Contents

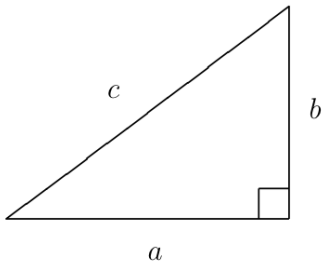
Preface v
Flowchart of Chapter Dependencies ix
Introduction 1
1 What Is Number Theory? 6
2 Pythagorean Triples 13
3 Pythagorean Triples and the Unit Circle 21
4 Sums of Higher Powers and Fermat's Last Theorem 26
5 Divisibility and the Greatest Common Divisor 30
6 Linear Equations and the Greatest Common Divisor 37
7 Factorization and the Fundamental Theorem of Arithmetic 46
8 Congruences 55
9 Congruences, Powers, and Fermat's Little Theorem 65
10 Congruences, Powers, and Euler's Formula 71
11 Euler's Phi Function and the Chinese Remainder Theorem 75
12 Prime Numbers 83
13 Counting Primes 90
14 Mersenne Primes 96
15 Mersenne Primes and Perfect Numbers 101
16 Powers Modulo m and Successive Squaring 111
17 Computing k^{th} Roots Modulo m 118
18 Powers, Roots, and "Unbreakable" Codes 123
19 Primality Testing and Carmichael Numbers 129
20 Squares Modulo p 141
21 Is -1 a Square Modulo p? Is 2? 148
22 Quadratic Reciprocity 159

23 Proof of Quadratic Reciprocity 171
24 Which Primes Are Sums of Two Squares? 181
25 Which Numbers Are Sums of Two Squares? 193
26 As Easy as One, Two, Three 199
27 Euler's Phi Function and Sums of Divisors 206
28 Powers Modulo p and Primitive Roots 211
29 Primitive Roots and Indices 224
30 The Equation $X^4+Y^4=Z^4$ 231
31 Square–Triangular Numbers Revisited 236
32 Pell's Equation 245
33 Diophantine Approximation 251
34 Diophantine Approximation and Pell's Equation 260
35 Number Theory and Imaginary Numbers 267
36 The Gaussian Integers and Unique Factorization 281
37 Irrational Numbers and Transcendental Numbers 297
38 Binomial Coefficients and Pascal's Triangle 313
39 Fibonacci's Rabbits and Linear Recurrence Sequences 324
40 Oh, What a Beautiful Function 339
41 Cubic Curves and Elliptic Curves 353
42 Elliptic Curves with Few Rational Points 366
43 Points on Elliptic Curves Modulo p 373
44 Torsion Collections Modulo p and Bad Primes 384
45 Defect Bounds and Modularity Patterns 388
46 Elliptic Curves and Fermat's Last Theorem 394
Further Reading 396
Index 397
47 The Topsy-Turvy World of Continued Fractions [online] 410
48 Continued Fractions and Pell's Equation [online] 426
49 Generating Functions [online] 442
50 Sums of Powers [online] 452
A Factorization of Small Composite Integers [online] 464
B A List of Primes [online] 466

2-3. Pythagorean Triples.

- def. pythagorean Triples (a,b,c)

$a^2+b^2=c^2$



- primitive pythagorean triple (PPT)

(a,b,c) 其中两两分别互质

(a,b,c) — 一奇一偶

注意区分 pythagorean triple 与 primitive ~

ex. $(3,4,5)$ $(5,12,13)$ $(7,24,25)$ $(9,40,41)$ $(15,8,17)$ ...

- pythagorean triples Theorem

$(a,b,c)=\left(st,\ \frac{s^2-t^2}{2},\ \frac{s^2+t^2}{2}\right)$ $(s>t\geq 1)$

奇 偶 奇

proof: Let a odd, b even.

$a^2+b^2=c^2$

$a^2=c^2-b^2=(c-b)(c+b)$

$$3^2=5^2-4^2=(5-4)(5+4)=1\cdot 9,$$
$$15^2=17^2-8^2=(17-8)(17+8)=9\cdot 25,$$
$$35^2=37^2-12^2=(37-12)(37+12)=25\cdot 49,$$
$$33^2=65^2-56^2=(65-56)(65+56)=9\cdot 121.$$

→ prove $(c-b)$ & $(c+b)$ have no common factors.

Let $d\mid c-b$ ∧ $d\mid c+b$.

∴ $d\mid (c+b)+(c-b)$ $\quad d\mid 2c$

$d\mid (c-b)-(c-b)$ $\quad d\mid 2b$.

∵ b & c has no common factor

∴ $d=1$ or $d=2$.

∵ $d\mid (c-b)(c+b)=a^2$ ∧ a is odd.

∴ $d=1$. $(c-b)$ & $(c+b)$ has no common factor

→ prove $(c-b)$ & $(c+b)$ are both squares

∵ $(c-b)$ & $(c+b)$ 互质. 且 $(c-b)(c+b)=a^2$

∴ 只可能为 square. $c+b=s^2$ $\quad c-b=t^2$.

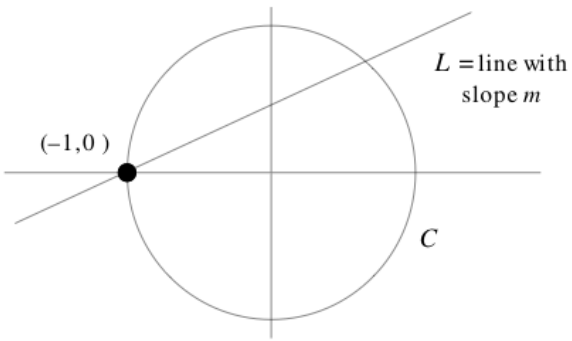
$c=\frac{s^2+t^2}{2}$ $\quad b=\frac{s^2-t^2}{2}$

∴ $a=\sqrt{(c-b)(c+b)}=st$

- Theorem

Every point on the circle $x^2+y^2=1$ can be obtained from the formula

$(x,y)=\left(\frac{1-m^2}{1+m^2},\ \frac{2m}{1+m^2}\right)$



proof. $a^2+b^2=c^2$

$\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$

Let $L: y=m(x+1)$

將 $y=m(x+1)$ 代入 $x^2+y^2=1$

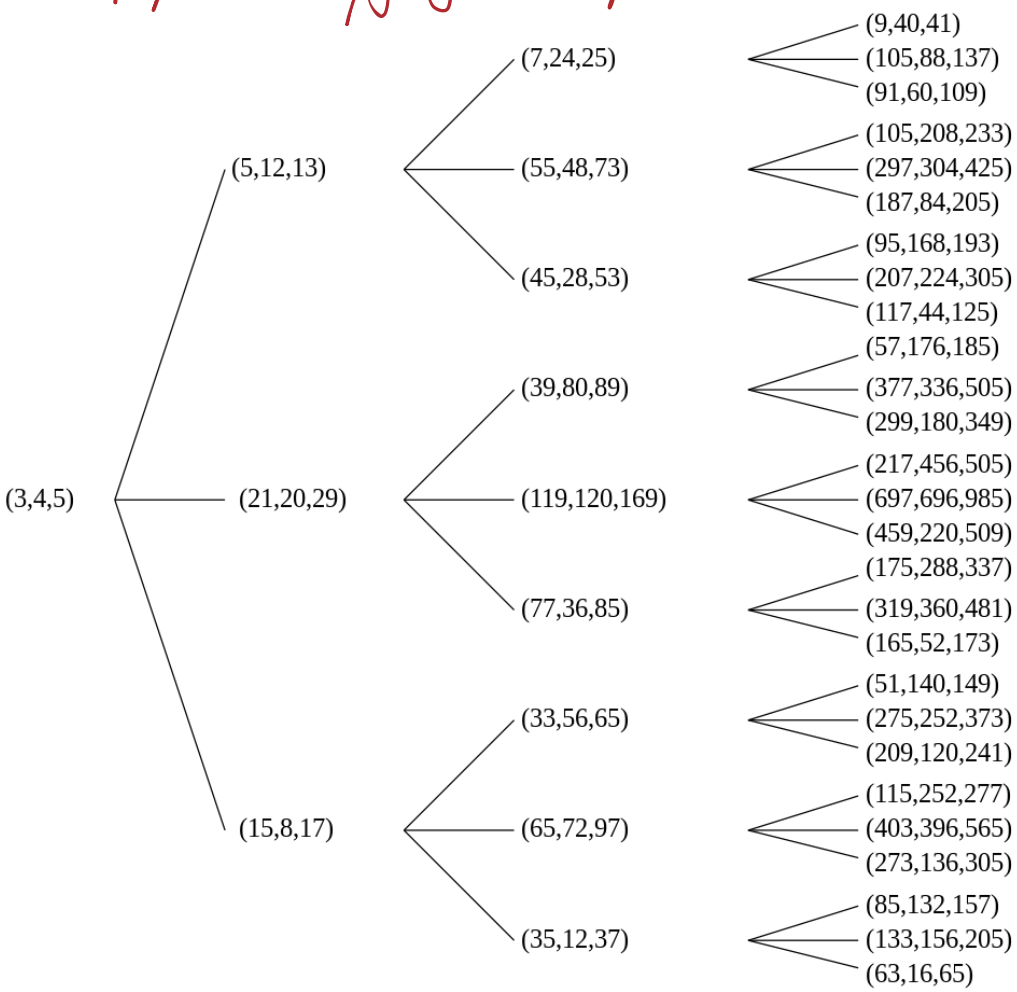
$x^2+(m(x+1))^2=1$

$(m^2+1)x^2+2m^2x+(m^2-1)=0$

$x=\frac{1-m^2}{1+m^2}$ $\quad y=m(x+1)=\frac{2m}{1+m^2}$

$\therefore (x,y)=\left(\frac{1-m^2}{1+m^2},\ \frac{2m}{1+m^2}\right)$

Tree of primitive pythagorean triple



8. Congruence

- def. congruent.

  a congruent to b mod m

  $a \equiv b \pmod m$

- property

$$\begin{cases} a_1 \equiv b_1 \pmod m \\ a_2 \equiv b_2 \pmod m \end{cases} \Rightarrow \begin{array}{l} a_1 \pm a_2 \equiv b_1 \pm b_2 \pmod m \\ a_1 a_2 \equiv b_1 b_2 \pmod m \end{array}$$

- Linear Congruence Theorem (LCT)

  Let $a, c, m \in \mathbb{Z}$. $m \geq 1$. $g = \gcd(a, m)$

  1) $g \nmid c \Rightarrow ax \equiv c \pmod m$ has no sol

  2) $g \mid c \Rightarrow ax \equiv c \pmod m$ has g incongruent sol.

  ↳ How to find sol?

  ① 找一个解. (u_0, v_0) 满足 $au + mv = g$

  ② $x_0 = \frac{cu_0}{g}$ $\quad x \equiv x_0 + k\frac{m}{g} \pmod m$ $\quad k \in \{0, 1, \cdots, g-1\}$

ep. 解 $943x \equiv 381 \pmod{2576}$

$\gcd(943, 2576) = 23$ $\quad 23 \nmid 381$. → No Sol

ep. 解 $893 \equiv 266 \pmod{2432}$

$\gcd(893, 2432) = 19$ $\quad 19 \mid 266$. → $893u - 2432v = 19$. 19 个 Sol

① 找解. $(u, v) = (79, 29)$. $\quad 266 \div 19 = 14$.

② $(x, y) = (1106, 406)$ $\quad 893x - 2432y = 266$.

$893x \equiv 266 \pmod{2432}$

$x_0 = 1106$. $\quad x = 1106 + \frac{2432}{19}k$ $\quad k \in \{0, 1, \cdots, 18\}$

* $\gcd(a, m) = 1$. $ax \equiv c \pmod m$. 有一个解. $\therefore x \equiv \frac{c}{a} \pmod m$

- Polynomial Roots mod p theorem

$f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d$. $d \geq 1$. $p \in$ prime. $p \nmid a_0$.

$\Rightarrow$ $f(x) \equiv 0 \pmod{p}$ has at most d sols.

9. Fermat's little theorem

- Fermat's little theorem. (FLT)

$$p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

- Lemma

$$p \nmid a \Rightarrow \{a, 2a, \cdots, (p-1)a\} \pmod{p}$$
$$\equiv \{1, 2, \cdots, (p-1)\} \pmod{p}$$ 數字相同 (order 可能不同)

proof: $A = \{a, 2a, 3a, \cdots, (p-1)a\}$ $ja \in A$ $ka \in A$

Let all elements in A is divisible by p. $ja \equiv ka \pmod{p}$

$\Rightarrow p \mid (j-k)a$ $\because p \nmid a$ $\therefore p \mid (j-k)$

$\Rightarrow \because 1 \le j, k \le p-1$ $\therefore |j-k| < p-1$

$\because (p-1)$ 以下能被 p 整除的只有 0 $\therefore |j-k| > 0$.

$\Rightarrow \because a, 2a, \cdots, (p-1)a \pmod{p} = 1, 2, \cdots, (p-1) \pmod{p}$

$\therefore a(2a)\cdots((p-1)a) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

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

10. Euler's Formula

- $\phi(m)$: 不超过 m 且与 m 互质的数字总量　　$\#\{a : 1 \le a \le m \wedge \gcd(a,m)=1\}$

- Euler's Formula

$$\gcd(a,m)=1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod m$$

ex.

m	1	2	3	4	5	6	7	8	9	10
$\phi(m)$	1	1	2	2	4	2	6	4	6	4

$1, 3, 7, 9 \pmod{10}$

$7 \cdot 1 \equiv 7 \pmod{10}$　　$7 \cdot 3 \equiv 1 \pmod{10}$

$7 \cdot 7 \equiv 9 \pmod{10} \to 7 \cdot 9 \equiv 3 \pmod{10}$

$(7\cdot1)(7\cdot3)(7\cdot7)(7\cdot9) \equiv 1\cdot3\cdot7\cdot9 \pmod{10}$

$7^4(1\cdot3\cdot7\cdot9) \equiv 1\cdot3\cdot7\cdot9 \pmod{10}$

$7^4 \equiv 1 \pmod{10}$

- Lemma

$$\gcd(a,m)=1 \Rightarrow \{b_1 a, b_2 a, \cdots, b_{\phi(m)} a\} \pmod m$$
$$\text{與 } \{b_1, b_2, \cdots, b_{\phi(m)}\} \pmod m \text{ 數字相同 (order不同)}$$

proof: ∵ b 與 m 互質　∴ ab 與 m 互質

∴ $\{b_1 a, b_2 a, b_3 a, \cdots, b_{\phi(m)} a \pmod m\}$ 與 $\{b_1, b_2, b_3, \cdots, b_{\phi(m)} \pmod m\}$ 全等

↳ 兩個 list 中永遠存在 $b_j a \equiv b_k a \pmod m$

$\Rightarrow m \mid (b_j - b_k)a$.

∵ m & a are 互質　∴ $m \mid b_j - b_k$.

∵ $1 \le b_j, b_k \le m$.　∴ $|b_j - b_k| \le m-1$

only 1 num with absolute value strictly less than m which divisible by m → 0

∴ $b_j = b_k$.　⇒ 兩個 list 裡的數一定一一對應

11. ϕ-function & CRT.

- Phi function formulas

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

b) $\gcd(m,n) = 1 \Rightarrow \phi(mn) = \phi(m)\phi(n)$ → 可得出 ϕ. 然后用 Euler's

ex. $\phi(2401) = \phi(7^4) = 7^4 - 7^3 = 2058$

$\gcd(14,15) = 1 \Rightarrow \phi(14 \cdot 15) = \phi(14)\phi(15) = 6 \times 8 = 48$

$\phi(14)$ ↓ 1, 3, 5, 9, 11, 13

- Chinese Remainder theorem

$\gcd(m,n) = 1 \Rightarrow \begin{cases} x \equiv b \pmod m \\ x \equiv c \pmod n \end{cases}$ 只有一个解. $0 \leq x < mn$

ex. $\gcd(11,19) = 1 \Rightarrow$ 解 $\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 3 \pmod{19} \end{cases}$

let $x = 11y + 8$.

$11y + 8 \equiv 3 \pmod{19} \Rightarrow 11y \equiv 14 \pmod{19}$

$y_1 \equiv 3 \pmod{19}$ $\quad x_1 = 11y_1 + 8 = 11 \cdot 3 + 8 = 41$

proof: → 首先解 $x \equiv 3 \pmod{19}$. solution 带回时满足 $x = my + b$.

$my \equiv c - b \pmod n$

→ ∵ $\gcd(m,n) = 1$

∴ 只有一个 y_1 满足 $0 \leq y_1 < n$ (by LCT)

↓

$x_1 = my_1 + b$. $\quad (0 \leq x_1 < mn)$ $\quad (0 \leq y < n)$

16. Successive Squaring

- Successive squaring 用于计算 $a^k \pmod m$

1. 将 k 写作 power of 2 in 形式 $k = u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r,$

2. 用 successive squaring 做出一个 power of modular 表格

$$\begin{aligned}
a^1 &\equiv A_0 \pmod m \\
a^2 \equiv (a^1)^2 &\equiv A_0^2 \equiv A_1 \pmod m \\
a^4 \equiv (a^2)^2 &\equiv A_1^2 \equiv A_2 \pmod m \\
a^8 \equiv (a^4)^2 &\equiv A_2^2 \equiv A_3 \pmod m \\
&\vdots \qquad\qquad \vdots \\
a^{2^r} \equiv \left(a^{2^{r-1}}\right)^2 &\equiv A_{r-1}^2 \equiv A_r \pmod m
\end{aligned}$$

3. $a^k \pmod m = A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \cdots A_r^{u_r} \pmod m$

ep. compute $9^{53} \pmod{67}$

$53 = 2^5 + 2^4 + 2^2 + 2^0$

1. $9^{53} = 9^{32} \cdot 9^{16} \cdot 9^4 \cdot 9^1$

2. $9^1 \equiv 9 \pmod{67}$
$9^4 \equiv (9^2)^2 \equiv 18^2 \equiv 56 \pmod{67}$
$9^{16} \equiv (9^4)^4 \equiv 56^4 \equiv 35 \pmod{67}$
$9^{32} \equiv (9^{16})^2 \equiv 35^2 \equiv 19 \pmod{67}$

3. $9^{53} \pmod{67} \equiv 9^{32} \cdot 9^{16} \cdot 9^4 \cdot 9^1 \pmod{67}$
$\equiv 9 \cdot 56 \cdot 35 \cdot 19 \pmod{67}$
$\equiv 26 \pmod{67}$

17. Compute kth root (mod m)

- 计算 kth roots mod m:

已知 $\gcd(b,m)=1$ $\gcd(k,\phi(m))=1$ 求 x. s.t $x^k \equiv b \pmod m$ (x 一定是 unique sol)

1. 求 $\phi(m)$
2. 找 u, v s.t $ku-\phi(m)v=1$ / $ku \equiv 1 \pmod{\phi(m)}$
3. $x \equiv b^u \pmod m$ (用 successive squaring 计算)

proof: $x^k = (b^u)^k = b^{uk} = b^{1+\phi(m)v}$ ($ku-\phi(m)v=1$)

$= b(b^{\phi(m)})^v \equiv b \pmod m$ (Euler's formula)

ep. Solve $x^{131} \equiv 758 \pmod{1073}$

1. $\phi(1073) = \phi(29)\phi(37) = 28 \cdot 36 = 1008$.
2. $ku-\phi(m)v=1 \rightarrow 131u-1008v=1$.

∵ $\gcd(k,\phi(m))=1$ ∴ 一定有解

$u=731$. $v=95$.

3. $x = 758^{731} \pmod{1073}$ 算出 x 即可

ep. Solve $x^4 \equiv 7 \pmod{15}$

1. $\phi(15)=8$ $\gcd(k,\phi(m)) = \gcd(4,8) = 4$
2. 若 x_0 is a sol. x must be coprime 3 & 5

↳ By FLT. $x_0^4 \equiv 1 \pmod 3$ $x_0^4 \equiv 1 \pmod 5$

By CRT $x_0^4 \equiv 1 \pmod{15}$

∵ $1 \not\equiv 7 \pmod{15}$ ∴ no solution

※ $x^k \equiv b \pmod m$ 可能超过 k 个 solution / less than k solution in congment class

※ 若 $\gcd(b,m) \neq 1$. $x^k \equiv b \pmod m$ 可能有 u 个 sol ep. $k=3$. $b=2$. $m=4$

20. Squares mod p.

引出: $p=2$ Solve a equation (mod 2) is easy

$p>2$ (p is odd). $\phi(p)=p-1$ is even.

Consider congruence equation $x^k \equiv b \pmod m$.

- $\gcd(b,m)=1$. $\gcd(k, \phi(m))=1$. 则 得出解
- $\gcd(k, \phi(m)) \neq 1$

Consider $m=p$. (prime) $k=2$.

$\Rightarrow \gcd(2, p-1) = 2 \neq 1$

∴ 我们要解 $x^2 \equiv a \pmod p$.

describe this pattern as formula

$(p-b)^2 = p^2 - 2pb + b^2 \equiv b^2 \pmod p$

$$(p-b)^2 \equiv b^2 \pmod p$$

→ 除0外所有数出现2遍

找QR.

$(p-b)^2$	b	b^2
	0	0
12	1	1
11	2	4
10	3	9
9	4	3
8	5	12
7	6	10
6	7	10
5	8	12
4	9	$3 = 4^2 \pmod{13}$
3	10	$9 = 3^2$
2	11	4
1	12	1

Modulo 13

- def. quadratic residue mod p. (QR)

A nonzero num(n) congruent to a square mod p. 存在 $x^2 \equiv n \pmod p$

n与p互质

def. nonresidue mod p. (NR).

A number not congruent to a square mod p.

$(13-9)^2 \equiv 9^2 \pmod{13}$

ep. 跟据表格: QRs mod 13 $\{1, 3, 4, 9, 10, 12\}$

NRs mod 13 $\{2, 5, 6, 7, 8, 11\}$

- Theorem.

Let p be an odd prime. Then there are:
exactly $\frac{p-1}{2}$ quadratic residues mod p, $\frac{p-1}{2}$ nonresidues mod p

Claim: For $1 \le i \le j \le \frac{p-1}{2}$, $i^2 \equiv j^2 \pmod p \Rightarrow i = j$

proof: The quadratic residues are the nonzero numbers that are squares mod p: $1^2, 2^2, \cdots, (p-1)^2 \pmod p$

根据此式, we only need to go halfway:

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

$\left(\frac{p+1}{2}\right)^2, \cdots, (p-2)^2, (p-1)^2 \pmod p$ (repeat in reverse order)

→ check $1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ are all different numbers mod p.

Suppose b_1 & b_2 be number 1 & $\frac{p-1}{2}$. $b_1^2 \equiv b_2^2 \pmod p$

Show $b_1 = b_2$

$\because b_1^2 \equiv b_2^2 \pmod p$

$\therefore p \mid b_1^2 - b_2^2$ $\quad p \mid (b_1 - b_2)(b_1 + b_2)$

$\because b_1 + b_2$ is between 2 & $p-1$. $\therefore p \nmid b_1 + b_2$. $\therefore p \mid b_1 - b_2$.

$|b_1 - b_2| < \frac{p-1}{2}$. $\therefore$ 只有 $b_1 = b_2$ 时才能被 p 整除

$\therefore 1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2$ are different numbers mod p.

$\therefore$ There are exactly $\frac{p-1}{2}$ quadratic residues mod p.

- Quadratic Residue Multiplication Rule I

1) $QR \times QR = QR$

2) $QR \times NR = NR$

3) $NR \times NR = QR$

$QR \times NR \equiv ??$ (mod p)	
$2 \times 5 \equiv 3 \pmod 7$	NR
$5 \times 6 \equiv 8 \pmod{11}$	NR
$4 \times 5 \equiv 7 \pmod{13}$	NR
$10 \times 7 \equiv 5 \pmod{13}$	NR

$NR \times NR \equiv ??$ (mod p)	
$3 \times 5 \equiv 1 \pmod 7$	QR
$6 \times 7 \equiv 9 \pmod{11}$	QR
$5 \times 11 \equiv 3 \pmod{13}$	QR
$7 \times 11 \equiv 12 \pmod{13}$	QR

proof. 1) $\because a_1, a_2 \in QR$.

$\therefore \exists\, b_1, b_2 \in \mathbb{Z}$. s.t $a_1 \equiv b_1^2$, $a_2 \equiv b_2^2 \pmod p$

$a_1 a_2 \equiv b_1^2 b_2^2 \equiv (b_1 b_2)^2 \pmod p$

Thus $a_1 a_2$ is a QR.

2). Let a_1 is a QR. $a_1 \equiv b_1^2 \pmod p$

a_2 is a NR.

Assume $a_1 a_2$ is a QR.

prove by contradiction:

$\because a_1 a_2$ is QR

$\therefore b_3^2 \equiv a_1 a_2 \equiv b_1^2 a_2 \pmod p$.

$\because \gcd(b_1, p) = 1$ $p \nmid a_1$ $a_1 = b_1^2$

$\therefore \exists\, c_1$ s.t $c_1 b_1 \equiv 1 \pmod p$ (LCT)

$c_1^2 b_3^2 \equiv c_1^2 a_1 a_2 \pmod p$

$\equiv (c_1 b_1)^2 a_2 \pmod p$

$\equiv a_2 \pmod p$

$\Rightarrow a_2 \equiv (c_1 b_3)^2 \pmod p$ is a QR.

contradicts to a_2 is NR.

So $QR \times NR = NR$.

3) Let $S = \{1, 2, \cdots, p-1\}$.

$A = \{a \in S : a \text{ is a } QR\}$ $B = \{a \in S : a \text{ is an } NR\}$

$S = A \cup B \quad |A| = \frac{p-1}{2} \quad |B| = \frac{p-1}{2}$

Claim: Let $a_1 \in \mathbb{Z}$. $p \nmid a_1 \Rightarrow a_1 S \equiv S \pmod p$

i.e. $\{a_1 \cdot 1, a_1 \cdot 2, \cdots, a_1(p-1)\} \equiv \{1, 2, \cdots, p-1\} \pmod p$

proof: It is done from the proof of FLT.

$a_1 \cdot A = \{a_1 a : a \text{ is a QR}\} \quad (a \in B)$

$\equiv B \pmod p \quad (\text{Since } |A| = |B|)$

$a_1 \cdot B \equiv a_1 (S \setminus A)$

$\equiv a_1 S \setminus a_1 A$

$\equiv S \setminus B$

$\equiv A \pmod p$

简单的判断方式: QR: +1 NR: -1. 两者相乘

Legendre symbol of a mod p: $\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is QR mod } p \\ -1 & a \text{ is NR mod } p \end{cases}$

ex. $\left(\frac{3}{13}\right) = 1 \quad \left(\frac{11}{13}\right) = -1 \quad \left(\frac{2}{7}\right) = 1 \quad \left(\frac{3}{7}\right) = -1$

- Quadratic Residue Multiplication Rule II

Let p be an odd prime. Then $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

ex. 75 is a square modulo 97.

$\left(\frac{75}{97}\right) = \left(\frac{3 \cdot 5 \cdot 5}{97}\right) = \left(\frac{3}{97}\right)\left(\frac{5}{97}\right)\left(\frac{5}{97}\right) = \left(\frac{3}{97}\right) = 1$

$\because 10^2 \equiv 3 \pmod{97}$

$\therefore 3$ is a QR.

21. Is -1 / 2 Square Modulo p?

- Euler's Criterion

Let p be an odd prime. $a \in \mathbb{Z}$. $p \nmid a$

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

Q. What is $\left(\frac{-1}{p}\right)$? $x^2 \equiv -1 \pmod{p}$?

$p=3$ $\left(\frac{-1}{3}\right) = -1$

$p=5$ $\left(\frac{-1}{5}\right) = \left(\frac{5-1}{5}\right) = \left(\frac{4}{5}\right) = 1$

p	3	5	7	11	13	17	19
$x^2 \equiv -1 \pmod{p}$	NR	QR 2, 3	NR	NR	QR 5, 8	QR 4, 13	NR

Observation: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$

In general, can we find a formula for $\left(\frac{a}{p}\right)$ in terms of a & p?

Consider $A = a^{\frac{p-1}{2}}$ $p \nmid a$

What is the value of $A \pmod p$?

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

$A^2 \equiv 1 \pmod p$

$A \equiv \pm 1 \pmod p$

$\therefore x^2 \equiv 1 \pmod p$ only has 2 solutions mod p.

proof • Suppose a is a QR. $a \equiv b^2 \pmod p$.

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

Thus, a is a QR implies $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$

Consider the congruence $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ (*)

$\therefore$ every QR is a sol to (*)

(*) has at most $\frac{p-1}{2}$ sols mod p.

On the other hand, there are exactly $\frac{p-1}{2}$ QRs.

Hence, solutions to $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ $\Leftrightarrow$ QRs mod p.

- Suppose a is a NR. FLT tells us. $a^{p-1} \equiv 1 \pmod p$

$a^{p-1} \equiv 0 \pmod p$

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

Since a is an NR. $a^{\frac{p-1}{2}} + 1 \not\equiv 0 \pmod p$

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

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

prove (Using primitive roots):

Let $a \in \mathbb{Z}$. $p \nmid a$.

case 1: a is a QR. $\left(\frac{a}{p}\right) = 1$

We know $I(a)$ is even. i.e $I(a) = 2k$ $k \in \mathbb{Z}$.

$a \equiv g^{I(a)} \equiv g^{2k} \pmod p$ g is a primitive root mod p.

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

(by FLT)

case 2: a is an NR. $\left(\frac{a}{p}\right) = -1$.

We know that $I(a)$ is odd. i.e. $I(a) = 2k+1$ $k \in \mathbb{Z}$

$a \equiv g^{I(a)} \equiv g^{2k+1} \pmod p$

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

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

$g^{p-1} - 1 \equiv 0 \pmod p$

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

$\because g$ is a primitive root.

$\therefore g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$

$g^{\frac{p-1}{2}} - 1 \not\equiv 0 \pmod p \quad \Rightarrow g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod p$

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

- Quadratic Reciprocity I $\pmod 4$

Let p be an odd prime.

- $\begin{cases} p \equiv 1 \pmod 4 & -1 \text{ is a quadratic residue mod } p \\ p \equiv 3 \pmod 4 & -1 \text{ is a nonresidue mod } p. \end{cases}$

- 用 Legendre symbol

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

proof:

By Euler's Criterion. $(-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \pmod p$

Case 1: $p \equiv 1 \pmod 4$

Let $p = 4k+1$

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

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

$\because \left(\frac{-1}{p}\right) = -1$ or 1. $\therefore p = 1$

$p \equiv 1 \pmod 4$

Case 2: $p \equiv 3 \pmod 4$

Let $p = 4k+3$.

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

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

$\therefore \left(\frac{-1}{p}\right) = -1$

- Prime $1 \pmod 4$ Theorem

There are ∞ primes congruent to $1 \bmod 4$.

- Quadratic Reciprocity II. $(\bmod 8)$

Let p be odd prime

Then $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \quad (1,7) \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \quad (3,5) \end{cases}$

proof. Consider $2\cdot 1, 2\cdot 2, \cdots, 2\cdot\frac{p-1}{2}$. or $\{2i : 1 \le i \le \frac{p-1}{2}\}$

We would like to count how many $2i$, $1 \le i \le \frac{p-1}{2}$ greater that $\frac{p}{2}$

Instead, there are $\lfloor \frac{p}{4} \rfloor$ i s.t. $2i < \frac{p}{2}$

Number is : $\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$

→ By Gauss' Criterion, $\left(\frac{2}{p}\right) = (-1)$

case 1 : $p \equiv \pm 1 \pmod 8 \Rightarrow p = 8k \pm 1 \cdot k \in \mathbb{Z}$.

$$\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = \frac{8k\pm1-1}{2} - \lfloor \frac{8k\pm1}{4} \rfloor = \frac{\pm1-1}{2} + 4k + \lfloor 2k \pm \frac{1}{4} \rfloor$$

$$\equiv \begin{cases} \frac{+1-1}{2} + \lfloor 2k + \frac{1}{4} \rfloor \equiv 0 \pmod 2 \\ \frac{-1-1}{2} + \lfloor 2k - \frac{1}{4} \rfloor \equiv 0 \pmod 2 \end{cases}$$

$$\frac{p^2-1}{8} = \frac{(8k\pm1)^2-1}{8} = \frac{(64k^2 \pm 16k)+1-1}{8} = 8k^2 \pm 2k \equiv 0 \pmod 2$$

case 2 : $p \equiv \pm 3 \pmod 8 \Rightarrow p = 8k \pm 3 \quad k \in \mathbb{Z}$

$$\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor = \frac{8k\pm3-1}{2} - \lfloor \frac{(8k\pm3)}{4} \rfloor = \frac{\pm3-1}{2} - \lfloor 2k \pm \frac{3}{4} \rfloor$$

$$\equiv \begin{cases} \frac{+3-1}{2} - k \equiv 1 \pmod 2 \\ \frac{-3-1}{2} - (2k-1) \equiv -2+1 \equiv 1 \pmod 2 \end{cases}$$

$$\frac{p^2-1}{8} = \frac{(8k\pm3)^2-1}{8} = \frac{(64k^2 \pm 48k + 9)-1}{8} = 8k^2 \pm 6k + 1 \equiv 1 \pmod 2$$

∴ 2 is a quadratic residue for any prime p that is congruent to 7 mod 8

22-23. Quadratic Reciprocity & Proof

Chap 11 告訴 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

那如果是 $\left(\frac{p}{q}\right)$ (p, q are distinct primes) 會怎麼呢?

ex. Compute $\left(\frac{90}{101}\right)$

$$\left(\frac{90}{101}\right) = \left(\frac{2\cdot 3^2\cdot 5}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{3}{101}\right)^2\left(\frac{5}{101}\right) \quad \text{(product rules)}$$

$$= (-1)\cdot 1\cdot\left(\frac{5}{101}\right) = -\left(\frac{5}{101}\right)$$

ex. Compute $\left(\frac{5}{p}\right)$

It is much easier to compute $\left(\frac{p}{5}\right)$

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & p \equiv 1, 4 \pmod 5 \\ -1 & p \equiv 2, 3 \pmod 5 \end{cases}$$

p	3	5	7	11	13	17	19	23	29
$\left(\frac{p}{5}\right)$	-1		-1	1	-1	-1	1	-1	1
$\left(\frac{5}{p}\right)$	-1		-1	1	-1	-1	1	-1	1

$\hookrightarrow \left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$

ex. Compute $\left(\frac{7}{p}\right)$

p	3	5	7	11	13	17	19	23	29
$\left(\frac{p}{7}\right)$	-1	-1		1	-1	-1	-1	1	1
$\left(\frac{7}{p}\right)$	1	-1		-1	-1	-1	1	-1	1

$\hookrightarrow \left(\frac{p}{7}\right) \neq \left(\frac{7}{p}\right)$

ex. $p = 7$. $3a \equiv 6 \pmod 7$

$\because -1 \equiv 6 \pmod 7$ $\quad -\frac{p-1}{2} < -1 \leq \frac{p-1}{2}$

$\therefore 3a \equiv -1 \pmod 7$

- Gauss' Criterion

Let p be odd prime. $a \in \mathbb{Z}$. $p \nmid a$.

Take numbers $a, 2a, \cdots, (\frac{p-1}{2})a$ and reduce by mod p. to get numbers between $-\frac{p-1}{2}$ & $\frac{p-1}{2}$

If s = # resulting residues < 0, then $(\frac{a}{p}) = (-1)^s$

$(\frac{a}{p}) = (-1)^{\mu(a,p)}$ $\mu(a,p)$ = # ints of $(a, 2a, \cdots, (\frac{p-1}{2})a)$ that become negative when reduced by mod p.

- Lemma 23.3

Let p be an odd prime and a be an odd int. $p \nmid a$.

Then $(\frac{a}{p}) = (-1)^{\mu(a,p)}$ where $\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor \equiv \mu(a,p) \pmod 2$

proof: Consider the reduced residues of $a, 2a, \cdots, (\frac{p-1}{2})a$.
↳ lying between $-(\frac{p-1}{2}) \sim (\frac{p-1}{2})$

Let $u_1, \cdots, u_s$ be those less than 0.
$v_1, \cdots, v_t$ be those greater than 0.

By Gauss' Criterion. $(\frac{p}{q}) = (-1)^s$

To prove this lemma, we only need to show $s \equiv T(a,p) \pmod 2$

The division algorithm tells us that $1 \le j \le \frac{p-1}{2}$.

$$ja = p\lfloor \frac{ja}{p} \rfloor + r_j \quad (r_j \in \{p+u_\ell, v_m\})$$

Add $\frac{p-1}{2}$ of this sort.

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \cdot \lfloor \frac{ja}{p} \rfloor + \sum_{\ell=1}^{s} (p - u_\ell) + \sum_{m=1}^{t} v_m$$

$$= p\left(\sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor\right) + \sum_{\ell=1}^{s} (p+u_\ell) + \sum_{m=1}^{t} v_m \quad ①$$

$$\sum_{j=1}^{\frac{p-1}{2}} j = -\sum_{\ell=1}^{s} u_\ell + \sum_{m=1}^{t} v_t. \quad ②$$

① - ② $\sum_{j=1}^{\frac{p-1}{2}} j(a-1) = p\,T(a,p) + ps + 2\sum_{\ell=1}^{s} u_\ell$ ③

③ $\times 2$ $0 \equiv T(a,p) + s + 0 \pmod 2$

$\because a-1$ is even. p is odd $\therefore s \equiv T(a,p) \pmod 2$

- Conjecture

If $p \equiv 1 \pmod 4 \vee q \equiv 1 \pmod 4$. Then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

If $p \equiv 3 \pmod 4 \vee q \equiv 3 \pmod 4$. Then $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$

- Law of Quadratic Reciprocity

Let p & q be 2 distinct odd primes. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)$

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

eg. $\left(\frac{90}{101}\right) = -\left(\frac{5}{101}\right) = (-1)\cdot\left(\frac{101}{5}\right) = (+1)\left(\frac{1}{5}\right) = (+1)\cdot 1 = -1$

$\therefore$ 90 is not a QR.

proof: By Lemma, we need to show.

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$$

Consider the lattice point in the box $B = B_{p,q} = [1, \frac{p-1}{2}] \times [1, \frac{q-1}{2}]$

lattice pts in B is $\left(\frac{p-1}{2}\right)\cdot\left(\frac{q-1}{2}\right)$

Consider the line L. $qx = py$.

lattice pt (m,n) in B under L are $\{(m,n): qm > pn,\ (m,n) \in B\}$

For $m=1$. there are $\left\lfloor \frac{q-1}{p} \right\rfloor$ lattice pts in B.

→ For $m=j$. there are $\left\lfloor \frac{q-j}{p} \right\rfloor$ lattice pts in B.

Thus, the total number of lattice pts in B under L is $\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor$

the total number of lattice pts in B above L is $\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor$

lattice pts in B $= \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$

$$= \#\text{ l.p under } L + \#\text{ l.p above } L + \#\text{ l.p on } L.$$

Let (m,n) be on L. $m,n \in \mathbb{Z}$. Then $qm = pn$. ← 矛盾

$\because p$ is prime & $q \neq p$. $\therefore p \mid qm \Rightarrow p \mid m$.

However, $\because 1 \le m \le \frac{p-1}{2}$ $\therefore p \nmid m$ $\therefore$ impossible to have l.p on L

Q. Compute $\left(\frac{713}{1009}\right)$

by def. 1009 must be a prime

$$\left(\frac{713}{1009}\right) = \left(\frac{23}{1009}\right)\left(\frac{31}{1009}\right)$$

$$= \left(\frac{1009}{23}\right)\left(\frac{1009}{31}\right)$$

$$= \left(\frac{20}{23}\right)\left(\frac{17}{31}\right)$$

$$= \left(\frac{2^2}{23}\right)\left(\frac{5}{23}\right)\left(\frac{31}{17}\right) \quad \text{by 2 OR}$$

$$= \left(\frac{23}{5}\right)\left(\frac{14}{17}\right)$$

$$= \left(\frac{5}{3}\right)\left(\frac{2}{17}\right)\left(\frac{7}{17}\right)$$

$$= (-1)(1)\left(\frac{17}{7}\right)$$

$$= (-1)\left(\frac{3}{7}\right)$$

$$= \left(\frac{1}{3}\right)$$

$$= 1$$

- def. Jacob Symbol

Let n be an odd positive int. $n = p_1^{t_1} \cdots p_m^{t_m}$ $a \in \mathbb{Z}$.

$\gcd(a, n) = 1$

The Jacob Symbol $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1} \cdots \left(\frac{a}{p_m}\right)^{t_m}$

where $\left(\frac{a}{p_i}\right)$ are legendre symbols

* If $n = p$ a prime, then $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)$

i.e. the Jacobi Symbol is the same as the Legendre symbol.

☆ - Thm.

Let n be an odd positive int. $a, b \in \mathbb{Z}$. $\gcd(a, n) = \gcd(b, n) = 1$

Then i) $a \equiv b \pmod n \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$

iii) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$

iv) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

v) $\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}$

Q. Compute Jacobi symbol $\left(\frac{37603}{48611}\right)$

$\left(\frac{37603}{48611}\right) = \left(\frac{48611}{37603}\right)\cdot(-1)^{\frac{48611-1}{2}\cdot\frac{37603-1}{2}}$ (v)

$= (-1)\left(\frac{11008}{37603}\right)$ (i)

$= (-1)\left(\frac{2^8}{37603}\right)\left(\frac{43}{37603}\right)$ (ii)

$= (-1)\cdot 1\cdot\left(\frac{37603}{43}\right)(-1)^{\frac{43-1}{2}\cdot\frac{37603-1}{2}}$ (v)

$= (-1)^2\cdot\left(\frac{21}{43}\right)$ (i)

$= \left(\frac{43}{21}\right)^{\frac{43-1}{2}\cdot\frac{21-1}{2}}$ (v)

$= \left(\frac{1}{21}\right)$ (i)

$= \left(\frac{1}{3}\right)\left(\frac{1}{7}\right)$

$= 1$

* If $n=p$, a prime. $a \in \mathbb{Z}$. $\gcd(a,n)=1$

the Legendre symbol $\left(\frac{a}{p}\right)=1 \Leftrightarrow x^2 \equiv a \pmod{p}$ has a sol

However, for general $n \in \mathbb{Z}$. n odd. $\left(\frac{a}{n}\right)=1$ can't imply the congruence eq.

$x^2 = a \pmod{n}$ has a sol in general.

24. Which primes are sum of 2 squares?

Q. Given an equation $f(x)=0$. If $f(x) \equiv 0 \pmod n$ has a solution. Can we find a solution of $f(x)=0$ in $\mathbb{Z}$?

No.

Q. Which prime can be written as a sum of 2 squares?

Let p be a prime.

This question is equivalent to the existence of the solution to $x^2+y^2=p$

p	2	3	5	7	11	13	17	...
Y or N	1^2+1^2	N	1^2+2^2	N	N	2^2+3^2	1^2+4^2	...

- Conj

If p is an odd prime.

p is a sum of 2 squares $\Leftrightarrow$ $p \equiv 1 \pmod 4$

proof:

($\Rightarrow$) Assume p is odd. $\exists x, y \in \mathbb{Z}$ s.t. $x^2+y^2=z^2$ Law of QR

$\because p \nmid x$, $p \nmid y$

$\therefore$ If $x=pm$, $p=x^2+y^2 \geq (pm)^2 = p^2m^2 > pm$ contradiction

Thus $x^2+y^2=p$

$\Rightarrow x^2+y^2 \equiv 0 \pmod p$

$\Rightarrow x^2 \equiv -y^2 \pmod p$

$\Rightarrow (y^{-1})^2 \cdot x^2 \equiv -1 \pmod p$ Since $p \nmid y$, y has an inverse mod p

$\Rightarrow (y^{-1}x)^2 \equiv -1 \pmod p$

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

$\Rightarrow p \equiv 1 \pmod 4$

($\Leftarrow$) Assume $p \equiv 1 \pmod 4$ Method of descent

By congruence equation, $x^2 \equiv -1 \pmod p$ has a sol. $x_0 \in \mathbb{Z}$.

i.e. $x_0^2 \equiv -1 \pmod p$

$\exists\, m \in \mathbb{Z}$, $x^2 = -1 + mp$

$x^2 + 1^2 = mp$ $\square$

Q. Find another pair (a, b) s.t $a^2+b^2 = mp$ with $m < M$. ↓

- Method of descent

$A^2 + B^2 = M \cdot p$

$A \cdot B \cdot M \in \mathbb{N}$

$p - 1 \geq M \geq 2$

$\xrightarrow{\text{descent}}$

$a^2 + b^2 = mp$

$m \cdot a \cdot b \in \mathbb{N}$

$m \in M$.

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

Q. Consider the equality

$A^2 + B^2 = Mp$ where $p = 881$. $A = 387$. $B = 1$. $M = 170$

$387^2 + 1^2 = 170 \cdot 881$. Find $a, b \in \mathbb{N}$. $m < M$. s.t $a^2 + b^2 = mp$

Step 1 → Write $387^2 + 1^2 = 170 \cdot 881$ $\quad 170 < 881$.

Step 2 → Choose num with $387 \equiv 47 \pmod{170}$ $\quad 1 \equiv 1 \pmod{170}$

$-\frac{170}{2} \leq 47$. $\quad 1 \leq \frac{170}{2}$

Note that : $47 \cdot 1 \equiv 387 \cdot 1 \pmod{170}$

$47 \cdot 387 + 1 \cdot 1 \equiv 0 \pmod{170}$

Step 3 → Observe that $47^2 + 1^2 \equiv 387^2 + 1^2 \equiv 0 \pmod{170}$

So we can write $47^2 + 1^2 = 170 \cdot 13$

$387^2 + 1^2 = 170 \cdot 881$

Step 4 → multiply them together and set

$(47^2+1^2)(387^2+1^2) = 170^2 \cdot 13 \cdot 88 \cdot 1$

$(13^2+2^2)(170^2+2^2) = 13^2 \cdot 1 \cdot 881$

Step 5 → Use the identity

$(47 \cdot 387+1 \cdot 1)^2 + (47 \cdot 1 - 387 \cdot 1)^2 = 170^2 \cdot 13 \cdot 881$

$(3 \cdot 107 + 2 \cdot 2)^2 + (3 \cdot 2 - 107 \cdot 2)^2 = 13^2 \cdot 1 \cdot 881$

Step 6 → $\because 47 \cdot 387 + 1 \cdot 1 \equiv 0 \pmod{170}$

$47 \cdot 1 - 387 \cdot 1 \equiv 0 \pmod{170}$

$\because 3 \cdot 107 + 2 \cdot 2 \equiv 0 \pmod{13}$

$2 \cdot 107 - 3 \cdot 2 \equiv 0 \pmod{13}$

We have $\left(\frac{3 \cdot 107 + 2 \cdot 2}{13}\right)^2 + \left(\frac{3 \cdot 2 - 107 \cdot 2}{13}\right)^2 = 1 \cdot 881$

Take $m = 1 < M = 13$.

Proof of descent:

Assume $A^2+B^2 = Mp$. $A, B, M \in \mathbb{N}$. p: odd prime.

$2 \le M \le p-1$

Find $a, b, m \in \mathbb{N}$. $a^2+b^2 = mp$ $m < M$

Step 1: Write $A^2+B^2 = M \cdot p$. with $2 \le M \le p-1$

Step 2: Choose number with $u \equiv A \pmod{M}$
$v \equiv B \pmod{M}$

$-\frac{M}{2} < u, v \le \frac{M}{2}$

Note that $u \cdot B \equiv v \cdot A \pmod{M}$

Step 3: Observe that $u^2+v^2 \equiv A^2+B^2 \equiv 0 \pmod{M}$

So we can write $u^2+v^2 = mM$

$A^2+B^2 = M \cdot p$

Since $-\frac{M}{2} \le u, v \le \frac{M}{2}$ $\quad u^2+v^2 \le \left(\frac{M}{2}\right)^2 + \left(\frac{M}{2}\right)^2 = \frac{M^2}{2}$

Thus, $m = \frac{u^2+v^2}{m} \le \frac{M}{2} < M$

Step 4: multiply together

$$(u^2+v^2)(A^2+B^2) = M \cdot m \cdot p$$

Step 5: Use identity

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

$$(uA+vB)^2 + (vA-uB)^2 = M^2 \cdot m \cdot p$$

Step 6: Dividing M^2 on both sides, and we have

$$\left(\frac{uA+vB}{M}\right)^2 + \left(\frac{vA-uB}{M}\right)^2 = mp$$

□

25. Sum of 2 Squares

? Which numbers are sum of 2 squares?

- 方法：Divide & Conquer.

  $m = 1105$

  0也算是 Square

  → 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 的形式

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

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

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

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

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

  $= 33^2 + 4^2$

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

- Sum of 2 Squares Theorem

  Let $m \in \mathbb{Z}^+$.

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

  m can be written as a sum of 2 squares $\Leftrightarrow$ 每个 $p_i = 2$ 或 $p_i \equiv 1 \pmod 4$

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

- Pythagorean Hypotenuse Proposition.

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

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

proof: ($\Rightarrow$) We know that $a^2+b^2=c^2$

$\because (a,b,c)$ is a PPT

$\therefore \gcd(a,b)=1$. c is odd.

$\therefore$ By our thm, c is a product of odd primes p which $\equiv 1 \pmod 4$

ep. Can 1479 by hypotenuse of a primitive Pythagorean triple?

$1479 = 3 \times 17 \times 29$ No

ep. Can 1105 by hypotenuse of a primitive Pythagorean triple?

$1105 = 5 \times 13 \times 17$ Yes

* Let p be an odd prime. g be a primitive root mod p.

Let a be an Int. p$\nmid$a. I(a): the index of a mod p with base g.

Consider the congruence e.g. $x^2 \equiv a \pmod p$

case 1: $x \equiv 0 \pmod p$

$\because p \nmid a$ $\therefore$ impossible

case 2: $x \not\equiv 0 \pmod p$

$I(x^2) = I(a) \pmod{p-1}$

$2I(x) = I(a) \pmod{p-1}$

$\gcd(2, p-1) = 2$ $2 \mid I(a)$ (by LOT)

I(a) is even $\Leftrightarrow$ a is QR.

ex. $\left(\frac{1}{p}\right)=1$ $\left(\frac{a^2}{p}\right)=1$ $\left(\frac{a}{p}\right)^2=(\pm 1)^2$

27. Euler's - ϕ & Sum of divisors

- Lemma

$F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$ $\quad d_i$ 為 n 的因數

$\gcd(m, n) = 1 \Rightarrow F(mn) = F(m) F(n)$

proof: n 的 divisor : $d_1, d_2, \cdots, d_r$

m 的 divisor : $e_1, e_2, \cdots, e_s$

$\because \gcd(m, n) = 1$

$\therefore mn$ 的 divisor : $d_j e_k$ $\forall j \in r$ $k \in s$

$$F(mn) = \sum \phi(d_j e_k)$$
$$= \sum \phi(d_j)\phi(e_k)$$
$$= (\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)) \cdot (\phi(e_1) + \cdots + \phi(e_s))$$
$$= F(m) F(n)$$

- Euler's Phi Function Summation Formula

$\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n$ $\quad (d_i$ 為 n 的因數)

proof: Let $\phi(d_1) + \phi(d_2) + \cdots + \phi(d_r) = n$

$F(n) = \phi(d_1) + \phi(d_2) + \cdots + \phi(d_r)$

$F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t})$

$= F(p_1^{k_1}) F(p_2^{k_2}) \cdots F(p_t^{k_t})$

$= p_1^{k_1} \cdots p_t^{k_t}$ $\quad (F(p^k) = p^k, \forall k \in \text{prime})$

$= n$

- Quadratic Reciprocity (Part I)

Let p be an odd prime.

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

proof: Apply Euler's criterion to $a = -1$.

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

Thus $\left(\frac{-1}{p}\right) = 1$

$\Leftrightarrow \frac{p-1}{2}$ is even.

$\Leftrightarrow \frac{p-1}{2} = 2k \quad k \in \mathbb{Z}$

$\Leftrightarrow p = 1 + 4k$

$\Leftrightarrow p \equiv 1 \pmod 4$

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

$\Leftrightarrow \frac{p-1}{2}$ is odd

$\Leftrightarrow \frac{p-1}{2} = 2k+1 \quad k \in \mathbb{Z}$

$\Leftrightarrow p = 3 + 4k$

$\Leftrightarrow p \equiv 3 \pmod 4$

- Thm

Let p be an odd prime.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8 \end{cases}$$

* By Euler's Criterion, we need to compute $a^{\frac{p-1}{2}} \pmod p$

Q. What is $\left(\frac{2}{p}\right)$? ↓ Find $\left(\frac{2}{11}\right)$

By Euler's Theorem, we need to find out $2^{\frac{11-1}{2}} \pmod{11} \equiv (-1) \pmod{11}$

与证明 FLT 的方法相同:

→ Begin with half of the num from 1 to 11

1, 2, 3, 4, 5 (共2)

$$2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 = 2^{\frac{11-1}{2}} \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$$

$$= 2^{\frac{11-1}{2}} \cdot 5!$$

→ take numbers 2, 4, 6, 8, 10. and reduce each of them mod 11. to get a number between -5 & 5.

$2 \cdot 4 \cdot 6 \cdot 8 \cdot 10$

$\equiv 2 \cdot 4 \cdot (-5)(-3)(-1)$

$\equiv 2 \cdot 4 \cdot 5 \cdot 3 \cdot 1 \cdot (-1)^3 \pmod{11}$

$\equiv (-1)^3 \cdot 5! \pmod{11}$.

$\rightarrow 2^{\frac{11-1}{2}} \cdot 5! \equiv (-1)^3 5! \pmod{11}$

$2^{\frac{11-1}{2}} \equiv (-1)^3 \equiv -1 \pmod{11}$

- Gauss' Criterion.

Let p be an odd prime. $a \in \mathbb{Z}$ $p \nmid a$.

Take the numbers $a, 2a, \cdots, a(\frac{p-1}{2})$ and reduce each of them mod p to get a number lying between $-\frac{p-1}{2}$ & $\frac{p-1}{2}$. If s is the number of resulting residues less than 0. Then $(\frac{a}{p}) = (-1)^s$

proof: For $1 \le i \le \frac{p-1}{2}$. Let $i \cdot a \equiv u_i \pmod{p}$

$-\frac{p-1}{2} \le u_i \le \frac{p-1}{2}$

s is the num of elements $(u_1, \cdots u_{\frac{p-1}{2}}$ less than 0

$\rightarrow$ Claim: $\{|u_1||u_2| \cdots |u_{\frac{p-1}{2}}|.\} = \{1, 2, \cdots, \frac{p-1}{2}\}$.

proof of claim: By counting, it is sufficient to show

28. Powers mod p & Primitive Roots.

- exponent at modulo p. ($e_p a$)

$e_p(a) = $ (smallest exponent $e \geq 1$ s.t. $a^e \equiv 1 \pmod p$)

e_p

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

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

$e_7(1) = 1$
$e_7(2) = 3$
$e_7(3) = 6 = 7-1$

$p = 11$
$1^1 \equiv 1 \pmod{11}$
$2^{10} \equiv 1 \pmod{11}$
$3^5 \equiv 1 \pmod{11}$
$4^5 \equiv 1 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$6^{10} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$
$8^{10} \equiv 1 \pmod{11}$
$9^5 \equiv 1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$

$e_p(a)$

$a^x \equiv 1 \pmod p$

- $\psi(d)$

$\psi_p(d) = \#(a : 1 \leq a < p,\ e_p(a) = d)$ 在 table ψ 出現的次數

ep. $\psi_7(1) = 1$ $\quad \psi(1) = 1$
$\psi_7(3) = 2$ $\quad \psi(3) = 2$
$\psi_7(6) = 2$. $\quad \psi(6) = 2$

- def. primitive root mod p.

Let p be a prime. $g \in \mathbb{Z}$ with most exponent. $e_p(g) = p-1$.

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

$5-1=4$
2, 3

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

$7-1=6$
3, 5

$p = 11$
$1^1 \equiv 1 \pmod{11}$
$2^{10} \equiv 1 \pmod{11}$
$3^5 \equiv 1 \pmod{11}$
$4^5 \equiv 1 \pmod{11}$
$5^5 \equiv 1 \pmod{11}$
$6^{10} \equiv 1 \pmod{11}$
$7^{10} \equiv 1 \pmod{11}$
$8^{10} \equiv 1 \pmod{11}$
$9^5 \equiv 1 \pmod{11}$
$10^2 \equiv 1 \pmod{11}$

2 is a primitive root mod 7.

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

$3^7 \equiv 3 \pmod 7$

period = 6.

- Order Divisibility Property

$p \nmid a \wedge a^n \equiv 1 \pmod p \Rightarrow e_p(a) \mid \phi(m)$

* $e_p(a) \mid p-1$
* $e_p(a) \le \phi(p)$
* 不一定对于每个 $d \mid n$ 都存在 $e_m(a)=d$

  若 m 是 prime，则一定存在 $e_p(g)=p-1$

prof: by def. $a^{e_p(a)} \equiv 1 \pmod p$

Let $d=\gcd(n, e_p(a))$ $\rightarrow d = e_p(a)$

By EA. $\exists u, v \in \mathbb{Z}$. s.t $e_p(a)\cdot u - nv = d$

$$\begin{aligned} a^d &= a^{e_p(a)u - nv} \\ &= (a^{e_p(a)})^u \cdot (a^n)^{-v} \\ &\equiv 1^u \cdot 1^{-v} \pmod p \\ &\equiv 1 \pmod p \end{aligned}$$

$d \ge e_p(a)$ (by def $e_p(a)$)

$\therefore e_p(a) = d$

- Primitive Root Theorem

There are $\underbrace{\phi(p-1)}_{\text{period}}$ primitive roots mod p. ($p \in$ prime)

ex. There are $\phi(10)$ primitive roots mod 11.

proof: $\exists \phi(p-1)$ 个 primitive roots mod p.

Let $p-1=nk$.

$$\underbrace{X^{p-1}-1}_{\substack{\text{exactly } p-1=nk \\ \text{roots mod } p}} = \underbrace{(X^n-1)}_{\substack{\text{at most } n \\ \text{roots mod } p}} \times \underbrace{\left((X^n)^{k-1} + (X^n)^{k-2} + \cdots + X^n + 1\right)}_{\text{at most } nk-n \text{ roots mod } p}$$

FLT

Polynomial Roots mod p theorem. (Thm 8.2)

恒等式成立，个 $= n$.

- Artin's Conjecture

There are ∞ ps s.t 2 is a primitive roots mod p.

Here is a list of the order $e_p(2)$ for all primes up to 100, where we write e_p instead of $e_p(2)$ to save space.

$e_3 = 2$	$e_5 = 4$	$e_7 = 3$	$e_{11} = 10$	$e_{13} = 12$	$e_{17} = 8$
$e_{19} = 18$	$e_{23} = 11$	$e_{29} = 28$	$e_{31} = 5$	$e_{37} = 36$	$e_{41} = 20$
$e_{43} = 14$	$e_{47} = 23$	$e_{53} = 52$	$e_{59} = 58$	$e_{61} = 60$	$e_{67} = 66$
$e_{71} = 35$	$e_{73} = 9$	$e_{79} = 39$	$e_{83} = 82$	$e_{89} = 11$	$e_{97} = 48$

Looking at this list, we see that 2 is a primitive root for the primes

$$p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83.$$

- The generalized Artin's Conjecture

$a \in \mathbb{Z}$. not perfect square. $a \neq -1$.

There are ∞ ps s.t a is primitive roots mod p.

29. Primitive Roots & Indices.

- def. index of a mod p

$I(a)$: index of modulo p for the base g.

需要滿足 primitive root of 13

$p = 13$, $g = 2$

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

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

- Index Rules theorem

1. (Product Rule) $I(ab) \equiv I(a) + I(b) \pmod{p-1}$
2. (Power Rule) $I(a^k) \equiv kI(a) \pmod{p-1}$

proof:

by def., we have $a \equiv g^{I(a)}$, $b \equiv g^{I(a)} \pmod{p}$

1) compute $g^{I(a)} \equiv ab \equiv g^{I(a)} \cdot g^{I(b)} \equiv g^{I(a)+I(b)} \pmod{p}$

$g^{I(a)+I(b)+I(c)} \equiv 1 \pmod{p}$

$ep(g) \mid I(a)+I(b)-I(ab)$

$(p-1) \mid I(a)+I(b)-I(ab))$

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

2) Prove by induction

- $k=1$

$\because I(a) \equiv I(a) \pmod{p-1}$

$\therefore k=1$ is true

- Let $I(a^k)$ is true

$I(a^k) = kI(a) \pmod{p-1}$

- Prove $I(a^{k+1})$

$I(a^{k+1}) = I(a^k \cdot a)$

$$\equiv I(a^k) + I(a) \pmod{p-1} \quad (\text{proved in } 1))$$
$$\equiv k\,I(a) + I(a) \pmod{p-1} \quad (\text{I.H})$$
$$\equiv (k+1)\,I(a) \pmod{p-1}$$

$\therefore k+1$ is true QED

ex. Compute $12 \times 11 \pmod{13}$

$I(12\times 11) = I(12) + I(11) \pmod{12} \equiv 6+7 \pmod{12} \equiv 1 \pmod{12}$

$12 \cdot 11 \equiv 2 \pmod{13}$

ex. Compute $11^{100} \pmod{13}$

$I(11^{100})$

$\equiv 100\, I(11) \pmod{12}$ (by index rule)

$\equiv 100 \cdot 7 \equiv 4 \pmod{12}$.

$11^{100} \equiv 2^4 \equiv 3 \pmod{13}$

ex. Solve $11x \equiv 2 \pmod{13}$

$\because \gcd(11, 13) = 0 \quad \therefore 13 \nmid x$

$11x \equiv 2 \pmod{13}$

$I(11x) \equiv I(2) \pmod{12}$

$I(11) + I(x) \equiv I(2) \pmod{12}$

$7 + I(x) \equiv 1 \pmod{12}$ (product rule)

$I(x) \equiv 6 \pmod{12}$ → $I(11) = 7$.

$x \equiv 12 \pmod{13}$ → $I(12) = 6$ (根据表格)

ex. Solve $3x^{30} \equiv 4 \pmod{37}$ ⇒ $p = 37, g = 2$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$I(a)$	36	1	26	2	23	27	32	3	16	24	30	28	11	33	13	4	7	17

a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$I(a)$	35	25	22	31	15	29	10	12	6	34	21	14	9	5	20	8	19	18

$30\,I(x) = 120 \equiv 12 \pmod{36}$

$ax \equiv c \pmod m$

$\gcd(a,m) \mid c$ 有解.

$\gcd(a,m) \nmid c$ 无解

→ $I(3x^{30}) \equiv I(4)$

$I(3) + 30\,I(x) \equiv I(4) \pmod{36}$

$16 + 30\,I(x) \equiv 2 \pmod{36}$

$30\,I(x) \equiv -24 \equiv 12 \pmod{36}$

→ $\gcd(30, 36) = 6$

$30 \cdot 4 \equiv 12 \pmod{36}$

$I(x) =$	4	10	16	22	28	34
$x =$	16	25	9	21	12	28

(+6 between each pair)

ep. Solve $3x^{21} \equiv 11 \pmod{13}$

$p = 13,\ q = 2$

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

a	1	2	3	4	5	6	7	8	9	10	11	12
$I_{13,7}(a) = I(a)$	12	11	8	10	3	7	1	9	4	2	5	6

case 1: $x \equiv 0 \pmod{13}$ is not a solution.

case 2: $I(3x^{21}) \equiv I(11) \pmod{12}$

$I(3) + 21\,I(x) = I(11) \pmod{12}$

$8 + 21\,I(x) \equiv 5 \pmod{12}$

$9\,I(x) \equiv -3 \pmod{12}$

$9\,I(x) \equiv 9 \pmod{12}$

$I(x) \equiv 1, 5, 9 \pmod{12}$

$x \equiv 7, 11, 8 \pmod{13}$

$ax \equiv c \pmod m$
- $\gcd(a,m) \mid c$ ⇒ 有 $\gcd(a,m)$ 个解
- $\gcd(a,m) \nmid c$ ⇒ 无解

30. Fermat's Last theorem.

- Fermat's Last theorem

$x^4 + y^4 = z^2$ $(x, y, z \in \mathbb{Z})$ has no sol

proof: $x^4 + y^4 = z^2$

let $a = x^2$. $b = y^2$. $c = z$.

$a^2 + b^2 = c^2$

$x^2 = a = st$ $\quad y^2 = b = \frac{s^2 - t^2}{2}$ $\quad z = c = \frac{s^2 + t^2}{2}$

$\because$ st is odd and equal to a square

the only squares mods are $0 \wedge 1$.

$\therefore st \equiv 1 \pmod 4 \Rightarrow s \equiv t \pmod 4$

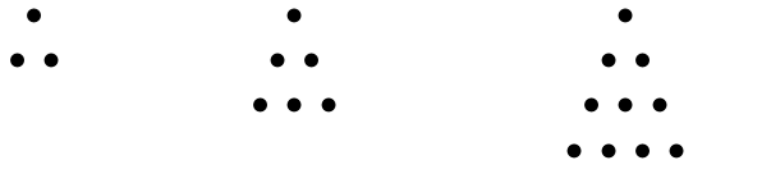
$2y^2 = s^2 - t^2 = (s-t)(s+t)$

$\begin{cases} s+t = 2u^2 \\ s-t = 4v^2. \end{cases}$ $\quad \begin{cases} s = u^2 + 2v^2 \\ t = u^2 - 2v^2 \end{cases}$

$x^2 + 4v^4 = u^4$ $\quad A = x$ $\quad B = 2v^2$ $\quad C = u^2$

同理 $z = u^4 + 4v^4 \Rightarrow u < z$

31. Square-Triangular Numbers



$1+2=3$ $\quad 1+2+3=6$ $\quad 1+2+3+4=10$

Triangular Numbers

$2^2=4$ $\quad 3^2=9$ $\quad 4^2=16$

Square Numbers

Triangular Numbers 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105

Square Numbers 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169

- def. triangular numbers

  mth triangular number : $1+2+\cdots+m=\frac{m(m+1)}{2}$

- def. square-triangular numbers

  A number both square & triangular. $n^2=\frac{m(m+1)}{2}$ (1)

  ep. 1. 36 ...

  (1) 两边同乘 8. $8n^2=4m^2+4m$

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

  Let $y=2n$ $x=2m+1$.

  $2y^2=x^2-1$ $\qquad x^2-2y^2=1$

  If x, y is a sol to (1). $x=2m+1$ odd.

  $2y^2=x^2-1=(2m+1)^2-1=4m^2+4m$

  $y^2=2m^2+2m$ even

  $y=2n$ even

Thus. set $m=\frac{x-1}{2}$ $\quad n=\frac{y}{2}$. we have $n^2=\frac{m(m+1)}{2}$

∴ We can only consider the equation $x^2-2y^2=1$

∵ $n=1$, $n=6$ are sol of $n^2=\frac{m(m+1)}{2}$

$\begin{cases}x=3\\y=2\end{cases}$ $\begin{cases}x=17\\y=12\end{cases}$ are sol to $x^2-2y^2=1$

- def. Pell's equation

$d\neq\square$ $\quad x^2-dy^2=1$

例子 Square-triangular.

$N=1,\quad 36,\quad ?$

$\downarrow\qquad\downarrow$

$n=1\qquad n=6$

$m=1\qquad m=8$

$\updownarrow\qquad\updownarrow$

$x=3\qquad x=17$

$y=2\qquad y=12$

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

Then $1=(3+2\sqrt{2})(3-2\sqrt{2})\cdots$ ①

Taking square on (1), we get:

$1^2=(3+2\sqrt{2})^2(3-2\sqrt{2})^2$ $\quad(1=17^2-2\cdot 12^2)$

$=\left((3^2+2\cdot 3\cdot 2\sqrt{2})+(2\sqrt{2})^2\right)\left((3^2-2\cdot 3\cdot 2\sqrt{2})+(2\sqrt{2})^2\right)$ $\quad(x=17,\ y=12$ is a sol)

$=(17+12\sqrt{2})(17-12\sqrt{2})$

$=(3^3+3\cdot 3^2\cdot(2\sqrt{2})+3\cdot 3\cdot(2\sqrt{2})^2+(2\sqrt{2})^3)(3^3-3\cdot 3^2\cdot(2\sqrt{2})+3\cdot 3\cdot(2\sqrt{2})^2-(2\sqrt{2})^3)$

$=(99+70\sqrt{2})(99-70\sqrt{2})$

$x=99$ $\quad y=70$

x	y	m	n	$n^2=\frac{m(m+1)}{2}$
3	2	1	1	1
17	12	8	6	36
99	70	49	35	1225
577	408	288	204	41616
3363	2378	1681	1189	1413721
19601	13860	9800	6930	48024900
114243	80782	57121	40391	1631432881
665857	470832	332928	235416	55420693056

- Square - Triangular Number Theorem.

a) Every solution in positive integer to the equation $x^2 - 2y^2 = 1$ is obtained by raising $3+2\sqrt{2}$ to powers.

That is, the solution (x_k, y_k) can all be found by multiplying out

$$x_k + y_k\sqrt{2} = (3+2\sqrt{2})^k \qquad k = 1, 2, 3 \cdots$$

b) Every square-triangular number $n^2 = \frac{1}{2}m(m+1)$ is given by

$$m = \frac{x_k - 1}{2} \qquad n = \frac{y_k}{2} \qquad k = 1, 2, 3 \cdots$$

where $(x_k, y_k)'$ are the solutions from (a).

proof:

→ Show $u + v\sqrt{2} = (3+2\sqrt{2})^k$ by method of descent.

If $u = 3$, then $v = 2$.

If $u > 3$, then $\exists (s, t)$ s.t $u + v\sqrt{2} = (3+2\sqrt{2})(s+t\sqrt{2})$ $(s < t)$

- $s + t\sqrt{2} = (3+2\sqrt{2})(q + r\sqrt{2})$

$$u + v\sqrt{2} = (3+2\sqrt{2})^2(q + r\sqrt{2})$$
$$= (3+2\sqrt{2})(s + \sqrt{2}t)$$
$$= (3s+4t) + \sqrt{2}(2s+3t)$$

$u = 3s + 4t \qquad v = 2s + 3t$

$s = 3u - 4v \qquad t = -2u + 3v$

- $s < u$

$\because u = 3s + 4t$

$\therefore s < u.$

- s, t both positive

$u^2 = 1 + 2v^2 > 2v^2 \qquad u > \sqrt{2}v.$

$s = 3u - 4v > (3\sqrt{2} - 4)v > 0$

s pos / t pos

$u > 3$

$\cdot\ 9u^2 > 9 + 8u^2.$

$u^2 - 1 > \frac{8}{9}u^2$

$2v^2 > \frac{8}{9}u^2$ (Since $u^2 - 2v^2 = 1$)

$v > \frac{2}{3}u.$

32. Pell's Equation

- Pell's Equation Theorem.

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.

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. $x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k$

→ 找到 (x_1, y_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

→ find new sols

$x^2 - Dy^2 = 1$

$1 = x_1^2 - Dy_1^2 = (x_1 + y_1\sqrt{D})(x_1 - y_1\sqrt{D})$

$1 = 1^2 = (x_1 + y_1\sqrt{D})^2 (x_1 - y_1\sqrt{D})^2$

$= ((x_1^2 + y_1^2 D) + 2x_1 y_1\sqrt{D})((x_1^2 + y_1^2 D) - 2x_1 y_1\sqrt{D})$

$= (x_1^2 + y_1^2 D)^2 - (2x_1 y_1)^2 D$

∴ new sol : $(x_1^2 + y_1^2 D,\ 2x_1 y_1)$

ex. $x^2 - 3y^2 = 1$ is Pell's equation.

Consider $1 = x^2 - 3y^2 = (x + \sqrt{3}y)(x - \sqrt{3}y)$ (*)

Taking square on (*):

$1^2 = (x + \sqrt{3}y)^2 (x - \sqrt{3}y)^2$

$= ((x^2 + 3y^2) + 2\sqrt{3}xy)((x^2 + 3y^2) - 2\sqrt{3}xy)$

$= (x^2 + 3y^2)^2 - (2xy)^2 \cdot 3$

$= (x^2 + 3y^2)^2 - 12x^2y^2$

33. Diophantine Approximation

如何找 Pell's equation in 一个解?

$x^2 - Dy^2 = 1$

$(x - y\sqrt{D})(x + y\sqrt{D}) = 1$

$$x - y\sqrt{D} = \frac{1}{x + y\sqrt{D}}$$

For any positive integer y, if we take x to be int closet to $y\sqrt{D}$.

Then $|x - y\sqrt{D}|$ is at most $\frac{1}{2}$.

Table for $D = 13$:

x	y	$\lvert x - y\sqrt{13}\rvert$	$x^2 - 13y^2$	x	y	$\lvert x - y\sqrt{13}\rvert$	$x^2 - 13y^2$
4	1	0.394449	3.000	76	21	0.283423	43.000
7	2	0.211103	−3.000	79	22	0.322128	−51.000
11	3	0.183346	4.000	83	23	0.072321	12.000
14	4	0.422205	−12.000	87	24	0.466769	81.000
18	5	0.027756	−1.000	90	25	0.138782	−25.000
22	6	0.366692	16.000	94	26	0.255667	48.000
25	7	0.238859	−12.000	97	27	0.349884	−68.000
29	8	0.155590	9.000	101	28	0.044564	9.000
32	9	0.449961	−29.000	105	29	0.439013	92.000
36	10	0.055513	−4.000	108	30	0.166538	−36.000
40	11	0.338936	27.000	112	31	0.227910	51.000
43	12	0.266615	−23.000	115	32	0.377641	−87.000
47	13	0.127833	12.000	119	33	0.016808	4.000
50	14	0.477718	−48.000	123	34	0.411257	101.000
54	15	0.083269	−9.000	126	35	0.194295	−49.000
58	16	0.311180	36.000	130	36	0.200154	52.000
61	17	0.294372	−36.000	133	37	0.405397	−108.000
65	18	0.100077	13.000	137	38	0.010948	−3.000
69	19	0.494526	68.000	141	39	0.383500	108.000
72	20	0.111026	−16.000	144	40	0.222051	−64.000

always $< \frac{1}{2}$

- Pigeonhole Pricple

Consider multiples: $0\sqrt{D}, 1\sqrt{D}, \cdots, Y\sqrt{D}$.

Write each multiples as sum of a whole num and a decimal between 0&1:

$0\sqrt{D} = N_0 + F_0$ with $N_0 = 0$ $F_0 = 0$ → Pigeohole 1: $\frac{0}{Y} \le t \le \frac{1}{Y}$

$1\sqrt{D} = N_1 + F_1$ with N_1 int $0 \le F_1 < 1$ → Pigeohole 2: $\frac{1}{Y} \le t \le \frac{2}{Y}$

$\vdots$

$Y\sqrt{D} = N_Y + F_Y$ with N_Y int $0 \le F_Y < 1$ → Pigeohole Y: $\frac{Y-1}{Y} \le t \le \frac{Y}{Y}$

共 Y+1 个 pigeon. 每个都 [0, 1]

→ Let F_m, F_n be 2 pigeons in same pigeonhole $(m < n)$

$\therefore |F_m - F_n| < \frac{1}{Y}$

$\because m\sqrt{D} = N_m + F_m \quad n\sqrt{D} = N_n + F_m$.

$\therefore |(m\sqrt{D} - N_m) - (n\sqrt{D} - N_n)| < \frac{1}{Y}$

$|(N_n - N_m) - (n-m)\sqrt{D}| < \frac{1}{Y}$

$\because N_n - N_m \in \mathbb{Z}^+ \quad n-m \in \mathbb{Z}^+$

$\therefore$ 我们目标是找 $|x - y\sqrt{D}|$ 尽量小

→ estimate $y = n - m$.

$\because n, m$ chosen from $F_0, \cdots, F_Y$

$\therefore 0 < m < n \le Y$.

$\therefore 0 < y \le Y$.

→ x, y 满足 $0 < y \le Y \quad |x - y\sqrt{D}| < \frac{1}{Y}$

随着 Y 逐渐↑, 可不断取 x, y.

Y large enough, $|x - y\sqrt{D}| < \frac{1}{Y}$. is false.

$\therefore \frac{1}{Y} \le \frac{1}{Y}$

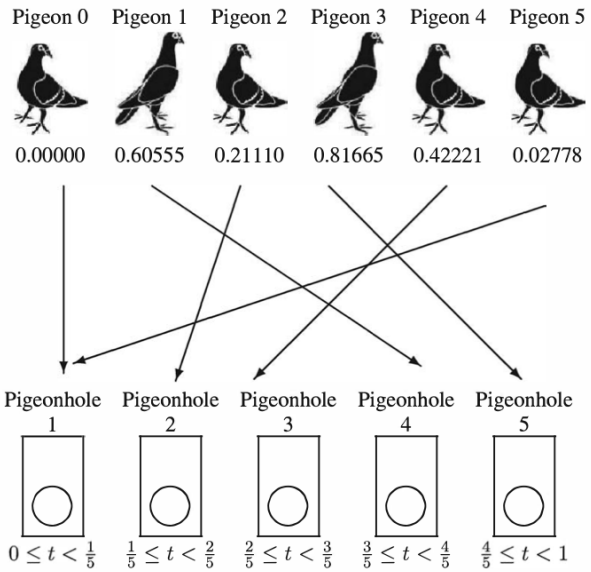


Figure 33.1: Pigeons and Pigeonholes for $D = 13$ and $Y = 5$

part 1 finitely many pigieons

说有finitely many鸽子

但是鸽子窝比鸽子少

那么就有至少一个鸽子窝会有至少两只鸽子

part 2 infinitely many pigeons

有无限只鸽子

和有限的鸽子窝

那么就有至少一个鸽子窝含有infinitely many鸽子

- Dirichlet's Diophantine Approximation Theorem. (Version 1)

Suppose D is a positive int. that is not a perfect square.
Then there are ∞ pairs of positive int (x, y) s.t $|x - y\sqrt{D}| < \frac{1}{y}$

ex. $D = 13$.

$\exists \infty$ pairs of num (x, y) that satisfy $|x - y\sqrt{13}| < \frac{1}{y}$:

$(4,1)$ $(7,2)$ $(11,3)$ $(18,5)$ $(36,10)$ $(119,33)$ $(137,38)$

$(256,71)$ $(393,109)$ ...

- Dirichlet's Diophantine Approximation Theorem. (Version 2)

Suppose $\alpha > 0$ is irrational num. $(\alpha \in \mathbb{R},\ \alpha \neq \frac{a}{b})$
Then $\exists \infty$ (x, y) s.t $|x - y\alpha| < \frac{1}{y}$

ex. $\alpha = \pi$.

x	y	$\lvert x - y\pi \rvert \cdot y$	x/y
3	1	0.141593	3.0000000000
19	6	0.902664	3.1666666667
22	7	0.061960	3.1428571429
333	106	0.935056	3.1415094340
355	113	0.003406	3.1415929204

- Smallest solution algorithm.

1) set $r_0 = \sqrt{D}$. $a_0 = \lfloor r_0 \rfloor$. $E_0 = a_0$

2) check if $(a_0, 1)$ is sol to Pell's equation

3) $\forall n \geq n$. set $r_n = \frac{1}{r_{n-1} - a_{n-1}}$ $a_n = \lfloor r_n \rfloor$

$$E_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$ 写作 $E_n = \frac{x_n}{y_n}$

4) check if (x_n, y_n) is sol to Pell's eq. 若成, 则返回 1)

34. Diophane Approximation & Pell's Equation.

Find the solutions to Pell's equation: $x^2 - Dy^2 = 1$

$\because |x - y\sqrt{D}| = \frac{1}{|x + y\sqrt{D}|} < \frac{1}{y}$

$\therefore (x, y)$ 应满足使 $|x - y\sqrt{D}|$ 尽量小.

eg: $D = 13$

从 Char 33 得 $(x_1, y_1) = (11, 3)$ $(x_2, y_2) = (119, 33)$ are both sols of $x^2 - 13y^2 = 4$.

$$\rightarrow \frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}} = \left(\frac{119 - 33\sqrt{13}}{11 - 3\sqrt{13}}\right)\left(\frac{11 + 3\sqrt{13}}{11 + 3\sqrt{13}}\right)$$

$$= \frac{22 - 6\sqrt{13}}{4}$$

$$= \frac{11}{2} - \frac{3}{2}\sqrt{13}$$

△ △

得 $(\frac{11}{2}, \frac{3}{2})$ is a 非整数解 to Pell's equation $x^2 - 13y^2 = 1$.

→ 当 $(x_2, y_2) = (14159, 3927)$

得 $\frac{14159 - 3927\sqrt{13}}{11 - \sqrt{13}} = 649 - 180\sqrt{13}$.

$\therefore (x, y) = (649, 180)$.

Why $(11, 3)$ & $(14159, 3927)$ 能得到整数解?

$11 \equiv 14159 \pmod 4$ △ $3 \equiv 3927 \pmod 4$ △ ↓

$y_2 \equiv x_2 \pmod{x_1^2 - y_1^2 \cdot D}$

4? $11^2 - 3^2 \cdot 13 = 4$.

$x_1^2 - y_1^2 \cdot D$

– Pell's Equation Thm

Let D be a positive int that is not a perfect square.

$x^2 - Dy^2 = 1$ must have a sol in pos int.

$$x_k + y_k\sqrt{D} = (x_1 + y_1\sqrt{D})^k \qquad k \in 1, 2, 3, \cdots$$

proof:

→ Show Pell's equation has at least 1 sol.

By Dirichlet's Diophantine Approximation Theorem,

$\exists \infty (x, y)$ s.t $|x - y\sqrt{D}| < \frac{1}{y}$

→ Estimate the size of $|x^2 - Dy^2| = |x - y\sqrt{D}|\,|x + y\sqrt{D}|$

$\because |x - y\sqrt{D}| < \frac{1}{y}$

$\therefore x$ is bounded by $x < y\sqrt{D} + \frac{1}{y}$

$\therefore x + y\sqrt{D} < (x\sqrt{D} + \frac{1}{y}) + y\sqrt{D} < 2y\sqrt{D} + \frac{1}{y} < 3y\sqrt{D}$

兩邊同乘 $|x - y\sqrt{D}|$

$|x^2 - Dy^2| < |x - y\sqrt{D}| \cdot 3y\sqrt{D} < \frac{1}{y} \cdot 3y\sqrt{D} = 3\sqrt{D}.$

→ "Pell-like" equation : $x^2 - Dy^2 = M$ has ∞ solutions.

(X_1, Y_1) (X_2, Y_2) $\cdots$

找 2 pairs of sol (pigeons) s.t $X_j \equiv X_k \pmod M$ $Y_j \equiv Y_k \pmod M$

pigeonholes are the pairs (A, B) $0 \le A < M$. $0 \le B < M$.

→ M^2 个

$X_i \equiv A \pmod M$ $Y_i \equiv B \pmod M$ $0 \le A, B < M$

35. Gaussian integers

- def. Gaussian integer

$\mathbb{G}$ = the set of Gaussian integers

$= \{a+bi : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$. $\quad i = \sqrt{-1}$

- Fundamental Theorem of Algebra

If $a_0, a_1, \cdots, a_d$ be complex numbers with $a_0 \neq 0$. $d \geq 1$.

Then the equation $a_0x^d + a_1x^{d-1} + a_2x^{d-2} + \cdots + a_{d-1}x + a_d = 0$ has 1 sol.

Recall, $\alpha = a+bi$ $\quad \beta = c+di \neq 0$.

$$\frac{\alpha}{\beta} = \frac{(ac+bd)+(ad+bc)i}{c^2+d^2}$$ we have division in $\mathbb{C}$.

However, if $\alpha, \beta \in \mathbb{G}$. i.e. $a, b, c, d \in \mathbb{Z}$

$$\alpha/\beta = \frac{(ac+bd)+(-ad+bc)}{c^2+d^2}$$

$$= \frac{ac+bd}{c^2+d^2} + \frac{-ad+bc}{c^2+d^2}$$ might not in $\mathbb{G}$.

It happens on $\mathbb{Z}$ as well.

- def. Gaussian integer $\quad a+bi \quad a, b \in \mathbb{Z}$

The Gaussian integer $\beta = c+di$ decides the Gaussian integer $\alpha = a+bi$

if we can find another Gaussian integer $\gamma = e+fi$. s.t $\alpha = \beta \cdot \gamma$.

記作 $\beta \mid \alpha$

Q. Check if $3+4i$ is divisible by $1+2i$

$$\frac{3+4i}{1+2i} = \frac{(3+4i)(1-2i)}{(1-2i)(1+2i)}$$

$$= \frac{(3\cdot 1+8)+(4\cdot 1-3\cdot 2)i}{1^2+2^2}$$

$$= \frac{11}{5} + \left(\frac{-2}{5}\right)i \notin \mathbb{G}$$

Recall the division algorithm for int $\mathbb{Z}$. $a, b \in \mathbb{Z}$ $b \neq 0$.

The exist $q, r \in \mathbb{Z}$. $0 \leq |r| \leq |b|$ s.t $a = bq + r$. $q = \lfloor \frac{a}{b} \rfloor$

$r = 0 \Leftrightarrow b \mid a$ (In DA, q, r are unique)

- Gaussian Integer Division with the remainder.

Let $\alpha, \beta \in \mathbb{G}$. $\beta \neq 0$.

Then $\exists \gamma, \rho \in \mathbb{G}$. $0 \leq |\rho| < |\beta|$. s.t $\alpha = \beta\gamma + \rho$. where $w = a + bi \in \mathbb{C}$.

$|w| = \sqrt{a^2 + b^2}$

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

proof of PA in $\mathbb{G}$.

Consider $w = \frac{\alpha}{\beta} = x + yi$ $x, y \in \mathbb{R}$.

We can find $a, b \in \mathbb{Z}$. s.t $|a - x| \leq \frac{1}{2}$. $|b - y| \leq \frac{1}{2}$

Let $r = a + bi$ $\rho = \alpha - \beta r$.

$$
\begin{aligned}
N\left(\frac{\rho}{\beta}\right) &= \left|\frac{\rho}{\beta}\right|^2 \\
&= \left|\frac{\alpha - \beta r}{\beta}\right|^2 \\
&= |w - r|^2 \\
&= \left(\sqrt{(a-x)^2 + (b-a)^2}\right)^2 \\
&= (a-x)^2 + (b-y)^2 \\
&= \frac{1}{4} + \frac{1}{4} \\
&= \frac{1}{2} < 1
\end{aligned}
$$

By DA in $\mathbb{G}$. we can establish all properties of gcd in $\mathbb{G}$.

In particular. we have a unique factorization thm:

"Every Gaussian int is a product of primes."

- Gaussian Unit Theorem.

The only units in Gaussian integers are $\pm 1, \pm i$.

These are the only Gaussian int. that have Gaussian int multiplicative inverses.

proof.

[Method 1] Let $z = a+bi \in G.$ be a unit

By def., $\exists\, w = c+di \in G$ s.t $z \cdot w = 1.$

All we have are $a, b, c, d \in \mathbb{Z}.$

$$1 = (a+bi)(c+di) = (ac-bd) + (bc+ad)i$$

case 1. $a=0.$ $\Rightarrow bc=0$ $bd=-1.$

$\Rightarrow c=0.$ $b=\pm 1.$ i.e $z=\pm i.$

case 2. $b=0$ $\Rightarrow ad=0$ $ac=1$

$\Rightarrow d=0.$ $a=\pm 1.$ i.e $z=\pm 1$

case 3. $a \cdot b \neq 0.$ $\Rightarrow c = \frac{1+bd}{a}$

$\Rightarrow ad + b \cdot \frac{1+bd}{a} = 0.$

$\Rightarrow a^2 d + b + b^2 d = 0$

$\Rightarrow -b = (a^2+b^2)d$ impossible since $b < a^2+b^2.$

[Method 2] Consider norm of $z.$

$N(z) = a^2+b^2 = |z|^2$

$N(z \cdot w) = |z \cdot w|^2 = (z \cdot \bar{z})(w \cdot \bar{w}) = N(z)\, N(w)$

$\because N(z)\, N(w) \in \mathbb{Z}.$ (non-neg)

$N(z) = N(w) = 1$ i.e. $a^2+b^2 = 1.$

$\therefore a=0$ $b=\pm 1.$ $\Rightarrow z = \pm i$

or $b=0$ $a=\pm 1.$ $\Rightarrow z = \pm 1$

- Normalized.

A complex number $x+iy$ is said to be normalized if $x>0$, $y\geq 0$.
This is the replacement of positivity in integers Real num.

- Gaussian prime

A Gaussian integer α is called a Gaussian prime.
if the only Gaussian integer divide α are the 8 numbers:

$$\pm\alpha,\ \pm i\alpha,\ \pm 1,\ \pm i$$

- We say $\alpha+G$ is a normalized Gaussian prime if $\alpha=a+bi$
  α is a Gaussian prime. $a>0$. $b\geq 0$.
- α is a Gaussian prime if α only has 2 diff normalized divisors in G

- Gaussian prime Thm

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

i) $p+i$

ii) p: $p\equiv 3 \pmod 4$

iii) $u+vi$: $p\equiv 1 \pmod 4$ 将 p 写成 sum of 2 square 的形式

$$\Rightarrow p=u^2+v^2$$

How to identify Gaussian primes?

Q: Factor 6 in Gaussian integers: $6 = 2 \times 3$.

M1: For 2, Let $2 = \alpha \cdot w$ $\alpha = a + bi$ $w = c + di$.

$$2 = (ac - bd) + (ad + bc)i$$

$$\begin{cases} ac - bd = 2. \\ ad + bc = 0 \end{cases}$$

case 1: $a = 0$ or $b = 0$. $\Rightarrow a = \pm 2.\ \pm 2i$ $w = \pm 1, \pm i$

case 2: $a \neq 0$ $b \neq 0$. $|b| \leq |d|$

$\because ac - bd = 2.$

$\therefore c = \frac{2 + bd}{a} \Rightarrow 0 = ad + b\left(\frac{2 + bd}{a}\right)$

$\Rightarrow \frac{a^2 d + 2b + b^2 d}{a} = 0$

$\Rightarrow a^2 d + 2b + b^2 d = 0$

$\Rightarrow -2b = (a^2 + b^2) d$

$\because a \neq 0$ $b \neq 0$. $\therefore |b| < (a^2 + b^2)$ $\therefore 2 \mid (a^2 + b^2)$ $|d| \mid |b|$

$\because$ We assume $|b| \leq |d|$ $\therefore a^2 + b^2 = 2$

$\therefore a = \pm 1$ $b = \pm 1$.

M2: Note that $2 = \alpha \cdot w$.

Taking norm: $N(2) = N(\alpha w) = N(\alpha) N(w)$

$\Rightarrow 4 = N(\alpha) N(w) = 4 \cdot 1 = 2 \cdot 2.$

case 1: $N(\alpha) = 4$ $N(w) = 1$

$\because N(w) = 1$ w is a unit $w = \pm 1, \pm i$

case 2: $N(\alpha) = N(w) = 2.$

i.e. $a^2 + b^2 = c^2 + d^2 = 2.$ $a = 1 \pm i$ $w = 1 \pm i$.

The unique factorization for 6 in Gaussian Int is

$6 = 2 \times 3 = (1+i)(-i)(1+i)3. = (-i)(1+i)^2 3.$

Remark

1) If p is a rational prime (prime in $\mathbb{Z}$)

$p \equiv 3 \pmod 4 \Rightarrow p$ is Gaussian int.

proof. To prove a Gaussian int $\alpha \neq \pm 1, \pm i$ is a Gaussian prime.

We can say that if $\alpha = \beta \cdot \gamma$ $\beta \cdot \gamma \in \mathbb{G}$.

then one of β & γ is a unit.

Assume $p = \beta \cdot \gamma$. $\beta \cdot \gamma \in \mathbb{G}$.

Taking norm. $N(p) = N(\beta \cdot \gamma) = N(\beta) N(\gamma)$ $p^2 = N(\beta) N(\gamma)$.

case 1: $N(\beta)$ or $N(\gamma) = 1$ → In this case, we do not set any factorization.

case 2: $N(\beta) = N(\gamma) = p$

$a^2 + b^2 = c^2 + d^2 = p$ where $\beta = a + bi$ $\gamma = c + di$

However. $\because p \equiv 3 \pmod 4$ $\therefore p$ is not sum of 2 squares.

2) $p = 2 \cdot p = (-1)(1+i)^2 = 2$

3) Let p be odd rational prime with $p \equiv 1 \pmod 4$

$\therefore p$ is sum of 2 squares

Claim: π and $\bar{\pi}$ are different Gaussian primes.

proof: case 1: π & $\bar{\pi}$ are Gaussian primes. $N(\pi) = a^2 + b^2 = p$

Similarly, $N(\bar{\pi}) = a^2 + (-b)^2 = a^2 + b^2 = p$

Let $\pi = \alpha \cdot \beta$. $\alpha\beta \in \mathbb{G}$

$N(\pi) = N(\alpha\beta)$ $p = N(\alpha) N(\beta)$

$\because p$ is a prime. $N(\alpha) \cdot N(\beta) \in \mathbb{N}$.

Thus, π is a Gaussian prime similar for $\bar{\pi}$

case 2: $N(\beta) = N(\gamma) = p$

$a^2 + b^2 = c^2 + d^2 = p$ where $\beta = a + bi$ $\gamma = c + di$

- Gaussian divisibility Lemma.

Let $\alpha = a+bi$ be a Gaussian integer.

a) If $2 \mid N(\alpha)$, then $(1+i) \mid \alpha$.

b) If $\pi = p$ be the prime in Gaussian prime Thm (ii) ↑

Then $p \mid N(\alpha) \Rightarrow \pi \mid \alpha$

c) Let $\pi = a+bi$ $\bar{\pi} = a-bi$ be Gaussian primes in (iii) ↑

If $p = (a^2+b^2) \mid N(\alpha)$, then either $\pi \mid \alpha$ or $\bar{\pi} \mid \alpha$

proof:

a) Suppose $2 \mid N(\alpha) = a^2 + b^2$

Thus a^2+b^2 is even. $a \equiv b \pmod 2$

It implies $2 \mid (a-b)$ $2 \mid (a+b)$

$$\frac{\alpha}{1+i} = \frac{(a+bi)(1-i)}{(1+i)(1-i)} = \frac{(a+bi)-i(a+bi)}{2} = \frac{a+bi}{2} + \left(\frac{b-a}{2}\right) i \in \mathbb{G}.$$

Thus $(1+i) \mid \alpha$.

b) Let $p \equiv 3 \pmod 4$ be an integer (rational) prime.

Suppose $p \mid N(\alpha) \rightarrow p \mid a^2+b^2$

case 1. $p \mid \alpha$ (or b)

$p \mid (a^2+b^2) \Rightarrow p \mid [(-a)\cdot a + (a^2+b^2)] = b^2$

$\because p$ is a prime $p \mid b$

$\therefore \frac{\alpha}{p} = \frac{a+bi}{p} = \frac{a}{p} + \frac{b}{p} i \in \mathbb{G}$. $\therefore \pi = p \mid \alpha$.

case 2: $p \nmid a$ or $p \nmid b$.

$p \mid a^2+b^2 \Rightarrow a^2+b^2 \equiv 0 \pmod p \Rightarrow b^2 \equiv -a^2 \pmod p$

$\Rightarrow (a^{-1}\cdot b)^2 \equiv -1 \pmod p$ $p \nmid a$ $a^{-1}a \equiv 1 \pmod p$

$\Rightarrow \left(\frac{-1}{p}\right) \equiv 1$

$\Rightarrow p \equiv 1 \pmod 4$ contradic

c) Let p be an integer prime. $p \mid N(w)$

case 1: $p = 2$. $\Rightarrow$ $(1+i) \mid w$ (by GPL)

$\Rightarrow$ w is a product of $1+i$ and a unit.

case 2: $p \equiv 3 \pmod 4$ a prime

$p \mid N(w) \Rightarrow p \mid w$ (GPL)

$\Rightarrow$ w is a product of p and a unit

case 3: $p \equiv 1 \pmod 4$ $p = u^2 + v^2$

$p \mid N(w) \Rightarrow \pi \mid w$ or $\bar{\pi} \mid w$ (GPL)

$\Rightarrow$ w is a product of π or $\bar{\pi}$ and a unit

36. Gaussian integers & unique factorization

- Division Algorithm for Gaussian (DA)

Let $\alpha, \beta \in G$. $\beta \neq 0$. Then there are Gaussian integer γ and ρ.

s.t. $\alpha = \beta\gamma + \rho$. $\quad N(\rho) \leq N(\beta)$

e.g. $\alpha = 37 + 25i \quad \beta = 7 + 3i$

Find 2 Gaussian integers γ & ρ s.t.

$\alpha = \beta\gamma + \rho$. $\quad N(\rho) < N(\beta)$

$$\frac{\alpha}{\beta} = \frac{37+25i}{7+3i}$$

$$= \frac{(37\cdot 7 + 25\cdot 3) + (25\cdot 7 - 37\cdot 3)i}{7^2+3^2}$$

$$= 5.75\cdots + 1.101\cdots i$$

Then let $a=6$. $b=1$. $\quad \gamma = a+bi = 6+i$

Then $\rho = \alpha - \beta\gamma = (37+25i) - (7+3i)(6+i)$

$$= 37+25i - [(42-3) + (18+7)i]$$

$$= (37+25i) - (39+25i)$$

$$= -2$$

$N(\rho) = 2\cdot 2 = 4 \qquad N(\beta) = 7^2+3^2 = 58$

- The Unique Factorization Thm in G (UFT)

Let $\alpha \in G$. There exists a unique expression $\alpha = u \cdot \pi_1^{\alpha_1} \cdots \pi_l^{\alpha_l}$

where u is a unit $(\pm 1, \pm i)$

$\pi_1, \cdots, \pi_l$ are distinct normalized Gaussian primes.

$\alpha_1, \cdots, \alpha_l \in \mathbb{N}$

- Common Divisor property

Let α, β be Gaussian integers $\alpha \cdot \beta \neq 0$.

S be the collection of Gaussian integers $A\alpha + B\beta$. $A \cdot B \in G$

$S = \{ A\alpha + B\beta : \alpha, \beta \in G \}$

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

proof: We use DA for G. to divide α by g.

$\alpha = gr + \rho$. $0 \leq N(\rho) < N(g)$ $1, \rho \in G$.

$\rho = \alpha - g \cdot r$

$= \alpha - (a\alpha + b\beta) r$

$= (1 - ar)\alpha + (-br)\beta$

$\because 1 - ar, -b \cdot r \in G$. $\therefore \rho \in S$.

$\because N(\rho) < N(g)$. $\rho \in S$

$\therefore$ By the minimality of g. $\rho = 0$ $g \mid \alpha$

同理 $g \mid \beta$ □

* In ring theorey, an element π is called "irreducible" if:

$\pi = \alpha \cdot \beta$ $\alpha, \beta \in R$. a ring. Then either α or β is a unit.

↳ 相当于 all the divisor of π are units or $\pi \times$ units

- Gaussian Prime Divisibility Property

Let π be a Gaussian prime. α, β be Gaussian int

If $\pi \mid \alpha\beta$. $\alpha, \beta \in \mathbb{G}$. Then $\pi \mid \alpha$ or $\pi \mid \beta$.

proof:

Apply prev property on α & π. $g = a\alpha + b\pi$. $g \mid \alpha$, $g \mid \pi$

π irreducible

case 1: $g = u$, a unit

两边同乘 β.

$u\beta = g\beta = a\alpha\beta + b\beta\pi$.

$\beta = (u^{-1}a)\alpha\beta + u^{-1}(b\beta)\pi$

$\because \pi \mid \alpha\beta$. $\exists \gamma \in \mathbb{G}$ s.t. $\alpha\beta = \gamma \cdot \pi$

$\therefore \beta = (u^{-1}a\gamma + u^{-1}b\beta)\pi \Rightarrow \pi \mid \beta$

case 2: $g = u\pi$, u is a unit

$\because g \mid \alpha$ $\exists \delta \in \mathbb{G}$. $\alpha = g\delta = u\pi\delta = (u\delta)\pi$

$\therefore \pi \mid \alpha$

- Cor

If π is Gaussian prime. $\pi \mid \alpha_1\alpha_2\cdots\alpha_l$. $(\alpha_i \in \mathbb{G}. \ 1 \le i \le l)$

Then $\pi \mid \alpha_i$ $\forall i$

- def. $R(n)$

Let $n \in \mathbb{N}$. $R(n)$ be the number of ways to write n as a sum of 2 squares

Q. How many ways n can be written as a sum of 2 squares?

Use Gaussian int

Assume $n = A^2 + B^2$

$= (A+iB)(A-iB)$

$= N(A+iB)$

n is a sum of 2 squares $\Leftrightarrow$ $n = N(\alpha)$ $\alpha \in G$.

Thus, # of ways that n is a sum of 2 squares $= \#\{\alpha \in G \ N(\alpha) = n\}$

$n = N(\alpha) = (A+iB)(A-iB)$

- Legendre's Sum of 2 squares Thm

Let $n \in \mathbb{N}$. $n = 2^t p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$

where $p_1 \equiv \cdots \equiv p_r \equiv 1 \pmod 4$ $\quad q_1 \equiv \cdots \equiv q_s \equiv 3 \pmod 4$

$$R(n) = \begin{cases} 0 & \text{if } \exists\, 1 \le j \le s,\ f \equiv j \pmod 2 \\ 4(e_1+1)\cdots(e_r+1) & \text{otherwise} \end{cases}$$

$= 4(D_1 - D_3)$

ex. $R(52)$

$52 = 13 \cdot 4$

Thus $R(52) \geq 1$. $(\pm 4, \pm 6)$ $(\pm 6, \pm 4)$

$R(52) = 4 + 4 = 8$

ex. $R(65)$

方法1: $65 = 13 \cdot 5$

$(\pm 1, \pm 8)$ $(\pm 8, \pm 1)$ $(\pm 7, \pm 4)$ $(\pm 4, \pm 7)$

$R(65) = 4 \cdot 4 = 16$

方法2: $65 = 13 \cdot 5$

$= (2+3i)(2-3i)(+2i)(1-2i)$

$= (A+iB)(A-iB)$

$A+iB = (2+3i)(+2i)(\pm 1)(\pm i)$ 4

$= (2+3i)(1-2i)(\pm 1)(\pm i)$ 4

$= (2-3i)(1-2i)(\pm 1)(\pm i)$ 4

$= (2-3i)(+2i)(\pm 1)(\pm i)$ 4

In general. Let $n = (A+iB)(A-iB)$

The choice of $A+iB$ can not be random.

If $\pi = a+bi$ $\bar{\pi} = a-bi$ $\pi^e \mid A+Bi$ $\bar{\pi}^e \mid A-Bi$

Thus, $n = 2^t p_1^{e_1} \cdots p_r^{e_r} \cdot q_1^{t_1} \cdots q_s^{t_s}$ $p \equiv 1 \pmod 4$ $q \equiv 3 \pmod 4$

$= (1+i)^t (1-i)^t (\pi_1^{e_1} \bar{\pi}^{e_1}) \cdots (\pi_1^{e_r} \bar{\pi}^{e_r}) q_1^{t_1} \cdots q_s^{t_s}$

Thus, the number of choices of $A+iB$ is $4(e_1+1)(e_2+1)\cdots(e_r+1)$

41. Cubic Curves & Elliptic Curves 椭圆曲线

- def. ellipse

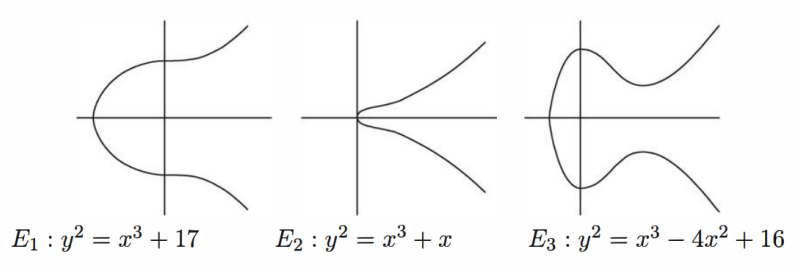
An ellipse curve E is given by the equation of the form. $y^2 = x^3 + ax^2 + bx + c$

3 sample ellipse curves:

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 $(x, y) = (0, 0)$

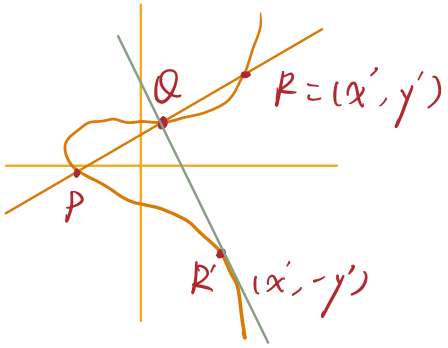
- Siegel's Thm

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

To find the rational point (x, y) on E.

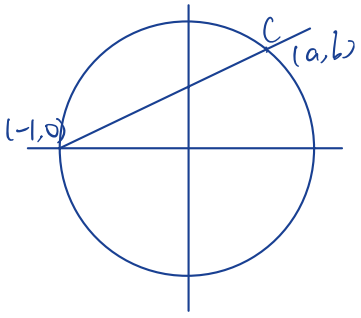
we can use "two" rational solutions P, Q. to produce one rational solution $R = (x', y')$ $\overleftrightarrow{PQ} \cap E = R$.



Q. How to solve quadratic equations (in 2 variables) in rational?

Assume we have a rational solution

ex. Find all rational solutions to $x^2 + y^2 = 1$



slope $\overleftrightarrow{AC}$: $\frac{b}{a+1}$

Conversely, let L be a line through $(-1, 0)$ with a rational slope $m \in \mathbb{Q}$

$L: y = m(x+1)$

$L \cap$ circle $\Rightarrow x^2 + (m(x+1))^2 = 1$

$\Rightarrow x^2 + m^2(x^2+2x+1) = 1$

$\Rightarrow (m^2+1)x^2 + \frac{2m}{m^2+1}x + \frac{m^2-1}{m^2+1} = 0$