ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**TRẦN QUANG HUY**

# THẶNG DƯ BÌNH PHƯƠNG, SỐ GIẢ NGUYÊN TỐ EULER VÀ ỨNG DỤNG

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

**THÁI NGUYÊN, NĂM 2013**

Số hoá bởi trung tâm học liệu http://www.lrc.tnu.edu.vn/

ĐẠI HỌC THÁI NGUYÊN
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**TRẦN QUANG HUY**

# THẶNG DƯ BÌNH PHƯƠNG, SỐ GIẢ NGUYÊN TỐ EULER VÀ ỨNG DỤNG

**Chuyên ngành: Phương pháp toán sơ cấp**
**Mã số : 60 46 01 13**

**LUẬN VĂN THẠC SĨ TOÁN HỌC**

**Người hướng dẫn khoa học:**
**TS. TSKH. HÀ HUY KHOÁI**

**THÁI NGUYÊN, NĂM 2013**

Số hoa bởi trung tam học lieu http://www.lrc.tnu.edu.vn/

**ĐẠI HỌC THÁI NGUYÊN**
**TRƯỜNG ĐẠI HỌC KHOA HỌC**

**Trần Quang Huy**

# THẶNG DƯ BÌNH PHƯƠNG, SỐ GIẢ NGUYÊN TỐ EULER VÀ ỨNG DỤNG

LUẬN VĂN THẠC SĨ TOÁN HỌC
Ngành: Phương pháp Toán sơ cấp
Mã số 60.46.01.13

**Người hướng dẫn: GS-TSKH HÀ HUY KHOÁI**

**Thái Nguyên - 2013**

So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

**LỜI CẢM ƠN**

Trước khi trình bày nội dung chính của luận văn, em xin bày tỏ lòng biết ơn sâu sắc tới GS-TSKH Hà Huy Khoái, người đã tận tình hướng dẫn để em có thể hoàn thành luận văn này. Em cũng xin bày tỏ lòng biết ơn chân thành tới toàn thể các thầy cô giáo trong khoa Toán - Tin học, trường Đại Học Khoa Học - Đại Học Thái Nguyên đã dạy bảo em tận tình trong suốt quá trình học tập tại trường.

*Thái Nguyên, ngày 08 tháng 07 năm 2013*

Học viên

**Trần Quang Huy**

So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

# Mục lục

**Chương 1.Thặng dư bình phương ..... 5**

**1.1.Thặng dư bình phương cho modulo số nguyên tố ..... 5**

**1.2.Thặng dư bình phương cho modulo hợp số ..... 18**

**1.3.Một vài tổng của kí hiệu Legendre ..... 23**

**1.4.Số giả nguyên tố Euler ..... 27**

**Chương 2.Ứng dụng ..... 35**



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

# LỜI MỞ ĐẦU

## 1. Lý do chọn đề tài

Có thể nói: thặng dư bình phương, kí hiệu Legendre, kí hiệu Jacobi là những kiến thức hay và khó liên quan đến lí thuyết đồng dư, đồng thời có nhiều ứng dụng trong số học. Vì thế, nó là một phần kiến thức quan trọng trong các kì thi học sinh giỏi (nhất là các kì thi chọn đội tuyển Olympic Toán). Ở nước ta việc giảng dạy các kiến thức này ở bậc THPT gặp rất nhiều khó khăn, nhất là khi giáo viên thường chưa được đào tạo chuyên sâu về phần này.

Vì vậy tôi chọn đề tài "Thặng dư bình phương và ứng dụng" để nghiên cứu.

## 2. Mục đích và nhiệm vụ nghiên cứu

Mục đích của luận văn là tìm hiểu định nghĩa thặng dư bình phương và các kí hiệu Legendre, Jacobi và số giả nguyên tố Euler.

Trong chương 1 tôi trình bày lí thuyết về thặng dư bình phương.

Trong chương 2 tôi trình bày ứng dụng và các bài tập.

## 3. Đối tượng và phạm vi nghiên cứu

Nghiên cứu thặng dư bình phương và các kí hiệu Legendre, Jacobi và số giả nguyên tố Euler dựa trên lí thuyết về đồng dư.

## 4. Phương pháp nghiên cứu

Trong luận văn này tôi thu thập các tài liệu từ nhiều nguồn khác nhau, đặc biệt dưới sự hướng dẫn của GS Hà Huy Khoái, để tôi viết lại theo ý hiểu của cá nhân tôi.

## 5. Ý nghĩa của luận văn

Bố cục của khóa luận bao gồm 2 chương:



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

- Chương 1 .Thặng dư bình phương và số giả nguyên tố Euler
- Chương 2 .Ứng dụng

Luận văn nhằm làm tài liệu tham khảo cho giáo viên và học sinh ôn luyện học sinh giỏi.

Do thời gian thực hiện luận văn không nhiều, kiến thức còn hạn chế nên khi làm luận văn không tránh khỏi những hạn chế và sai sót. Tác giả mong nhận được sự góp ý và những ý kiến phản biện của quý thầy cô và bạn đọc. Xin chân thành cảm ơn!

*Thái Nguyên, ngày 07 tháng 08 năm 2013*

Học viên

**Trần Quang Huy**



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

# Chương 1

# Thặng dư bình phương

## 1.1. Thặng dư bình phương cho modulo số nguyên tố

**Định nghĩa 1.1.1.** *Giả sử m là số nguyên dương. Số a được gọi là thặng dư bình phương của m nếu (a,m)=1 và đồng dư* $x^2 \equiv a(\mathrm{mod}\, m)$ *có nghiệm.*

*Nếu ngược lại, ta nói a là không thặng dư bình phương của m.*

Cụ thể 1, 3 là các thặng dư bình phương của 13 vì $1 = 1^2 \equiv 1(\mathrm{mod}\ 13)$; $81 = 9^2 \equiv 3(\mathrm{mod}13)$.

**Bổ đề 1.1.1.** *Giả sử p là số nguyên tố lẻ, a là số nguyên không chia hết cho p. Khi đó đồng dư sau đây không có nghiệm, hoặc có đúng hai ngiệm không đồng dư modulo p:*

$$x^2 \equiv a(\mathrm{mod}p).$$

**Chứng minh**. Giả sử $x^2 \equiv a(\mathrm{mod}p)$ có nghiệm $x = x_0$. Khi đó, dễ chứng minh rằng $x = -x_0$ là một nghiệm không đồng dư với $x_0$. Ta sẽ chỉ ra rằng, nghiệm tùy ý khác $x = x_1$ đồng dư với $x_0$ hoặc $-x_0$. Thật vậy, ta có

$x_0^2 \equiv x_1^2(\mathrm{mod}p)$, tức là $x_0^2 - x_1^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0(\mathrm{mod}p)$.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Do đó, hoặc p là ước của $(x_0 + x_1)$, hoặc p là ước của $(x_0 - x_1)$, điều phải chứng minh.

**Định lý 1.1.1.** *Nếu p là một số nguyên tố lẻ thì trong các số* $1, 2, \ldots, p-1$ *có đúng* $\frac{p-1}{2}$ *thặng dư bình phương.*

**Chứng minh.** Để tìm tất cả các thặng dư bình phương modulo p trong các số $1, 2, \ldots, p-1$, trước tiên ta bình phương các số đó và xét các thặng dư dương bé nhất modulo p của các kết quả tìm được. Các thặng dư dương bé nhất này là tất cả các thặng dư bình phương trong các số từ 1 đến p-1. Giả sử a là một thặng dư như vậy. Vì phương trình đồng dư $x^2 \equiv a(\mathrm{mod}p)$ có đúng hai nghiệm, nên trong số (p-1) bình phương đang xét, phải có hai bình phương đồng dư a: Số thặng dư bình phương đúng bằng $\frac{p-1}{2}$.

Một kí hiệu liên kết đặc biệt với thặng dư bình phương được mô tả trong định nghĩa sau:

**Định nghĩa 1.1.2.** *Cho p là một số nguyên tố lẻ và a là một số nguyên, kí hiệu Legendre* $\left[\begin{array}{c} a \\ p \end{array}\right]$ *được định nghĩa như sau:*

$$\left[\begin{array}{c} a \\ p \end{array}\right] = \begin{cases} 1 & \text{nếu } p \nmid a \text{ và } a \text{ là thặng dư bình phương của } p; \\ -1 & \text{nếu } p \nmid a \text{ và } a \text{ là không thặng dư bình phương của } p; \\ 0 & \text{nếu } p \mid a \ . \end{cases}$$

*Ví dụ.* Ta có 2 là thặng dư bình phương của 7 và 3 là không thặng dư bình phương của 7, nên $\left[\begin{array}{c} 2 \\ 7 \end{array}\right] = 1$; $\left[\begin{array}{c} 3 \\ 7 \end{array}\right] = -1$

Tiêu chuẩn sau đây thường dùng để chứng minh các tính chất của kí hiệu



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Legendre.

**Định lý 1.1.2.** *(Tiêu chuẩn Euler). Giả sử p là một số nguyên tố lẻ, và a là số nguyên dương không chia hết cho p. Khi đó*

$$\left[\begin{array}{c} a \\ \\ p \end{array}\right] \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p).$$

**Chứng minh**

Trước tiên, giả sử rằng $\left[\begin{array}{c} a \\ \\ p \end{array}\right] = 1$. Khi đó, đồng dư $x^2 \equiv a(\mathrm{mod} p)$ có nghiệm $x = x_0$. Theo định lí Fermat bé ta có

$$a^{\frac{p-1}{2}} = (x_0^2)^{\frac{p-1}{2}} = x_0^{p-1} \equiv 1(\mathrm{mod} p).$$

Chỉ còn xét trường hợp $\left[\begin{array}{c} a \\ \\ p \end{array}\right] = -1$. Khi đó, đồng dư $x^2 \equiv a(\mathrm{mod} p)$ vô nghiệm. Với mỗi i sao cho $1 \leq i \leq p-1$, tồn tại duy nhất j, $1 \leq j \leq p-1$ để ij $\equiv a(\mathrm{mod} p)$. Rõ ràng $i \neq j$, nên ta có thể nhóm các số $1, \ldots, p-1$ thành $\frac{p-1}{2}$ từng cặp với tích từng cặp đồng dư a modulo p. Nhân các cặp này với nhau ta được

$$(p-1)! \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p).$$

Theo định lí Wilson ta có

$$-1 \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

Định lí được chứng minh.

Những tính chất sau đây cho phép tính được dễ ràng kí hiệu Legendre.

**Định lý 1.1.3.** *Giả sử p là một số nguyên tố lẻ, a và b là các số nguyên không chia hết cho p. Khi đó:*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

*(i) Nếu* $a \equiv b(\mathrm{mod}p)$ *thì* $\left[\begin{array}{c} a \\ p \end{array}\right] = \left[\begin{array}{c} b \\ p \end{array}\right]$

*(ii)* $\left[\begin{array}{c} a \\ p \end{array}\right]\left[\begin{array}{c} b \\ p \end{array}\right] = \left[\begin{array}{c} ab \\ p \end{array}\right]$

*(iii)* $\left[\begin{array}{c} a^2 \\ p \end{array}\right] = 1.$

**Chứng minh**.

(i). Nếu $a \equiv b(\mathrm{mod}p)$ thì $x^2 \equiv a(\mathrm{mod}p)$ có nghiệm khi và chỉ khi $x^2 \equiv b(\mathrm{mod}p)$ có nghiệm. Do đó $\left[\begin{array}{c} a \\ p \end{array}\right] = \left[\begin{array}{c} b \\ p \end{array}\right]$.

(ii). Theo tiêu chuẩn Euler ta có:

$$\left[\begin{array}{c} a \\ p \end{array}\right] \equiv a^{\frac{p-1}{2}}(\mathrm{mod}p),\ \left[\begin{array}{c} b \\ p \end{array}\right] \equiv b^{\frac{p-1}{2}}(\mathrm{mod}p),\ \left[\begin{array}{c} ab \\ p \end{array}\right] \equiv ab^{\frac{p-1}{2}}(\mathrm{mod}p)$$

Như vậy,

$$\left[\begin{array}{c} a \\ p \end{array}\right]\left[\begin{array}{c} b \\ p \end{array}\right] \equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left[\begin{array}{c} ab \\ p \end{array}\right](\mathrm{mod}p)$$

Vì vậy giá trị của kí hiệu Legendre chỉ có thể là $\pm 1$ nên ta có đẳng thức cần chứng minh.

(iii). Vì $\left[\begin{array}{c} a \\ p \end{array}\right] = \pm 1$, nên từ phần trên ta có

$$\left[\begin{array}{c} a^2 \\ p \end{array}\right] = \left[\begin{array}{c} a \\ p \end{array}\right]\left[\begin{array}{c} a \\ p \end{array}\right] = 1$$

Định lí trên cho thấy rằng tích của hai thặng dư bình phương hoặc hai không thặng dư bình phương là một thặng dư bình phương, tích của một



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

thặng dư bình phương và một không thặng dư bình phương là một không thặng dư bình phương.

Tiêu chuẩn Euler cho biết khi nào thì các số nguyên tố lẻ nhận -1 là thặng dư bình phương.

**Ví dụ**: Chứng minh rằng tồn tại số tự nhiên a, với $a < \sqrt{p} + 1$ mà a là không thặng dư bình phương modulo p.

**Chứng minh**

Gọi a là số tự nhiên nhỏ nhất là không thặng dư bình phương modulo p

Đặt $b = \left[\frac{p}{a}\right] + 1 \Rightarrow 0 < ab - p < a$, do đó ab-p là thặng dư bình phương modulo p. Vậy

$$1 = \left[\begin{array}{c} ab-p \\ \\ p \end{array}\right] = \left[\begin{array}{c} ab \\ \\ p \end{array}\right] = \left[\begin{array}{c} a \\ \\ p \end{array}\right]\left[\begin{array}{c} b \\ \\ p \end{array}\right] = -\left[\begin{array}{c} b \\ \\ p \end{array}\right]$$

Suy ra b là không thặng dư bình phương modulo p.

Vậy $a \leq b < \frac{p}{a} + 1 \Rightarrow a < \sqrt{p} + 1$

**Định lý 1.1.4.** *Nếu p là số nguyên tố lẻ thì*

$$\left[\begin{array}{c} -1 \\ \\ p \end{array}\right] = \begin{cases} 1 & khi\ p \equiv 1(\mathrm{mod}4), \\ -1 & khi\ p \equiv -1(\mathrm{mod}4) \end{cases}$$

**Chứng minh.** Theo tiêu chuẩn Euler ta có:

$$\left[\begin{array}{c} -1 \\ \\ p \end{array}\right] \equiv (-1)^{\frac{p-1}{2}}(\mathrm{mod}p)$$

Nếu $p \equiv 1(\mathrm{mod}4)$ thì p=4k+1 với k là số nguyên nào đó. Như vậy,

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

tức là $\left[\begin{array}{c} -1 \\ \\ p \end{array}\right] = 1.$

Nếu $p \equiv -1(\mathrm{mod}4)$ thì p=4k+3 với k là số nguyên nào đó. Như vậy,

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1$$

tức là $\left[\begin{array}{c} -1 \\ \\ p \end{array}\right] = -1$. Từ hai điều trên, ta có điều phải chứng minh.

**Ví dụ**

Giả sử p là số nguyên tố có dạng 4k+1. Chứng minh rằng, với $p' = \frac{p-1}{2}$ khi đó $x = (p')!$ là một nghiệm của phương trình đồng dư $x^2+1 \equiv 0(\mathrm{mod}\, p)$.

**Chứng minh.** Với mỗi $i = 1, 2, ..., p'$ ta có: $i \equiv -(p-i)(\mathrm{mod}p)$

Cho i chạy từ 1 đến $p'$ và nhân lại với nhau ta được:

$$(p')! \equiv (-1)^{p'}(p-1)...(p-p')(\mathrm{mod}p)$$

hay $(p')! \equiv (-1)^{p'}(p'+1)...(p-2)(p-1)(\mathrm{mod}p)$.

Khi đó ta có $x^2 = (p')!^2 \equiv (-1)^{p'}(p-1)!(\mathrm{mod}p)$

Vì p=4k+1 nên $p' = 2k$ là số chẵn, suy ra $(p')!^2 \equiv (p-1)! \equiv -1(\mathrm{mod}\, p)$ (theo định lí Wilson). Đó là điều cần chứng minh.

*Nhận xét*

Người ta có thể kết luận từ ví dụ trên rằng, mọi thừa số nguyên tố của số $x^2+y^2$ (trong đó x,y là các số tự nhiên và nguyên tố cùng nhau) hoặc có dạng 4k+1, hoặc bằng 2. Kết luận này có thể được khái quát hóa theo định lí sau.

**Định lý 1.1.5.** *Cho x, y là các số nguyên tố cùng nhau và a, b, c là các số nguyên. Nếu p là một ước nguyên tố của số $ax^2+bxy+cy^2$, p không là ước của abc, thì:*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$D = b^2 - 4ac$$

*là một thặng dư bình phương modulo p.*

*Đặc biệt, nếu p là ước của $x^2 - Dy^2$ và (x,y)=1, thì D là một thặng dư bình phương modulo p.*

**Chứng minh**

Đặt $N = ax^2 + bxy + cy^2$.Từ $4aN = (2ax + by)^2 - Dy^2$, ta có

$$(2ax + by)^2 \equiv Dy^2 (\mathrm{mod} p).$$

Hơn nữa y không chia hết cho p; nếu không thì p chia hết cho 2ax+by và x, điều này trái với giả thiết.

Vậy (y,p)=1 nên tồn tại $y'$ sao cho $yy' \equiv 1 (mod p)$.

Suy ra $(2axy' + byy')^2 \equiv D(yy')^2 \equiv D(mod p)$. Vậy D là thặng dư bình phương modulo p.

Cho a là một số nguyên, p là một số nguyên tố sao cho (a,p)=1. Với mỗi $k = 1, 2, ..., p'$ tồn tại $r_k \in \{\pm 1, \pm 2, ..., \pm p'\}$ sao cho $ka \equiv r_k (mod p)$, dễ thấy không tồn tại hai $r_k$ có cùng giá trị tuyệt đối, do đó $|r_1|, |r_2|, ..., |r_{p'}|$ là một hoán vị của tập hợp $\{1, 2, ..., p'\}$.

Cho k chạy rừ 1 đến $p'$ rồi nhân các vế với nhau ta được:

$$a^{p'} \equiv \frac{r_1 ... r_{p'}}{1.2...p'} = \frac{r_1 ... r_{p'}}{|r_1| ... \left|r_{p'}\right|} (\mathrm{mod} p)$$

Đặt $\varepsilon_k = \frac{r_k}{|r_k|}$; $\varepsilon_k = \pm 1$ ta có $a^{p'} \equiv \varepsilon_1 ... \varepsilon_{p'} (\mathrm{mod} p)$

Ta có $\varepsilon_k = -1$ khi và chỉ khi phần dư khi chia ka cho p lớn hơn $p'$, khi đó $\frac{2ka}{p} = 2p + \frac{2r}{p} \Leftrightarrow \left[\frac{2ka}{p}\right] = 2\left[\frac{ka}{p}\right] + 1$ suy ra $r_k = (-1)^{\left[\frac{2ka}{p}\right]}$.

Vậy

$$a^{p'} \equiv (-1)^{\sum\limits_{k=1}^{p'} \left[\frac{2ka}{p}\right]}$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

**Định lý 1.1.6.** *(Bổ đề Gauss) Giả sử p là số nguyên tố lẻ và (a,p)=1. Nếu s là số các thặng dư dương bé nhất của các số nguyên* $a, 2a, ..., \frac{p-1}{2}a$ *lớn hơn* $\frac{p}{2}$*, thì* $\left[\begin{array}{c} a \\ \\ p \end{array}\right] = (-1)^s$.

**Chứng minh**. Trong số các thặng dư dương bé nhất của các số nguyên $a, 2a, ..., \frac{p-1}{2}a$, giả sử $u_1, u_2, ..., u_s$ là các thặng dư lớn hơn $\frac{p}{2}$, và $v_1, v_2, ..., v_t$ là các thặng dư nhỏ hơn $\frac{p}{2}$.

Vì (ja,p)=1 với mọi j, $1 \leq j \leq \frac{p-2}{2}$, nên tất cả các thặng dư dương bé nhất nói trên đều nằm trong tập $\{1, 2, ..., p-1\}$.

Ta sẽ chứng tỏ rằng, $p-u_1, p-u_2, ..., p-u_s, v_1, v_2, ..., v_t$ chính là tập hợp các số $1, 2, ..., \frac{p-1}{2}$ xếp theo thứ tự nào đó. Có tất cả $\frac{p-1}{2}$ không vượt quá $\frac{p-1}{2}$, nên chỉ còn chứng minh rằng không có hai số nào đồng dư với nhau.

Rõ ràng không có hai số $u_i$ nào, cũng như không có hai số $v_j$ nào đồng dư với nhau modulo p. Thật vậy, nếu ngược lại, ta sẽ có đồng dư $ma \equiv na(\mathrm{mod}p)$ với m, n là số dương nào đó không vượt quá $\frac{p-1}{2}$. Vì (a,p)=1 nên từ đó suy ra $m \equiv n(\mathrm{mod}p)$. Điều này mâu thuẫn.

Tương tự như trên, ta có thể thấy rằng không có $p-u_i$ nào có đồng dư với $v_j$. Vậy ta có

$$(p-u_1)(p-u_2)...(p-u_s)v_1...v_t \equiv \left(\tfrac{p-1}{2}\right)!(\mathrm{mod}p).$$

Từ đó suy ra

$$(-1)^s u_1u_2...u_sv_1v_2...v_t \equiv \left(\tfrac{p-1}{2}\right)!(\mathrm{mod}p).$$

Mặt khác, vì $u_1, u_2, ..., u_s, v_1, v_2, ..., v_t$ là các thặng dư dương bé nhất của $a, 2a, ..., \frac{p-1}{2}a$ nên



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$u_1u_2...u_sv_1v_2...v_t \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!(\mathrm{mod}p).$$

Như vậy ta có

$$(-1)^s a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(\mathrm{mod}p).$$

Vì $\left(p, (\frac{p-1}{2})!\right) = 1$ nên suy ra

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}p)$$

tức là

$$a^{\frac{p-1}{2}} \equiv (-1)^s(\mathrm{mod}p).$$

Định lí suy ra từ tiêu chuẩn Euler.

Bổ đề Gauss gúp cho việc tính toán giá trị của kí hiệu Legendre cho số nhỏ a hoặc số nhỏ p. Chẳng hạn như, a=2, ta có $\left[\begin{array}{c} 2 \\ p \end{array}\right] = (-1)^S$ , với $S = \sum_{k=1}^{p'} \left[\frac{4k}{p}\right]$. Chính xác $\left[\frac{1}{2}p'\right]$ số hạng trong tổng trên có giá trị bằng 0, một nửa còn lại $p' - \left[\frac{1}{2}p'\right]$ số hạng có giá trị bằng 1. Vì thế $S = p' - \left[\frac{1}{2}p'\right] = \left[\frac{p+1}{4}\right]$, là số chẵn khi $p \equiv \pm 1$ và là số lẻ khi $p \equiv \pm 3(\mathrm{mod}8)$. Ta có chứng minh sẽ được đề cập đến sau đây.

**Định lý 1.1.7.** . *Nếu p là một số nguyên tố lẻ thì*

$$\left[\begin{array}{c} 2 \\ p \end{array}\right] = (-1)^{\frac{p^2-1}{8}}$$

*Như vậy 2 là thặng dư bình phương modulo số nguyên tố p lớn hơn 2 dạng* $p \equiv \pm 1(\mathrm{mod}8)$ *và là không thặng dư bình phương modulo số nguyên tố p lớn hơn 2 dạng* $p \equiv \pm 3(\mathrm{mod}8)$

**Chứng minh**. Áp dụng tiêu chuẩn Gauss, ta cần tính số thặng dư dương bé nhất lớn hơn $\frac{p}{2}$ của dãy số



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$1.2, 2.2, ..., \tfrac{p-1}{2}2.$$

Vì các số đều nhỏ hơn p nên các thặng dư dương bé nhất của mỗi số trùng với nó. Như vậy, ta cần tính số các số của dãy lớn hơn $\frac{p}{2}$. Số các số đó là

$$s = \tfrac{p-1}{2} - \left[\tfrac{p}{4}\right].$$

Như vậy ta có

$$\left[\begin{array}{c} 2 \\ p \end{array}\right] = (-1)^{\frac{p-1}{2}-\left[\frac{p}{4}\right]}.$$

Dễ kiểm tra đồng dư thức sau đay bằng cách phân ra các trường hợp $p \equiv 1, 3, 5, 7(\text{mod}8)$

$$\tfrac{p-1}{2} - \left[\tfrac{p}{4}\right] \equiv \tfrac{p^2-1}{8}(\text{mod}2).$$

Từ đó ta có

$$\left[\begin{array}{c} 2 \\ p \end{array}\right] = (-1)^{\frac{p^2-1}{8}}(\text{mod}2).$$

Bằng cách tính lớp đồng dư của $\frac{p^2-1}{8}(\text{mod}2)$ ta suy ra

$$\left[\begin{array}{c} 2 \\ p \end{array}\right] = 1, \text{ nếu p} \equiv \pm 1(\text{mod}8)$$

và

$$\left[\begin{array}{c} 2 \\ p \end{array}\right] = -1, \text{ nếu p} \equiv \pm 3(\text{mod}8)$$

**Định lý 1.1.8.** *Cho p là số nguyên tố, ta có các kết quả sau:*

- *-2 là thặng dư bình phương modulo p khi và chỉ khi* $p \equiv 1(\text{mod}8)$ *hoặc* $p \equiv 3(\text{mod}8)$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

- *-3 là thặng dư bình phương modulo p khi và chỉ khi* $p \equiv 1(\mathrm{mod}6)$
- *3 là thặng dư bình phương modulo p khi và chỉ khi* $p \equiv \pm 1(\mathrm{mod}12)$
- *5 là thặng dư bình phương modulo p khi và chỉ khi* $p \equiv \pm 1(\mathrm{mod}10)$

**Ví dụ 1:** Chứng minh rằng có vô số số nguyên tố dạng

a. 4k+1

b. 10k+9

**Chứng minh**

a. Giả sử có hữu hạn số nguyên tố dạng 4k+1, ta gọi tất cả các số đó là $p_1, p_2, ..., p_n$. Đặt $N = (2p_1...p_n)^2 + 1$ và có dạng 4k+1 Nếu N là số nguyên tố thì mâu thuẫn; nếu N là hợp số thì N có ước p do đó p có dạng 4k+1. Dễ thấy p khác $p_i$ trái với giả thiết.

b. Tương tự ta đặt $N = 5(2p_1...p_n)^2 - 1$.

**Ví dụ 2** Chứng minh rằng mọi ước nguyên tố của $n^4 - n^2 + 1$ có dạng 12k+1

**Chứng minh**

Giả sử p là một ước nguyên tố của $n^4 - n^2 + 1$.

Ta có $n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2 = (n^2 + 1)^2 - 3n^2$ và $(n^2 + 1, n) = 1$; $(n^2 11, n) = 1$

Theo định lí 4, 5 và 8 thì $\begin{cases} \left[\dfrac{3}{p}\right] = 1 \\ \left[\dfrac{-1}{p}\right] = 1 \end{cases} \Leftrightarrow \begin{cases} p \equiv \pm 1(\mathrm{mod}12) \\ p \equiv 1(\mathrm{mod}4) \end{cases} \Rightarrow$

$p \equiv 1(\mathrm{mod}12)$

**Ví dụ 3** Tính tổng:



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$A = \left[\frac{1}{2013}\right] + \left[\frac{2}{2013}\right] + \left[\frac{2^2}{2013}\right] + .... + \left[\frac{2^{2001}}{2013}\right]$

**Chứng minh**

Vì 2003 là số nguyên tố, do đó theo tiêu chuẩn Euler và định lí 8 thì $2^{1001} \equiv -1(\text{mod}2003)$

Suy ra $2^{1001} + 1 \vdots 2013 \Rightarrow 2^{1001+i} + 2^i \vdots 2003 \Rightarrow \frac{2^{1001+i}}{2003} + \frac{2^i}{2003}$ là số nguyên

Cho i=0,1,...,1000 ta có $\frac{1+2+2^2+...+2^{2001}}{2003} - 1001 = \frac{2^{2002}-1}{2003} - 1001$

**Định lý 1.1.9.** *(Luật tương hỗ Gauss)*

$$\left[\begin{array}{c} p \\ q \end{array}\right] \left[\begin{array}{c} q \\ p \end{array}\right] = (-1)^{p'q'} \text{ Với } p' = \frac{p-1}{2};\ q' = \frac{q-1}{2}$$

**Chứng minh**

Đặt $S(p,q) = \sum_{k=1}^{q'} \left[\frac{kp}{q}\right]$ Ta chứng minh $S(p,q) + S(q,p) = p'q'$.

Với mỗi k : $0 < k < p'$ thì $\left[\frac{kp}{q}\right]$ chính là số điểm nguyên (k;1) trong mặt pẳng tọa độ Okl với k, l thỏa mãn $0 < 1 < \frac{kp}{q}$, vậy tổng S(p,q) chính là số điểm nguyên thuộc miền trong hình chữ nhật OBCD nằm phía dưới đường OE với O(0;0),B(p';0),C(0;q'),D(p';q'),E(p;q).

Tương tự S(p,q) chính là số điểm nguyên thuộc miền trong của hình chữ nhật OBCD nằm phía trên đường OE. Vậy $S(p,q) + S(q,p) = p'q'$.

Trong lập luận trên ta được $S(p+q,p) - S(p,q) = 1+2+...+p' = \frac{p^2-1}{8}$.

Theo định lí 7 $\left[\begin{array}{c} 2 \\ p \end{array}\right] = (-1)^{\frac{p^2-1}{8}}$, Bổ đề Gauss cho ta.

$$\left[\begin{array}{c} 2 \\ q \end{array}\right] \left[\begin{array}{c} p \\ q \end{array}\right] = \left[\begin{array}{c} 2p \\ q \end{array}\right] = \left[\begin{array}{c} 2(p+q) \\ q \end{array}\right] = \left[\begin{array}{c} \frac{p+q}{2} \\ q \end{array}\right] = (-1)^{S(p+q,q)} =$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\left[\begin{array}{c}2\\p\end{array}\right](-1)^{S(p,q)}$$

Suy ra $\left[\begin{array}{c}p\\q\end{array}\right] = (-1)^{S(p,q)}$, Tương tự $\left[\begin{array}{c}q\\p\end{array}\right] = (-1)^{S(q,p)}$. Nhân hai vế của hai nhị thức trên ta được điều phải chứng minh.

Luật tương hỗ giúp tính các kí hiệu Legendre cho số lớn bằng cách chuyển về số nhỏ nhờ $\left[\begin{array}{c}b+a\\p\end{array}\right] = \left[\begin{array}{c}a\\p\end{array}\right]$

**Ví dụ 1**

Tính $\left[\begin{array}{c}814\\2003\end{array}\right]$. Ta có 814=2.11.37

Vậy $\left[\begin{array}{c}814\\2003\end{array}\right] = \left[\begin{array}{c}2\\2003\end{array}\right]\left[\begin{array}{c}11\\2003\end{array}\right]\left[\begin{array}{c}37\\2003\end{array}\right]$

Tong đó $\left[\begin{array}{c}2\\2003\end{array}\right] = -1$

$$\left[\begin{array}{c}11\\2003\end{array}\right] = -\left[\begin{array}{c}2003\\11\end{array}\right] = -\left[\begin{array}{c}1\\11\end{array}\right] = -1$$

$$\left[\begin{array}{c}37\\2003\end{array}\right] = \left[\begin{array}{c}2003\\37\end{array}\right] = \left[\begin{array}{c}5\\37\end{array}\right] = \left[\begin{array}{c}37\\5\end{array}\right] = \left[\begin{array}{c}2\\5\end{array}\right] = \left[\begin{array}{c}1\\2\end{array}\right] = 1$$

Vậy $\left[\begin{array}{c}814\\2003\end{array}\right] = 1$. Nghĩa là 814 là thặng dư bình phương của 2003.

**Ví dụ 2**. Chứng minh rằng số nguyên a là thặng dư bình phương của mọi số nguyên tố khi và chỉ khi a là số chính phương.

**Chứng minh**

Giả sử a không là số chính phương. Chúng ta có thể giả thiết mà không



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

mất tính tổng quát rằng a là số không có ước chính phương. Giả sử $a > 0$, thì $a = p_1 p_2 ... p_k$ Với $p_i$ là các số nguyên tố. Cho mỗi số nguyên tố p khi đó ta có:

$$\left[\begin{array}{c} a \\ p \end{array}\right] = \prod_{i=1}^{k} \left[\begin{array}{c} p_i \\ p \end{array}\right] \text{ và } \left[\begin{array}{c} p_i \\ p \end{array}\right] = (-1)^{p_i' p'} \left[\begin{array}{c} p \\ p_i \end{array}\right].$$

Nếu $a = 2$, chỉ cần chọn $p = 5$. Nếu không thì a có một ước lẻ, chẳng hạn là $p_k$. Chúng ta chọn một số nguyên tố p sao cho $p \equiv 1(mo\mathrm{d}8)$, $p \equiv 1(mo\mathrm{d}p_i)$ với $i = 1, 2, ..., k-1$, và $p \equiv a(mo\mathrm{d}p_k)$, trong đó a là một số không thặng dư bình phương tùy ý modulo $p_k$. Như vậy số p tồn tại theo định lí Dirichlet về số nguyên tố trong cấp số cộng. Khi đó $p_1, ..., p_k - 1$ là những thặng dư bình phương modulo p, nhưng $p_k$ thì không phải. Do đó a là không thặng dư bình phương modulo p.

Trong trường hợp $a < 0$ được chứng minh tương tự.

## 1.2. Thặng dư bình phương cho modulo hợp số

Trong phần này chúng ta nghiên cứu kí hiệu Jacobi, nó là sự mở rộng của kí hiệu Legendre, dùng để đánh giá kí hiệu Legendre và định nghĩa số giả nguyên tố Euler.

**Định nghĩa 1.2.1.** *Cho a là một số nguyên và b là số nguyên dương lẻ, b có phân tích tiêu chuẩn* $p = {p_1}^{\alpha_1} {p_2}^{\alpha_2} .... {p_r}^{\alpha_r}$. *Kí hiệu Jacobi được định nghĩa như sau:*

$$\left[\begin{array}{c} a \\ b \end{array}\right] = \left[\begin{array}{c} a \\ p_1 \end{array}\right]^{\alpha_1} \left[\begin{array}{c} a \\ p_2 \end{array}\right]^{\alpha_2} ... \left[\begin{array}{c} a \\ p_r \end{array}\right]^{\alpha_r}$$

*trong đó vế phải là kí hiệu Legendre.*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Trong trường hợp b là số nguyên tố thì kí hiệu Jacobi trùng với kí hiệu Legendre. Tuy nhiên khác với kí hiệu Legendre, khi b là hợp số, kí hiệu Jacobi không cho biết phương trình đồng dư $x^2 \equiv a(mo\text{dp})$ có nghiệm hay không. Mặc dù vậy, kí hiệu Jacobi có nhiều tính chất tương tự như kí hiệu Legendre.

Dễ thấy rằng $\left[\begin{array}{c} a \\ b \end{array}\right] = -1$ không thể chỉ ra rằng a là không thặng dư bình phương modulo b. Thật vậy, nếu $\left[\begin{array}{c} a \\ b \end{array}\right] = -1$ thì từ định nghĩa $\left[\begin{array}{c} a \\ p_i \end{array}\right] = -1$ thì ít nhất $p_i$ là ước của b; hơn nũa a là không thặng dư bình phương modulo $p_i$. Tuy vậy điều ngược lại thì không đúng, ta xét ví dụ sau:

**Ví dụ 1**

$$\left[\begin{array}{c} 2 \\ 15 \end{array}\right] = \left[\begin{array}{c} 2 \\ 3 \end{array}\right]\left[\begin{array}{c} 2 \\ 5 \end{array}\right] = (-1)(-1) = 1$$

2 là không thặng dư bình phương modulo 15, cũng là không thặng dư bình phương modulo 3 và 5.

Tóm lại, ta chưa thể kết luận được nếu p không là số nguyên tố.

**Định lý 1.2.1.** *Cho a là số nguyên và b là số nguyên dương, và b có phân tích ra thừa số nguyên tố* $p = {p_1}^{\alpha_1}{p_2}^{\alpha_2}....{p_r}^{\alpha_r}$. *thì a là thặng dư bình phương modulo b nếu và chỉ nếu a là thặng dư bình phương modulo* $p^{\alpha_i}$ *với mỗi i=1,2,...,r.*

**Chứng minh**



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Nếu a là thặng dư bình phương modulo b, thì hiển nhiên nó là thặng dư bình phương modulo với mỗi $p^{\alpha_i}$; i=1,2,...,r. Khi đó tồn tại $x_i$ là số nguyên sao cho $x_i^2 \equiv a(\mathrm{mod} p^{\alpha_i})$. Theo định lí "Trung Hoa về đồng dư" thì có số x sao cho $x \equiv x_i(\mathrm{mod} p^{\alpha_i})$. Thì $x^2 \equiv x_i^2 \equiv a(\mathrm{mod} p^{\alpha_i})$ chứng tỏ $x \equiv a(\mathrm{mod} b)$.

**Định lý 1.2.2.** *Số thặng dư bình phương modulo $p^n(n > 0)$. Được tính bởi công thức:*

$$\left[\frac{2^{n-1}-1}{3}\right] + 2 \text{ với } p=2, \text{ và } \left[\frac{p^{n+1}-1}{2(p+1)}\right] + 1 \text{ với } p>2.$$

**Chứng minh**

Cho $k_n$ là số thặng dư bình phương modulo $p^n(n > 0)$. Cho p là số lẻ và $n \geq 2$. Số a là một thặng dư bình phương modulo $p^n$ nếu và chỉ nếu p không là ước của a và a là một thặng dư bình phương modulo p, hoặc $p^2$ là ước của a và $\frac{a}{p^2}$ là một thặng dư bình phương modulo $p^{n-2}$. Điều đó chỉ ra rằng $k_n = k_{n-2} + p'p^{n-1}$.

Cho p=2 và $n \geq 3$. Số a là một thặng dư bình phương modulo $2^n$ nếu và chỉ nếu một trong hai khả năng sau xảy ra $a \equiv 1(\mathrm{mod} 8)$ hoặc 4 là ước của a và $\frac{a}{4}$ là thặng dư bình phương modulo $2^{n-2}$. Ta được $k_n = k_{n-2} + 2^{n-3}$.

Bay giờ sự trình bày là phương pháp quy nạp đơn giản với n.

**Định lý 1.2.3.** *Cho tất cả các số nguyên a, b và các số lẻ c, d. Ta có:*

$$\left[\begin{array}{c} a+bc \\ c \end{array}\right] = \left[\begin{array}{c} a \\ c \end{array}\right], \left[\begin{array}{c} ab \\ c \end{array}\right] = \left[\begin{array}{c} a \\ c \end{array}\right]\left[\begin{array}{c} b \\ c \end{array}\right], \left[\begin{array}{c} a \\ cd \end{array}\right] = \left[\begin{array}{c} a \\ c \end{array}\right]\left[\begin{array}{c} a \\ d \end{array}\right]$$

**Định lý 1.2.4.** *Cho mỗi số nguyên lẻ a. Ta có:*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\left[\begin{array}{c} -1 \\ a \end{array}\right] = (-1)^{\frac{a-1}{2}}, \left[\begin{array}{c} 2 \\ a \end{array}\right] = (-1)^{\left[\frac{a+1}{4}\right]}.$$

**Định lý 1.2.5.** $\left[\begin{array}{c} a \\ b \end{array}\right]\left[\begin{array}{c} b \\ a \end{array}\right] = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$

**Ví dụ 2**. Chứng minh rằng phương trình $x^2 = y^3 - 3$ không có nghiệm nguyên (x,y).

**Chứng minh**

Với mỗi y chẵn ta có $x^2 = y^3 - 3 \equiv 3(\text{mod}8)$, điều đó không thể xẩy ra.

Bây giờ cho y là số lẻ. Nếu $y \equiv 3(\text{mod}4)$, thì $x^2 = y^3 - 3 \equiv 3^3 - 5 \equiv 2(\text{mod}4)$ cũng không xẩy ra.

Vậy y phải có dạng 4z+1, z là số nguyên. Ta có:

$x^2 + 4 = 64z^3 + 48z^2 + 12z = 4z(16z^2 + 12z + 3)$. Điều đó chỉ ra rằng $x^2 \equiv 4(\text{mod}16z^2 + 12z + 3)$.

Hơn nữa theo kí hiệu Jacobi thì $\left[\begin{array}{c} -4 \\ 16z^2 + 12z + 3 \end{array}\right] = \left[\begin{array}{c} -1 \\ 16z^2 + 12z + 3 \end{array}\right]$ nhận giá tri bằng -1 vì $16z^2 + 12z + 3 \equiv 3(\text{mod}4)$.

**Ví dụ 3**

Chứng minh rằng 4kxy-1 không chia hết cho $x^m + y^n$ với x,y,k,m,n là số nguyên dương.

**Chứng minh**

Để ý rằng $(x^m, y^n, 4kxy - 1) = 1$. Ta đặt $m' = \left[\frac{m}{2}\right]$, $n' = \left[\frac{n}{2}\right]$. Chúng ta cần kiểm tra ba khả năng sau.

$1^o$) m=2m' và n=2n' thì 4kxy-1 là ước của $(x^{m'})^2 + (y^{n'})^2$. Theo định



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

lí 5 phần 1 thì $\left[\begin{array}{c} -1 \\ 4kxy-1 \end{array}\right] = 1$, điều này không đúng.

$2^o$) m=2m' và n=2n'+1 (cũng như n=2n' và m=2m'+1 ). Thì 4kxy-1 là ước của $(x^{m'})^2 + y(y^{n'})^2$ hơn nữa $\left[\begin{array}{c} -y \\ 4kxy-1 \end{array}\right] = 1$. Điều chúng ta cần là nó không xẩy ra.

Chứng minh khi y là số lẻ. Theo định lí trên ta có:

$$\left[\begin{array}{c} -y \\ 4kxy-1 \end{array}\right] = \left[\begin{array}{c} -1 \\ 4kxy-1 \end{array}\right]\left[\begin{array}{c} y \\ 4kxy-1 \end{array}\right] =$$

$$(-1)(-1)^{\frac{y-1}{2}}\left[\begin{array}{c} -1 \\ y \end{array}\right] = -1$$

Bây giờ đặt $y = 2^t y_1$, với $t \geq 1$ là một số nguyên và $y_1$ là số tự nhiên. Theo định lí 4 phần 2, ta có $\left[\begin{array}{c} 2 \\ 4kxy-1 \end{array}\right] = 1$ , ngược lại y là số lẻ, $\left[\begin{array}{c} -y_1 \\ 4kxy-1 \end{array}\right] = \left[\begin{array}{c} -y_1 \\ 4.2^t kxy_1-1 \end{array}\right] = -1$. Nó có nghĩa là:

$$\left[\begin{array}{c} -y \\ 4kxy-1 \end{array}\right] = \left[\begin{array}{c} 2 \\ 4kxy-1 \end{array}\right]^t \left[\begin{array}{c} -y_1 \\ 4kxy-1 \end{array}\right] = -1.$$

$3^o$) m=2m'+1 và n=2n'+1. Thì 4kxy-1 là ước của $x(x^{m'})^2 + y(y^{n'})^2$, và từ $\left[\begin{array}{c} -y_1 \\ 4kxy-1 \end{array}\right] = \left[\begin{array}{c} -y_1 \\ 4.2^t kxy_1-1 \end{array}\right] = 1$. Bên cạnh đó,

$$\left[\begin{array}{c} -xy \\ 4kxy-1 \end{array}\right] = \left[\begin{array}{c} -4xy \\ 4kxy-1 \end{array}\right] = \left[\begin{array}{c} -1 \\ 4kxy-1 \end{array}\right] = -1,$$ vô lí. Vậy vấn đề được chứng minh.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

## 1.3. Một vài tổng của kí hiệu Legendre

Việc tìm số nghiệm của một đồng dư thường quy về đếm các giá trị $x \in \{0, 1, ..., p-1\}$ sao cho đa thức đã cho $f(x)$ với hệ số nguyên nào đó là thặng dư bình phương modulo một số nguyên tố lẻ p. Câu trả lời hiển nhiên là có liên hệ với giá trị của tổng $\sum_{x=0}^{p-1} \left[ \begin{array}{c} f(x) \\ p \end{array} \right]$.
Trong phần này chúng ta quan tâm đến những tổng thuộc loại này.

Đối với một đa thức tuyến tính f, tổng đang xét rất dễ đánh giá.

**Định lý 1.3.1.** *Với các số nguyên a,b tùy ý và số nguyên tố p không là ước của a,*

$$\sum_{x=0}^{p-1} \left[ \begin{array}{c} \mathrm{ax} + b \\ p \end{array} \right] = 0$$

**Chứng minh**

Do p không là ước của a, các số ax+b, $x = 0, 1, ..., p-1$ lập nên hệ thặng dư đầy đủ modulo p. Có đúng $\frac{p-1}{2}$ là thặng dư bình phương, $\frac{p-1}{2}$ là không thặng dư bình phương, và một trong số đó chia hết cho p. Nghĩa là:

$$\sum_{x=0}^{p-1} \left[ \begin{array}{c} \mathrm{ax} + b \\ p \end{array} \right] = \tfrac{p-1}{2}.1 + \tfrac{p-1}{2}.(-1) + 0 = 0.$$

Để đánh giá tổng của các đa thức bậc hai, chúng ta cần sử dụng định lí sau:

**Định lý 1.3.2.** *Giả sử* $f(x)^{p'} = a_0 + a_1 x + ... + a_{kp'} x^{kp'}$, *với k là bậc của đa thức f. Ta có:*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\sum_{x=0}^{p-1}\left[\begin{array}{c} f(x) \\ p \end{array}\right] \equiv -(a_{p-1} + a_{2(p-1)} + ... + a_{k'(p-1)})(\mathrm{mod}p).$$

**Chứng minh**

Định nghĩa $S_n = \sum_{x=0}^{p-1} x^n$ với n là số tự nhiên và $S_0 = p$. Ta chỉ ra rằng $S_n \equiv -1(\mathrm{mod}p)$, cho n>0 và p-1 là ước của n và $S_n \equiv 0(\mathrm{mod}p)$ nếu ngược lại. Theo tiêu chuẩn Euler ta có:

$$\sum_{x=0}^{p-1}\left[\begin{array}{c} f(x) \\ p \end{array}\right] \equiv \sum_{x=0}^{p-1} f(x)^{p'} = \sum_{i=0}^{kp'} a_i S_i \equiv -(a_{p-1} + ... + a_{k'(p-1)})(\mathrm{mod}p)$$

**Định lý 1.3.3.** *Đối với các số a,b,c và số nguyên tố p không là ước của a, tổng*

$$\sum_{x=0}^{p-1}\left[\begin{array}{c} ax^2 + bx + c \\ p \end{array}\right]$$

*nhận giá trị bằng* $-\left[\begin{array}{c} a \\ p \end{array}\right]$ *nếu p không là ước của* $b^2 - 4ac$,

*bằng* $(p-1)\left[\begin{array}{c} a \\ p \end{array}\right]$ *nếu p là ước của* $b^2 - 4ac$.

**Chứng minh**

Ta có

$$\left[\begin{array}{c} 4a \\ p \end{array}\right] \sum_{x=0}^{p-1}\left[\begin{array}{c} ax^2 + bx + c \\ p \end{array}\right] = \sum_{x=0}^{p-1}\left[\begin{array}{c} (2ax + b) - D \\ p \end{array}\right] \text{ với}$$

$$D = b^2 = 4ac.$$

Vì các số ax+b, x=0,1,...,p-1, làm thành hệ thặng dư đầy đủ modulo p, ta có

$$\left[\begin{array}{c} a \\ p \end{array}\right] \sum_{x=0}^{p-1}\left[\begin{array}{c} ax^2 + bx + c \\ p \end{array}\right] = \sum_{x=0}^{p-1}\left[\begin{array}{c} x^2 - D \\ p \end{array}\right] = S.$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Theo định lí 2 ở trên thì $S \equiv -1(\mathrm{mod}p)$, mặt khác $|S| \leq p$ cho ta S=-1 hoặc S=p-1.

Giả sử S=p-1, khi đó những số $\left[\begin{array}{c} x^2-D \\ \\ p \end{array}\right]$ nhận giá tri bằng 1, khi $x = x_0$ thì nó nhận giá trị bằng 0, nghĩa là p là ước của $x_0^2 - D$. Do p là ước của $(-x_0)^2 - D = x_0 - p$ ta phải có $x_0 = 0$ do đó p là ước của D. Ngược lại, nếu p là ước của D, ta có S=p-1, mặt khác S=-1, đó là điều phải chứng minh.

**Ví dụ**

Số nghiệm của đồng dư $x^2 - y^2 \equiv D(\mathrm{mod}p)$, với $D \not\equiv 0(\mathrm{mod}p)$ nhận giá trị bằng p-1.

**Chứng minh**

Đây chính là hệ quả được suy ra trực tiếp của định lí trên vì khi cố định x thì số các nghiệm y của đồng dư $y^2 \equiv x^2 - D(\mathrm{mod}p)$ bằng

$$\left[\begin{array}{c} x^2-D \\ \\ p \end{array}\right] + 1.$$

Đánh giá tổng của kí hiệu Legendre đối với đa thức $f(x)$ bậc lớn hơn hai có ý nghĩa đặc biệt và khó. Trong phần này chúng ta xét trường hợp đa thức bậc ba thuộc một kiểu nào đó.

Cho số nguyên a, định nghĩa

$$K(a) = \sum_{x=0}^{p-1} \left[\begin{array}{c} x(x^2+a) \\ \\ p \end{array}\right]$$

Giả sử p không là ước của a. Dễ suy ra rằng với mỗi số nguyên t,



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$K(at^2) = \left[\begin{array}{c} t \\ p \end{array}\right] \sum_{x=0}^{p-1} \left[\begin{array}{c} \frac{x}{t}((\frac{x}{t})^2 + a) \\ p \end{array}\right] = \left[\begin{array}{c} t \\ p \end{array}\right] K(a).$$

Do đó $|K(a)|$ chỉ phụ thuộc vào việc a có là thặng dư bình phương modulo p hay không.

Bây giờ chúng ta đưa ra một chứng minh không tiêu chuẩn rằng mỗi số nguyên tố $p \equiv 1(\mathrm{mod}4)$ là tổng của hai bình phương.

**Định lý 1.3.4.** *Giả sử a và b là một thặng dư bình phương và một không thặng dư bình phương modulo số nguyên tố p có dạng 4k+1. Khi đó $|K(a)|$ và $|K(b)|$ là những số nguyên chẵn và thỏa mãn*

$$(\tfrac{1}{2}\,|K(a)|)^2 + (\tfrac{1}{2}\,|K(b)|)^2 = p.$$

**Chứng minh**

Ta thấy $p'(K(a)^2 + K(b)^2) = \sum_{n=1}^{p-1} K(n)^2 = \sum_{n=0}^{p-1} K(n)^2$, do K(0)=0. Bây giờ ta tính $\sum_{n=0}^{p-1} K(n)^2$. Với mỗi n ta có:

$$K(n)^2 = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left[\begin{array}{c} xy(x^2+n)(y^2+n) \\ p \end{array}\right],$$

suy ra

$$\sum_{n=0}^{p-1} K(n)^2 = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left[\begin{array}{c} xy \\ p \end{array}\right] \sum_{n=0}^{p-1} \left[\begin{array}{c} xy(x^2+n)(y^2+n) \\ p \end{array}\right]$$

Chú ý rằng theo định lí 2 ở trên thì $\sum_{n=0}^{p-1} \left[\begin{array}{c} xy(x^2+n)(y^2+n) \\ p \end{array}\right]$ nhận giá trị bằng p-1 nếu $x = \pm y$ và bằng -1 nếu ngược lại. Như vậy

$$\sum_{n=0}^{p-1} K(n)^2 = p(2p-2) - \sum_{x=0}^{p-1}\sum_{y=0}^{p-1} \left[\begin{array}{c} xy \\ p \end{array}\right] = 4pp'$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Chúng ta thấy rằng $K(a)^2 + K(b)^2 = 4p$, Hơn nữa $K(a)^2 + K(b)^2$ chia hết cho 4 nên cả $K(a)^2$ và $K(b)^2$ đều chẵn.

## 1.4. Số giả nguyên tố Euler

Giả sử p là số nguyên tố lẻ và b là số nguyên không chia hết cho p. Khi đó theo tiêu chuẩn Euler ta có

$$b^{\frac{p-1}{2}} \equiv \left[ \begin{array}{c} b \\ \\ p \end{array} \right] (\mathrm{mod} p).$$

Như vậy để kiểm tra n có phải là số nguyên tố hay không, ta có thể lấy một số b nguyên tố cùng nhau với n, và kiểm tra đồng dư sau có nghiệm hay không

$$b^{\frac{p-1}{2}} \equiv \left[ \begin{array}{c} b \\ \\ n \end{array} \right] (\mathrm{mod} n),$$

trong đó vế phải là kí hiệu Jacobi. Nếu đồng dư thức không đúng thì n phải là hợp số, ngược lại chưa kết luận được nhung nhiều khả năng n là nguyên tố.

**Định nghĩa 1.4.1.** *Số nguyên dương n được gọi là số giả nguyên tố Euler cơ sở b nếu nó là hợp số và đồng dư sau nghiệm đúng*

$$b^{\frac{p-1}{2}} \equiv \left[ \begin{array}{c} b \\ \\ n \end{array} \right] (\mathrm{mod} n),$$

**Định lý 1.4.1.** *Mọi số giả nguyên tố Euler cơ sở b đều là số giả nguyên tố cơ sở b.*

**Định lý 1.4.2.** *Mọi số giả nguyên tố mạnh cơ sở b đều là số giả nguyên tố Euler cơ sở b.*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

**Chứng minh**

Cho n là số giả nguyên tố mạnh cơ sở b. Khi đó, nếu $n-1=2^s t$, t lẻ thì, hoặc $b^t \equiv 1(\mathrm{mod} n)$, hoặc $b^{2^r t} \equiv -1(\mathrm{mod} n)$, với r nào đó $0 \leq r \leq s-1$. Giả sử $\prod_{j=1}^{m} p_j^{a_j}$ là phân tích của n thành thừa số nguyên tố. Ta xét hai trường hợp.

Thứ nhất, $b' \equiv 1(\mathrm{mod} n)$. Giả sử p là một ước nguyên tố của n. Khi đó $ord_d p$ là ước của t, và do đó $\mathrm{or}d_p b$ là số lẻ. Mặt khác, $ord_d p$ là ước của $\phi(p)=p-1$, nên nó phải là ước của $\frac{p-1}{2}$. Vậy ta có

$$b^{\frac{p-1}{2}} \equiv 1(\mathrm{mod} p).$$

Theo tiêu chuẩn Euler, $\left[\begin{array}{c} b \\ \\ p \end{array}\right] = 1$ và $\left[\begin{array}{c} b \\ \\ n \end{array}\right] = 1$ . Mặt khác ta có

$$b^{\frac{n-1}{2}} = (b^t)^{2^s-1} \equiv 1(\mathrm{mod} p).$$

Vậy n là số giả nguyên tố Euler cơ sở b.

Trường hợp thứ hai: $b^{2^{r+1}t} \equiv -1(\mathrm{mod} n)$. Nếu p là một ước nguyên tố của n thì $b^{2^{r+1}t} \equiv -1(\mathrm{mod} p)$. Bình phương cả hai vế của đồng dư thức này ta được

$$b^{2^{r+1}t} \equiv 1(\mathrm{mod} p)$$

Từ đó suy ra $ord_d p$ là ước của $2^{r+1}t$, nhưng $ord_d p$ không là ước của $2^r t$. Như vậy, $ord_d p = 2^{r+1}c$, trong đó c là một số nguyên lẻ. Mặt khác, vì $ord_d p$ là ước của p-1, $2^{r+1}$ là ước của $ord_d p$, nên $2^{r+1}$ là ước của p-1. Như vậy, ta có $p = 2^{r+1}d + 1$, trong đó d là số nguyên. Vì

$$b^{\frac{ord_p b}{2}} \equiv 1(\mathrm{mod} p)$$

nên ta có



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\left[\begin{array}{c} b \\ \\ p \end{array}\right] \equiv b^{\frac{p-1}{2}} = b^{\frac{ord_p b}{2}\frac{p-1}{ord_p b}} \equiv (-1)^{\frac{p-1}{ord_p b}} = (-1)^{\frac{p-1}{2^{r+1}}c} (\mathrm{mod} p).$$

vì c lẻ nên từ đó suy ra $\left[\begin{array}{c} b \\ \\ p \end{array}\right] = (-1)^d$. Bây giờ ta giả sử có phân tích thành thừa số nguyên tố dạng

$$n = \prod_{j=1}^{m} p_j^{a_j}.$$

Theo chứng minh phần trên, các ước nguyên tố $p_i$ có dạng $p_i = 2^{r+1}d_i + 1$, và ta có

$$\left[\begin{array}{c} b \\ \\ m \end{array}\right] = \prod_{j=1}^{m} \left[\begin{array}{c} b \\ \\ p_i \end{array}\right]_i^a = (-1)\sum_{i=1}^{m} a_i d_i.$$

Mặt khác, dễ thấy rằng $n \equiv 1 + 2^{r+1}\sum_{i=1}^{m} a_i d_i (\mathrm{mod} 2^{2r+2})$. Do đó

$$t2^{s-1} = \frac{n-1}{2} \equiv 2^r \sum_{i=1}^{m} a_i d_i (\mathrm{mod} 2^{r+1}),$$

tức là $t2^{s-1-r} \equiv \sum_{i=1}^{m} a_i d_i (\mathrm{mod} 2)$ và $b^{\frac{n-1}{2}} = (b^{2^r t})^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{m} a_i d_i} (\mathrm{mod}\ n)$.

Như vậy,

$$b^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} b \\ \\ n \end{array}\right] (\mathrm{mod} n)$$

và n là số giả nguyên tố Euler cơ sở b. Định lí được chứng minh.

Chú ý rằng, điều ngược lại không phải luôn luôn đúng: tồn tại những số nguyên tố giả Euler cơ sở b không là số giả nguyên tố mạnh cơ sở đó. Ví dụ n=1105, b=2

Tuy nhiên, với những điều kiện bổ sung, một số giả nguyên tố Euler sẽ là số giả nguyên tố mạnh cùng cơ sở. Ta có định lí sau.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

**Định lý 1.4.3.** *Số n giả nguyên tố Euler cơ sở b là số giả nguyên tố mạnh cơ sở b nếu* $n \equiv 3(\mathrm{mod}4)$, *hoặc* $\left[\begin{array}{c} b \\ \\ n \end{array}\right] = -1.$

Chứng minh. Trường hợp thứ nhất: $n \equiv 3(\mathrm{mod}4)$. Khi đó n-1=2t và t lẻ.

Vì n là số giả nguyên tố Euler cơ sở b nên

$$b' = b^{\frac{p-1}{2}} \equiv \left[\begin{array}{c} b \\ \\ n \end{array}\right] (\mathrm{mod}n).$$

Như vậy, n là số giả nguyên tố mạnh cơ sở b.

Tong trường hợp thứ hai, ta viết $n - 1 = 2^s t$, trong đó t lẻ, s là số nguyên dương. Vì n là số giả nguyên tố mạnh cơ sở b nên

$$b^{2^{s-1}t} = b^{\frac{p-1}{2}} \equiv \left[\begin{array}{c} b \\ \\ n \end{array}\right] (\mathrm{mod}n).$$

Theo giả thiết ta có $b^{2^{s-1}t} \equiv -1(\mathrm{mod}n)$. Vì $\left[\begin{array}{c} b \\ \\ n \end{array}\right] = \pm 1$ cho nên

$$\text{hoặc } b' \equiv 1(\mathrm{mod}n), \text{ hoặc } b' \equiv -1(\mathrm{mod}n)$$

vậy n là số giả nguyên tố mạnh cơ sở b.

Dùng số giả nguyên tố Euler, ta có thể xây dựng thuật toán xác suất để kiểm tra một số nguyên tố hay không. Thuật toán này được Solovay và Strassen tìm ra đầu tiên năm 1977.

Ta bắt đầu bằng bổ đề sau.

**Bổ đề 1.4.1.** *Giả sử n là một số nguyên dương lẻ không chính phương. Khi đó tồn tại ít nhất một số b với* $1 < b < n$, *(b,n)=1, sao cho*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\left[\begin{array}{c} b \\ \\ n \end{array}\right] = -1.$$

Chứng minh. Nếu n là số nguyên tố thì số b tồn tại. Khi n là hợp số không chính phương, ta viết n=rs, trong đó (r,s)=1 và $r = p^e$, với p là một số nguyên tố lẻ và e là số nguyên dương lẻ. Bây giờ giả sử t là một không thặng dư bình phương của số nguyên tố p. Ta dùng định lí Trung Hoa về phần dư để tìm số nguyên b sao cho $1 < b < n$, (b,n)=1 và $b \equiv t(\mathrm{mod} r)$, $b \equiv 1(\mathrm{mod} s)$

Khi đó ta có $\left[\begin{array}{c} b \\ \\ r \end{array}\right] = \left[\begin{array}{c} b \\ \\ p^e \end{array}\right] = (-1)^e = -1 = -1$, $\left[\begin{array}{c} b \\ \\ s \end{array}\right] = 1$, tức là $\left[\begin{array}{c} b \\ \\ n \end{array}\right] = -1.$

**Bổ đề 1.4.2.** *Với mỗi hợp số lẻ n, tồn tại ít nhất một số b sao cho* $1 < b < n$, *(b,n)=1 và*

$$b^{\frac{n-1}{2}} \not\equiv \left[\begin{array}{c} b \\ \\ n \end{array}\right] (\mathrm{mod} n)$$

Giả sử ngược lại, với mọi số nguyên không vượt quá n và nguyên tố cùng nhau với n, ta có

$$b^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} b \\ \\ n \end{array}\right] (\mathrm{mod} n).$$

Từ đó suy ra, nếu (b,n)=1 thì $b^{n-1} \equiv 1(\mathrm{mod} n)$.

Như vậy, n phải là số Carmicheal, và do đó, $n = q_1 q_2 ... q_r$ là tích của các số nguyên tố lẻ khác nhau. Ta sẽ chỉ ra rằng

$$b^{\frac{n-1}{2}} \equiv 1(\mathrm{mod} n).$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

đối với số nguyên tố b không vượt quá n và nguyên tố cùng nhau với n. Giả sử ngược lại, tồn tại b thỏa mãn

$$b^{\frac{n-1}{2}} \equiv -1(\mathrm{mod}n).$$

Dùng định lí Trung Hoa về phần dư, ta tìm được số a, $1 < a < n$, (a,n)=1 sao cho $a \equiv b(\mathrm{mod}q_1)$, $a \equiv 1(\mathrm{mod}q_1q_2...q_r)$ .

Như vậy

$$a^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \equiv -1(\mathrm{mod}q_1),\ a^{\frac{n-1}{2}} \equiv 1(\mathrm{mod}q_1q_2...q_r).$$

Do đó

$$a^{\frac{n-1}{2}} \not\equiv \pm 1(\mathrm{mod}q_1q_2...q_r),$$

trái với giả thiết phản chứng. Như vậy với mọi b, $1 < a < n$, (b,n)=1 ta có

$$b^{\frac{n-1}{2}} \equiv 1(\mathrm{mod}n).$$

Từ đồng dư trên và giả thiết của bổ đề, ta có

$$b^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} b \\ \\ n \end{array}\right] \equiv 1(\mathrm{mod}n).$$

Điều này mâu thuẫn với bổ đề 1 nên bổ đề 2 được chứng minh.

Định lí trên đây được dùng làm cơ sở cho một thuật toán kiểm tra xác suất số nguyên tố. Ta có định lí sau:

**Định lý 1.4.4.** *Đối với mỗi hợp số lẻ n, tồn tại không quá* $\frac{\phi(n)}{2}$ *số nguyên dương b nhỏ hơn n, nguyên tố cùng nhau với n, sao cho n là số giả nguyên tố Euler cơ sở b.*

Chứng minh. Theo bổ đề 2, tồn tại số b $1 < a < n$, (b,n)=1, sao cho



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$b^{\frac{n-1}{2}} \not\equiv \left[\begin{array}{c} b \\ n \end{array}\right] (\mathrm{mod} n).$$

Giả sử $a_1, a_2, ..., a_m$ là các số thỏa mãn $1 \leq a_j < n$, $(a_j, n) = 1$ và

$$a_j^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} a_j \\ n \end{array}\right] = (\mathrm{mod} n).$$

Giả sử $r_1, r_2, ..., r_m$ là thặng dư dương bé nhất của các số $ba_1, ba_2, ..., ba_m$. Các số $r_j$ khác nahu và nguyên tố cùng nhau với n. Ta sẽ chứng tỏ rằng chúng không thỏa mãn đồng dư thức như đối với các số $a_j$. Thật vậy, nếu ngược lại

$$r_j^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} r_j \\ n \end{array}\right] = 1(\mathrm{mod} n)$$

thì ta có

$$ba_j^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} ba_j \\ n \end{array}\right] = 1(\mathrm{mod} n),$$

và như vậy

$$b^{\frac{n-1}{2}} a_j^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} b \\ n \end{array}\right] \left[\begin{array}{c} ba_j \\ n \end{array}\right] (\mathrm{mod} n).$$

Từ đó suy ra

$$b^{\frac{n-1}{2}} \equiv \left[\begin{array}{c} b \\ n \end{array}\right] (\mathrm{mod} n),$$

mâu thuẫn với tính chất của b.

Như vậy, tập hợp các số $a_j$ và $r_j$ không giao nhau. Gộp cả hai tập hợp này ta được 2m số khác nhau, bé hơn n và nguyên tố cùng nhau với n. Từ đó suy ra $m < \frac{\phi(n)}{2}$, định lí được chứng minh.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Nhận xét. Từ định lí trên ta thấy rằng, nếu n là một hợp số lẻ, b là số chọn nhẫu nhiên trong các số 1,2,...,n-1, thì xác suất để n là số giả nguyên tố Euler cơ sở b sẽ bé hơn $\frac{1}{2}$. Ta có định lí sau:

**Định lý 1.4.5.** *Thuật toán kiểm tra nguyên tố xác suất Solovay-Strassen Cho n là số nguyên dương, ta chọn ngẫu nhiên k số $b_1, b_2, ..., b_k$ từ các số 1,2,...,n-1. Đối với mỗi số nguyên $b_j$, xét đồng dư thức*

$$b_j^{\frac{n-1}{2}} \equiv \left[ \begin{array}{c} b_j \\ n \end{array} \right] (\mathrm{mod} n),$$

*ta có kết luận sau:*

- *Nếu một trong các đồng dư thức đó không nghiệm đúng thì n là hợp số.*
- *Nếu n là nguyên tố thì mọi đồng dư thức đều nghiệm đúng.*
- *Nếu n là hợp số, thì xác suất để mọi đồng dư thức nghiệm đúng là bé hơn $\frac{1}{2^k}$.*

*Như vậy, nếu k đủ lớn, và n trải qua được kiểm tra xác suất trên đây, thì "hầu như chắc chắn" n là số nguyên tố.*



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

# Chương 2

# Ứng dụng

Sau đây tôi trình bày một số bài tập vận dụng lí thuyết ở chương I, các bài tập này được trích dẫn từ các đề thi chọn học sinh giỏi.

**Bài 1** Tìm tất cả nghiệm nguyên không âm của phương trình

$$12^x + y^4 = 2008^z$$

**Lời giải**

Nếu z>0, ta có y>0.

Với x chẵn thì vế trái có dạng $a^2+b^2$, với x lẻ thì vế trái có dạng $a^2+3b^2$. Dễ thấy 2008 có ước nguyên tố là 251, a và b đều không chia hết cho 251, theo định lí 1.1.5 ta có -1 hoặc -3 sẽ là thặng dư bậc hai modulo 251, tức là $\left[\begin{array}{c} -1 \\ \\ 251 \end{array}\right] = 1$ hoặc $\left[\begin{array}{c} -3 \\ \\ 251 \end{array}\right] = 1$.

Mặt khác ta có:

$$\left[\begin{array}{c} -1 \\ \\ 251 \end{array}\right] = (-1)^{\frac{251-1}{2}} = -1$$

và

$$\left[\begin{array}{c} -3 \\ \\ 251 \end{array}\right] = -\left[\begin{array}{c} 3 \\ \\ 251 \end{array}\right] = -(-1)^{\frac{251-1}{2}} \left[\begin{array}{c} 251 \\ \\ 3 \end{array}\right] = \left[\frac{2}{3}\right] = -1$$



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

Điều này vô lí. Vậy z=0, y=0, x=0 hay là phương trình đã cho có nghiêm nguyên (0,0,0)

**Bài 2** Tìm tất cả cặp số nguyên dương (x,n) sao cho: $x^3 + 2x + 1 = 2^n$

**Lời giải**

Phương trình đã cho tương đương với phương trình sau:

$$x(x^2 + 2) = 2^n - 1$$

Dễ thấy $x(x^2 + 2) \vdots 3$ do n chẵn. Từ phương trình ban đầu suy ra x lẻ.

Nếu n>2 ta có: $x^3 + 2x + 1 \equiv 0 (\mathrm{mod} 8)$, suy ra $x \equiv 5 (\mathrm{mod} 8)$.

Mặt khác ta lại có

$x^3 + 2x + 1 = 2^n \Leftrightarrow x^3 + 2x + 3 = 2^n + 2 \Leftrightarrow (x + 1)(x^2 - x - 3) = 2^n + 2$

Gọi p là một ước nguyên tố của $x^2 - x + 3$ suy ra p lẻ và -2 là thặng dư bình phương modulo p. Theo định lí 1.1.8 số nguyên tố p có dạng 8m+1 hoặc 8m+3.

Vì $x \equiv 5 (\mathrm{mod} 8)$ suy ra $x^2 - x + 3 \equiv 7 (\mathrm{mod} 8)$. Vì mọi ước nguyên tố của $x^2 - x + 3$ đều có dạng 8m+1 và 8m+3 nên $x^2 - x + 3 \equiv 3^n (\mathrm{mod} 8)$ suy ra $3^n \equiv 7 (\mathrm{mod} 8)$. Kiểm tra với n từ 0 đến 7 ta thấy điều này không xẩy ra, vậy n>2 không thỏa mãn.

Nếu n=2, ta có $x^3 + 2x + 1 = 2^2 \Leftrightarrow x = 1$

Nếu n=1, ta có $x^3 + 2x + 1 = 2 \Leftrightarrow x = 0$ (loại).

Vậy phương trình đã cho chỉ có nghiệm x=1 với n=2.

**Bài 3** Cho số nguyên dương n. Chứng minh rằng $2^n + 1$ không có ước nguyên tố dạng 8k-1 với k là số nguyên dương.

**Lời giải**

Nếu n chẵn, gọi p là ước nuyên tố bất kì của $2^n + 1$. Ta có



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\left[\begin{array}{c} -1 \\ \\ p \end{array}\right] = 1 \Rightarrow p = 4k + 1$$

do đó $2^n + 1$ không có ước nguyên tố dạng 8k-1 với k là số nguyên dương. Nếu n lẻ, gọi p là ước nuyên tố bất kì của $2^n + 1$, thì p là ước của $2^{n+1} + 2$, do đó -2 là thặng dư bậc hai modulo p. Theo định lí 1.1.8, p có dạng 8k+1 hoặc 8k+3

Vậy $2^n + 1$ không có ước nguyên tố dạng 8k-1 với k là số nguyên dương.

**Bài 4** Chứng minh rằng phương trình $x^2+1 = k(y^2-5)$ không có nghiệm nguyên dương với x, y>2.

**Lời giải**

Nếu y chẵn thì $y^2 - 5$ có dạng 4m+3, do đó nó có ước nguyên tố dạng p=4n+3. Từ đó suy ra p phải là ước của x và 1, điều này vô lí.

Nếu y lẻ thì $y^2 - 5$ chia hết cho 4, nhưng $x^1 + 1$ luôn đồng dư với 1 hoặc 2 mod4 điều này không thỏa mãn phương trình đã cho.

Vậy phương trình đã cho vô nghiệm nguyên.

**Bài 5** Chứng minh rằng mỗi số nguyên tố p thì tồn tại các số nguyên a,b sao cho $a^2 + b^2 + 1$ là bội của p.

**Lời giải**

Xét hai tập hợp :

$$A = \left\{a^2\right\}, \text{ và } B = \left\{-1 - b^2\right\}, \text{ với a,b là số nguyên}$$

Lấy theo modulo p thì mỗi tập có đúng $\frac{p+1}{2}$ phần tử, vậy tổng số phần tử của hai tập hợp là p+1. Theo nguyên lí Dirichlet tồn tại phần tử chung của A và B theo modulo p. Do đó ta có, $a^2 + b^2 + 1$ là bội của p.

**Bài 6** Cho số nguyên tố p. Chứng minh rằng số $3^p + 7p - 4$ không là



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

bình phương của một số nguyên.

**Lời giải**

Giả sử tồn tại x sao cho: $3^p + 7^p - 4 = x^2$

Theo định lí Fecmat, ta có $3^p \equiv 3(\mathrm{mod}p)$. Vậy $x^2 \equiv -1(\mathrm{mod}p)$, nên p có dạng 4k+1.

Mặt khác $3^{4k+1}$ có dạng 4k+3, do đó $3^p + 7p - 4$ có dạng 4k+2, suy ra:

$$x^2 \equiv 2(\mathrm{mod}4)$$

điều này mâu thuẫn vì $x^2$ luôn đồng dư với 1 hoặc 0 mod4. Vậy ta có điều phải chứng minh.

**Bài 7** Tìm tất cả nghiệm nguyên của phương trình $1 + 2^x + 2^{2x+1} = y^2$

**Lời giải**

Nếu x=0 ta được $y = \pm 2$

Nếu x>0, giả sử (x,y) là một nghiệm của phương trình thì (x,-y) cũng là một nghiệm của phương trình, do đó ta có thể giả sử y>0

Biến đổi phương trình về dạng:

$$2^x(2^{x+1} + 1) = (y - 1)(y + 1)$$

Vì ước chung lớn nhất của y-1 và y+1 bằng 1 hoặc bằng 2

Nếu ước chung lớn nhất của y-1 và y+1 bằng 1, thì ta có:

$$\begin{cases} y - 1 = 2^x \\ y + 1 = 2^{x+1} + 1 \end{cases}$$

Hệ này vô nghiệm.

Nếu ước chung lớn nhất của y-1 và y+1 bằng 2, thì ta có:



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

$$\left[\begin{array}{l} y-1=2^x a \\ y+1=2^{x+1}a \end{array}\right. \Leftrightarrow \left[\begin{array}{l} y=2^x a+1 \\ y=2^{x+1}a-1 \end{array}\right.$$

Nếu $y=2^{x-1}a+1$, thay vào phương trình ban đầu ta được:

$$2^x(2^{x+1}+1)=a(2^{x-1}a+2) \Leftrightarrow 2^{x-2}(8-a^2)=a-1$$

Suy ra $1 \neq a \leq 2$ vậy a=2, thay vào phương trình ta thấy không thỏa mãn.

Nếu $y=2^{x-1}a-1$, thay vào phương trình ban đầu ta được:

$$2^x(2^x+1)=a(2^{x-1}a-2) \Leftrightarrow 2^{x-1}(4-a^2)=-2(a+1) \Leftrightarrow 2^{x-2}=\frac{a+1}{a^2-8}$$

Dễ thấy phương trình này chỉ có nghiệm a=3, x=4. Thay vào ta được y=23

Vậy phương trình đã cho có nghiệm (0,2), (0,-2), (4,23), (-4,23).

## BÀI TẬP

**Bài 8** Giả sử p>3 là một số nguyên tố, và a,b là các số tự nhiên sao cho:

$$1+\frac{1}{2}+...+\frac{1}{p-1}=\frac{a}{b}$$

Chứng minh rằng $p^2$ là ước của a.

**Bài 9** Tìm tất cả giá trị của n là số tự nhiên sao cho tập $A=n,n+1,...,n+1997$ có thể phân hoạch thành ít nhất hai tập con mà tích của hai phần tử trong mỗi tập con đó bằng nhau.

**Bài 10** Tìm tất cả các số nguyên dương sao cho:

$$\frac{a^2+b^2+c^2}{3(ab+bc+ca)}$$

là một số nguyên.

**Bài 11** Cho hai số nguyên dương a, b sao cho $(4a^2-1)^2$ chia hết cho $(4ab-1)$. Chứng minh rằng a=b.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

## KẾT LUẬN

Trong khóa luận này tôi đã trình bày : Lí thuyết đồng dư, Kí hiệu Lagrange, Jacobi và số giả nguyên tố Euler và ứng dụng

1 Tìm hiểu kí hiệu Lagrange, kí hiệu Jacobi

2 Tìm hiểu số giả nguyên tố

3 Đề cập phân tích một số dạng bài toán

Tuy nhiên do thời gian thực hiện khóa luận không nhiều còn có những sai sót em rất mong nhận được sự góp ý của quý thầy cô và bạn đọc.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/

# Tài liệu tham khảo

[1] Hà Huy Khoái - Phạm Huy Điển, *Số học thuật toán*, NXB Đại học Quốc Gia Hà Nội (2003) 237 trang.

[2] Hà Huy Khoái, *Nhập môn số học thuật toán*, NXB Khoa Học (1997) 156 trang.



So hoa bôi trung tam hoc lieu http://www.lrc.tnu.edu.vn/