

Notes on the book:  
*Apostol, Modular Functions and  
Dirichlet Series in Number Theory,  
2nd edition*

Meng-Gen Tsai  
plover@gmail.com

July 31, 2021

## Contents

<b>Chapter 1: Elliptic functions</b>	<b>3</b>
Exercise 1.1. . . . .	3
Supplement 1.1.1. . . . .	4
Exercise 1.2. . . . .	4
Exercise 1.3. . . . .	5
Exercise 1.4. . . . .	6
Supplement 1.4.1. (Divisor class group) . . . . .	7
Exercise 1.5. . . . .	8
Exercise 1.6. . . . .	9
Exercise 1.7. . . . .	10
Exercise 1.8. . . . .	11
Exercise 1.9. . . . .	12
Exercise 1.10. . . . .	14
Exercise 1.11. . . . .	15
Exercise 1.12. . . . .	16
Exercise 1.13. . . . .	17
Exercise 1.14. (Lambert series) . . . . .	18
Exercise 1.15. . . . .	21
<b>Chapter 2: The modular group and modular functions</b>	<b>25</b>
Exercise 2.2. . . . .	25
Congruence subgroups . . . . .	25
Exercise 2.11. . . . .	26
Exercise 2.12. . . . .	26
Exercise 2.13. . . . .	27
Exercise 2.14. . . . .	27

Exercise 2.15. . . . .	28
Supplement 2.15.1. (Chinese remainder theorem) . . . . .	29
Exercise 2.16. . . . .	29
Exercise 2.17. . . . .	30
Exercise 2.18. . . . .	30
Exercise 2.19. . . . .	30
Exercise 2.20. . . . .	31

## Chapter 1: Elliptic functions

### Exercise 1.1.

Given two pairs of complex numbers  $(\omega_1, \omega_2)$  and  $(\omega'_1, \omega'_2)$  with nonreal ratios  $\omega_1/\omega_2$  and  $\omega'_1/\omega'_2$ . Prove that they generate the same set of periods if, and only if, there is a  $2 \times 2$  matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  with integer entries and determinant  $\pm 1$  such that

$$\begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}.$$

*Proof.*

- (1) ( $\implies$ ) Suppose  $(\omega_1, \omega_2)$  and  $(\omega'_1, \omega'_2)$  generate the same set of periods.

In particular, there is a  $2 \times 2$  matrix  $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{M}_{2 \times 2}(\mathbb{Z})$  (resp.

$A' := \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathbf{M}_{2 \times 2}(\mathbb{Z})$ ) such that

$$\begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix} = A \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}, \quad \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix} = A' \begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix}.$$

Hence it suffices to show  $\det(A) = \pm 1$ .

- (2) Note that

$$\begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix} = AA' \begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix}.$$

Hence

$$AA' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Take the determinant on the both sides to get

$$\det(A) \det(A') = 1.$$

Since  $\det(\mathbf{M}_{2 \times 2}(\mathbb{Z})) \subseteq \mathbb{Z}$ ,  $\det(A) = \pm 1$ .

- (3) ( $\impliedby$ )  $\Omega(\omega'_1, \omega'_2) \subseteq \Omega(\omega_1, \omega_2)$  is obvious. Note that

$$\begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix} = \underbrace{\frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}_{\in \mathbf{M}_{2 \times 2}(\mathbb{Z})} \begin{pmatrix} \omega'_2 \\ \omega'_1 \end{pmatrix}.$$

Thus  $\Omega(\omega_1, \omega_2) \subseteq \Omega(\omega'_1, \omega'_2)$ . Therefore  $\Omega(\omega_1, \omega_2) = \Omega(\omega'_1, \omega'_2)$ .

□

**Supplement 1.1.1.**

(Exercise I.1.1 in the textbook: *Jürgen Neukirch, Algebraic Number Theory*.)  
 $\alpha \in \mathbb{Z}[i]$  is a unit if and only if  $N(\alpha) = 1$ .

*Proof.*

- (1) ( $\implies$ ) Since  $\alpha$  is a unit, there is  $\beta \in \mathbb{Z}[i]$  such that  $\alpha\beta = 1$ . So  $N(\alpha\beta) = N(1)$ , or  $N(\alpha)N(\beta) = 1$ . Since the image of  $N$  is nonnegative integers,  $N(\alpha) = 1$ .
- (2) ( $\impliedby$ )  $N(\alpha) = \alpha\bar{\alpha}$ , or  $1 = \alpha\bar{\alpha}$  since  $N(\alpha) = 1$ . That is,  $\bar{\alpha} \in \mathbb{Z}[i]$  is the inverse of  $\alpha \in \mathbb{Z}[i]$ . (Or we solve the equation  $N(\alpha) = a^2 + b^2 = 1$ , and show that all four solutions ( $\pm 1$  and  $\pm i$ ) are units.)
- (3) Conclusion: a unit  $\alpha = a + bi$  of  $\mathbb{Z}[i]$  is satisfying the equation  $N(\alpha) = a^2 + b^2 = 1$  by (1)(2). That is, the only unit of  $\mathbb{Z}[i]$  are  $\pm 1$  and  $\pm i$ .

□

**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  $f$ . (Hint: Integrate  $z \frac{f'(z)}{f(z)}$ .)

*Proof.*

- (1) Similar to Theorem 1.8, the integral

$$\frac{1}{2\pi i} \int_C z \frac{f'(z)}{f(z)}$$

taken around the boundary  $C$  of a cell (no zeros or poles on its boundary) counts the difference between the sum of the zeros and the sum of the poles inside the cell, that is,

$$S(0) - S(\infty) = \frac{1}{2\pi i} \int_C z \frac{f'(z)}{f(z)}.$$

(The proof is similar to the proof of the argument principle.)

- (2) Let  $C_1$  be the path from 0 to  $\omega_1$ ,  $C_2$  be the path from  $\omega_1$  to  $\omega_1 + \omega_2$ ,  $C_3$

be the path from  $\omega_1 + \omega_2$  to  $\omega_2$ , and  $C_4$  be the path from  $\omega_2$  to 0. Hence

$$\begin{aligned}
& \frac{1}{2\pi i} \int_{C_1} z \frac{f'(z)}{f(z)} + \frac{1}{2\pi i} \int_{C_3} z \frac{f'(z)}{f(z)} \\
&= \frac{1}{2\pi i} \int_{C_1} z \frac{f'(z)}{f(z)} + \frac{1}{2\pi i} \int_{-C_1} (z + \omega_2) \frac{f'(z + \omega_2)}{f(z + \omega_2)} \\
&= \frac{1}{2\pi i} \int_{C_1} z \frac{f'(z)}{f(z)} - \frac{1}{2\pi i} \int_{C_1} (z + \omega_2) \frac{f'(z)}{f(z)} \\
&= -\omega_2 \frac{1}{2\pi i} \int_{C_1} \frac{f'(z)}{f(z)}
\end{aligned}$$

and

$$\begin{aligned}
& \frac{1}{2\pi i} \int_{C_2} z \frac{f'(z)}{f(z)} + \frac{1}{2\pi i} \int_{C_4} z \frac{f'(z)}{f(z)} \\
&= \frac{1}{2\pi i} \int_{-C_4} (z + \omega_1) \frac{f'(z + \omega_1)}{f(z + \omega_1)} + \frac{1}{2\pi i} \int_{C_4} z \frac{f'(z)}{f(z)} \\
&= -\frac{1}{2\pi i} \int_{C_4} (z + \omega_1) \frac{f'(z)}{f(z)} + \frac{1}{2\pi i} \int_{C_4} z \frac{f'(z)}{f(z)} \\
&= -\omega_1 \frac{1}{2\pi i} \int_{C_4} \frac{f'(z)}{f(z)}
\end{aligned}$$

Therefore

$$S(0) - S(\infty) = -\omega_1 \frac{1}{2\pi i} \int_{C_4} \frac{f'(z)}{f(z)} - \omega_2 \frac{1}{2\pi i} \int_{C_1} \frac{f'(z)}{f(z)}.$$

So it suffices to show that  $\frac{1}{2\pi i} \int_{C_1} \frac{f'(z)}{f(z)} \in \mathbb{Z}$ . (Other cases are similar.)

(3) By choosing one branch of log, we have

$$\begin{aligned}
\frac{1}{2\pi i} \int_{C_1} \frac{f'(z)}{f(z)} &= \frac{1}{2\pi i} \log \frac{f(\omega_1)}{f(0)} \\
&= \frac{1}{2\pi i} \log(1) && (f(\omega_1) = f(0)) \\
&= \frac{1}{2\pi i} (2\pi i m) \text{ for some } m \in \mathbb{Z} \\
&= m \in \mathbb{Z}.
\end{aligned}$$

□

### Exercise 1.3.

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

- (b) Let  $a_1, \dots, a_n$  and  $b_1, \dots, b_m$  be complex numbers such that none of the numbers  $\wp(a_i) - \wp(b_j)$  is zero. Let

$$f(z) = \frac{\prod_{k=1}^n [\wp(z) - \wp(a_k)]}{\prod_{r=1}^m [\wp(z) - \wp(b_r)]}.$$

Prove that  $f$  is an even elliptic function with zeros at  $a_1, \dots, a_n$  and poles at  $b_1, \dots, b_m$ .

*Proof of (a).*

- (1) Let  $\Omega$  be the lattice generated by periods of  $\wp$ .
- (2) ( $\implies$ ) It is equivalent to show that the equation  $\wp(u) = \wp(v)$  in terms of  $u$  has exactly two roots in some period parallelogram.  $u \equiv v \pmod{\Omega}$  is a root clearly and  $u \equiv -v \pmod{\Omega}$  is also a root since  $\wp$  is even. Since  $\wp$  is an elliptic function of order 2 (Theorem 1.8),  $u \equiv \pm v \pmod{\Omega}$  is the only two roots of  $\wp(u) = \wp(v)$ .
- (3) ( $\impliedby$ ) Obvious.

□

*Proof of (b).*

- (1) Since  $\wp$  is an even elliptic function,  $f$  is an even elliptic function too.
- (2)  $f$  has zeros at  $a_1, \dots, a_n$  and poles at  $b_1, \dots, b_m$  (by construction and (a)).

□

#### Exercise 1.4.

Prove that every even elliptic function  $f$  is a rational function of  $\wp$ , where periods of  $\wp$  are a subset of the periods of  $f$ .

*Proof.*

- (1) Nothing to do if  $f$  is constant. Let  $C$  be one period parallelogram of  $f$  and  $\wp$ . Let  $\Omega(\omega_1, \omega_2)$  be the lattice generated by periods of  $\wp$ . Suppose  $f$  has zeros at  $a_1, \dots, a_n$  and poles at  $b_1, \dots, b_m$ .
- (2) Might assume that  $\wp(z) - \wp(a_k)$  (resp.  $\wp(z) - \wp(b_r)$ ) has a simple zero in  $a_k$  (resp.  $b_r$ ) for all  $k, r$ . So the function

$$g(z) := f(z) \cdot \frac{\prod_{r=1}^m [\wp(z) - \wp(b_r)]^{\beta_r}}{\prod_{k=1}^n [\wp(z) - \wp(a_k)]^{\alpha_k}}$$

is an elliptic function with no zeros or poles in  $C$  where  $\alpha_k$  (resp.  $\beta_r$ ) is the order of the zero  $a_k$  (resp. the pole  $b_r$ ). By Theorems 1.4 and 1.5,  $g(z)$  is a constant. Hence

$$f(z) = C \cdot \frac{\prod_{k=1}^n [\wp(z) - \wp(a_k)]^{\alpha_k}}{\prod_{r=1}^m [\wp(z) - \wp(b_r)]^{\beta_r}}$$

for some constant  $C \in \mathbb{C}$ .

- (3) Now we consider the case  $a_k$  (resp.  $b_r$ ) is a zero of  $\wp'(z)$ . Since  $f$  is an even elliptic function, the order of  $a_k$  (resp.  $b_r$ ) of  $f$  is even. Note that the order of  $a_k$  (resp.  $b_r$ ) of  $\wp(z) - \wp(a_k)$  (resp.  $\wp(z) - \wp(b_r)$ ) is 2. Hence the function

$$g(z) := f(z) \cdot \frac{\prod_{\wp'(b_r) \neq 0} [\wp(z) - \wp(b_r)]^{\beta_r}}{\prod_{\wp'(a_k) \neq 0} [\wp(z) - \wp(a_k)]^{\alpha_k}} \cdot \frac{\prod_{\wp'(b_r) = 0} [\wp(z) - \wp(b_r)]^{\frac{\beta_r}{2}}}{\prod_{\wp'(a_k) = 0} [\wp(z) - \wp(a_k)]^{\frac{\alpha_k}{2}}}$$

is a constant too.

□

#### Supplement 1.4.1. (Divisor class group)

(Problem 8.6 in the textbook: *William Fulton, Algebraic Curves*.) Let  $D(X)$  be the group of divisors on  $X$ ,  $D_0(X)$  the subgroup consisting of divisors of degree zero, and  $P(X)$  the subgroup of  $D_0(X)$  consisting of divisors of rational functions. Let  $C_0(X) = D_0(X)/P(X)$  be the quotient group. It is the **divisor class group** on  $X$ .

- (a) If  $X = \mathbf{P}^1$ , then  $C_0(X) = 0$ .
- (b) Let  $X = C$  be a nonsingular cubic. Pick  $P_0 \in C$ , defining  $\oplus$  on  $C$ . Show that the map from  $C$  to  $C_0(X)$  that sends  $P$  to the residue class of the divisor  $P - P_0$  is an isomorphism from  $(C, \oplus)$  onto  $C_0(X)$ .

*Proof of (a).*

- (1) Given a divisor

$$D = \sum_{P \in X} n_P P \in D_0(X)$$

where  $n_P \in \mathbb{Z}$  and  $\sum_P n_P = 0$ .

- (2) Note that  $\sum_P n_P = 0$ . We can define a rational function  $z \in k(X)$  by

$$z = \prod_{P=[a_P:b_P] \in X} (b_P x - a_P y)^{n_P}.$$

Hence  $\text{div}(z) = D \in P(X)$ . Therefore  $C_0(X) = D_0(X)/P(X) = 0$ .

□

*Proof of (b).*

- (1) Define  $\alpha : (C, \oplus) \rightarrow C_0(X)$  by  $P \mapsto [P - P_0]$ .
- (2) Show that  $\alpha$  is a group homomorphism. If  $P \oplus Q = R$ , then

$$\begin{aligned}
 P \oplus Q &= R \\
 \iff [P + Q] &= [R + P_0] && \text{(Problem 8.3(c))} \\
 \iff [P - P_0] + [Q - P_0] &= [R - P_0] && \text{(Proposition 2)} \\
 \iff \alpha(P) + \alpha(Q) &= \alpha(R) = \alpha(P \oplus Q).
 \end{aligned}$$

- (3) Show that  $\alpha$  is injective.

$$\begin{aligned}
 \alpha(P) = 0 &\iff [P - P_0] = 0 \\
 &\iff [P] = [P_0] && \text{(Proposition 2)} \\
 &\iff P = P_0. && \text{(Problem 8.3(a))}
 \end{aligned}$$

- (4) Show that  $\alpha$  is surjective. Given  $[D] \in C_0(X)$  and we want to find a point  $P \in C$  such that  $\alpha(P) = [D]$ . Write

$$D = (P_1 + \cdots + P_r) - (Q_1 + \cdots + Q_r)$$

for some  $P_i, Q_i \in C$ . So

$$\begin{aligned}
 [D] &= [P_1 - P_0] + \cdots + [P_r - P_0] - [Q_1 - P_0] - \cdots - [Q_r - P_0] \\
 &= \alpha(P_1) + \cdots + \alpha(P_r) - \alpha(Q_1) - \cdots - \alpha(Q_r) \\
 &= \alpha(P_1) + \cdots + \alpha(P_r) + \alpha(Q'_1) + \cdots + \alpha(Q'_r) \\
 &= \alpha(P_1 \oplus \cdots \oplus P_r \oplus Q'_1 \oplus \cdots \oplus Q'_r).
 \end{aligned}$$

where  $Q'_i$  is the inverse of  $Q_i$  in  $(C, \oplus)$ . Hence there is a point  $P := P_1 \oplus \cdots \oplus P_r \oplus Q'_1 \oplus \cdots \oplus Q'_r \in C$  such that  $\alpha(P) = [D]$ .

□

### Exercise 1.5.

*Prove that every elliptic function  $f$  can be expressed in the form*

$$f(z) = R_1[\wp(z)] + \wp'(z)R_2[\wp(z)]$$

*where  $R_1$  and  $R_2$  are rational functions and  $\wp$  has the same set of periods as  $f$ .*



*Proof.*

$$\begin{aligned}
f(z) &= \underbrace{\frac{f(z) + f(-z)}{2}}_{\text{even}} + \wp'(z) \underbrace{\frac{f(z) - f(-z)}{2\wp'(z)}}_{\text{even}} \\
&= R_1[\wp(z)] + \wp'(z)R_2[\wp(z)] \text{ for some rational functions } R_1, R_2
\end{aligned}$$

(by Exercise 1.4).  $\square$

**Exercise 1.6.**

Let  $f$  and  $g$  be two elliptic functions with the same set of periods. Prove that there exists a polynomial  $P(x, y)$ , not identically zero, such that

$$P[f(z), g(z)] = C$$

where  $C$  is a constant (depending on  $f$  and  $g$  but not on  $z$ ).

*Proof.*

(1) By Exercise 1.5, we have

$$f(z) = R_1[\wp(z)] + \wp'(z)R_2[\wp(z)]$$

for some rational functions  $R_1, R_2$  and  $\wp$  has the same set of periods as  $f$ . By cleaning the denominators of  $R_1$  and  $R_2$ , we might assume

$$S[\wp(z)]f(z) = R_1[\wp(z)] + \wp'(z)R_2[\wp(z)]$$

for some polynomials  $R_1, R_2, S$ .

(2) So

$$\begin{aligned}
&\wp'(z)R_2[\wp(z)] = S[\wp(z)]f(z) - R_1[\wp(z)] \\
\implies &\wp'(z)^2 R_2[\wp(z)]^2 = (S[\wp(z)]f(z) - R_1[\wp(z)])^2 \\
\implies &(4\wp(z)^3 - 60G_4\wp(z) - 140G_6)R_2[\wp(z)]^2 \\
&= (S[\wp(z)]f(z) - R_1[\wp(z)])^2. \quad (\text{Theorem 1.12}) \\
\implies &F(\wp(z), f(z)) = 0
\end{aligned}$$

for some polynomials  $F(x, y) \in \mathbb{C}[x, y]$ . Note that  $F(x, y)$  is of degree 2 if we view  $F \in (\mathbb{C}[x])[y]$ .

(3) Similarly,

$$G(\wp(z), g(z)) = 0$$

for some polynomials  $G(x, y) \in \mathbb{C}[x, y]$ .

- (4) Let  $P = \text{Res}_x(F, G)$  be the resultant of two polynomials  $F$  and  $G$  with respect to  $x$  to eliminate  $\wp(z)$ . Note that  $P$  is a nonzero polynomial (since  $F$  and  $G$  are nonzero) and  $P[f(z), g(z)] = 0$ . So  $P$  is our desired polynomial.

□

**Exercise 1.7.**

The discriminant of the polynomial  $f(x) = 4(x - x_1)(x - x_2)(x - x_3)$  is the product  $16\{(x_2 - x_1)(x_3 - x_2)(x_3 - x_1)\}^2$ . Prove that the discriminant of  $f(x) = 4x^3 - ax - b$  is  $a^3 - 27b^2$ .

*Proof.*

- (1) Since

$$f'(x) = 4(x - x_2)(x - x_3) + 4(x - x_1)(x - x_3) + 4(x - x_1)(x - x_2),$$

we have

$$f'(x_1) = 4(x_1 - x_2)(x_1 - x_3),$$

$$f'(x_2) = 4(x_2 - x_1)(x_2 - x_3),$$

$$f'(x_3) = 4(x_3 - x_1)(x_3 - x_2).$$

Hence

$$f'(x_1)f'(x_2)f'(x_3) = -4\text{disc}(f)$$

where  $\text{disc}(f)$  is the discriminant of  $f(x)$ .

- (2) As  $f(x) = 4x^3 - ax - b$ , we have  $f'(x) = 12x^2 - a$ . So

$$f'(x_1)f'(x_2)f'(x_3) = (12x_1^2 - a)(12x_2^2 - a)(12x_3^2 - a).$$

Note that

$$x_1x_2x_3 = \frac{b}{4},$$

$$x_1x_2 + x_2x_3 + x_3x_1 = -\frac{a}{4},$$

$$x_1 + x_2 + x_3 = 0,$$

we have

$$x_1^2x_2^2x_3^2 = \frac{b^2}{4^2},$$

$$x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2 = (x_1x_2 + x_2x_3 + x_3x_1)^2 - 2x_1x_2x_3(x_1 + x_2 + x_3)$$

$$= \frac{a^2}{4^2},$$

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1)$$

$$= \frac{a}{2}.$$

(3) Hence

$$\begin{aligned}
f'(x_1)f'(x_2)f'(x_3) &= (12x_1^2 - a)(12x_2^2 - a)(12x_3^2 - a) \\
&= 12^3(x_1^2x_2^2x_3^2) - 12^2a(x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2) \\
&\quad + 12a^2(x_1^2 + x_2^2 + x_3^2) - a^3 \\
&= 12^3 \cdot \frac{b^2}{4^2} - 12^2a \cdot \frac{a^2}{4^2} + 12a^2 \cdot \frac{a}{2} - a^3 \\
&= -4(a^3 - 27b^2).
\end{aligned}$$

Therefore

$$\text{disc}(4x^3 - ax - b) = a^3 - 27b^2.$$

□

### Exercise 1.8.

The differential equation for  $\wp$  shows that  $\wp'(z) = 0$  if  $z = \frac{\omega_1}{2}, \frac{\omega_2}{2}$  or  $\frac{\omega_1 + \omega_2}{2}$ . Show that

$$\wp''\left(\frac{\omega_1}{2}\right) = 2(e_1 - e_2)(e_1 - e_3)$$

and obtain corresponding formulas for  $\wp''\left(\frac{\omega_2}{2}\right)$  and  $\wp''\left(\frac{\omega_1 + \omega_2}{2}\right)$ .

*Proof.*

(1) Differentiation of the equation

$$4\wp(z)^3 - g_2\wp(z) - g_3 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

in Theorem 1.14 to get

$$\begin{aligned}
12\wp(z)^2\wp'(z) - g_2\wp'(z) &= 4\wp'(z)(\wp(z) - e_2)(\wp(z) - e_3) \\
&\quad + 4\wp'(z)(\wp(z) - e_1)(\wp(z) - e_3) \\
&\quad + 4\wp'(z)(\wp(z) - e_1)(\wp(z) - e_2).
\end{aligned}$$

Since  $\wp''(z) = 6\wp(z)^2 - \frac{g_2}{2}$ , we have

$$\begin{aligned}
\wp''(z) &= 2(\wp(z) - e_2)(\wp(z) - e_3) \\
&\quad + 2(\wp(z) - e_1)(\wp(z) - e_3) \\
&\quad + 2(\wp(z) - e_1)(\wp(z) - e_2).
\end{aligned}$$

(2) Hence

$$\begin{aligned}
\wp''\left(\frac{\omega_1}{2}\right) &= 2(e_1 - e_2)(e_1 - e_3), \\
\wp''\left(\frac{\omega_2}{2}\right) &= 2(e_2 - e_1)(e_2 - e_3), \\
\wp''\left(\frac{\omega_1 + \omega_2}{2}\right) &= 2(e_3 - e_1)(e_3 - e_2).
\end{aligned}$$

□

**Exercise 1.9.**

According to Exercise 1.4, the function  $\wp(2z)$  is a rational function of  $\wp(z)$ . Prove that, in fact,

$$\wp(2z) = \frac{\{\wp(z)^2 + \frac{1}{4}g_2\}^2 + 2g_3\wp(z)}{4\wp(z)^3 - g_2\wp(z) - g_3} = -2\wp(z) + \frac{1}{4} \left( \frac{\wp''(z)}{\wp'(z)} \right)^2.$$

*Proof.*

(1) By  $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$  and  $\wp''(z) = 6\wp(z)^2 - \frac{1}{2}g_2$ , we have

$$\begin{aligned} & -2\wp(z) + \frac{1}{4} \left( \frac{\wp''(z)}{\wp'(z)} \right)^2 \\ &= -2\wp(z) + \frac{1}{4} \cdot \frac{(6\wp(z)^2 - \frac{1}{2}g_2)^2}{4\wp(z)^3 - g_2\wp(z) - g_3} \\ &= \frac{-2\wp(z)[4\wp(z)^3 - g_2\wp(z) - g_3] + \frac{1}{4}(6\wp(z)^2 - \frac{1}{2}g_2)^2}{4\wp(z)^3 - g_2\wp(z) - g_3} \\ &= \frac{\wp(z)^4 + \frac{1}{2}g_2\wp(z)^2 + \frac{1}{16}g_2^2 + 2g_3\wp(z)}{4\wp(z)^3 - g_2\wp(z) - g_3} \\ &= \frac{\{\wp(z)^2 + \frac{1}{4}g_2\}^2 + 2g_3\wp(z)}{4\wp(z)^3 - g_2\wp(z) - g_3}. \end{aligned}$$

So it suffices to show that  $\wp(2z) = -2\wp(z) + \frac{1}{4} \left( \frac{\wp''(z)}{\wp'(z)} \right)^2$ .

(2) Let  $\Omega$  be the lattice generated by periods of  $\wp$ . Suppose the addition theorem of  $\wp$  holds, that is,

$$\wp(u) + \wp(v) + \wp(u+v) = \frac{1}{4} \left( \frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \right)^2$$

with  $u, v, u+v \not\equiv 0 \pmod{\Omega}$ . Then letting  $v \rightarrow u$ , we have

$$\begin{aligned} \wp(2u) &= \lim_{v \rightarrow u} \wp(u+v) \\ &= \lim_{v \rightarrow u} \left\{ -\wp(u) - \wp(v) + \frac{1}{4} \left( \frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \right)^2 \right\} \\ &= -2\wp(u) + \frac{1}{4} \lim_{v \rightarrow u} \frac{\wp'(v) - \wp'(u)}{\wp(v) - \wp(u)} \\ &= -2\wp(u) + \frac{1}{4} \left( \frac{\wp''(u)}{\wp'(u)} \right)^2. \end{aligned}$$

The last equality is followed by L'Hospital's rule. So it suffices to show the addition theorem of  $\wp$  is true.

- (3) Let  $u + v + w = 0$ , with  $u, v, w \not\equiv 0 \pmod{\Omega}$ . Show that

$$\begin{vmatrix} \wp(u) & \wp'(u) & 1 \\ \wp(v) & \wp'(v) & 1 \\ \wp(w) & \wp'(w) & 1 \end{vmatrix} = 0.$$

Consider the elliptic function

$$f(z) := \wp'(z) - \underbrace{\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}}_{:=A} \wp(z) - \underbrace{\frac{\wp(u)\wp'(v) - \wp(v)\wp'(u)}{\wp(u) - \wp(v)}}_{:=B}.$$

$f$  has exactly 3 zeros in a period parallelogram as  $f$  has order 3. Note that  $f$  has a pole at 0 of order 3. By Exercise 1.2, the sum of the zeros is equal to the sum of poles in a period parallelogram. Since  $u$  and  $v$  are zeros of  $f$  (by verifying  $f(u) = f(v) = 0$  directly), the third zero must be  $-u - v = w$ . Hence there is a line

$$y = Ax + B$$

passing through 3 points  $(\wp(u), \wp'(u))$ ,  $(\wp(v), \wp'(v))$  and  $(\wp(w), \wp'(w))$ . So the determinant is zero.

- (4) Now we are going to remove the term  $\wp'(w)$  to prove the addition theorem of  $\wp$ . By Theorem 1.12, we have the system of equations

$$\begin{cases} y = Ax + B, \\ y^2 = 4x^3 - g_2x - g_3, \end{cases}$$

where  $(x, y) = (\wp(z), \wp'(z))$ . Hence

$$\begin{aligned} (Ax + B)^2 &= 4x^3 - g_2x - g_3 \\ \iff 4x^3 - A^2x^2 - (2AB + g_2)x - (B^2 + g_3) &= 0 \\ \implies \text{sum of three roots of } x \text{ is } \frac{A^2}{4} \\ \implies \wp(u) + \wp(v) + \wp(w) &= \frac{1}{4} \left( \frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \right)^2 \\ \implies \wp(-u - v) &= -\wp(u) - \wp(v) + \frac{1}{4} \left( \frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \right)^2 \\ \implies \wp(u + v) &= -\wp(u) - \wp(v) + \frac{1}{4} \left( \frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)} \right)^2. \quad (\wp: \text{ even}) \end{aligned}$$

So the addition theorem of  $\wp$  is established.

□

*Note.*

- (1) In the proof, part (4) is similar to defining an addition  $\oplus$  on a nonsingular cubic  $E$  in  $\mathbf{P}^2(k)$ . It is equivalent to defining the divisor class group on  $E$ . See Problem 8.6 in the textbook: *William Fulton, Algebraic Curves*.
- (2) If  $E \in \mathbf{P}^2(\mathbb{C})$  is the elliptic curve corresponding to the lattice  $\Omega$ , then there is an isomorphism

$$\alpha : \mathbb{C}/\Omega \longrightarrow E : y^2z = 4x^3 - g_2xz^2 - g_3z^3$$

defined by

$$\alpha(z) = \begin{cases} [\wp(z) : \wp'(z) : 1] & \text{if } z \neq 0 \in \Omega, \\ [0 : 1 : 0] & \text{if } z = 0 \in \Omega, \end{cases}$$

such that  $\alpha$  is both analytic (as a mapping of complex manifolds) and algebraic (as a homomorphism of groups).

### Exercise 1.10.

Let  $\omega_1$  and  $\omega_2$  be complex numbers with nonreal ratio. Let  $f(z)$  be an entire function and assume there are constants  $a$  and  $b$  such that

$$f(z + \omega_1) = af(z), \quad f(z + \omega_2) = bf(z),$$

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

*Proof.*

- (1) Might assume that  $a \neq 0$  and  $b \neq 0$  (otherwise  $f = 0$  on  $\mathbb{C}$ ).
- (2) Define

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

It suffices to show  $g$  is a constant. Note that  $g(z)$  is entire (since  $f$  and  $e^{Bz} \neq 0$  are entire). By Theorem 1.4, it suffices to show  $g$  is doubly periodic, that is, to show

$$g(z + \omega_1) = g(z) \text{ and } g(z + \omega_2) = g(z)$$

for suitable  $B$ .

(3) Note that

$$\begin{aligned}
& g(z + \omega_1) = g(z) \text{ and } g(z + \omega_2) = g(z) \\
& \iff \frac{a}{e^{B\omega_1}} \cdot g(z) = g(z) \text{ and } \frac{b}{e^{B\omega_2}} \cdot g(z) = g(z) \\
& \iff e^{B\omega_1} = a \text{ and } e^{B\omega_2} = b \\
& \iff \exists B \text{ such that } e^{B\omega_1} = a \text{ and } e^{B\omega_2} = b.
\end{aligned}$$

Take  $B$  such that  $e^{B(\omega_1 - \omega_2)} = \frac{a}{b}$  (since  $\frac{a}{b}$  is well-defined,  $\omega_1 - \omega_2 \neq 0$ , and  $z \mapsto \exp(z)$  is a onto map from  $\mathbb{C}$  to  $\mathbb{C} \setminus \{0\}$ ). Hence  $g$  is doubly periodic.

□

**Exercise 1.11.**

If  $k \geq 2$  and  $\tau \in H$  prove that the Eisenstein series

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

has the Fourier expansion

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

*Proof.*

(1) Let  $q = e^{2\pi i \tau}$ . Similar to Lemma 1.3 on page 19, we have

$$(2k-1)! \sum_{m=-\infty}^{+\infty} \frac{1}{(\tau + m)^{2k}} = (2\pi i)^{2k} \sum_{r=1}^{\infty} r^{2k-1} q^r.$$

(2) Similar to Theorem 1.18, we have

$$\begin{aligned}
G_{2k}(\tau) &= \sum_{(m,n) \neq (0,0)} (m+n\tau)^{-2k} \\
&= \sum_{\substack{m=-\infty \\ m \neq 0 (n=0)}}^{+\infty} m^{-2k} + \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} ((m+n\tau)^{-2k} + (m-n\tau)^{-2k}) \\
&= 2\zeta(2k) + 2 \sum_{n=1}^{\infty} \sum_{m=-\infty}^{+\infty} (m+n\tau)^{-2k} \\
&= 2\zeta(2k) + 2 \sum_{n=1}^{\infty} \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{r=1}^{\infty} r^{2k-1} q^{nr} \\
&= 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \underbrace{\sum_{d|n} d^{2k-1}}_{=\sigma_{2k-1}(n)} q^n.
\end{aligned}$$

In the last double sum we collect together those terms for which  $nr$  is constant.

□

### Exercise 1.12.

Refer to Exercise 1.11. If  $\tau \in H$  prove that

$$G_{2k}\left(-\frac{1}{\tau}\right) = \tau^{2k} G_{2k}(\tau)$$

and deduce that

$$\begin{aligned}
G_{2k}\left(\frac{i}{2}\right) &= (-4)^k G_{2k}(2i) && \text{for all } k \geq 2, \\
G_{2k}(i) &= 0 && \text{if } k \text{ is odd,} \\
G_{2k}(e^{\frac{2\pi i}{3}}) &= 0 && \text{if } k \not\equiv 0 \pmod{3}.
\end{aligned}$$

*Proof.*



(1)

$$\begin{aligned}
G_{2k}\left(-\frac{1}{\tau}\right) &= \sum_{(m,n) \neq (0,0)} \left(m - \frac{n}{\tau}\right)^{-2k} \\
&= \tau^{2k} \sum_{(m,n) \neq (0,0)} (\tau m - n)^{-2k} \\
&= \tau^{2k} G_{2k}(\tau).
\end{aligned}$$

(2) Let  $\tau = 2i$ . We have  $G_{2k}\left(\frac{i}{2}\right) = (-4)^k G_{2k}(2i)$ .

(3) Let  $\tau = i$ . We have  $G_{2k}(i) = (-1)^k G_{2k}(i)$ . Hence  $G_{2k}(i) = 0$  if  $k$  is odd.

(4) Let  $\tau = e^{\frac{\pi i}{3}}$ . We have  $G_{2k}(e^{\frac{2\pi i}{3}}) = e^{\frac{2k\pi i}{3}} G_{2k}(e^{\frac{\pi i}{3}})$ . Since

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

and each Eisenstein series is a periodic function of  $\tau$  of period 1, we have  $G_{2k}(e^{\frac{2\pi i}{3}}) = G_{2k}(e^{\frac{\pi i}{3}})$ . So  $G_{2k}(e^{\frac{2\pi i}{3}}) = e^{\frac{2k\pi i}{3}} G_{2k}(e^{\frac{2\pi i}{3}})$ . Therefore  $G_{2k}(e^{\frac{2\pi i}{3}}) = 0$  if  $k \not\equiv 0 \pmod{3}$ .

□

### Exercise 1.13.

Ramanujan's tau function  $\tau(n)$  is defined by the Fourier expansion

$$\Delta(\tau) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n \tau},$$

derived in Theorem 1.19. Prove that

$$\tau(n) = 8000\{(\sigma_3 \circ \sigma_3) \circ \sigma_3\}(n) - 147(\sigma_5 \circ \sigma_5)(n),$$

where  $f \circ g$  denotes the Cauchy product of two sequences,

$$(f \circ g)(n) = \sum_{k=0}^n f(k)g(n-k),$$

and  $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$  for  $n \geq 1$ , with  $\sigma_3(0) = \frac{1}{240}$ ,  $\sigma_5(0) = -\frac{1}{504}$ . (Hint: Theorem 1.18.)

*Proof.*

(1) Let  $q = e^{2\pi i\tau}$ . Write

$$g_2(\tau) = \frac{4\pi^4}{3} \left\{ 1 + 240 \sum_{k=1}^{\infty} \sigma_3(k) q^k \right\} = \frac{4\pi^4}{3} \left\{ 240 \sum_{k=0}^{\infty} \sigma_3(k) q^k \right\},$$

$$g_3(\tau) = \frac{8\pi^6}{27} \left\{ 1 - 504 \sum_{k=1}^{\infty} \sigma_5(k) q^k \right\} = \frac{8\pi^6}{27} \left\{ -504 \sum_{k=0}^{\infty} \sigma_5(k) q^k \right\}$$

(Theorem 1.18).

(2) Similar to the proof of Theorem 1.19,

$$\begin{aligned} \Delta(\tau) &= g_2(\tau)^3 - 27g_3(\tau)^2 \\ &= \frac{64\pi^{12}}{27} \left\{ \left( 240 \sum_{k=0}^{\infty} \sigma_3(k) q^k \right)^3 - \left( -504 \sum_{k=0}^{\infty} \sigma_5(k) q^k \right)^2 \right\} \\ &= (2\pi)^{12} \left\{ 8000 \left( \sum_{k=0}^{\infty} \sigma_3(k) q^k \right)^3 - 147 \left( \sum_{k=0}^{\infty} \sigma_5(k) q^k \right)^2 \right\} \\ &= (2\pi)^{12} \sum_{n=0}^{\infty} \{ 8000 \{ (\sigma_3 \circ \sigma_3) \circ \sigma_3 \}(n) - 147 (\sigma_5 \circ \sigma_5)(n) \} q^n \\ &= (2\pi)^{12} \sum_{n=1}^{\infty} \{ 8000 \{ (\sigma_3 \circ \sigma_3) \circ \sigma_3 \}(n) - 147 (\sigma_5 \circ \sigma_5)(n) \} q^n. \end{aligned}$$

(Here  $8000 \{ (\sigma_3 \circ \sigma_3) \circ \sigma_3 \}(0) - 147 (\sigma_5 \circ \sigma_5)(0) = 0$ .)

(3) Therefore

$$\tau(n) = 8000 \{ (\sigma_3 \circ \sigma_3) \circ \sigma_3 \}(n) - 147 (\sigma_5 \circ \sigma_5)(n)$$

for  $n \geq 1$ .

□

#### Exercise 1.14. (Lambert series)

A series of the form  $\sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n}$  is called a **Lambert series**. 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  $|x| < 1$ .

(a)

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

(b)

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

(c)

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

(d)

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

(e) Use the result in (c) to express  $g_2(\tau)$  and  $g_3(\tau)$  in terms of Lambert series in  $x = e^{2\pi i\tau}$ .

*Note.* In (a),  $\mu(n)$  is the Möbius function; In (b),  $\varphi(n)$  is Euler's totient; and in (d),  $\lambda(n)$  is Liouville's function.

*Proof.* Similar to the proof of Exercise 1.11.

$$\begin{aligned} \sum_{n=1}^{\infty} f(n) \frac{x^n}{1-x^n} &= \sum_{n=1}^{\infty} f(n) \sum_{r=1}^{\infty} x^{rn} \\ &= \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} f(n) x^{rn} \\ &= \sum_{n=1}^{\infty} \underbrace{\left( \sum_{d|n} f(d) \right)}_{=F(n)} x^n. \end{aligned}$$

□

*Proof of (a).* Theorem 2.1 in the textbook: *T. M. Apostol, Introduction to Analytic Number Theory* shows that

$$F(n) := \sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

Hence

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

□

*Proof of (b).* Theorem 2.2 in the textbook: *T. M. Apostol, Introduction to Analytic Number Theory* shows that  $F(n) := \sum_{d|n} \varphi(d) = n$ . Hence

$$\sum_{n=1}^{\infty} \varphi(n) \frac{x^n}{1-x^n} = \sum_{n=1}^{\infty} F(n) x^n = \sum_{n=1}^{\infty} n x^n = \frac{x}{(1-x)^2}.$$

□

*Proof of (c).* Since

$$F(n) := \sum_{d|n} d^\alpha = \sigma_\alpha(n),$$

we have

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

□

*Proof of (d).* Theorem 2.19 in the textbook: *T. M. Apostol, Introduction to Analytic Number Theory* shows that

$$F(n) := \sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise.} \end{cases}$$

Hence

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

□

*Proof of (e).*

(1) Let  $q = x = e^{2\pi i \tau}$ .

$$\begin{aligned} g_2(\tau) &= \frac{4\pi^4}{3} \left\{ 1 + 240 \sum_{k=1}^{\infty} \sigma_3(k) q^k \right\} && \text{(Theorem 1.18)} \\ &= \frac{4\pi^4}{3} \left\{ 1 + 240 \sum_{k=1}^{\infty} \frac{k^3 q^k}{1-q^k} \right\} && ((c)). \end{aligned}$$

(2) Similarly,

$$\begin{aligned} g_3(\tau) &= \frac{8\pi^6}{27} \left\{ 1 - 504 \sum_{k=1}^{\infty} \sigma_5(k) q^k \right\} && \text{(Theorem 1.18)} \\ &= \frac{8\pi^6}{27} \left\{ 1 - 504 \sum_{k=1}^{\infty} \frac{k^5 q^k}{1-q^k} \right\} && ((c)). \end{aligned}$$

□

*Note.*

(1)

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)x^n}{1-x^n} = \sum_{n=1}^{\infty} \log(n)x^n,$$

where  $\Lambda(n)$  is von Mangoldt function.

(2) Similar to Exercise 1.15, we have a similar formula for (a)

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

by noting that

$$\sum_{n=1}^{\infty} \frac{f(n)x^n}{1+x^n} = \sum_{n=1}^{\infty} \frac{f(n)x^n}{1-x^n} - 2 \sum_{n=1}^{\infty} \frac{f(n)x^{2n}}{1-x^{2n}}.$$

**Exercise 1.15.**

*Let*

$$G(x) = \sum_{n=1}^{\infty} \frac{n^5 x^n}{1-x^n},$$

*and let*

$$F(x) = \sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^5 x^n}{1+x^n}.$$

(a) *Prove that*  $F(x) = G(x) - 34G(x^2) + 64(x^4)$ .

(b) *Prove that*

$$\sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^5}{1+e^{n\pi}} = \frac{31}{504}.$$

(c) *Use Theorem 12.17 in the textbook: T. M. Apostol, Introduction to Analytic Number Theory to prove the more general result*

$$\sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^{4k+1}}{1+e^{n\pi}} = \frac{2^{4k+1}-1}{8k+4} B_{4k+2}.$$

*Proof of (a).*

(1) Consider the general case. *Let*

$$G(x) = \sum_{n=1}^{\infty} \frac{n^{4k+1}x^n}{1-x^n},$$

*and let*

$$F(x) = \sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^{4k+1}x^n}{1+x^n}.$$

*Show that*  $F(x) = G(x) - (2^{4k+1} + 2)G(x^2) + 2^{4k+2}G(x^4)$ .

(2) The identity

$$\sum_{n=1}^{\infty} \frac{x^n}{1+x^n} = \sum_{n=1}^{\infty} \frac{x^n}{1-x^n} - 2 \sum_{n=1}^{\infty} \frac{x^{2n}}{1-x^{2n}}$$

is always true. Hence  $H(x) := \sum_{n=1}^{\infty} \frac{n^{4k+1}x^n}{1+x^n} = G(x) - 2G(x^2)$ .

(3) Note that

$$\begin{aligned} H(x) &= \sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^{4k+1}x^n}{1+x^n} + \sum_{\substack{n=1 \\ (n \text{ even})}}^{\infty} \frac{n^{4k+1}x^n}{1+x^n} \\ &= F(x) + \sum_{n=1}^{\infty} \frac{(2n)^{4k+1}x^{2n}}{1+x^{2n}} \\ &= F(x) + 2^{4k+1} \sum_{n=1}^{\infty} \frac{n^{4k+1}x^{2n}}{1+x^{2n}} \\ &= F(x) + 2^{4k+1}H(x^2). \end{aligned}$$

Hence

$$\begin{aligned} F(x) &= H(x) - 2^{4k+1}H(x^2) \\ &= [G(x) - 2G(x^2)] - 2^{4k+1}[G(x^2) - 2G(x^4)] \\ &= G(x) - (2^{4k+1} + 2)G(x^2) + 2^{4k+2}G(x^4). \end{aligned}$$

□

*Proof of (b).* Take  $k = 1$  in part (c), we have

$$\sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^5}{1+e^{n\pi}} = \frac{31}{12} \cdot \frac{1}{42} = \frac{31}{504}.$$

□

*Proof of (c).*

(1) Let  $q = e^{2\pi i\tau}$ . So

$$\begin{aligned} G_{4k+2}(\tau) &= 2\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} \sum_{n=1}^{\infty} \sigma_{4k+1}(n) q^n \quad (\text{Exercise 1.11}) \\ &= 2\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} G(q) \quad (\text{Exercise 1.14(c)}) \end{aligned}$$

Hence

$$\begin{aligned} &G_{4k+2}(\tau) - (2^{4k+1} + 2)G_{4k+2}(2\tau) + 2^{4k+2}G_{4k+2}(4\tau) \\ &= \left[ 2\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} G(q) \right] \\ &\quad - (2^{4k+1} + 2) \left[ 2\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} G(q^2) \right] \\ &\quad + 2^{4k+2} \left[ 2\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} G(q^4) \right] \\ &= (1 - (2^{4k+1} + 2) + 2^{4k+2}) \cdot 2\zeta(4k+2) \\ &\quad + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} [G(q) - (2^{4k+1} + 2)G(q^2) + 2^{4k+2}G(q^4)] \\ &= (2^{4k+2} - 2)\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} F(q). \end{aligned}$$

(2) By taking  $\tau = \frac{i}{2}$ , we have

$$F(q) = F(e^{-\pi}) = \sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^{4k+1}}{1 + e^{n\pi}}$$

and

$$\begin{aligned} &G_{4k+2}(\tau) - (2^{4k+1} + 2)G_{4k+2}(2\tau) + 2^{4k+2}G_{4k+2}(4\tau) \\ &= G_{4k+2}\left(\frac{i}{2}\right) - (2^{4k+1} + 2)G_{4k+2}(i) + 2^{4k+2}G_{4k+2}(2i) \\ &= (-4)^{2k+1}G_{4k+2}(2i) - (2^{4k+1} + 2) \cdot 0 + 2^{4k+2}G_{4k+2}(2i) \\ &= 0. \end{aligned}$$

(Exercise 1.12). Hence

$$0 = (2^{4k+2} - 2)\zeta(4k+2) + \frac{2(2\pi i)^{4k+2}}{(4k+1)!} \sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^{4k+1}}{1 + e^{n\pi}}.$$

(3) Theorem 12.17 in the textbook: *T. M. Apostol, Introduction to Analytic Number Theory* shows that

$$\zeta(4k+2) = (-1)^{2k+1+1} \frac{(2\pi)^{4k+2} B_{4k+2}}{2(4k+2)!} = \frac{(2\pi)^{4k+2} B_{4k+2}}{2(4k+2)!}.$$

Hence

$$\sum_{\substack{n=1 \\ (n \text{ odd})}}^{\infty} \frac{n^{4k+1}}{1+e^{n\pi}} = \frac{2^{4k+1}-1}{8k+4} B_{4k+2}.$$

□



## Chapter 2: The modular group and modular functions

In these exercises,  $\Gamma$  denotes the modular group,  $S$  and  $T$  denote its generators  $S(\tau) = -\frac{1}{\tau}$ ,  $T(\tau) = \tau + 1$ , and  $I$  denotes the identity element.

### Exercise 2.2.

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

*Proof.*

(1)  $n = 3$ .

(2) Write

$$ST = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

So

$$(ST)^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix},$$

$$(ST)^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = I \in \Gamma.$$

Here we identify each matrix with its negative, since both of them represent the same transformation.

□

## Congruence subgroups

The modular group  $\Gamma$  has many subgroups of special interest in number theory. The following exercises deal with a class of subgroups called **congruence** subgroups. Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

be two unimodular matrices. (In this discussion we do not identify a matrix with its negative.) If  $n$  is a positive integer write

$$A \equiv B \pmod{n} \text{ whenever } a \equiv \alpha, b \equiv \beta, c \equiv \gamma \text{ and } d \equiv \delta \pmod{n}.$$

This defines an equivalence relation with the property that

$$A_1 \equiv A_2 \pmod{n} \text{ and } B_1 \equiv B_2 \pmod{n}$$

implies

$$A_1 B_1 \equiv A_2 B_2 \pmod{n} \text{ and } A_1^{-1} \equiv A_2^{-1} \pmod{n}.$$

Hence

$$A \equiv B \pmod{n} \text{ if, and only if, } AB^{-1} \equiv I \pmod{n},$$

where  $I$  is the identity matrix. We denote by  $\Gamma^{(n)}$  the set of all matrices in  $\Gamma$  congruent modulo  $n$  to the identity. This is called the ***congruence subgroup of level  $n$*** .

Prove each of the following statements:

**Exercise 2.11.**

$\Gamma^{(n)}$  is a subgroup of  $\Gamma$ . Moreover, if  $B \in \Gamma^{(n)}$  then  $A^{-1}BA \in \Gamma^{(n)}$  for every  $A$  in  $\Gamma$ . That is,  $\Gamma^{(n)}$  is a normal subgroup of  $\Gamma$ .

*Proof.*

- (1) Show that  $\Gamma^{(n)}$  is a subgroup of  $\Gamma$ .  $\Gamma^{(n)} \neq \emptyset$  since  $I \in \Gamma^{(n)}$ . Suppose  $A, B \in \Gamma^{(n)}$ , that is,  $A \equiv I \pmod{n}$  and  $B \equiv I \pmod{n}$ . Hence  $AB^{-1} \equiv II^{-1} \equiv I \pmod{n}$  or  $AB^{-1} \in \Gamma^{(n)}$ .
- (2) Show that  $\Gamma^{(n)}$  is normal in  $\Gamma$ . Note that

$$A^{-1}BA \equiv A^{-1}IA \equiv A^{-1}A \equiv I \pmod{n}$$

for every  $B \in \Gamma^{(n)}$  and  $A$  in  $\Gamma$ . Hence  $A^{-1}BA \in \Gamma^{(n)}$ .

□

**Exercise 2.12.**

The quotient group  $\Gamma/\Gamma^{(n)}$  is finite. That is, there exist a finite number of elements of  $\Gamma$ , say  $A_1, \dots, A_k$ , such that every  $B$  in  $\Gamma$  is representable in the form

$$B = A_i B^{(n)} \text{ where } 1 \leq i \leq k \text{ and } B^{(n)} \in \Gamma^{(n)}.$$

The smallest such  $k$  is called the index of  $\Gamma^{(n)}$  in  $\Gamma$ .

*Proof.*

- (1) Consider the exact sequence

$$1 \rightarrow \Gamma^{(n)} \rightarrow SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow 1.$$

The surjectivity of the residue class map is proved in Exercise 2.14.

(2) Hence  $\Gamma/\Gamma^{(n)} \cong SL_2(\mathbb{Z}/n\mathbb{Z})$  is a finite group.

□

**Exercise 2.13.**

*The index of  $\Gamma^{(n)}$  in  $\Gamma$  is the number of equivalence classes of matrices modulo  $n$ .*

*Proof.* The index is the number of all cosets of  $\Gamma/\Gamma^{(n)} = |SL_2(\mathbb{Z}/n\mathbb{Z})|$  (by Exercise 2.12). □

*The following exercises determine an explicit formula for the index.*

**Exercise 2.14.**

*Given integers  $a, b, c, d$  with  $ad - bc \equiv 1 \pmod{n}$ , there exist integers  $\alpha, \beta, \gamma, \delta$  such that  $\alpha \equiv a, \beta \equiv b, \gamma \equiv c$  and  $\delta \equiv d \pmod{n}$  with  $\alpha\delta - \beta\gamma = 1$ .*

It is equivalent to show that the residue class map

$$SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/n\mathbb{Z})$$

is surjective.

*Proof.*

(1) Might assume  $a \neq 0$ . Suppose  $a = 0$ , we can lift

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

from  $SL_2(\mathbb{Z}/n\mathbb{Z})$  to  $SL_2(\mathbb{Z})$  (where  $b \neq 0$ ) by the following proof, say

$$\begin{pmatrix} \beta & -\alpha \\ \delta & -\gamma \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Thus

$$\begin{pmatrix} \beta & -\alpha \\ \delta & -\gamma \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

is our desired.

(2) Since  $ad - bc \equiv 1 \pmod{n}$ , there is an integer  $s \in \mathbb{Z}$  such that

$$ad - bc + sn = 1.$$

Note that  $a \neq 0$  and  $\gcd(a, b, n) = 1$ . Take

$$t = \prod_{\substack{p|a \\ p \nmid b}} p$$

where  $p$  is a prime factor of  $a$ . (We take  $t = 1$  if  $a = \pm 1$ .)

- (3) Hence  $\gcd(a, b + tn) = 1$  by the construction of  $t$  and  $\gcd(a, b, n) = 1$ . So 1 is a linear combination of  $a$  and  $b + tn$ . In particular, there exist  $u, v \in \mathbb{Z}$  such that

$$ua - v(b + tn) = s + tc.$$

Define

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a & b + tn \\ c + vn & d + un \end{pmatrix}.$$

- (4) Therefore  $\alpha \equiv a, \beta \equiv b, \gamma \equiv c$  and  $\delta \equiv d \pmod{n}$  and

$$\begin{aligned} \det \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} &= \det \begin{pmatrix} a & b + tn \\ c + vn & d + un \end{pmatrix} \\ &= a(d + un) - (b + tn)(c + vn) \\ &= \underbrace{(ad - bc + sn)}_{=1} + \underbrace{(au - (b + tn)v - s - ct)n}_{=0} \\ &= 1. \end{aligned}$$

□

### Exercise 2.15.

If  $\gcd(m, n) = 1$  and  $A \in \Gamma$  there exists  $\bar{A} \in \Gamma$  such that

$$\bar{A} \equiv A \pmod{n}, \quad \bar{A} \equiv I \pmod{m}.$$

*Proof.*

- (1) Suppose

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{Z}/mn\mathbb{Z}).$$

- (2) First we solve  $\alpha$  in the system of equations

$$\begin{cases} \alpha \equiv a \pmod{n} \\ \alpha \equiv 1 \pmod{m} \end{cases}$$

The chinese remainder theorem guarantees that  $\alpha$  exists. Similarly,  $\beta, \gamma$  and  $\delta$  exist.

- (3) Note that  $\det(B) \equiv 1 \pmod{n}$  and  $\det(B) \equiv 1 \pmod{m}$ . Hence  $\det(B) \equiv 1 \pmod{mn}$  by the Chinese remainder theorem. That is,  $B \in \Gamma^{(mn)}$ . By Exercise 2.14, we can lift  $B \in \Gamma^{(mn)}$  to some  $\bar{A} \in \Gamma$ .

□

**Supplement 2.15.1. (Chinese remainder theorem)**

(Exercise I.3.5 in the textbook: *Jürgen Neukirch, Algebraic Number Theory*.)  
*The quotient ring  $\mathcal{O}/\mathfrak{a}$  of a Dedekind domain by an ideal  $\mathfrak{a} \neq 0$  is a principal ideal domain. (Hint: For  $\mathfrak{a} = \mathfrak{p}^n$  the only proper ideals of  $\mathcal{O}/\mathfrak{a}$  are given by  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ . Choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  and show that  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$ .)*

*Proof.*

- (1) By the Chinese remainder theorem, it suffices to show the case  $\mathfrak{a} = \mathfrak{p}^n$  where  $\mathfrak{p}$  is prime.
- (2) There is a natural correspondence between

$$\{\text{ideals of } \mathcal{O}/\mathfrak{p}^n\} \longleftrightarrow \{\text{ideals of } \mathcal{O} \text{ containing } \mathfrak{p}^n\}.$$

Hence the proper ideals of  $\mathcal{O}/\mathfrak{p}^n$  are given by  $\mathfrak{p}/\mathfrak{p}^n, \dots, \mathfrak{p}^{n-1}/\mathfrak{p}^n$ .

- (3) Similar to Exercise I.3.4, choose  $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$  and thus  $\mathfrak{p}^\nu = \mathcal{O}\pi^\nu + \mathfrak{p}^n$  ( $\nu = 1, \dots, n-1$ ) since they have the same prime factorization. Hence  $\mathfrak{p}^\nu/\mathfrak{p}^n = (\pi^\nu + \mathfrak{p}^n)$  is principal.

□

**Exercise 2.16.**

*Let  $f(n)$  denote the number of equivalence classes of matrices modulo  $n$ . The  $f$  is a multiplicative function.*

*Proof.*

- (1) Exercise 2.20 shows everything.
- (2) Or use the same proof in Exercise 2.15. Suppose  $\gcd(m, n) = 1$  and it is equivalent to show  $f(mn) = f(m)f(n)$ . Define a natural group homomorphism

$$\alpha : SL_2(\mathbb{Z}/mn\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/m\mathbb{Z}) \times SL_2(\mathbb{Z}/n\mathbb{Z}).$$

$\alpha$  is well-defined. So it suffices to show that  $\alpha$  is an isomorphism.

- (3) Both the injectivity and the surjectivity are guaranteed the chinese remainder theorem. Hence  $\alpha$  is isomorphic.

□

**Exercise 2.17.**

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

$$ax - by \equiv 1 \pmod{n}$$

has exactly  $n$  solutions, distinct congruent modulo  $n$ . (A solution is an ordered pair  $(x, y)$  of integers.)

*Proof.*

- (1) No idea.

□

**Exercise 2.18.**

For each prime  $p$  the number of solutions, distinct modulo  $p^r$ , of all possible congruences of the form

$$ax - by \equiv 1 \pmod{p^r}, \text{ where } \gcd(a, b, p) = 1$$

is equal to  $f(p^r)$ .

*Proof.* Note that  $\gcd(a, b, p^r) = \gcd(a, b, p) = 1$ . So the number of is exactly the same as  $|SL_2(\mathbb{Z}/p^r\mathbb{Z})| = f(p^r)$ . □

**Exercise 2.19.**

If  $p$  is the number of pairs of integers  $(a, b)$ , incongruent modulo  $p^r$ , which satisfy the condition  $\gcd(a, b, p) = 1$  is  $p^{2r-2}(p^2 - 1)$ .

*Proof.*

- (1) The number is

$$\sum_{d|p^r} \mu(d) \left( \frac{p^r}{d} \right)^2 = p^{2r} \sum_{d|p^r} \frac{\mu(d)}{d^2} = p^{2r} \left( 1 - \frac{1}{p^2} \right) = p^{2r-2}(p^2 - 1)$$

by the definition of the Möbius function  $\mu$ .

(2) In particular,  $f(p^r) = p^r \cdot p^{2r-2}(p^2 - 1) = p^{3r-2}(p^2 - 1)$ .

□

**Exercise 2.20.**

$f(n) = n^3 \sum_{d|n} \frac{\mu(d)}{d^2}$ , where  $\mu$  is the Möbius function.

*Proof.*

(1)

$$\begin{aligned} f(n) &= |SL_2(\mathbb{Z}/n\mathbb{Z})| \\ &= n |\{(a, b) \pmod{n} : \gcd(a, b, n) = 1\}| && \text{(Exercise 2.17)} \\ &= n \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)^2 && \text{(Inclusion-exclusion principle)} \\ &= n^3 \sum_{d|n} \frac{\mu(d)}{d^2}. \end{aligned}$$

(2) Since  $n \mapsto \frac{1}{n^2}$  is multiplicative, Theorem 2.18 in the textbook: *T. M. Apostol, Introduction to Analytic Number Theory* shows that

$$\sum_{d|n} \frac{\mu(d)}{d^2} = \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

Hence we can also write

$$f(n) = n^3 \sum_{d|n} \frac{\mu(d)}{d^2} = n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right).$$

(3) In particular,  $f$  is a multiplicative function (Exercise 2.16).

(4) Or we can use Exercises 2.16 and 2.19 to show

$$f(n) = n^3 \prod_{p|n} \left(1 - \frac{1}{p^2}\right) = n^3 \sum_{d|n} \frac{\mu(d)}{d^2}.$$

□

*Note.* See “ProjectEuler 193: Squarefree Numbers” for the same trick. The answer should be

$$\sum_{d=1}^{\sqrt{n}} \mu(d) \left\lfloor \frac{n}{d^2} \right\rfloor.$$