NUMBER THEORY

MATHEMATICAL TRIPOS PART II

Familiarity with IA Numbers and Sets is assumed.

1. Divisibility

Theorem 1.1 (Division Algorithm)**.** *Given $a, b \in \mathbb{Z}$ with $b > 0$, there exists $q, r \in \mathbb{Z}$ with $a = bq + r$ and $0 \le r < b$.*

Proof. Let $S = \{a - nb : n\mathbb{Z}\}$, then S contains some nonnegative integer. Let the smallest be r. Then $r < b$, as otherwise $r - b \in S$ would be nonnegative and smaller than r. So $a - qb = r$ for some $q \in \mathbb{Z}$, or $a = qb + r$. □

Definition 1.2. If $r = 0$, we write $b \mid a$ ("*b divides a*"), otherwise we write $b \nmid a$.

Given $a_1, \ldots, a_n \in \mathbb{Z}$ not all zero, let $I = \{\lambda_1 a_1 + \cdots + \lambda_n a_n \mid \lambda_i \in \mathbb{Z}\}$. Then for $a, b \in I$ and $l, m \in \mathbb{Z}$, we have $la + mb \in I$.

Lemma 1.3. *$I = d\mathbb{Z} = \{md \mid m \in \mathbb{Z}\}$ for some $d > 0$.*

Proof. Let d be the least positive element in I. Then $d\mathbb{Z} \subset I$. Conversely, if $a \in I$, write $a = qd + r$ for some $0 \le r < a$. If $r = 0$, then $a \in d\mathbb{Z}$. Otherwise, $r = a - qd \in I$ is positive and smaller than d, contradiction. □

In particular, $d \mid a_i$ for all i; Conversely, if $c \mid a_i$ for all i, then $d\mathbb{Z} = I \subset c\mathbb{Z}$, hence $c \mid d$.

Definition 1.4. We write $d = \gcd(a_1, \ldots, a_n)$ or $(a_1, \ldots, a_n)$ and say d is the *greatest common divisor* of $a_1, \ldots, a_n$.

Corollary 1.5 (Bézout)**.** *Suppose $a, b, c \in \mathbb{Z}$ and a, b not both 0. There exists $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $(a, b) \mid c$.*

Theorem 1.6 (Euclid's Algorithm)**.** *Given $a, b \in \mathbb{N}$ with $a > b$, setting $b = r_0 > 0$ we can repeatedly apply the division algorithm to get*

$$\begin{aligned} a &= q_1 r_0 + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_{k+1} r_k + 0, \end{aligned}$$

where $0 < r_i < r_{i-1}$ for $i \le k$. Then $r_k = (a, b)$.

Proof. Note that $r_k \mid r_0$ and $r_k \mid a$, so $r_k \le (a, b)$. Also if $m \mid a$ and $m \mid b$ then $m \mid r_k$. Hence $(a, b) \le r_k$, and $(a, b) = r_k$. □

Lemma 1.7 (Euclid's Lemma)**.** *Let p be a prime and let $a, b \in \mathbb{Z}$. Then $p \mid ab$ if and only if $p \mid a$ or $p \mid b$.*

Date: June 8, 2023.

Proof. The "if" direction is clear. Conversely, suppose $p \mid ab$ yet $p \nmid a$, then $(a,p) \neq p$ but $(a,p) \mid p$ and p is prime, so $(a,p) = 1$, therefore there are some integers n, y such that $ax + py = 1$. Now $b = b(ax+py) = x(ab) + (by)p \implies p \mid b$ □

Theorem 1.8 (Fundamental Theorem of Arithmetic)**.** *Every $n > 1$ can be written a a product of primes. Furthermore, this is unique up to reordering.*

Proof. Existence follows easily by strong induction. For uniqueness we also use induction. Suppose that n has two prime factorisations $n = p_1 \cdots p_k = q_1 \cdots q_l$. We have $p_1 \mid q_1 \cdots q_k$, so $p_1 \mid q_i$ for some i. We can label that prime q_1. Hence $p_1 = q_1$. So $n/p_1 = p_2 \cdots p_k = q_2 \cdots q_l$, and by induction $k = l$ and $p_2 = q_2, p_3 = q_3$, etc. □

Theorem 1.9 (Euclid)**.** *The number of primes is infinite.*

Proof. If there was finitely many primes, say $p_1, \ldots, p_k$, then the number $N = p_1 p_2 \cdots p_k + 1$ would have no prime factors which is a contradiction. □

2. Congruences

Definition 2.1. Let $n \geq 1$ be an integer. We say a is *congruent* to b modulo n, written $a \equiv b \pmod{n}$, if $n \mid a - b$.

Theorem 2.2. *There exists x such that $ax \equiv 1 \pmod{n}$ if and only if $(a,n) = 1$.*

Proof. The "only if" direction is clear. For the "if" direction, by Bézout we can write $ax + ny = 1$ for some d, and so $ax \equiv 1 \pmod{n}$ as required. □

Theorem 2.3 (Chinese Remainder Theorem)**.** *Given $m_1, \ldots, m_k \in \mathbb{N}$ pairwise coprime, the set of congruences $x \equiv a_i \pmod{m_i}$, $1 \leq i \leq k$, has a unique solution x modulo $M = m_1 \cdots m_k$.*

Proof. Write $M_i = M/m_i$, then $(m_i, M_i) = 1$ for all i. Therefore for each i there is a b_i such that $M_i b_i \equiv 1 \pmod{m_i}$. We also have $M_i b_i \equiv 0 \pmod{m_j}$ for all $j \neq i$. Take $x = \sum_i a_i b_i M_i$. For uniqueness, if x, y satisfies the system, then $m_i \mid x - y$ for all i, therefore $M \mid x - y$ since there is no prime that divides two distinct m_i's. □

Theorem 2.4 (Fermat's Little Theorem)**.** *If $a, p \in \mathbb{Z}$ with p prime, then $a^p \equiv a \pmod{p}$.*

Proof. For $p = 2$ this is true. Then for $p \neq 2$, $a^p - (a-1)^p \equiv 1 \pmod{p}$ by the binomial theorem. □

Definition 2.5 (Euler Totient Function)**.** Let $\phi(n)$ denote the number of integers a, $1 \leq a \leq n$, with $(a,n) = 1$.

Remark. Directly from the definition we get that $\phi(p^k) = p^k - p^{k-1}$ for p prime, that $\phi(n)$ is multiplicative and thus $\phi(n) = n \prod_{p \mid n} (1 - 1/p)$.

Theorem 2.6 (Euler-Fermat)**.** *If $a, n \in \mathbb{Z}$ have $(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{p}$.*

Proof. By Lagrange's theorem (on groups), the order of a in $(\mathbb{Z}/n\mathbb{Z})^\times$ divides the order of the group, $\phi(n)$. □

Theorem 2.7 (Wilson)**.** $(p-1)! \equiv -1 \pmod{p}$.

Proof. We can pair up terms in the product $(p-1)!$ with their inverses which then multiply to one, but this leaves only 1 and $p - 1$ unpaired. □

Theorem 2.8 (Lagrange)**.** *Let p be a prime and let $f(x)$ be an integer polynomial of degree n. Then $f(x) \equiv 0 \pmod{p}$ has at most n solutions modulo p.*

Definition 2.9. For $a, n \in \mathbb{Z}$ with $n > 0$, the *order* of a modulo n is the least positive integer d such that $a^d \equiv 1 \pmod{n}$. We say that a is a *primitive root* if its order is $\phi(n)$.

Theorem 2.10. *There exists a primitive root mod n if and only if $n = 2, 4, p^j$ or $2p^j$, where p is an odd prime.*

Proof. For $n = 2, 4$ this is easy. We first find a primitive root modulo p. Let $\psi_p(d)$ count the number of $1, 2, \ldots, p-1$ of order d modulo p. Observe that $\psi_p(d) = 0$ if $d \nmid p-1$, so $\sum_{d|p-1} \psi_p(d) = p - 1$. If a has order d, $\{a, a^2, \ldots, a^d\}$ are solutions to $x^d \equiv 1 \pmod{p}$ and hence are all of them by Lagrange. So $\psi(d) \leq \phi(d)$. But $\sum_{d|n} \phi(d) = n$ as $\phi(d)$ counts $\{m \mid (m, n) = n/d\}$. Thus $\psi(d) = \phi(d)$ for all d. In particular, there are $\phi(p-1)$ elements of order $p-1$. Let g be one of them.

If $n = p^j$, $j > 1$, suppose g has orders $p^k s$ modulo n, $s \mid p-1$. By Fermat's Little Theorem $g^{p^k s} \equiv g^s \pmod{p}$, so $s = p - 1$. $g^{p-1} \equiv 1 \pmod{p^2}$ implies $(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \pmod{p^2}$, so WLOG $g^{p-1} \not\equiv 1 \pmod{p^2}$, thus g is a primitive root mod p^2. $g^{p^{j-2}(p-1)} = (1 + \ell p)^{p^{j-2}} \equiv 1 + \ell p^{j-1} \not\equiv 1 \pmod{p^j}$, so g is also a primitive root mod p^j for all $j \geq 2$. One of $g, g + p^j$ is odd, and thus also serves as a primitive root mod $2p^j$, noting $\phi(2p^j) = \phi(p^j)$.

For the other direction, for n not a prime power, $n = rs$ with $(r, s) = 1$ and $\phi(r), \phi(s)$ both even. $a^{\phi(n)}/2 \equiv a^{\phi(r)\phi(s)/2} \equiv 1$ modulo r and s. So $a^{\phi(n)/2} \equiv 1 \pmod{n}$. For $n = 2^j$, $j \geq 3$, $a^2 \equiv 1 \pmod{8}$ for all odd a, thus $a^{2^{k+1}} \equiv (a^2)^{2^k} \equiv 1 \pmod{2^{k+3}}$. ☐

3. Quadratic Residues

Definition 3.1. We call a a *quadratic residue* modulo n if there exists x such that $x^2 \equiv a \pmod{n}$.

Lemma 3.2. *Let p be an odd prime. Then there are exactly $(p-1)/2$ quadratic residues modulo p.*

Proof. Take g to be a primitive root modulo p. Then the set of quadratic residues is exactly $\{g^{2n} \bmod p \mid n \in \mathbb{Z}\}$ which has size $(p-1)/2$. ☐

Definition 3.3. Let p be an odd prime and $a \in \mathbb{Z}$. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

Theorem 3.4 (Euler's Criterion)**.** *Let p be an odd prime, and $a \in \mathbb{Z}$, then*

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

Proof. If a is a quadratic residue, we can write $x^2 \equiv a \pmod{p}$ and then $a^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p}$, as required. By Lagrange, $a^{(p-1)/2} \equiv 1 \pmod{p}$ has at most $(p-1)/2$ solutions, so if a is not a quadratic residue, we must have $a^{(p-1)/2} \equiv -1 \pmod{p}$. ☐

Corollary 3.5. *Let p be an odd prime and let $a, b \in \mathbb{Z}$, then*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Corollary 3.6. *Let p be an odd prime, then*

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

Definition 3.7. The *numerically least residue* a' of $a \pmod n$ to $a' \equiv a$ with $-n/2 < a' \leq n/2$.

Theorem 3.8 (Gauss' Lemma)**.** *Given an odd prime p and a with $(a,p) = 1$, let a_j denote the numerically least residue of $a \cdot j \pmod p$. Then $(a/p) = (-1)^\ell$, where $\ell = |\{j \leq (p-1)/2 \mid a_j < 0\}|$.*

Proof. We have $a_j = \pm a_k$ if and only if $j = \pm k$, so $|a_j|$ takes all values $1, \ldots, (p-1)/2$. Hence $\prod_{j \leq (p-1)/2} a_j = (-1)^\ell r!$, so $a^{(p-1)/2} \equiv (-1)^\ell \pmod p$. The result then follows from Euler's Criterion. $\square$

Theorem 3.9 (Law of Quadratic Reciprocity)**.** *If p, q are distinct odd primes, $(p/q) = (q/p)$ unless $p \equiv q \equiv 3 \pmod 4$, in which case $(p/q) = -(q/p)$. More concisely, $(p/q)(q/p) = (-1)^{((p-1)/2)((q-1)/2)}$.*

Proof. By Gauss' lemma, $(p/q) = (-1)^\ell$, where ℓ is the number of lattice points (x, y) satisfying $0 < x < q/2$, $-q/2 < px - qy < 0$. For such points $q(y - 1/2) < px$, so $y < p/2 + 1/2/$ We therefore lose nothing in imposing the extra symmetrising condition $0 < y < p/2$. Similarly $(q/p) = (-1)^m$ where m is the number of lattice points in the rectangle $0 < x < q/2$. $0 < y < p/2$, satisfying $-p/2 < qx - py < 0$ or equivalently $0 < px - qy < p/2$. Now it suffices to prove that $((p-1)/2)((q-1)/2) - (\ell + m)$ is even. But $((p-1)/2)((q-1)/2)$ is just the number of lattice points in our rectangle and we have a bijection between such points with $px - qy \leq -q/2$ and those with $px - qy \geq p/2$ by means of transformation $x' = (q+1)/2 - x$, $y' = (p+1)/2 - y$. (This does *not* fix the line $px - qy = 0$, so we cannot say the same for our original sets. $\square$

Definition 3.10. For n odd, $(m, n) = 1$, we define the *Jacobi symbol* (m/n) by

$$\left(\frac{m}{p_1^{\alpha_1} \cdots p_k^{\alpha_k}}\right) = \left(\frac{m}{p_1}\right)^{\alpha_1} \cdots \left(\frac{m}{p_k}\right)^{\alpha_k}$$

in terms of Legendre symbols.

Remark. All of our previously stated theorems hold for Jacobi symbols, though Jacobi symbols are not a test for quadratic residuality, only a computational technique.

4. Quadratic Forms

Definition 4.1. A *binary quadratic form* is a function $f(x, y) = ax^2 + byx + cy^2$, $a, b, c \in \mathbb{Z}$. This may sometimes be represented more simply as (a, b, c). Note that

$$f(x, y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Definition 4.2. A *unimodular substitution* is a transformation $X = px + qy$, $Y = rs + sy$ with $ps - qr = 1$. Equivalently, $\begin{pmatrix} X & Y \end{pmatrix}^\intercal = A \begin{pmatrix} x & y \end{pmatrix}^\intercal$, with $A \in \mathrm{SL}_2(\mathbb{Z})$.

Definition 4.3. Two binary quadratic forms f and f' are *equivalent* of they are related by a unimodular substitution. We then write $f \sim f'$.

Definition 4.4. $4af(x, y) = (2ax + by)^2 - dy^2$ where $d = \mathrm{disc}(f) = b^2 - 4ac$ is the *discriminant* of f.

Theorem 4.5. *Equivalent forms have the same discriminant.*

Proof. We have

$$\begin{aligned}\operatorname{disc}(f) &= -4\left|\begin{pmatrix} a & b/2 \\ b/2 & c\end{pmatrix}\right| \\ &= -4\left|\begin{pmatrix} p & q \\ r & s\end{pmatrix}^{\intercal}\begin{pmatrix} a & b/2 \\ b/2 & c\end{pmatrix}\begin{pmatrix} p & q \\ r & s\end{pmatrix}\right|\end{aligned}$$

as $(ps-qr)^2 = 1$, and this is equal to $\operatorname{disc}(f')$. □

Definition 4.6. A binary quadratic form with $d \neq 0$ is *positive definite* if $f(x,y) \geq 0$ for all x, y. It's *negative definite* if $f(x,y) \leq 0$, and *indefinite* otherwise.

Theorem 4.7. *A positive definite form (a,b,c) is equivalent to some* reduced *form satisfying $-a < b \leq a < c$ or $0 \leq b \leq a = c$.*

Proof. Using unimodular substitution $S : (a,b,c) \mapsto (c,-b,a)$ and $T_{\pm} : (a,b,c) \to (a, b \pm 2a, a \pm b + c)$, if $a > c$. i.e. S to decrease a while keeping $|b|$ fixed. If $a < c$ and $|b| > a$, then use T_+ or T_- to decrease $|b|$ whilst keeping a fixed, noting all the while that $a + |b|$ is strictly decreasing so this process must stop. Finally if $b = -a$, apply T_+ to get $+a$ and if $a = c$, apply S to get $b > 0$. □

Theorem 4.8. *The smallest integer $\neq 0$ represented by a reduced positive definite form (a,b,c) all coprime are a, c and $a - |b| + c$ in that order.*

Proof. $f(0,0) = 0$. $f(1,0) = a$, $f(0,1) = c$, $0 < a \leq c$ since f is reduced. Now, for $|x| \geq |y| > 0$, $f(x,y) \geq a|x|^2 - |b||x|^2 + c|y|^2 = (a-|b|)|x|^2 + c|y|^2 \geq a - |b\ + c$. Similarly if $|y| \geq |x| > 0$, and we can only achieve equality at $(\pm 1, \pm 1)$ and indeed we do. □

Theorem 4.9. *No two reduced forms are equivalent.*

Proof. By our result on the smallest represented integer, $f \sim f'$ implies $a = a'$ and $c = c'$. Then by equivalent forms having the same discriminant, $d = d'$ hence $b = \pm b'$. If $b = 0$ or $b = b'$ we are done, so suppose $b > 0$ and $(a,b,c) \sim (a,-b,c)$. Then both reduced implies $a < c$ and $|b| < a$, or $b = -a$ (which cannot happen). Now f, f' both satisfy $f(x,y) = a$ if and only if $(x,y) = (\pm 1, 0)$ and $f(x,y) = c$ if and only if $(x,y) = (0, \pm 1)$. so if they are equivalent under substitution $\begin{pmatrix} p & q \\ r & s\end{pmatrix}$ we must have $\begin{pmatrix} p & q \\ r & s\end{pmatrix}\begin{pmatrix} \pm 1 \\ 0\end{pmatrix} = \begin{pmatrix} \pm 1 \\ 0\end{pmatrix}$ implying $p = \pm 1, r = 0$ and $\begin{pmatrix} p & q \\ r & s\end{pmatrix}\begin{pmatrix} 0 \\ \pm 1\end{pmatrix} = \begin{pmatrix} 0 \\ \pm 1\end{pmatrix}$ implying $q = 0$, $s = \pm 1$. det $\begin{pmatrix} p & q \\ r & s\end{pmatrix} = \pm I$ implies $f = f'$ as required. □

Theorem 4.10. *There are finitely many reduced forms with discriminant d. Indeed, $|b| \leq a \leq \sqrt{d/2}$.*

Proof. $d = b^2 - 4ac \leq ac - 4ac \leq -3a^2$ which implies our claim. $c = (b^2-d)/4a$. □

Theorem 4.11. *Given $n \in \mathbb{N}$, n is properly represented by a form f, that is $f(x,y) = n$ for some coprime x, y if and only if f is equivalent to a form (n, w, c) with first coefficient n.*

Proof. If f is equivalent to this form $f \sim f'$, $f'(1,0) = n$ so $f(x,y) = n$ properly represented as coprimality is preserved under $\mathrm{SL}_2(\mathbb{Z})$. If $f(x,y) = n$ with $(x,y) = 1$ then there exists q, s such that $xs - qy = 1$. Then

$$\begin{pmatrix} x \\ y\end{pmatrix} = \begin{pmatrix} x & q \\ y & s\end{pmatrix}\begin{pmatrix} 1 \\ 0\end{pmatrix},$$

so applying this matrix being in $\mathrm{SL}_2(\mathbb{Z})$ to f, we get f' with $f'(1,0) = n$. □

Theorem 4.12. *Given $n \in \mathbb{N}$, n is properly represented by some form of discriminant d if and only if there is a solution w to $w^2 = d \pmod{4n}$.*

Proof. By the previous theorem, $w^2 - 4nc = d$. Conversely, $w^2 \equiv d \pmod{4n}$ implies there exists c such that $w^2 = d + 4nc$ implies (n, w, c) has discriminant d. □

5. Prime Numbers

Definition 5.1. The *prime counting function* is $\pi(x)$, the number of primes $\leq x$.

Definition 5.2. The *Möbius function* $\mu(n)$, $n \in \mathbb{N}$ is such that $\mu(n) = 0$ if n is not squarefree, and $\mu(n) = (-1)^r$ if n is a product of r distinct primes.

Observe that $\sum_{d|n} \mu(d) = 0$ for $n > 1$.

Theorem 5.3 (Legendre's Formula)**.** $\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d|P} \mu(d)\lfloor x/d \rfloor$, *where P denotes the product $P = p_1 \cdots p_k$ of primes $\leq \sqrt{x}$.*

Proof. The Eratosthenes sieve up to $\sqrt{x}$ applied to $\{1,\ 2,\ \ldots,\ x\}$ crosses out all multiples of $p_1, \ldots, p_k$ leaving behind only primes p with $\sqrt{x} < p \leq x$ and 1. The result now follows by the Inclusion-Exclusion principle. □

Theorem 5.4. $\sum_{i=1}^{\infty} 1/p_i$ *diverges.*

Proof. Otherwise, there exists k such that the truncated series $\sum_{i>k} 1/p_i < 1/2$. Set $P = p_1 \cdots p_k$ and observe that every number equivalent to $1 \pmod p$ can be factorised as a product of j of the primes $P_{k+1}, p_{k+2}, \ldots$ for some j. Hence

$$\sum_{n \equiv 1 \bmod p} \frac{1}{n} \leq \sum_{j=1}^{\infty} \left(\sum_{i=k+1}^{\infty} \frac{1}{p_i} \right)^j \leq \sum_{j=1}^{\infty} \left(\frac{1}{2} \right)^j = 1,$$

which is a contradiction. □

Theorem 5.5. $\prod_{p \leq n} p \leq 4^n$.

Proof. The proof is by induction, observing

$$\prod_{n < p \leq 2n} p \mid \binom{2n}{n} \leq 2^{2n} = 4^n.$$

□

Corollary 5.6. $\pi(x) \leq x \log 4 / \log x$.

Theorem 5.7 (Prime Number Theorem)**.** $\pi(x) \sim \frac{x}{\log x}$.

Definition 5.8. The *Riemann zeta function* is defined for $s = \sigma + it$ for $\sigma > 1$ by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$.

Theorem 5.9 (Euler Product)**.** $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$, $\sigma > 1$.

Proof. For any N, $\prod_{p \leq N} (1 - p^{-s})^{-1} = \prod_{p \leq N} (1 + p^{-s} + p^{-2s} + \cdots) = \sum_m m^{-s}$, where m runes through all integers with no prime factors $> N$. the difference between this and $\sum_{n \leq N} n^{-s}$ is bounded in absolute value by $\sum_{n > N} n^{-\sigma} \to 0$ as $N \to \infty$. □

Theorem 5.10. *There are infinitely many primes in the arithmetic progression a, $a + d$, $\ldots$ provided $(a, d) = 1$.*

6. Diophantine Approximation

Theorem 6.1 (Dirichlet)**.** *Given $\theta \in \mathbb{R}$, $N \in \mathbb{N}$, there exists integers p, q with $q \leq N$ such that $|\theta - p/q| \leq 1/q^N \leq 1/q^2$.*

Proof. Two of θ, 2θ, $\dots$, $N\theta$ must differ by $\leq 1/N$ modulo 1. Their difference $q\theta$ differs from some p by $\leq 1/N$. $\square$

Definition 6.2. Given $\theta \in \mathbb{R}$, define $a_0 = \lfloor \theta \rfloor$, $\theta_1 = \frac{1}{\theta - a_0}$, $a_1 = \lfloor \theta_1 \rfloor$, $\theta_2 = \frac{1}{\theta_1 - a_1}$, etc. terminating if some θ_i is an integer. Then

$$\theta = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots}}$$

is the *continued fraction* representation of θ. The integers a_i are called *partial quotients* of θ, and we write $\theta = [a_0, a_1, \dots]$. $p_n/q_n = [a_0, a_1, \dots, a_n]$ are called *convergents.*

Theorem 6.3. *(i) The p_n, q_n satisfy the recurrence relations*

$$p_n = a_n p_{n-1} + p_{n-2},$$
$$q_n = a_n q_{n-1} + q_{n-2},$$

with $p_0 = a_0$ and $q_0 = 1$, $p_1 = a_0 a_1 + 1$ and $q_1 = a_1$. (ii) $|p_{n-1}/q_{n-1} - p_n/q_n| = \frac{1}{q_{n-1}q_n}$. (iii) θ lies in $[p_{n-1}/q_{n-1}, p_n/q_n]$ and thus $|\theta - p_n/q_n| \leq 1/q_n^2$.

Proof. (i) We check this is true for $n = 2$. Then supposing it is true for $n = m - 1 \geq 2$, we observe $p_j/q_j = a_0 + q'_j/p'_j$, where $p'_j/q'_j = [a_1, a_2, \dots, a_j]$. Then $p_j = a_0 p'_j + q'_j$ and $q_j = p'_j$ expanded implies our result. (ii) $p_n q_{n+1} - p_{n+1} q_n = (-1)^{n+1}$ follows from (i) by induction. (iii) Observe $\theta = [a_0, a_1, \dots, a_n, \theta_{n+1}]$ and $0 < 1/\theta_{n+1} \leq 1/a_{n+1}$ so θ lies in the interval $[p_n/q_n,\ p_{n+1}/q_{n+1}]$ and this with the other results gives the stated bound. $\square$

Theorem 6.4. *The continued fractions process terminates if θ is rational.*

Proof. If $\theta = a/b$ then $1/q_n^2 \geq |\theta - p_n/q_n| \geq 1/q_n b$ for $p_n/q_n \neq a/b$, so q_n may never exceed b. The partial quotients $a_0, a_1, \dots$ are in fact the q_i of Euclid's algorithm on (a, b). $\square$

Theorem 6.5. $\theta = \frac{p_n \theta_{n+1} + p_{n-1}}{q_n \theta_{n+1} + q_{n-1}}$ *from $\theta = [a_0,\ \dots,\ a_n,\ \theta_{n+1}]$. The p_n/q_n give successively better approximations of θ as n increases.*

Proof. Multiplying up $|q_n\theta - p_n|$, we find that it equals $(q_n \theta_{n+1} + q_{n-1})^{-1}$ and the denominator of the latter exceeds $q_n + q_{n-1} = (a_n + 1)q_{n-1} + q_{n-2} > q_{n-1}\theta_n + q_{n-2}$. $\square$

Theorem 6.6. *If $0 < q < q_{n+1}$, $|q\theta - p| \geq |q_n\theta - p_n|$.*

Proof. Define u, v by $p = up_n + vp_{n+1}$, $q = uq_n + vq_{n+1}$. Solving by multiplying the former by q_{n+1} and the latter by p_{n+1} and q_n, p_n respectively observe that u, v are integers. $|q\theta - p| = |u(q_n\theta - p_n) + v(q_{n+1}\theta - p_{n+1})| \geq |q_n\theta - p_n|$ as $u \neq 0$ and $\operatorname{sgn}(v) \neq \operatorname{sgn}(u)$. $\square$

Theorem 6.7. *If rational p/q satisfies $|\theta - p/q| < \frac{1}{2q^2}$, then it is convergent to θ.*

Proof. Suppose $q_n < q < q_{n+1}$. Then $|p/q - p_n/q_n| \leq |\theta - p/q| + |\theta - p_n/q_n| \leq 2|q\theta - p|/q_n < 1/qq_n$, which is a contradiction. $\square$

Definition 6.8. The equation $x^2 - dy^2 = 1$, where d is a positive integer which is not a square is known as *Pell's equation.*

Theorem 6.9. *If (x, y) is a solution to the Pell equation $x^2 - dy^2 = 1$, then x/y must be a convergent to $\sqrt{d}$.*

Proof. $(x - y\sqrt{d})(x + y\sqrt{d}) = 1$ implies $x - y\sqrt{d} = \frac{1}{x+y\sqrt{d}}$. Certainly $x > y\sqrt{d}$, whence $x - y\sqrt{d} < \frac{1}{2y\sqrt{d}}$ and thus $|\sqrt{d} - x/y| < \frac{1}{2y^2}$. The previous theorem hen gives us our result. □

Theorem 6.10. *If (x, y) is the solution of $x^2 - dy^2 = 1$ with $x + y\sqrt{d}$ minimal, then every solution is given by (x_n, y_n), where $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$ for some n.*

Proof. Denoting $x + y\sqrt{d} \in \mathbb{R}$ by $\varepsilon > 1$, suppose to the contrary we have a solution (a, b) with $\varepsilon^k < a + b\sqrt{d} < \varepsilon^{k+1}$. Define $N(a + b\sqrt{d}) = a^2 - db^2$ and observe that $N(\alpha\beta) = N(\alpha)N(\beta)$, $N(\varepsilon) = 1 = N(\varepsilon^{-k}(a + b\sqrt{d}))$, where $\varepsilon^{-1} = x - y\sqrt{d}$, which gives us a contradiction. □

Definition 6.11. $\alpha \in \mathbb{R}$ or $\mathbb{C}$ is *algebraic* if it is the root of a polynomial with integer coefficients. If $P(\alpha) = 0$ with P irreducible and $\deg P = n$ then $\alpha$is said to have *degree n*. Non-algebraic numbers are called *trancendental*.

Theorem 6.12 (Liouville's Theorem)**.** *If $\alpha \in \mathbb{R}$ is algebraic of degree $n > 1$, there exists c depending on α such that $|\alpha - p/q| > c/q^n$ for all $p/q \in \mathbb{Q}$.*

Proof. Observe $P(\alpha) - P(p/q) = (\alpha - p/q)p'(\xi)$ for some ξ between α and p/q. Choose P to be the minimal polynomial of α, so $P(\alpha) = 0$ and P irreducible implies $0 \neq |P(p/q)| \geq 1/q^n$. WLOG $|\alpha - p/q| < p$ and choose C so that $|P'(\xi)| < C$ for $|\xi - \alpha| < 1$. Then $|\alpha - p/q| \geq c/q^n$ with $c = 1/C$. □

7. Primality Testing

Definition 7.1. If n is an odd composite number and $(b, n) = 1$, then n is a *Fermat pseudoprime* to the base b if $b^{n-1} \equiv 1 \pmod{n}$. If it is a pseudoprime to every b, then it is a *Carmichael number*.

Theorem 7.2. *Let $N > 1$. If N is not a Fermat pseudoprime to some base b_0, then it is not a Fermat pseudoprime to base b for at least half of b coprime to N.*

Proof. The set B of integers $1 \leq b < N$ such that $(b, N) = 1$ where N is a Fermat pseudoprime to base b is clearly a subgroup of $(\mathbb{Z}/NZ)^\times$. It's proper as $b_0 \in (\mathbb{Z}/NZ)^\times$is not in B. Consequently $|B| \leq |(\mathbb{Z}/NZ)^\times|/2$ which concludes the proof. □

Definition 7.3. Let $b \in \mathbb{N}$. An odd composite integer $N > 1$ is said to be an Euler pseudoprime to base b if $b^{(N-1)/2} \equiv \left(\frac{b}{N}\right) \mod N$.

Theorem 7.4. *Let $N > 1$. If N is not an Euler pseudoprime to some base b_0, then it is not a Euler pseudoprime to base b for at least half of b coprime to N.*

Proof. Same as the corresponding theorem for Fermat pseudoprimes. □