

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐỒNG THỊ HUYỀN TRANG

PHƯƠNG TRÌNH ĐỒNG DƯ

LUẬN VĂN THẠC SĨ TOÁN HỌC

Thái Nguyên - Năm 2012

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC KHOA HỌC

ĐỒNG THỊ HUYỀN TRANG

PHƯƠNG TRÌNH ĐỒNG DƯ

Chuyên ngành: PHƯƠNG PHÁP TOÁN SƠ CẤP

Mã số : 60.46.40

LUẬN VĂN THẠC SĨ TOÁN HỌC

NGƯỜI HƯỚNG DẪN KHOA HỌC
PGS.TS ĐÀM VĂN NHỈ

Thái Nguyên - Năm 2012

Mục lục

Mục lục	i
LỜI NÓI ĐẦU	1
Nội dung	4
1 Lý thuyết đồng dư	4
1.1 Phép chia trong vành $\mathbb{Z}$	4
1.2 Quan hệ đồng dư và tính chất	8
1.3 Vành $\mathbb{Z}_m$ các lớp thặng dư môđun m	11
1.4 Định lý Euler và Định lý Fermat	14
1.5 Một vài ví dụ tổng hợp	15
2 Phương trình đồng dư	20
2.1 Phương trình đồng dư một ẩn	20
2.2 Phương trình đồng dư bậc nhất	22
2.3 Hệ phương trình đồng dư một ẩn	24
2.4 Phương trình đồng dư một ẩn bậc cao	26
2.5 Phương trình đồng dư bậc cao theo môđun p	31
2.6 Thặng dư bậc hai	33
3 Phương trình Mordell	38
3.1 Chuẩn trong vành $\mathbb{Z}[\sqrt{d}]$ và số học	38
3.2 Phương trình Mordell	43

Kết luận	49
Tài liệu tham khảo	51

LỜI NÓI ĐẦU

Trong số học, thường ta phải xác định tất cả các số với tính chất p cho trước. Có thể có những số thỏa mãn tính chất p , nhưng có nhiều khi không có. Nếu ta xét tất cả các số thuộc tập $\mathbb{Z}$ thì đây là một công việc không thể thực hiện được. Nhưng nếu ta xét trên một tập hữu hạn nào đấy thì việc kiểm tra có thể thực hiện được. Lý thuyết đồng dư chính là việc chuyển những bài toán xét trên tập vô hạn $\mathbb{Z}$ về một tập hữu hạn những lớp đồng dư theo một môđun m nào đấy. Chẳng hạn:

Xác định x, y nguyên thỏa mãn: $x^2 + 1 = 3y$. Giả sử phương trình có nghiệm nguyên. Lấy môđun 3 ta có $x^2 + 1 \equiv 0 \pmod{3}$. Biểu diễn $x = 3k$ hoặc $x = 3k \pm 1$. khi đó $x^2 + 1 = 3h + 1$ hoặc $3h + 2$. Vậy $x^2 + 1 \not\equiv 0 \pmod{3}$: Mâu thuẫn. Tóm lại phương trình vô nghiệm.

Xác định x, y nguyên thỏa mãn: $x^2 + 2 = 5y$. Giả sử phương trình có nghiệm nguyên. Lấy môđun 5 ta có $x^2 + 2 \equiv 0 \pmod{5}$. Biểu diễn $x = 5k$ hoặc $x = 5k \pm 1$ hoặc $x = 5k \pm 2$. Khi đó $x^2 + 2 = 5h + 2$ hoặc $5h + 3$ hoặc $5h + 6$. Vậy $x^2 + 2 \not\equiv 0 \pmod{5}$: Mâu thuẫn. Tóm lại phương trình vô nghiệm.

Qua ví dụ trên thay cho việc x, y thuộc tập $\mathbb{Z}$ vô hạn thì ta chỉ việc kiểm tra $\bar{x}$ nhận $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$.

Nội dung luận văn được chia thành ba chương:

Chương 1 “**Lý thuyết đồng dư**” bao gồm 5 mục. Mục 1.1 được dành trình bày về *Phép chia trong vành $\mathbb{Z}$* , kết quả chính trình bày lại thuật toán Euclid để tìm ƯCLN và định lý cơ bản của số học. Mục 1.2 được dành trình bày về *Quan hệ đồng dư và tính chất* kết quả chính đã chỉ ra

được những tính chất cơ bản của quan hệ đồng dư. Mục 1.3 *Vành $\mathbb{Z}_m$ các lớp thặng dư môđun m* chứng minh được $\mathbb{Z}$ là vành giao hoán, chứng minh được $\mathbb{Z}_m^*$ là nhóm nhân. Mục 1.4 *Định lý Euler và Định lý Fermat*. Mục 1.5 *Một số ví dụ tổng hợp*.

Chương 2 “**Phương trình đồng dư**” bao gồm 6 mục. Mục 2.1 *Phương trình đồng dư một ẩn*. Mục 2.2 *Phương trình đồng dư bậc nhất*. Mục 2.3 *Hệ phương trình đồng dư một ẩn*. Mục 2.4 *Phương trình đồng dư một ẩn bậc cao*. Mục 2.5 *Phương trình đồng dư một ẩn bậc cao theo môđun p* . Mục 2.6 *Phương trình đồng dư bậc hai*. Kết quả chính của chương là trình bày chi tiết việc giải một số dạng phương trình đồng dư và trình bày lại chứng minh định lý Wilson.

Chương 3 “**Phương trình Mordell**” bao gồm 5 mục. Mục 3.1 *Chuẩn trong vành $\mathbb{Z}[\sqrt{d}]$ và số học*. Mục 3.2 *Khái niệm phương trình Mordell*. Mục 3.3 *Một vài phương trình có nghiệm*. Mục 3.4 *Một vài phương trình vô nghiệm*. Mục 3.5 *Ứng dụng của thặng dư bậc 3*. Kết quả chính của chương là trình bày được phương trình Mordell. Đã chỉ ra một số dạng phương trình có nghiệm hoặc vô nghiệm. Trình bày được thặng dư bậc ba.

Do thời gian và kiến thức còn hạn chế nên trong quá trình viết luận văn cũng như trong xử lý văn bản chắc chắn không tránh khỏi những sai sót nhất định. Tác giả luận văn rất mong nhận được sự góp ý của các thầy cô và các bạn đồng nghiệp để luận văn được hoàn thiện hơn.

Nhân dịp này, tác giả xin bày tỏ lòng biết ơn sâu sắc đến thầy hướng dẫn PGS.TS Đàm Văn Nhĩ đã tận tình giúp đỡ trong suốt quá trình làm luận văn.

Tác giả xin trân trọng cảm ơn các thầy, cô giáo Trường Đại học Khoa học- Đại học Thái Nguyên đã giảng dạy và tạo mọi điều kiện thuận lợi trong quá trình tác giả học tập và nghiên cứu.

Tác giả cũng xin chân thành cảm ơn tập thể bạn bè đồng nghiệp và gia đình đã quan tâm giúp đỡ, động viên tác giả hoàn thành tốt luận văn này.

Thái Nguyên, tháng 07 năm 2012.

Tác giả luận văn

Đồng Thị Huyền Trang

Chương 1

Lý thuyết đồng dư

Phương pháp đồng dư do Gauss đề xuất là một phương pháp hữu ích trong việc giải quyết nhiều vấn đề có liên quan đến tính chia hết của các số nguyên.

1.1 Phép chia trong vành $\mathbb{Z}$

Định lý 1.1.1. Với mỗi cặp số nguyên a và $b \neq 0$, luôn tồn tại duy nhất một cặp số nguyên q, r với $0 \leq r < |b|$ để $a = qb + r$.

Chứng minh: Sự tồn tại: Đặt $T = \{n|b| \text{ sao cho } n|b| \leq a, n \in \mathbb{Z}\}$. Vì $|b| \geq 1$ nên

$$-|a||b| \leq -|a| \leq a$$

Do đó $-|a||b| \in T$. Vậy $T \neq \emptyset$. Vì T là tập bị chặn trên T có một số lớn nhất $m|b|$. Từ $m|b| \leq a$ ta suy ra $r = a - m|b| \geq 0$. Ta lại có

$$(m+1)|b| = m|b| + |b| > m|b|.$$

Do $m|b|$ lớn nhất trong T nên $(m+1)|b| \notin T$. Như vậy $|b| > a - m|b| = r$ và ta có $a = qb + r$ với $0 \leq r < |b|$. Bây giờ ta chứng minh tính duy nhất. Giả sử có hai biểu diễn $a = qb + r$ với $0 \leq r < |b|$ và $a = q_1b + r_1$ với $0 \leq r_1 < |b|$. Trừ từng vế, ta có $r - r_1 = b(q_1 - q)$. Từ $|r - r_1| < |b|$ ta

suy ra $|q_1 - q| |b| < |b|$. Vậy $q = q_1$ và do đó $r = r_1$.

Giả sử $a = qb + r, 0 \leq r < |b|$. Khi đó nếu $r = 0$ thì q được gọi là thương của phép chia a cho b ., nếu $r \neq 0$ thì q gọi là thương hụt, còn gọi r là số dư của phép chia a cho b .

Định lý 1.1.2. [Định lý cơ bản của số học] Mọi số tự nhiên lớn hơn 1 đều phân tích được thành một tích hữu hạn thừa số nguyên tố, và phân tích này là duy nhất nếu không kể đến thứ tự các thừa số.

Chứng minh: Xét tập F gồm tất cả các số nguyên lớn hơn 1 không biểu diễn thành tích một số hữu hạn các thừa số nguyên tố. Ta chỉ cần chỉ ra $F \neq \emptyset$. Thật vậy, giả sử $F \neq \emptyset$. Khi đó có hai số nguyên dương $q_1, q_2 > 0$ để $m = q_1 q_2$. Vì $q_1, q_2 < m$ nên $q_1, q_2 \notin F$. Như vậy ta có phân tích $q_1 = t_1 t_2 \dots t_h$ và $q_2 = u_1 u_2 \dots u_k$, ở đó các t_i, u_j đều là các số nguyên tố. Khi đó

$$m = q_1 q_2 = t_1 t_2 \dots t_h u_1 u_2 \dots u_k.$$

Điều này mâu thuẫn với giả thiết $m \in F$. Như vậy F là tập rỗng. Do đó mọi số tự nhiên lớn hơn 1 đều phân tích được thành tích của hữu hạn thừa số nguyên tố. Bây giờ giả sử một số được phân tích thành hai tích dạng A và B các thừa số nguyên tố. Khi đó $A = B$. Bằng cách lược bỏ các tất cả các thừa số nguyên tố xuất hiện trong cả A và B , ta nhận được đẳng thức tương đương $C = D$. Ta cần phải chứng minh $C = D = 1$. Thật vậy giả sử trái lại $C = D \leq 1$. Gọi p là thừa số nguyên tố xuất hiện trong C . Khi đó p không thể là thừa số xuất hiện trong biểu thức tích của D . Có nghĩa là D không là bội của p , và do đó C cũng không là bội của p (mâu thuẫn!). Vậy $C = D = 1$. Điều này chứng tỏ rằng sự phân tích ra các thừa số nguyên tố của một số nguyên > 1 là duy nhất nếu không kể đến thứ tự các thừa số.

Khi phân tích các số tự nhiên $q > 1$ thành tích các thừa số nguyên tố, có thể một số nguyên tố xuất hiện nhiều lần. Nếu các số nguyên tố $p_1, \dots, p_s$

xuất hiện theo thứ tự $\alpha_1, \dots, \alpha_s$ lần, ta viết $q = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ và ta gọi tích này là dạng phân tích tiêu chuẩn hay dạng phân tích chính tắc của q .

Khi hai số nguyên dương a, b ở dạng phân tích tiêu chuẩn, có thừa số nguyên tố p của a nhưng không là của b , thì ta có thể bổ sung vào phân tích của b thừa số p^0 (và ngược lại). Khi đó ta luôn viết được

$$a = p_1^{u_1} p_2^{u_2} \dots p_s^{u_s}$$

và

$$b = p_1^{v_1} p_2^{v_2} \dots p_s^{v_s},$$

trong đó có thể có những số mũ 0. Như vậy với hai số nguyên dương a, b luôn tồn tại các số nguyên tố $p_1, p_2, \dots, p_s$ để

$$a = p_1^{u_1} p_2^{u_2} \dots p_s^{u_s}$$

và

$$b = p_1^{v_1} p_2^{v_2} \dots p_s^{v_s},$$

với các số mũ nguyên không âm. Khi đó dễ thấy rằng:

$$(a, b) = p_1^{\min(u_1, v_1)} p_2^{\min(u_2, v_2)} \dots p_s^{\min(u_s, v_s)}$$

$$[a, b] = p_1^{\max(u_1, v_1)} p_2^{\max(u_2, v_2)} \dots p_s^{\max(u_s, v_s)}.$$

Thuật toán Euclid: Giả sử a và b là hai số nguyên dương với $a \geq b$ và đặt $r_0 = a, r_1 = b$. Bằng cách áp dụng liên tiếp thuật toán chia, ta được:

$$r_0 = r_1 q_0 + r_2, \quad r_1 = r_2 q_1 + r_3, \dots, \quad r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad r_{n-1} = r_n q_n$$

Với $r_1 > r_2 > \dots > r_0 > 0$. Cuối cùng, số 0 sẽ xuất hiện trong dãy phép chia liên tiếp, vì dãy các số dư $b = r_1 > r_2 > \dots \geq 0$ không chứa quá b số

được. Từ đây suy ra

$$(a, b) = (r_0, r_1) = (r_1, r_2) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

Do đó ước chung lớn nhất của a và b là số dư khác 0 cuối cùng trong dãy phép chia.

Từ thuật toán Euclid cùng với các tính chất nêu trên, ta dễ dàng tìm được ước chung lớn nhất của hai số nguyên, và do đó nhiều số nguyên.

Ví dụ 1.1.3. Đặt $(1 + 4\sqrt[3]{2} - 4\sqrt[3]{4})^n = a_n + b_n\sqrt[3]{2} + c_n\sqrt[3]{4}$ cho mọi n nguyên kông âm và a_n, b_n, c_n nguyên. Chứng minh a_n chia cho 8 dư 1, còn b_n, c_n cũng chia hết cho 4.

Bài giải: Ta có $a_{n+1} + b_{n+1}\sqrt[3]{2} + c_{n+1}\sqrt[3]{4} = (a_n + b_n\sqrt[3]{2} + c_n\sqrt[3]{4})(1 + 4\sqrt[3]{2} - 4\sqrt[3]{4})$. Vậy

$$\begin{cases} a_{n+1} = a_n - 8b_n + 8c_n \\ b_{n+1} = 4a_n + b_n - 8c_n \\ c_{n+1} = -4a_n + 4b_n + c_n. \end{cases} \Rightarrow \begin{cases} a_{n+1} \equiv a_n \pmod{8} \\ b_{n+1} \equiv b_n \pmod{4} \\ c_{n+1} \equiv c_n \pmod{4}. \end{cases}$$

Từ $a_1 = 1, b_1 = 4, c_1 = -4$ ta suy ra điều cần chứng minh.

Ví dụ 1.1.4. Cho 2012 hình chữ nhật với độ dài các cạnh là những số nguyên a, b thỏa mãn $100 \geq a \geq b \geq 1$. Hình chữ nhật với độ dài các cạnh (a, b) được gọi là chứa được hình chữ nhật với độ dài các cạnh (c, d) nếu $c \geq a, d \geq b$. Chứng minh rằng khi đó có ít nhất 41 hình chữ nhật lần lượt chứa được nhau.

Bài giải: Ta chia 2012 hình chữ nhật này ra làm 50 lớp

$$\begin{cases} \{(100, b_1) \mid 100 \geq b_1 \geq 1\} \cup \{(a_1, 1) \mid 100 \geq a_1 \geq 1\} \\ \{(99, b_2) \mid 99 \geq b_2 \geq 2\} \cup \{(a_2, 2) \mid 99 \geq a_2 \geq 2\} \\ \{(98, b_3) \mid 98 \geq b_3 \geq 3\} \cup \{(a_3, 3) \mid 98 \geq a_3 \geq 3\} \\ \dots \\ \{(52, b_{49}) \mid 52 \geq b_{49} \geq 49\} \cup \{(a_{49}, 49) \mid 52 \geq a_{49} \geq 49\} \\ \{(51, b_{50}) \mid 51 \geq b_{50} \geq 50\} \cup \{(50, 50)\}. \end{cases}$$

Hình chữ nhật (a, b) thuộc một trong 50 lớp trên và các hình chữ nhật

thuộc cùng một lớp thì chứa nha. Do số hình chữ nhật là 2012 phân vào 50 lớp, nên phải có ít nhất một lớp chứa nhiều hơn 40 hình chữ nhật.

1.2 Quan hệ đồng dư và tính chất

Định nghĩa 1.2.1. Cho số nguyên dương m . Hai số nguyên a và b được gọi là đồng dư theo môđun m nếu hiệu $a - b$ chia hết cho m . Nếu a đồng dư với b theo môđun m thì ta viết $a \equiv b \pmod{m}$ và gọi đó là một đồng dư thức.

Một số tính chất sau đây của đồng dư thức là hiển nhiên.

Mệnh đề 1.2.2. Cho số nguyên dương m . Ta có:

(i) $a \equiv b \pmod{m}$ khi và chỉ khi $a = b + mt$, $t \in \mathbb{Z}$, hay $a - b$ chia hết cho m .

(ii) Quan hệ đồng dư theo môđun m là một quan hệ tương đương trong tập $\mathbb{Z}$.

Do quan hệ đồng dư là một quan hệ tương đương nên các phần tử thuộc tập $\mathbb{Z}$ sẽ được phân ra thành các lớp tương đương. Ký hiệu tập thương $\mathbb{Z}/\equiv$ bởi $\mathbb{Z}_m$

Định nghĩa 1.2.3. Các lớp tương đương theo quan hệ đồng dư theo môđun m được gọi là các lớp thặng dư theo môđun m .

Mệnh đề 1.2.4. Số các lớp thặng dư theo môđun m đúng bằng m .

Định nghĩa 1.2.5. Nếu từ mỗi lớp thặng dư theo môđun m ta lấy ra một đại diện, thì tập các đại diện đó được gọi là một hệ thặng dư đầy đủ theo môđun m . Nếu từ mỗi lớp thặng dư đầy đủ theo môđun m ta lấy ra một đại diện không âm bé nhất, thì tập hợp các đại diện đó được gọi là một hệ thặng dư đầy đủ không âm bé nhất theo môđun m .

Hệ thặng dư đầy đủ không âm bé nhất theo môđun m là $0, 1, \dots, m - 1$,

còn hệ thặng dư đầy đủ với giá trị tuyệt đối nhỏ nhất theo môđun m là

$$\begin{cases} \left\{ -\frac{m-1}{2}, -\frac{m-1}{2} + 1, \dots, \frac{m-1}{2} \right\} & \text{khi } m \text{ lẻ} \\ \left\{ -\frac{m}{2}, -\frac{m}{2} + 1, \dots, \frac{m}{2} - 1 \right\} & \text{hoặc} \\ \left\{ -\frac{m}{2} + 1, -\frac{m}{2} + 2, \dots, \frac{m}{2} \right\} & \text{khi } m \text{ chẵn.} \end{cases}$$

Định lý 1.2.6. Cho a, b là những số nguyên tùy ý. Nếu $(a, m) = 1$ và x chạy khắp một hệ thặng dư đầy đủ theo môđun m thì $ax + b$ cũng chạy khắp một hệ thặng dư đầy đủ theo môđun m .

Chứng minh: Nếu x_1, x_2 nguyên và $ax_1 + b \equiv ax_2 + b \pmod{m}$ thì $a(x_1 - x_2) \equiv 0 \pmod{m}$. Do $(a, m) = 1$ nên $x_1 \equiv x_2 \pmod{m}$. Điều này chứng tỏ khi x chạy qua các lớp tương đương khác nhau $ax + b$ cũng chạy qua các lớp tương đương khác nhau. Vậy, nếu $(a, m) = 1$ và x chạy khắp một hệ thặng dư theo môđun m thì $ax + b$ cũng chạy khắp một hệ thặng dư theo môđun m .

Tính chất của đồng dư thức

Một số tính chất sau đây của đồng dư thức là hiển nhiên.

(i) Nếu $a_i \equiv b_i \pmod{m}, i = 1, \dots, n$, thì $\sum_{i=1}^n a_i \equiv \sum_{i=1}^n b_i \pmod{m}$.

(ii) Nếu $a \equiv b + c \pmod{m}$ thì $a - c \equiv b \pmod{m}$.

(iii) Nếu $a \equiv b \pmod{m}$ thì $a + hm \equiv b \pmod{m}$.

(iv) Nếu $a_i \equiv b_i \pmod{m}, i = 1, \dots, n$, thì $\prod_{i=1}^n a_i \equiv \prod_{i=1}^n b_i \pmod{m}$.

(v) Nếu $a \equiv b \pmod{m}$ thì $ah \equiv bh \pmod{m}$.

(vi) Nếu $a_i \equiv b_i \pmod{m}, i = 1, \dots, n$, và $x \equiv y \pmod{m}$ thì ta luôn có $\sum_{i=1}^n a_i x^i \equiv \sum_{i=1}^n b_i y^i \pmod{m}$.

(vii) Nếu $a \equiv b \pmod{m}, d \in \text{uc}(a, b), (m, d) = 1$ thì $\frac{a}{d} \equiv \frac{b}{d} \pmod{m}$.

(viii) Nếu $a \equiv b \pmod{m}$ thì $ah \equiv bh \pmod{mh}$.

(ix) Nếu $a \equiv b \pmod{m}, d \in \text{uc}(a, b, m)$ thì $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

(x) Nếu $a \equiv b \pmod{m}$ thì $(a, m) = (b, m)$.

Tính chất (x), ta thấy các số của cùng một lớp thặng dư theo môđun m

có cùng ước chung lớn nhất với (m) . Do đó ta định nghĩa:

$$(\bar{a}, m) := (b, m), \forall b \in \bar{a}.$$

Khi $(\bar{a}, m) = 1$ thì lớp $\bar{a}$ được gọi là *lớp nguyên tố với môđun m* .

Định nghĩa 1.2.7. Nếu từ mỗi lớp thặng dư nguyên tố với môđun m ta lấy ra một đại diện, thì tập hợp các lớp đại diện đó được gọi là *một hệ thặng dư thu gọn theo môđun m* .

Thông thường ta chọn hệ thặng dư thu gọn theo môđun m từ hệ thặng dư đầy đủ không âm bé nhất $\{0, 1, \dots, m-1\}$. Ký hiệu $\varphi(m)$ là số các số $a \in \{0, 1, \dots, m-1\}$ và $(a, m) = 1$. Khi đó số các phần tử của một hệ thu gọn theo môđun m là $\varphi(m)$.

Ví dụ 1.2.8. Hệ thặng dư thu gọn theo môđun 14 là $\{1, 3, 5, 9, 11, 13\}$ và $\varphi(14) = 6$.

Hệ thặng dư thu gọn theo môđun 18 là $\{1, 5, 7, 11, 13, 17\}$, $\varphi(18) = 6$.

Định lý 1.2.9. Nếu $(a, m) = 1$ và x chạy khắp một hệ thặng dư thu gọn theo môđun m thì ax cũng chạy khắp một hệ thặng dư thu gọn theo môđun m .

Chứng minh: Nếu x_1, x_2 nguyên và $ax_1 \equiv ax_2 \pmod{m}$ thì $a(x_1 - x_2) \equiv 0 \pmod{m}$. Do $(a, m) = 1$ nên $x_1 \equiv x_2 \pmod{m}$. Điều này chứng tỏ khi x chạy qua các lớp tương đương khác nhau thì ax cũng chạy qua các lớp tương đương khác nhau. Vậy $\varphi(m)$ giá trị của x cho $\varphi(m)$ giá trị của ax và các giá trị này không đồng dư theo môđun m . Vì $(a, m) = 1$ và $(x, m) = 1$ nên $(ax, m) = 1$. Điều này chứng tỏ $\varphi(m)$ giá trị của ax lập thành một hệ thặng dư thu gọn theo môđun m .

1.3 Vành $\mathbb{Z}_m$ các lớp thặng dư môđun m

Xét tập thương $\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\}$ các lớp thặng dư môđun m . Để biến tập này thành một vành ta định nghĩa hai phép toán cộng và nhân sau đây:

$$\bar{a} + \bar{b} = \overline{a + b}, \bar{a} \cdot \bar{b} = \overline{ab}, \forall a, b \in \mathbb{Z}.$$

Mệnh đề 1.3.1. Xét tập thương $\mathbb{Z}_m$ các lớp thặng dư môđun m . Khi đó

- (i) Với phép cộng $\mathbb{Z}_m$ trở thành một nhóm giao hoán.
- (ii) Với phép nhân $\mathbb{Z}_m$ trở thành một vị nhóm giao hoán.
- (iii) Với phép cộng và nhân, $\mathbb{Z}_m$ là một vành giao hoán có đơn vị $\bar{1}$.

Định nghĩa 1.3.2. $\mathbb{Z}_m$ được gọi là vành các lớp thặng dư theo môđun m . Lớp $\bar{a} \in \mathbb{Z}_m$ được gọi là lớp khả nghịch nếu có $\bar{b} \in \mathbb{Z}_m$ để $\bar{a} \cdot \bar{b} = \bar{1}$.

Định lý 1.3.3. Lớp $\bar{a} \in \mathbb{Z}_m$ là khả nghịch nếu và chỉ nếu $(\bar{a}, m) = 1$.

Chứng minh: Giả thiết lớp $\bar{a} \in \mathbb{Z}_m$ là khả nghịch. Khi đó có $\bar{b} \in \mathbb{Z}_m$ để $\bar{a} \cdot \bar{b} = \bar{1}$ hay $\overline{ab} = \bar{1}$. Như vậy $ab \equiv 1 \pmod{m}$, tức là có $x \in \mathbb{Z}$ để $ab + mx = 1$. Ta có $(\bar{a}, m) = (a, m) = 1$.

Ngược lại, giả sử $(\bar{a}, m) = (a, m) = 1$. Ta có $b, x \in \mathbb{Z}$ để $ab + mx = 1$. Vậy $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{1}$ và ta có lớp $\bar{a} \in \mathbb{Z}_m$ là khả nghịch.

Ký hiệu $\mathbb{Z}_m^*$ là tập các phần tử khả nghịch của vành các lớp thặng dư $\mathbb{Z}_m$.

Định lý 1.3.4. Tập $\mathbb{Z}_m^*$ là một nhóm giao hoán.

Chứng minh: Trước tiên ta chỉ ra $\mathbb{Z}_m^*$ đóng kín đối với phép nhân. Giả sử lớp $\bar{a}, \bar{b} \in \mathbb{Z}_m^*$. Theo Định lý 1.3.3 có $(\bar{a}, m) = 1, (\bar{b}, m) = 1$. Do đó $(\bar{a}\bar{b}, m) = 1$. Điều này chứng tỏ $\bar{a} \cdot \bar{b} \in \mathbb{Z}_m^*$ hay $\mathbb{Z}_m^*$ đóng kín đối với phép nhân. Hơn nữa, phép nhân các lớp thặng dư thỏa mãn luật kết hợp $\bar{1} \in \mathbb{Z}_m^*$. Do đó $\mathbb{Z}_m^*$ là một vị nhóm.

Ta chỉ ra, nếu lớp $\bar{a} \in \mathbb{Z}_m^*$ thì lớp $\bar{a}$ có nghịch đảo cũng thuộc $\mathbb{Z}_m^*$. Thật vậy, vì $\bar{a} \in \mathbb{Z}_m^*$ nên có $\bar{b} \in \mathbb{Z}_m$ để $\bar{a} \cdot \bar{b} = \bar{1}$. Hiển nhiên $\bar{b} \in \mathbb{Z}_m^*$ và $\bar{b}$ là nghịch đảo của $\bar{a}$. Tóm lại $\mathbb{Z}_m^*$ là một nhóm với phép nhân nói trên. Nhóm này

giao hoán vì phép nhân giao hoán.

Chú ý 1.3.5. Khi $m = p$ là số nguyên tố. Do đó $\mathbb{Z}_p$ là một trường và $\mathbb{Z}_p^*$ có $p - 1$ phần tử hay $\varphi(p) = p - 1$.

Ví dụ 1.3.6. Nhóm $\mathbb{Z}_9^* = \{\bar{1}, \bar{2}, \bar{2}^2 = \bar{4}, \bar{2}^3 = \bar{8}, \bar{2}^4 = \bar{7}, \bar{2}^5 = \bar{5}\}$ là một nhóm xiclic cấp 6. Từ đó suy ra $2^{2011} = 2^{6 \cdot 331 + 5}$ chia cho 9 dư 2.

Ví dụ 1.3.7. Nhóm $\mathbb{Z}_{15}^* = \{\bar{1}, \bar{2}, \bar{4}, \bar{8}, \bar{7}, \bar{11}, \bar{13}, \bar{14}\}$ là một nhóm cấp 8. Các phần tử của $\mathbb{Z}_{15}^*$ chỉ có cấp 2 hoặc cấp 4. Từ đó suy ra $28^{2011} = 28^{4 \cdot 502 + 3}$ chia cho 15 dư 7.

Ví dụ 1.3.8. Tìm tất cả các nghiệm nguyên của phương trình

$$x^3 + y^3 = z^6 + 3.$$

Bài giải: Nếu phương trình có nghiệm trong $\mathbb{Z}$ thì nó cũng có nghiệm trong $\mathbb{Z}_7$. Khi đó có $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_7$ để $\bar{x}^3 + \bar{y}^3 = \bar{z}^6 + \bar{3}$.

Trong $\mathbb{Z}_7$ có $\bar{0}^3 = \bar{0}, \bar{1}^3 = \bar{1}, \bar{2}^3 = \bar{1}, \bar{3}^3 = -\bar{1}, \bar{4}^3 = -\bar{1}, \bar{5}^3 = -\bar{1}, \bar{6}^3 = -\bar{1}$. Vậy $\bar{x}^3$ hay $\bar{y}^3$ chỉ có thể là $\bar{0}$ hoặc $\bar{1}$ hoặc $-\bar{1}$. Qua kiểm tra ta có $\bar{x}^3 + \bar{y}^3$ chỉ có thể là $\bar{0}, \bar{1}, \bar{2}, -\bar{1}, -\bar{2}$. Nhưng $\bar{z}^6 + \bar{3}$ chỉ có thể là $\bar{0} + \bar{3} = \bar{3}$ hoặc $\bar{1} + \bar{3} = \bar{4}$. Điều này chứng tỏ phương trình vô nghiệm.

Ví dụ 1.3.9. Xét hai dãy số $(x_n), (y_n)$ với $x_0 = 0, y_0 = 2$ và số hạng khác:

$$\begin{cases} x_{n+1} = 17x_n - 6y_n + 22 \\ y_{n+1} = 35x_n - 12y_n + 48, n \geq 0. \end{cases}$$

Chứng minh rằng $x_n \equiv 3^{n+2} - 1 \pmod{2^{n+3}}, y_n \equiv -5 \cdot 2^{n+2} + 1 \pmod{3^{n+1}}$.

Bài giải: Thực hiện phép biến đổi $\begin{cases} x_{n+1} + 1 = 17(x_n + 1) - 6(y_n - 1) \\ y_{n+1} - 1 = 35(x_n + 1) - 12(y_n - 1). \end{cases}$

Nếu coi $x_n + 1$ và $y_n - 1$ như a_n và b_n thì có biểu diễn sau đây

$$\begin{cases} a_0 = 1, b_0 = 1 \\ a_{n+1} = 17a_n - 6b_n \\ b_{n+1} = 35a_n - 12b_n \end{cases}$$

Quy nạp theo n chỉ ra công thức xác định như sau: $\begin{cases} a_n = -8 \cdot 2^n + 9 \cdot 3^n \\ b_n = -20 \cdot 2^n + 21 \cdot 3^n. \end{cases}$

Do vậy $x_n \equiv 3^{n+2} - 1 \pmod{2^{n+3}}, y_n \equiv -5 \cdot 2^{n+2} + 1 \pmod{3^{n+1}}$.

Chú ý 1.3.10. Biểu diễn dạng ma trận $\begin{pmatrix} a_{n+1} \\ b_{n+1} \end{pmatrix} = \begin{pmatrix} 17 & -6 \\ 35 & -12 \end{pmatrix} \begin{pmatrix} a_n \\ b_n \end{pmatrix}$.
 $V_i \begin{pmatrix} 17 & -6 \\ 35 & -12 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} -7 & 3 \\ 5 & -2 \end{pmatrix}$ nên ta có ngay biểu
 diễn $\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 5 & 7 \end{pmatrix} \begin{pmatrix} 2^n & 0 \\ 0 & 3^n \end{pmatrix} \begin{pmatrix} -7 & 3 \\ 5 & -2 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ hay có biểu diễn
 $\begin{pmatrix} x_n + 1 \\ y_n - 1 \end{pmatrix} = \begin{pmatrix} -8.2^n + 9.3^n \\ -20.2^n + 21.3^n \end{pmatrix}$ hay $\begin{cases} x_n = -8.2^n + 9.3^n - 1 \\ y_n = -20.2^n + 21.3^n + 1. \end{cases}$

Do vậy $x_n \equiv 3^{n+2} - 1 \pmod{2^{n+3}}$, $y_n \equiv -5.2^{n+2} + 1 \pmod{3^{n+1}}$.

Ví dụ 1.3.11. Ba dãy số $(x_n), (y_n), (z_n)$ xác định bởi các phương trình sau:

$$\begin{cases} x_0 = 12, y_0 = 8, z_0 = 16 \\ x_n = 30x_{n-1} + 21y_{n-1} - 21z_{n-1} \\ y_n = 14x_{n-1} + 23y_{n-1} - 14z_{n-1} \\ z_n = 28x_{n-1} + 28y_{n-1} - 19z_{n-1}, n \geq 1. \end{cases}$$

Hãy chứng minh $x_n : 2^{4n+2}, y_n : 2^{4n+3}, z_n : 2^{4n+4}$ và $x_n \not\vdots 2^{4n+3}, y_n \not\vdots 2^{4n+4}, z_n \not\vdots 2^{4n+5}$ với mọi $n \geq 0$.

Bài giải: Xét $x_n + ty_n = (30 + 14t)x_{n-1} + (21 + 23t)y_{n-1} - (21 + 14t)z_{n-1}$.

Chọn t sao cho $21 + 23t = t(30 + 14t)$ hay $2t^2 + t - 3 = 0$ và như vậy $t = 1$ hoặc $t = -\frac{3}{2}$. Với $t = -\frac{3}{2}$ ta có $x_n - \frac{3}{2}y_n = 9(x_{n-1} - \frac{3}{2}y_{n-1})$ và suy ra $x_n - \frac{3}{2}y_n = 9^n(x_0 - \frac{3}{2}y_0) = 9^n(12 - \frac{3}{2}8) = 0$. Ta nhận được $x_n = \frac{3}{2}y_n$. Xét $y_n + uz_n = (14 + 28u)x_{n-1} + (23 + 28u)y_{n-1} - (14 + 19u)z_{n-1}$. Chọn u sao cho $(23 + 28u)u = -14 - 19u$ hay $28u^2 + 42u + 14 = 0$ và như vậy $u = -1$ hoặc $u = -\frac{1}{2}$. Với $u = -\frac{1}{2}$ ta có $y_n - \frac{1}{2}z_n = 9(y_{n-1} - \frac{1}{2}z_{n-1})$ và suy ra $y_n - \frac{1}{2}z_n = 9^n(y_0 - \frac{1}{2}z_0) = 9^n(8 - \frac{1}{2}16) = 0$. Ta nhận được $y_n = \frac{1}{2}z_n$.

Tóm lại ta đã có $\begin{cases} x_n = \frac{3}{2}y_n \\ y_n = \frac{1}{2}z_n \end{cases}$ hay $\begin{cases} x_n = \frac{3}{4}z_n \\ y_n = \frac{1}{2}z_n, n \geq 0. \end{cases}$

Quy nạp theo n dễ dàng suy ra $x_n = 12.16^n, y_n = 8.16^n, z_n = 16.16^n$.

Tóm lại $x_n = 3.2^{4n+2}, y_n = 2^{4n+3}$ và $z_n = 2^{4n+4}$ thỏa mãn $x_n : 2^{4n+2}, y_n : 2^{4n+3}, z_n : 2^{4n+4}$ và $x_n \not\vdots 2^{4n+3}, y_n \not\vdots 2^{4n+4}, z_n \not\vdots 2^{4n+5}$ với mọi $n \geq 0$.

1.4 Định lý Euler và Định lý Fermat

Định lý 1.4.1. [Euler] Nếu $a, m \in \mathbb{Z}, m > 0, (a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Chứng minh: Vì $(a, m) = 1$ nên $\bar{a} \in \mathbb{Z}_m^*$. Giả sử $\mathbb{Z}_m^* = \{\bar{a}_1, \dots, \bar{a}_{\varphi(m)}\}$. Vì $\mathbb{Z}_m^*$ là một nhóm giao hoán hữu hạn theo Định lý 1.3.4, nên $\mathbb{Z}_m^* = \{\overline{a\bar{a}_1}, \dots, \overline{a\bar{a}_{\varphi(m)}}\}$. Nhân tất cả các phần tử của $\mathbb{Z}_m^*$ theo hai cách viết trên ta có $\prod_{i=1}^{\varphi(m)} \bar{a}_i = \bar{a}^{\varphi(m)} \prod_{i=1}^{\varphi(m)} \bar{a}_i$. Do $\prod_{i=1}^{\varphi(m)} \bar{a}_i$ khả nghịch nên $\bar{a}^{\varphi(m)} = \bar{1}$ hay $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Định lý 1.4.2. [Fermat bé] Nếu số nguyên a không chia hết cho số nguyên tố p thì $a^{p-1} \equiv 1 \pmod{p}$.

Chứng minh: Ta có $\varphi(p) = p-1$. Vì a không chia hết cho p nên $(a, p) = 1$. Theo Định lý 1.4.1, ta có $a^{p-1} \equiv 1 \pmod{p}$.

Hệ quả 1.4.3. Nếu p là số nguyên tố thì $a^p \equiv a \pmod{p}$ với mọi $a \in \mathbb{Z}$.

Chứng minh: Nếu a không chia hết cho p thì $a^{p-1} \equiv 1 \pmod{p}$ theo Định lý 1.4.2. Nhân hai vế với a ta nhận được $a^p \equiv a \pmod{p}$. Nếu a chia hết cho p , thì $a \equiv 0 \pmod{p}$ và lũy thừa p lần có $a^p \equiv 0 \pmod{p}$. Vậy $a^p \equiv a \pmod{p}$.

Định lý 1.4.4. [Wilson] Với số nguyên tố p có $(p-1)! + 1 \equiv 0 \pmod{p}$.

Chứng minh: Khi $p = 2$, kết quả là hiển nhiên. Khi $p > 2$, mỗi số nguyên n thỏa mãn $1 \leq n \leq p-1$ đều nguyên tố với p . Vậy có đúng một số nguyên s thỏa mãn $1 \leq s \leq p-1$ và $ns \equiv 1 \pmod{p}$. Ta có $\frac{p-1}{2}$ cặp (n, s) như vậy. Lấy tích $\frac{p-1}{2}$ các phương trình $ns \equiv 1 \pmod{p}$ với $n \geq 2$ như vậy được $2 \cdot 3 \cdot 4 \dots (p-3)(p-2) \equiv 1 \pmod{p}$. Nhân hai vế phương trình này với tích 1 và $p-1$ được $(p-1)! + 1 \equiv 0 \pmod{p}$.

Ví dụ 1.4.5. Phương trình $\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1 \equiv 0 \pmod{p}$ thỏa mãn với tất cả các số nguyên tố p dạng $4n+1$.

Bài giải: Theo Định lý 1.4.4 có $(p-1)! + 1 \equiv 0 \pmod{p}$ hay có thể viết

$$\prod_{k=1}^{p-1} k \prod_{k=1}^{p-1} (p-k) + 1 \equiv 0 \pmod{p}.$$

$$\text{Vậy } \left(\left(\frac{p-1}{2} \right)! \right)^2 + 1 = (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} k \prod_{k=1}^{\frac{p-1}{2}} (p-k) + 1 \equiv 0 \pmod{p}.$$

1.5 Một vài ví dụ tổng hợp

Ví dụ 1.5.1. *Tìm tất cả các nghiệm nguyên của phương trình sau đây:*

$$x^2 + 4y^4 = z^6 + 6.$$

Bài giải: Nếu phương trình trong có nghiệm trong $\mathbb{Z}$ thì nó cũng có nghiệm trong $\mathbb{Z}_8$. Khi đó có $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_8$ để $\bar{x}^2 + 4\bar{y}^4 = \bar{z}^6 + \bar{6}$. Trong $\mathbb{Z}_8$ có các hệ thức: $\bar{0}^2 = \bar{0}, \bar{1}^2 = \bar{1}, \bar{2}^2 = \bar{4}, \bar{3}^2 = \bar{1}, \bar{4}^2 = \bar{0}, \bar{5}^2 = \bar{1}, \bar{6}^2 = \bar{4}, \bar{7}^2 = \bar{1}$. Vậy $\bar{x}^2$ chỉ có thể là $\bar{0}$ hoặc $\bar{1}$ hoặc $\bar{4}$ và $4\bar{y}^4$ chỉ có thể là $\bar{0}$ hoặc $\bar{1}$. Qua kiểm tra ta có $\bar{x}^2 + 4\bar{y}^4$ chỉ có thể là $\bar{0}, \bar{1}, \bar{2}, \bar{4}, \bar{5}$. Nhưng $\bar{z}^6 + \bar{6}$ chỉ có thể là $\bar{0} + \bar{6} = \bar{6}$ hoặc $\bar{1} + \bar{6} = \bar{7}$. Điều này chứng tỏ phương trình vô nghiệm.

Ví dụ 1.5.2. *Giả sử A và B là hai số đều gồm 9 chữ số dương với tính chất: Nếu một chữ số bất kỳ của A được thay bởi một chữ số của B vào đúng vị trí tương ứng thì số nhận được chia hết cho 7. Chứng minh rằng số nhận được qua việc thay đổi chữ số của B bởi một chữ số của A vào đúng vị trí tương ứng cũng chia hết cho 7. Tìm một số nguyên $d > 9$ để tính chất trên còn đúng khi A và B là hai số đều gồm d chữ số dương.*

Bài giải: Biểu diễn duy nhất $A = a_d 10^d + a_{d-1} 10^{d-1} + \dots + a_1 10 + a_0$ và $B = b_d 10^d + b_{d-1} 10^{d-1} + \dots + b_1 10 + b_0$. Đặt $A^* = a_d 10^d + a_{d-1} 10^{d-1} + \dots + b_k 10^k + \dots + a_1 10 + a_0$ và số này chia hết cho 7 theo giả thiết. Vậy

$A^* - A \equiv -A \pmod{7}$ hay $10^k(b_k - a_k) \equiv -A \pmod{7}$ với bất kỳ số nguyên không âm k . Cho $k = 0, 1, \dots, d$ và cộng tất cả lại, ta nhận được $A - B \equiv dA \pmod{7}$. Ta chỉ ra kết quả đúng cho bất kỳ $\equiv 2 \pmod{7}$. Khi đó $A - B \equiv 2A \pmod{7}$ hay $A \equiv -B \pmod{7}$. Điều này chỉ ra $10^k(a_k - b_k) \equiv -B \pmod{7}$ với bất kỳ số nguyên không âm k . Do đó, khi thay một chữ số bất kỳ trong B bởi một chữ số bất kỳ tương ứng trong A ta cũng được một số chia hết cho 7.

Ví dụ 1.5.3. Cho số nguyên tố $p > 3$. Chứng minh rằng dư của phép chia số $\prod_{j=1}^p (j^2 + 1)$ cho p là 0 hoặc 4.

Bài giải: Ta xét trường hợp các lớp thặng dư $\mathbb{Z}_p$. Mở rộng trường thành trường $\mathbb{Z}_p[i]$ với $i^2 = -1$. Ta viết $\bar{j} \in \mathbb{Z}_p$ qua j , phân tích

$$\prod_{j=1}^p (j^2 + 1) = \prod_{j=1}^p (j + i) \cdot \prod_{j=1}^p (j - i) = f(i) \cdot f(-i),$$

trong đó $f(x) = \prod_{j=1}^p (j + x)$. Hiển nhiên $f(x) \equiv x^p - x$ trên $\mathbb{Z}_p$ và như vậy

$$\begin{aligned} \prod_{j=1}^p (j^2 + 1) &= (i^p - i)((-i)^p + i) = i(-i)[i^{p-1} - 1][(-i)^{p-1} - 1] \\ &= [(-1)^{\frac{p-1}{2}} - 1]^2. \end{aligned}$$

Do đó $\prod_{j=1}^p (j^2 + 1) = [(-1)^{\frac{p-1}{2}} - 1]^2$ chia cho p dư 0 hoặc 4.

Ví dụ 1.5.4. Cho số nguyên tố $p > 3$. Chứng minh rằng nếu dư của phép chia số p cho 8 bằng 1 thì $2^{\frac{p-1}{2}} - 1$ chia hết cho p .

Bài giải: Ta xét trường hợp các lớp thặng dư $\mathbb{Z}_p$. Mở rộng trường thành $\mathbb{Z}_p(\alpha)$ với $\alpha^4 = -1$. Khi đó trường $\mathbb{Z}_p(\alpha)$ có đặc số $p = 8t + 1, t \in \mathbb{N}^*$. Ta có $(\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1}$. Nhân hai vế với $\alpha + \alpha^{-1}$ ta nhận được hệ thức dưới đây:

$$[(\alpha + \alpha^{-1})^2]^{\frac{p+1}{2}} = (\alpha + \alpha^{-1})^2 = \alpha^2 + 2 + \alpha^{-2} = 2 + \frac{\alpha^4 + 1}{\alpha^2} = 2.$$

Từ $\alpha + \alpha^{-1})^2 = 2$ ta suy ra $2^{\frac{p+1}{2}} \equiv 2 \pmod{p}$ hay $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Ví dụ 1.5.5. Cho k là số nguyên dương lớn hơn 1. Dãy số $\{a_n\}$ xác định như sau: $a_1 = 1$, còn a_n là số nguyên dương thứ n lớn hơn a_{n-1} đồng dư với n theo môđun k . Tìm công thức tính a_n cho mọi n .

Bài giải: Theo giả thiết $a_1 \equiv 1 \pmod{k}$ và $a_n \equiv n \pmod{k}$, $a_n > a_{n-1}$ cho mọi n . Ta thấy số nguyên dương đầu tiên thỏa mãn điều kiện này là $a_{n-1} + 1$. Số nguyên dương thứ n lớn hơn a_{n-1} và đồng dư với n theo môđun k chính là $a_n = a_{n-1} + 1 + (n-1)k$. Từ công thức này ta suy ra $a_n = \frac{n[2 + (n-1)k]}{2}$.

Ví dụ 1.5.6. Cho p là số nguyên tố lớn hơn 2. Đặt $n(p) = p^{11} + p^{10} + \dots + p + 1$. Tìm dư của phép chia $n(p^{2016})$ cho $n(p)$.

Bài giải: Vì $p^{12} \equiv 1 \pmod{n(p)}$, nên $p^{2016} \equiv 1 \pmod{n(p)}$. Vậy $n(p^{2016}) \equiv n(1) \pmod{n(p)}$ hay dư của phép chia $n(p^{2016})$ cho $n(p)$ là 12.

Ví dụ 1.5.7. Với số nguyên $n \geq 2$ xét $p_n(x) = \binom{n}{2} + \binom{n}{5}x + \dots + \binom{n}{3k+2}x^k$ với phần nguyên $k = \lfloor \frac{n-2}{3} \rfloor$. Khi đó

(i) $p_{n+3}(x) = 3p_{n+2}(x) - 3p_{n+1}(x) + (x+1)p_n(x)$.

(ii) Tìm tất cả các số nguyên a để $3^{\lfloor \frac{n-1}{2} \rfloor}$ chia hết $p_n(a^3)$ với mọi $n \geq 3$.

Bài giải: (i) suy từ $\binom{n+3}{3m+2} = 3\binom{n+2}{3m+2} - 3\binom{n+1}{3m+2} + \binom{n}{3m+2} + \binom{n}{3m-1}$.

(ii) Nếu a thỏa mãn đầu bài thì $p_5(a^3) = 10 + a^3$ chia hết cho 9. Vậy $a \equiv -1 \pmod{3}$. Ngược lại, nếu $a \equiv -1 \pmod{3}$ thì $a^3 + 1 \equiv 0 \pmod{9}$. Vì $p_2(a^3) = 1$, $p_3(a^3) = 3$ và $p_4(a^3) = 6$ nên từ (i) ta suy ra $3^{\lfloor \frac{n-1}{2} \rfloor}$ chia hết $p_n(a^3)$ với mọi $n \geq 3$.

Ví dụ 1.5.8. Chứng minh rằng $\frac{3^n + (-1)^{\binom{n}{2}} - 2^{n+1}}{2} : 5$ với mọi số nguyên $n \geq 2$.

Bài giải: Vì $3^4 \equiv 1 \pmod{5}$ và $2^4 \equiv 1 \pmod{5}$ cùng $\binom{n+4}{2} \equiv \binom{n}{2} \pmod{2}$ nên khi đặt $f(n) = \frac{3^n + (-1)^{\binom{n}{2}}}{2} - 2^n$ ta sẽ có $f(n+4) \equiv f(n) \pmod{5}$. Kiểm tra $f(0) = f(1) = f(2) = 0$ và $f(3) = 5$ nên $f(n) : 5$ với

mọi số nguyên dương n .

Ví dụ 1.5.9. [DB-IMO1991] *Xác định tất cả các nghiệm nguyên dương của phương trình $3^x + 4^y = 5^z$.*

Bài giải: Giả sử $x > 0, y > 0, z > 0$ là nghiệm nguyên dương của phương trình đã cho. Khi đó $1 \equiv 5^z \equiv 2^z \pmod{3}$. Do vậy $z = 2z_1, z_1 \in \mathbb{N}$ và nhận được phương trình $(5^{z_1} - 2^y)(5^{z_1} + 2^y) = 3^x$. Từ đây có $\begin{cases} 5^{z_1} - 2^y = 1 \\ 5^{z_1} + 2^y = 3^x \end{cases}$

hay $\begin{cases} (-1)^{z_1} - (-1)^y \equiv 1 \pmod{3} \\ (-1)^{z_1} + (-1)^y \equiv 0 \pmod{3} \end{cases}$ từ phương trình đầu suy ra z_1 lẻ y

chẵn. Đặc biệt $y \geq 2$. Do đó $5^{z_1} \equiv 3^x \pmod{4}$ hay $3^x \equiv 1 \pmod{4}$. Như vậy x chẵn. Nếu $y > 2$ thì $2^y : 8$. Ta có ngay $5 \equiv 5^{z_1} \equiv 3^x \equiv 1 \pmod{8}$: mâu thuẫn. Tóm lại, $y = 2, z_1 = 1$ và như thế $x = 2$ hay $x = y = z = 2$.

Ví dụ 1.5.10. *Giả sử p là số nguyên tố lẻ. Đặt S_k là tổng của tất cả các tích gồm k số phân biệt từ tập $\{1, 2, \dots, p-1\}$. Chứng minh rằng $S_k : p$ với mọi k thỏa mãn $2 \leq k \leq p-2$ và $S_{p-1} + 1 : p$.*

Bài giải: Theo Định lý 1.4.2 có $x^{p-1} - 1 \equiv 0 \pmod{p}$ với $x = 1, 2, \dots, p-1$. Từ đây suy ra $x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-p+1) \pmod{p}$ và như thế $x^{p-1} - 1 \equiv x^{p-1} - S_1x^{p-2} + S_2x^{p-3} - \dots + (-1)^{p-1}S_{p-1} \pmod{p}$. Vậy $S_k : p$ với mọi k thỏa mãn $2 \leq k \leq p-2$ và $S_{p-1} + 1 : p$.

Ví dụ 1.5.11. *Giả sử hai số nguyên dương p và q thỏa mãn $(p, q) = 1$. Khi đó $p^{\varphi(q)} + q^{\varphi(p)} \equiv 1 \pmod{pq}$.*

Bài giải: Theo Định lý 1.4.1 ta có $(p^{\varphi(q)} - 1)(q^{\varphi(p)} - 1) \equiv 0 \pmod{pq}$ và $2^p \equiv 2 \pmod{p}$. từ đây suy ra $p^{\varphi(q)} + q^{\varphi(p)} \equiv 1 \pmod{pq}$.

Ví dụ 1.5.12. *Xác định tất cả các cặp số nguyên tố p và q thỏa mãn điều kiện $(5^p - 2^p)(5^q - 2^q) : pq$.*

Bài giải: Theo Định lý 1.4.2 ta có $5^p \equiv 5 \pmod{p}$ và $2^p \equiv 2 \pmod{p}$. Từ đây suy ra $5^p - 2^p \equiv 5 - 2 \pmod{p}$.

Nếu $(5^p - 2^p) : p$ thì $3 : p$. Vì p là số nguyên tố nên $p = 3$. Tương tự $q = 3$. Ta có cặp $(3, 3)$.

Nếu $p, q \neq 3$ thì $\begin{cases} 5^p - 2^p : q \\ 5^q - 2^q : p \end{cases}$ và $2^p \equiv 2 \pmod{p}$. Từ đây suy ra quan

hệ đồng dư $5^p - 2^p \equiv 5 - 2 \pmod{p}$.

Ví dụ 1.5.13. Dãy (a_n) xác định bởi $\begin{cases} a_0 = 1, a_1 = -1 \\ a_{n+2} = 7a_{n+1} - 6a_n, n \geq 0 \end{cases}$. Hãy

(i) Xác định a_n theo n .

(ii) Chứng minh $a_{n+1}^2 - 7a_{n+1}a_n + 6a_n^2 = 14 \cdot 6^n$ với mọi $n \geq 0$.

(iii) Chứng minh $a_n \not\equiv 10$ với mọi $n \geq 0$.

(iv) Chứng minh $a_{2012} + 13 \equiv 2011$.

Bài giải: (i) Đặt $b_n = a_{n-1}$ với mọi $n \geq 1$. Khi đó $\begin{cases} a_1 = -1, b_1 = 1 \\ a_{n+1} = 7a_n - 6b_n \\ b_{n+1} = a_n, n \geq 0 \end{cases}$

Do $a_{n+1} + tb_{n+1} = 7a_n - 6b_n + ta_n = (7+t)a_n - 6a_n$ nên ta sẽ chọn t sao cho $(7+t)t = -6$. Từ đó $t_1 = -1$ và $t_2 = -6$. Xét ánh xạ $a_{n+1} + tb_{n+1} = f(a_n + tb_n) = (7+t)(a_n + tb_n)$. Qua n lần f có $a_{n+1} + tb_{n+1} = f^n(a_1 + tb_1) = (7+t)^n(a_1 + tb_1)$. Thay $t = -1$ và $t = -6$ được hệ phương trình tuyến tính sau:

$$\begin{cases} a_n - b_n = -2 \cdot 6^{n-1} \\ a_n - 6b_n = -7. \end{cases}$$

Vậy $a_n = b_{n+1} = \frac{-2 \cdot 6^n + 7}{5}$ với mọi $n \geq 0$.

(ii) Vì $\begin{cases} a_{n+1} - b_{n+1} = -2 \cdot 6^n \\ a_{n+1} - 6b_{n+1} = -7 \end{cases}$ nên $a_{n+1}^2 - 7a_{n+1}a_n + 6a_n^2 = 14 \cdot 6^n$ mọi số nguyên $n \geq 0$.

(iii) Vì a_n luôn luôn là số nguyên lẻ nên $a_n \not\equiv 10$ với mọi $n \geq 0$.

(iv) Vì $5a_{2012} = -2 \cdot 6^{2012} + 7$ nên $5a_{2012} \equiv -65 \pmod{2011}$ hay $a_{2012} + 13 \equiv 2011$.

Ví dụ 1.5.14. Giả sử a_n được xác định bởi: $\begin{cases} a_0 = 2, a_1 = -9, a_2 = 5 \\ a_{n+3} = a_{n+2} + 4a_{n+1} - 4a_n \\ n \geq 0 \end{cases}$.

Chứng minh rằng $a_{2012} \equiv 1 \pmod{2^{2012}}$.

Bài giải: Phương trình $x^3 - x^2 - 4x + 4 = 0$ có ba nghiệm $x_1 = 1, x_2 = 2, x_3 = -2$. Dễ dàng suy ra $a_n = 1 - 2^{n+1} + 3(-2)^n$ với mọi $n \geq 0$. Vậy $a_{2012} \equiv 1 \pmod{2^{2012}}$.

Chương 2

Phương trình đồng dư

2.1 Phương trình đồng dư một ẩn

Định nghĩa 2.1.1. Cho m là số nguyên dương, $a_0, a_1, \dots, a_n$ là các số nguyên. Phương trình đồng dư dạng

$$(1) : \begin{cases} a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \equiv 0 \pmod{m} \\ a_0 \not\equiv 0 \pmod{m} \end{cases}$$

được gọi là *phương trình đồng dư bậc n* . Việc tìm tất cả các giá trị nguyên của x thỏa mãn (1) được gọi là *giải phương trình đồng dư*.

Định nghĩa 2.1.2. Cho phương trình đồng dư $f(x) \equiv 0 \pmod{m}$. Số $\alpha \in \mathbb{Z}$ được gọi là *một nghiệm đúng* của phương trình nếu $f(\alpha) \equiv 0 \pmod{m}$.

Định nghĩa 2.1.3. Nếu phương trình $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \equiv 0 \pmod{m}$, $a_0 \neq 0$, có nghiệm đúng α thì nó cũng nhận tất cả các y thuộc lớp $x \equiv \alpha \pmod{m}$ làm nghiệm. Khi đó ta nói lớp $x \equiv \alpha \pmod{m}$ là *nghiệm của phương trình*.

Chứng minh: Ta có $y - \alpha \equiv 0 \pmod{m}$. Vì $f(\alpha) \equiv 0 \pmod{m}$ nên $f(y) \equiv f(y) - f(\alpha) \equiv (y - \alpha)h(y, \alpha) \equiv 0 \pmod{m}$.

Chú ý rằng trong phương trình (1) ta có thể đưa tất cả các hệ số $a_0, a_1, \dots, a_n$ về các số không âm, nhỏ hơn m . Do $\mathbb{Z}_m$ chỉ có m lớp thặng dư nên *số nghiệm* của phương trình (1) là số các phần tử trong một hệ thặng dư đầy đủ theo môđun m hay trong hệ $\{0, 1, \dots, m-1\}$ thỏa mãn nó. Chú ý rằng, nếu m

là số đủ nhỏ thì ta chỉ cần thử lần lượt các phần tử thuộc $\{0, 1, \dots, m-1\}$ để tìm nghiệm; còn đối với m là số quá lớn thì số phép thử rất nhiều. Chẳng hạn, khi giải phương trình đồng dư $2x(2x+1)(2x+2) \equiv 0 \pmod{8}$, ta chỉ cần thử tất cả $0, 1, \dots, 7$. Tất cả đều thỏa mãn phương trình. Vậy mọi $\alpha \in \mathbb{Z}$ đều là nghiệm đúng.

Định nghĩa 2.1.4. Hai phương trình đồng dư được gọi là *tương đương* nếu chúng có cùng những giá trị nghiệm đúng.

Mệnh đề 2.1.5. Ta có một số phép biến đổi tương đương và hệ quả sau đây:

$$(i) \quad f(x) \equiv 0 \pmod{m} \Leftrightarrow f(x) + mb \equiv 0 \pmod{m}.$$

$$(ii) \quad f(x) \equiv 0 \pmod{m} \Leftrightarrow af(x) \equiv 0 \pmod{m}, \text{ với } (a, m) = 1.$$

$$(iii) \quad f(x) \equiv 0 \pmod{m} \Leftrightarrow af(x) \equiv 0 \pmod{am}, \text{ với } a > 0, a \in \mathbb{Z}.$$

$$(iv) \quad \text{Nếu } d \in uc(a_0, \dots, a_n) \text{ và } (d, m) = 1 \text{ thì}$$

$$f(x) \equiv 0 \pmod{m} \Leftrightarrow \frac{a_0}{d}x^n + \dots + \frac{a_n}{d} \equiv 0 \pmod{m}.$$

$$(v) \quad \text{Nếu } d \in uc(a_0, \dots, a_n, m) \text{ và } d > 0 \text{ thì}$$

$$f(x) \equiv 0 \pmod{m} \Leftrightarrow \frac{a_0}{d}x^n + \dots + \frac{a_n}{d} \equiv 0 \pmod{\frac{m}{d}}.$$

2.2 Phương trình đồng dư bậc nhất

Định nghĩa 2.2.1. *Phương trình đồng dư bậc nhất* là phương trình dạng sau đây:

$$(2) : \begin{cases} ax \equiv b \pmod{m} \\ a, b \in \mathbb{Z}, a \not\equiv 0 \pmod{m}. \end{cases}$$

Mệnh đề 2.2.2. *Nếu $(a, m) = 1$ thì phương trình (2) có đúng một nghiệm.*

Chứng minh: Theo Định lý 1.2.3, khi x chạy khắp một hệ thặng dư đầy đủ theo môđun m thì ax cũng chạy khắp một hệ thặng dư đầy đủ theo môđun m . Do đó có một và chỉ một giá trị x trong một hệ thặng dư đầy đủ theo môđun m để $ax \equiv b \pmod{m}$. Vậy phương trình đã cho có đúng một nghiệm.

Bổ đề 2.2.3. *Nếu $m = m_1 d$ thì lớp $x \equiv x_0 \pmod{m_1}$ là hợp của d lớp $x \equiv x_0 \pmod{m}, x \equiv x_0 + m_1 \pmod{m}, x \equiv x_0 + (d-1)m_1 \pmod{m}$.*

Mệnh đề 2.2.4. *Nếu $(a, m) = d$ thì phương trình (2) có nghiệm khi và chỉ khi $d \mid b$. Khi đó nó sẽ có d nghiệm.*

Chứng minh: Giả sử phương trình (2) có nghiệm. Khi đó tồn tại số nguyên x_0 sao cho $ax_0 \equiv b \pmod{m}$. Vậy $ax_0 = b + mt \Leftrightarrow ax_0 - mt = b$. Do đó $d \mid b$. Ngược lại, giả sử $d = (a, m) \mid b$. Khi đó $ax \equiv b \pmod{m}$ tương ứng với $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$. Vì $(\frac{a}{d}, \frac{m}{d}) = 1$ nên phương trình đã cho có nghiệm duy nhất $x \equiv x_0 \pmod{\frac{m}{d}}$. Vậy phương trình (2) có d nghiệm duy nhất $x \equiv x_0 + \frac{m}{d} \pmod{m}, \dots, x \equiv x_0 + (d-1)\frac{m}{d} \pmod{m}$.

Ví dụ 2.2.5. *Giải phương trình $12x \equiv 8 \pmod{20}$.*

Bài giải: Ta có $(12, 20) = 4$ và phương trình đã cho tương đương với $3x \equiv 2 \pmod{5}$. Trong một hệ thặng dư môđun 5 là $\{0, 1, 2, 3, 4\}$, phương trình này có một nghiệm đúng $x_1 = 4$. Vậy phương trình đã cho có nghiệm đúng là 4, 9, 14, 19 trong hệ thặng dư theo môđun 20.

Phương pháp giải $ax \equiv b \pmod{m}$

Theo lập luận trên, phương trình bậc nhất luôn đưa được về phương trình

dạng $ax \equiv b \pmod{m}$ với $(a, m) = 1$. Số nghiệm của phương trình đúng bằng 1. Do đó ta chỉ cần tìm một nghiệm $ax \equiv b \pmod{m}$, $(a, m) = 1$, $0 < a < m$, $b < m$. Sau đây ta nêu một số cách giải thường được sử dụng :

Thử qua một hệ thặng dư đầy đủ: Vì $(a, m) = 1$, nên khi x chạy qua một hệ thặng dư đầy đủ theo môđun a thì $mx + b$ cũng chạy qua một hệ thặng dư đầy đủ theo môđun a . Do đó với mỗi một hệ thặng dư đầy đủ theo môđun a có k để $mk + b \equiv 0 \pmod{a}$. Vậy $ax \equiv b \pmod{m}$ khi và chỉ khi $ax \equiv b + mk \pmod{m}$. Ta có nghiệm của phương trình $x \equiv \frac{b + mk}{a} \pmod{m}$.

Ví dụ 2.2.6. Giải phương trình $5x \equiv 4 \pmod{7}$.

Bài giải: Thử trên hệ thặng dư đầy đủ môđun 5 là $\{-2, -1, 0, 1, 2\}$ ta có $k = -2$ để $mk + b = 7 \cdot (-2) + 4 = -10 \equiv 0 \pmod{5}$. Vậy $x \equiv -2 \pmod{7}$.

Dùng thuật toán: Tìm $t \in \mathbb{Z}$ sao cho $a \mid b + mt$. Khi đó $x \equiv \frac{b + mt}{a} \pmod{m}$ là nghiệm. Việc tìm t dẫn tới việc giải phương trình $mt \equiv -b \pmod{a}$. Giả sử $m \equiv m_1 \pmod{a}$, $0 < m_1 < a$, $-b \equiv b_1 \pmod{a}$, $0 < b_1 < a$. Phương trình trên tương đương với $m_1 t \equiv b_1 \pmod{a}$. Rõ ràng sau một bước ta đã chuyển phương trình đã cho về phương trình với các hệ số nhỏ hơn. Quá trình sẽ dừng sau một số hữu hạn bước.

Ví dụ 2.2.7. Giải phương trình $37x \equiv 25 \pmod{117}$.

Bài giải: Tìm $t \in \mathbb{Z}$ sao cho $117t \equiv -25 \pmod{37}$. Khi đó $x \equiv \frac{25 + 117t}{37} \pmod{117}$ là nghiệm của phương trình. Việc tìm t dẫn tới giải phương trình $6t \equiv 12 \pmod{37}$. Tìm t_1 sao cho $37t_1 \equiv -12 \pmod{6} \Leftrightarrow t_1 \equiv 0 \pmod{6}$. Chọn $t_1 = 0$. Khi đó $t = \frac{12 + 37 \cdot t_1}{6} = 2$ là một nghiệm đúng của phương trình. Do đó $x \equiv \frac{25 + 117t}{37} \equiv 7 \pmod{117}$ là nghiệm của phương trình đang xét.

Áp dụng định lý Euler: Vì $a^{\varphi(m)} \equiv 1 \pmod{m}$ nên $a \cdot a^{\varphi(m)-1} b \equiv b \pmod{m}$. Vậy $x \equiv a^{\varphi(m)-1} b \pmod{m}$ là nghiệm của phương trình (2) .

Ví dụ 2.2.8. Giải phương trình $7x \equiv 5 \pmod{20}$.

Bài giải: Ta có $\varphi(20) = 8$ và phương trình có nghiệm $x \equiv 5 \cdot 7^7 \pmod{20}$.

Áp dụng liên phân số: Biểu diễn $\frac{m}{a} = [q_0; q_1, \dots, q_n]$. Ta có $aP_{n-1} - mQ_{n-1} = (-1)^n$. Như vậy $aP_{n-1} \equiv (-1)^n \pmod{m}$. Nghiệm của phương trình là $x \equiv (-1)^n bP_{n-1} \pmod{m}$.

Ví dụ 2.2.9. Giải phương trình $27x \equiv 13 \pmod{143}$.

Bài giải: Biểu diễn $\frac{143}{27} = [5; 3, 2, 1, 2]$. Khi đó $x \equiv 117 \pmod{143}$.

Ví dụ 2.2.10. Giải phương trình $9x \equiv 2 \pmod{41}$.

Bài giải: Ta có $41 = 9 \cdot 4 + 5$, $9 = 5 \cdot 1 + 4$, $5 = 4 \cdot 1 + 1$. Do đó $1 = 5 - 4 \cdot 1 = 5 - (9 - 5 \cdot 1) = -9 + 5 \cdot 2 = -9 + (41 - 9 \cdot 4) \cdot 2 = 9 \cdot (-9) + 41 \cdot 2$. Như vậy, phương trình có nghiệm $x \equiv -9 \cdot 2 \equiv -18 \pmod{41}$.

2.3 Hệ phương trình đồng dư một ẩn

Xét hệ các phương trình đồng dư dưới đây:

$$(3) : \begin{cases} f_1(x) \equiv 0 \pmod{m_1} \\ f_2(x) \equiv 0 \pmod{m_2} \\ \dots \\ f_n(x) \equiv 0 \pmod{m_n}, \end{cases}$$

trong đó $f_i(x) \in \mathbb{Z}[x]$, m_i là các số nguyên dương với $i = 1, 2, \dots, n$.

Định nghĩa 2.3.1. Phần tử $\alpha \in \mathbb{Z}$ được gọi là một nghiệm đúng của hệ (3) nếu $f_i(\alpha) \equiv 0 \pmod{m_i}$ với mọi $i = 1, 2, \dots, n$.

Mệnh đề 2.3.2. Nếu α là nghiệm đúng của hệ (3) thì mọi phần tử thuộc lớp $x \equiv \alpha \pmod{m}$ cũng là nghiệm của hệ với m là bội chung nhỏ nhất của $m_1, m_2, \dots, m_n$. Khi đó ta nói lớp $x \equiv \alpha \pmod{m}$ là một nghiệm của hệ (3).

Định nghĩa 2.3.3. Hai hệ phương trình được gọi là tương đương nếu chúng có cùng những giá trị nghiệm đúng. Giả sử mỗi phương trình $f_i(x) \equiv 0 \pmod{m_i}$ có nghiệm $x \equiv a_i \pmod{m_i}$. Khi đó nghiệm của hệ (3) chính

là nghiệm của hệ phương trình

$$(4) : \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n}. \end{cases}$$

Người đầu tiên nghiên cứu hệ phương trình đồng dư bậc nhất là nhà toán học Trung Hoa Sten-Zu vào khoảng thế kỷ thứ nhất trước công nguyên nên định lý sau được gọi là định lý Trung Hoa về dư.

Trong (3), giả sử các số nguyên dương $m_1, \dots, m_n$ là những số đôi một nguyên tố cùng nhau.

Định lý 2.3.4. [Định lý Trung Hoa về phần dư] *Hệ (3) có một nghiệm duy nhất theo môđun $m = \prod_{i=1}^n m_i$.*

Chứng minh: Đặt $M_i = \frac{m}{m_i}, i = 1, \dots, n$. Ta có $(M_i, m_i) = 1$ và $m_j | M_i$ cho mọi $j \neq i$. Vì $(M_i, m_i) = 1$ nên các phương trình $M_i y \equiv 1 \pmod{m_i}$ bao giờ cũng có nghiệm duy nhất $y \equiv N_i \pmod{m_i}$. Đặt

$$x_0 = M_1 N_1 a_1 + M_2 N_2 a_2 + \dots + M_n N_n a_n.$$

Ta có $x_0 \equiv M_i N_i a_i \equiv a_i \pmod{m_i}, i = 1, \dots, n$. Vậy x_0 là nghiệm đúng của hệ đã cho. Nếu x và x' đều nghiệm đúng hệ đã cho thì ta có $x - x' \equiv 0 \pmod{m_i}, i = 1, \dots, n$. Do đó $x - x' \equiv 0 \pmod{m}$. Ngược lại, nếu x nghiệm đúng hệ đã cho và $x' \equiv x \pmod{m}$ thì $x' \equiv x \pmod{m_i}, i = 1, \dots, n$. Vậy x' cũng nghiệm đúng hệ đã cho. Tóm lại, nghiệm của hệ (3) xác định theo môđun m là duy nhất.

Ví dụ 2.3.5. *Tìm số tự nhiên nhỏ nhất biết rằng khi chia nó cho 7, 5, 3, 11 ta lần lượt được các số dư 3, 2, 1, 9.*

Bài giải: Bài toán được đưa về dạng tìm số tự nhiên nhỏ nhất x thỏa mãn hệ

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 2 \pmod{5} \\ x \equiv 1 \pmod{3} \\ x \equiv 9 \pmod{11}. \end{cases}$$

Ta ký hiệu $m = 7.5.3.11 = 1155$, $M_1 = 5.3.11 = 165$, $M_2 = 7.3.11 = 231$, $M_3 = 7.5.11 = 385$, $M_4 = 7.5.3 = 105$. Xét phương trình đồng dư:

$$M_1x \equiv 1 \pmod{7} \Leftrightarrow 165x \equiv 1 \pmod{7} \Leftrightarrow 4x \equiv 1 \pmod{7}.$$

Chọn $N_1 = 2$ là một nghiệm đúng của phương trình đồng dư này. Tương tự $M_2x \equiv 1 \pmod{5}$ có một nghiệm đúng $N_2 = 1$; $M_3x \equiv 1 \pmod{3}$ có một nghiệm đúng $N_3 = 1$ và $M_4x \equiv 1 \pmod{11}$ có một nghiệm đúng $N_4 = 2$. Khi đó $x_0 = \sum_{i=1}^4 M_i N_i a_i = 165.2.3 + 231.1.2 + 385.1.1 + 105.2.9$. Từ $x_0 \equiv 262 \pmod{1155}$ ta suy ra số tự nhiên nhỏ nhất cần tìm là 262. Đối với hệ phức tạp

$$\begin{cases} b_1x \equiv a_1 \pmod{m_1} \\ b_2x \equiv a_2 \pmod{m_2} \\ \dots \\ b_nx \equiv a_n \pmod{m_n}. \end{cases}$$

Ta giải từng phương trình $b_ix \equiv a_i \pmod{m_i}$ có nghiệm $x \equiv c_i \pmod{m_i}$ cho mỗi $i = 1, \dots, n$. Hệ đã cho trở thành hệ dưới đây mà ta đã biết cách giải.

$$\begin{cases} x \equiv c_1 \pmod{m_1} \\ x \equiv c_2 \pmod{m_2} \\ \dots \\ x \equiv c_n \pmod{m_n}. \end{cases}$$

2.4 Phương trình đồng dư một ẩn bậc cao

Cho $m > 1$ là số nguyên dương. Xét phương trình đồng dư

$$(5) : \begin{cases} f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \equiv 0 \pmod{m} \\ a_0 \not\equiv 0 \pmod{m}, n > 1. \end{cases}$$

Định lý 2.4.1. Khi số m có sự phân tích chính tắc $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$

thành các thừa số nguyên tố, thì (5) tương đương với hệ phương trình đồng dư

$$(6) : \begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \dots \\ f(x) \equiv 0 \pmod{p_s^{\alpha_s}}. \end{cases}$$

Chứng minh: Giả thiết $x \equiv x_0 \pmod{m}$ là nghiệm của (5). Khi đó $f(x_0) \equiv 0 \pmod{m}$. Vì m là bội của các $p_i^{\alpha_i}$, nên ta cũng có

$$\begin{cases} f(x_0) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x_0) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \dots \\ f(x_0) \equiv 0 \pmod{p_s^{\alpha_s}}. \end{cases}$$

Như vậy $x \equiv x_0 \pmod{m}$ là một nghiệm của (6).

Ngược lại, giả thiết $x \equiv x_0 \pmod{m}$ là một nghiệm của (6). Khi đó $f(x_0) \equiv 0 \pmod{p_i^{\alpha_i}}, i = 1, \dots, s$. Do $f(x_0)$ chia hết cho các $p_i^{\alpha_i}$ và các $p_i^{\alpha_i}$ là nguyên tố khác đôi, nên $f(x_0)$ chia hết cho tích $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} = m$ hay $f(x_0) \equiv 0 \pmod{m}$, tức là (5) có nghiệm.

Chú ý 2.4.2: Việc giải phương trình (5) được thay bằng việc giải hệ (6). Nếu ta tìm được nghiệm của mỗi phương trình $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ là $x \equiv x_i \pmod{p_i^{\alpha_i}}$ cho mỗi $i = 1, \dots, s$, thì ta sẽ giải hệ

$$\begin{cases} x \equiv x_1 \pmod{p_1^{\alpha_1}} \\ x \equiv x_2 \pmod{p_2^{\alpha_2}} \\ \dots \\ x \equiv x_s \pmod{p_s^{\alpha_s}} \end{cases}$$

theo mục 6.3 để tìm hệ (6).

Thực ra để giải (5) ta chỉ cần giải các phương trình dạng dưới đây là đủ

$$(7) : \begin{cases} f(x) \equiv 0 \pmod{p^\alpha} \\ \alpha \in \mathbb{N}^+, p \text{ là số nguyên tố} \end{cases}$$

Ta bắt đầu công thức khai triển Taylor của hàm đa thức $f(x)$ bậc n tại

$x = a$ là

$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \cdots + \frac{f^{(i)}(a)}{i!}(x-a)^i + \cdots + \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

Dễ dàng chỉ ra $\frac{f^{(i)}(a)}{i!} \in \mathbb{Z}$ khi a là số nguyên. Thay $x = a + pt$ ta có $f(a + pt) = f(a) + \frac{f'(a)}{1!}pt + \frac{f''(a)}{2!}p^2t^2 + \cdots + \frac{f^{(n)}(a)}{n!}p^nt^n$.

Định lý 2.4.3. Xét phương trình (7) và phương trình (8) : $f(x) \equiv 0 \pmod{p}$ với p là số nguyên tố. Khi đó mỗi nghiệm của (7) cũng là nghiệm của (8). Ngược lại, mỗi nghiệm $x \equiv x_1 \pmod{p}$ của (8) với điều kiện $f'(x_1)$ không chia hết cho p cũng là một nghiệm của (7).

Chứng minh: Hiển nhiên, mỗi nghiệm của (7) cũng là nghiệm của (8). Giả sử $x_1 \equiv x_1 \pmod{p}$ là một nghiệm của (8). Khi đó $x = x_1 + pt_1$ với $t_1 \in \mathbb{Z}$. Thay nó vào phương trình $f(x) \equiv 0 \pmod{p^2}$ ta có $f(x_1 + pt_1) \equiv 0 \pmod{p^2}$. Theo công thức khai triển Taylor cho hàm đa thức ở vế trái $f(x_1) + pt_1f'(x_1) \equiv 0 \pmod{p^2}$. Chia hai vế cho p ta nhận được $\frac{f(x_1)}{p} + t_1f'(x_1) \equiv 0 \pmod{p}$ hay

$$\begin{cases} f'(x_1)t_1 \equiv -\frac{f(x_1)}{p} \pmod{p} \\ (f'(x_1), p) = 1, p \text{ là số nguyên tố} \end{cases}$$

Do $f'(x_1)$ không chia hết cho p , nên theo cách giải ở mục 6.3 phương trình có một nghiệm duy nhất $t_1 \equiv z_1 \pmod{p}$ hay $t_1 = z_1 + pt_2$. Khi đó $x = x_1 + pt_1 = x_1 + p(z_1 + pt_2)$ hay $x = (x_1 + pz_1) + p^2t_2 = x_2 + p^2t_2$. Thay x vào phương trình $f(x) \equiv 0 \pmod{p^3}$ ta có $f(x_2 + p^2t_2) \equiv 0 \pmod{p^3}$. Khai triển Taylor cho hàm đa thức ở vế trái, ta có

$$f(x_2) + p^2t_2f'(x_2) \equiv 0 \pmod{p^3}.$$

Chia tất cả cho p^2 phương trình trở thành $\frac{f(x_2)}{p^2} + t_2f'(x_2) \equiv 0 \pmod{p}$. $f'(x_2)$ không chia hết cho p , vì $x_2 \equiv x_1 \pmod{p}$ và như thế $f'(x_2) \equiv f'(x_1) \pmod{p}$. Ta lại coi đây là phương trình đồng dư bậc nhất theo t_2 . Lặp lại

y như vậy cho các trường hợp khác (7).

Trong trường hợp $f'(x_1)$ chia hết cho p , ta kiểm tra $f(x_1)$ có chia hết cho p hay không. Nếu $f(x_1)$ không chia hết cho p thì phương trình vô nghiệm; còn nếu nó chia hết cho p chúng ta xét $x = x_1, x = x_1 + pt_1, \dots, x = x_1 + (p-1)t_1$ theo môđun p^2 . Khi cả hai $f(x_1)$ và $f'(x_1)$ đều chia hết cho p^i thì ta xét phương trình đồng dư tương ứng theo môđun p^{i+1} . Lập lại y như vậy cho các trường hợp khác.

Ví dụ 2.4.4. Phương trình đồng dư $f(x) = x^4 + 2x^3 - 9x + 1 \equiv 0 \pmod{125}$.

Bài giải: Trước tiên xét $x^4 + 2x^3 - 9x + 1 \equiv 0 \pmod{5}$. Thử trên một hệ thặng dư đầy đủ, ta có $x \equiv 1 \pmod{5}$ và $x \equiv 2 \pmod{5}$ là nghiệm của phương trình. Ta có $f'(x) = 4x^3 + 6x^2 - 9$. Xét nghiệm $x \equiv 1 \pmod{5}$: Ta có $f'(1) = 1$ không chia hết cho 5. Đặt $x = 1 + 5t_1$. Ta có $f(1) + 5t_1f'(1) \equiv 0 \pmod{25}$ hay $-5 + 5t_1 \equiv 0 \pmod{25}$. Chia cho 5 ta có $t_1 \equiv 1 \pmod{5}$. Vậy $t_1 = 1 + 5t_2$ và $x = 1 + 5(1 + 5t_2) = 6 + 25t_2$. Thay $x = 6 + 25t_2$ vào phương trình đồng dư $f(x) = x^4 + 2x^3 - 9x + 1 \equiv 0 \pmod{125}$ và khai triển ta có $f(6) + 25t_2f'(6) \equiv 0 \pmod{125}$. Vậy $50 + 25t_2 \cdot 1071 \equiv 0 \pmod{125}$. Chia hai vế cho 25 ta được $2 + t_2 \cdot 1071 \equiv 0 \pmod{5}$ hay $t_2 \equiv 3 \pmod{5}$. Cuối cùng ta được $t_2 = 3 + 5t_3, t_3 \in \mathbb{Z}$ và $x = 81 + 125t_3$ với $t_3 \in \mathbb{Z}$.

Xét nghiệm $x \equiv 2 \pmod{5}$: Hoàn toàn tương tự ta có $x = 57 + 125t_3$ và $t_3 \in \mathbb{Z}$.

Tóm lại, phương trình đồng dư $f(x) = x^4 + 2x^3 - 9x + 1 \equiv 0 \pmod{125}$ có hai nghiệm $x \equiv 81 \pmod{125}$ và $x \equiv 57 \pmod{125}$.

Ví dụ 2.4.5. Phương trình đồng dư $f(x) = x^3 + 6x^2 - 1 \equiv 0 \pmod{81}$.

Bài giải: Xét $x^3 + 6x^2 - 1 \equiv 0 \pmod{3}$. Thử trên một hệ thặng dư đầy đủ, $x \equiv 1 \pmod{3}$ là nghiệm của phương trình. Ta có $f'(x) = 3x^2 + 12x$ và $f'(1) = 15$ chia hết cho 3. Lớp $x \equiv 1 \pmod{3}$ chia ra thành 3 lớp theo môđun 9 là $x \equiv 1 \pmod{9}, x \equiv 4 \pmod{9}, x \equiv 7 \pmod{9}$. Song cả 3

lớp này không có lớp nào là nghiệm của phương trình đồng dư $f(x) = x^3 + 6x^2 - 1 \equiv 0 \pmod{9}$ vì khi giải $f(1) + 3t_1f'(1) \equiv 0 \pmod{9}$ hay $6 + 3.t_1.15 \equiv 0 \pmod{9}$ có 6 không chia hết cho 9. Tóm lại, phương trình đồng dư $f(x) = x^3 + 6x^2 - 1 \equiv 0 \pmod{81}$ là vô nghiệm.

Ví dụ 2.4.6. Giải phương trình đồng dư $f(x) = x^3 + 6x^2 + 2 \equiv 0 \pmod{1323}$.

Bài giải: Vì $m = 3^3.7^2$, nên theo Định lý 2.4.1 phương trình đã cho tương đương với hệ phương trình đồng dư

$$\begin{cases} f(x) \equiv 0 \pmod{3^3} \\ f(x) \equiv 0 \pmod{7^2}. \end{cases}$$

Trước tiên ta giải phương trình $f(x) = x^3 + 6x^2 + 2 \equiv 0 \pmod{3^3}$: Xét $x^3 + 6x^2 + 2 \equiv 0 \pmod{3}$. Thử trên một hệ thặng dư đầy đủ, ta có $x \equiv 1 \pmod{3}$ là nghiệm của phương trình. Ta viết $x = 1 + 3t, t \in \mathbb{Z}$. Đạo hàm $f'(x) = 3x^2 + 12x$. Ta có $f(1) = 9, f'(1) = 15, f''(1) = 18$. Biểu diễn

$$f(1 + 3t) = f(1) + 3t \frac{f'(1)}{1!} + 9t^2 \frac{f''(1)}{2!} + \dots$$

hay $f(1 + 3t) = 9 + 45t + 81t^2 + \dots$ luôn chia hết cho 9 với mọi t nguyên. Ta viết $x \equiv 1 \pmod{3}$ thành $x = 1 + 9t_1, x = 4 + 9t_1, x = 7 + 9t_1, t_1 \in \mathbb{Z}$. Xét $x = 1 + 9t_1$. Ta có $f(1) + 9t_1f'(1) \equiv 0 \pmod{27}$ hay $9 + 135t_1 \equiv 0 \pmod{27} \Rightarrow 9 \equiv 0 \pmod{27} \Rightarrow x = 1 + 9t_1$ không thỏa mãn phương trình.

Xét $x = 4 + 9t_1$. Ta có $f(4) + 9t_1f'(4) \equiv 0 \pmod{27}$ hay $162 + 9.96t_1 \equiv 0 \pmod{27} \Rightarrow 0 \equiv 0 \pmod{27} \Rightarrow x = 4 + 9t_1$ luôn luôn không thỏa mãn phương trình.

Xét $x = 7 + 9t_1$. Ta có $f(7) + 9t_1f'(7) \equiv 0 \pmod{27}$ hay $637 + 9.231t_1 \equiv 0 \pmod{27} \Rightarrow 16 \equiv 0 \pmod{27} \Rightarrow x = 7 + 9t_1$ không thỏa mãn phương trình. Như thế, $f(x) \equiv 0 \pmod{3^3}$ có nghiệm $x = 4 + 27t_1, x = 13 + 27t_1, x = 22 + 27t_1$ với $t_1 \in \mathbb{Z}$.

Tiếp theo giải phương trình $f(x) = x^3 + 6x^2 + 2 \equiv 0 \pmod{7^2}$. Thử

trên một hệ thặng dư đầy đủ, ta có $x \equiv -1 \pmod{7}$ là nghiệm của $f(x) = x^3 + 6x^2 + 2 \equiv 0 \pmod{7}$. Viết $x = -1 + 7t, t \in \mathbb{Z}$. Đạo hàm $f'(x) = 3x^2 + 12x$. Ta có $f(-1) = 7, f'(-1) = -9$. Vì $f'(-1) = -9$ không chia hết cho 7, ta xét $f(-1) + 7tf'(-1) \equiv 0 \pmod{49}$ hay $7 - 7.9t \equiv 0 \pmod{49} \Rightarrow 1 + 5t \equiv 0 \pmod{7}$. Ta có $t = 4 + 7t_1$. Vậy $f(x) \equiv 0 \pmod{7^2}$ có nghiệm $x = -1 + 7t = -1 + 7(4 + 7t_1) = 27 + 49t_1$ với $t_1 \in \mathbb{Z}$.

Tóm lại, phương trình đã cho tương đương với ba hệ sau

$$\begin{cases} x \equiv 4 \pmod{27} \\ x \equiv 27 \pmod{49} \end{cases} \quad \begin{cases} x \equiv 13 \pmod{27} \\ x \equiv 27 \pmod{49} \end{cases} \quad \begin{cases} x \equiv 22 \pmod{27} \\ x \equiv 27 \pmod{49} \end{cases}.$$

Giải các hệ này, phương trình đồng dư $x^3 + 6x^2 + 2 \equiv 0 \pmod{1323}$ có 3 nghiệm là $\begin{cases} x \equiv 76 \pmod{1323}, \\ x \equiv 51 \pmod{1323} \\ x \equiv 958 \pmod{1323}. \end{cases}$

2.5 Phương trình đồng dư bậc cao theo môđun p

Định lý 2.5.1. *Phương trình đồng dư bậc n sau đây có không quá n nghiệm*

$$(9) : \begin{cases} f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n \equiv 0 \pmod{p} \\ a_0 \not\equiv 0 \pmod{p}, p \text{ là số nguyên tố} \end{cases}$$

Chứng minh: Ta chứng minh bằng phương pháp qui nạp theo bậc n . Nếu $n = 0$ thì phương trình đồng dư có dạng $a_0 \equiv 0 \pmod{p}$. Vì $a_0 \not\equiv 0 \pmod{p}$ nên phương trình đồng dư này vô nghiệm hay số nghiệm bằng 0. Giả sử phương trình đồng dư bậc $n > 0$ và định lý là đúng cho các phương trình đồng dư bậc $\leq n - 1$. Giả sử $f(x) \equiv 0 \pmod{p}$ có nghiệm $x \equiv x_0 \pmod{p}$. Khi đó $f(x_0) \equiv 0 \pmod{p}$ và ta có $f(x) \equiv f(x) - f(x_0) \equiv \sum_{i=0}^{n-1} a_i(x^{n-i} - x_0^{n-i}) \equiv 0 \pmod{p}$. Như vậy ta có phương trình đồng dư

$$(x - x_0)(a_0x^{n-1} + b_1x^{n-2} + \dots + b_{n-1}) \equiv 0 \pmod{p}.$$

Nếu $f(x) \equiv 0 \pmod{p}$ có một nghiệm khác nữa $x \equiv x_1 \pmod{p}$. Khi đó

$$(x_1 - x_0)(a_0x_1^{n-1} + b_1x_1^{n-2} + \cdots + b_{n-1}) \equiv 0 \pmod{p}.$$

Vì p là số nguyên tố và $x_1 \not\equiv x_0 \pmod{p}$, nên

$$a_0x_1^{n-1} + b_1x_1^{n-2} + \cdots + b_{n-1} \equiv 0 \pmod{p}.$$

Điều này chứng tỏ các nghiệm khác của phương trình đồng dư (9) là nghiệm của (10): $a_0x^{n-1} + b_1x^{n-2} + \cdots + b_{n-1} \equiv 0 \pmod{p}$. Vì bậc của (10) là $n - 1$ nên theo giả thiết qui nạp (10) có không nhiều hơn $n - 1$ nghiệm. Do đó (9) có không quá n nghiệm.

Hệ quả 2.5.2. *Nếu phương trình đồng dư $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \equiv 0 \pmod{p}$, với p là số nguyên tố, bậc không quá n có nhiều hơn n nghiệm thì tất cả các hệ số của nó phải chia hết cho p .*

Chứng minh: Nếu có một hệ số nào đó không chia hết cho p , chẳng hạn a_0 không chia hết cho p , thì phương trình này có không quá n nghiệm theo Định lý 2.5.1. Điều này mâu thuẫn với giả thiết. Từ Hệ quả 2.5.2 ta có định lý sau đây:

Định lý 2.5.3. [Wilson] *Nếu p là số nguyên tố thì*

$$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Chứng minh: Nếu $p = 2$, định lý là hiển nhiên. Nếu $p > 2$, ta xét phương trình đồng dư theo $\text{mod } p$.

$$\prod_{i=1}^{p-1} (x - i) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Phương trình này có bậc $\leq p - 2$ và nhận $\overline{1}, \dots, \overline{p - 1}$ làm nghiệm. Khi đó tất cả các hệ số của nó đều chia hết cho p theo Hệ quả 2.5.2. Vậy số hạng tự do chia hết cho p hay $(p - 1)! + 1 \equiv 0 \pmod{p}$.

Hệ quả 2.5.4. *Nếu số tự nhiên $p > 1$ thỏa mãn $(p - 1)! + 1 \equiv 0 \pmod{p}$*

thì p là số nguyên tố.

Chứng minh: Nếu p là hợp số thì có số nguyên tố q , với $p > q > 1$, là ước của p . Khi đó $(p-1)!$ chia hết cho q . Theo Định lý 2.5.3 ta có $(p-1)! + 1$ chia hết cho p , nhưng nó không chia hết cho q : mâu thuẫn. Vậy p là số nguyên tố.

Hệ quả 2.5.5. Nếu số nguyên tố p có dạng $4n+1$ thì $[(\frac{p-1}{2})!]^2 + 1 \equiv 0 \pmod{p}$.

Chứng minh: Theo Định lý 2.5.3 có $(p-1)! + 1 \equiv 0 \pmod{p}$ và suy ra

$$\begin{aligned} [(\frac{p-1}{2})!]^2 + 1 &\equiv (-1)^{\frac{p-1}{2}} [(\frac{p-1}{2})!]^2 + 1 \\ &\equiv \prod_{i=1}^{\frac{p-1}{2}} i \cdot \prod_{i=1}^{\frac{p-1}{2}} (p-i) + 1 = (p-1)! + 1 \equiv 0 \pmod{p}. \end{aligned}$$

Vậy $[(\frac{p-1}{2})!]^2 + 1 \equiv 0 \pmod{p}$.

2.6 Thặng dư bậc hai

Cho p là một số nguyên tố lẻ và phương trình đồng dư bậc hai

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

với a nguyên tố với p . Do p nguyên tố lẻ và $(a, p) = 1$, nên phương trình đồng dư bậc hai

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

được đưa về dạng tương đương

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

Đặt $y = 2ax + b$, $d = b^2 - 4ac$. Ta có phương trình $y^2 \equiv d \pmod{p}$.

Cho phương trình $x^2 \equiv a \pmod{p}$. Trong đó p là một số nguyên tố lẻ và a

nguyên tố với p .

Định nghĩa 2.6.1. Số nguyên a được gọi là *một thặng dư bậc hai theo môđun p* , hay *thặng dư toàn phương môđun p* , nếu phương trình đồng dư bậc hai $x^2 \equiv a(\text{mod } p)$ có nghiệm. Số nguyên a được gọi là *một bất thặng dư bậc hai môđun p* , hay *thặng dư phi toàn phương môđun p* , nếu phương trình đồng dư bậc hai $x^2 \equiv a(\text{mod } p)$ vô nghiệm.

Ví dụ 2.6.2. Xét một vài ví dụ sau:

(i) $x^2 \equiv 5(\text{mod } 11)$ có nghiệm $x \equiv \pm 4(\text{mod } 11)$. Vì $(5, 11) = 1$, nên 5 là một thặng dư bậc hai môđun 11.

(ii) $x^2 \equiv 2(\text{mod } 11)$ vô nghiệm. Vì $(2, 11) = 1$, nên 2 là một bất thặng dư bậc hai môđun 11.

Mệnh đề 2.6.3. Cho một số nguyên tố lẻ p và một số nguyên a nguyên tố với p . Khi đó

(i) Nếu a là một thặng dư bậc hai môđun p thì mọi phần tử thuộc lớp thặng dư $\bar{a}(\text{mod } p)$ cũng là thặng dư bậc hai môđun p .

(ii) Nếu a là một bất thặng dư bậc hai môđun p thì mọi phần tử thuộc lớp thặng dư $\bar{a}(\text{mod } p)$ cũng là bất thặng dư bậc hai môđun p .

Chứng minh: Do a là một thặng dư bậc hai môđun p . Khi đó tồn tại $x_0 \in \mathbb{Z}$ để

$$x_0^2 \equiv a(\text{mod } p).$$

Với $b \in \bar{a}$ có $b \equiv a(\text{mod } p)$ và suy ra $x_0^2 \equiv b(\text{mod } p)$. Như vậy, b cũng là một thặng dư bậc hai môđun p .

(ii) Giả sử a là một bất thặng dư bậc hai môđun p . Khi đó không tồn tại số nguyên x_0 nào để $x_0^2 \equiv a(\text{mod } p)$. Lấy $b \in \bar{a}$. Nếu có số nguyên x_0 để $x_0^2 \equiv b(\text{mod } p)$, thì $x_0^2 \equiv a(\text{mod } p)$. (mâu thuẫn.) Như vậy, b cũng là một bất thặng dư bậc hai môđun p .

Định lý 2.6.4. Nếu a là một thặng dư bậc hai modun p thì phương trình $x_0^2 \equiv a(\text{mod } p)$ có đúng hai nghiệm.

Chứng minh: Do a là một thặng dư bậc hai môđun p nên có $x_0 \in \mathbb{Z}$ để

$$x_0^2 \equiv a \pmod{p}.$$

Do

$$(-x_0)^2 = x_0^2 \equiv a \pmod{p},$$

nhên $x \equiv -x_0 \pmod{p}$ cũng là một nghiệm của phương trình đã cho. Giả sử $x_0 \equiv -x_0 \pmod{p}$. Khi đó ta có $2x_0 \equiv 0 \pmod{p}$. Vì p là một số nguyên tố lẻ nên $x_0 \equiv 0 \pmod{p}$ (mâu thuẫn). Vậy $x \equiv x_0 \pmod{p}$ và $x \equiv -x_0 \pmod{p}$ là hai nghiệm phân biệt của phương trình đã cho. Mà phương trình $x^2 \equiv a \pmod{p}$ có không quá hai nghiệm. Do vậy $x^2 \equiv a \pmod{p}$ chỉ có đúng hai nghiệm.

Ví dụ 2.6.5. Giải phương trình đồng dư $x^2 + 3x + 1 \equiv 0 \pmod{7}$.

Bài giải: Phương trình đồng dư bậc hai $x^2 + 3x + 1 \equiv 0 \pmod{7}$ được đưa về phương trình tương đương

$$4x^2 + 12x + 4 \equiv 0 \pmod{7}$$

hay

$$(2x + 3)^2 - 5 \equiv 0 \pmod{7}.$$

Đặt $y = 2x + 3$. Ta có phương trình $y^2 \equiv 5 \pmod{7}$. Vì phương trình này vô nghiệm, nên phương trình đã cho vô nghiệm.

Định lý 2.6.6. Trong một hệ thặng dư thu gọn môđun p có $\frac{p-1}{2}$ thặng dư bậc hai tương ứng cùng lớp với các thặng dư $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ và có $\frac{p-1}{2}$ bất thặng dư bậc hai.

Chứng minh: Các số

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

là những thặng dư bậc hai môđun p đôi một không cùng thuộc một lớp thặng dư môđun p . Thật vậy, phương trình

$$x^2 \equiv k^2 \pmod{p}$$

là thặng dư bậc hai môđun p đôi một không cùng thuộc một lớp thặng dư môđun p . Thật vậy, phương trình

$$x^2 \equiv k^2 \pmod{p}$$

với $1 \leq k \leq \frac{p-1}{2}$ có nghiệm

$$x \equiv \pm k \pmod{p}.$$

Giả sử $h^2 \equiv k^2 \pmod{p}$ với $1 \leq h, k \leq \frac{p-1}{2}$. Khi đó

$$(h - k)(h + k) \equiv 0 \pmod{p}$$

với $1 \leq k \leq \frac{p-1}{2}$. Do $(h + k, p) = 1$, nên $h \equiv k \pmod{p}$. Từ

$$h \equiv k \pmod{p}$$

và $h^2 \equiv k^2 \pmod{p}$, ta suy ra $h = k$.

Giả sử a là một thặng dư bậc hai môđun p . Khi đó trong hệ thặng dư thu gọn môđun p với giá trị tuyệt đối nhỏ nhất có số nguyên x_0 để

$$x_0^2 \equiv a \pmod{p}.$$

Do $1 \leq |x_0| \leq \frac{p-1}{2}$ nên khi lấy $k = |x_0|$, ta được $a \equiv k^2 \pmod{p}$. Như vậy a cùng lớp với

$$k^2 \in \left\{ 1^2, 2^2, \dots, \left(\frac{p-1}{2} \right)^2 \right\}.$$

Định lý 2.6.7. Cho một số nguyên tố lẻ p và một số nguyên a nguyên tố với p . Khi đó ta có:

(i) Nếu a là một thặng dư bậc hai môđun p thì $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(ii) Nếu a là một bất thặng dư bậc hai môđun p thì $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Chứng minh: (i) Giả sử a là một thặng dư bậc hai môđun p . Khi đó tồn tại $x_0 \in \mathbb{Z}$ với $(x_0, p) = 1$ để $x_0^2 \equiv a \pmod{p}$. Theo Định lý Euler

$$a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod{p}.$$

(ii) Giả sử a là một bất thặng dư bậc hai môđun p . Vì mỗi thặng dư bậc hai môđun p đều nghiệm đúng phương trình $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ và phương trình này có không quá $\frac{p-1}{2}$ nghiệm nên, trong một hệ thặng dư thu gọn môđun p có đúng $\frac{p-1}{2}$ nghiệm của phương trình này là các thặng dư bậc hai môđun p đều không nghiệm đúng phương trình này. Chính vì thế $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Điều này có nghĩa $(a^{\frac{p-1}{2}} - 1, p) = 1$. Vì a nguyên tố với p nên $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$. Như vậy

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

Tóm lại, ta có $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Hệ quả sau đây còn được gọi là *dấu hiệu Euler* về thặng dư bậc hai.

Hệ quả 2.6.8. Cho một số nguyên tố lẻ p và một số nguyên a nguyên tố với p . Khi đó:

(i) a là một thặng dư bậc hai môđun p khi và chỉ khi

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

(ii) a là một bất thặng dư bậc hai môđun p khi và chỉ khi

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Chương 3

Phương trình Mordell

3.1 Chuẩn trong vành $\mathbb{Z}[\sqrt{d}]$ và số học

Chuẩn trong vành $\mathbb{Z}[\sqrt{d}]$

Sử dụng vành $\mathbb{Z}[\sqrt{d}]$ đối với bài toán số học. Các kết quả sau đây dễ dàng có được qua kiểm tra trực tiếp.

Mệnh đề 3.1.1. *Giả thiết số dương $d \neq 1$ không là số chính phương. Khi đó*

(i) Tập $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Z}\}$ cùng phép cộng và nhân lập thành một vành giao hoán với đơn vị và ánh xạ $f : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}[\sqrt{d}], a + b\sqrt{d} \mapsto a - b\sqrt{d}$, là một tự đẳng cấu (liên hợp), có nghĩa: f là một song ánh và thỏa mãn $f(z_1 + z_2) = f(z_1) + f(z_2), f(z_1 z_2) = f(z_1)f(z_2)$ với mọi $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$.

(ii) Tập $\mathbb{Z}[\sqrt{-d}] = \{a + ib\sqrt{d} | a, b \in \mathbb{Z}\}$ cùng phép cộng và nhân lập thành một vành giao hoán với đơn vị và ánh xạ $f : \mathbb{Z}[\sqrt{-d}] \rightarrow \mathbb{Z}[\sqrt{-d}], a + ib\sqrt{d} \mapsto a - ib\sqrt{d}$, là một tự đẳng cấu (liên hợp), có nghĩa: f là một song ánh và thỏa mãn $f(z_1 + z_2) = f(z_1) + f(z_2), f(z_1 z_2) = f(z_1)f(z_2)$ với mọi $z_1, z_2 \in \mathbb{Z}[\sqrt{-d}]$.

Với $z = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ và $u = a + ib\sqrt{d} \in \mathbb{Z}[\sqrt{-d}]$ ta ký hiệu $N(z) = a^2 - db^2, N(u) = a^2 + db^2$ và gọi là chuẩn của z hay u . Khi đó có:

Hệ quả 3.1.2. *Với $z_1, z_2, \dots, z_n \in \mathbb{Z}[\sqrt{d}]$ và $u_1, u_2, \dots, u_n \in \mathbb{Z}[\sqrt{-d}]$ ta luôn có hệ thức*

$$\begin{aligned} N(z_1 z_2 \dots z_n) &= N(z_1) N(z_2) \dots N(z_n) \\ N(u_1 u_2 \dots u_n) &= N(u_1) N(u_2) \dots N(u_n). \end{aligned}$$

Chứng minh: Giả sử $\mathbb{Z}_k = a_k + b_k \sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ với $k = 1, \dots, n$, và viết tích $\prod_{k=1}^n (a_k + b_k \sqrt{d}) = a + b \sqrt{d}$. Qua tự đẳng cấu liên hợp có ngay $\prod_{k=1}^n (a_k - b_k \sqrt{d}) = a - b \sqrt{d}$. từ đây suy ra $N(z_1 z_2 \dots z_n) = N(z_1) N(z_2) \dots N(z_n)$ vì

$$a^2 - b^2 d = \prod_{k=1}^n (a_k + b_k \sqrt{d}) \prod_{k=1}^n (a_k - b_k \sqrt{d}) = \prod_{k=1}^n (a_k^2 - b_k^2 d).$$

Hoàn toàn tương tự ta cũng có $N(u_1 u_2 \dots u_n) = N(u_1) N(u_2) \dots N(u_n)$.

Mệnh đề 3.1.3. Giả thiết p, q là hai số nguyên dương không có nhân tử là số chính phương với $(p, q) = 1$. Khi đó tập $\mathbb{Z}[\sqrt{p}, \sqrt{q}] = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \mid a, b, c, d \in \mathbb{Z}\}$ cùng phép cộng và nhân lập thành một vành giao hoán với đơn vị và các ánh xạ dưới đây :

$$\begin{aligned} \phi_i : \mathbb{Z}[\sqrt{p}, \sqrt{q}] &\rightarrow \mathbb{Z}[\sqrt{p}, \sqrt{q}] \\ z = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} &\mapsto \begin{cases} \phi_1(z) = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \\ \phi_2(z) = a - b\sqrt{p} + c\sqrt{q} - d\sqrt{pq} \\ \phi_3(z) = a + b\sqrt{p} - c\sqrt{q} - d\sqrt{pq} \\ \phi_4(z) = a - b\sqrt{p} - c\sqrt{q} + d\sqrt{pq} \end{cases} \end{aligned}$$

là những tự đẳng cấu. Với $z \in \mathbb{Z}[\sqrt{p}, \sqrt{q}]$, đặt $N(z) = \phi_1(z)\phi_2(z)\phi_3(z)\phi_4(z)$.

Khi đó ta luôn có:

Hệ quả 3.1.4. Với $z_1, z_2 \in \mathbb{Z}[\sqrt{p}, \sqrt{q}]$ có hệ thức $N(z_1 z_2) = N(z_1) N(z_2)$.

Chứng minh: Với $z_1, z_2 \in \mathbb{Z}[\sqrt{p}, \sqrt{q}]$ có $z_1 z_2 \in \mathbb{Z}[\sqrt{p}, \sqrt{q}]$ và $\phi_i(z_1 z_2) = \phi_i(z_1) \phi_i(z_2)$. Vậy $N(z_1 z_2) = \prod_{i=1}^4 \phi_i(z_1) \prod_{i=1}^4 \phi_i(z_2) = N(z_1) N(z_2)$.

Mệnh đề 3.1.5. p, q là hai số nguyên dương không có nhân tử là số chính phương với $(p, q) = 1$. Khi đó $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. Đặc biệt ta còn có $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}[\sqrt{p}, \sqrt{q}]$.

Chứng minh: Vì $\sqrt{p} + \sqrt{q} \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ nên $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

Đặt $u = \sqrt{p} + \sqrt{q}$. Khi đó ta có hệ
$$\begin{cases} \sqrt{p} + \sqrt{q} = u \\ (p + 3q)\sqrt{p} + (q + 3p)\sqrt{q} = u^3. \end{cases}$$

Vậy $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(u)$ và như vậy $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \supset \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Tóm lại $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. Dễ dàng ta chỉ ra $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}[\sqrt{p}, \sqrt{q}]$.

Phương trình nghiệm nguyên với chuẩn

Bây giờ chúng ta sử dụng chuẩn và tự đẳng cấu để xét một vài bài toán về phương trình nghiệm nguyên.

Ví dụ 3.1.6. Với số nguyên dương n , giả sử các số $a_1, b_1, \dots, a_n, b_n, a, b \in \mathbb{Z}$ thỏa mãn quan hệ $\prod_{i=1}^n (a_i + b_i\sqrt{5}) = a + b\sqrt{5}$. Khi đó

$$(i) \prod_{i=1}^n (a_i^2 - 5b_i^2) = a^2 - 5b^2.$$

(ii) Giả sử $(9 + 4\sqrt{5})^n = a_n + b_n\sqrt{5}$. Ta có $a_n^2 - 5b_n^2 = 1$. Từ đó suy ra phương trình $x^2 - 5y^2 = 4$ có nhiều vô hạn nghiệm nguyên dương x, y .

Bài giải: (i) Xét vành giao hoán $\mathbb{Z}[\sqrt{5}] = \{r + s\sqrt{5} | r, s \in \mathbb{Z}\}$. Đồng cấu $f : \mathbb{Z}[\sqrt{5}] \rightarrow \mathbb{Z}[\sqrt{5}], r + s\sqrt{5} \mapsto r - s\sqrt{5}$, là một đẳng cấu. Tác động f lên hai vế $f(\prod_{i=1}^n (a_i + b_i\sqrt{5})) = f(a + b\sqrt{5})$ hay $\prod_{i=1}^n (a_i - b_i\sqrt{5}) = a - b\sqrt{5}$. Do

$$\text{đó } \prod_{i=1}^n (a_i + b_i\sqrt{5}) \prod_{i=1}^n (a_i - b_i\sqrt{5}) = (a + b\sqrt{5})(a - b\sqrt{5}) = a^2 - 5b^2.$$

(ii) Ta có $a_n^2 - 5b_n^2 = (9 + 4\sqrt{5})^n (9 - 4\sqrt{5})^n = 1$ theo (i). Đặt $x_n + y_n\sqrt{5} = (a_n + b_n\sqrt{5})(3 + \sqrt{5}) = (3a_n + 5b_n) + (a_n + 3b_n)\sqrt{5}$. Khi đó $x_n^2 - 5y_n^2 = (a_n^2 - 5b_n^2)(3^2 - 5 \cdot 1^2) = 4$ với mọi n . Như thế phương trình $x^2 - 5y^2 = 4$ có nhiều vô hạn nghiệm nguyên x, y . Khi x, y là nghiệm của $x^2 - 5y^2 = 4$ thì $\pm x, \pm y$ cũng là nghiệm. Do vậy $x^2 - 5y^2 = 4$ có nhiều vô hạn nghiệm nguyên dương x, y .

Ví dụ 3.1.7. Với bất kỳ số nguyên $n \geq 3$ đều có hai số nguyên lẻ x và y để $2^n = 7x^2 + y^2$.

Bài giải: Xét vành giao hoán $\mathbb{Z}[\sqrt{-7}] = \{r + is\sqrt{7} | r, s \in \mathbb{Z}\}$. Chuẩn của $z = r + is\sqrt{7}$ là $N(z) = r^2 + 7s^2 = (r + is\sqrt{7})(r - is\sqrt{7})$. Hiển nhiên

$N(z_1 z_2) = N(z_1)N(z_2)$, chứng minh như trong ví dụ 3.1.6. Bằng phương pháp qui nạp theo n để chỉ ra, với bất kỳ số nguyên $n \geq 3$ đều có hai số nguyên lẻ x và y để $2^n = 7x^2 + y^2$.

Với $n = 3$ có $2^3 = 8 = 1 + 7 = 1^2 + 7 \cdot 1^2$.

Giả sử đã có hai số nguyên lẻ x, y để $y^2 + 7x^2 = 2^n$ với số nguyên $n \geq 3$.

Với số nguyên $n + 1$ ta xét

$$\begin{aligned} z_1 &= (y + ix\sqrt{7})(1 + i\sqrt{7}) = (y + x - 8x) + i(x + y)\sqrt{7} \\ z_2 &= (y + ix\sqrt{7})(1 - i\sqrt{7}) = (y - x + 8x) + i(x - y)\sqrt{7}. \end{aligned}$$

Vì x, y là số lẻ nên $x = 2k + 1, y = 2h + 1$. Khi đó $x + y = 2(k + h + 1)$, $y - x = 2(h - k)$ và $(x + y) - (y - x) = 4k + 2$. Do đó trong hai số $x + y$ và $y - x$ chỉ có đúng một số chia hết cho 4.

Nếu $x + y$ chia hết cho 4 thì $\frac{y - x}{2}$ là số nguyên lẻ. Khi đó $z_3 = (\frac{y - x}{2} + 4x) + i\frac{x - y}{2}\sqrt{7}$ với $N(z_3) = \frac{N(y + ix\sqrt{7})N(1 - i\sqrt{7})}{4} = 2^n \cdot 2 = 2^{n+1}$.

Nếu $y - x$ chia hết cho 4 thì $\frac{y + x}{2}$ là số lẻ. Khi đó $z_4 = (\frac{x + y}{2} - 4x) + i\frac{x + y}{2}\sqrt{7}$ với $N(z_4) = \frac{N(y + ix\sqrt{7})N(1 + i\sqrt{7})}{4} = 2^n \cdot 2 = 2^{n+1}$.

Ví dụ 3.1.8. Với bất kỳ số nguyên $n \geq 1$ đều có hai số nguyên lẻ x và y để $4 \cdot 3^n = 11x^2 + y^2$.

Bài giải: Xét vành giao hoán $\mathbb{Z}[\sqrt{-11}] = \{r + is\sqrt{11} | r, s \in \mathbb{Z}\}$. Chuẩn của $z = r + is\sqrt{11}$ là $N(z) = r^2 + 11s^2 = (r + is\sqrt{11})(r - is\sqrt{11})$. Hiển nhiên $N(z_1 z_2) = N(z_1)N(z_2)$. Ta có một vài số cụ thể : $4 \cdot 3 = 12 = 11 \cdot 1^2 + 1^2$, $4 \cdot 3^2 = 36 = 11 \cdot 1^2 + 5^2$, $4 \cdot 3^3 = 108 = 11 \cdot 3^2 + 3^2$. Bằng phương pháp qui nạp theo n để chỉ ra, với bất kỳ số nguyên $n \geq 1$ đều có hai số nguyên lẻ x và y để $4 \cdot 3^n = 11x^2 + y^2$.

Với $n = 1$ có $4 \cdot 3 = 11 \cdot 1^2 + 1^2$.

Giả sử đã có hai số nguyên lẻ x, y để $11x^2 + y^2 = 4 \cdot 3^n$ với số nguyên $n \geq 1$.

Với số nguyên $n + 1$ ta xét

$$z_1 = (y + ix\sqrt{11}) (1 + i\sqrt{11}) = (y + x - 12x) + i(x + y)\sqrt{11}$$

$$z_2 = (y + ix\sqrt{11}) (1 - i\sqrt{11}) = (y - x + 12x) + i(x - y)\sqrt{11}.$$

Vì x, y là số lẻ nên $x = 2k + 1, y = 2h + 1$. Khi đó $x + y = 2(k + h + 1)$, $y - x = 2(h - k)$ và $(x + y) - (y - x) = 4k + 2$. Do đó trong hai số $x + y$ và $y - x$ chỉ có đúng một số chia hết cho 4.

Nếu $x + y$ chia hết cho 4 thì $\frac{y - x}{2}$ là số lẻ. Khi đó $z_3 = (\frac{y - x}{2} + 6x) + i\frac{x - y}{2}\sqrt{11}$ với $N(z_3) = \frac{N(y + ix\sqrt{11})N(1 - i\sqrt{11})}{4} = 4.3^n.3 = 4.3^{n+1}$.

Nếu $y - x$ chia hết cho 4 thì $\frac{y + x}{2}$ là số lẻ. Khi đó $z_4 = (\frac{x + y}{2} - 6x) + i\frac{x + y}{2}\sqrt{11}$ với $N(z_4) = \frac{N(y + ix\sqrt{11})N(1 + i\sqrt{11})}{4} = 4.3^n.3 = 4.3^{n+1}$. Tóm lại, đã chứng minh xong bài toán.

Ví dụ 3.1.9. Chứng minh rằng luôn tồn tại hai số nguyên x và y để

$$19^n = x^2 - 6y^2 \text{ với } \begin{cases} x \text{ lẻ và } y \text{ lẻ khi } n \text{ lẻ} \\ x \text{ lẻ và } y \text{ chẵn khi } n \text{ chẵn} \end{cases}$$

Bài giải: Xét vành giao hoán $\mathbb{Z}[\sqrt{6}] = \{r + s\sqrt{6} | r, s \in \mathbb{Z}\}$. Đồng cấu $f : \mathbb{Z}[\sqrt{6}] \rightarrow \mathbb{Z}[\sqrt{6}], r + s\sqrt{6} \mapsto r - s\sqrt{6}$, là một đẳng cấu. Do như vậy mà khi $(a + b\sqrt{6})(c + d\sqrt{6}) = u + v\sqrt{6}$ thì tác động f lên hai vế ta được $(a - b\sqrt{6})(c - d\sqrt{6}) = u - v\sqrt{6}$. Sử dụng kết quả này, với $z = a + b\sqrt{6}$ và đặt $N(z) = a^2 - 6b^2$ có ngay $N(z_1 z_2) = N(z_1)N(z_2)$. Với $n = 1$ có $19 = 5^2 - 6.1^2$ và $19^2 = 31^2 - 6.10^2$. Giả sử số nguyên $n \geq 1$ và hai số nguyên a, b để $19^n = a^2 - 6b^2$, trong đó a và b đều lẻ khi n lẻ, còn a lẻ và b chẵn khi n chẵn. Với $n + 1$ ta xét:

(ii) Nếu n lẻ thì có số a lẻ và số b lẻ để $a^2 - 6b^2 = 19^n$. Khi đó $n + 1$ là số chẵn và $19^{n+1} = (5a + 6b)^2 - 6(a + 5b)^2$ với $5a + 6b$ lẻ và $a + 5b$ chẵn.

(ii) Nếu n chẵn thì có số a lẻ và số b chẵn để $a^2 - 6b^2 = 19^n$. Khi đó $n + 1$ là số lẻ và $19^{n+1} = (5a + 6b)^2 - 6(a + 5b)^2$ với $5a + 6b$ lẻ và $a + 5b$ cũng lẻ. Tóm lại ta đã có điều cần chứng minh.

Tiếp theo là việc vận dụng tự đẳng cấu liên hợp để chứng minh phương trình vô nghiệm hoặc tìm giới hạn.

Ví dụ 3.1.10. *Tìm các số $x, y, z, t \in \mathbb{Z}$ thỏa mãn phương trình dưới đây:*

$$(x + y\sqrt{3})^4 + (z + t\sqrt{3})^4 = 20 + 12\sqrt{3}.$$

Bài giải: Giả sử có $x, y, z, t \in \mathbb{Z}$ thỏa mãn $(x + y\sqrt{3})^4 + (z + t\sqrt{3})^4 = 20 + 12\sqrt{3}$. Sử dụng tự đẳng cấu liên hợp của vành $\mathbb{Z}[\sqrt{3}]$ cho đồng nhất thức này có mâu thuẫn $(x - y\sqrt{3})^4 + (z - t\sqrt{3})^4 = 20 - 12\sqrt{3} < 0$.

3.2 Phương trình Mordell

3.2.1. Định nghĩa phương trình Mordell Phương trình dạng $y^2 = x^3 + k$ với $k \in \mathbb{Z}$ được gọi là *phương trình Mordell*.

3.2.2. Một vài phương trình có nghiệm nguyên

Mệnh đề 3.2.2.1. *Phương trình $x^3 = y^2 - 16$ chỉ có nghiệm nguyên $(0; \pm 4)$.*

Chứng minh: Ta có $x^3 = (y - 4)(y + 4)$. Nếu y lẻ nên $(y - 4, y + 4) = 1$. Vì $(y - 4)(y + 4) = x^3$ nên $y - 4$ và $y + 4$ nên $y - 4, y + 4$ đều là lập phương của số nguyên. Vì y lẻ và $+4 - y + 4 = 8$ nên y chẵn và suy ra x chẵn. Do $y^2 = x^3 + 16$ chia hết cho 8 nên y chia hết cho 4. Đặt $y = 4y_1$. Dễ dàng suy ra $x = 4x_1$. Như vậy $y_1^2 = 4x_1^3 + 1$ và suy ra $y_1 = 2z + 1$. Ta có $z^2 + z = x_1^3$. Vì $(z, z + 1) = 1$ nên $x_1 = 0$. Vậy $x = 0, y = \pm 4$ là nghiệm nguyên của phương trình.

Mệnh đề 3.2.2.2. *Có duy nhất $x, y \in \mathbb{Z}$ thỏa mãn $y^2 = x^3 - 1$ là $(x, y) =$*

$(1, 0)$.

Chứng minh: Trước tiên chúng ta kiểm tra tính chẵn lẻ của nghiệm. Giả sử x chẵn, vì vậy $y^2 + 1 = x^3 \equiv 0 \pmod{8}$. Khi đó $y^2 \equiv -1 \pmod{8}$. Nhưng $-1 \pmod{8}$ không là số chính phương, (mâu thuẫn). Nếu x lẻ thì y phải chẵn.

Phương trình $y^2 = x^3 - 1$ được viết thành $x^3 = y^2 + 1$. Trong $\mathbb{Z}[i]$ phân tích thành thừa số nguyên tố $x^3 = (y + i)(y - i)$.

Để thấy $y + i$ và $y - i$ nguyên tố cùng nhau, ta có $y + i = (m + ni)^3$ với $m, n \in \mathbb{Z}$. Khai triển lập phương và cho phần thực phần ảo hai vế bằng nhau ta được:

$$y = m^3 - 3mn^2 = m(m^2 - 3n^2), \quad 1 = 3m^2n - n^3 = n(3m^2 - n^2).$$

Khi đó ta được $n = \pm 1$. Nếu $n = 1$ thì $1 = 3m^2 - 1$ do đó $3m^2 = 2$, phương trình không có nghiệm nguyên. Nếu $n = -1$ thì $1 = -(3m^2 - 1)$ do đó $m = 0$. Vì vậy $y = 0$ suy ra $x^3 = y^2 + 1 = 1$. Vậy $x = 1$.

3.2.3. Một vài phương trình không có nghiệm nguyên

Không phải phương trình Mordell nào cũng có nghiệm nguyên. Một số kết quả dưới đây đã chỉ ra rằng nhiều phương Mordell không có nghiệm nguyên.

Mệnh đề 3.2.3.1. *Phương trình $x^3 = y^2 - 7$ không có nghiệm nguyên.*

Chứng minh: Giả sử phương trình trên có nghiệm nguyên. Từ $x^3 = y^2 - 7$ ta có $y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$. Nếu $2|x$ thì $8|x$, do đó $y^2 \equiv 7 \pmod{8}$: mâu thuẫn.

Nếu $x \equiv 1 \pmod{4}$ thì $x + 2 \equiv 3 \pmod{4}$. Do đó tồn tại một ước nguyên tố p của $(x + 2)$ sao cho $p \equiv 3 \pmod{4}$. Do đó $y^2 + 1 \equiv 0 \pmod{p}$. Theo ví dụ p của $x + 2$ sao cho $p \equiv 3 \pmod{4}$. Vậy phương trình vô nghiệm.

Nếu $x \equiv 3 \pmod{4}$ thì $x^3 \equiv 3 \pmod{8}$. Do đó $y^2 \equiv 2 \pmod{8}$: mâu thuẫn. Vậy phương trình vô nghiệm.

Mệnh đề 3.2.3.2. *Phương trình $x^3 = y^2 + 16$ không có nghiệm nguyên.*

Chứng minh: Giả sử phương trình có nghiệm nguyên. Từ giả thiết suy ra x, y có cùng tính chẵn lẻ.

Nếu x, y cùng chẵn, ta có $x = 2k, y = 2t$. Phương trình tương đương với $2k^3 = t^2 + 4$, suy ra $t = 2u$ và $k = 2v$. Do đó $4v^3 = u^2 + 1$, suy ra $v^2 \equiv 3 \pmod{4}$, (mâu thuẫn).

Nếu x, y cùng lẻ thì $x^2 \equiv y^2 \equiv 1 \pmod{8}$. Từ phương trình suy ra $x^3 \equiv 1 \pmod{8}$. Từ phương trình suy ra $x^3 \equiv 1 \pmod{8}$. ta biết rằng một số lẻ khi chia cho 8 có số dư chỉ có thể là 1, 3, 5, 7. Bằng cách thử trực tiếp suy ra $x \equiv 1 \pmod{8}$. Mặt khác từ phương trình trên ta có $y^2 + 8 = x^3 - 8 = (x - 2)(x^2 + 2x + 4)$.

Vì $x = 3$ không là nghiệm của phương trình nên $x > 3$. Giả sử p là một ước nguyên tố của $x - 2$. Ta có $y^2 \equiv -8 \pmod{p}$. Suy ra $1 = \left(\frac{-8}{p}\right) = \left(\frac{-2}{p}\right)$, do đó $p \equiv 1 \pmod{8}$ hoặc $p \equiv 3 \pmod{8}$. Do $x - 2$ là tích của các số nguyên tố có dạng trên nên suy ra $x - 2 \equiv 1 \pmod{8}$ hoặc $x - 2 \equiv 3 \pmod{8}$. Do đó $x \equiv 3 \pmod{8}$ hoặc $x \equiv 5 \pmod{8}$, (mâu thuẫn). Vậy phương trình đã cho vô nghiệm.

Mệnh đề 3.2.3.3. Phương trình $x^3 = y^2 - 6$ không có nghiệm nguyên.

Chứng minh: Giả sử phương trình đã cho có nghiệm x và y nguyên. Nếu x chẵn thì y chẵn và $y^2 \equiv 6 \pmod{8}$: vô lý, vì $6 \not\equiv 4$. Do vậy x và y đều lẻ. Nếu $y : 3$ thì $x^3 \equiv -6 \equiv 3 \pmod{9}$: mâu thuẫn, vì $x^3 \equiv 0$ hoặc $\equiv \pm 1 \pmod{9}$. Tóm lại, x, y lẻ và y không chia hết cho 3.

Trong vành $\mathbb{Z}[\sqrt{6}]$ ta có $x^3 = (y - \sqrt{6})(y + \sqrt{6})$. Gọi u là một ước chung của $y - \sqrt{6}$ và $y + \sqrt{6}$. Khi đó chuẩn $N(u) | y^2 - 6$ trong $\mathbb{Z}$. Vì u là ước của $y + \sqrt{6} - y + \sqrt{6} = 2\sqrt{6}$ nên $N(u) | 24$. Vì y lẻ và $N(u) | y^2 - 6$ nên $N(u)$ lẻ. Nếu $N(u) = \pm 3$ thì y chia hết cho 3: mâu thuẫn. Vì $N(u) = \pm 1$. Do đó u là ước của đơn vị và $y + \sqrt{6}, y - \sqrt{6}$ nguyên tố nhau. Vì $y + \sqrt{6}, y - \sqrt{6}$ nguyên tố cùng nhau và $x^3 = (y - \sqrt{6})(y + \sqrt{6})$ nên $y + \sqrt{6} = u(a + b\sqrt{6})^3$, trong đó u là ước của đơn vị, còn a và b nguyên. Vì các ước đơn vị đều có dạng $\pm(5 + 2\sqrt{6})^s, s \in \mathbb{Z}$, nên có ba khả năng xảy ra: $y + \sqrt{6} = (a + b\sqrt{6})^3$ hoặc $y + \sqrt{6} = (5 + 2\sqrt{6})(a + b\sqrt{6})^3$ hoặc $y + \sqrt{6} = (5 + 2\sqrt{6})^2(a + b\sqrt{6})^3$. Trường hợp: $y + \sqrt{6} = (a + b\sqrt{6})^3$. Khi đó $1 = 3a^2b + 6b^3$. Điều này không

thể xảy ra, do a, b nguyên.

Trường hợp $y + \sqrt{6} = (5 + 2\sqrt{6})(a + b\sqrt{6})^3$. Khi đó ta có $1 = 5(3a^2b + 6b^3) + 2(a^3 + 18ab^2)$. Từ đây suy ra $1 \equiv 2a^3 \pmod{3} \equiv 2a \pmod{3}$. Vậy $a \equiv 2 \pmod{3}$ và suy ra $a^2 \equiv 1 \pmod{3}$ và $a^3 \equiv 8 \pmod{9}$. Từ phương trình $1 = 5(3a^2b + 6b^3) + 2(a^3 + 18ab^2)$ và $a^2 \equiv 1 \pmod{3}$ và $a^3 \equiv 8 \pmod{9}$ ta suy ra $1 \equiv 5(3b + 6b^3) + 2.8 \pmod{9}$. Từ đây suy ra $b^3 + 2b + 2 \equiv 0 \pmod{3}$. Vì $b^3 + 2b \equiv 0 \pmod{3}$ nên $2 \equiv 0 \pmod{3}$: vô lý.

Trường hợp $y + \sqrt{6} = (5 + 2\sqrt{6})^2(a + b\sqrt{6})^3$. Khi đó có thể viết dạng $(5 + 2\sqrt{6})(y + \sqrt{6}) = (a + b\sqrt{6})^3$ hay $y + \sqrt{6} = (5 - 2\sqrt{6})(a + b\sqrt{6})^3$. Lấy liên hợp $y - \sqrt{6} = (5 + 2\sqrt{6})(a - b\sqrt{6})^3$. Từ đây suy ra $1 = 5(3a^2b + 6b^3) + 2[(-a)^3 + 18(-a)b^2]$. Phương trình này cũng không có nghiệm nguyên a, b . Tóm lại, $x^3 = y^2 - 6$ không có nghiệm nguyên.

3.3.3. Ứng dụng của thặng dư bậc 3

Một phương pháp khác là phương pháp sử dụng đồng dư thức cho số nguyên tố $p > 3$. Chúng ta gọi là đồng dư.

$$x^3 \equiv l \pmod{p}, \quad (l, p) = 1$$

luôn giải được nếu $p \equiv 2 \pmod{3}$.

Nếu $p \equiv 1 \pmod{3}$ khả năng giải được đòi hỏi điều kiện trên l , gọi l là thặng dư bậc ba của p được viết $(l/p)_3 = 1$ và vì vậy $l^{(p-1)/3} \equiv 1 \pmod{p}$. Nếu $l = 2$ trở thành điều kiện tồn tại của các số nguyên r, s sao cho

$$r^2 + 27s^2 = p$$

Nếu $l = 3$, điều kiện là

$$r^2 + 243s^2 = 4p$$

Bây giờ chúng ta chứng minh

Mệnh đề 3.5.1. Cho phương trình

$$y^2 = x^3 + k, k = 2a^3 - 3b^2 \quad (10)$$

không có nghiệm nguyên nếu a, b là các số nguyên, $ab \neq 0, a \not\equiv 1 \pmod{3}, b \not\equiv 0 \pmod{3}$, và nếu khi $b \equiv 0 \pmod{2}$ thì $a \equiv 1 \pmod{2}$; nếu 2 là thặng dư bậc ba của các số nguyên tố lẻ $p \equiv 1 \pmod{3}$.

Chứng minh: Được viết $x^3 + 2a^3 = y^2 + 3b^2$

Các số nguyên tố có thể chia được ở vế trái là những thừa số nguyên tố phổ biến của x và $a, 2, 3$, các số nguyên tố $q \equiv 2 \pmod{3}$ và các số nguyên tố $p \equiv 1 \pmod{3}$ sao cho $(2/p)_3 = 1$.

Đầu tiên chúng ta đặt vế trái là L là nguyên tố với 6. Sao cho $x = 2x_1$ khi đó $y \equiv b \pmod{2}$ vậy là hoặc $y \equiv b \equiv 0 \pmod{2}$ hoặc $y \equiv b \equiv 1 \pmod{2}$.

Trường hợp thứ nhất không thể làm được vì $a \equiv 1 \pmod{2}$. Trường hợp thứ hai cho $x^3 + 3a^3 \equiv 4 \pmod{8}$ và trường hợp này cũng không thể giải được.

Tiếp theo nếu $x^3 + 2z^3 \equiv 0 \pmod{3}, y \equiv 0 \pmod{3}$ và vì vậy $x^3 + 2z^3 \equiv 3 \pmod{9}$. Cũng không thể giải được vì $a^3 \equiv 0, -1 \pmod{9}$. Giả sử số nguyên tố $q \equiv 2 \pmod{3}$ chia hết cho L thì $y \equiv b \equiv 0 \pmod{q}$. Do đó chúng ta có thể viết $y = Qy_1, b = Qb_1$ trong đó Q là thương của q chia cho L . Khi đó Q^2 phải chia hết cho cả hai vế của phương trình (10) và thừa số nguyên tố duy nhất của L là các số nguyên tố dạng $p = A^2 + 27B^2$.

Khi đó phép nhân trong trường $Q(\sqrt{-3})$ là duy nhất, chúng ta có

$$(y_1 + b_1\sqrt{-3}) p^\alpha = \prod_p (A + B\sqrt{-27}) = C + D\sqrt{-27}$$

Trong đó $p = \frac{1}{2}(-1 + \sqrt{-3}), \alpha = 0, \pm 1$. Nếu $\alpha = 0$ thì $b_1 \equiv 0 \pmod{3}$ trái với giả sử. Nếu $\alpha = \pm 1, y_1 + b_1 \equiv 0 \pmod{2}$ và khi đó $L \equiv 0 \pmod{2}$ và điều này bị loại trừ.

Trường hợp cho $k = 51$ với $a = 3, b = 1$ và $k = 13$ với $a = 2, b = 1$.

Kết quả tương tự là

Mệnh đề 3.5.2. Cho phương trình

$$x^3 + 4a^3 = y^2 + 3b^2, ab \neq 0(11)$$

không có nghiệm nguyên nếu $b \equiv \pm 1(\text{mod } 6)$, $a \equiv 0, 2(\text{mod } 6)$ và không có thừa số nguyên tố $p \equiv 1(\text{mod } 3)$.

Sử dụng biến thức bậc ba của chương 3 được cho bởi.

Mệnh đề 3.5.3. Cho phương trình

$$x^3 + 3a^3 = y^2 + 3b^2(12)$$

không có nghiệm nguyên nếu $k/3 = a^3 - 3b^2 \not\equiv 0(\text{mod } 3)$ trừ phi một trong những cái của $b, b \pm (1 - k)$ chia hết cho 3 cũng chia hết cho 9.

Chứng minh: Vế bên trái chia hết cho 3, điều này đòi hỏi $y \equiv 0(\text{mod } 3)$, $x \equiv 0(\text{mod } 3)$, $a^3 - b^2 \equiv 0(\text{mod } 3)$. Do đó

$$y \equiv \pm 1(\text{mod } 3), x^3 \equiv 1(\text{mod } 3), x^3 \equiv 1(\text{mod } 9)$$

và sau đó

$$y^2 \equiv 1 + k(\text{mod } 9), y \equiv \pm(1 - k)(\text{mod } 9).$$

Do đó số chia duy nhất của vế trái là ước chung của x và a , các số nguyên tố $p \equiv 1(\text{mod } 3)$ mà 3 là thặng dư bậc ba và các số nguyên tố $q \equiv 2(\text{mod } 3)$. Nếu q là số chia thì $(-3/q = 1)$, $y \equiv 0(\text{mod } q)$, $b \equiv 0(\text{mod } q)$.

Do đó

$$x^3 + 3a^3 = Q^2(y_1^2 + 3b_1^2)$$

Trong đó Q là tích của các số nguyên tố q . Thừa số Q^2 chia ra và vì vậy

$$(y_1 + b_1\sqrt{-3})p^\alpha = \prod_p \left(\frac{A + B\sqrt{-243}}{2} \right) = \frac{C + D\sqrt{-243}}{2}$$

Trong đó C, D là các số nguyên và $\alpha = 0, \pm 1$.

Nếu $\alpha = 0, b_1 \equiv 0 \pmod{9}$ và vì vậy $b \equiv 0 \pmod{9}$. Nếu $\alpha = \pm 1, y_1 \pm b_1 \equiv 0 \pmod{9}$ và vì vậy $y \pm b \equiv 0 \pmod{9}$

Định lý bây giờ trở thành $y \equiv \pm(1 - k) \pmod{9}$.

Được minh họa bởi $y^2 = x^3 - 24$ trong đó $24 = 3.3^2 - 3^2.1^3$

Kết luận

Trong luận văn này chúng tôi đã trình bày được.

- $\mathbb{Z}_m$ là một vành giao hoán có đơn vị, $\mathbb{Z}_m^*$ là một nhóm nhân.
- Chứng minh được định lý Euler và định lý Fermat.
- Trình bày chi tiết việc giải một dạng phương trình đồng dư. Chứng minh được định lý Wilson.
- Trình bày được phương trình Mordell. Đã chỉ ra một số dạng phương trình có nghiệm hoặc vô nghiệm. Trình bày được thặng dư bậc ba.

Tài liệu tham khảo

Tài liệu tiếng Việt

- [1] Dương Quốc Việt(Chủ biên) - Đàm Văn Nhĩ(2008) *Cơ sở lý thuyết số và đa thức*, NXB Đại học Sư phạm Hà Nội.

Tài liệu tiếng Anh

- [2] L.G Mordell(1947). *A Chapter in the Theory of Numbers*. Cambridge Univ.
- [3] L.G Mordell(1969). *Diophantine equations*. ST. John's college Cambridge, England. Chapter 26.