ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ ANH

MỘT SỐ DẠNG BIỂU DIỄN SỐ NGUYÊN DƯƠNG

LUẬN VĂN THẠC SĨ TOÁN HỌC

THÁI NGUYÊN - 2018

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

NGUYỄN THỊ ANH

MỘT SỐ DẠNG BIỂU DIỄN SỐ NGUYÊN DƯƠNG

Chuyên ngành: Phương pháp Toán sơ cấp

Mã số: 8460113

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC

GS.TSKH. Hà Huy Khoái

THÁI NGUYÊN - 2018

Lời cảm ơn

Để hoàn thành luận văn này, tôi xin bày tỏ lòng biết ơn sâu sắc tới ***GS.TSKH. Hà Huy Khoái***, người đã định hướng chọn đề tài và tận tình hướng dẫn tôi trong suốt quá trình nghiên cứu và thực hiện luận văn.

Tôi cũng xin chân thành cảm ơn sự giúp đỡ quý báu của các giảng viên giảng dạy lớp cao học K10 chuyên ngành Phương pháp Toán sơ cấp nói riêng, các thầy, cô giáo trường Đại học Khoa học - Đại học Thái Nguyên nói chung.

Đồng thời, tôi xin gửi lời cảm ơn tới gia đình, bạn bè và đồng nghiệp đã luôn quan tâm, động viên tôi trong quá trình học tập và hoàn thành luận văn.

Thái Nguyên, tháng 05 năm 2018

Tác giả

Nguyễn Thị Anh

Mục lục

Mở Đầu

Vấn đề biểu diễn số nguyên dương là một trong những vấn đề quan trọng của số học, có nhiều ứng dụng trong những lĩnh vực khác nhau và luôn nhận được sự quan tâm của các của các nhà toán học. Nhiều nhà toán học nổi tiếng đã bỏ nhiều công sức để nghiên cứu nó, ví dụ Fermat, Lagrange, Wilson, Euler....

Albert Girard là người đầu tiên đưa ra nhận xét "Mỗi số nguyên tố lẻ bất kì mà đồng dư với 1 theo *modulo* 4 đều biểu diễn được dưới dạng tổng của 2 số chính phương" vào năm 1632. Fermat là người đầu tiên chứng minh và đưa ra thông báo trong lá thư gửi cho Marin Mersenne năm 1640.

Cũng như Fermat, Lagrange là một nhà lý thuyết số kiệt xuất. Trong những công trình của ông, có thể kể đến: chứng minh đầu tiên cho định lý Wilson rằng n là một số nguyên tố khi và chỉ khi $(n-1)! \equiv -1 \pmod{n}$; kiểm tra các điều kiện để ± 2 và ± 5 là thặng dư hoặc phi thặng dư bình phương của một số nguyên tố lẻ (trường hợp -1 và ± 3 đã từng được đề cập bởi Euler); tìm ra các nghiệm nguyên của phương trình $x^2 - ay^2 = 1$ và lời giải của một số bài toán đặt ra bởi Fermat, dẫn tới kết quả khẳng định rằng mỗi số nguyên tố $p \equiv 3 \pmod{8}$ đều có dạng $p = a^2 + 2b^2$,....

Mục tiêu của luận văn này là trình bày một số kết quả liên quan đến những lĩnh vực nghiên cứu kể trên, cụ thể là bài toán về biểu diễn số nguyên dương dưới dạng tổng các bình phương, và bài toán biểu diễn số nguyên dương dưới dạng tổng các số hạng của một cấp số cộng.

Chương 1

Một số kết quả kinh điển về bài toán biểu diễn số nguyên dương

1.1 Biểu diễn số nguyên dương dưới dạng tổng của hai bình phương

Về mặt lịch sử vấn đề "biểu diễn một số nguyên dưới dạng tổng các bình phương" là bài toán thu hút được nhiều sự quan tâm chú ý.

Phần này sẽ được dành để trình bày một số kết quả của hướng nghiên cứu nhằm trả lời câu hỏi "Giá trị n nhỏ nhất là bao nhiêu để mọi số nguyên dương đều có thể biểu diễn được dưới dạng tổng của không quá n bình phương?"

Khi thử với vài số nguyên dương ta thấy:

$$\begin{aligned}
&1 = 1^2\\
&2 = 1^2 + 1^2\\
&3 = 1^2 + 1^2 + 1^2\\
&4 = 2^2\\
&5 = 2^2 + 1^2\\
&6 = 2^2 + 1^2 + 1^2\\
&7 = 2^2 + 1^2 + 1^2 + 1^2.
\end{aligned}$$

Do tổng của bốn bình phương là cần thiết khi biểu diễn số 7, ta suy ra ngay số cần tìm phải thoả mãn $n \geq 4$. Vẫn còn một khả năng xảy ra là một số nguyên nào đó chỉ có thể biểu diễn được dưới dạng tổng của nhiều hơn bốn bình phương. Tuy nhiên, một định lý rất nổi tiếng của Lagrange được chứng minh vào năm 1770, khẳng định rằng $n = 4$

là đủ, nghĩa là: Mọi số nguyên dương có thể biểu diễn thành tổng của bốn bình phương (trong đó có thể $0 = 0^2$).

Ta sẽ bắt đầu từ những trường hợp đơn giản. Trước tiên ta hãy tìm điều kiện cần và đủ để một số nguyên dương có thể biểu diễn được thành tổng của hai bình phương. Vấn đề này có thể được quy về xem xét các số nguyên tố bằng bổ đề dưới đây.

Bổ đề 1.1.1 *Nếu m và n đều là tổng của hai bình phương thì tích $m.n$ cũng vậy.*

Chứng minh.
Giả sử $\begin{cases} m & = a^2 + b^2 \\ n & = c^2 + d^2 \end{cases}$ với a, b, c, d nguyên.

Ta có :

$$m.n = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Bổ đề đã được chứng minh.

Ví dụ 1.1 .

$$5 = 2^2 + 1^2$$
$$3 = 2^2 + 3$$

và
$$5.13 = 65 = 4^2 + 7^2$$

hoặc

$$25 = 3^2 + 4^2$$
$$61 = 5^2 + 6^2$$

và
$$25.61 = 1525 = 25^2 + 30^2$$

Tuy nhiên không phải mọi số nguyên hay số nguyên tố nào đều có thể viết dưới dạng tổng của hai bình phương.

Ví dụ 1.2 . Không tồn tại a, b nguyên dương nào thỏa mãn $3 = a^2 + b^2$.

Và trước khi chứng minh định lý Fermat thì ta đi chứng minh Bổ Đề sau:

Bổ đề 1.1.2 *Với p là số nguyên tố và $gcd(a, p) = 1$ thì phương trình đồng dư $ax \equiv y (\mathrm{mod} p)$ có nghiệm x_0, y_0 thoả mãn*

$$\begin{cases} 0 & < |x_0| < \sqrt{p} \\ 0 & < |y_0| < \sqrt{p}. \end{cases}$$

Chứng minh.
Đặt $k = [\sqrt{p}] + 1$ và tập các số nguyên:

$$S = \{ax - y | 0 \leq x \leq k - 1; 0 \leq y \leq k - 1\}.$$

Từ đó $ax - y$ nhận $k^2 > p$ giá trị, theo nguyên lý chuồng bồ câu của Dirichlet thì tồn tại ít nhất hai phần tử của tập S đồng dư theo modulo p. Giả sử hai phần tử này là $ax_1 - y_1$ và $ax_2 - y_2$ với $x_1 \neq x_2$ hoặc $y_1 \neq y_2$. Ta có thể viết:

$$a(x_1 - x_2) \equiv (y_1 - y_2) (\text{mod} p).$$

Đặt

$$\begin{cases} x_0 & = x_1 - x_2 \\ y_0 & = y_1 - y_2. \end{cases}$$

Ta có x_0, y_0 thỏa mãn phương trình đồng dư

$$ax \equiv y (\text{mod} p).$$

Nếu nghiệm $x_0 = 0$ hoặc $y_0 = 0$ thì do $gcd(a, p) = 1$ suy ra nghiệm còn lại cũng bằng không, mâu thuẫn với giả thiết. Do đó:

$$\begin{cases} 0 & < |x_0| \leq (k - 1) < \sqrt{p} \\ 0 & < |y_0| \leq (k - 1) < \sqrt{p}. \end{cases}$$

Bây giờ ta có thể chứng minh được định lý Fermat.

Định lý 1.1.1 *(Định lý Fermat) Một số nguyên tố lẻ p có thể biểu diễn được dưới dạng tổng của hai bình phương khi và chỉ khi $p \equiv 1(\text{mod} 4)$.*

Chứng minh: Giả sử $p = a^2 + b^2$. Vì p là số nguyên tố nên $p \not| \ a$, $p \not| \ b$ (Nếu $p \mid a$ thì $p \mid b^2$ nên $p \mid b$ dẫn đến mâu thuẫn $p^2 \mid p$). Vì vậy theo thuyết đồng dư tuyến tính tồn tại một số c để $bc \equiv 1 \pmod{p}$. Theo modulo p thì quan hệ $(ac)^2 + (bc)^2 = pc^2$ trở thành:

$$(ac)^2 \equiv -1 (\text{mod} p).$$

Như vậy, (-1) là một thặng dư bình phương của p, và theo một kết quả đã biết, $(\frac{-1}{p}) = 1$ chỉ khi $p \equiv 1(\text{mod} 4)$.

Điều ngược lại, giả sử $p \equiv 1(\text{mod}4)$. Vì (-1) là một thặng dư bình phương của p nên tồn tại một số nguyên a sao cho $a^2 \equiv -1(\text{mod}p)$ .Một trong những giá trị a thoả mãn là : $a = \left[\dfrac{(p-1)}{2}\right]!$. Do $(a,p) = 1$ phương trình đồng dư $ax \equiv y(\text{mod}p)$ nhận một nghiệm x_0, y_0 và ta có

$$-x_0^2 \equiv a^2x_0^2 \equiv (ax_0)^2 \equiv y_0^2(\text{mod}p)$$

hoặc

$$x_0^2 + y_0^2 \equiv 0(\text{mod}p).$$

Suy ra $x_0^2 + y_0^2 = kp$ với số nguyên $k \geq 1$ nào đó.

Mặt khác theo bổ đề 2 ta có

$$\begin{cases} 0 & < |x_0| < \sqrt{p} \\ 0 & < |y_0| < \sqrt{p} \end{cases}$$

suy ra $0 < x_0^2 + y_0^2 < 2p$ suy ra $k = 1$ và $x_0^2 + y_0^2 = p$.
Vậy định lí được chứng minh.

Để ý rằng $(-a)^2 = a^2$, ta có hệ quả sau.

Hệ quả 1.1.1 *Số nguyên tố p bất kỳ có dạng $4k+1$ có thể biểu diễn duy nhất (không kể thứ tự của số hạng) thành tổng của hai bình phương.*

Ví dụ 1.3 . Xét số nguyên tố $p = 13$. Số nguyên a tương ứng trong chứng minh định lý trên có thể lấy là $a = \left[\dfrac{(p-1)}{2}\right]! = 6! = 720$.

Một nghiệm của phương trình đồng dư

$$720x \equiv y(\text{mod}13) \text{ hay } 5x \equiv y(\text{mod}13)$$

tìm được bằng cách xét tập hợp $S = \{5x - y | 0 \leq x, y < 4\}$. Các phần tử của tập S là các số nguyên:

$$\begin{array}{cccc} 0 & 5 & 10 & 15 \\ -1 & 4 & 9 & 14 \\ -2 & 3 & 8 & 13 \\ -3 & 2 & 7 & 12 \end{array}$$

Theo modulo 13 trở thành

$$\begin{array}{cccc} 0 & 5 & 10 & 2 \end{array}$$

$$\begin{matrix} 12 & 4 & 9 & 1 \\ 11 & 3 & 8 & 0 \\ 10 & 2 & 7 & 12. \end{matrix}$$

Trong số các khả năng khác nhau ta có.

$$5.1 - 3 \equiv 2 \equiv 5.3 - 0 (\text{mod} 13)$$

hoặc

$$5(1 - 3) \equiv 3 (\text{mod} 13).$$

Vì vậy ta có thể lấy

$$\begin{cases} x_0 &= -2 \\ y_0 &= 3 \end{cases}$$

để được

$$13 = x_0^2 + y_0^2 = 2^2 + 3^2.$$

Chú ý: $13 = 2^2 + 3^2 = 2^2 + (-3)^2 = (-2)^2 + 3^2 = (-2)^2 + (-3)^2 = 3^2 + 2^2 = 3^2 + (-2)^2 = (-3)^2 + 2^2 = (-3)^2 + (-2)^2$. Tám cách viết này chỉ là một khi không kể đến thứ tự. Nên biểu diễn $13 = 2^2 + 3^2$ là duy nhất.

Ta đã chỉ ra rằng mọi số nguyên tố có dạng $p = 4k + 1$ đều có thể biểu diễn duy nhất thành tổng của hai bình phương, câu hỏi đặt ra là: Số nguyên tố tích có chứa thừa số là $4k + 3$ có tính chất trên không? Để trả lời câu hỏi trên ta đi xét định lý sau.

Định lý 1.1.2 *Cho số nguyên dương n có dạng $n = N^2 m$, trong đó m là số squarefree (số không có ước chính phương khác 1). Khi đó n có thể biểu diễn được dưới dạng tổng của hai bình phương khi và chỉ khi m không chứa thừa số nguyên tố dạng $4k + 3$.*

Chứng minh.

- Nếu $m = 1$ thì $n = N^2 + 0^2$: luôn đúng.
- Giả sử $m > 1$.

1. Điều kiện đủ: $m > 1$, ta phân tích m thành tích các thừa số nguyên tố $m = p_1 p_2 p_3 ... p_r$. Mỗi số nguyên tố $p_r = 2$ hoặc có dạng $4k + 1$, có thể viết dưới dạng tổng của hai bình phương. Khi đó đồng nhất thức
$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2,$$