3}$ nên ta suy ra

$$0 \leq \frac{i^2 + \lambda_i a}{3a} = \frac{i^2 + a}{3a} < 1$$

và do đó

$$\left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor = 0.$$

Hơn nữa, vì

$$\left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i\right) (a + 3) = 2(a + 3) < (3b + 2)^2 = (i + 3)^2,$$

nên theo 2.8, ta có $(a - i)^2 \notin S$.

Trường hợp 4. Giả sử $a \equiv 2 \pmod{3}$ và $(3b + 2)^2 \leq 2(a + 3) < (3b + 4)^2$.

Nếu $i \leq 3b - 1$ thì

$$(i + 3)^2 = (3b + 2)^2 \leq 2(a + 3) \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i\right) (a + 3).$$

Do đó, theo 2.8, ta có $(a - i)^2 \in S$.

Nếu $i = 3b$ thì $a^2 \in S$ khi $b = 0$ và $b \geq 1$ nên

$$(i+3)^2 = (3b+3)^2 < \frac{3}{2}(3b+2)^2 \leq 3(a+3) \leq \left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i\right) (a+3)$$

Do đó, từ đẳng thức 2.8, ta có $(a-i)^2 \in S$.

Nếu $i = 3b + 1$, do $b \geq 1$ nên

$$i^2 = (3b+1)^2 = 9b^2 + 6b + 1 < 9b^2 + 12b - 2 = (3b+2)^2 - 6 \leq 2a.$$

Mặt khác, $i^2 = 1 < 2a$ khi $b = 0$ nên ta suy ra

$$0 \leq \frac{i^2 + \lambda_i a}{3a} = \frac{i^2 + a}{3a} < 1.$$

Điều đó có nghĩa là

$$\left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor = 0.$$

Hơn nữa, vì

$$\left(3 \left\lfloor \frac{i^2 + \lambda_i a}{3a} \right\rfloor + 3 - \lambda_i\right) (a+3) = 2(a+3) < (3b+4)^2 = (i+3)^2$$

nên theo 2.8, ta có $(a-i)^2 \notin S$. □

Dựa vào cách chứng minh định lý trên, ta có thể chứng minh hai định lý dưới đây với trường hợp $d = 4, 5$ một cách hoàn toàn tương tự.

2.2.3 Định lý. Cho $a \geq 3$ là một số nguyên lẻ và đặt $S = \langle a, a+4 \rangle$. Khi đó

$${}^2g(S) = \begin{cases} (a - (4b-1))^2 \text{ nếu hoặc } (4b+1)^2 \leq a+4 < (4b+2)^2 \text{ và } a \equiv 1 \pmod{4} \\ \text{hoặc } (4b+1)^2 \leq 3(a+4) < (4b+3)^2 \text{ và } a \equiv 3 \pmod{4}, \\ (a - (4b+1))^2 \text{ nếu hoặc } (4b+3)^2 \leq a+4 < (4b+5)^2 \text{ và } a \equiv 1 \pmod{4} \\ \text{hoặc } (4b+3)^2 \leq 3(a+4) < (4b+5)^2 \text{ và } a \equiv 3 \pmod{4}. \end{cases}$$

2.2.4 Định lý. Cho $a \geq 2$ là một số nguyên không chia hết cho 5 và đặt $S = \langle a, a + 5 \rangle$. Khi đó

$${}^2g(S) = \begin{cases} (a - (5b - 2))^2 \text{ nếu hoặc } (5b + 2)^2 \leq a + 5 < (5b + 3)^2 \text{ và } a \equiv 4 \pmod{5} \\ \text{hoặc } (5b + 2)^2 \leq 2(a + 5) < (5b + 3)^2 \text{ và } a \equiv 2 \pmod{5}, \\ (a - (5b - 1))^2 \text{ nếu hoặc } (5b + 1)^2 \leq a + 5 < (5b + 4)^2 \text{ và } a \equiv 1 \pmod{5} \\ \text{hoặc } (5b + 1)^2 \leq 2(a + 5) < (5b + 4)^2 \text{ và } a \equiv 3 \pmod{5}, a \neq 13, \\ (a - (5b + 1))^2 \text{ nếu hoặc } (5b + 4)^2 \leq a + 5 < (5b + 6)^2 \text{ và } a \equiv 1 \pmod{5} \\ \text{hoặc } (5b + 4)^2 \leq 2(a + 5) < (5b + 6)^2 \text{ và } a \equiv 3 \pmod{5}, \\ (a - (5b + 2))^2 \text{ nếu hoặc } (5b + 3)^2 \leq a + 5 < (5b + 7)^2 \text{ và } a \equiv 4 \pmod{5}, a \neq 4 \\ \text{hoặc } (5b + 3)^2 \leq 2(a + 5) < (5b + 7)^2 \text{ và } a \equiv 2 \pmod{5}, a \neq 2, 27, 32. \end{cases}$$

2.3 Số Frobenius bình phương của nửa nhóm số $S = \langle a, a + d \rangle$ với $d = 1, 2$.

Định lý sau đây chúng ta trình bày công thức tính số Frobenius bình phương cho nửa nhóm số có dạng $\langle a, a + 1 \rangle$ trong trường hợp a hoặc $a + 1$ không là số chính phương và $a \geq 2$.

2.3.1 Định lý. Cho a là một số nguyên dương thỏa mãn $b^2 < a < a + 1 < (b + 1)^2$ với b là một số nguyên dương nào đó. Khi đó,

$${}^2g(\langle a, a + 1 \rangle) = (a - b)^2.$$

Chứng minh. Theo Hệ quả 1.2.8, ta có $g(\langle a, a + 1 \rangle) = a^2 - a - 1$ nên

$$(a - 1)^2 \leq g(\langle a, a + 1 \rangle) < a^2$$

và ${}^2g(\langle a, a + 1 \rangle) < a^2$.

Ta sẽ chứng minh rằng $(a - i)^2 \in \langle a, a + 1 \rangle$ với mọi $i \in \{1, 2, \dots, b - 1\}$.

Đầu tiên, ta nhận thấy

$$(a - i)^2 = a^2 - 2ai + i^2 = (a - 2i)a + i^2 = (a - 2i - i^2)a + i^2(a + 1), \quad (2.9)$$

với mọi số nguyên i . Do với mọi $i \in \{1, 2, \dots, b-1\}$, ta có

$$a - 2i - i^2 = a - i(i+2) \geq a - (b-1)(b+1) = a - b^2 + 1 > 0$$

và $i^2 > 0$ nên từ 2.9, ta suy ra $(a-i)^2 \in \langle a, a+1 \rangle$ với mọi $i \in \{1, 2, \dots, b-1\}$.

Cuối cùng, vì $a+1 < (b+1)^2$ (nghĩa là $a - 2b - b^2 < 0$) và $0 < b^2 < a$ nên từ 2.9, ta có $(a-b)^2 \notin \langle a, a+1 \rangle$. $\square$

2.3.2 Nhận xét. Sau đây chúng tôi đưa ra một cách chứng minh khác cho định lý trên, khác với chứng minh trình bày trong [4].

Áp dụng Mệnh đề 2.1.1 với $k = d = 1$, ta có $(a-i)^2 \in \langle a, a+1 \rangle$ khi và chỉ khi $(i+1)^2 \leq (a+1) \left(\left\lfloor \frac{i^2}{a} \right\rfloor + 1 \right)$. Ta xét hai trường hợp.

Trường hợp 1. Với $i \leq b-1$ ta có

$$(i+1)^2 \leq b^2 < a+1 < (a+1) \left(\left\lfloor \frac{i^2}{a} \right\rfloor + 1 \right).$$

Do đó $(a-i)^2 \in \langle a, a+1 \rangle$ với $i \leq b-1$.

Trường hợp 2. Với $i = b$, do $0 < \frac{b^2}{a} < 1$ nên ta có $\left\lfloor \frac{b^2}{a} \right\rfloor = 0$. Do đó

$$(i+1)^2 = (b+1)^2 > a+1 = (a+1) \cdot 1 = (a+1) \left(\left\lfloor \frac{i^2}{a} \right\rfloor + 1 \right)$$

tức là $(a-i)^2 \notin \langle a, a+1 \rangle$.

Như vậy, $(a-i)^2 \in \langle a, a+1 \rangle$ với mọi $i \in \{1, 2, \dots, b-1\}$ và $(a-b)^2 \notin \langle a, a+1 \rangle$. Do đó, ${}^2g(\langle a, a+1 \rangle) = (a-b)^2$.

Tiếp theo, chúng ta trình bày công thức tính số Frobenius bình phương của nửa nhóm số có dạng $S = \langle a, a+2 \rangle$ với $a \geq 3$ là một số nguyên lẻ, a và $a+2$ không là số chính phương.

2.3.3 Định lý. Cho số nguyên lẻ $a \geq 3$ thỏa mãn

$$(2b+1)^2 < a < a+2 < (2b+3)^2$$

với b là một số nguyên dương nào đó. Khi đó,

$${}^2g(\langle a, a+2 \rangle) = (a - (2b+1))^2.$$

Chứng minh. Theo Hệ quả 1.2.8, ta có $g(\langle a, a+2 \rangle) = (a-1)(a+1)-1 = a^2-2$ nên

$$(a-1)^2 < g(\langle a, a+2 \rangle) < a^2.$$

Từ đó ta suy ra

$$^2g(\langle a, a+2 \rangle) < a^2.$$

Ta sẽ chứng minh rằng $(a-i)^2 \in \langle a, a+2 \rangle$ với $i \in 1, 2, \dots, 2b$. Thật vậy, với mọi số nguyên i , ta có

$$(a-2i)^2 = a^2 - 4ai + 4i^2 = (a-4i)a + 4i^2 = (a-4i-2i^2)a + 2i^2(a+2). \quad (2.10)$$

Mặt khác, với mọi $i \in \{1, 2, \dots, b\}$, ta có

$$a-4i-2i^2 = a-2i(i+2) \geq a-2i(2i+1) > a-(2i+1)^2 \geq a-(2b+1)^2 > 0$$

và do $2i^2 > 0$ nên từ 2.10, ta suy ra $(a-2i)^2 \in \langle a, a+2 \rangle$ với mọi $i \in \{1, 2, \dots, b\}$.

Hơn nữa, với mọi số nguyên i , ta có

$$\begin{aligned} (a-(2i+1))^2 &= a^2 - 2a(2i+1) + (2i+1)^2 \\ &= (a-2(2i+1))a + (2i+1)^2 \\ &= (a-4i-3)a + (2i+1)^2 + a \\ &= \left(a-4i-3 - \frac{(2i+1)^2 + a}{2}\right)a + \frac{(2i+1)^2 + a}{2}(a+2) \\ &= \frac{a-4i^2-12i-7}{2}a + \frac{(2i+1)^2 + a}{2}(a+2) \\ &= \frac{a+2-(2i+3)^2}{2}a + \frac{(2i+1)^2 + a}{2}(a+2). \end{aligned} \quad (2.11)$$

Do đó, với mọi $i \in \{0, 1, \dots, b-1\}$ thì

$$\frac{a+2-(2i+3)^2}{2} \geq \frac{a+2-(2b+1)^2}{2} > 0$$

và

$$\frac{(2i+1)^2 + a}{2} > 0,$$

từ đó kết hợp với 2.11, ta suy ra $(a - (2i+1))^2 \in \langle a, a+2 \rangle$. Cuối cùng, vì

$$0 < \frac{(2b+1)^2 + a}{2} < a$$

và

$$\frac{a+2 - (2b+3)^2}{2} < 0$$

nên từ 2.11, ta có $(a - (2b+1))^2 \notin \langle a, a+2 \rangle$.

Vì vậy ta có

$${}^2g(\langle a, a+2 \rangle) = (a - (2b+1))^2.$$

□

2.3.4 Nhận xét. Chứng minh trên của Định lý 2.3.3 được trình bày trong [4]. Sau đây, chúng tôi đưa ra một cách chứng minh khác cho định lý này.

Với i là số nguyên tùy ý, với định nghĩa của ký hiệu λ_i như trong Định nghĩa 2.1.2, ta có

$$0 \leq \lambda_i \leq 1 \text{ và } a\lambda_i + i^2 \equiv 0 \pmod{2}.$$

Do đó

$$\lambda_i = \begin{cases} 0 & \text{khi } i \equiv 0 \pmod{2}, \\ 1 & \text{khi } i \equiv 1 \pmod{2}. \end{cases}$$

Ta xét ba trường hợp

Trường hợp 1. Với $i \leq 2b-1$, ta có

$$(i+1)^2 \leq (2b+1)^2 < a+2 = (a+2) \left(2 \left\lfloor \frac{i^2 + \lambda_i a}{2a} \right\rfloor + 2 - \lambda_i \right).$$

Do đó, theo Mệnh đề 2.1.1, $(a-i)^2 \in \langle a, a+1 \rangle$ với $i \leq 2b-1$.

Trường hợp 2. Với $i = 2b$, nghĩa là $\lambda_i = 0$, ta có

$$(i+2)^2 = (2b+2)^2 < 2(2b+1)^2 < 2(a+2) \leq (a+2) \left(2 \left\lfloor \frac{i^2 + \lambda_i a}{2a} \right\rfloor + 2 - \lambda_i \right).$$

Do đó, theo Mệnh đề 2.1.1, $(a - i)^2 \in \langle a, a + 1 \rangle$ với $i = 2b$.

Trường hợp 3. Với $i = 2b + 1$, nghĩa là $\lambda_i = 1$, ta có

$$0 < \frac{i^2 + \lambda_i a}{2a} = \frac{(2b + 1)^2 + \lambda_i a}{2a} < \frac{a + a}{2a} < 1.$$

Từ đó suy ra

$$\left\lfloor \frac{i^2 + \lambda_i a}{a} \right\rfloor = \left\lfloor \frac{(2b + 1)^2 + a}{2a} \right\rfloor = 0.$$

Do đó

$$(i + 2)^2 = (2b + 3)^2 > (a + 2) = (a + 2) \left(2 \left\lfloor \frac{i^2 + \lambda_i a}{2a} \right\rfloor + 2 - \lambda_i \right).$$

Vì vậy, theo Mệnh đề 2.1.1 $(a - i)^2 \notin \langle a, a + 2 \rangle$.

Từ những chứng minh trên, ta suy ra

$${}^2g(\langle a, a + 1 \rangle) = (a - (2b + 1))^2.$$

KẾT LUẬN

Nội dung chính của luận văn là trình bày các kết quả trong bài báo [4] của Jonathan Chappelton và Joge Luis Ramírez Alfonsín. Cụ thể là chúng tôi đã trình bày được những nội dung sau đây.

1. Trình bày chứng minh cho một chặn trên của số Frobenius bình phương của nửa nhóm số sinh bởi cấp số cộng với điều kiện cho trước (Định lý 2.1.5), đồng thời từ đó suy ra công thức tính số Frobenius bình phương khi nửa nhóm số sinh bởi hai phần tử (Hệ quả 2.1.6). Trong phần này, chúng tôi cũng có cải tiến một phần trong chứng minh của Định lý 2.1.5 (xem Nhận xét 2.1.4) và chỉ ra ví dụ chứng tỏ điều kiện đưa ra trong Hệ quả 2.1.6 là không thể bỏ đi được (Ví dụ 2.1.7).
2. Trình bày công thức tính số Frobenius bình phương của nửa nhóm số có dạng $\langle a, a + d \rangle$ với $d = 3, 4, 5$ (Định lý 2.2.2, Định lý 2.2.3, Định lý 2.2.4).
3. Trình bày và đưa ra một cách chứng minh khác cho công thức tính số Frobenius bình phương của nửa nhóm số có dạng $S = \langle a, a + 1 \rangle$ và $S = \langle a, a + 2 \rangle$ (Định lý 2.3.1, Định lý 2.3.3).

TÀI LIỆU THAM KHẢO

Tiếng Việt

- [1] Lương Ngọc Nhật (2017), *Một số bất biến của nửa nhóm số*, Luận văn thạc sĩ toán học, Trường Đại học Vinh.
- [2] Nguyễn Quang Phúc (2018), *Số Frobenius và giống của nửa nhóm số với chiều nhúng bằng 3*, Luận văn thạc sĩ toán học, Trường Đại học Vinh.
- [3] Hoàng Thế Toàn (2017), *Về vấn đề số Frobenius cho các nửa nhóm số*, Luận văn thạc sĩ toán học, Trường Đại học Vinh.

Tiếng Anh

- [4] J. Chappelton and J. L. R. Alfosín (2020), The square Frobenius number, *HAL Id: hal-02879706*<https://hal.archives-ouvertes.fr/hal-02879706>, *Preprint submitted on 24 Jun 2020*; <https://arxiv.org/abs/2006.14219>, *Preprint submitted on 25 Jun 2020*.
- [5] J.B. Roberts (1956), Note in linear forms, *Proc.Amer.Math.Soc*, **7**, 465-469.
- [6] J.C. Rosales, P.A. García- Sánchez (2009), *Numerical semigroups*, Development in mathematics, **20**, Springer.
- [7] J. J. Sylvester (1882), Excursus on rational fractions and partitions, *American Journal of Mathematics*, **5**, 119-136.