2nd sym. Theorems about Number Thoery

Choi Pooreunhaneul

May 31, 2023

1 The Quadratic Reciprocity Law

Definition. Let p be an odd prime and *gcd(a,p)=1*. If the quadratic congruence $x^2 \equiv a\ (mod\ p)$ has a sol, then a is said to be a quadratic residue of p. Otherwise, a is called a quadratic nonresidue of p.

Theorem 1.1 Euler's criterion. Let p be an odd prime and *gcd(a,p)=1*. Then a is a quadratic residue of p iff $a^{(p-1)/2} \equiv 1\ (mod\ p)$.

Corollary. Let p be an odd prime and *gcd(a,p)=1*. Then a is a quadratic residue or nonresidue of p according to whether

$$a^{(p-1)/2} \equiv 1\ (mod\ p) \qquad \text{or} \qquad a^{(p-1)/2} \equiv -1\ (mod\ p) \tag{1}$$

Definition. Let p be an odd prime and let *gcd(a,p)=1*. The Legendre symbol *(a/p)* is defined by

$$1 \text{ if } a \text{ is a quadratic residue of } p \tag{2}$$
$$-1 \text{ if } a \text{ is a quadratic nonresidue of } p \tag{3}$$

Theorem 1.2. Let p be an odd prime and let a and b be int. that are relatively prime to p. Then the Legendre symbol has the following properties:

$$(a) \text{ If } a \equiv b\ (mod\ p), \text{ then } (a/p) = (b/p). \tag{4}$$
$$(b)\ (a^2/p) = 1 \tag{5}$$
$$(c)\ (a/p) = a^{(p-1)/2}\ (mod\ p) \tag{6}$$
$$(d)\ (ab/p) = (a/p)(b/p) \tag{7}$$
$$(e)\ (1/p) \text{ and } (-1/p) = (-1)^{(p-1)/2} \tag{8}$$

Corollary. If p is an odd prime, then

$$(-1/p) = \begin{cases} 1 & \text{if } p \equiv 1\ (mod\ 4) \\ 2 & \text{if } p \equiv 3\ (mod\ 4) \end{cases} \tag{9}$$

Theorem 1.3. If p is an odd prime, then

$$\sum_{a=1}^{p-1} (a/p) = 0 \tag{10}$$

Corollary. The quadratic residues of an odd prime p are congruent modulo p to the even powers of a primitive root r of p; the quadratic nonresidues are congruent to the odd powers of r.

Theorem 1.4 Gauss' lemma. Let p be an odd prime and let gcd(a,p) = 1. If n denotes the number of int. in the set

$$S = \left\{ a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a \right\} \tag{11}$$

whose remainders upon division by p exceed $p/2$, then

$$(a/p) = (-1)^n \tag{12}$$

Theorem 1.5. If p is an odd prime, then

$$(2/p) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \ (mod\ 8) \\ -1 & \text{if } p \equiv \pm 3 \ (mod\ 8) \end{cases} \tag{13}$$

Corollary. If p is an odd prime, then

$$(2/p) = (-1)^{(p^2-1)/8} \tag{14}$$

Theorem 1.6. If p and $2p+1$ are both odd primes, then the int. $2(-1)^{(p^2-1)/8}$ is a primitive root of *2p+1*.

Lemma. If p is an odd prime and a an odd int, with gcd(a,p) = 1, then

$$(a/p) = (-1)^{\sum_{k=1}^{(p-1)/2} [ka/p]} \tag{15}$$

Theorem 1.7 Quadratic Reciprocity Law. If p and q are distinct odd primes, then

$$(p/q)(q/p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{16}$$

Corollary 1. If p and q are distinct odd primes, then

$$(p/q)(q/p) = \begin{cases} 1 & \text{if } p \equiv 1 \ or\ q \equiv 1 \ (mod\ 4) \\ -1 & \text{if } p \equiv q \equiv 3 \ (mod\ 4) \end{cases} \tag{17}$$

Corollary 2. If p and q are distinct odd primes, then

$$(p/q) = \begin{cases} (q/p) & \text{if } p \equiv 1 \ or\ q \equiv 1 \ (mod\ 4) \\ -(q/p) & \text{if } p \equiv q \equiv 3 \ (mod\ 4) \end{cases} \tag{18}$$

Theorem 1.8. If $p \neq 3$ is an odd prime, then

$$(3/q) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \ (mod\ 12) \\ -1 & \text{if } p \equiv \pm 5 \ (mod\ 12) \end{cases} \tag{19}$$

Theorem 1.9. If p is an odd prime and gcd(a,p) = 1, then the congruence

$$x^2 \equiv a \ (mod\ p^n) \quad n \geq 1 \tag{20}$$

has a sol. iff $(a/p) = 1$.

Theorem 1.10. Let a be an odd int. Then we have the following:

$$(a)\ x^2 \equiv a \ (mod\ 2) \text{ always has a sol.} \tag{21}$$

$$(b)\ x^2 \equiv a \ (mod\ 4) \text{ has a sol. iff } a \equiv 1 \ (mod\ 4) \tag{22}$$

$$(c)\ x^2 \equiv a \ (mod\ 2^n), \text{for } n \geq 3, \text{has a sol. iff } a \equiv 1 \ (mod\ 8) \tag{23}$$

Theorem 1.11. Let $n = 2^{k_0} p_1^{k_1} \cdots p_r^{k_r}$ be the prime factorization of $n > 1$ and let $\gcd(a,n) = 1$. Then $x^2 \equiv a \ (mod\ n)$ is solvable iff.

$$(a)\ (a/p_i) = 1 \text{ for } i = 1, 2, \dots, r; \tag{24}$$

$$(b)\ a \equiv 1\ (mod\ 4) \text{ if } 4|n, \text{ but } 8 \nmid n;\ a \equiv 1\ (mod\ 8) \text{ if } 8|n. \tag{25}$$

Definition. Jacobi Symbol. Defined as

$$(a/p) = \begin{cases} 0 & p|a \\ 1 & p \nmid a \quad \text{residue} \\ -1 & p \nmid a \quad \text{nonresidue} \end{cases} \tag{26}$$

Theorem 1.12. For odd positive int. $b,\ b_1,\ b_2$ and $a,\ a_1,\ a_2$,

$$(a)\ (a/1) = 1 \tag{27}$$

$$(b)\ (a_1/b) = (a_2/b)\ if\ a_1 \equiv a_2\ (mod\ b) \tag{28}$$

$$(c)\ (a_1 a_2/b) = (a_1/b)(a_2/b). \tag{29}$$

$$(d)\ (a/b_1 b_2) = (a/b_1)(a/b_2). \tag{30}$$

Lemma. Let int. $r, \quad s$ is odd. Then,

$$(a)\ \frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2}\ (mod\ 2) \tag{31}$$

$$(b)\ \frac{r^2 s^2 - 1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8}\ (mod\ 2) \tag{32}$$

Corollary. Let $r_1, \dots, r_m$ be odd. Then,

$$(a)\ \sum_{i=1}^{m} \frac{r_i - 1}{2} \equiv \frac{r_1 \cdots r_m - 1}{2}\ (mod\ 2) \tag{33}$$

$$(b)\ \sum_{i=1}^{m} \frac{r_i^2 - 1}{8} \equiv \frac{r_1^2 \cdots r_m^2 - 1}{8}\ (mod\ 2) \tag{34}$$

Theorem 1.13. For odd natural num. $a, \quad b$,

$$(a)\ (-1/b) = (-1)^{\frac{b-1}{2}} \tag{35}$$

$$(b)\ (2/b)(-1)^{b^2-1}8 \tag{36}$$

$$(c)\ (a/b)(b/a) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} \tag{37}$$

Theorem 1.14. Let int. a not a perfect square. Then $\exists$ ∞ly many primes p for which a is a quad. res.

Lemma. Let $a, \quad b$ natural odd and $\gcd(a,b) = 1$. Then,

$$(a)\ \epsilon = \pm 1\ \Rightarrow\ (\epsilon a/b)(b/a) = (-1)^{\frac{\epsilon a-1}{2}\frac{b-1}{2}} \tag{38}$$

$$(b)\ \epsilon_1,\ \epsilon_2 = \pm 1\ \Rightarrow\ (\epsilon_1 a/b)(\epsilon_2 b/a) = (-1)^{\frac{\epsilon_1 a-1}{2}\frac{\epsilon_2 b-1}{2} + \frac{\epsilon_1 - 1}{2}\frac{\epsilon_2 - 1}{2}} \tag{39}$$

$$\tag{40}$$

Theorem 1.15 Eisenstein's Method. Let b is natural odd and int. a is odd. Then, following holds.

$$set.\ a_1 = a, a_2 = b,\ a_i = 2n-1,\ \epsilon_i = \pm 1 \tag{41}$$

$$a_n = q_n a_{n+1} + \epsilon_n a_{n+2}\ \ with\ \ a_2 > a_3 > \cdots > a_{n+2} = 1 \tag{42}$$

$$For\ each\ i,\ let.\ s_i = \begin{cases} 0 & \text{if at least one of } a_{i+1} \text{ and } \epsilon_i a_{i+2} \equiv 1\ (mod\ 4) \\ 1 & \text{if both } a_{i+1} \text{ and } \epsilon_i a_{i+2} \equiv 3\ (mod\ 4) \end{cases} \tag{43}$$

$$let.\ t = \sum_{i=1}^{n} s_i.\ \Rightarrow\ (a/b) = (-1)^t. \tag{44}$$

Corollary. Let $t = \sum_{i=1}^{n} s_i$. Then for any $k \geq n$,

$$(a/b) = (-1)^{t_k} \left(\frac{a_{k+1}}{a_{k+2}} \right) \tag{45}$$

Theorem 1.16. The number N of sol. with $1 \leq x, y \leq p$ of $y^2 \equiv ax^2 + bx + c\ (mod\ p)$ is:

$$N = \begin{cases} p - (a/p) & \text{if } p \nmid D \\ p + (p-1)(a/p) & \text{if } p \mid D \end{cases} \tag{46}$$

where $D = b^2 - 4ac$.

2 Number of Special Forms

Definition. If $\sigma(n) = 2n$, n is perfect number.

Theorem 2.1. If $2^k - 1$ is prime, then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.

Lemma. If $a^k - 1$ $(a > 0, k \geq 2)$ is prime, then a=2 and k is also prime.

Theorem 2.2. An even perfect number ends in the digit 6 or 8; equivalently.

Definition. $M_n = 2^n - 1$ is defined as Mersenne prime.

Theorem 2.3. If p and $q = 2p + 1$ are primes, then either $q|M_p$ or $q|M_p + 2$, but not both.

Theorem 2.4. If $q = 2n + 1$ is prime, then we have the following:

$$(a)\ q|M_n,\ \text{provided that } q \equiv 1\ (mod\ 8)\ or\ q \equiv 7\ (mod\ 8) \tag{47}$$

$$(b)\ q|M_n,\ \text{provided that } q \equiv 3\ (mod\ 8)\ or\ q \equiv 5\ (mod\ 8) \tag{48}$$

(49)

Corollary. If p and $q = 2p + 1$ are both odd primes, with $p \equiv 3\ (mod\ 4)$, then $q|M_n$.

Theorem 2.5. If p is an odd prime, then any prime divisor of M_n is of the form $2kp + 1$.

Theorem 2.6. If p is an odd prime, then any prime divisor q of M_n is of the form $q \equiv \pm 1\ (mod\ 8)$

Remark. Define S_k by $S_1 = 4$, $S_{k+1} = S_k^2 - 2$.
Then for prime, M_p is prime $\Longleftrightarrow S_{p-1} \equiv 0\ (mod\ M_p) \Longleftrightarrow S_{p-2} \equiv \pm 2^{\frac{p+1}{2}}\ (mod\ M_p)$.

Theorem 2.7 Euler. If n is an odd perfect num, then

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r} \tag{50}$$

where the p_i's are distinct odd primes and $p_1 \equiv k_1 \equiv 1\ (mod\ 4)$.

Corollary. If n is an odd perfect, then n is of the form

$$n = p^k m^2 \tag{51}$$

where p is a prime, $p \nmid m$, and $p \equiv k \equiv 1\ (mod\ 4)$; in particular, $n \equiv 1\ (mod\ 4)$).

Definition. m, n satisfying $\sigma(m) = \sigma(n) = m + n$ are called amicable numbers.

Fact. $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, and $r = 9 \cdot 2^{2n-1} - 1$ are all primes and $n \geq 2$, then $2^n pq$ and $2^n r$ are amicable numbers.

Definition. $F_n = 2^{2^n} + 1$ is called Fermat number. If it is prime, we more specially call it Fermat prime.

Theorem 2.8. F_5 is divisible by 641.

Theorem 2.9. F_n and F_m, where $m > n$, gcd(F_m, F_n)=1.

Theorem 2.10 Pepin's test. For natural n, F_n is prime iff $3^{\frac{F_n - 1}{2}} \equiv -1\ (mod\ F_n)$.

Theorem 2.11. Any prime divisor p of F_n where $n \geq 2$ is of the form $p = k \cdot 2^{n+2} + 1$.

3 Elliptic Curve

Definition. An elliptic curve $E/Q\ :\ \ y^2 = x^3 + ax + b,\ \ a, b \in \mathbb{Q}$ should has no repeated root(smooth), and together with ∞(projective) where $\Delta = -2^4(4a^3 + 27b^2) \neq 0$.

Definition. For E/Q,

$$E(Q) = \{(x, y) \mid x.y \in \mathbb{Q}\ and\ y^2 = x^3 + ax + b\} \cup \{\infty\} \tag{52}$$

is the set of Q-rational points of E.

Definition. let. $P = (x_1, y_1)$ and $Q = (x_2, y_2)$.

$$(1)\ if\ Q = (x_2, y_2) = (x_1, -y_1),\ \ P + Q = \infty \tag{53}$$

$$(2)\ if\ Q = P,\ \ P + Q = 2P\ as: \tag{54}$$

$$\text{Find the tangent line which pass } P \text{ and find intersection of tangent line and } E. \tag{55}$$

$$\text{Just let } R = (x_3, y_3). \text{ Then } 2P = (x_3, -y_3). \tag{56}$$

$$(3)\ if\ Q \neq P,\ \ \text{Find the segment intersection of it and } E. \tag{57}$$

Theorem 3.1. For $P_1,\ P_2,\ P_3 \in \mathbb{Q}$,

$$(1)\ P_1 + P_2 \in E(Q) \tag{58}$$
$$(2)\ P_1 + P_2 = P_2 + P_1 \tag{59}$$
$$(3)\ P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3. \tag{60}$$

Remark. $(E(Q),\ +)$ forms abelian qroup with identity ∞.

Theorem 3.2 Mordell-Weil. Given E/Q, $\exists\infty$ly many $\mathbb{Q}$ sol. $P_1, \ldots, P_n$ s.t. $\forall P \in E(Q)$ is of the form $P = \sum_{j=1}^{m} n_j p_j$ for int. $n_1, \ldots, n_m$.

Definition. For prime p, $\mathbb{F} = \mathbb{Z} = \{0, \ldots, p-1\}$ is a finite field order p.

Definition. For $p \neq 2, 3$, a prime, $E/\mathbb{F}_p$ is defined by $y^2 = x^3 + ax + b,\ \ a, b \in \mathbb{F}_p$ with $\Delta = -2^4(4a^3 + 27b^2) \not\equiv 0\ (mod\ p)$. Then,

$$E(\mathbb{F}) = \{(x, y) \mid x.y \in \mathbb{F}_p\ and\ y^2 \equiv x^3 + ax + b\ (mod\ p)\} \tag{61}$$

Remark. If we count $\mathbb{Z}$ points fof E, we should consider ∞. For ex, 17 points $\Rightarrow$ total 18 points because of the existence of ∞.

Theorem 3.3 Hasse's bound. $|\#E(\mathbb{F}_p) - p - 1| \leq 2\sqrt{p}$

Remark. Shimura-Taniyama-Weil Theorem and Birdu & Swinnerton-Dyer Conjucture

4 Representation of Integers as Sums of Squares

Lemma. If m and n are each the sum of two squares, then so is their product mn.

Theorem 4.1. No prime p of the form $4k + 3$ is a sum of two squares.

Lemma Thue. Let p be a prime and $\gcd(a, p) = 1$. Then the congruence

$$ax \equiv y\ (mod\ p) \tag{62}$$

admits a sol. x_0, y_0, where

$$0 < |x_0| < \sqrt{p} \qquad and \qquad 0 < |y_0| < \sqrt{p} \tag{63}$$

Theorem 4.2 Fermat. An odd prime p is expressible as a sum of two squares iff $p \equiv 1\ (mod\ 4)$.

Corollary. Any prime p of the form $4k + 1$ can be represented uniquely (aside from the order of the summands) as a sum of two squares.

Theorem 4.3. Let the positive int. n be written as $n = N^2 m$, where m is squarefree. Then n can be represented as the sum of two squares iff m contains no prime factor of the form $4k + 3$.

Corollary. A positive int. n is representable as the sum of two squares iff each of its prime factors of the form $4k + 3$ occurs to an even power.

Theorem 4.4. A positive int. n can be represented as the difference of two squares iff n is not of the form $4k+2$.

Corollary. An odd prime is the difference of two successive squares.

Theorem 4.5. No positive int. of the form $4^n(8m+7)$ can be represented as the sum of three squares. Converse also holds.

Lemma 1 Euler. If the int. m and n are each the sum of the four squares, then mn is likewise so representable.

Lemma 2. If p is an odd prime, then the congruence

$$x^2 + y^2 + 1 \equiv 0 \ (mod\ p) \tag{64}$$

has a sol. x_0, y_0 where $0 \leq x_0 \leq (p-1)/2$ and $0 \leq y_0 \leq (p-1)/2$

Corollary. Given an odd prime p, $\exists$ an int. $k < p$ s.t. kp is the sum of four squares.

Theorem 13.6. Any prime can be written as the sum of four squares.

Theorem 13.7 Lagrange. Any positive int. can be written as the sum of four squares, some of which may be zero.

Remark. Waring's problem & Easier one

5 Fibonacci Numbers

Remark. Fibonacci numbers grow rapidly!

Theorem 5.1. For the Fibonacci sequence, $\gcd(u_n, u_{n+1}) = 1$ for every natural n.

Fact. $3|u_{4n},\ 5|u_{5n},\ 7|u_{8n}$.

Lemma. $u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$.

Theorem 5.2. For natural m and n, u_{mn} is divisible by u_m.

Lemma. If $m = qn + r$, then $\gcd(u_m, u_n) = \gcd(u_r, u_n)$.

Theorem 5.3. The gcd of two Fibo. num. is again a Fibo. num; specifically,

$$gcd(u_m, u_n) = u_d \qquad where\ d = (gcd(m, n) \tag{65}$$

Corollary. In the Fibo. sequence, $u_m | u_n$ iff $m|n$ for $n \geq m \geq 3$.

Corollary. if $n > 4$ is composite, then u_n also.

Remark. If u_n is prime, n is odd prime or 4.

Lemma. $u^2 - u_{n+1}u_{n-1} = (-1)^{n-1}$

Theorem 5.4. Any positive int. N can be expressed as a sum of distinct Fibo. num, no two of which are consecutive; that is,

$$N = u_{k_1} + \cdots + u_{k_r} \tag{66}$$

where $k_1 \geq 2$ and $k_{j+1} \geq k_j + 2$ for $j = 1, \ldots, r-1$.

Lemma 1. $u_3 + u_5 + \cdots + u_{2s-1} = u_{2s} - 1 = u_r - 1.$

Lemma 2. $u_2 + u_4 + \cdots + u_{2s} = u_{2s-1} - 1 = u_r - 1.$

Lemma. $u_n = \dfrac{1}{\sqrt{5}}\left[\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n\right]$

Theorem 5.5. For a prime $p > 5$, either $p|u_{p-1}$ or $p|u_{n+1}$, but not both.

Theorem 5.6. Let $p \geq 7$ be a prime for which $p \equiv 2 \ (mod\ 5)$, or $p \equiv 4 \ (mod\ 5)$. If $2p-1$ is also prime, then $2p-1|u_p$.

6 Continued Fractions

Remark. Representation is not unique.

Theorem 6.1. Any rational nu can be written as a finite simple continued fraction.

Definition. $[a_0; a_1, \ldots, a_n] = [a_0; a_1, \ldots, a_{n-1} + 1]$

Definition. For $[a_0; a_1, \ldots, a_n]$, by cutting off the expansion after the kth partial denomiator a_k is called the kth convergent of the given continued fraction and denoted by C_k; in symbols,

$$C_k = [a_0; a_1, \ldots, a_k] \quad 1 \leq k \leq n \tag{67}$$

We let the zeroth convergent C_0 be equal to the number a_0.

Lemma. $C_{k+1} = [a_0; a_1, \ldots, a_{k+1}] = [a_0; a_1, \ldots, a_k + \frac{1}{a_{k+1}}]$.

Definition.

$$p_0 = a_0 \qquad q_0 = 1 \tag{68}$$

$$p_1 = a_1 a_0 + 1 \qquad q_1 = a_1 \tag{69}$$

$$p_k = a_k p_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2} \tag{70}$$

Theorem 6.2. $C_k = \dfrac{p_k}{q_k} \quad 0 \leq k \leq n.$

Remark. It is convenient to define $p_{-2} = 0, p_{-1} = 1$ and $q_{-2} = 1, q_{-1} = 0$.

Theorem 6.3. If C_k is the kth convergent of the finite simple continued fraction, then

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}. \tag{71}$$

Corollary. For $1 \le k \le n$, p_k and q_k are relatively prime.

Lemma. If q_k is the denominator of the kth convergent C_k of the simple continued fraction, then $q_{k-1} \le q_k$, with strict inequality when $k > 1$.

Theorem 6.4. $\forall$ natural n,

$$C_0 < C_2 < \cdots < C_{2n} < C_{2n+1} < \cdots < C_3 < C_1. \tag{72}$$

Definition. If $a_0, \ldots$ is an infinite sequence of int, all positive except possibly a_0, then the infinite simple contunued fraction $[a_0; a_1, a_2, \ldots]$ has the value

$$\lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n] \tag{73}$$

Remark.

$$\lim_{n\to\infty} \frac{u_{n+1}}{u_n} = \frac{1+\sqrt{5}}{2} \tag{74}$$

Theorem 6.5. The value of any infinite continued fraction is irrational.

Theorem 6.6. Two distinct infinite continued fractions represents two distinct irrational numbers, i.e. representation is unique.

Remark. First let

$$a_k = [x_k] \qquad x_{k+1} = \frac{1}{x_k - a_k}. \tag{75}$$

Then $x_0 = [a_0; a_1, \ldots, a_n, x_{n+1}] = C'_{n+1} = \dfrac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$.

Because of this,

$$x_0 - C_n = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n} \quad \Rightarrow \quad |x_0 - C_n| < \frac{1}{q_k^2}. \tag{76}$$

Theorem 6.7. Every irrational has a unique representation as an infinite continued fraction, which obtained from the continued fraction algorithm described as (75).

Lemma. Let p_n/q_n be the nth convergents of the continued fraction representing the irrational number x. If a and b are int, with $1 \le b < q_{n+1}$, then

$$|q_n x - p_n| \le |bx - a| \tag{77}$$

Theorem 6.8. If $1 \le b \le q_n$, the irrational a/b satisfies

$$\left| x - \frac{p_n}{q_n} \right| \le \left| x - \frac{a}{b} \right| \tag{78}$$

Theorem 6.9. Let x be an arbitrary irrational. If the rational a/b, where $b \geq 1$ and $\gcd(a, b) = 1$, satisfies

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}, \tag{79}$$

then a/b is one of the convergents p_n/q_n in the continued fraction representation of x.

Remark. When deal with Pell's equation, we only consider positive sol.

Theorem 6.10. If $p,\ q$ is a positive sol. of Pell's eq, then p/q is a convergent of the continued fraction expansion of $\sqrt{d}$.

Theorem 6.11. If $p,\ q$ is a convergent of the continued fraction expansion of $\sqrt{d}$, then there are a sol. of one of the eq.

$$x^2 - dy^2 = k \tag{80}$$

where $|k| < 1 + 2\sqrt{d}$.

Remark. All irrational took the periodic infinite sequence.

Remark.

$$x_0 = \sqrt{d} \quad and \quad x_{k+1} = \frac{1}{x_k - [x_k]} \quad \Rightarrow \quad x_{k+1} = \frac{1}{x_k - a_k}. \tag{81}$$

Lemma. Given the continued fraction expansion $\sqrt{d} = [a_0; a_1, a_2, \ldots]$, define s_k and t_k recursively by the relations

$$s_0 = 0 \quad t_0 = 1 \tag{82}$$

$$s_{k+1} = a_k t_k - s_k \quad t_{k+1} = \frac{d - s_{k+1}^2}{k} \quad k = \mathbb{Z}_{>0} \tag{83}$$

Then

$$(a)\ s_k, t_k \in \mathbb{Z},\ t_k \neq 0 \tag{84}$$

$$(b)\ t_k | (d - s_k^2) \tag{85}$$

$$(c)\ x_k = (s_k + \sqrt{d})/t_k,\ k \geq 0. \tag{86}$$

Theorem 6.12. If p_k/q_k are the convergents of the continued fraction expansion of $\sqrt{d}$ then

$$p_k^2 = dq_k^2 = (-1)^{k+1} t_{k+1} \quad where\ t_{k+1} > 0 \quad k \in \mathbb{Z}_{>0} \tag{87}$$

Corollary. If n is the length of the period of the expansion of $\sqrt{d}$, then

$$t_j = 1 \quad \Longleftrightarrow \quad n | j \tag{88}$$

Theorem 6.13. Let p_k/q_k be the convergents of the continued fraction expansion of $\sqrt{d}$ and let n be the length of the expansion.

$$(a)\ n = 2k \Rightarrow \text{All positive sol. of Pell's eq. are given by} \tag{89}$$

$$x = p_{kn-1} \quad y = q_{kn-1} \tag{90}$$

$$(b)\ n = 2k+1 \Rightarrow \text{All positive sol. of Pell's eq. are given by} \tag{91}$$

$$x = p_{2kn-1} \quad y = q_{2kn-1} \qquad k \in \mathbb{Z}_{>0} \tag{92}$$

Theorem 6.14. Let x_1, y_1 be the fundamental solution of Pell's eq. Then every pair of int. x_n, y_n defined by the condition

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \qquad n \in \mathbb{N} \tag{93}$$

Also, every positive sol. of the eq. are determined as above.

This is end. ■