A	B	$A \Rightarrow B$	$B \Rightarrow A$	$(\neg B) \Rightarrow (\neg A)$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	T
F	F	T	T	T

Congruence (8, 9, 10, 11)

- $a \equiv b \pmod m \Rightarrow$ ($i \in \mathbb{Z}^+$)
  - CAM: $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \pmod m$
    $a_1 \cdots a_n \equiv b_1 \cdots b_n \pmod m$
  - CP: $a^n \equiv b^n \pmod m$
- CD: $ac \equiv bc \pmod m$, $\gcd(c, m) = 1 \Rightarrow a \equiv b \pmod m$
- ★ LCT: $g = \gcd(a, m)$ { $g \nmid c$: $ax \equiv c \pmod m$ 无解; $g \mid c$: $ax \equiv c \pmod m$ g 个解在 1 和 m 之间
- ★ FLT: p : prime, $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$
- $\gcd(a, m) = 1 \Rightarrow$ Euler's Formula: $a^{\varphi(m)} \equiv 1 \pmod m$
  $\Rightarrow \{b_1 a, \cdots, b_{\varphi(m)} a \pmod m\} = \{b_1, \cdots, b_{\varphi(m)} \pmod m\}$
- $\gcd(m, n) = 1 \Rightarrow$ ★ CRT: $\begin{cases} x \equiv b \pmod m \\ x \equiv c \pmod n \end{cases}$ 1 sol: $x \in [0, mn)$
  $\Rightarrow$ SMT: $\begin{cases} x \equiv a \pmod m \\ x \equiv a \pmod n \end{cases}$ $x \equiv a \pmod{mn}$
  $\Rightarrow F(mn) = F(m)F(n)$

Primitive Roots (11.27.28.29)

- $\phi(m) = \#\{a : 1 \le a \le m,\ \gcd(a, m) = 1\}$

  Phi function formula: ① $\phi(p^k) = p^k - p^{k-1}$

  ② $\phi(mn) = \phi(m)\phi(n)$

  $F(n) = \phi(d_1) + \cdots + \phi(d_r) = n$ ($d_1, \cdots, d_n$ 是 n 的因数)

- Primitive Root mod p $\quad e_p(g) = p-1$

  ↓

  $x^{p-1} \equiv 1 \pmod p$

  ep. 3 & 5 are primitive root mod 7

$p = 7$
$1^1 \equiv 1 \pmod 7$
$2^3 \equiv 1 \pmod 7$
$3^6 \equiv 1 \pmod 7$
$4^3 \equiv 1 \pmod 7$
$5^6 \equiv 1 \pmod 7$
$6^2 \equiv 1 \pmod 7$

$\psi(6) = 2$, 5和6

- $e_p(a)$: $a^{e_p(a)} \equiv 1 \pmod p$ 最小的正数
- $\psi(d) = \#(1 \le a < p : e_p(a) = d) = \phi(d)$

  ↑ when $n \mid p-1$, $n = d$ is prime

- Order divisibility property $\quad p \nmid a \wedge a^n \equiv 1 \pmod p \Rightarrow e_p(a) \mid n \quad e_p(a) \mid p-1$

- Primitive Root Thm $\quad \exists\ \phi(p-1)$ 个 primitive root mod p.

- $\exists\ \infty$ ps s.t. 2 is primitive root (mod p)

- 若 m 是 prime, 则 $\psi(p) = \phi(m) \quad e_m(a) \mid \phi(m)$

- Indice

I	1	2	3	4	5	6	7	8	9	10	11	12
$2^I \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

a	1	2	3	4	5	6	7	8	9	10	11	12
$I(a)$	12	1	4	2	9	5	11	3	8	10	7	6

Table of Indices Modulo 13 for the Base 2

$I(ab) \equiv I(a) + I(b) \pmod{p-1}$

$I(a^k) \equiv k\, I(a) \pmod{p-1}$

↓

$2 \mid I(a) \Rightarrow a$ is QR

$\Rightarrow \left(\frac{a}{p}\right) = 1$

Square Modulo (20, 4, 22, 23)

Legendre symbol

$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{QR (quadratic residue)} \\ -1 & \text{NR (nonresidue)} \end{cases}$

a is QR mod p

$a \equiv x^2 \pmod p$

判断式：$(p-b)^2 \equiv b^2 \pmod p$

找QR

b	b^2
0	0
1	1
2	4
3	9
4	3
5	12
6	10
7	10
8	12
9	3
10	9
11	4
12	1

Modulo 13

• Quadratic Residue Multiplication Rule

I $\quad QR \times QR = QR \qquad QR \times NR = NR \qquad NR \times NR = QR$

II $\quad \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

• p (odd prime) 中存在 $\frac{p-1}{2}$ 个 QR. $\frac{p-1}{2}$ 个 NR.

• Euler's Criterion

$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$

p	3	5	7	11	13	17	19	23	29	31
Solution(s) to $x^2 \equiv -1 \pmod p$	NR	2, 3	NR	NR	5, 8	4, 13	NR	NR	12, 17	NR

• Quadratic Reprocity

快速计算QR

I. $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases} \quad \equiv (-1)^{\frac{p-1}{2}}$

II. $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases} \quad \equiv (-1)^{\frac{p^2-1}{8}}$

Law.. $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$

$$\begin{aligned}
\left(\frac{55}{179}\right) &= \left(\frac{5}{179}\right)\left(\frac{11}{179}\right) \\
&= \left(\frac{179}{5}\right) \times (-1) \times \left(\frac{179}{11}\right) && \text{since } 5 \equiv 1 \pmod 4 \text{ and} \\
&&& \quad 11 \equiv 179 \equiv 3 \pmod 4, \\
&= \left(\frac{4}{5}\right) \times (-1) \times \left(\frac{3}{11}\right) && \text{since } 179 \equiv 4 \pmod 5 \text{ and} \\
&&& \quad 179 \equiv 3 \pmod{11}, \\
&= 1 \times (-1) \times \left(\frac{3}{11}\right) && \text{since } 4 = 2^2 \text{ is a square,} \\
&= 1 \times (-1) \times (-1) \times \left(\frac{11}{3}\right) && \text{since } 3 \equiv 11 \equiv 3 \pmod 4, \\
&= 1 \times (-1) \times (-1) \times \left(\frac{2}{3}\right) && \text{since } 11 \equiv 2 \pmod 3, \\
&= 1 \times (-1) \times (-1) \times (-1) && \text{since 2 is a nonresidue mod 3,} \\
&= -1.
\end{aligned}$$

$\mu(a,p)$ = (# $a, 2a, \cdots, Pa \pmod p$ 中负数个数)

We illustrate by computing Gauss's μ value for $p = 13$ and $a = 7$, so $P = \frac{13-1}{2} = 6$. We start with the six numbers

$$1 \cdot 7, \quad 2 \cdot 7, \quad 3 \cdot 7, \quad 4 \cdot 7, \quad 5 \cdot 7, \quad 6 \cdot 7$$

and reduce them modulo 13 to get numbers between -6 and 6. This yields

$$\begin{aligned} 1 \cdot 7 &= 7 \equiv -6 \pmod{13} & 4 \cdot 7 &= 28 \equiv 2 \pmod{13} \\ 2 \cdot 7 &= 14 \equiv 1 \pmod{13} & 5 \cdot 7 &= 35 \equiv -4 \pmod{13} \\ 3 \cdot 7 &= 21 \equiv -5 \pmod{13} & 6 \cdot 7 &= 42 \equiv 3 \pmod{13} \end{aligned}$$

Three of the residues are negative, so $\mu(7, 13) = 3$.

- 计算 $\mu(a,b)$ (似乎没啥用)

$P = \frac{p-1}{2}$, $p \nmid a$, a odd. $\Rightarrow \sum_{k=1}^{P} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2$

- Gauss's Criterion

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a,b)}$$

$$\begin{aligned} \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{\mu(p,q)} \cdot (-1)^{\mu(q,p)} \\ &= (-1)^{\mu(p,q)+\mu(q,p)} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \end{aligned}$$

判断 $ax^2+bx+c \equiv 0 \pmod k$ 是否有解

1. 解 $ax^2+bx+c=0$
2. 判断"根号里的数"是否是 QR mod k.

$$\left(\frac{\square}{k}\right)$$

$x^2+12x-37 \equiv 0 \pmod{431}$

$x = \frac{-12 \pm \sqrt{12^2+4\times37}}{2} = -6 \pm \frac{\sqrt{292}}{2}$

$x^2 \equiv 292 \pmod{431}$

↓ determine whether 292 is QR mod 431.

$$\begin{aligned} \left(\frac{292}{431}\right) &= \left(\frac{2}{431}\right)^2\left(\frac{73}{431}\right) && \text{(iii)} \\ &= \left[(-1)^{\frac{431^2-1}{8}}\right]^2\left(\frac{431}{73}\right)(-1)^{\frac{431-1}{2}\cdot\frac{73-1}{2}} && \text{(iv)} \\ &= \left(\frac{66}{73}\right) && \text{(i)} \\ &= \left(\frac{2}{73}\right)\left(\frac{3}{73}\right)\left(\frac{11}{73}\right) && \text{(iii)} \\ &= (-1)^{\frac{73^2-1}{8}}\left(\frac{73}{3}\right)^{\frac{73-1}{2}\cdot\frac{3-1}{2}}\left(\frac{73}{11}\right)^{\frac{73-1}{2}\cdot\frac{11-1}{2}} && \text{(v) (iv)} \\ &= \left(\frac{1}{3}\right)\left(\frac{7}{11}\right) && \text{(i)} \\ &= 1\cdot\left(\frac{11}{7}\right)\cdot(-1)^{\frac{11-1}{2}\cdot\frac{7-1}{2}} && \text{(v) (iv)} \\ &= \left(\frac{4}{7}\right)(-1) && \text{(i)} \\ &= \left(\frac{2}{7}\right)^2(-1) && \text{(iii)} \\ &= (-1)^{\frac{7^2-1}{8}}(-1) && \text{(iv)} \\ &= -1 \end{aligned}$$

So $x^2 \equiv 292 \pmod{431}$ has no solution

So $x^2+12x-37 \equiv 0 \pmod{431}$ has no solutions.

Successive Squaring 求 $a^k \pmod m$

1. $k = u_0 + 2u_1 + 2^2u_2 + \cdots + 2^r u_r$
2. $a^{2^r} \equiv (a^{2^{r-1}})^2 \equiv A_{r-1}^2 \equiv A_r \pmod m$
3. $A_0^{u_0} \cdots A_r^{u_r} \equiv a^k \pmod m$

※ 结合 FLT. $a^{m-1} \equiv 1 \pmod m \Rightarrow m$ 是 prime

kth root mod m (求 $x^k \equiv b \pmod m$)

eg. $x^{11} \equiv 5 \pmod{19}$

已知 $\gcd(b, m) = 1$ $\gcd(k, \phi(m)) = 1$. 求 $x^k \equiv b \pmod m$

→ 若 $\gcd(b, m) \neq 1$ 则分解 m. 用 CRT.

1. 求 $\phi(m)$
2. 找 u. v s.t $ku + \phi(m)v = 1$
3. $x \equiv b^u \pmod m$ (用 SS)

求 $a^{???} \equiv 1 \pmod m$

↓

$\phi(m)$

求 x. $x \equiv a^b \pmod m$ (← 欧) $x \neq a$

1. 求 $\phi(m)$

   $\gcd(m, n) = 1$ $\phi(mn) = \phi(m)\phi(n)$

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

2. $b \to b \div \phi(m)$ 的余数

$a^2 \equiv -1 \pmod m$ (← 找 p 也行) $m = p_1 p_2$.

1. By CRT $\begin{cases} a^2 \equiv -1 \pmod{p_1} \\ a^2 \equiv -1 \pmod{p_2} \end{cases}$
2. 根据 QR 求 $\left(\frac{-1}{p_1}\right)$ & $\left(\frac{-1}{p_2}\right)$

   ( ) = -1 NR 无解

   ( ) = 1 QR 有解

Sum of 2 Squares (24, 25)

- 判断: Which numbers are sum of 2 squares?

1) factor m: $m = p_1 p_2 \cdots p_r M^2$.

$m = a^2+b^2 \iff p_i = 2 \ / \ p_i \equiv 1 \pmod 4$

2) $m = a^2+b^2$ $\gcd(a,b)=1 \iff$ $\begin{cases} m \text{ odd}. \wedge\ m \text{ in质因数} \equiv 1 \pmod 4 \\ m \text{ even}. \ \frac{m}{2} \text{ odd}. \ \frac{m}{2} \text{ in质因数} \equiv 1 \pmod 4 \end{cases}$

3) p is sum of 2 squares $\iff \left(\frac{-1}{p}\right) = 1$

$\iff p \equiv 1 \pmod 4$

- 找 a & b. 方法: Divide & Conquer. $m = 1105$

→ Divide. 对 m 分解质因数 $m = 1105 = 5 \cdot 13 \cdot 17$

→ Conquer. 每个 p 写成 sum of 2 squares in 形式

→ Unity. 将 m 写成 sum of 2 squares in 形式

$5 = 2^2+1^2$
$13 = 3^2+2^2$
$17 = 4^2+1^2$

$m = 1105 = 5 \cdot 13 \cdot 17$

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

$= ((6+2)^2+(3-4)^2)(4^2+1^2)$

$= 33^2+4^2$

identity: $(u^2+v^2)(A^2+B^2) = (uA+vB)^2+(vA-uB)^2$

- Pythagorean Hypotenuse Proposition.

c is hypotenuse (斜边) of a primitive Pythagoren triple (a,b,c)

$\iff$ c is a product of primes each $\equiv 1 \pmod 4$.

Pythagorean Triples (2, 3)

- Pythagorean Triple theorem

$(a, b, c) = \left(st, \underbrace{\frac{s^2-t^2}{2}}_{\text{even}}, \underbrace{\frac{s^2+t^2}{2}}_{\text{odd}}\right)$

奇 偶 奇

区分 primitive 与非 primitive

Pell's Equation & Diophantine Approximation (32.33.34)

Let D be a positive integer that is not a perfect square.
Then Pell's Equation $x^2 - Dy^2 = 1$ always has solutions in positive integers.

通过 continued fraction algorithm 去找

给 positive int sol
求 int sol

$$x^2 - 83y^2 = 1$$

→ $r_0 = \sqrt{83}$. $a_0 = \lfloor \sqrt{83} \rfloor = 9$ $\therefore E_0 = 9$.

Check whether $(9, 1)$ is an available solution:

$9^2 - 83 \cdot 1^2 = -2 \neq 1$

$\therefore (9, 1)$ is not an available solution

→ $r_1 = \frac{1}{\sqrt{83} - 9}$ $a_1 = \lfloor \frac{1}{\sqrt{83} - 9} \rfloor = 9$ $\therefore E_1 = 9 + \frac{1}{9} = \frac{82}{9}$

Check whether $(82, 9)$ is an available solution:

$82^2 - 83 \cdot 9^2 = 6724 - 6723 = 1$

$\therefore (82, 9)$ is an available solution

→ 找 (x_1, y_1)

$$\underbrace{x - y\sqrt{D}}_{\leq \frac{1}{2}} = \frac{1}{x + y\sqrt{D}}$$

→ (x_k, y_k) (Pell's equation thm)

If (x_1, y_1) is the solution with smallest x_1, then every sol (x_k, y_k) can be obtained by taking powers. $x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$

存在 D $\Rightarrow$ 无数 (x, y) s.t. $|x - y\sqrt{D}| < \frac{1}{y}$

$\Rightarrow$ 无数 (x, y) s.t. $|x - y\alpha| < \frac{1}{y}$

α: irrational num

Pell-like equation $x^2 - Dy^2 = k$

→ 已知 $(197, 42)$ 是 $x^2 - 22y^2 = 1$ 的解. 求 $x^2 - 22y^2 = 9^{\leq k}$

两边同乘 k $9x^2 - 9 \cdot 22y^2 = 9$

找 $\sqrt{}$ $(3x)^2 - 22 \cdot (3y)^2 = 3^2$

$(197, 42) \longrightarrow (197 \times 3, 42 \times 3)$

Solution for Pell's equation $x^2 - ny^2 = 1$

n	x	y	n	x	y	n	x	y	n	x	y
1	–	–	33	23	4	65	129	16	97	62809633	6377352
2	3	2	34	35	6	66	65	8	98	99	10
3	2	1	35	6	1	67	48842	5967	99	10	1
4	–	–	36	–	–	68	33	4	100	–	–
5	9	4	37	73	12	69	7775	936	101	201	20
6	5	2	38	37	6	70	251	30	102	101	10
7	8	3	39	25	4	71	3480	413	103	227528	22419
8	3	1	40	19	3	72	17	2	104	51	5
9	–	–	41	2049	320	73	2281249	267000	105	41	4
10	19	6	42	13	2	74	3699	430	106	32080051	3115890
11	10	3	43	3482	531	75	26	3	107	962	93
12	7	2	44	199	30	76	57799	6630	108	1351	130
13	649	180	45	161	24	77	351	40	109	158070671986249	15140424455100
14	15	4	46	24335	3588	78	53	6	110	21	2
15	4	1	47	48	7	79	80	9	111	295	28
16	–	–	48	7	1	80	9	1	112	127	12
17	33	8	49	–	–	81	–	–	113	1204353	113296
18	17	4	50	99	14	82	163	18	114	1025	96
19	170	39	51	50	7	83	82	9	115	1126	105
20	9	2	52	649	90	84	55	6	116	9801	910
21	55	12	53	66249	9100	85	285769	30996	117	649	60
22	197	42	54	485	66	86	10405	1122	118	306917	28254
23	24	5	55	89	12	87	28	3	119	120	11
24	5	1	56	15	2	88	197	21	120	11	1
25	–	–	57	151	20	89	500001	53000	121	–	–
26	51	10	58	19603	2574	90	19	2	122	243	22
27	26	5	59	530	69	91	1574	165	123	122	11
28	127	24	60	31	4	92	1151	120	124	4620799	414960
29	9801	1820	61	1766319049	226153980	93	12151	1260	125	930249	83204
30	11	2	62	63	8	94	2143295	221064	126	449	40
31	1520	273	63	8	1	95	39	4	127	4730624	419775
32	17	3	64	–	–	96	49	5	128	577	51

Gaussian int $w = a+bi$

$N(w) = a^2+b^2$

unit: $\pm 1, \pm i$

Gaussian prime: $\Rightarrow \alpha$ in 因数为: $\pm\alpha \ \pm i\alpha \ \pm 1 \ \pm i$

- Gaussian prime Thm

Gaussian prime 与 unit $(\pm 1, \pm i)$ 乘以下3种形式:

i) $1+i$
ii) p: $p \equiv 3 \pmod 4$
iii) $u+vi$: $p \equiv 1 \pmod 4$ $\quad p = u^2+v^2$

- Gaussian divisibility Thm

i) $2 \mid N(\alpha) \Rightarrow 1+i \mid \alpha$
ii) $\pi = p \equiv 3 \pmod 4$ $\quad p \mid N(\alpha) \Rightarrow \pi \mid \alpha$
iii) $\pi = u+vi$ $\quad \bar{\pi} = u-vi$ $\Rightarrow \pi \mid \alpha$ or $\bar{\pi} \mid \alpha$

- Sum of 2 squares. $R(N)$

$D_1 = \#\{d : d \mid N \ . \ d \equiv 1 \pmod 4\}$ $\quad D_3 = \#\{d : d \mid N \ . \ d \equiv 3 \pmod 4\}$

$\Rightarrow N$ can be written as a sum of 2 squares in $R(N) = 4(D_1 - D_3)$ ways

- Common Divisor property

Let α, β be Gaussian integers $\alpha, \beta \neq 0$. $S = \{A\alpha + B\beta : \alpha, \beta \in G\}$

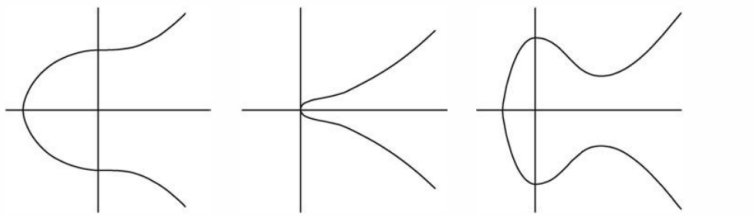
- Among all of the Gaussian integers in S, choose an element $g = a\alpha + b\beta$. has the smallest non-zero norm.
- $0 < N(g) \leq N(A\alpha + B\beta) \ \forall A, B \in G$. $\quad A\alpha + B\beta \neq 0 \Rightarrow g \mid \alpha, \ g \mid \beta$.

- Gaussian Prime Divisibility Property

$\pi \mid \alpha\beta$. $\alpha, \beta \in G \Rightarrow \pi \mid \alpha$ or $\pi \mid \beta$.

Elliptic curves

$y^2 = x^3 + ax^2 + bx + c$



$E_1 : y^2 = x^3 + 17$ $E_2 : y^2 = x^3 + x$ $E_3 : y^2 = x^3 - 4x^2 + 16$

- Mordell's Theorem

Let E be an elliptic curve given by $E: y^2 = x^3 + ax^2 + bx + c$

$\Delta E = -4a^3c + a^2b^2 - 4b^3 - 27c^2 + 18abc \neq 0.$

Then there is a finite list of sols: $P_1 = (x_1, y_1) \cdots P_r = (x_r, y_r)$

there exists an expression $P = P_{i1} \oplus P_{i2} \oplus \cdots \oplus P_{is}$.

- Thm

The only point with rational coordinates on the elliptic curve

$E_2: y^2 = x^3 + x$ is the point $(x, y) = (0, 0)$

- Siegel's Thm

Let E be elliptic curve $E: y^2 = x^3 + ax^2 + bx + c$. $a, b, c \in \mathbb{Z}$. $\Delta E \neq 0$

Then there are only finitely many sols in x, y

Let E be the curve $y^2 = x^3 - 30x + 133$. The points $P = (-7, 0)$ and $Q = (6, -13)$ both lie on E. Let L be the line through P and Q. Find the equation of L, and if P, Q and R are the three points which lie on both L and E, find the coordinates of R.

Let $L: y = ax + b$

$\rightarrow a = \frac{b-(-7)}{-13-0} = \frac{13}{-13} = -1$

$\rightarrow b$

substitute b into $(-7, 0)$

$0 = -(-7) + b$

$b = -7$

$\therefore L: y = -x - 7$

$y^2 = x^3 - 30x + 133$

$x^2 + 14x + 49 = x^3 - 30x + 133$

$x^3 - x^2 - 44x + 84 = 0$

$(x-2)(x-6)(x+7) = 0$

$x = 2 \quad x = 6 \quad x = -7$

	1	−1	−44	84
2		2	2	−84
	1	1	−42	0

	1	6	42
6		6	42
	1	7	0

$x = 2 \quad y^2 = x^3 - 30x + 133$

$= 2^3 - 30 \cdot 2 + 133$

$= 81$

$y = \pm 9$

$R = (2, -9)$

$R = (2, 9)$ X → Since $(2, 9)$ does not lie on $L: y = -x - 7$

So R can only be $(2, -9)$