

# Dictionary in Number Theory

Xiang Li

## 1 abc Conjecture

**Definition 1.1** (*S-integer*). Let  $R$  be a Dedekind domain,  $K = \text{Frac}(R)$ , and  $S$  be a set of nonzero prime ideals of  $R$ . Then the ring of  $S$ -integers of  $R$  is

$$R_S := R[1/S] := \{x \in K \mid \forall \mathfrak{p} \notin S, v_{\mathfrak{p}}(x) \geq 0\}$$

**Definition 1.2** (*Thrice-punctured Line*). Let  $R$  be a ring. Then  $\mathbb{P}_R^1 \setminus \{0, 1, \infty\}$  is the scheme over  $R$  defined by  $\text{Spec}(R[u^{\pm 1}, v^{\pm 1}]/(1 - u - v))$ .

**Remark 1.3.** We often denote  $\mathbb{P}^1 \setminus \{0, 1, \infty\} := \mathbb{P}_{\mathbb{Z}}^1 \setminus \{0, 1, \infty\}$ . In this remark,  $X := \mathbb{P}^1 \setminus \{0, 1, \infty\}$ . Let  $R$  be a ring. From the definition,  $X(R)$ , the  $R$ -points of  $X$ , is described below:

$$X(R) = \{(u, v) \in (R^{\times})^2 \mid u + v = 1\} \simeq \{u \in R^{\times} \mid 1 - u \in R^{\times}\}.$$

In particular, for a set  $S$  of nonzero prime ideals of  $\mathbb{Z}$  (i.e.,  $S \subseteq \text{Spec}\mathbb{Z} \setminus \{0\}$ ), we have

- $X(\mathbb{Z}_S) = \{(a, b, c) \in \mathbb{Z}^3 \mid a + b = c, \gcd(a, b, c) = 1, \forall \mathfrak{p} \in \text{Spec}\mathbb{Z} \setminus S, \mathfrak{p} \nmid a, b, c\} / \{\pm 1\}$ .
- $X(\mathbb{Z}) = \emptyset$  (the special case of  $S = \emptyset$ ).
- $X(\mathbb{Q}) = \{(a, b, c) \in \mathbb{Z}^3 \mid a + b = c, \gcd(a, b, c) = 1, a, b, c \neq 0\} / \{\pm 1\}$  ( $S = \text{Spec}\mathbb{Z} \setminus \{(0)\}$ ).

**Definition 1.4** (*Height, Conductor*). Let  $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ . With the above remark,

- the height of  $(a, b, c) \in X(\mathbb{Q})$  is  $\text{Ht}((a, b, c)) := \max(|a|, |b|, |c|)$ ;
- the conductor of  $(a, b, c) \in X(\mathbb{Q})$  is  $\text{Cond}((a, b, c)) := \prod_{\text{prime } p \mid abc} p$ .

**Conjecture 1.5** (*abc Conjecture*). Let  $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ . Then  $\forall \varepsilon > 0$ , the set

$$\{x \in X(\mathbb{Q}) \mid \text{Ht}(x) > \text{Cond}(x)^{1+\varepsilon}\}$$

is finite.

**Conjecture 1.6** (*Explicit abc Conjecture*). For  $\varepsilon \geq 1$  in the above statement of abc conjecture, the corresponding set is empty.

**Remark 1.7.** For  $\varepsilon \leq 0$ , it has been proven that the corresponding set is infinite.

**Theorem 1.8** (*Siegel*). Let  $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$  and  $S$  be a finite set of nonzero prime ideals of  $\mathbb{Z}$  (i.e., a finite subset of  $\text{Spec}\mathbb{Z} \setminus \{(0)\}$ ). Then  $X(\mathbb{Z}_S)$  is finite.

*Proof (using abc conjecture).* Let  $C \in \mathbb{N}$  be the product of prime numbers in  $S$  (The finiteness of  $S$  guarantees  $C < \infty$ ). Then for any  $x \in X(\mathbb{Z}_S)$ , we have  $\text{Cond}(x) \leq C$ . Note that

$$X(\mathbb{Z}_S) = \{x \in X(\mathbb{Z}_S) \mid \text{Ht}(x) \leq \text{Cond}(x)^2\} \cup \{x \in X(\mathbb{Z}_S) \mid \text{Ht}(x) > \text{Cond}(x)^2\}$$

where on the right hand side the first set is finite with cardinality  $\leq (2C^2)^3$  and the second set is finite by abc conjecture with  $\varepsilon = 1$ .  $\square$

**Remark 1.9.** Using explicit abc conjecture, the second set on the right hand side is empty.

**Conjecture 1.10** (*Fermat-Catlan*). There are finitely many tuples  $(x^p, y^q, z^r) \in \mathbb{Z}^3$  such that  $x, y, z, p, q, r$  are positive integers,  $x^p + y^q = z^r$ ,  $\gcd(x, y, z) = 1$ , and  $1/p + 1/q + 1/r < 1$ .

*Proof (using abc conjecture).* Let  $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$ . For such tuple  $\alpha := (x^p, y^q, z^r) \in \mathbb{Z}^3$ , we have  $\alpha \in X(\mathbb{Q})$ . Note that

- $1/p + 1/q + 1/r < 1$  implies  $1/p + 1/q + 1/r \leq \frac{41}{42}$ ;
- $\text{Ht}(\alpha) = z^r$ ;
- $\text{Cond}(\alpha) = \text{Cond}(x^p y^q z^r) \leq xyz < z^{r/p} z^{r/q} z = (z^r)^{(1/p+1/q+1/r)} \leq \text{Ht}(\alpha)^{41/42}$ .

In other words,  $\text{Ht}(\alpha) > \text{Cond}(\alpha)^{42/41}$ . So abc conjecture with  $\varepsilon = 1/41$  implies that there are finitely many such  $\alpha = (x^p, y^q, z^r)$ .  $\square$

**Remark 1.11.** In the statement of Fermat-Catalan conjecture, all of  $x, y, z, p, q, r$  can vary. But if we fix  $p, q, r$ , then the statement has been proven to be true unconditionally.

**Corollary 1.12 (Weak Fermat's Last Theorem).** *For sufficiently large positive integer  $n$ , there is no  $(x, y, z) \in \mathbb{Z}^3$  such that  $x, y, z > 0$ ,  $x^n + y^n = z^n$ , and  $\gcd(x, y, z) = 1$ .*

*Proof (using Fermat-Catalan conjecture).* By Fermat-Catalan conjecture, there are finitely many tuples  $(x^p, y^q, z^r) \in \mathbb{Z}^3$  with the conditions in the statement of the conjecture. So  $\max(p, q, r)$  has a maximum for such tuples, call it  $n_0$ . Then for  $n > n_0$ , Fermat's last theorem holds.  $\square$

**Theorem 1.13 (Fermat's Last Theorem).** *For  $n \geq 3$ , there is no  $(x, y, z) \in \mathbb{Z}^3$  such that  $x, y, z > 0$ ,  $x^n + y^n = z^n$ , and  $\gcd(x, y, z) = 1$ .*

*Proof (using explicit abc conjecture).* The case  $n = 4, 5, 6$  has been proven. So assume  $n > 6$ . In the proof of Fermat-Catalan conjecture using abc conjecture, for  $\alpha := (x^p, y^q, z^r)$  we got

$$\text{Cond}(\alpha) < (z^r)^{1/p+1/q+1/r} = \text{Ht}(\alpha)^{1/p+1/q+1/r}.$$

Here we apply  $p = q = r = n$ . Then  $1/p + 1/q + 1/r = 3/n < 1/2$ . So  $\text{Cond}(\alpha) < \text{Ht}(\alpha)^{1/2}$ , i.e.,  $\text{Ht}(\alpha) > \text{Cond}(\alpha)^{1+\varepsilon}$  with  $\varepsilon = 1$ . By explicit abc conjecture, there is no such  $\alpha$ .  $\square$

## 2 Dilogarithm

**Definition 2.1 (Dilogarithm).**

$$\text{Li}_2(x) := \sum_{k=1}^{\infty} \frac{x^k}{k^2}$$

More generally,

$$\text{Li}_n(x) := \sum_{k=1}^{\infty} \frac{x^k}{k^n}$$