Chương 7

ĐƯỜNG CONG ELLIPTIC

§1 Định nghĩa.

Chương này nhằm trình bày những khái niệm cơ bản của một đối tượng rất quan trọng của lí thuyết số và hình học đại số: các đường cong elliptic. Về mặt lịch sử, các đường cong elliptic xuất hiện lần đầu tiên trong các nghiên cứu về tích phân elliptic (từ đó có tên gọi của đường cong). Các đường cong này có mặt trong nhiều lĩnh vực khác nhau của toán học vì nó rất phong phú về mặt cấu trúc. Một mặt, đó là đường cong không kì dị, tức là các đa tạp một chiều. Mặt khác, các điểm của đương cong lập thành một nhóm Aben. Vì thế hầu như mọi công cụ của toán học đều được áp dụng vào nghiên cứu đường cong elliptic. Ngược lại, những kết quả về đường cong elliptic có ý nghĩa quan trọng đối với nhiều vấn đề khác nhau. Xin chỉ ra một vài ví dụ. Về mặt lí thuyết, định lí lớn Fermat đã được chứng minh (trong công trình của A. Wiles) bằng cách chứng minh giả thuyết Taniyama-Weil về các đường cong elliptic. Về mặt ứng dụng, rất gần đây, các đường cong elliptic được dùng trong việc xây dựng một số hệ mật mã khoá công khai.

Để có thể trình bày tương đối sâu về đường cong elliptic, chúng ta cần nhiều hiểu biết về hình học đại số. Bởi vậy, chúng tôi chỉ có thể đề cập ở đây những khái niệm cơ bản nhất. Mục đích của chương chỉ là làm thế nào để độc giả có thể hình dung lí do tại sao đường cong elliptic lại có nhiều ứng dụng như vậy. Mặt khác, chúng tôi cũng giới thiệu sơ lược một vài thuật toán liên quan đến đường cong elliptic trên trường hữu hạn. Trong khi trình bày, cũng giống như các phần khác của cuốn sách, chúng tôi luôn cố gắng dùng ngôn ngữ "sơ cấp" nhất có thể. Bởi vậy, đôi khi phải bỏ qua chứng minh. Độc giả nào quan tâm sâu hơn về các đường cong elliptic, có thể tìm đọc trong các tài liệu [Ha], [Sil].

Định nghĩa 7.1. *Đường cong elliptic trên trường K* là tập hợp các điểm *(x,y)* thoả mãn phương trình

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, \qquad (7.1)$$

với một điểm O gọi là *điểm tại vô cùng (*sẽ nói rõ về sau). Hơn nữa, phương trình (7.1) phải thoả mãn điều kiện *không kì dị*, tức là, nếu viết nó dưới dạng *F(x,y)=0* thì tại mọi điểm *(x,y)* thoả mãn phương trình, có ít nhất một trong các đạo hàm riêng $\partial F/\partial x, \partial F/\partial y$ khác 0.

Điều kiện không kì dị nói trên tương đươmg với điều kiện, nếu xét tập hợp các điểm nói trên như một đường cong, thì đường cong đó không có điểm bội. Như vậy, nếu biểu diễn y^2 như là một đa thức bậc 3 của x, thì đa thức đó không có nghiệm bội.

Chú ý rằng, phương trình trên đây không duy nhất: trong nhiều trường K, có thể tìm được "dạng tối thiểu" của phương trình biểu diễn đường cong.

Nếu ta xét phương trình (7.1) với các hệ số trong Z, thì vì Z có thể nhúng vào trong mọi trường K tuỳ ý nên có thể xét phương trình trên như là phương trình trong trường K. Một điều cần lưu ý ngay: phương trình đó có thể thoả mãn điều kiện không kì dị đối với trường này, nhưng lại không thoả mãn điều kiện đó đối với trường khác. Chẳng hạn, nếu trường đang xét có đặc trưng 2 thì ta có $(x^2)'=0$ với mọi x!

Điểm tại vô cùng nói trong định nghĩa là điểm vô cùng trong đường cong xạ ảnh tương ứng. Ta xét không gian xạ ảnh P^2, tức là không gian mà các điểm là các lớp tương đương của các bộ ba (x,y,z), trong đó x, y, z không đồng thời bằng 0, và bộ ba (x,y,z) tương đương với bộ ba $(\lambda x, \lambda y, \lambda z)$, $\lambda \neq 0$. Như vậy, nếu $z \neq 0$ thì lớp tương đương của (x,y,z) chứa bộ ba $(x/z,y/z,1)$. Ta có thể đồng nhất mặt phẳng xạ ảnh P^2 với mặt phẳng thông thường (aphin) cùng với các "điểm tại vô hạn" ứng với $z=0$.

Một đường cong trong mặt phẳng thông thường có thể tương ứng với đường cong trong mặt phẳng xạ ảnh bằng cách thêm vào các điểm tại vô cùng. Để làm việc đó, trong phương trình xác định đường cong, ta chỉ cần thay x bởi x/z, y bởi y/z và nhân hai vế của phương trình với một luỹ thừa thích hợp của z để khử mẫu số.

Ví dụ. Đường cong elliptic với phương trình (7.1) được thêm vào các điểm tại vô cùng để có đường cong tương ứng trong không gian xạ ảnh:

$$y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz^2+a_6z^3, \qquad (7.2)$$

Định lí sau đây cho ta thấy có thể định nghĩa phép cộng các điểm trên đường cong elliptic để trang bị cho nó cấu trúc nhóm Aben.

Định lí 7.2. *Xét đường cong elliptic xác định trên trường tuỳ ý bởi phương trình*

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6, \qquad (7.3)$$

Ta có thể trang bị cho tập hợp các điểm của đường cong cấu trúc nhóm Aben cộng tính như sau:

-Phần tử 0 là điểm tại vô cùng; (0,1,0).

-Điểm với toạ độ (x_1,y_1) có nghịch đảo là điểm với toạ độ($x_1,-y_1-a_1x_1-a_3$).

- Nếu hai điểm $P_1=(x_1,y_1)$ và $P_2 = (x_2,y_2)$ không phải là nghịch đảo của nhau thì $P_1+P_2=P_3$, $P_3 =(x_3,y_3)$xác đinh như sau.

Đặt

$$m=\frac{y_1-y_2}{x_1-x_2}, \text{ nếu } P_1 \neq P_2 \ ;$$

$$m=\frac{3x_1^2+2a_2x_1+a_4-a_1x_1}{2y_1+a_1x_1+a_3}, \text{ nếu } P_1=P_2.$$

và tính x_3,y_3 theo công thức

$$x_3=-x_1-x_2-a_2+m\,(m+a_1),$$

$$y_3=-y_1-a_3-a_1x_3+m\,(x_1-x_2)$$

Chứng minh. Bằng tính toán trực tiếp dựa vào phương trình xác định đường cong, dễ kiểm tra định nghĩa phép cộng trên đây thoả mãn các tiên đề của nhóm Aben.

Để thấy rõ ý nghĩa hình học của định nghĩa phép cộng trên đây, ta xét trường hợp quan trọng sau đây của các đường cong elliptic trên trường thực *R*.

§2. Đường cong elliptic trên trường thực. Trước tiên, ta có nhận xét sau đây. Trong những trường với đặc trưng khác 2 và 3, phương trình (7.1) có thể đưa về dạng

$$Y^2=4X^3+c_4X+c_6. \qquad (7.4)$$

Thật vậy, chỉ cần dùng phép đổi biến:

$$Y=2y+a_1x+a_3$$

$$X=x+(a_1^2+4a_2)/12$$

Để đơn giản, ta thường dùng dạng sau đây, gọi là *dạng Weierstrass* của đường cong:

$$y^2=x^3+a_4x+a_6.$$

Trong trường hợp này, biệt thức Δ của đường cong là

$$\Delta =-16(4a_4^3+27a_6^2)$$

Như vậy, điều kiện để đường cong không có kì dị (không có điểm bội)là:

$$4a_4^3+27a_6^2 \neq 0.$$

Ta sẽ sử dụng dạng Weierstrass của đường cong. Bằng tính toán trực tiếp tọa độ các điểm theo công thức đã cho trong định lí 7.2, ta có thể thấy luật cộng trong nhóm lập bởi các điểm của đường cong có mô tả hình học sau đây:

Nếu các điểm *P* và *Q* của đường cong có toạ độ *x* khác khác nhau thì đường thẳng đi qua *P* và *Q* sẽ cắt đường cong tại một điểm thứ ba. Điểm đối xứng với giao điểm đó qua trục hoành chính là diểm *P+Q*.

Trong trường hợp *P* và *Q* có cùng hoành độ, tung độ của chúng sẽ là các giá trị đối nhau, và *P,Q* là hai điểm đối xứng nhau qua trục hoành. Khi đó đường thẳng đi qua *P,Q* sẽ "cắt" đường cong tại vô cùng: đó chính là điểm 0 của nhóm cộng các điểm, và P,Q là các phần tử nghịch đảo của nhau.

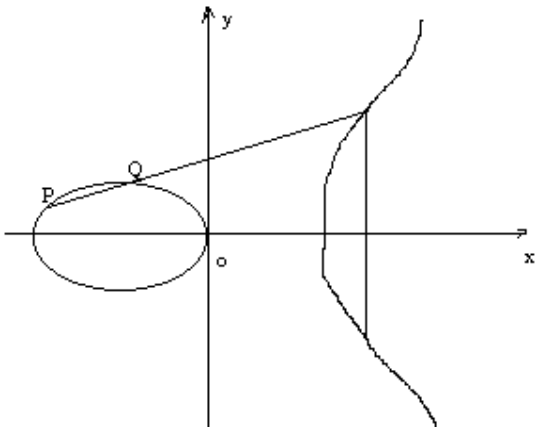
Rõ ràng "cộng" *P* với 0, thực hiện bằng cách nối *P* với điểm tại vô cùng bằng đường thẳng song song với trục tung sẽ cắt đường cong tại điểm đối xứng với *P* qua trục hoành, và như vậy *P+0=P*.

Trên hình 1 ta minh hoạ những điều vừa nói trên qua ví dụ đường cong với phương trình $y^2=x^3-x$.

Vì các điểm của đường cong là các phần tử của một nhóm cộng Aben, ta sẽ dùng kí hiệu *NP* để chỉ phần tử nhận được bằng cách cộng liên tiếp *N* lần điểm *P*.

Định nghĩa 7.3. Điểm *P* của đường cong được gọi là *điểm bậc hữu hạn* nếu tồn tại số nguyên dương *N* sao cho *NP=0*. Số *N* nhỏ nhất thoả mãn điều kiện đó gọi là bậc của *P*.

Dĩ nhiên không phải mọi điểm của đường cong đều có bậc hữu hạn.



Hình 1. Đường cong elliptic $y^2=x^3-x$ trên trường thực

§3. Đường cong elliptic trên trường các số hữu tỷ.

Trong rất nhiều vấn đề của Hình học đại số và số học, ta thường phải làm việc với các đường cong trên trường số hữu tỷ. Đó là các đường cong cho bởi phương trình (7.2), trong đó các hệ số là các số hữu tỷ, và ta cũng chỉ xét các điểm với toạ độ là các số hữu tỷ. Nghiên cứu đường cong elliptic trên trường số hữu tỷ cũng có nghĩa là nghiên cứu tập hợp nghiệm hữu tỷ của phương trình (7.2), một vấn đề quan trọng của số học. Trong phần cuối chương, ta sẽ thấy rằng, vấn đề này còn liên quan đến chứng minh định lí lớn Fermat.

Giả sử *E* là đường cong elliptic đã cho. Ta kí hiệu qua *E(Q)* tập hợp các điểm có toạ độ hữu tỷ. Như ta đã thấy, tập hợp này có cấu trúc nhóm Aben. Các điểm bậc hữu hạn của nhóm Aben *E(Q)* lập thành nhóm con $E(Q)_{tors}$, gọi là *nhóm con xoắn* của *E(Q)*. Khi đó, *E(Q)* sẽ là tổng trực tiếp của $E(Q)_{tors}$ với nhóm con các điểm bậc vô hạn. Định lí nổi tiếng của Mordell nói rằng nhóm con các điểm bậc vô hạn chỉ có hữu hạn phần tử sinh, và do đó đẳng cấu với nhóm Z^r, trong đó *r* là một số nguyên không âm. Số *r* gọi là hạng của đường cong, và là một đặc trưng hết sức quan trọng, chứa nhiều thông tin số học về đường cong. Chứng minh các kết luận này đòi hỏi phải sử dụng nhiều kiến thức sâu sắc về hình học đại số,và do đó vượt ra ngoài khuôn khổ của cuốn sách. Ta hạn chế ở đây phát biểu của định lí Mordell.

Định lí (Mordell). *Giả sử E là một đường cong elliptic trên Q. Khi đó tập hợp các điểm của E với toạ độ hữu tỷ E(Q) là một nhóm Aben hữu hạn sinh. Nói cách khác, ta có:*

$$E(Q)= E(Q)_{tors} \oplus Z^r,$$

trong đó r là một số nguyên không âm.

Nhóm con xoắn các điểm bậc hữu hạn của một đường cong có thể tính được không khó khăn lắm, trong khi hạng r lại hết sức khó xác định. Thậm chí, ngay đối với một đường cong cụ thể, chỉ ra r bằng 0 hay khác 0 cũng là một điều hết sức khó khăn. Ta có thể thấy ngay rằng, nếu $r=0$ thì đường cong đang xét chỉ có hữu hạn điểm hữu tỷ, trong trường hợp $r \neq 0$, tồn tại vô hạn điểm hữu tỷ trên đường cong. Điều đó tương đương với việc phương trình đã cho có hữu hạn hay vô hạn nghiệm hữu tỷ, một bài toán khó của số học.

Trong §5, ta sẽ thấy rằng, bài toán tìm điểm hữu tỷ của đường cong elliptic liên quan đến việc thành lập những hệ mật mã kiểu mới, cũng như các thuật toán khai triển nhanh số nguyên cho trước thành thừa số nguyên tố. Đó là những ứng dụng gần đây nhất của lí thuyết đường cong elliptic vào các vấn đề thực tiễn.

Như đã nói ở trên, việc xác định nhóm con xoắn của đường cong elliptic không phải là khó khăn. Tuy nhiên, việc chỉ ra tất cả các khả năng của các nhóm con đó (chỉ tồn tại 15 khả năng khác nhau) lại là một bài toán khó, và mới được giải quyết năm 1977 bằng định lí nổi tiếng sau đây của B. Mazur.

Định lí Mazur. *Giả sử E là đường cong elliptic trên trường Q. Khi đó nhóm con xoắn của $E(Q)$ đẳng cấu với một trong 15 nhóm sau đây :*

$$Z/mZ, \text{ trong đó } 1 \leq m \leq 10, \text{ hoặc } m=12.$$

$$Z/2Z \times Z/2mZ, \text{ với } 1 \leq n \leq 4$$

Như vậy, nhóm xoắn của đường cong elliptic có không quá 16 phần tử.

§4. Đường cong elliptic trên trường hữu hạn.

Để chứng minh một phương trình (hệ số nguyên) nào đó không có nghiệm nguyên, một trong những phương pháp thường được dùng là như sau. Ta xét phương trình mới, nhận được từ phương trình đã cho bằng cách thay các hệ số của nó bởi các thặng dư modulo một số p nào đó. Nếu phương trình này không có nghiệm (đồng dư modulo p) thì phương trình xuất phát cũng không có nghiệm. Việc làm đó được gọi là *sửa theo modulo p*. Rõ ràng rằng phương trình mới đơn giản hơn phương trình đã cho, hơn nữa, để xét nghiệm đồng dư modulo p, ta chỉ cần thử với hữu hạn giá trị. Nếu phương trình đã cho quả thật vô nghiệm, thì trong trường hợp chọn số p một cách may mắn, ta có thể đi đến kết luận đó khá dễ dàng.

Khi nghiên cứu các đường cong elliptic, đặc biệt là các đường cong trên trường số hữu tỷ, người ta cũng thường dùng phương pháp tương tự: sửa theo modulo p. Việc làm đó dẫn đến các đường cong trên trường hữu hạn.

Ta cần lưu ý ngay một điều. Khi "sửa" một đường cong elliptic bằng cách chuyển các hệ số thành các đồng dư modulo p, ta có thể nhận được một đường cong có kì dị. Thật vậy, biệt thức của đường cong (khác không) có thể đồng dư 0 modulo p, và khi đó, đường cong nhận được có điểm bội trên trường hữu hạn. Tuy nhiên, rõ ràng điều đó chỉ xảy ra khi p là một ước số của biệt thức của đường cong xuất phát, và do đó, chỉ xẩy ra với một số hữu hạn giá trị của p. Ta nói đường cong elliptic đã cho có *sửa xấu* tại những giá trị của p đó, và có *sửa tốt* tại những giá trị p khác.

Điều cần quan tâm đầu tiên khi nghiên cứu một đường cong elliptic trên trường hữu hạn là: đường cong đó có bao nhiêu điểm? Giả sử E là đường cong elliptic trên trường F_q có q phần tử. Các điểm của đường cong là các cặp (x,y), $x, y \in F_q$ thoả mãn phương trình trong F_q:

$$y^2=x^3+a_4x+a_6$$

Như vậy, nếu với giá trị x, $x^3+a_4x+a_6$ là một thặng dư bình phương modulo q thì sẽ có hai điểm (x,y) và $(x,-y)$ thuộc đường cong. Trong trường hợp ngược lại, không có điểm nào của đường cong ứng với giá trị x. Từ đó, khi q là số nguyên tố, theo định nghĩa của kí hiệu Legendre, số điểm của đường cong ứng với giá trị x là

$$1+\left[\frac{x^3+a_4x+a_6}{q}\right]$$

Thêm điểm tại vô cùng, ta có công thức tính số điểm của đường cong trong trường hợp q là số nguyên tố:

$$\#E(F_q)=1+\sum_{x\in F_q}1+\left[\frac{x^3+a_4x+a_6}{q}\right]$$

Trong trường hợp q không phải là số nguyên tố, trong công thức trên đây, thay cho kí hiệu Legedre, ta hiểu đó là kí hiệu Jacobi, và dấu đẳng thức được thay thế bởi bất đẳng thức $\leq$.

Định lí trên đây cho ta một ước lượng của số điểm của đường cong E trên trường F_q.

Định lí Hasse. *Giả sử N là số điểm của đường cong elliptic xác định trên trường F_q. Khi đó ta có:*

$$|N-(q+1)| \leq 2\sqrt{q}\,.$$

Bạn đọc có thể tìm thấy chứng minh của định lí này trong [Sil].

Một trong những ứng dụng mới nhất của đường cong elliptic trên trường hữu hạn, xuất hiện trong những năm gần đây, là các hệ mật mã khoá công khai elliptic. Phần tiếp theo được dành để trình bày vấn đề đó.

§5. Đường cong elliptic và hệ mật mã khoá công khai.

5.1. Hệ mật mã khoá công khai sử dụng đường cong elliptic dựa trên độ phức tạp của thuật toán tìm số nguyên x sao cho $xB=P$, trong đó P, B là các điểm cho trước của đường cong (nếu số như thế tồn tại). Chú ý rằng, các điểm của đường cong lập thành một nhóm, và ta có thể quan niệm xB như là "B^x": bài toán này hoàn toàn tương tự như bài toán tìm logarit cơ sở b của một số p cho trước (xem chương 6).

Trước tiên, ta cần xét thuật toán tìm bội của một điểm trên đường cong.

Định lí 7.4. *Cho E là một đường cong elliptic trên trường hữu hạn F_q, P là một điểm của đường cong. Khi đó có thể tính toạ độ của điểm kP bằng O(log klog^3 q) phép tính bit.*

Trước khi đi vào chứng minh định lí, ta tìm hiểu sơ qua phương pháp rất thông thường để tìm bội của các điểm trên đường cong: phương pháp nhân đôi liên tiếp. Xét ví dụ sau: giả sử cần tính *205P*. Ta viết :

$$205P=2(2(2(2(2(2P+P)+P)+P)+P))+P)$$

Như vậy, việc tính *205P* được đưa về 4 phép cộng hai điểm của đường cong và 7 phép nhân đôi một điểm cho trước.

Ta giả thiết rằng, trường F_q có đặc trưng khác 2, 3. Trong trường hợp $q=2^r$ hoặc $a=3^r$, có những thuật toán nhanh hơn để tính toạ độ của các bội của một điểm cho trước. Như vậy, phương trình xác định đường cong có thể cho dưới dạng Weierstrass:

$$y^2=x^3+ax+b.$$

Khi đó, theo định lí 7.2, tổng $P+Q=(x_3,y_3)$ của hai điểm khác nhau $P=(x_1,y_1)$ và $Q=(x_2,y_2)$ được tính theo công thức sau:

$$x_3=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2-x_1-x_2, \tag{7.6}$$

$$y_3=-y_1+\left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1-x_3). \tag{7.7}$$

Trong trường hợp $P=Q$, ta có công thức để tính *2P:*

$$x_3=\left(\frac{3x_1^2+a}{2y_1}\right)^2-2x_1, \tag{7.8}$$

$$y_3=-y_1+\left(\frac{3x_1^2+a}{2y_1}\right)(x_1-x_3). \tag{7.9}$$

Như vậy, ta phải dùng không quá 20 phép nhân, chia, cộng, trừ để tính toạ độ của tổng hai điểm khi biết các toạ độ của các điểm đó. Số các phép tính bit đòi hỏi là $O(\log^3 q)$ (xem chương 5). Khi dùng phương pháp nhân đôi liên tiếp, ta phải thực hiện $O(\log k)$ phép tính cộng hai diểm hoặc nhân đôi một điểm (xem chương 5). Như vậy, toàn bộ số phép tính bit phải dùng là $O(\log k \log^3 q)$. Định lí được chứng minh.

Tóm lại, ta có thuật toán thời gian đa thức để tính bội của một điểm. Ngược lại, khi biết *kP* và *P*, việc tìm ra *k* với những thuật toán nhanh nhất hiện nay lại đòi hỏi thời gian mũ. Điều này hoàn toàn tương tự như trong trường hợp các số mũ modulo *p,* và sẽ là cơ sở cho việc xây dựng hệ khoá công khai sử dụng đường cong elliptic.

5.2. Mã hoá nhờ các điểm của đường cong elliptic trên trường hữu hạn.

5.2.1. Như đã thấy trong chương 6, việc chuyển thông báo mật thực hiện bằng cách chuyển nó thành dạng chữ số, mã hoá thông báo "chữ số " này và chuyển đi. Vì thế, để đơn giản khi trình bày, ta sẽ xem thông báo cần chuyển là một số nguyên dương m nào đó.

Việc đầu tiên là phải chọn một đường cong elliptic E nào đó trên trường hữu hạn F_q. Sau đó, phải tìm cách tương ứng số nguyên m với một điểm của đường cong E.

Để dễ hiểu quá trình lập mã, ta sẽ xem đường cong E đã được chọn. Việc chọn đường cong sẽ được trình bày ở tiết sau.

5.2.2. Tương ứng một số m với một điểm của đường cong elliptic.

Cho đến nay, chưa có một thuật toán *quyết định* nào hữu hiệu để tìm được một số đủ lớn các điểm của đường cong elliptic. Thuật toán mà ta trình bày sau đây là một thuật toán xác suất với thời gian đa thức.

Trước hết ta chọn một số k nào đó theo yêu cầu sau: trường hợp thuật toán sẽ tiến hành không cho kết quả mong muốn chỉ xảy ra với xác suất không vượt quá 2^{-k}. Như vậy, nói chung $k=40$ là có thể chấp nhận được (ta nhắc lại rằng, trong trường hợp đó, xác suất sai lầm của một thuật toán sẽ bé hơn xác suất sai lầm của phần cứng của máy tính).

Giả sử số m nằm trong khoảng $1 \le m \le M$. Ta luôn chọn q sao cho $q>Mk$. Trước tiên, ta tương ứng mỗi số nguyên dương s không vượt quá M với một phần tử của trường hữu hạn F_q. Việc đó dễ dàng làm được bằng cách sau đây. Giả sử $q=p^r$, và số s biểu diễn dưới cơ số p có dạng $s=(c_0,c_1,...,c_{r-1})_p$. Khi đó, đa thức

$$S(X)=\sum_{i=0}^{r-1} c_i X^i$$

modulo một đa thức bất khả quy nào đó bậc r sẽ tương ứng với một phần tử của trường F_q (xem Chương 5).

Như vậy, với m đã cho, với mỗi j, $1 \le j \le k$, ta có một phần tử tương ứng x_j của trường F_q. Ta sẽ chỉ ra một thuật toán để , với xác suất rất lớn, tìm được một x_j trong số đó sao cho tồn tại điểm (x_j,y_j) trên đường cong E. Khi đó, ta tương ứng số m với điểm $P_m=(x_j,y_j) \in E$ vừa tìm được.

Thuật toán tìm P_m:

El1. Đặt $j \leftarrow 1$.

El2. Nếu $j>k$: kết thúc thuật toán. Trong trường hợp ngược lại, đặt $Y_j \leftarrow x_j^3+ax_j+b$. Nếu tồn tại y_j sao cho $Y_j \equiv y_j^2 \pmod q$, in ra $P_m=(x_j,y_j)$ và kết thúc thuật toán. Nếu ngược lại, chuyển sang bước El3.

El3. Đặt $j \leftarrow j+1$ và quay về bước El2.

Vì mỗi phần tử $x \in F_q$, xác suất để $f(x)$ là chính phương bằng 1/2, nên thuật toán trên đây cho ta tìm ra điểm P_m với xác suất thất bại là $1/2^k$.

Như vậy, ta đã có một thuật toán để mã hoá m bằng cách tương ứng nó với một điểm của đường cong elliptic E. Tuy nhiên, cần nhắc lại rằng, một trong những yêu cầu của mã hoá là khi biết đường cong E trên F_q, biết P_m, ta phải khôi phục được m một cách dễ dàng. Trong trường hợp này, yêu cầu đó được đảm bảo. Thật vậy, giả sử $P_m=(x,y)$. Khi đó m=$\left[\frac{x-1}{k}\right]$ (trong đó [ ] là kí hiệu phần nguyên).

5.3. Mật mã khoá công khai sử dụng đường cong elliptic.

Trong chương 6, ta làm quen với một hệ mã khoá công khai, trong đó sử dụng độ phức tạp của phép tính tìm logarit cơ số b modulo p. Ở đây, ta có khái niệm hoàn toàn tương tự.

Giả sử B,P là các điểm của đường cong elliptic E, k là một số nguyên và $P=kB$. Khi đó ta nói k là logarit cơ sở B của P. Trong trường hợp E là đường cong trên trường F_q, $q=p^r$, $p\neq 2$, bài toán tìm logarit của các điểm trên một đường cong đòi hỏi thời gian mũ, và do đó, không thể thực hiện được trong khoảng thời gian chấp nhận được (nếu q được chọn đủ lớn).

Bây giờ giả sử có một tập hợp n cá thể cần trao đổi thông tin mật với nhau: $A_1,A_2,...,A_n$.

Trước tiên, ta chọn một đường cong elliptic E trên trường hữu hạn F_q với một điểm $B\in E$ dùng làm "cơ sở". Những thông tin này được thông báo công khai. Dĩ nhiên q phải là số đủ lớn.

Sau đó, mỗi cá thể A_j chọn cho mình khoá e_j, là một số nguyên nào đó. Khoá này được giữ bí mật, nhưng A_j thông báo công khai phần tử e_jB. Điều này không làm lộ khoá e_j do độ phức tạp của phép tính logarit.

Giả sử A_j cần gửi thông báo mật m cho A_i. Trước tiên, m được tương ứng với điểm $P_m\in E$ như đã trình bày ở trên. Sau đó, A_j sẽ chọn ngẫu nhiên một số s và chuyển cho A_i cặp điểm sau: $(sB, P_m+s(e_iB))$, nhờ e_iB đã được công khai. Khi nhận được cặp điểm này, A_i chỉ việc lấy số sau trừ đi e_i lần số trước để nhận được P_m:

$$P_m=P_m+ s(e_iB)- e_i(sB).$$

Chú ý rằng, chỉ có A_i làm được điều này vì e_i được giữ bí mật, và số s không thể tìm thấy trong thời gian chấp nhận được mặc dù biết sB, vì đó là logarit của (sB) cơ sở B.

Trong hệ mã vừa trình bày, ta không cần biết số N của đường cong E.

5.4. Hệ mã tương tự mã mũ.

Trong trường hợp này, các cá thể chọn chung cho mình một đường cong elliptic E trên trường hữu hạn F_q với N điểm. Các tham số này được thông báo công khai.

Để xây dựng hệ mã, mỗi cá thể A_i chọn cho mình khoá e_i, là số nguyên dương nằm giữa 1 và N, sao cho $(e_i,N)=1$. Bằng thuật toán Euclid, A_i tìm được d_i thoả mãn

$d_i e_i \equiv 1 (mod\ N)$. Bây giờ, giả sử A_i cần gửi thông báo m cho A_j. Cũng như trước đây, A_i tìm điểm P_m tương ứng trên đường cong. Sau đó,

1) Bước 1: A_i gửi cho A_j thông báo $e_i P_m$. Dĩ nhiên, khi nhận được thông báo này, A_j chưa thể giải mã vì không biết e_i và d_i.

2) Bước 2: A_j nhận thông báo được với e_j và gửi trả lại cho A_i thông báo $e_j(e_i P_m)$.

3) Bước 3: A_i lại gửi cho A_j thông báo sau khi đã nhân với d_i: $d_i\ e_j(e_i P_m)$.

4) Nhận được thông báo cuối cùng này, A_j nhân nó với khoá d_j của mình để nhận được $P_m=d_j d_i e_i e_j P_m$. Do cách chọn e_i, d_i, e_j, d_j ta có: $d_j d_i e_i e_j \equiv 1 (mod\ N)$, tức là $P=(1+sN)P_m$ với số nguyên s nào đó. Vì N là số điểm của đường cong nên $NP_m=0$, và như vậy $P=P_m$. A_j đã nhận được thông báo ban đầu.

Để ý rằng, trong mỗi bước trên đây, các khoá mật e_i,d_i của các cá thể không hề bị phát hiện.

5.5. Chọn đường cong elliptic.

Có nhiều cách chọn đường cong và điểm B dùng làm "cơ sở" khi lập mã. Ở đây, ta trình bày hai cách đi theo hai hướng ngược nhau. Thứ nhất, chọn một điểm và một đường cong cụ thể. Thứ hai, lấy một đường cong trên trường số hữu tỷ và "sửa" theo modulo p khác nhau để thu được các đường cong trên trường hữu hạn.

Chọn đường cong và điểm ngẫu nhiên. Ta luôn luôn giả thiết rằng, đặc trưng của trường F_q khác 2, 3 (những trường hợp này có thể xét riêng). Khi đó, phương trình của đường cong có thể viết dưới dạng (7.2).

Giả sử x, y, a là ba phần tử lấy ngẫu nhiên của trường F_q. Ta đặt $b=y^2-(x^3+ax)$. Có thể kiểm tra dễ dàng đa thức x^3+ax+b có nghiệm bội hay không (xét biệt thức $4a^2+27b^3$). Nếu đa thức không có nghiệm bội, ta được đường cong E cho bởi phương trình

$$Y^2=X^3+aX+b$$

và điểm $B=(x,y) \in E$. Nếu đa thức có nghiệm bội, ta làm lại với một số a ngẫu nhiên khác.

Sửa theo modulo p. Ta xuất phát từ một đường cong elliptic E nào đó trên trường số hữu tỷ, và chọn $B \in E$ là một điểm bậc vô hạn. Sau đó, ta lấy một số nguyên tố p đủ lớn nào đó. Như đã nói, đường cong đã chọn chỉ có "sửa xấu"với một số hữu hạn số nguyên tố. Vì thế, nếu p chọn đủ lớn thì sửa theo modulo p sẽ cho ta đường cong elliptic E "modulo" p và điểm B modulo p. Cuối cùng, cũng chú ý là, cho đến nay, chưa có một thuật toán nào tương đối tốt để xác định số điểm N của một đường cong elliptic trên trường hữu hạn F_q với q là số rất lớn. Trong trường hợp N là tích cuả những số nguyên tố bé, có những thuật toán đặc biệt để tìm "logarit" cơ sở B, và do đó, hệ mã mà chúng ta đã xét sẽ không giữ được tính bảo mật nữa. Tuy nhiên, có nhiều phương pháp xác suất để tránh xảy ra tình trạng số điểm N của đường cong là tích của những số nguyên tố bé.

§6. L-hàm của đường cong elliptic

6.1. Như đã nói ở đầu chương, các đường cong elliptic có vai trò rất quan trọng trong nhiều vấn đề của số học. Tiết này có mục đích làm cho độc giả hình dung được phần nào ý nghĩa của đường cong elliptic trong Hình học đại số số học. Thực ra, đây là một lĩnh vực rất phong phú của toán học hiện đại. Vì thế, khó có thể trình bày trong một cuốn sách, hơn nữa, lại trong một giáo trình với yêu cầu khá sơ cấp. Chúng tôi cố gắng lựa chọn ở đây những kết quả và khái niệm cơ bản nhất, và cách trình bày là mô tả chứ không đi vào chi tiết.

Có thể nói, khái niệm quan trọng nhất trong nghiên cứu đường cong elliptic là *L-hàm*. Giả sử ta xét đường cong elliptic trên trường số hữu tỷ Q. Nếu cần thiết thì khử mẫu số ở các hệ số của phương trình xác định đường cong, ta cố thể giả thiết ngay tư đầu rằng, đường cong được cho bởi phương trình với các hệ số nguyên.

Để nghiên cứu đường cong cho trên trường số hữu tỷ, người ta *nghiên cứu đồng thời các sửa theo modulo p* của đường cong đó ứng với mọi số nguyên tố p. Ta nhắc lại rằng, đó là các đường cong nhận được bằng cách thay các hệ số bởi các thặng dư modulo p của chúng. Có thể tồn tại một số hữu hạn số nguyên tố p tại đó đường cong nhận được có điểm bội. Trước hết, ta xét các số nguyên tố p tại đó đường cong có " sửa tốt", tức là ta có đường cong elliptic trên trường F_p.

6.2. L-hàm của đường cong elliptic trên trường hữu hạn.

Giả sử E là đường cong elliptic trên trường số hữu tỷ Q, có sửa tốt tại số nguyên tố p. Đồng thời với việc xét E modulo p, ta có thể xét các điểm của đường cong E trên mọi trường F_q, với $q=p^r$, $r=1,2,...$Kí hiệu qua N_r số điểm của đường cong E trên F_q, $q=p^r$.

Như vậy, ta có dãy các số nguyên dương $N_1,N_2,...N_r...$ Để nghiên cứu một dãy nào đó, một trong những phương pháp rất hay được dùng trong số học là xét *hàm sinh* của chúng. Nhờ hàm sinh, người ta có thể xét các phần tử của dãy một cách đồng thời, thông qua tính chất của hàm sinh. Chẳng hạn, hàm sinh của dãy số trên đây là:

$$Z_p(T)=\exp\left(\sum_{r\geq 1}\frac{N_r}{r}T^r\right) \qquad (7.10)$$

Định nghĩa. Hàm $Z_p(T)$ được gọi là *Zeta-hàm* của đường cong E trên trường F_p.

Zeta-hàm được xây dựng không chỉ với các đường cong elliptic, mà còn với những đối tượng rộng hơn, là các đa tạp xạ ảnh. Zeta-hàm của các đa tạp xạ ảnh có nhiều tính chất tương tự với Zeta-hàm Riemann. Một trong những tính chất quan trọng nhất của các Zeta-hàm thể hiện trong định lí sau đây, mà ta chỉ phát biểu cho các đường cong elliptic.

Định lí Weil. *Zeta-hàm của một đường cong elliptic E trên trường hữu hạn F_q là một hàm hữu tỷ của T, có dạng:*

$$Z(T;E/F_q)=\frac{1-aT-qT^2}{(1-T)(1-qT)},$$

trong đó a là số tham gia trong công thức tính số điểm của đường cong E trên F_p: $N_1=1+q-a$. Định thức của đa thức ở tử số âm, và hai nghiệm (phức liên hợp) của nó có trị tuyệt đối bằng $\sqrt{q}$.

Nhận xét. 1) Khi biết Zeta-hàm, ta có thể khai triển để tìm các hệ số của nó trong công thức (7.10), nghĩa là biết được số điểm của E trên trường $F\ p^r$ với mọi r tuỳ ý. Vì Zeta-hàm chỉ phụ thuộc $a=1+q-N_1$ nên N_r xác định duy nhất qua N_1.

2) Tính chất định thức của tử số âm có nghĩa là: $|a|<2\sqrt{q}$. Như vậy, định lí Hasse là một hệ quả của định lí Weil.

Một tương tự của định lí Weil cho các đa tạp xạ ảnh được gọi là "giả thuyết Weil", và được P. Deligne chứng minh năm 1973.

6.3. L-hàm của đường cong trên trường số hữu tỷ

Như vậy, với mỗi số nguyên tố p, ta có Zeta-hàm $Z_p(T)$ ứng với đường cong elliptic E trên trường F_q, $q=p^r$. Để nghiên cứu đường cong E trên trường số hữu tỷ, ta có thể xét "đồng thời" các "Zeta-hàm địa phương" $Z_p(T)$ bằng cách xây dựng "Zeta-hàm toàn cục" của biến phức s.

Kí hiệu qua a_p số xác định bởi $a_p=p+1-N_p$, trong đó N_p là số điểm của đường cong trên trường F_p. Khi đó L-hàm Hasse-Weil của đường cong E được định nghĩa bởi công thức

$$\mathrm{L(E,s)}=\prod_p (1-a_p p^{-s}+p^{1-2s})^{-1}\ .$$

Nhận xét. Bằng cách khai triển tích trong định nghĩa L-hàm, ta có thể thấy rằng, L-hàm tương tự như Zeta-hàm Riemann, định nghĩa bởi công thức sau đây:

$$\zeta(s)=\sum_{n=1}^{\infty} n^{-s}\ .$$

Dễ thấy rằng, Zeta-hàm Riemann có thể được tính bởi công thức sau (xem phần bài tập):

$$\zeta(s)=\prod_{p\in P}(1-p^{-s})^{-1}$$

Đối với Zeta-hàm Riemann, các tính chất quan trọng nhất là:

1) $\zeta(s)$ có thể thác triển thành hàm phân hình trên toàn mặt phẳng phức với cực điểm đơn tại $s=1$.

2) Nếu đặt

$$\Lambda(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$$

thì $\Lambda(s)$ là hàm phân hình trên toàn mặt phẳng phức, và thoả mãn phương trình hàm

$$\Lambda(s) = \Lambda(1-s)$$

3) $\zeta(-2n) = 0$ với mọi n nguyên dương.

Giả thuyết Riemann nổi tiếng nói rằng, các không điểm còn lại của Zeta-hàm đều nằm trên đường thẳng *Re s=1/2*. Người ta đã kiểm tra giả thuyết đó đối với một số rất lớn không điểm (hàng triệu), nhưng vẫn chưa chứng minh được giả thuyết trong trường hợp tổng quát. Giả thuyết này cũng liên quan đến nhiều vấn đề của số học thuật toán.

Đối với L-hàm của đường cong elliptic, ta có:

Giả thuyết: Hàm *L(E,s)* có thể thác triển giải tích lên toàn mặt phẳng phức. Hơn nữa, tồn tại một số nguyên dương *N* sao cho, nếu đặt

$$\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

thì ta có phương trình hàm sau đây

$$\Lambda(E,2-s) = \pm\Lambda(E,s).$$

Số *N* nói trong giả thuyết là một bất biến quan trọng của đường cong, gọi là *conđuctơ* của nó.

6.4. Giả thuyết Birch-Swinnerton-Dyer.

Một trong những giả thuyết quan trọng khác của lí thuyết các đường cong elliptic là giả thuyết sau đây của Birch và Swinnerton-Dyer.

Trước tiên ta nhắc lại rằng, nhóm các điểm hữu tỷ của đường cong elliptic *E* là tổng trực tiếp của nhóm cấp hữu hạn với nhóm Z^r. Số *r* được gọi là hạng của đường cong.

Giả thuyết Birch-Swinnerton-Dyer. Nếu hạng của đường cong elliptic *E* bằng *r* thì L-hàm của đường cong có không điểm cấp *r* tại điểm *s=1*.

Như vậy, nếu *L(E,1)=0* thì hạng $r \geq 1$, và do đó, đường cong elliptic có vô hạn điểm hữu tỷ. Trong trường hợp ngược lại, đường cong E chỉ có hữu hạn điểm hữu tỷ. Đó chính là kết quả quan trọng đầu tiên theo hướng khẳng định giả thuyết Birch-Swinnerton-Dyer, được Coates và Wiles chứng minh năm 1977.

Thực ra, giả thuyết Birch-Swinnerton-Dyer còn cho công thức tính giới hạn

$$\lim_{s\to 1}(s-1)^r L(E,s).$$

Tuy nhiên, để phát biểu chính xác giả thuyết đó ta cần đến khái niệm nhóm Shafarevich của đường cong, là một trong những khái niệm sâu sắc nhất của hình học đại số.

Nhận xét. Để kết thúc chương này, chúng tôi xin nói qua vài lời về giả thuyết quan trọng nhất trong lí thuyết đường cong elliptic: giả thuyết Taniyama-Weil.

Giả sử N là một số nguyên dương. Ta kí hiệu qua nhóm $\Gamma_0(N)$ nhóm các ma trận vuông cấp 2 $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ trong đó a,b,c,d nguyên, $ad-bc=1$ và $c \equiv 0 (mod\ N)$. Nhóm các ma trận này tác động lên nửa mặt phẳng trên theo công thức sau:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z)=\frac{az+b}{cz+d}.$$

Một hàm $f(z)$ giải tích tại nửa mặt phẳng trên, kể cả tại các điểm hữu tỷ của trục thực và bằng không tại các điểm đó, được gọi là một *dạng modula trọng số 2 đối với nhóm* $\Gamma_0(N)$ nếu nó thoả mãn hệ thức sau:

$$f(\gamma z)=(cz+d)^2 f(z).$$

Từ định nghĩa trên suy ra rằng, nếu $f(z)$ là dạng modula trọng số 2 đối với nhóm $\Gamma_0(N)$ thì ta có $f(z+1)=f(z)$ với mọi z (lấy γ là ma trận $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Như vậy, $f(z)$ có thể khai triển theo dạng sau:

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

Từ đó ta có thể tương ứng f với L-hàm của nó:

$$L_f(s) = \sum_{n=1}^{\infty} a_n / n^s$$

Giả thuyết Taniyama-Weil: Nếu E là một đường cong elliptic trên trường số hữu tỷ côndưctơ N thì L-hàm của đường cong E là L-hàm của một dạng modula trọng số 2 đối với nhóm $\Gamma_0(N)$.

Giả thuyết trên đây liên quan chặt chẽ đến định lí lớn Fermat. Thật vậy, giả sử tồn tại số nguyên tố p lớn hơn 2 sao cho phương trình Fermat với số mũ p có các nghiệm không tầm thường a, b, c.

Ta đổi dấu c và viết phương trình dưới dạng:

$$a^p+b^p+c^p=0$$

Đường cong elliptic xác định bởi phương trình

$$y^2=x(x-a^p)(x+b^p)$$

có côndưctơ $N=N_0(abc)$ (xem định nghĩa N_0 ở chương 5). Đường cong này được G. Frey nghiên cứu lần đầu tiên năm 1983. Sau đó (1986), K. Ribet chứng minh rằng, L-hàm của đường cong đó không phải là L-hàm của bất kì một dạng modula trọng số 2 nào đối với nhóm $\Gamma_0(N)$. Như vậy, nếu chứng minh được giả thuyết

Taniyama-Weil thì cũng chứng minh được định lí lớn Fermat, bởi vì nếu phương trình Fermat có nghiệm thì tồn tại một đường cong elliptic không thoả mãn giả thuyết Taniyama-Weil.

Tháng 6 năm 1993, A.Wiles công bố chứng minh giả thuyết Taniyama-Weil, cũng tức là chứng minh được định lí lớn Fermat.

Bài tập chương 7

7.1. Cho dường cong elliptic trên trường thực $y^2=x^3-36x$ và các điểm trên đường cong: $P=(-3,9)$, $Q=(-2,6)$. Hãy tính các điểm $P+Q$ và $2P$.

7.2. Tìm bậc của điểm $P=(2,3)$ trên đường cong $y^2=x^3+1$.

7.3. Chứng minh rằng các đường cong elliptic sau đây có $q+1$ điểm trên trường F_q:

1) $y^2=x^3-x$, $q \equiv 3 (mod\ 4)$.

2) $y^2=x^3-1$, $q \equiv 2 (mod\ 3)$, q lẻ.

3) $y^2+y=x^3$, $q \equiv 2 (mod\ 3)$, (q có thể chẵn).

7.4. Tính số điểm của đường cong elliptic $y^2=x^3-x$ trên trường F_{71}.

7.5. Cho đường cong $y^2+y=x^3$ trên trường F_2. Hãy tìm Zeta-hàm của đường cong đó và tính số điểm của đường cong trên mọi trường F_q với $q=2^r$, $r=1,2,...$