

## 1. Primitive Pythagorean Triple

- (a) Definition  
a triple of numbers  $(a,b,c)$  such that  $a,b,c$  have no common factors and  $a^2 + b^2 = c^2$
- (b) PPT can be expressed as  $a = st, b = \frac{s^2-t^2}{2}, c = \frac{s^2+t^2}{2}, s > t \geq 1, \gcd(s,t) = 1, s$  and  $t$  are odd.  
Thm1:  $a$  and  $b$  cannot both be odd

*Proof.* suppose they are all odd

$$a = 2k+1, b = 2p+1, c = 2z$$

$$a^2 + b^2 = 4(k^2 + k + p^2 + p) + 2, c^2 = 4z^2$$

$$a^2 + b^2 \equiv 2 \pmod{4}, 4|c^2, \text{contradicts.}$$

So  $a$  and  $b$  cannot both be odd.  $\square$

Thm2: Suppose  $a \leftarrow \text{odd } b \leftarrow \text{even } c \leftarrow \text{odd}, a^2 = c^2 - b^2, a,b,c$  are coprime. we want to prove  $(c-b)(c+b)$  are coprime.

*Proof.* Then  $a^2 = (c-b)(c+b)$

Suppose they are not coprime (prove by contradict)

Then There exist a prime  $p$  s.t.  $p|c-b$  or  $p|c+b$

$$p|(c+b) + (c-b) \Rightarrow p|2c, p|(c+b) - (c-b) \Rightarrow p|2b$$

Since  $p|(c-b)(c+b) \Rightarrow p|a^2 \Rightarrow p|a \Rightarrow p$  is odd. Then

$p|c$  &  $p|b$ , contradicts with  $c, b$  are coprime.

$$a^2 = (c-b)(c+b) \text{ and } (c-b), (c+b) \text{ are coprime.} \quad \square$$

Thm3:  $x, y$  are coprime,  $a^2 = xy \Rightarrow x, y$  are perfect squares. Can be proved by Fundamental Theorem of Arithmetic.

We express  $c-b = s^2, c+b = t^2$ , then  $a = st, b = \frac{s^2-t^2}{2}, c = \frac{s^2+t^2}{2}$

## 2. Fermat's Last Theorem

If  $n \in \mathbb{N}, n \geq 3, x^n + y^n = z^n$  has no natural number solutions

## 3. Euclidean algorithm

Suppose  $A, B \in \mathbb{N}$  There exist unique  $Q$  and  $R$  such that  $Q \in \mathbb{N}, R \in \mathbb{N}, A = QB + R$ . Then  $\gcd(A, B) = \gcd(B, R)$

Proof of Correctness:

*Proof.* Let  $d = \gcd(A, B), d_0 = \gcd(B, R)$

On one hand

$$\Rightarrow d|A, d|B \Rightarrow d|R$$

$$d|B, d|R \Rightarrow d \leq d_0$$

On the other hand

$$d_0|B, d_0|R \Rightarrow d_0|A \Rightarrow d_0 \leq d$$

In all:  $d = d_0$  i.e.  $\gcd(A, B) = \gcd(B, R)$   $\square$

Thm  $\text{LCM}(a, b)\gcd(a, b) = ab$

*Proof.* let  $d = \gcd(a, b)$

we need to find  $\text{LCM}(a, b)$  by find the smallest  $\text{LCM}(a, b) = ja = kb$ .

$$\text{Then } j\frac{a}{d} = k\frac{b}{d}$$

$$\Rightarrow \frac{a}{d} | \frac{b}{d} k$$

$$\text{since } \gcd(\frac{a}{d}, \frac{b}{d}) = 1$$

$$\Rightarrow \frac{a}{d} | k$$

$$\text{smallest } k = \frac{a}{d}$$

Same process, we get  $j = \frac{b}{d}$

$$\text{Then } \text{LCM} = ja = \frac{ab}{d} \Rightarrow \text{LCM}(a, b) \cdot \gcd(a, b) = ab \quad \square$$

## 4. Linear Equations

we can use Euclidean algorithm to get a Linear Equation:  $ax_0 + by_0 = \gcd(a, b)$ . Thus, we can find a solution to  $ax + by = n$  iff  $\gcd(a, b) | n$

Thm1:  $\gcd(m, n) = 1, m | nc \Rightarrow m | c$

*Proof.*  $\exists x_0, y_0$  s.t.  $mx_0 + ny_0 = 1$

$$\text{Then } mx_0c + ny_0c = c$$

$$m | nc \Rightarrow m | (mx_0c + ny_0c) \Rightarrow m | c \quad \square$$

Thm2: suppose  $p$  is prime,  $p | ab \Rightarrow p | a$  or  $p | b$

*Proof.* if  $p | a$ , this is true. if  $p \nmid a$ , then  $\gcd(p, a) = 1$  since  $p$  is prime.

$$\text{Then } p | ab \Rightarrow p | b \quad \square$$

Thm3: all solutions to  $ax + by = \gcd(a, b)$

we can find  $ax_0 + by_0 = \gcd(a, b)$  by Euclidean algorithm.

Then we have  $ax + by = ax_0 + by_0 = \gcd(a, b)$

$$\text{Then } a(x_0 - x) + b(y_0 - y) = 0 \Rightarrow a(x_0 - x) = b(y - y_0)$$

Divides both sides by  $\gcd(a, b)$

$$\frac{a(x_0 - x)}{\gcd(a, b)} = \frac{b(y - y_0)}{\gcd(a, b)}$$

$$\Rightarrow \frac{a}{\gcd(a, b)} | \frac{b}{\gcd(a, b)} \cdot (y - y_0)$$

$$\text{since } \frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)} \text{ are co-prime} \Rightarrow \frac{a}{\gcd(a, b)} | y - y_0$$

$$y = y_0 + k \frac{a}{\gcd(a, b)}$$

$$\text{similarly, } x = x_0 - k \frac{b}{\gcd(a, b)}, \text{ where } k \text{ are the same.}$$

## 5. Fundamental Theorem of Arithmetic

For all  $n \in \mathbb{N}$  where  $n \geq 2$ ,  $n$  factors as a product of prime numbers, and does so in a unique way.

## 6. Chapter 8 Congruences

Properties:

$$\cdot a \equiv a \pmod{m}$$

$$\cdot a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

$$\cdot a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

$$\cdot \text{if } a \equiv b \pmod{m}, c \equiv d \pmod{m} \Rightarrow$$

$$a + c \equiv b + d \pmod{m}$$

$$a - c \equiv b - d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

*Proof.*  $m | a - b, m | c - d \Rightarrow m | ac - bc, m | bc - bd \Rightarrow$

$$m | ac - bc + bc - bd \Rightarrow m | ac - bd \Rightarrow ac \equiv bd \pmod{m} \quad \square$$

$$\cdot \gcd(m, c) = 1, ca \equiv cb \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

*Proof.*  $m | ca - cb \Rightarrow m | c(a - b)$  since  $\gcd(m, c) = 1$ , they are coprime  $\Rightarrow m | (a - b) \Rightarrow a \equiv b \pmod{m} \quad \square$

## 7. Fermat's Little Theorem

If  $p$  is prime, and  $p \nmid a$  then  $a^{p-1} \equiv 1 \pmod{p}$

## 8. Euler's phi function:

$$\phi : \mathbb{N} \rightarrow \mathbb{N}, \phi = \#\{a | 1 \leq a \leq m, \gcd(a, m) = 1\}$$

Properties:

$$(a) \text{ For prime } p: \phi(p) = p - 1$$

$$(b) \text{ If } \gcd(m, n) = 1, \phi(mn) = \phi(m) \cdot \phi(n)$$

(c) For prime  $p$ :  $\phi(p^k) = p^k - p^{k-1}$

(d) For number  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$   
 $\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k-1})$   
 $= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$

#### 9. Euler's Phi Formula:

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

*Proof.* Suppose  $\gcd(a, m) = 1$ .  $b_n, 1 \leq n \leq \phi(m)$  represents all numbers that are co-prime to  $m$ .

Consider  $A = ab_1, ab_2, ab_3, \dots, ab_{\phi(m)} \pmod{m}$  and  $B = b_1, b_2, b_3, \dots, b_{\phi(m)} \pmod{m}$ . They have the same number of elements. If all elements in  $A$  are congruent to different number mod  $m$ , two set are the same.

We prove by contradiction, suppose  $ab_i \equiv ab_j \pmod{m} \Rightarrow m | a(b_i - b_j) \Rightarrow m | (b_i - b_j) \Rightarrow b_i \equiv b_j$  contradicts!

Then  $b_1 b_2 \dots b_{\phi(m)} \equiv ab_1 ab_2 \dots ab_{\phi(m)} \pmod{m}$

$\Rightarrow \prod_{i=1}^{\phi(m)} b_i \equiv a^{\phi(m)} \prod_{i=1}^{\phi(m)} b_i \pmod{m}$

since  $b_i$ 's are coprime to  $m$ ,  $\prod_{i=1}^{\phi(m)} b_i$  are coprime to  $m$ .  
 $\Rightarrow 1 \equiv a^{\phi(m)} \pmod{m}$   $\square$

(d)  $x \equiv b \pmod{m}, x \equiv c \pmod{m}, \gcd(m, n) = 1$

Use Chinese Remainder Theorem's proof

#### 12. Prime Number Theorem:

$$\lim_{n \rightarrow \infty} \frac{\frac{\pi(n)}{n}}{\ln n} = 1$$

where  $\pi(n) := \#$  of prime numbers  $\leq n$

#### 10. Chinese Remainder Theorem

If  $\gcd(m, n) = 1$ , let  $b, c \in \mathbb{Z}$ . Then there exist a solution to the simultaneous congruence:

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv c \pmod{n} \end{cases} \quad (1)$$

and such a solution is unique modulo  $mn$

*Proof.* Existence:

$m | x - b, n | x - c \Rightarrow m\alpha = x - b, n\beta = x - c$

$\Rightarrow m\alpha - n\beta = c - b$  since  $m, n$  are coprime

$\Rightarrow$  we can find solution  $\alpha_0, \beta_0$  such that  $m\alpha_0 - n\beta_0 = 1$

$\Rightarrow m\alpha_0(c - b) - n\beta_0(c - b) = c - b$

We get  $x = m\alpha_0(c - b) + b$

Uniqueness:

suppose that there are two solution  $x_0, x_1$

$\Rightarrow x_0 \equiv x_1 \equiv b \pmod{m}, x_0 \equiv x_1 \equiv c \pmod{n}$

$\Rightarrow m | (x_1 - x_0), n | (x_1 - x_0) \Rightarrow mn | x_1 - x_0$

$\Rightarrow x_1 \equiv x_0 \pmod{mn}$   $\square$

#### 11. Solving congruences functions

(a)  $x^2 \equiv k^2 \pmod{p}$ ,  $p$  is prime

$p | x^2 - k^2 \Rightarrow p | (x - k)(x + k)$

$\Rightarrow x \equiv k \pmod{p}$  or  $x \equiv -k \pmod{p}$

(b)  $a^k \equiv 1 \pmod{m}, \gcd(m, a) = 1$

Use Euler's Phi Formula to decrease  $k$ .

(c)  $ax \equiv c \pmod{m}, \gcd(a, m) | c$

There is no solution if  $\gcd(a, m) \nmid c$

$m | ax - c \Rightarrow ym = ax - c \Rightarrow c = ax - ym$

Find an  $x_0$  suits the function by Euclidean Algorithm

Then  $ax_0 \equiv c \pmod{m}$ . We want to find all  $x$ .

Then  $ax_0 = ax \pmod{m}$

$m | a(x - x_0) \Rightarrow \frac{m}{\gcd(m, a)} | \frac{a}{\gcd(m, a)} (x - x_0)$

$\gcd(\frac{m}{\gcd(m, a)}, \frac{a}{\gcd(m, a)}) = 1 \Rightarrow \frac{m}{\gcd(m, a)} | x - x_0$

$\Rightarrow x = x_0 + k \frac{m}{\gcd(m, a)}$