TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN THÔNG TIN-
INFORMATION SECURITY

CHƯƠNG 3
KỸ THUẬT MÃ HOÁ

CƠ SỞ TOÁN HỌC

Giảng viên: TS. Trần Thế Vinh

CƠ SỞ TOÁN HỌC

THUẬT TOÁN VÀ ĐỘ PHỨC TẠP

Khái niệm về thuật toán:

Trong toán học và khoa học máy tính, thuật toán là một chuỗi hữu hạn các chỉ dẫn nghiêm ngặt được sử dụng để tìm lời giải cho một loại bài toán cụ thể.

Các thuật toán được sử dụng làm thông số kỹ thuật để thực hiện tính toán và xử lý dữ liệu. Một quy trình để giải quyết một vấn đề toán học trong một số bước hữu hạn thường bằng các phép toán đệ quy

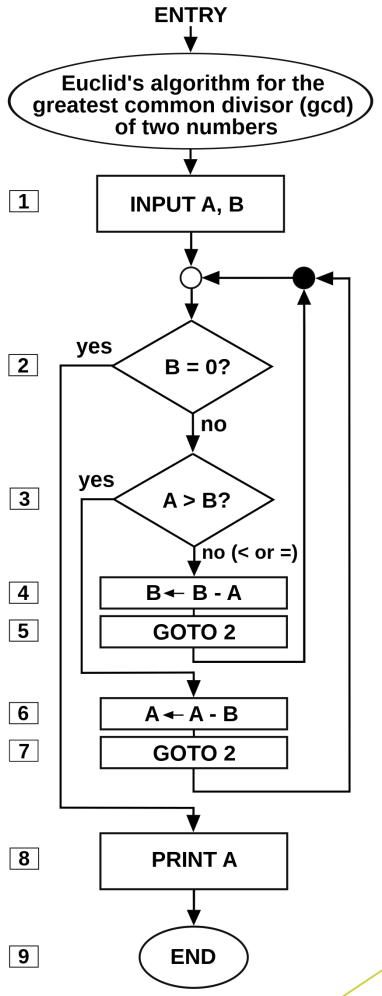
Diễn đạt thuật toán:

Các thuật toán có thể được thể hiện bằng nhiều loại ký hiệu, bao gồm mã giả, lưu đồ, biểu đồ drakon, ngôn ngữ lập trình hay bảng điều khiển (được sử lý bảo trình biên dịch).

Các thuật toán có thể đơn giản hay phức tạp tùy thuộc vào những gì chúng ta muốn đạt được.

Một thuật toán tốt phải thỏa mãn các đặc tính sau:

- Tính hữu hạn
- Tính xác định



Thuật toán Euclid tìm UCLN

CƠ SỞ TOÁN HỌC

THUẬT TOÁN VÀ ĐỘ PHỨC TẠP

Độ phức tạp của thuật toán:

Độ phức tạp của thuật toán dựa trên số các phép tính phải làm khi thực hiện thuật toán.
Khi tiến hành cùng một thuật toán, số các phép tính phải thực hiện còn phụ thuộc vào độ lớn của dữ liệu đầu vào (input). Vì thế, độ phức tạp của thuật toán sẽ là một hàm số của độ lớn của đầu vào.

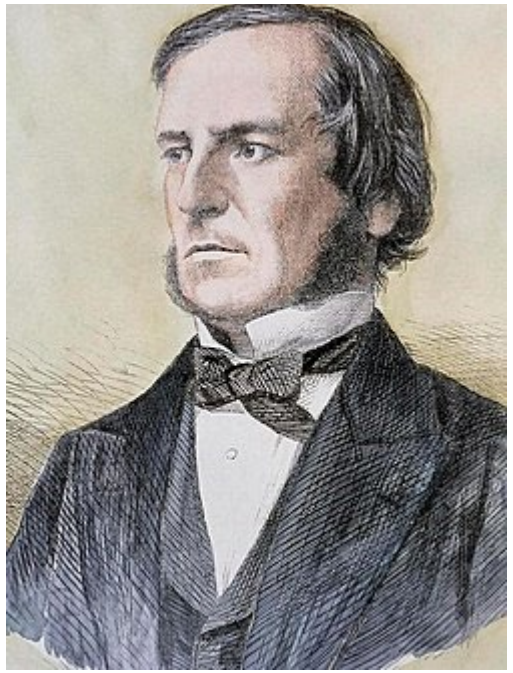
Trong máy tính thường ghi các chữ số bằng những bóng đèn "sáng, tắt" (bóng đèn sáng chỉ số 1, bóng đèn tắt chỉ số 0). Một ký hiệu 0 hoặc 1 được gọi là 1 bit.
Một ký tự N biểu diễn bởi k chữ số 0 và 1 được gọi là một ký tự có k-bit. Do đó độ phức tạp của một thuật toán được đo bằng số các phép tính bit. Phép tính bit là một phép tính logic hay số học thực hiện trên các số bit 0 và 1

CƠ SỞ TOÁN HỌC

TOÁN TỬ LOGIC

Khái niệm:

Exclusive OR hay là hàm cộng modulo 2 là một trong những hàm cơ bản được sử dụng khá phổ biến trong mật mã học (cũng như trong nhiều ứng dụng khác).
Nhà toán học người Anh George Boole ở cuối thế kỷ XIX đã sáng lập ra một ngành "Đại số học" mà sau này đã trở thành nền tảng cho việc xây dựng chế tạo các máy tính điện tử và các chip vi điện tử.



Boole đã định nghĩa một số toán tử logic hai biến cơ bản dạng: f = f(x,y) trong đó x, y (biến đầu vào: input) và f (biến đầu ra: output) đều là những biến logic, nghĩa là những biến số chỉ lấy giá trị trong tập hợp {0, 1} với 0 là giá trị phi lý - giá trị sai, còn 1 là giá trị chân lý - giá trị đúng.

CƠ SỞ TOÁN HỌC

TOÁN TỬ LOGIC

NOT

Các hàm Boole một và hai biến cơ bản thông dụng nhất là:

NOT

Hàm phủ định của biến đầu vào a là ā. Giá trị của biến đầu ra ā đối lập với biến đầu vào a. (Ý nghĩa: ā luôn trái ngược với a)

a	ā
0	1
1	0

AND

Hàm hội $f = a \cap b$. Giá trị của biến đầu ra f bằng 1 khi và chỉ khi cả hai biến đầu vào cùng có giá trị bằng 1, các trường hợp còn lại f lấy giá trị bằng 0. (Ý nghĩa: f đúng khi và chỉ khi vừa a vừa b cùng đúng)

a	b	a∩b
0	0	0
0	1	0
1	0	0
1	1	1

CƠ SỞ TOÁN HỌC

TOÁN TỬ LOGIC

OR

Hàm tuyển $f = a \cup b$. f bằng 1 khi và chỉ khi có hoặc a hoặc b, hoặc cả a và b có giá trị bằng 1. (Ý nghĩa: f đúng khi hoặc a đúng hoặc b đúng hoặc cả hai a và b cùng đúng)

a	b	aUb
0	0	0
0	1	1
1	0	1
1	1	1

XOR

Exclusive OR hay còn gọi là hàm cộng modulo 2: $f = a\ XOR\ b$ hay $f = a \oplus b$. f lấy giá trị 1 khi và chỉ khi chỉ có một trong hai biến a hoặc b có giá trị bằng 1. (Ý nghĩa: nếu cả a và b cùng sai hay cùng đúng thì f sai)

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

CƠ SỞ TOÁN HỌC

TOÁN TỬ LOGIC

Hàm XOR trong mật mã:

Ý nghĩa của toán tử XOR liên quan đến "tính chất đồng nhất" của các biến đầu vào: Nếu hai biến đầu vào có cùng giá trị thì XOR là sai, còn nếu hai biến đầu vào khác giá trị nhau thì XOR là đúng.

Ứng dụng trong các thuật toán lập mã: Giả sử ta lấy bản plaintext P và XOR nó với một chìa khóa K: nó sẽ biến thành một bản ciphertext C trong đó có một số bit đã thay đổi. Nếu ta lại lấy ciphertext XOR với chìa khóa K ấy một lần nữa thì ta được lại plaintext.

Ví dụ:

Plaintext:	P =	100110001
Khóa K:	K =	001111001
Mã hóa:	Ciphertext $C = P\ XOR\ K$ =	101001000
Giải mã:	Plaintext $P = C\ XOR\ K$ =	100110001

Nhận xét:

- Độ dài (kích thước số bit) của khóa K rõ ràng có tác động rất lớn đến khả năng bảo mật của mã đối xứng. Chẳng hạn trong mã block có kích thước block là 56 - 64 bit thì ta dùng khóa K có kích thước cũng là 56 - 64 bit. Vì mỗi vị trí trong khóa có thể tùy chọn 1 trong 2 giá trị 0 hay 1 nên có tất cả: 256 cách tạo khóa khác nhau! Đây là một con số rất lớn cho nên thông thường nguy cơ bị tấn công bạo lực thấp.

- Tuy nhiên vì phép toán XOR được thực hiện hoàn toàn đơn giản nên tốc độ lập mã, giải mã vẫn khá nhanh.

CƠ SỞ TOÁN HỌC

SỐ NGUYÊN TỐ

SỐ NGUYÊN TỐ:

Ký hiệu $\mathbb{Z}$ là tập hợp các số nguyên và $\mathbb{N}$ là tập hợp các số tự nhiên. Với $a,b \in \mathbb{Z}$ ta nói rằng b chia hết cho a nếu như b có thể viết thành tích của a với một số nguyên khác, lúc đó ta có thể nói rằng a chia hết b hay a là một ước số của b, ký hiệu a|b. Ta có 1 số tính chất sau:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

- Nếu $a,b,c \in \mathbb{Z}$ và $a|b$ thì $a|bc$;
- Nếu $a|b$ và $b|c$ thì $a|c$;
- Nếu $a|b$ và a|c thì $a|b \pm c$;
- Nếu $a|b$ và a$\nmid$ c thì $a \nmid b \pm c$;

Số tự nhiên lớn hơn 1 mà không chia hết cho số tự nhiên nào khác, trừ chính nó và 1 thì được gọi là số nguyên tố.

Hệ quả:

- Nếu p là một số nguyên tố và $p|ab$ thì ít nhất một trong 2 số a,b phải chia hết cho p.
- Ước chung lớn nhất của 2 số tự nhiên a,b là số lớn nhất trong tập các ước chung cửa 2 số đó, được ký hiệu là $gcd(a,b)$
- Khi 2 số tự nhiên có ước chung lớn nhất $gcd(a,b)=1$ thì chúng được gọi là nguyên tố cùng nhau

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID

GIẢI THUẬT EUCLID

Giải thuật Euclid, hay thuật toán Euclid, là một giải thuật tính ước số chung lớn nhất (gcd) của hai số (nguyên) một cách hiệu quả. Giải thuật này được biết đến từ khoảng năm 300 trước Công Nguyên. Nhà toán học Cổ Hy Lạp Euclid đã nêu giải thuật này trong cuốn sách "Cơ sở" (Elements) nổi tiếng.

Ví dụ:

Tính ước số chung lớn nhất của 36 và 129.

Trước hết lấy 129 (số lớn hơn trong 2 số) chia cho 36:

$129 = 36 \times 3 + 21$

(36 và 21 sẽ được dùng cho vòng lặp kế tiếp)

$36 = 21 \times 1 + 15$

$21 = 15 \times 1 + 6$

$15 = 6 \times 2 + 3$

$6 = 3 \times 2$

Cuối cùng ta có:

$3 = gcd(6,3) = gcd(15,6) = gcd(21,15) = gcd(36,21) = gcd(129,36)$.

Bổ đề. Giả sử $a = bq + r$, với a, b, q, r là các số nguyên, ta có:

$$gcd(a,b) = \begin{cases} b \text{ nếu } r = 0 \\ gcd(b,r) \text{nếu } r \neq 0 \end{cases}$$

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Giải thuật Euclid mở rộng sử dụng để giải phương trình vô định nguyên (còn được gọi là phương trình Diophantos):

$$a.x + b.y = c$$

Trong đó a, b, c là các hệ số nguyên; x, y là các biến nhận giá trị nguyên.

Điều kiện cần và đủ để phương trình này có nghiệm (nguyên) là $gcd(a, b)$ là ước của c.

Khẳng định này dựa trên mệnh đề sau trong số học:
"Ta biết rằng nếu $d = gcd(a, b)$ thì tồn tại các số nguyên x, y sao cho: $a.x + b.y = d$."

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG:

Giải thuật Euclid mở rộng kết hợp quá trình tìm $gcd(a, b)$ trong thuật toán Euclid với việc tìm một cặp số x, y thỏa mãn phương trình Diophantos.
Giả sử cho hai số tự nhiên a, b với $a > b > 0$.

Đặt $r_0 = a, r_1 = b$, chia r_0 cho r_1 được số dư r_2 .

Nếu $r_2 = 0$ thì dừng, nếu $r_2 \neq 0$, chia r_1 cho r_2 được số dư r_3 ,... Vì dãy các r_i là giảm thực sự nên sau hữu hạn bước ta được số dư $r_m = 0$.

$r_0 = q_1 \times r_1 + r_2$, $0 < r_2 < r_1$;
$r_1 = q_2 \times r_2 + r_3$, $0 < r_3 < r_2$;
....
$r_{m-1} = q_m \times r_m + r_{m+1}$, $0 < r_{m+1} < r_m$;
$r_m = q_{m+1} \times r_{m+1}$;
trong đó số dư cuối cùng khác 0 là r_{m+1} = d.

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Bài toán đặt ra là tìm x, y sao cho: $a.x + b.y = r_{m+1}$ (= d)

Để làm điều này, ta tìm x, y theo công thức truy hồi, nghĩa là tìm x_i và y_i sao cho:

$a.x_i + b.y_i = r_i$ với i = 0, 1,....

Ta có:

$a.1 + b.0 = a = r_0$ và $a.0 + b.1 = b = r_1$,

nghĩa là:

$x_0 = 1, x_1 = 0$ và $y_0 = 0, y_1 = 1$ (1)

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Tổng quát, giả sử có:

$$a.x_i + b.y_i = r_i; \text{ với } i = 0,1,\ldots.$$
$$a.x_{i+1} + b \times y_{i+1} = r_{i+1}; \text{ với } i = 0,1,\ldots.$$

Khi đó từ: $r_i = q_{i+1}.r_{i+1} + r_{i+2}$

suy ra:

$$r_i - q_{i+1}.r_{i+1} = r_{i+2}$$

$$(a.x_i + b.y_i) - q_{i+1}.(a.x_{i+1} + b.y_{i+1}) = r_{i+2}$$
$$a.(x_i - q_{i+1}.x_{i+1}) + b.(y_i - q_{i+1}.y_{i+1}) = r_{i+2}$$

từ đó, có thể chọn:

$$x_{i+2} = x_i - q_{i+1}.x_{i+1} \quad (2)$$
$$y_{i+2} = y_i - q_{i+1}.y_{i+1} \quad (3)$$

Khi $i = m - 1$ ta có được x_{m+1} và y_{m+1} .

Các công thức (1), (2), (3) là công thức truy hồi để tính *x, y.*

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Giải thuật sau chỉ thực hiện với các số nguyên $a > b > 0$, biểu diễn bằng:

Procedure Euclid_Extended (a,b)
Var Int $x_0 := 1, x_1 := 0, y_0 = 0, y_1$:=1;
While b>0
do {r:= a mod b
$q := a\ div\ b$
$x := x_0 - x_1.q$
$y := y_0 - y_1.q$
if $r = 0$ then Break
$a := b$
$b := r$
$x_0 := x_1$
$x_1 := x$
$y_0 := y_1$
y_1 :=y }
Return $d := b, x, y$;

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Ví dụ:

Giả sử cho $a = 29, b = 8$, giải thuật trải qua các bước như sau:

Bước i	r_i	r_{i+1}	r_{i+2}	q_{i+1}	x_i	x_{i+1}	x_{i+2}	y_i	y_{i+1}	y_{i+2}
0	29	8	5	3	1	0	1	0	1	-3
1	8	5	3	1	0	1	-1	1	-3	4
2	5	3	2	1	1	-1	2	-3	4	-7
3	3	2	1	1	-1	2	-3	4	-7	11
4	2	1	0	2						

Kết quả thuật toán cho đồng thời:

$$d = gcd(29,8) = 1 \text{ và } x = -3, y = 11.$$

Dễ dàng kiểm tra hệ thức $29.(-3) + 8.11 = 1$

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Áp dụng giải thuật Euclid mở rộng tìm số nghịch đảo trong vành Z_m

Trong lý thuyết số, vành Z_m được định nghĩa là vành thương của Z (vành các số nguyên) với quan hệ đồng dư theo modulo m (là một quan hệ tương đương) mà các phần tử của nó là các lớp đồng dư theo modulo m (m là một số nguyên dương lớn hơn 1). Ta cũng có thể xét Z_m chỉ với các đại diện của nó.

Khi đó:

$Z_m = \{0, 1, \dots, m-1\}$

Phép cộng và nhân trong Z_m là phép toán thông thường rút gọn theo modulo m:

$$a + b = (a + b) mod\ m$$
$$a.b = (a.b) mod\ m$$

Phần tử a của $\mathbf{Z_m}$ được gọi là khả đảo trong $\mathbf{Z_m}$ hay khả đảo theo modulo m nếu tồn tại phần tử a' trong $\mathbf{Z_m}$ sao cho $a \times a' = 1$ trong $\mathbf{Z_m}$.

Khi đó a' được gọi là nghịch đảo modulo m của a. Trong lý thuyết số đã chứng minh rằng, số a là khả đảo theo modulo m khi và chỉ khi $gcd(a, m) = 1$ (a và m nguyên tố cùng nhau).

Khi đó tồn tại các số nguyên x, y sao cho: $m.x + a.y = 1$.

Đẳng thức này lại chỉ ra y là nghịch đảo của a theo modulo m. Do đó có thể tìm được phần tử nghịch đảo của a theo modulo m nhờ thuật toán Euclid mở rộng khi chia m cho a.

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Giải thuật

Giải thuật sau chỉ thực hiện với các số nguyên $m > a > 0$, biểu diễn bằng dãy mã:

Procedure Euclid_Extended (a,m)
int, $y_0 = 0, y_1 := 1;$
While a>0
do {r:= m mod a
if r=0 then Break
q:= m div a
$y := y_0 - y_1 \times q$
m:=a
a:=r
$y_0 := y_1$
y_1 :=y}
If a>1 Then Return "A không khả nghịch theo modulo m"
else Return " Nghịch đảo modulo m của a là y"

CƠ SỞ TOÁN HỌC

GIẢI THUẬT EUCLID MỞ RỘNG

GIẢI THUẬT EUCLID MỞ RỘNG

Ví dụ:

Tìm số nghịch đảo (nếu có) của 30 theo modulo 101

Bước i	m	a	r	q	y_0	y_1	y
0	101	30	11	3	0	1	-3
1	30	11	8	2	1	-3	7
2	11	8	3	1	-3	7	-10
3	8	3	2	2	7	-10	27
4	3	2	1	1	-10	27	-37
5	2	1	0	.	.	.	.

Kết quả tính toán trong bảng cho ta -37. Lấy số đối của 37 theo modulo 101 được 64. Vậy $30^{-1} mod\ 101 = 64$.

CƠ SỞ TOÁN HỌC

HÀM MODULO – ĐỒNG DƯ THỨC

HÀM MODULO – ĐỒNG DƯ THỨC

Hàm modulo có thể hiểu một cách đơn giản chính là số dư trong phép chia các số nguyên. Muốn tính X modulo Y (thường ký hiệu là X mod Y) ta chỉ cần làm phép chia X cho Y và tìm số dư trong phép chia đó, nói khác đi: ta trừ vào X bội số lớn nhất của Y bé hơn X. Rõ ràng X mod Y chỉ có thể lấy các giá trị từ 0, 1,… cho đến $Y - 1$.

Ví dụ: $25\ mod\ 5\ =\ 0$

Trong số học, hai số nguyên a và b được gọi là "đồng dư theo modulo n" nếu chúng có cùng số dư trong phép chia cho n. Ta ký hiệu: $a \equiv b\ (mod\ n)$ và đọc là "a đồng dư với b theo modulo n". Biểu thức đó gọi là một đồng dư thức.

Ví dụ: $18 \equiv 4\ (mod\ 7)$

Một số tính chất của phép tính đồng dư:

- $a \equiv a\ (mod\ n)$;
- Nếu $a \equiv b\ (mod\ n)$ thì $b \equiv a\ (mod\ n)$;
- Nếu $a \equiv b\ (mod\ n)$ và $b \equiv c\ (mod\ n)$ thì $a \equiv c\ (mod\ n)$;
- Nếu $a \equiv b\ (mod\ n)$, $c \equiv d\ (mod\ n)$ thì

  $a \pm c \equiv b \pm d\ (mod\ n), ac \equiv bd\ (mod\ n)$;

CƠ SỞ TOÁN HỌC

HÀM MODULO – ĐỒNG DƯ THỨC

HÀM MODULO – ĐỒNG DƯ THỨC

Như vậy ta có thể tự do thực hiện các phép tính số học thông thường trên tập $\mathbb{Z}/n\mathbb{Z}$.
Nếu x là một phần tử trong $\mathbb{Z}/n\mathbb{Z}$ và *gcd(x,n)=1* thì tồn tại các số u, v sao cho $ux+vn=1$, tức là $ux \equiv 1(mod\ n)$, nên người ta gọi *x* có nghịch đảo (trong $\mathbb{Z}/n\mathbb{Z}$) là *u*, ký hiệu x^{-1} hay 1/x.

Ví dụ:

Xét vành $\mathbb{Z}/9\mathbb{Z}$ = {0, 1, 2,..., 8}. Để tìm phần tử nghịch đảo của 5 (tức là 5^{-1}) ta dùng thuật toán Euclid mở rộng, tức là phân tích:

$$9 = 1.5 + 4,\ 5 = 1.4 + 1,\ 4 = 1.2.2 + 0$$

Rồi thế ngược trở lại ta có:

$$1 = 5 - 1.4 = 5 - 1(9-1.5) = 2.5 - 1.9$$

Suy ra: $2.5 \equiv 1(mod\ 9)$ *hay* $5^{-1} = 2(mod\ 9)$

CƠ SỞ TOÁN HỌC

HÀM MODULO – ĐỒNG DƯ THỨC

HÀM MODULO – ĐỒNG DƯ THỨC

Tập các phần tử trong $\mathbb{Z}/n\mathbb{Z}$ mà có nghịch đảo thường được ký hiệu là $\mathbb{Z}/n\mathbb{Z}^*$.Rõ ràng tập này có số phần tử bằng f(m), và trên tập này, ngoài các phép tính cộng, trừ, nhân, ta còn có thể đưa vào phép chia.

Nếu $a \equiv b(mod\ n), c \equiv d(mod\ n)$ với $\gcd(c,n) = 1,$ thì

$$ac^{-1} \equiv bd^{-1}(mod\ n).$$

Ví dụ:

Với$\mathbb{Z}/9\mathbb{Z} = \{0,1,2,\dots,8\}, \mathbb{Z}/9\mathbb{Z}^* = \{1,2,4,5,7,8\},$ ta có 5^{-1}=*2(mod 9)* và phép chia của 2 cho 5 (trong $\mathbb{Z}/9\mathbb{Z}^*$) được thực hiện như sau:

$$\frac{2}{5} = 2.5^{-1} = 2.2 = 4(mod 9).$$

Ta cũng có 2 = 5.4(mod 9) vì 5.4=20=2.9 + 2

CƠ SỞ TOÁN HỌC

HÀM MODULO – ĐỒNG DƯ THỨC

HÀM MODULO – ĐỒNG DƯ THỨC

Phương trình đồng dư tuyến tính:

$$\boldsymbol{ax \equiv b(mod\ m)}$$

Khi *gcd(a,m)=1* thì ta có ngay nghiệm $x \equiv a^{-1}b(mod\ m)$. Khi *gcd(a,m)=g* thì có 2 khả năng xảy ra:

- Phương trình có nghiệm khi g chia hết b, vì rằng khi ấy phương trình đã cho tương đương với phương trình $\left(\frac{a}{g}\right)x = b/g(mod\frac{m}{g})$, trong đó hệ số *a/g* là nguyên tố cùng nhau với *m/g*
- Phương trình vô nghiệm nếu *g* không chia hết *b*, vì hiệu của 2 số chia hết cho *g* thì không thể là một số không chia hết cho *g*;

CƠ SỞ TOÁN HỌC

HÀM MODULO – ĐỒNG DƯ THỨC

ĐỊNH LÝ FERMAT VÀ CÁC MỞ RỘNG

Định lý Fermat (nhỏ):

Nếu p là một số nguyên tố, a là một số nguyên thì $a^p \equiv a(mod\ p)$. Nếu p không chia hết a (tức là $a(mod\ p) \neq 0$) thì $a^{p-1} \equiv 1(mod\ p)$.

Ví dụ:

$$2^5 \equiv 2(mod\ 5); 2^{5-1} \equiv 1(mod\ 5)$$
$$15^{5-1} \equiv 0(mod\ 5).$$

Định lý mở rộng: Nếu $\gcd(a,n) = 1$ thì $a^{g(n)} \equiv 1(mod\ m)$.
Trong trường hợp riêng, khi n là số nguyên tố thì $g(n) = n - 1$, lúc đó ta có định lý Fermat

Ví dụ:

Với $n = 15$ ta có $g(15) = g(3).g(5) = 2.4 = 8$ và do đó

$$7^8 \equiv 1(mod\ 15), 11^8 \equiv 1(mod\ 15), \ldots.$$

CƠ SỞ TOÁN HỌC

HÀM MODULO – ĐỒNG DƯ THỨC

ĐỊNH LÝ FERMAT VÀ CÁC MỞ RỘNG

Hệ quả 1:

Nếu $\gcd(c,n) = 1$ và $a \equiv b(mod\ g(n))$ với a.b là các số tự nhiên, thì $c^a \equiv c^b(mod\ n)$ và ta có:

$$c^a\ mod\ n = \ c^{b\ mod\ g(n)}\ mod\ n$$

Nhận xét:

Hệ quả trên, giúp ta giảm nhẹ việc tính toán đồng dư của lũy thừa bậc cao một cách rất đáng kể.

Ví dụ:

Tính $5^{1005}(mod\ 14)$ ta lưu ý rằng g(14)=g(7).g(2)=6.1=6 và $1005 \equiv 3(mod 6)$, cho nên từ kết quả trên ta có:

$$5^{1005}(mod\ 14) = 5^3(mod\ 14) = 125(mod\ 14) = 13$$

Hệ quả 2:

Nếu e, d là các số nguyên thỏa mãn $e.d \equiv 1(mod\ g(n))$ thì với mọi số c nguyên tố cùng nhau với m, ta có

$$(c^e)^d \equiv c\ (mod\ n).$$

Rõ ràng, với a=e.d và b=1, từ Hệ quả 1 ta có ngay hệ quả 2. Hệ quả này đóng vai trò then chốt trong việc thiết lập các hệ mã sau này (kể cả hệ mã bất đối xứng RSA)

CƠ SỞ TOÁN HỌC

ĐỊNH LÝ SỐ DƯ TRUNG QUỐC
CHINESE THEOREM OF REMAINDERS

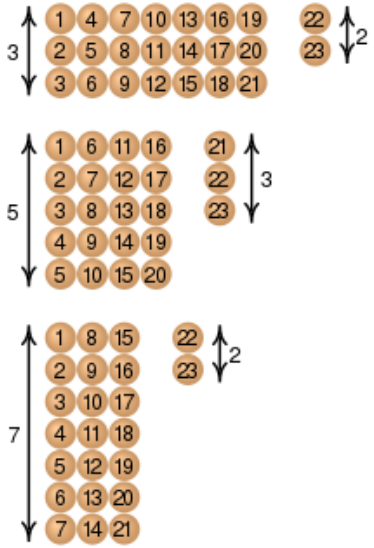
Chinese Theorem of Remainders

Định lý số dư Trung Quốc (Chinese Theorem of Remainders) là tên người phương tây đặt cho định lý này. Người Trung Quốc gọi nó là bài toán Hàn Tín điểm binh.

Hàn Tín là một danh tướng thời Hán Sở từng được phong tước vương thời Hán Cao Tổ Lưu Bang dựng nghiệp. Sử ký của Tư Mã Thiên viết rằng Hàn Tín là tướng trói gà không nổi, nhưng rất có tài quân sự.

Tương truyền rằng khi Hàn Tín điểm quân, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi báo cáo số dư. Từ đó ông tính chính xác quân số đến từng người.

Gần đây, định lý số dư Trung Quốc có nhiều ứng dụng trong các bài toán về số nguyên lớn áp dụng vào lý thuyết mật mã.



CƠ SỞ TOÁN HỌC

ĐỊNH LÝ SỐ DƯ TRUNG QUỐC
CHINESE THEOREM OF REMAINDERS

Định lý:

Cho n số nguyên dương $m_1, m_2, m_3, \ldots m_n$ đôi một nguyên tố cùng nhau. Khi đó hệ đồng dư tuyến tính:

$$\begin{cases} x \equiv a_i (mod\ m_i) \\ i = \overline{1,n} \end{cases}$$

có nghiệm duy nhất modulo M = $m_1\ m_2 \ldots\ m_m$

Định lý số dư Trung Quốc khẳng định về sự tồn tại duy nhất của một lớp thặng dư các số nguyên thỏa mãn đồng thời nhiều đồng dư thức tuyến tính. Do đó có thể sử dụng định lý để giải quyết những bài toán về sự tồn tại và đếm các số nguyên thỏa mãn một hệ các điều kiện quan hệ đồng dư, chia hết…, hay đếm số nghiệm của phương trình đồng dư. Bản chất của bài toán Hàn Tín điểm binh là việc giải hệ phương trình đồng dư bậc nhất.

CƠ SỞ TOÁN HỌC

ĐỊNH LÝ SỐ DƯ TRUNG QUỐC
CHINESE THEOREM OF REMAINDERS

Định lý:

$$\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \quad\quad ... \\ x \equiv a_k (mod\ m_k) \end{cases}$$

trong đó m_1 , m_2,… ,m_k đôi một nguyên tố cùng nhau.

Hệ phương trình đồng dư nói trên có nghiệm duy nhất theo modulo M = $m_1\ m_2 \dots\ m_k$ là:

$$x \equiv\ a_1 \times M_1 \times y_1 + a_2 \times M_2 \times y_2 + \dots + a_k \times M_k \times y_k (mod\ M)$$

Trong đó:

$$M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, M_k = \frac{M}{m_k}$$

và :

$$y_1 = (M_1)^{-1}\ (mod\ m_1),$$
$$y_2 = (M_2)^{-1}\ (mod\ m_2),$$
$$\dots\dots\dots$$
$$y_k = (M_k)^{-1}\ (mod\ m_k),$$

trong đó: $(M_1)^{-1}\ (mod\ m_1)$ là nghịch đảo theo modulo của m_1

với : $y_1 = (M_1)^{-1}\ (mod\ m_1) \Leftrightarrow y_1 M_1 = 1\ (\text{mod}\ m_1)$

CƠ SỞ TOÁN HỌC

ĐỊNH LÝ SỐ DƯ TRUNG QUỐC
CHINESE THEOREM OF REMAINDERS

Ví dụ:

Một đội quân, nếu xếp hàng 3 thì dư ra 2 người, xếp hàng 5 thì dư ra 3 người còn xếp hàng 7 thì dư ra 5 người. Hãy tính chính xác quân số x của đội quân đó.

Giải hệ phương trình đồng dư:

$$\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 5(mod\ 7) \end{cases}$$

Ta có:

$$M = 3 \times 5 \times 7 = 105;\ M_1 = 5 \times 7 = 35$$
$$M_2 = 3 \times 7 = 21, M_3 = 3 \times 5 = 15.$$
$$y_1 = 35^{-1}(mod\ 3) = 2^{-1}(mod\ 3) = 2;$$
$$y_2 = 21^{-1}(mod\ 5) = 1^{-1}(mod\ 5) = 1$$
$$y_3 = 15^{-1}(mod\ 7) = 1^{-1}(mod\ 7) = 1$$

Từ đó:

$$x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 5 \times 15 \times 1(mod\ 105)$$
$$x \equiv 140 + 63 + 75\ (mod\ 105) \equiv 278\ (mod\ 105)$$
$$x \equiv 68(mod\ 105)$$

Như vậy x có dạng $x = 68 + k.105$, k là số nguyên bất kỳ

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Trường G_p:

Với p là một số nguyên bất kỳ, trên tập các lớp đồng dư theo modulo p, tức là $\mathbb{Z}/p\mathbb{Z}$, ta có thể thực hiện được các phép tính +, - , x như đã biết ở trên.

Khi p là một số nguyên tố thì mỗi phần tử khác 0, $\alpha \in \mathbb{Z}/p\mathbb{Z}$ ta luôn tìm được phần tử nghịch đảo $\alpha^{-1} \in \mathbb{Z}/p\mathbb{Z}$ theo nghĩa $\alpha.\alpha^{-1} \equiv 1(mod\ p)$ và do đó có thể thực hiện phép chia. Như vậy $\mathbb{Z}/p\mathbb{Z}$ có cấu trúc của một trường và ta ký hiệu trường này là G_p.

Tập các phần tử khác 0 của trường này lập thành một nhóm đối với phép nhân và được ký hiệu là G_p^*. Như vậy $G_p^* = G_p\{0\} = \{1, 2, \dots, p-1\}$, với p là số nguyên tố.

Một phần tử $g \in G_p^*$ được coi là phần tử sinh (hay căn nguyên thủy) của nhóm G_p^* nếu như tập các lũy thừa của g cũng chính là nhóm này, tức là 2 tập sau đây trùng nhau

$$\{g, g^2, \dots, g^{p-1}\}, \{1, 2, \dots, p-1\}$$

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Ví dụ:

Với p. Các phần tử của $\mathbb{Z}/p\mathbb{Z}$ là các lớp đồng dư của {1, 2, …, p-1}
(tập hợp các nguyên tố cùng nhau với p)

Ta có:

p=11, {1, 2,..,10}

m :	$m^k (mod\ 11)$
1 :	1
2 :	2, 4, 8, 5, 10, 9, 7, 3, 6, 1
3 :	3, 9, 5, 4, 1
4 :	4, 5, 9, 3, 1,
5 :	5, 3, 4, 9, 1,
6 :	6, 3, 7, 9, 10, 5, 8, 4, 2, 1
7 :	7, 5, 2, 3, 10, 4, 6, 9, 8, 1
8 :	8, 9, 6, 4, 10, 3, 2, 5, 7, 1 (*)
9 :	9, 4, 3, 5, 1
10:	10, 1

2, 6, 7, 8 căn nguyên thủy modulo 11.

p=14, {1, 3, 5, 9, 11, 13}

m :	$m^k (mod\ 14)$
1 :	1
3 :	3, 9, 13, 11, 5, 1
5 :	5, 11, 13, 9, 3, 1
9 :	9, 11, 1
11:	11, 9, 1
13:	13, 1

3 và 5 là căn nguyên thủy của modulo 14.

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Nếu g là phần tử sinh (căn nguyên thủy) của nhóm G_p^* còn b là một số nguyên tố cùng nhau với (p -1) (b, (p-1))=1 thì g^b cũng là một phần tử sinh (căn nguyên thủy) của nhóm G_p^*

Do đó, số các phần tử sinh của nhóm G_p^* đúng bằng số các số nguyên tố cùng nhau với (p-1), tức là bằng $f(p-1)$.

Ví dụ trên G_{11}^*, ta tính được số phần tử sinh của nhóm G_{11}^* là:
$f(11-1) = f(10) = f(2.5) = f(2).f(5) = (2-1)(5-1) = 4$

2 là phần tử sinh của G_{11}^*. Thấy rằng 7 là số nguyên tố cùng nhau với 10 (=11-1) cho nên $2^7 (mod\ 11) = 7$ cũng là một phần tử sinh của G_{11}^*.

Cho phần tử sinh $g \in G_p^*$. Khi đó mọi phần tử bất kỳ $h \in G_p^*$ có thể biểu diễn dưới dạng một lũy thừa nào đó của g. Tuy nhiên vấn đề tìm ra số x để có được biểu diễn $h = g^x$ là vô cùng gian nan, và được mang danh là bài toán logarit rời rạc.

Một điều thú vị là tính khó giải của bài toán này không làm cho người ta "khó chịu", mà ngược lại đã làm vui lòng các nhà mã hóa thời hiện đại.

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Trường G_{2^n}:

Đây cũng là một loại trường hữu hạn phần tử, nhưng có bản chất khác biệt so với loại trường hữu hạn đã xem xét ở trên.

Ta cho $G_2(x)$ là tập hợp các đa thức với hệ số nằm trong trường G_2. Có thể chỉ ra rằng tập này có 2 đa thức bậc 0 (là 2 hằng số 0,1), 2 đa thức bậc 1 (x và x+1), tức là có 4 đa thức bậc không vượt quá 1, và không khó để ta có thể nhận ra rằng, với mỗi số tự nhiên n, ta có tất cả 2^{n+1} đa thức với bậc không vượt quá n, có dạng tổng quát như sau

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_i \in G_2 = \{0,1\}$$

Hai đa thức được cộng hoặc nhân với nhau theo quy tắc thông thường, chỉ lưu ý các hệ số là những phần tử của trường G_2, trong đó 1+1=0. Ví dụ:

$$(x^4 + x^2 + x)(x^2 + x) = x^6 + x^5 + x^4 + x^3 + x^3 + x^2 = x^6 + x^5 + x^4 + x^2$$

Đa thức gọi là bất khả quy (trên một trường nào đó) nếu nó không thể phân tích thành tích của các đa thức bậc nhỏ hơn.

Ví dụ:

$x^2 - 3, x^2 + 3$ là những đa thức bất khả quy trên trường số hữu tỷ, nhưng trên trường số thực thì chỉ có $x^2 + 3$ là *bất khả quy*, còn $x^2 - 3$ là *khả quy*.

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Trường G_{2^n}:

Tương tự như trên $\mathbb{Z}$, trên tập $G_2(x)$ ta cũng có phép tính đồng dư theo modulo một đa thức(một phần tử) nào đó, khi đó $G_2(x)$ sẽ được phân thành các lớp với các đại diện là đa thức bậc thấp hơn đa thức ta đã lấy làm modulo.

Ví dụ: Nếu cho đa thức $x^3 + x + 1$(bất khả quy) làm modulo thì tập $G_2(x)/(x^3 + x + 1)$ gồm các đa thức bậc nhỏ hơn 3, gồm tập $\{0, 1, x, x + 1, x^2 + 1, x^2 + x + 1\}$, trong đó đại diện của phần tử 0 chính là đa thức chọn làm modulo, nghĩa là $x^3 + x + 1 = 0$. Trên tập này ta có thể thực hiện các phép cộng, trừ, nhân thông thường với lưu ý $x^3 = x + 1$, vì điều này tương đương với $x^3 + x + 1 = 0$ (trên G_2).

Ta có:
$(x^2 + x + 1)(x + 1) = x^3 + 1 \equiv (x + 1) + 1 = x (mod\ x^2 + x + 1)$.
Ngoài ra, trên tập $G_2(x)/(x^3 + x + 1)$ ta thấy rằng:

$$x^4 = x^3 x = (x + 1)x = x^2 + x.$$

Trong trường hợp tổng quát, người ta chứng minh được rằng, với mỗi đa thức bất khả quy $GF_d(x)$ với bậc d, tập hợp $G_2(x)/GF_d(x)$ là một trường chứa đúng 2^d phần tử, ký hiệu là G_{2^d}; mỗi phần tử của nó được đại diện bởi một đa thức với bậc không vượt quá $d - 1$.

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Trường G_{2^n}:

Ta cũng chứng minh được rằng tập các phần tử khác 0 của trường G_{2^d}, được ký hiệu là $G_{2^d}^*$, cũng lập thành một nhóm và được sinh bởi một phần tử nào đó, có nghĩa là cũng có cấu trúc tương tự như nhóm G_p^* đã được xét. Phần tử sinh (căn nguyên thủy) của nó cũng phải có các lũy thừa bậc là ước của $(2^d - 1)$ khác đơn vị, và số lượng phần tử sinh trong nhóm này là $f(2^d - 1)$.

Ta dễ dàng thấy rằng x là phần tử sinh của $G_{2^3}^* = G_8^*$. Thật vậy, với $g = x$, ta có:
$g^2 = x^2, g^3 = x^3 = x + 1, g^4 = x^4 = x^3x = (x + 1)x = x^2 + x, g^5 = x^4x = x^2 + x + 1, g^6 = x^6 = x^3x^3 = x^2 + 1, g^7 = x^7 = x^6x = x^3 + x = 1$

Một phần tử của nhóm $G_{2^3}^*$ được gọi là *chính phương* nếu nó là bình phương của một phần tử khác trong nhóm.

Như vậy, trên G_{2^d}, chúng ta làm việc với 2 phép toán đồng dư: các hệ số được lấy theo modulo 2, còn các đa thức thì lấy theo modulo một đa thức bất khả quy (đã chọn).

Ví dụ: với trường G_8 đã xét ở trên, ta làm việc trên $\mathbb{Z}(x)$ với 2 phép toán đồng dư: các hệ số theo $mod\ 2$ và các đa thức với $mod\ x^2 + x + 1$.

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Trường G_{2^n}:

Mỗi phần tử(đa thức) của trường G_{2^d} (hay nhóm $G_{2^d}^*$) có thể được biểu diễn một cách dễ dàng trên máy tính bởi một xâu chuỗi nhị phân(binary) lập thành từ các hệ số của đa thức tương ứng.
Ví dụ:
$x^4 + x^2 + 1 = 1.x^4 + 0.x^3 + 1.x^2 + 0.x + 1$ sẽ được biểu diễn bởi chuỗi nhị phân(binary) 10101.
Chính vì vậy, trường hữu hạn dạng G_{2^d} thường hay được sử dụng nhiều hơn là G_p, nhất là khi p khá lớn (ví dụ: $p \approx 10^{100} \approx 2^{333}$, tức là với d vào khoảng 333 trở lên). Khi đó số lượng phần tử là quá nhiều cho nên việc biểu diễn chúng là một vấn đề nan giải.

Lưu ý:

Hoàn toàn tương tự như trên, ta có thể xây dựng các trường hữu hạn dạng $G_{p^d}^*$, với p là một số nguyên tố bất kỳ (thay vì với $p = 2$). Khi $p > 2$, ta có thể chỉ ra rằng một phần tử là chính phương khi và chỉ khi lũy thừa của nó với bậc $(p^d - 1)/2$ chính là đơn vị (và ta cũng tìm được thuật toán để "khai căn" số chính phương này).

CƠ SỞ TOÁN HỌC

TRƯỜNG HỮU HẠN

Bài toán logarit rời rạc trên trường hữu hạn:

Cho trước nhóm G_p^* và một phần tử sinh (căn nguyên thủy) nào đó $g \in G_p^*$. Với một phần tử b trong nhóm này, hãy tìm số nguyên x thỏa mãn phương trình $g^x = b$.
Số nguyên x như vậy được ký hiệu là $log_g b$.

Ví dụ:
Cho p=101, ta có 2 là phần tử sinh của nhóm G_{101}^*. Với b=5, hãy cho biết 2 mũ bao nhiêu thì đồng dư với 5 theo modulo 101?
Khi đó ta phải ngồi đoán "mò" để ra được câu trả lời là 24. Với b=6? Cũng lại tiếp tục ngồi dò từng số tiếp cho đến khi ra được câu trả lời là 70. Tóm lại, nếu không có 1 cách tính gì đặc biệt thì cứ thử cho đã trước khi phải tính tới $b^{100}(mod 101)$.
Bài toán là rất khó khi p đủ lớn. Khi đó, ngay cả với những máy tính có độ tính toán lớn, cũng đành bó tay trước bài toán này.
Tuy nhiên, sau này sẽ thấy, bài toán chỉ thực sự khó khi p-1 không phải là tích của các số nguyên tố nhỏ(vì trong trường hợp đó có thể tìm ra cách tính logarit dễ dàng hơn).

Tóm lại, bài toán logarit rời rạc trên trường hữu hạn G_p có độ phức tạp cao hơn so với trên trường G_{2^d}. Nhưng việc triển khai các tính toán trên máy tính là G_{2^d}. Cho nên, trong thực tế, bài toán logarit rời rạc thường được xem xét trên trường G_{2^d} nhiều hơn là trên trường G_p.

CƠ SỞ TOÁN HỌC

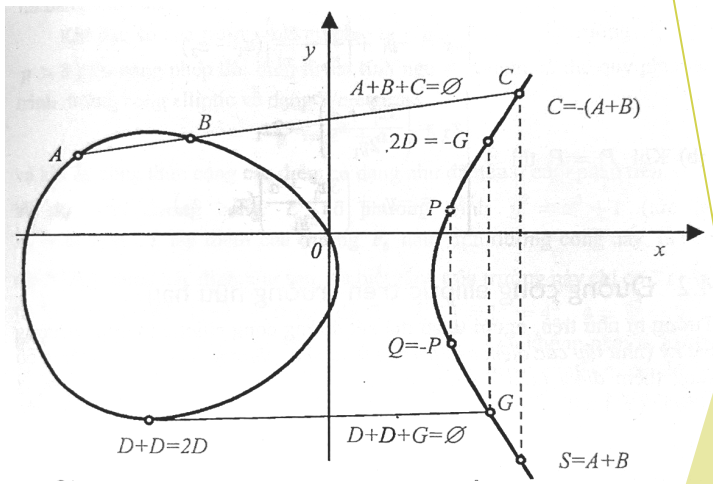
ĐƯỜNG CONG ELLIPTIC

Đường cong elliptic là tập các điểm thỏa mãn phương trình có dạng sau đây:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

và ngoài ra được bổ sung thêm 1 điểm nữa, gọi là điểm tại vô cùng, được ký hiệu là $\emptyset$. Nói một cách khác, đây là một điểm người ta quy ước ra và hình dung nó như là điểm "dính" 2 đầu của các đường thẳng song song với trục tung. Nó được xem như là điểm "làm đầy" hay "điểm nóng" đối với đường cong tạo bởi tập điểm thỏa mãn phương trình nói trên.

Trên tập điểm của ECC, ta sẽ thiết lập phép tính cộng các điểm để biến nó thành một nhóm.
Quy tắc cộng: tổng của 3 điểm a, b, c thẳng hàng (cùng ở trên 1 đường cong) là bằng điểm tại vô cùng, tức là $a + b + c = \emptyset$ (tại điểm vô cùng được quy ước là 0 – điểm của phép cộng.
Từ quy tắc chung này, ta suy ra nguyên tắc lấy điểm nghịch đảo và phép cộng các cặp 2 điểm như sau:



- Khi 2 điểm P, Q (của ECC) cùng năm trên 1 đường thẳng đứng thì nó thẳng hàng với điểm vô cùng $P + Q + \emptyset = \emptyset$ hay $P = -Q$. Vậy 2 điểm (nằm trên ECC) có cùng hoành độ là nghịch đảo của nhau.

- Khi 2 điểm A, B (của ECC) không năm trên cùng 1 đường thẳng đứng(tức khác nhau về hoành độ), thì tồn tại 1 điểm C (trên ECC) thẳng hàng với 2 điểm này, và ta có $A + B + C = \emptyset \; hay \; A + B = -C$.

CƠ SỞ TOÁN HỌC

ĐƯỜNG CONG ELLIPTIC

Ví dụ:

Phép cộng 2 điểm (khác hoành độ) $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, $x_1 \neq x_2$ có thể tính theo công thức: $P_1 + P_2 = P_3 = (x_3, y_3)$, trong đó:

$$\begin{cases} x_3 = \alpha^2 + a_1\alpha - (x_1 + x_2 + a_2) \\ y_3 = \alpha(x_1 - x_3) - a_1 x_3 - a_3 - y_1 \end{cases}, \text{với } \alpha = \frac{y_2 - y_1}{x_2 - x_1}$$

Còn công thức cộng một điểm với chính nó, tức là khi $P_1 = P_2$, thì phức tạp hơn nhiều (vì phải tính tiếp tuyến thông qua đạo hàm), và người ta không mấy khi nhớ được công thức tổng quát trên với giá trị α phức tạp hơn hẳn:

$$\alpha = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

Đối với đường cong elliptic có dạng Weierstrass:

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

$(a_1 = a_2 = a_3 = 0)$, thì công thức tính phần nào đơn giản hơn

Khi $x_1 \neq x_2$ thì $\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2) \\ y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) \end{cases}$

Khi $P_1 = P_2$ thì $\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) \end{cases}$

CƠ SỞ TOÁN HỌC

ĐƯỜNG CONG ELLIPTIC

Đường cong elliptic trên trường hữu hạn:

Ta xét ECC (E) trên trường G_p, với p là số nguyên tố lớn hơn 2. Tập hợp các điểm của đường cong (E) sẽ được ký hiệu là $E(G_p)$. Đây là một tập hợp điểm rời rạc, không phải là một "đường cong" theo nghĩa thông thường, và do đó không có hình ảnh minh họa như trường số thực. Các hình ảnh về "tiếp tuyến" theo nghĩa cổ điển tuy không còn nhưng khái niệm về "nghiệm bội" thì vẫn vậy, và công thức cộng các điểm vẫn hoàn toàn có thể thực hiện được.
Một điều thú vị là chính các "đường cong" rời rạc này đã đem lại một tương lai mới cho công nghệ mã hóa.

Ta biết rằng trên nhóm G_p^* thì một nửa số phần tử là "chính phương". Ví dụ trong nhóm G_{13}^* có 6 số "chính phương" là 1, 3, 4, 9, 10, 12, vì:

$$1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12, 6^2 = 10, 7^2 = 10, 8^2 = 12, 9^2 = 3, 10^2 = 9, 11^2 = 4, 12^2 = 1.$$

Nếu g là một phần tử sinh nhóm (căn nguyên thủy) thì các lũy thừa bậc chẵn của nó là số "chính phương", các lũy thừa bậc lẽ thì không. Như vậy phương trình $y^2 = a$, hoặc có 2 nghiệm, hoặc là vô nghiệm.
Ví dụ:
Ta có phương trình $y^2 = 3$, có 2 nghiệm là 4 và 9(rõ ràng $9 \equiv -4 \ mod \ 13$), nên có thể viết nghiệm dưới dạng $y = \pm 4$

Khi đặc số của trường không phải là 2 hay 3 (như các trường G_p, với p>3) thì bằng phép đổi biến tuyến tính người ta luôn có thể quy phương trình đường cong elliptic về dạng Weierstrass:

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

và khi đó công thức cộng các điểm có dạng như đã nêu trên.

CƠ SỞ TOÁN HỌC

ĐƯỜNG CONG ELLIPTIC

Đường cong elliptic trên trường hữu hạn:

Ví dụ:
Với đường cong E có phương trình $y^2 = x^3 + 1$ (tức là $a_4 = 0, a_6 = 0$), tập điểm của trường G_5 nằm trên đường cong này, tức là tập $E(G_5)$, được xác định như sau:
Trên trường này chỉ có 3 phần tử "chính phương" là 0, 1, 4 (trong đó $0 = 0^2, 1 = 1^2 = 4^2, 4 = 3^2 = 2^2$), do đó với x là 1 hay 3 ta thấy ngay phần tử $x^3 + 1$ không phải là chính phương, và như vậy hoành độ của các điểm trên đường cong chỉ có thể là 1 trong các số còn lại: 0, 2, 4. Thế vào phương trình, ta nhận được các điểm sau:
A=(0, 1), B=(0, -1)=(0, 4), C=(2, 2), D=(2, -2)=(2, 3), G=(4, 0) và điểm $\emptyset$. Như vậy $E(G_5)$ có 6 điểm rời rạc và chẳng có gì giống với đường cong theo cách hiểu thông thường.

Lấy điểm D=(2, 3) trên "đường cong", ta tính được các bội của điểm này (theo công thức ở phần cuối mục trên) như sau:

$$2D = (0,1) = A;\ 3D = (4,0) = G;\ 4D = (0,4) = B;\ 5D = (2,2) = C;\ 6D = 2D + 4D = \emptyset$$

(vì rằng 2D và 4D có cùng hoành độ, nên là nghịch đảo của nhau).
Tóm lại, các bội của điểm D lại cho ta tất cả các điểm trên đường cong hay nói cách khác, điểm D có thể được xem là phần tử sinh của tập $E(G_5)$.

CƠ SỞ TOÁN HỌC

TÓM LƯỢC

Các tính toán sử dụng trong công nghệ mã hóa hiện đại đều có độ phức tạp rất cao. Ngoài việc các phép toán thường gặp là không đơn giản chút nào, ta còn phải làm việc với các số cực lớn, các đối tượng trừu tượng như các số đại số, các phần tử trên trường hữu hạn hoặc các điểm trên đường cong elliptic.

Hiển nhiên, các tính toán này không thể thực hiện được bằng thủ công, dù có cố gắng đến đâu đi chăng nữa, do đó việc học và nghiên cứu công nghệ mã không thể thiếu sự hỗ trợ của các phương tiện tính toán trên máy tính. Việc thiết lập các gói chương trình có khả năng thực hiện được các tính toán như yêu cầu trong công nghệ mã thường nằm ngoài khả năng của con người. Vì vậy sự hỗ trợ của các chương trình tính toán chuyên dụng là vô cùng cần thiết.