Solutions to *Modular Functions and Dirichlet Series in Number Theory* by Tom M. Apostol

Blaze Okonogi-Neth

Contents

Chapter 1

Exercise 1.1. Prove that two lattice bases, (ω_1, ω_2) and (ω_1', ω_2') generate the same lattice, that is $(\omega_1, \omega_2) \sim (\omega_1', \omega_2')$, if and only if there is a 2×2 matrix with integer entries and determinant equal to ± 1 such that,

$$\begin{bmatrix} \omega_2' \\ \omega_1' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \omega_2 \\ \omega_1 \end{bmatrix}$$

Solution. Note that this is equivalent to the following condition,

$$\begin{aligned} \omega_2' &= a\omega_2 + b\omega_1 \\ \omega_1' &= c\omega_2 + d\omega_1 \end{aligned}$$

Let A and B be our two lattice basis and assume that our two pairs generate the same lattice, $(\omega_1, \omega_2) = (\omega_1', \omega_2')$. By definition there exists integer square matrices, V and W, such that,

$$\begin{aligned} A &= BV \\ B &= AW \end{aligned}$$

We can rewrite this equation as,

$$\begin{aligned} A &= AWV \\ 0 &= A(I - VW) \end{aligned}$$

Of course, B is a lattice basis, and thus linear independent. This implies that $VW = I$. Calculating the determinant and noting that since V and W are integer matrices we have $\det(V), \det(W) \in \mathbb{Z}$ we get,

$$\begin{aligned} \det(V) \cdot \det(W) = \det(V \cdot W) = \det(I) = 1 \\ \det(V) = \det(W) = \pm 1 \end{aligned}$$

For the other direction, assume that $A = BU$ where A, B are lattice basis and U is a unimodular, integer matrix. Then, U^{-1} exists and is also a unimodular integer matrix. It follows that,

$$\begin{aligned} A &= BU \\ B &= AU^{-1} \end{aligned}$$

and thus that $(\omega_1, \omega_2) \subseteq (\omega_1', \omega_2')$ and $(\omega_1', \omega_2') \subseteq (\omega_1, \omega_2)$. It follows that $(\omega_1, \omega_2) \sim (\omega_1', \omega_2')$. $\square$

Exercise 1.2. Let $S(0)$ denote the sum of the zeros of an elliptic function f in a period parallelogram, and let $S(\infty)$ denote the sum of the poles in the same parallelogram. Prove that $S(0) - S(\infty)$ is a period of f by integrating $zf'(z)/f(z)$.

Solution. By the argument principle we have the following relation between the difference of sums $S(0) - S(\infty)$ and the integral of the logarithmic derivative.

$$2\pi i(S(0) - S(\infty)) = \int_{\partial P} \frac{f'(z)}{f(z)} dz$$

We can adjust this integral to $\int_{\partial P} z\frac{f'(z)}{f(z)}dz$. Our problem then reduces to showing that $\frac{1}{2\pi i}\int_{\partial P} z\frac{f'(z)}{f(z)}dz$ is a lattice point. We can consider the contribution of two opposite sides of the fundamental parallelogram,

$$\begin{aligned}\frac{1}{2\pi i}\int_a^{a+\omega_1} z\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi i}\int_{a+\omega_1+\omega_2}^{a+\omega_2} z\frac{f'(z)}{f(z)}d &= \frac{1}{2\pi i}\int_a^{a+\omega_1} z\frac{f'(z)}{f(z)}dz - \frac{1}{2\pi i}\int_{a+\omega_2}^{a+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz \\ &= \frac{1}{2\pi i}\int_a^{a+\omega_1} z\frac{f'(z)}{f(z)}dz - \frac{1}{2\pi i}\int_a^{a+\omega_1} (z+\omega_2)\frac{f'(z)}{f(z)}dz\end{aligned}$$

Note that f is ω_2 periodic, which implies the following simplification,

$$\frac{-\omega_2}{2\pi i}\int_a^{a+\omega_1} \frac{f'(z)}{f(z)}dz = -\frac{1}{2\pi i}\frac{f'(z)}{f(z)}dz \cdot \omega_2.$$

Now, $\frac{1}{2\pi i}\frac{f'(z)}{f(z)}dz$ must be in $\mathbb{Z}$, since it is the winding number of a closed curve. This shows that our two original sides add up to an integer multiple of ω_2. A similar argument will show that the other two sides add to an integer multiple of ω_1, which gives the final result. □

Exercise 1.3. Prove that $\wp(u) = \wp(v)$ if and only if $u - v$ or $u + v$ is a period of $\wp$.

Solution. Begin by assuming that either $u - v$ or $u + v$ is a period of $\wp$. If $u - v$, then we have,

$$\wp(u) = \wp((u - v) + v) = \wp(v)$$

If $u + v$ is a period, then we have,

$$\wp(u) = \wp((u + v) - v) = \wp(-v) = \wp(v),$$

since $\wp(-x) = \wp(x)$ by the evenness of $\wp$.

For the other direction, suppose that $\wp(u) = \wp(v)$. Note that $\wp$ only has a pole of order 2, which implies that it takes on each complex value on the fundamental parallelogram twice. Now, by evenness, $\wp(u) = \wp(-u)$. When u and v are in the fundamental parallelogram we have $v = -u \mod L$, and thus $u + v = 0 \mod L$. Alternatively, in the only other case, in which u and v are not in the same quadrant, we have $v = \pm u \mod L$, and so $u - v = 0 \mod L$. This finishes the proof.

□

Exercise 1.7. Prove that the discriminant of $f(x) = 4x^3 - ax - b$ is $a^3 - 27b^2$.

Solution. The discriminant of a cubic polynomial $ax^3 + bx^2 + cx + d$ is given by,

$$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$$

We simply plug in our coefficients and solve,

$$\begin{aligned} \Delta &= -4(4)(-a)^3 - 27(4^2)(-b)^2 \\ &= 16(a^3 - 27b^2) \end{aligned}$$

Which is the desired result up to a constant factor. □

Exercise 1.10. Let ω_1 and ω_2 be complex numbers with nonreal ratio. Let $f(z)$ be an entire function and assume there are constants a and b such that

$$\begin{aligned} f(z + \omega_1) &= af(z) \\ f(z + \omega_2) &= bf(z) \end{aligned}$$

for all z. Prove that $f(z) = Ae^{Bz}$, where A and B are constants.

Solution. Define the following function

$$g(z) = \frac{f(z)}{e^{Bz}}$$

We want to choose B such that the above function is doubly periodic in ω_1 and ω_2. Consider the following

$$\begin{aligned} e^{Bz+B\omega_1} &= ae^{Bz} \\ e^{Bz+B\omega_2} &= be^{Bz} \end{aligned}$$

Solving this gives

$$B = \frac{\log a - \log b}{\omega_1 - \omega_2}$$

Now $g(z)$ is a doubly periodic entire function. By Liouvilles theorem $g(z)$ is constant and equal to some $A \in \mathbb{C}$, and so the result follows,

$$f(z) = Ae^{Bz}$$

□

Exercise 1.11. If $K \geq 2$ and $\tau \in H$ prove that the Eisenstein series

$$G_{2k}(\tau) = \sum_{m,n \neq 0} (m + n\tau)^{-2k}$$

has the Fourier expansion

$$G_{2k}(\tau) = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

Solution. We are guided by Apostol's proof of lemma 3 on pg. 19. We reproduce the argument here for completion's sake before extending it to the general case.

The proof starts with the partial fraction expansion of the cotangent function. Let $\tau \in H$, the upper half complex plane, and $k \geq 2$.

$$\pi \cot \pi\tau = \frac{1}{\tau} + \sum_{m\in\mathbb{Z}, m\neq 0} \left(\frac{1}{\tau + m} - \frac{1}{m} \right)$$

Since τ has positive imaginary part $|q| = |e^{2\pi i\tau}| < 1$. Then,

$$\pi \cot \pi\tau = -\pi i \left(1 + 2\sum_{r=1}^{\infty} q^r \right)$$

Taking the derivative with respect to τ we get,

$$-\frac{1}{\tau^2} - \sum_{m\in\mathbb{Z}, m\neq 0}^{\infty} \frac{1}{(\tau+m)^2} = -(2\pi i)^2 \sum_{r=1}^{\infty} re^{2\pi i r\tau}$$

We can repeat this derivative repeatedly and obtain a formula for $\sum (m+\tau)^{-2k}$. Then we can replace τ by $n\tau$ and take the sum over n. This gives the following,

$$\begin{aligned}
\sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^{2k}} &= \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{r=1}^{\infty} r^{2k-1} \exp(2\pi i r n\tau) \\
&= \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{r=1}^{\infty} r^{2k-1} q^{nr}
\end{aligned}$$

We can use this result to derive the general Fourier expansion.

$$\begin{aligned}
G_{2k}(\tau) &= \sum_{m,n=-\infty, (m,n)\neq(0,0)}^{\infty} \frac{1}{(m+n\tau)^{2k}} \\
&= \sum_{m\in\mathbb{Z}, m\neq 0} \frac{1}{m^{2k}} + \sum_{n=1}^{\infty} \sum_{m\in\mathbb{Z}} \left(\frac{1}{(m+n\tau)^{2k}} + \frac{1}{(m-n\tau)^{2k}} \right) \\
&= 2\zeta(2k) + 2\sum_{n=1}^{\infty} \sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^{2k}} \\
&= 2\zeta(2k) + 2 \cdot \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} r^{2k-1} q^{nr} \\
&= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{r=1}^{\infty} \frac{r^{2k-1} q^r}{1-q^r} \\
&= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \\
&= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n
\end{aligned}$$

$\square$

Exercise 1.12. If $\tau \in H$ prove that

$$G_{2k}(-1/\tau) = \tau^{2k} G_{2k}(\tau)$$

and deduce that

$$\begin{aligned} G_{2k}(i/2) &= (-4)^k G_{2k}(2i) \text{ for all } k \geq 2 \\ G_{2k}(i) &= 0 \text{ if } k \text{ is odd} \\ G_{2k}(e^{2\pi i/3} &= 0 \text{ if } k \neq 0 \mod 3 \end{aligned}$$

Solution. We will use the series representation of $G_{2k}(\tau)$ to prove $G_{2k}(-1/\tau) = \tau^{2k} G_{2k}(\tau)$.

$$\begin{aligned} G_{2k}(-1/\tau) &= \sum (m + n(-1/\tau))^{-2k} \\ &= \sum \frac{1}{(m + \frac{-n}{\tau})^{2k}} \\ &= \tau^{2k} \sum \frac{1}{(m\tau - n)^{2k}} \\ &= \tau^{2k} G_{2k}(\tau) \end{aligned}$$

We will use this identity to show the desired identities. Making our first substitution gives us,

$$\begin{aligned} \frac{-1}{\tau} &= \frac{i}{\tau} \\ \tau &= 2i \end{aligned}$$

Plugging into our equation we see that,

$$\begin{aligned} G_{2k}(i/2) &= (2i)^{2k} G_{2k}(2i) \\ &= -4^k G_{2k}(2i) \end{aligned}$$

For the next identity we make the substitution,

$$-\frac{1}{\tau} = i$$

Which implies that $\tau = i$. Then we have,

$$G_{2k}(i) = i^{2k} G_{2k}(i)$$

Which forces $G_{2k}(i) = 0$ when k is odd.

To prove the third identity we substitute as follows,

$$-\frac{1}{\tau} = e^{2\pi i/3}$$

Which implies that $\tau = -e^{-2\pi i/3}$. Then,

$$G_{2k}(e^{2\pi i/3}) = (-e^{-2\pi i/3})^{2k} G_{2k}(-e^{-2\pi i/3})$$

Recall that $G_{2k}(\tau) = G_{2k}(\tau+1)$. It follows that $G_{2k}(e^{2\pi i/3}) = G_{2k}(-e^{-2\pi i/3})$, and thus,

$$G_{2k}(e^{2\pi i/3}) = (-e^{-2\pi i/3})^{2k} G_{2k}(e^{2\pi i/3})$$

This forces $G_{2k}(e^{2\pi i/3}) = 0$ when $k \neq 0 \mod 3$. This completes the exercise. $\square$

Exercise 1.14. A Lambert series is a series of the form $\sum_{n=1}^{\infty} f(n)x^n/(1-x^n)$. Assuming absolute convergence, prove that,

$$\sum_{n=1}^{\infty} f(n)\frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} F(n)x^n$$

where

$$F(n) = \sum_{d|n} f(d)$$

Apply this result to obtain the following formulas, valid for $|x| < 1$.

$$\sum_{n=1}^{\infty} \frac{\mu(n)x^n}{1-x^n} = x \tag{1}$$

$$\sum_{n=1}^{\infty} \frac{\phi(n)x^n}{1-x^n} = \frac{x}{(1-x)^2} \tag{2}$$

$$\sum_{n=1}^{\infty} \frac{n^{\alpha}x^n}{1-x^n} = \sum_{n=1}^{\infty} \sigma_{\alpha}(n)x^n \tag{3}$$

$$\sum_{n=1}^{\infty} \frac{\lambda(n)x^n}{1-x^n} = \sum_{n=1}^{\infty} x^{n^2} \tag{4}$$

Then, use the third identity to express $g_2(\tau)$ and $g_3(\tau)$ in terms of Lambert series in $x = e^{2\pi i\tau}$.

Solution. First, we will show that $\sum_{n=1}^{\infty} f(n)\frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} F(n)x^n$ when $F(n) = \sum_{d|n} f(d)$. Note that

$$\frac{x^n}{1-x^n} = \sum_{m=1}^{\infty} x^{nm}$$

Then,

$$\sum_{n=1}^{\infty} f(d)\frac{x^d}{1-x^d} = \sum_{n=1}^{\infty} f(n) \sum_{m=1}^{\infty} x^{nm}$$

Reindex by letting $k = nm$ and note that the index of the coefficient $f(n)$ must divide the power of each term x. This gives the desired identity,

$$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n} = \sum_{k=1}^{\infty} \sum_{d|k} f(d) x^k \tag{5}$$

Also, note that $(\mathbf{1} * f)(d) = \sum_{d \nmid n} f(d)$, which gives the following alternative representation,

$$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} (\mathbf{1} * f)(n) x^n$$

We will now prove the other identities. First, we will show that

$$\sum_{n=1}^{\infty} \frac{\mu(n) x^n}{1-x^n} = x$$

We can rewrite Equation (5) as,

$$\sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n} = \sum_{k=1}^{\infty} \left(\sum_{d|k} \mu(k) \right) x^k$$

Let $k \neq 1$. First, consider the case in which $k = p_1 p_2 ... p_r$ is square free. There are 2^r subsets of $\{p_1 p_2 ... p_r\}$. Subsets with even parity correspond to an even number of prime divisors, and thus add -1 to the sum, where as subsets with odd parity correspond to an odd number of prime divisors, and add 1 to the sum. The number of even and odd subsets are both given by 2^{r-1}, and thus the sum is 0. If k is not square free, then of course the sum is 0 as well. The only case in which the sum is not 0 is when $k = 1$, in which case we are simply summing over $\mu(1) = 1$, and so it collapses and becomes,

$$\sum_{k=1}^{\infty} \left(\sum_{d|k} \mu(k) \right) x^k = x$$

Next, we will prove Equation (2). Recall that

$$\sum_{d|k}^{\infty} \phi(k) = k$$

We can then express the sum as follows,

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{\phi(n)x^n}{1-x^n} &= \sum_{k=1}^{\infty} \left(\sum_{d|k}^{\infty} \phi(k) \right) x^k \\
&= \sum_{k=1}^{\infty} kx^k \\
&= x^{k-1} \sum_{k=1}^{\infty} kx^{k-1} \\
&= x \left(\sum_{k=0}^{\infty} x^k \right)' \\
&= x \left(\frac{1}{1-x} \right)' \\
&= \frac{x}{(1-x)^2}
\end{aligned}$$

which is the form we were looking for.
To show Equation (3) take $\alpha \in \mathbb{C}$ and simply note that due to Equation (5) we have

$$\sum_{n=1}^{\infty} \frac{n^\alpha x^n}{1-x^n} = \sum_{k=1}^{\infty} \left(\sum_{d|k}^{\infty} d^\alpha \right) x^k$$

Which is exactly $\sum_{k=1}^{\infty} \sigma_\alpha(k) x^k$.

□

Chapter 2

Exercise 2.2. Find the smallest integer $n > 0$ such that $(ST)^n = I$.

Solution. Recall,

$$S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$
$$T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Then direct computation shows that

$$T = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$$

And

$$
\begin{aligned}
(ST)^3 &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\
(ST)^6 &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\end{aligned}
$$

□

Exercise 2.4. Determine all elements A of Γ which leave i fixed.

Solution. Select some $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. A fixes i exactly when $ai + b = (ci + d)i = -c + di$. This implies that either $a = d$ and $b = -c$ or $d = a$ and $c = -b$. Then,

$$a = ad - bc = a^2 + b^2$$

Now, $(a, b) = (\pm 1, 0)$ or $(a, b) = (0, \pm 1)$. That is,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is either $\pm I$ or $\pm S$. These matrices fix i, and so,

$$\mathrm{Stab}_i = \{\pm I, \pm S\} = \langle S \rangle$$

□

Exercise 2.5. Determine all elements A of Γ which leave $\rho = e^{2\pi i/3}$ fixed.

Solution. Select some $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. A fixes ρ exactly when $a\rho + b = (c\rho + d)\rho = c\rho^2 + d\rho$. note that $\rho^2 = -1 - \rho$, which means that $a\rho + b = (d - c)\rho - c$, and so,

$$
\begin{aligned}
b &= -c \\
a &= d - c \\
&= d + b
\end{aligned}
$$

And so,

$$
\begin{aligned}
c &= -b \\
d &= a - b
\end{aligned}
$$

Then,

$$
\begin{aligned}
1 &= ad - bc \\
&= a(a - b) + b^2 \\
&= a^2 - ab + b^2 \\
&= (a - b/2)^2 + (3/4)b^2
\end{aligned}
$$

This implies that b must be 0, 1, or -1. This gives six possibilities for $(a, b) : \pm(1, 0), \pm(0, 1), \pm(1, 1)$. Then,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a-b \end{pmatrix}$$

has 6 values. These values are the powers of ST, and since ST fixes ρ, its powers fix ρ. That is,

$$\mathrm{Stab}_\rho = \langle ST \rangle$$

□

Exercise 2.6. If x and y are subjected to unimodular transformations, say,

$$\begin{aligned} x &= \alpha x' + \beta y' \\ y &= \gamma x' + \delta y' \end{aligned}$$

where

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \Gamma$$

prove that $Q(x, y)$ gets transforms to a quadratic form $Q_1(x', y')$ having the same discriminant.

Solution. We have the following transformation of the form $f(x, y)$:

$$f'(x', y') = a'x'^2 + b'x'y' + cc'y'^2$$

where

$$\begin{aligned} a' &= \alpha a^2 + b\alpha\gamma + c\gamma^2 \\ b' &= b(\alpha\delta + \beta\gamma) + 2(a\alpha\beta + c\gamma\delta) \\ c' &= \alpha\beta^2 + b\beta\delta + c\delta^2 \end{aligned}$$

Which implies that,

$$\Delta' = b'^2 = 4a'c' = (\alpha\delta - \beta\gamma)^2\Delta$$

Clearly $f'(x', y')$ is a qudartic form, and the discriminant is unchanged up to a constant factor. □

Exercise 2.11. Prove that $\Gamma(n)$ is a normal sugroup of $\Gamma = SL_2(\mathbb{Z})$

Solution. We can give a direct proof. First, note that since elements of $SL_2(\mathbb{Z})$ have determinant 1 we have the following inverse matrices,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

We give the following computation,

$$\begin{aligned}
\left(\begin{array}{cc} a & b \\ c & d \end{array}\right)^{-1}\left(\begin{array}{cc} x & y \\ z & w \end{array}\right)\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) &= \left(\begin{array}{cc} d & -b \\ -c & a \end{array}\right)\left(\begin{array}{cc} x & y \\ z & w \end{array}\right)\left(\begin{array}{cc} a & b \\ c & d \end{array}\right) \\
&= \left(\begin{array}{cc} d & -b \\ -c & d \end{array}\right)\left(\begin{array}{cc} ax+cy & bx+dy \\ az+cw & bz+dw \end{array}\right) \\
&= \left(\begin{array}{cc} (ax+cy)d-(az+cw)b & (xb+dy)d-(zb+dw)b \\ (az+cw)a-(ax+cy)c & (zb+dw)a-(xb+dy)c \end{array}\right).
\end{aligned}$$

Then, working mod N, if $x = w = 1$ and $y = z = 0$ we have,

$$\begin{aligned}
(ax+cy)d-(az+cw)b &\equiv ad-cb \equiv 1 \pmod N \\
(xb+dy)d-(zb+dw)b &\equiv bd-db \equiv 0 \pmod N \\
(az+cw)a-(ax+cy)c &\equiv ca-ac \equiv 0 \pmod N \\
(zb+dw)a-(xb+dy)c &\equiv da-bc \equiv 1 \pmod N
\end{aligned}$$

Which is in $\Gamma(N)$. One could also prove that $\Gamma(N)$ is the kernal of the natural homomorphism $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$. □

Exercise 2.12. The quotient group $\Gamma/\Gamma(N)$ is finite.

Solution. Note that the ring homomorphism $\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$ given by $x \to [x]$ induces the following group homomorphism:

$$\phi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$$

with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \to \begin{pmatrix} [a] & [b] \\ [c] & [d] \end{pmatrix}$.

Invoking isomorphism theorems give us,

$$SL_2(\mathbb{Z})/\ker(\phi) \cong \operatorname{im}(\phi) \leq SL_2(\mathbb{Z}/N/Z)$$

The kernal of this map is given by,

$$\ker(\phi) = \{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a = d = 1 \mod N, b = c = 0 \mod N\} = \Gamma(N)$$

The image is a subgroup of $SL_2(\mathbb{Z}/N\mathbb{Z})$, which is finite, and so the quotient is finite. □

Exercise 2.13. The index of $\Gamma(N)$ in Γ is the number of equivalence classes of matrices modulo n.

Solution. This question is equivalent to determining that the map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/n\mathbb{Z})$ is onto.

Lemma. We will show that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$ then c and d are coprime mod N.
Suppose there is some $x \in \mathbb{Z}/N\mathbb{Z}$ such that $xc = xd = 0$. Then, $x = x(ad - bc) = a(xd) - b(xc) = 0$, which implies that $x = 0$. That is, c and d are coprime mod N.

Lemma. For any pair (c, d) that is coprime mod N there exists c' and d' in $\mathbb{Z}$ such that $c' = c \mod N$ and $d' - d \mod N$ and $gcd(c', d') = 1$.
Lift c and d to $\mathbb{Z}$ and suppose WLOG that $d \neq 0$. Then, let p be a prime which divides d. If $p|d$, then p cannot divide both c and N. For each prime we can construct λ_p such that $c + \lambda_p N$ is not divisible by p. If p does not divide c then $\lambda_p = 0$. If $p|c$ then $\lambda_p = 0$. Now, by CRT, select $\lambda \in \mathbb{Z}$ such that $\lambda = \lambda_p \mod p$ fpr each prime which divides d. No prime can divide both $c + \lambda N$ and d, which implies that $(c + \lambda N, d)$ is a coprime pair and that $(c + \lambda N, d) = (c, d) \mod N$.

Returning to our original claim, we select $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}/N/Z)$. The previous lemma shows that we can lift c and d to a pair of coprime integers, and we can select arbitrary lifts of a and b such that we have the matric $\begin{pmatrix} a + \lambda N & b + \mu N \\ c & d \end{pmatrix}$. This matrix has determinant $(ad - bc) + N(\lambda d - \mu c)$. We can always find λ and μ such that this determinant is 1, and so we have a lifting from the original matrix to $SL_2(\mathbb{Z})$. $\square$

Exercise 2.17. If a, b, n are integers with $n \geq 1$ and $(a, b, n) = 1$ the congruence

$$ax - by = 1(\mod n)$$

has exactly n solutions, distinct mod n. Here, a solution is an ordered pair (x, y) of integers.

Solution. Begin by letting the $\gcd(a, n) = d$. It follows that $\gcd(b, d) = 1$, and thus the equation

$$by + 1 = 0 \mod d$$

has a unique solution. We can lift this to mod n where it has n/d many solutions. For each such value of y,

$$\left(\frac{a}{d}\right) x = \frac{(by + 1)}{d} \mod \frac{n}{d}$$

has a unique solution mod n/d. This lifts to d solutions mod n. This means there are, in total, $(n/d) \cdot d = n$ many solutions. $\square$

Chapter 3

Exercise 3.1. If $\tau \in H$ prove that

$$G_2(\tau) = 2\zeta(2) + \sum_{n=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} \frac{1}{(m + n\tau)^2}$$

where $n \neq 0$.

Solution. Beginning with the definition of Eisenstein series one can break off the terms where $n = 0$ and find the following,

$$G_k(\tau) = \sum_{(m,n)\neq(0,0)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^k} = 2\sum_{n\geq 1}\frac{1}{n^k} + 2\sum_{n\geq 1}\left(\sum_{m\in\mathbb{Z}}\frac{1}{(m\tau+n)^k}\right)$$

Specializing to $G_2(\tau)$ gives the desired identity. □

Exercise 3.3. In the gamma function integral $\Gamma(z) = \int_0^\infty t^{z-1}dt$ make the change of variable $t = \alpha u$, where $\alpha > 0$, to obtain the formula

$$\alpha^{-z}\Gamma(z) = \int_0^\infty e^{-\alpha u}u^{z-1}du$$

Solution. The Gamma function is fined by the following integral formula

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}dt$$

By definition the laplace transform is as follows

$$L(t^{z-1}; s) = \int_0^\infty e^{-\alpha t}t^{z-1}dt$$

Make the change of variable $\tau = \alpha t$ where $\alpha > 0$. Then the laplace integral becomes,

$$\begin{aligned}\int_0^\infty e^{-st}t^{z-1}dt &= \int_0^\infty \left(\frac{\tau}{s}\right)^{z-1} e^{-\tau}\frac{d\tau}{s}\\ &= \frac{1}{s^z}\int_0^\infty \tau^{z-1}e^{-\tau}\\ &= \frac{\Gamma(z)}{s^z}d\tau\end{aligned}$$

And so $L(t^{z-1}; s) = \frac{\Gamma(z)}{s^z}$. Both are analytic on $Re(s) > 0$, and we know that two functions which agree on non-discrete subsets of a connected region are equal. □

Exercise 3.6. Derive the reciprocity law for the Dedekind sum $s(h, k)$ from the following transformation formula for $\log\eta(\tau)$

$$\log\eta\left(\frac{a\tau+b}{c\tau+d}\right) = \log\eta(\tau) + \frac{1}{2}\log\left(\frac{a\tau+d}{i}\right) + \pi i\frac{a+d}{12c} - \pi i s(d,c)$$

Solution. Consider

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix} b & -a\\ d & -c\end{pmatrix}$$

With $c > 0$ and $d > 0$, $\tau' = -1/\tau$ and $\tau'' = (a\tau' + b)/(c\tau' + d)$ we arrive at the following formula,

$$\log \eta(\tau') = \log \eta(\tau) + \frac{1}{2} \log \frac{\tau}{i}$$

Now we have the following,

$$\begin{aligned}
\log \eta(\tau'') &= \log \eta(tau') + \frac{1}{2} \log \left(\frac{c\tau' + d}{i} \right) + \pi i \frac{a+d}{12c} - \pi i s(d, c) \\
&= \log \eta(\tau) + \frac{1}{2} \log \frac{\tau}{i} + \frac{1}{2} \log \left(\frac{-c/\tau + d}{i} \right) + \pi i \frac{a+d}{12c} - \pi i s(d, c) \\
&= \log \eta(\tau) + \frac{1}{2} \log (c - d\tau) + \pi i \frac{a+d}{12c} - \pi i s(d, c)
\end{aligned}$$

If we let $\tau' = (b\tau - a)/(d\tau - c)$ then we arrive at another formula for $\log \eta(\tau'')$:

$$\log \eta(\tau'') = \log \eta(\tau) + \frac{1}{2} \log \left(\frac{d\tau - c}{i} \right) + \pi i \frac{b-c}{12d} - \pi i s(-c, d)$$

Equating these two expressions gives the following,

$$\pi i (s(d, c) - s(-c, d)) = \frac{\pi i}{12} \left(\frac{a+d}{c} - \frac{b-c}{d} \right) + \frac{1}{2} \log \left(\frac{c - d\tau}{d\tau - c} i \right)$$

Equivalently,

$$s(d, c) - s(-c, d) = \frac{1}{12} \left(\frac{d}{c} + \frac{c}{d} + \frac{ad - bc}{dc} \right) + \frac{1}{2\pi i} \log(-i)$$

It is the case that $s(-c, d) = -s(c, d)$ and $ad - bc = 1$, which means we have the final equality,

$$s(d, c) + s(c, d) = -\frac{1}{4} + \frac{1}{12} \left(\frac{d}{c} + \frac{1}{cd} + \frac{c}{d} \right)$$

Which is the reciprocity formula we were looking for. □

Exercise 3.9. Define Dedekind sums as follows

$$s(h, k) = \sum_{r \mod k} \left(\left(\frac{r}{k} \right) \right) \left(\left(\frac{hr}{k} \right) \right)$$

From this definition prove that

$$s(qh, qk) = s(h, k)$$

for $q > 0$

Solution. First, recall two properties of the symbol $((x))$. If $x_1 = x_2 \mod 1$ then

$$((x_1)) = ((x_2))$$

Also,

$$\sum_{\mu \mod k} \left(\left(\frac{\mu + x}{k}\right)\right) = ((x))$$

Now, following the definition given in the exercise statement and making use of the above properties we have,

$$\begin{aligned}
s(qh, qk) &= \sum_{\mu=1}^{qk} \left(\left(\frac{\mu}{qk}\right)\right)\left(\left(\frac{qk\mu}{qk}\right)\right) \\
&= \sum_{v=0}^{q-1}\sum_{p=1}^{k} \left(\left(\frac{vk+p}{qk}\right)\right)\left(\left(\frac{h(vk+p)}{k}\right)\right) \\
&= \sum_{p=1}^{k} \left(\left(\frac{hp}{k}\right)\right)\sum_{v=0}^{q-1}\left(\left(\frac{p}{qk} + \frac{v}{q}\right)\right) \\
&= \sum_{p=1}^{k} \left(\left(\frac{hp}{k}\right)\right)\left(\left(\frac{p}{k}\right)\right) \\
&= s(h, k)
\end{aligned}$$

□

Exercise 3.10. If p is prime prove that

$$(p+1)s(h,k) = s(ph,k) + \sum_{m=0}^{p-1} s(h+mk, pk)$$

Solution. As in 3.9, recall that

$$\sum_{\mu mod k} \left(\left(\frac{\mu + x}{k}\right)\right) = ((x))$$

From this we see that

$$\sum_{m=0}^{p-1} \left(\left(y + \frac{\mu m}{p}\right)\right) = \begin{cases} ((py)) \text{ if } p \nmid \mu \\ p((y)) \text{ if } p \nmid \mu \end{cases}$$

Then,

$$\begin{aligned}
s(ph,k) + \sum_{m=0}^{p-1} s(h+mk,pk) &= s(ph,k) + \sum_{m=0}^{p-1}\sum_{\mu=1}^{pk} \left(\left(\frac{\mu}{pk}\right)\right)\left(\left(\frac{(h+mk)\mu}{pk}\right)\right) \\
&= s(ph,k) + \sum_{\mu=1}^{p-1} \left(\left(\frac{\mu}{pk}\right)\right)\sum_{m=0}^{p-1}\left(\left(\frac{h\mu}{pk} + \frac{\mu m}{p}\right)\right) \\
&= s(ph,k) + \sum_{\mu=1}^{pk} \left(\left(\frac{\mu}{pk}\right)\right)\left(\left(\frac{ph\mu}{pk}\right)\right) + \sum_{v=1}^{k}\left(\left(\frac{pv}{pk}\right)\right)\left(p\left(\left(\frac{phv}{pk}\right)\right) - \left(\left(\frac{p^2vh}{pk}\right)\right)\right)
\end{aligned}$$

Which completes the proof. □

Chapter 4

Exercise 4.3. Let p be a prime and let k be an integer, $1 \leq k \leq p-1$. Show that there exists an integer h such that

$$\tau^{12}\Delta\left(\frac{\tau+h}{p}\right) = \Delta\left(\frac{k\tau-1}{p\tau}\right)$$

and that h runs through a reduced residue system mod p with k.

Solution. First, recall that Δ is a modular form of weight 12, meaning it satisfies the relation

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12}\Delta(z)$$

with a, b, c, d integers and $ad-bc=1$. Now, for $1 \leq k \leq p-1$, we have that k and p are coprime. From Bezout's identity this implies the existence of $h, y \in \mathbb{Z}$ where h runs through $1, ..., p-1$ such that

$$kh + py = -1$$

Now select the following variables

$$\begin{aligned}
\tau' &= \frac{\tau+h}{p} \\
a &= k \\
b &= m \\
c &= p \\
d &= -h
\end{aligned}$$

These values satisfy

$$ad - bc = 1$$

And so,

$$\frac{a\tau'+b}{c\tau'+d} = \frac{a\tau+b}{\tau} = \frac{z\tau+ah+bp}{p\tau} = \frac{k\tau-1}{p\tau}$$

Now, using the transformation law stated at the beginning,

$$\Delta\left(\frac{k\tau-1}{p\tau}\right) = \Delta\left(\frac{a\tau'+b}{c\tau'+d}\right) = (c\tau'+d)^{12}\Delta(\tau') = \tau^{12}\Delta\left(\frac{\tau+h}{p}\right)$$

$\square$

Exercise 4.4. If p is prime, define

$$F_p(\tau) = p^{12}\Delta(p\tau) + \sum_{k=0}^{p-1}\Delta\left(\frac{\tau+k}{p}\right)$$

Prove the following transformation laws

$$F_p(\tau + 1) = F_p(\tau)$$
$$F_p\left(\frac{-1}{\tau}\right) = \tau^{12} F_p(\tau)$$

Solution. We begin by proving the first transformation law. First, recall that since Δ is a cusp form of weight 12 we have two properties. First of all,

$$\Delta(p\tau + p) = \Delta(p\tau)$$

And secondly,

$$\Delta\left(\frac{\tau + p}{p}\right) = \Delta\left(\frac{\tau}{p} + 1\right) = \Delta\left(\frac{\tau}{p}\right)$$

These identities will be used in conjunction with some straightforward algebriac manipulation to obtain the desired result.

$$\begin{aligned}
F_p(\tau + 1) &= p^{12}\Delta(p(\tau + 1)) + \sum_{k=0}^{p-1} \Delta\left(\frac{(\tau + 1) + k}{p}\right) \\
&= p^{12}\Delta(p\tau + p) + \sum_{k=0}^{p-1} \Delta\left(\frac{(\tau + 1) + k}{p}\right) \\
&= p^{12}\Delta(p\tau) + \sum_{k=0}^{p-2} \Delta\left(\frac{\tau + (k + 1)}{p}\right) + \Delta\left(\frac{(\tau + 1) + (p - 1)}{p}\right) \\
&= p^{12}\Delta(p\tau) + \sum_{k=1}^{p-1} \Delta\left(\frac{\tau + k}{p}\right) + \Delta\left(\frac{\tau + p}{p}\right) \\
&= p^{12}\Delta(p\tau) + \sum_{k=1}^{p-1} \Delta\left(\frac{\tau + k}{p}\right) + \Delta\left(\frac{\tau}{p}\right) \\
&= p^{12}\Delta(p\tau) + \sum_{k=0}^{p-1} \Delta\left(\frac{\tau + k}{p}\right) \\
&= F_p(\tau)
\end{aligned}$$

Which is the desired result. Now we will move to proving the second transformation law.

We will perform some algebraic maniuplation to get the question into a desirable form.

From there, we will be able to leverage the result from exercise 4.3 to finish the problem.

$$\begin{aligned}
F_p\left(-\frac{1}{\tau}\right) &= p^{12}\Delta\left(-\frac{p}{\tau}\right) + \sum_{k=0}^{p-1}\Delta\left(\frac{(-1/\tau)+k}{p}\right) \\
&= p^{12}\Delta\left(-\frac{1}{\frac{\tau}{p}}\right) + \sum_{k=0}^{p-1}\Delta\left(\frac{\tau k - 1}{\tau p}\right) \\
&= p^{12}\left(\frac{\tau^{12}}{p^{12}}\right)\Delta\left(\frac{\tau}{p}\right) + \sum_{k=0}^{p-1}\Delta\left(\frac{\tau k - 1}{\tau p}\right) \\
&= \tau^{12}\Delta\left(\frac{\tau}{p}\right) + \sum_{k=0}^{p-1}\Delta\left(\frac{\tau k - 1}{\tau p}\right) \\
&= \tau^{12}p^{12}\Delta(\tau) + \sum_{k=0}^{p-1}\Delta\left(\frac{\tau k - 1}{\tau p}\right)
\end{aligned}$$

Now, recall the result from exercise 4.3

$$\tau^{12}\Delta\left(\frac{\tau+h}{p}\right) = \Delta\left(\frac{k\tau-1}{p\tau}\right)$$

This tells us that

$$F_p\left(-\frac{1}{\tau}\right) = \tau^{12}\left(p^{12}\Delta(\tau) + \sum_{k=0}^{p-1}\Delta\left(\frac{\tau+k}{p}\right)\right) = \tau^{12}F_p(\tau)$$

Which completes the proof. $\square$

Exercise 4.5. Prove that $F_p(\tau) = \tau(p)\Delta(\tau)$ where $\tau(p)$ is Ramanujan's function.

Solution. Define the following function

$$f(\tau) = \frac{F_p(\tau)}{\Delta(\tau)}$$

Note that $f(\tau)$ inherits the transformation laws from $F_p(\tau)$ and $\Delta(\tau)$. That is,

$$\begin{aligned}
f(\tau+1) &= f(\tau) \\
f(-\frac{1}{\tau}) &= f(\tau)
\end{aligned}$$

We can rewrite our original functions in terms of the Ramanujan-Tau function.

$$\Delta(\tau) = \sum_{n=1}^{\infty}\tau(n)q^n$$

And

$$\begin{aligned}
F_p(\tau) &= p^{12}\sum_{n=1}^{\infty}\tau(n)q^{pn} + \sum_{k=0}^{p-1}\sum_{n=1}^{\infty}\tau(n)q^{n/p}e^{2\pi ikn/p} \\
&= p^{12}\sum_{n=1}^{\infty}\tau(n)q^{pn} + \sum_{n=1}^{\infty}\tau(n)q^{n/p}\sum_{k=0}^{p-1}e^{2\pi ikn/p} \\
&= p^{12}\sum_{n=1}^{\infty}\tau(n)q^{pn} + p\sum_{n=1}^{\infty}\tau(pn)q^{n}
\end{aligned}$$

It follows that

$$f(z) = p\tau(p) + x_1 q + x_2 q^2 ...$$

and that $f(z)$ is a weakly modular function of weight 0 and thus equal to $p\tau(p)$. This gives that

$$F_p(\tau) = p\tau(p)\Delta(\tau)$$

which is the identity we were looking for up to a constant factor. □

Exercise 4.6. Deduce the following formulas

$$\begin{aligned}
\tau(p^{n+1}) &= \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1}) \text{ for } n \geq 1 \\
\tau(p^{\alpha}n) &= \tau(p)\tau(p^{\alpha-1}n) - p^{11}\tau(p^{\alpha-1}n) \text{ for } \alpha \geq 2 \text{ and } (n,p) = 1
\end{aligned}$$

Solution. The result of the previous exercise gives the following identity

$$\tau(p)\sum_{n=1}^{\infty}\tau(n)q^n = p^{11}\sum_{n=1}^{\infty}\tau(n)q^{pn} + \sum_{n=1}^{\infty}\tau(pn)q^n$$

Taking the $n'th$ coefficient of q in the above expression gives

$$\tau(p^{\alpha}n) = \tau(p)\tau(p^{\alpha-1}n) - p^{11}\tau(p^{\alpha-2}n)$$

Letting $n = 1$ we get

$$\tau(p^{\alpha}) = \tau(p)\tau(p^{\alpha-1}) - p^{11}\tau(p^{\alpha-2})$$

□

Exercise 4.7. If α is an integer, $\alpha \geq 0$ and if $(n.p) = 1$ let

$$g(\alpha) = \tau(p^{\alpha}n) - \tau(p^{\alpha})\tau(n)$$

deduce that $g(\alpha) = 0$ for all α.

Solution. If $\alpha = 0$ then the identity holds trivially. Equating the $n'th$ coefficient of the identity from exercise 4.6 gives

$$\tau(pn) = \tau(p)\tau(n)$$

We can then define a recursion on $\alpha \in \mathbb{Z}$ using

$$g(\alpha) = \tau(p^\alpha n) - \tau(p^\alpha)\tau(n)$$

We have that $g_0 = g_1 = 0$, and so we can induct and show that $g = 0$ for all α. It follows that

$$\tau(p^k n) = \tau(p^k)\tau(n)$$

This is equivalent to showing the multiplicative property of the tau function. It follows that for any $m, n \in \mathbb{Z}$ such that $(m, n) = 1$ we have

$$\tau(mn) = \tau(m)\tau(n)$$

□

Chapter 5

Exercise 5.1. Two reduced fractions a/b and c/d are said to be similarly ordered if $(c - a)(c - d) \geq 0$. Let $a_1/b_1 < a_2/b_2 < \dots$ denote the Farey fractions in F_n.
a. Prove that any two neighbors a_i/b_i and a_{i+1}/b_{i+1} are similarly ordered.
b. Prove that any two second neighbors a_i/b_i and a_{i+2}/b_{i+2} are similarly ordered.

Solution.
a. Consider consecutive Farey fractions, a/b and c/d, and recall the following identities: $a/b < a_{i+1}/b_{i+1}$ and $a_{i+1}b_i - a_i b_{i+1} = 1$. Suppose for the sake of contradiction that $(a_{i+1} - a_i)(b_{i+1} - b_i) < 0$. Then, since $a/b < a_{i+1}/b_{i+1}$, we must have

$$\begin{aligned} a_{i+1} &\geq a_i + 1 \\ b_{i+1} &\leq b_i - 1 \end{aligned}$$

It follows that

$$\begin{aligned} a_{i+1}b_i - a_i b_{i+1} &\geq b_i(a_i + 1) - a_i(b_i - 1) \\ &\geq a_i + b_i \\ &> 1 \end{aligned}$$

which is a contradiction.

b. Consider two Farey fractions, a_i/b_i and a_{i+2}/b_{i+2}. We will handle two cases: $b_{i+2} \geq b_i$ and $b_{i+2} < b_i$.

First, if $b_{i+2} \geq b_i$, then $a_{i+2} > b_{i+2}a_i/b_i \geq a_i$. It follows that the fractions are similarly ordered.

Then, if $b_{i+1} < b_i$, the goal is to show that $a_{i+2} \leq a_i$. Suppose that is not the case. Then,

$$\begin{aligned}\frac{a_{i+2}}{b_{i+2}} &> \frac{a_{i+2}-1}{b_{i+2}} \\ &\geq \frac{a_i}{b_{i+2}} \\ &\geq \frac{a_i}{b_i - 1} \\ &> \frac{a_i}{b_i}\end{aligned}$$

This forces $a_{i+2} = a_i + 1$ and $b_{i+2} = b_i - 1$. We also have that

$$\frac{a_{i+1}}{b_{i+1}} = \frac{a_i + a_{i+2}}{b_i + b_{i+2}}$$

From here, we know that $a_i/b_i - 1 = 2a_i + 1/2b_i - 1$. This implies that $2b_i - 1/b_i - 1 = 2a_i + 1/a_1$, which in turn tells us that $a_1 = b_1 - 1$. Finally, we have the following

$$\begin{aligned}\frac{a_{i+2}}{b_{i+2}} &= \frac{a_i + 1}{b_i - 1} \\ &= \frac{b_i}{b_i - 1} \\ &> 1\end{aligned}$$

This is a contradiction, and so the two fractions must be similarly ordered. $\square$

Exercise 5.2. If a, b, c, d are positive integers such that $a/b < c/d$ and if λ and μ are positive integers prove that the fraction

$$\theta = \frac{\lambda a + \mu c}{\lambda b + \mu d}$$

lies between a/b and c/d, a

Solution. Consider fractions $a/b < c/d$. Multiplying through by $bd\mu$ gives

$$ad\mu < bc\mu$$

Then, add $ab\lambda$ to both sides to receive

$$a(d\mu + b\lambda) < b(c\mu + a\lambda)$$

Then divide through by $b(d\mu + b\lambda)$. The result is that

$$\frac{a}{b} < \frac{a\lambda + c\mu}{b\lambda + d\mu}$$

For the other inequality, start with

$$ad\mu < bc\mu$$

and add $cd\lambda$ to both sides

$$d(a\mu + c\lambda) < c(b\mu + c\lambda)$$

Then divide through by $d(b\mu + c\lambda)$ to get

$$\frac{a\mu + c\lambda}{b\mu + c\lambda} < \frac{c}{d}$$

□

Exercise 5.3. If $bc - ad = 1$ and $n > \max(b, d)$, prove that the terms of the Farey sequence F_n between a/b and c/d are the fractions of the form $\lambda a + \mu c)/(\lambda b + \mu d)$ for which λ and μ are positive relatively prime integers with $\lambda b + \mu d \leq n$.

Solution. Consider the fractions $c/d < a'/b' < a/b$ with positive denominators and $ad - bc = 1$, and a' and b' coprime. Then consider the system of equations

$$\begin{aligned} La + Mc &= a' \\ Lb + Md &= b' \end{aligned}$$

This comes with the following unique solution for L and M

$$\begin{aligned} L &= a'd - b'c \\ M &= ab' - a'b \end{aligned}$$

Now, we have that L and M are greater than 0 if and only if $a'/b' > c/d$ and $a/b > a'/b'$ respectively. If there is a common divisor of L and M, then that common divisor divides both a' and b', and so it must be equal to 1. □

Exercise 5.6. Assign a weight $f(x, y)$ to each lattice point (x, y) and let S_n be the sum of all the weights in T_n,

$$S_n = \sum_{(x,y) \in T_n} f(x, y)$$

(a) By comparing the regions T_r and T_{r-1} for $r \geq 2$ show that

$$S_2 - S_{r-1} = f(r, r) + \sum_{k=1}^{r-1} \{f(k, r) + f(r, k)\} - \sum_{k=1}^{r} f(k, r - k)$$

and deduce that

$$S_n = \sum_{r=1}^{n} f(r, r) + \sum_{r=2}^{n} \sum_{k=1}^{r-1} \{f(k, r) + f(r, k)\} - \sum_{r=2}^{n} \sum_{k=1}^{r} f(k, r - k).$$

Solution. Begin by noting that T_n contains all coprime pairs (x, y) contained in the region bounded by the following lines

$$
\begin{aligned}
x + y &= r + 1 \\
x &= r \\
y &= r
\end{aligned}
$$

including those pairs which fall on one of these lines. It follows that the points of T_n which are not found in T_{n-1} are the coprime pairs (x, y) on the line segments $x = r$, $o \leq y \leq r$ and $y = r$, $0 \leq x \leq r$. Likewise, the points of T_{n-1} which are not in T_n are the pairs on the line segment $x + y = r$, $0 \leq x,\ y \leq r$. This gives the desired identity

$$S_2 - S_{r-1} = f(r, r) + \sum_{k=1}^{r-1} \{f(k, r) + f(r, k)\} - \sum_{k=1}^{r} f(k, r - k)$$

The second result follows from summing over r. □

Exercise 5.7. Let

$$S_n = \sum_{(b,d) \in T_n} \frac{1}{bd(b + d)}$$

(a) Show that $1/(2n - 1) \leq S_n \leq 1/(n + 1)$
(b) Choose $f(x, y) = 1/xy(x + y))$ and show that

$$S_n = \frac{3}{2} - 2 \sum_{r=1}^{n} \sum_{k=1,(k,r)=1}^{r} \frac{1}{r^2(r + k)}$$

Solution. (a) Let $f(b, d) = 1/bd(b + d)$. Then we have the following identity,

$$\sum_{(b,d) \in T_n} \frac{1}{bd} = \sum_{(b,d) \in T_n} \left(\frac{c}{d} - \frac{a}{b} \right) = 1$$

and $n + 1 \leq b + d \leq 2n - 1$. From here the result follows:

$$\frac{1}{2n - 1} \leq S_n \leq \frac{1}{n + 1}$$

(b) Continuing with this choice of f we are able to invoke the result from problem 6 to obtain the following

$$
\begin{aligned}
S_r - S_{r-1} &= \sum_{1 \leq k \leq r, (k,r)=1} \left(\frac{1}{kr(k + r)} + \frac{1}{rk(r + k)} - \frac{1}{k(r - k)r} \right) \\
&= \sum_{1 \leq k \leq r, (k,r)=1} \frac{1}{r^2} \left(\frac{1}{k} - \frac{2}{r + k} - \frac{1}{r - k} \right) \\
&= -2 \sum_{1 \leq k \leq r, (k,r)=1} \frac{1}{r^2(r + k)}
\end{aligned}
$$

We have that $f(1,1) = 1/2$ and so

$$S_n = \frac{3}{2} - 2\sum_{r=1}^{n} \sum_{k=1,(k,r)=1}^{r} \frac{1}{r^2(r+k)}$$

$\square$

Exercise 5.8. Exercise 7(a) shows that $S_n \to 0$ as $n \to \infty$. This exercise outlines a proof of the asymptotic formula

$$S_n = \frac{12\log 2}{\pi^2 n} + O\left(\frac{\log n}{n^2}\right)$$

Let

$$A_r = \sum_{k=1,(k,r)=1}^{r} \frac{1}{r^2(r+k)} = \sum_{k=1}^{r} \sum_{d|(r,k)} \frac{\mu(d)}{r^2(r+k)}$$

(a) Show that

$$S_r = \sum_{d|r} \sum_{h=1}^{d} \frac{d\mu(r/d)}{r^3(h+d)}$$

and deduce that

$$A_r = \log 2\frac{\phi(r)}{r^3} + O\left(\frac{1}{r^3}\sum_{d|r}|\mu(d)|\right)$$

(b) Show that $\sum_{r=1}^{n}\sum_{d|r}|\mu(d)| = O(n\log n)$ and deduce that

$$\sum_{r>n} \frac{1}{r^3}\sum_{d|r}|\mu(d)| = O\left(\frac{\log n}{n^2}\right)$$

(c) Use the formula $\sum_{r\leq n}\phi(r) = 3n^2/\pi^2 + O(n\log n)$ to deduce that

$$\sum_{r>n} \frac{\phi(r)}{r^3} = \frac{6}{n\pi^2} + O\left(\frac{\log n}{n^2}\right)$$

(d) Use (a), (b), and (c) to deduce

$$S_n = \frac{12\log 2}{\pi^2 n} + O\left(\frac{\log n}{n^2}\right)$$

Solution. (a) recall that

$$A_r = \sum_{k=1,(k,r)=1}^{r} \frac{1}{r^2(r+k)} = \sum_{k=1}^{r} \sum_{d|(r,k)} \frac{\mu(d)}{r^2(r+k)}$$

Then, substitute hd for k to find

$$A_r = \sum_{k=1,(k,r)=1}^{r} \frac{1}{r^2(r+k)} = \sum_{d|r} \sum_{1 \le h \le r/d} \frac{\mu(d)}{r^2(r+hd)}$$

Then, replace d by r/d to get

$$A_r = \sum_{k=1,(k,r)=1}^{r} \frac{1}{r^2(r+k)} = \sum_{d|r} \sum_{1 \le h \le d} \frac{\mu(r/d)}{r^3(h+d)}$$

Now,

$$\sum_{h=1}^{d} \frac{1}{h+d} = \log 2 + O\left(\frac{1}{d}\right)$$

and so

$$\begin{aligned} A_r &= \sum_{d|r} \frac{d\mu(r/d)}{r^3} \left(\log 2 + O\left(\frac{1}{d}\right)\right) \\ &= \log 2 \frac{\phi(r)}{r^3} + O\left(\frac{1}{r^3} \sum_{d|r} |\mu(d)|\right) \end{aligned}$$

(b) For the next part, we have

$$\begin{aligned} \sum_{r=1}^{n} \sum_{d|r} |\mu(d)| &= \sum_{r=1}^{n} \sum_{s=1}^{\infty} |\mu(r)| \left(\left[\frac{r}{s}\right] - \left[\frac{r-1}{s}\right]\right) \\ &= \sum_{r=1}^{n} |\mu(r)| \left[\frac{n}{r}\right] \\ &= O(n \log n) \end{aligned}$$

Then, upon partial summation, we have

$$\sum_{r>n} \frac{1}{r^3} \sum_{d|r} |\mu(d)| = O\left(\frac{\log n}{n^2}\right)$$

(c) If we have $\sum_{r \le n} \phi(r) = 3n^2/\pi^2 + O(n \log n)$ then

$$\sum_{r>n} \frac{\phi(r)}{r^3} = \frac{6}{n\pi^2} + O\left(\frac{\log n}{n^2}\right)$$

follows from partial summation as well.

(d) The following asymptotic formula is now an immediate consequence

$$S_n = \frac{12 \log 2}{\pi^2 n} + O\left(\frac{\log n}{n^2}\right)$$

□

Chapter 6

Exercise 6.4. If f is α-multiplicative prove that

$$\alpha(n)f(m) = \sum_{d|n} \mu(d) f(mnd) f\left(\frac{n}{d}\right).$$

Solution. First, note that

$$\sum_{d|n} \mu(d) f(mnd) f(\frac{n}{d}) = \sum_{d|n} \mu(d) \left(\sum_{r|(mnd, \frac{n}{d})} \alpha(r) f(\frac{mn^2}{r^2}) \right)$$

Then, since $\frac{n}{d}|mnd$ we have

$$\sum_{d|n} \sum_{r|\frac{n}{d}} \mu(d)\alpha(r) f(\frac{mn^2}{r^2}) = \sum_{r|n} \sum_{d|\frac{n}{r}} \mu(d)\alpha(r) f(\frac{mn^2}{r^2}) = \alpha(n) f(m)$$

□

Exercise 6.7. Let $E_k(\tau) = G_{2k}(\tau)/\zeta(2k)$. If $x = e^{2\pi i\tau}$ computer the Fourier expansion of $E_k(\tau)$ for $k = 4, 6, 8, 10, 12$ and 14.

Solution. Recall the representation of the normalized weight k Eisenstein series in terms of Bernoulli numbers

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \sum \sigma_{k-1} x^n$$

From here simply plug in the values of k and use the relevant Bernoulli number. □

Exercise 6.10. Derive the following identity

$$\tau(n) = \frac{65}{756}\sigma_{11}(n) + \frac{691}{756}\sigma_5(n) - \frac{691}{3}\sum_{m=1}^{n-1} \sigma_5(m)\sigma_5(n-m)$$

and show that this identity implies Ramanujan's congruence

$$\tau(n) \equiv \sigma_{11}(n) \mod 691$$

Solution. Consider the following $q-$expansions

$$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n$$

$$E_6 = 1 + 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$

Note the fact that Δ is a cusp form of weight 12, and the above $q-$expansions are of weight 4 and 6 respectively. We can create two monomials of weight 12, namely E_4^3 and E_6^2. The constant term of Δ vanishes and E_4^3 and E_6^2 both have constant term 1. This means that Δ is proportional to $E_4^3 - E_6^2$. The coefficient of q in Δ is 1, $\tau(1) = 1$, and the coefficient of q in $E_4^3 - E_6^2$ is 1728, which means

$$E_4^3 - E_6^2 = 1728\Delta$$

From here we find that

$$756\tau(n) = 65\sigma_{11}(n) + 691\sigma_5(n) - 174132\sum_{m=1}^{n-1}\sigma_5(m)\sigma_5(n-m)$$

Dividing through by 756 gives the result. Alternatively, we can treat this equation modulo 691 and see that

$$65\tau(n) \equiv 65\sigma_{11}(n) \mod 691$$

and note that since 65 and 691 are coprime we have

$$\tau(n) \equiv \sigma_{11}(n) \mod 691$$

which is the congruence we were after. □

Exercise 6.13. Show that the Dirichlet series associated with the normalized modular form

$$f(\tau) = \frac{(2k-1)!}{2\pi i^{2k}}\zeta(2k) + \sum_{m=1}^{\infty}\sigma_{2k-1}(m)e^{2\pi i m\tau}$$

is $\phi = \zeta(s)\zeta(s+1-2k)$

Solution. Recall the Eisenstein series

$$G_{2k}(\tau) = \sum_{(n,m)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m+n\tau)^{2k}}$$

and its Fourier transform

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)e^{2i\pi n\tau}$$

We can take the mellin transform of $G_{2k}(ix) - 2\zeta(2k)$,

$$\begin{aligned}
F(s) &= \int_0^{\infty} x^{s-1}(G_{2k}(ix) - 2\zeta(k))dx \\
&= 2\frac{(2i\pi)^{2k}}{(2k-1)!}\int_0^{\infty} x^{s-1}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)e^{-2\pi nx}dx \\
&= 2\frac{(2i\pi)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)\int_0^{\infty} x^{s-1}e^{-2\pi nx}dx \\
&= 2\frac{(2i\pi)^{2k}}{(2k-1)!}\Gamma(s)(2\pi)^{-s}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)n^{-s} \\
&= \frac{2(-1)^k}{(2k-1)!}(2i\pi)^{2k-s}\Gamma(s)\zeta(s)\zeta(s-2k+1),
\end{aligned}$$

and we see $\zeta(s)\zeta(s-2k+1)$ fall out. $\square$

Exercise 6.15. Prove the functional equation

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{(s-1)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

from the functional equation

$$\vartheta\left(\frac{-1}{\tau}\right) = (-i\tau)^{1/2}\vartheta(\tau)$$

satisfied by Jacobi's theta function

$$\vartheta(\tau) = 1 + 2\sum_{n=1}^{\infty} e^{\pi i n^2 \tau}$$

Solution. Recall the definition of the gamma function

$$\Gamma(s) = \int_0^\infty t^{s-1}e^{-1}\,\mathrm{d}x$$

and make the change $s \to \frac{s}{2}$ which results in

$$\Gamma\left(\frac{s}{2}\right) = \int_0^\infty t^{\frac{s}{2}-1}e^{-t}\,\mathrm{d}x$$

Now, let $t = \pi n^2 x$ and $\mathrm{d}t = \pi n^2 \mathrm{d}x$. This gives us

$$\begin{aligned}\Gamma\left(\frac{s}{2}\right) &= \int_0^\infty (\pi n^2 x)^{\frac{s}{2}-1}e^{-\pi n^2 x}\pi n^2\,\mathrm{d}x \\ &= \int_0^\infty \pi^{\frac{s}{2}} n^s x^{\frac{s}{2}-1}e^{-\pi n^2 x}\,\mathrm{d}x\end{aligned}$$

Now, we can divide through by $\pi^{\frac{s}{2}}$.

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\frac{1}{n^s} = \int_0^\infty x^{\frac{2}{s}-1}e^{-\pi n^2 x}\,\mathrm{d}x$$

Now we can take the sum over both sides, which will give the zeta function on the left and ultimately connect the right to the Jacobi theta function.

$$\sum_{n=1}^{\infty}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\frac{1}{n^s} = \sum_{n=1}^{\infty}\int_0^\infty x^{\frac{s}{2}-1}e^{-\pi n^2 x}\,\mathrm{d}x$$

Pulling the constants out of the sum gives

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\sum_{n=1}^{\infty}\frac{1}{n^s} = \int_0^\infty x^{\frac{s}{2}-1}\sum_{n=1}^{\infty}e^{-\pi n^2 x}\,\mathrm{d}x$$

Now we see the zeta function in the left-hand side. On the right what we have is the positive branch of the Jacobi theta function. In terms of the theta function,

$$\vartheta(x) = \sum_{n \in \mathbb{Z}} e^{-\pi n^2 x} = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 x} = 1 + 2\psi(x)$$

Making these substitutions gives us,

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \int_0^{\infty} \psi(x) x^{\frac{s}{s}-1} \, \mathrm{d}x$$

We can now use properties of the theta function when integrating. Taking a closer look at the integral on the right hand side we can split it into two parts,

$$\int_0^{\infty} \psi(x) x^{\frac{s}{2}-1} \, \mathrm{d}x = \int_0^{1} \psi(x) x^{\frac{s}{2}-1} \, \mathrm{d}x + \int_1^{\infty} \psi(x) x^{\frac{s}{2}-1} \, \mathrm{d}x$$

Recall the following expression regarding the theta function

$$\vartheta(x) = \frac{1}{\sqrt{x}} \vartheta\left(\frac{1}{x}\right)$$

Alternatively,

$$2\psi(x) + 1 = \frac{1}{\sqrt{x}} \left(2\psi\left(\frac{1}{x}\right) + 1\right)$$

Isolating $\psi(x)$ on the left results in

$$\psi(x) = \frac{1}{\sqrt{x}} \psi\left(\frac{1}{x}\right) + \frac{1}{2\sqrt{x}} - \frac{1}{2}$$

Substituting this back into our integral gives us

$$\int_0^1 x^{\frac{s}{2}-1} \psi(x) \, \mathrm{d}x = \int_0^1 x^{\frac{s}{2}-1} \left(\frac{1}{\sqrt{x}} \psi\left(\frac{1}{x}\right) + \frac{1}{2\sqrt{x}} - \frac{1}{2}\right) \mathrm{d}x$$

Multiplying through by $x^{\frac{s}{2}-1}$ results in

$$\int_0^1 \left[x^{\frac{s}{2}-\frac{3}{2}} \psi\left(\frac{1}{x}\right) + \frac{1}{2}\left(x^{\frac{s}{2}-\frac{3}{2}} - x^{\frac{s}{2}-1}\right)\right] \mathrm{d}x$$

We can split this integral and compute the simpler half

$$\int_0^1 x^{\frac{s}{2}-\frac{3}{2}} \psi\left(\frac{1}{x}\right) \mathrm{d}x + \frac{1}{2} \int_0^1 \left(x^{\frac{s}{2}-\frac{3}{2}} - x^{\frac{s}{2}-1}\right) \mathrm{d}x = \int_0^1 x^{\frac{s}{2}-\frac{3}{2}} \psi\left(\frac{1}{x}\right) \mathrm{d}x + \frac{1}{s(s-1)}$$

Now let $x = \frac{1}{u}$, $\mathrm{d}x = -\frac{1}{u^2}\mathrm{d}u$, and adjust the boundaries appropriately.

$$\int_{\infty}^1 \left(\frac{1}{u}\right)^{\frac{s}{2}-\frac{3}{2}} \psi(u) \left(-\frac{\mathrm{d}u}{u^2}\right) + \frac{1}{s(s-1)}$$

We can now return to our earlier integral, making sure to fix the boundaries as needed.

$$\int_0^\infty x^{\frac{s}{2}-1}\psi(x)\,\mathrm{d}x = \int_1^\infty x^{\frac{s}{2}-1}\psi(x)\,\mathrm{d}x + \int_1^\infty x^{-\frac{s}{2}-\frac{1}{2}}\psi(x)\,\mathrm{d}x + \frac{1}{s(s-1)}$$

Bringing our integrals together,

$$\int_0^\infty x^{\frac{s}{2}-1}\psi(x)\,\mathrm{d}x = \int_1^\infty \left(x^{\frac{s}{2}-1} + x^{-\frac{s}{2}-\frac{1}{2}}\right)\psi(x)\,\mathrm{d}x + \frac{1}{s(s-1)}$$

Recall the expression from earlier,

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_0^\infty x^{\frac{s}{2}-1}\psi(x)\,\mathrm{d}x,$$

and make the natural substitution, with a minor adjustment.

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \int_1^\infty \left(x^{\frac{s}{2}} + x^{\left(\frac{1-s}{2}\right)}\right)\frac{\psi(x)}{x}\,\mathrm{d}x - \frac{1}{s(s-1)}$$

If we let $s = 1 - s$ the integral does not change, which implies the Riemann functional equation.

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{\frac{s-1}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

$\square$

Chapter 7

Exercise 7.1. Given n real numbers $x_1, ..., x_n$ and given an integer $n \geq 1$, there exist integers $h_1, ..., h_n$ and k, with $1 \leq k \leq n^m$, such that

$$|kx_i - h_i| < \frac{1}{n} \text{ for } i = 1, 2, ..., m$$

Solution. Consider the fractional parts of $n^m + 1$ many vectors in the unit cube $[0,1)^m$: $(\{kx_1\}, ..., \{kx_m\}]$ for $k = 0, ..., n^m$. Divide the unit cube into n^m equal subcubes and note that since there are $n^m + 1$ many vectors we can apply the pigeonhole principle. That is, there are two integers $0 < k_v < k_w < n^m$ such that $\{k_v x_i\}$ and $\{k_w x_i\}$ belong to the same subcube. This implies that, for integer h_i,

$$|(k_w - k_v)x_i - h_i| < \frac{1}{n}$$

Setting $k = (k_w - k_v)$ gives the result.

$$|kx_i - h_i| < \frac{1}{n}$$

$\square$

Exercise 7.2. Given n real numbers $x_1, ..., x_n$ prove that there exist integers $h_1, ..., h_n$ and $k > 0$ such that

$$\left| x_i - \frac{h_i}{k} \right| < \frac{1}{k^{1+1/m}} \text{ for } i = 1, 2, ..., n$$

Solution. This follows immediately from 7.1 since $1/N < 1/k^{1/n}$. □

Exercise 7.4 & 7.5. Since the book omits a proof of Hurwitz's theorem we will take this as an opportunity to fill it in. Proving that Hurwitz gives the best possible bound will subsume the results of exercises 7.4 and 7.5. I learned this proof from a paper titled "An Easy Proof of Hurwitz's Theorem" by Manuel Benito and J. Javier Escribano.

Solution. Our proof will make use of Brocot series. We will identity pairs of integers, (p, q), with rational numbers p/q. The pairs $(1, 0)$ and $(0, 1)$ will be seen as $1/0$ and $0/1$, where the precise meaning of $1/0$ is unimportant. We denote those two pairs by B_0. To generate B_{n+1}, the Brocot series of order $n + 1$, simply insert the mediant between each adjacent pair.

To prove our main result we will need two lemmas. We will use $\phi = \frac{1+\sqrt{5}}{2}$ and $\overline{\phi} = \frac{1-\sqrt{5}}{2}$ for both.

Lemma. Let $x = \frac{b}{d}$. Then, $-\overline{\phi} < x < \phi$ and $-\overline{\phi} < \frac{1}{x} < \phi$ if and only if $b^2 - bd\sqrt{5} + d^2 < 0$.

Proof. To prove the forward direction, note that

$$\left(\frac{b}{d} - \phi\right)\left(\frac{b}{d} + \overline{\phi}\right) < 0$$

Collecting terms gives the desired equation.
For the reverse direction, consider

$$\begin{aligned} x^2 - x\sqrt{5} + 1 &< 0 \\ x^{-2} - x^{-1}\sqrt{5} + 1 &< 0 \end{aligned}$$

and note that the roots are ϕ and $\overline{\phi}$. □

Now for the second lemma.

Lemma. If (b, d) satisfies $b^2 - bd\sqrt{5} + d^2 < 0$ then the following hold

$$\begin{aligned} (b + d)^2 - (b + d)d\sqrt{5} + d^2 &> 0 \\ b^2 - b(d + b)\sqrt{5} + (d + b)^2 &> 0 \end{aligned}$$

Proof. Our proof will make use of the first lemma. Let $x = \frac{b}{d}$ and see that

$$x + 1 = \frac{b + d}{d} > 1 - \overline{\phi} = \phi.$$

This implies that $\frac{b+d}{d} > \phi$ and thus

$$\left(\frac{b+d}{d} - \phi\right)\left(\frac{b+d}{d} - \overline{\phi}\right) > 0$$

Collecting terms gives the result, and the same argument works for the second case upon considering $1/x$. $\square$

With these lemmas we can proof the main result. Note that since α is irrational in the statement of Hurwitz's theorem we can always find two adjacent Brocot fractions,

$$\frac{a}{b}, \alpha, \frac{c}{d}$$

We will proceed in cases.

Case 1: Suppose that $b^2 - bd\sqrt{5} + d^2 > 0$. We will show that either $\alpha - \frac{a}{b} < \frac{1}{b^2\sqrt{5}}$ or $\frac{c}{d} - \alpha < \frac{1}{d^2\sqrt{5}}$. Suppose that neither are true. Then,

$$\frac{1}{bd} = \frac{c}{d} - \frac{a}{b} = \frac{c}{d} - \alpha + \alpha - \frac{a}{b} > \frac{1}{d^2\sqrt{5}} + \frac{1}{b^2\sqrt{5}}$$

Where the first equality is a basic property of Brocot series, similar to Farey fractions. This implies that

$$b^2 + d^2 - bd\sqrt{5} < 0$$

Which is a contradiction. This shows that one of $\frac{a}{b}$ and $\frac{b}{d}$ is a valid candidate for our approximation, and since we can always take the mediant $\frac{a+c}{b+d}$ and generate another valid candidate, this gives us infinitely many solutions. Now for our second case.

Case 2: Suppose we have $\frac{a}{b} < \alpha < \frac{c}{d}$ and $b^2 + d^2 - bd\sqrt{5} < 0$. Then, it is possible for neither of the fractions to be a valid approximation. However, we can move to B_{n+1} and we will get one of the following

$$\frac{a}{b} < \alpha < \frac{a+c}{b+d} \text{ or } \frac{a+c}{b+d} < \alpha < \frac{c}{d}$$

By our second lemma we have

$$(b+d)^2 + d^2 - (b+d)d\sqrt{5} > 0$$

And so by moving to B_{n+1} one of the approximations is forced to be valid. We have shown that one of the following is true

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2\sqrt{5}}$$
$$\left|\alpha - \frac{a+c}{b+d}\right| < \frac{1}{(b+d)^2\sqrt{5}}$$
$$\left|\alpha - \frac{c}{d}\right| < \frac{1}{d^2\sqrt{5}}$$

This proves the theorem as we can generate infinite solutions by continuing to make use of the mediant. Now we will show that $\sqrt{5}$ gives the best possible bound. That is, if we pick a larger constant there will only be finitely many solutions.

Let f_n represent the Fibonacci numbers. It is known that

$$f_n = (\phi^n - \overline{\phi}^n)\frac{1}{\sqrt{5}}.$$

It is also the case that

$$f_n\phi - f_{n+1} = \overline{\phi}^n = \frac{-1^n}{\phi^n}$$

If we take a constant greater than $\sqrt{5}$, say $\sqrt{5}+\varepsilon$, we will see that

$$\left|\phi - \frac{f_{n+1}}{f_n}\right| = \frac{1}{\sqrt{5}f_n(f_n+\overline{\phi}^n} = \frac{1}{\sqrt{5}f_n^2+\sqrt{5}f_n\overline{\phi}^n} < \frac{1}{f_n^2(\sqrt{5}+\varepsilon)}$$

Which means

$$\varepsilon f_n < \sqrt{5}\overline{\phi}^n$$

However, as $n \to \infty$, this inequality will eventually no longer be satisfied, as the right hand side goes to 0 while the left hand side blows up. This means there could only be finitely many solutions for any constant greater than $\sqrt{5}$.

□

Exercise 8.1 & 8.2.

Solution. See Leathem and Hardy's "The General Theory of Dirichlet Series", Theorem 7 and Theorem 9. They work under the assumption that $\sigma_c > 0$ but only slight modifications are needed to make their arguments go through when $\sigma_c < 0$. □