Due Date: 15 May 2013, Wednesday NAME:..

Ali Sinan Sertöz STUDENT NO:..

Math 504 Complex Analysis II – Take-Home Exam 09 – Solutions

1	2	3	4	5	TOTAL
100	0	0	0	0	100

Please do not write anything inside the above boxes!

Write your name on top of every page. Show your work in reasonable detail.

NAME: STUDENT NO:

Q-1) Find the index of $\Gamma(n)$ in Γ.

[page 317, Exercise 6L]

Solution:

Let $n \geq 2$ be an integer and $Z_n = \{0, 1, 2, \ldots, n-1\}$ be endowed with the addition and multiplication $\mod n$, making it a ring. Let

$$R_n = \{(a, b) \in Z_n \times Z_n\}.$$

We want to count the number of pairs $(a, b) \in R_n$ such that $\gcd(a, b, n) = 1$.

There are n^2 pairs in R_n. Let $p_1, \ldots, p_r$ be the list of distinct prime factors of n. There are $\dfrac{n}{p_1}$ integers in Z_n which are divisible by p_1, giving us $\dfrac{n^2}{p_1^2}$ pairs $(a, b) \in R_n$ whose greatest common divisor is divisible by p_1. Thus we have

$$n^2 - \frac{n^2}{p_1^2} = n^2 \left(1 - \frac{1}{p_1^2}\right)$$

pairs $(a, b) \in R_n$ with $\gcd(p_1, \gcd(a, b)) = 1$. Arguing in exactly the same way we see that $\dfrac{1}{p_2^2}$ of these pairs have their greatest common divisor divisible by p_2, and we have

$$n^2 \left(1 - \frac{1}{p_1^2}\right) \left(1 - \frac{1}{p_2^2}\right)$$

pairs $(a, b) \in R_n$ with $\gcd(p_i, \gcd(a, b)) = 1$ for $i = 1, 2$. Continuing in this way we see that there are

$$n^2 \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^2}\right)$$

pairs $(a, b) \in R_n$ such that $gcd(a, b)$ is not divisible by any of the primes dividing n. Hence this is the number we are looking for.

Let

$$R'_n = \{(a, b) \in Z_n \times Z_n \mid \gcd(a, b, n) = 1\}.$$

We just showed that

$$\#R'_n = n^2 \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^2}\right),$$

where p_i are the distinct primes dividing n.

We claim that for every pair $(a, b) \in R'_n$, there exist exactly n pairs $(c, d) \in R_n$ such that $ad - bc \equiv 1 \mod n$.

First we show that if $\gcd(a, b, n) = 1$, then there exists at least one pair $(c, d) \in R_n$ such that $ad - bc \equiv 1 \mod n$. For this note that since $\gcd(a, b, n) = 1$, then there exist integers α, β, γ such that $\alpha a + \beta b + \gamma n = 1$. Write $\alpha = d + \alpha_1 n$ and $\beta = -c + \beta_1 n$ for some integers α_1 and β_1 where

c and d are integers with $0 \le c, d < n$. Putting these new expressions for α and β into the above equation for 1 we get $ad - bc \equiv 1 \mod n$.

Next we show that there are n such solutions. Let $(c, d) \in R_n$ be a solution whose existence we just proved. Let $(c_t, d_t) \in R_n$ be defined as $c_t \equiv c + ta \mod n$ and $d_t \equiv d + tb \mod n$, for $t = 0, 1, \dots, n-1$. Then it is clear that $ad_t - bc_t \equiv 1 \mod n$ for all $t = 0, 1, \dots, n-1$. We show that these solutions are all distinct. Assume that $(c_t, d_t) = (c_s, d_s) \in R_n$. This gives

$$a(t-s) \equiv 0 \mod n, \text{ and } b(t-s) \equiv 0 \mod n.$$

If p is a prime dividing n, then

$$p|a(t-s), \text{ and } p|b(t-s).$$

If $p|a$, then $p \not| b$ so $p|(t-s)$. If $p \not| a$, then $p|(t-s)$. This shows that $n|(t-s)$. But as $0 \le t, s < n$, we have $t = s$. This shows that we have at least n distinct solutions.

Now we show that any solution is of this form. Let $(c, d) \in R_n$ be a solution to $ad - bc \equiv 1 \mod n$. Since $(c, d) \neq (0, 0)$, we may without loss of generality assume that $d \neq 0$. Let $(x, y) \in R_n$ be another solution. Then we have

$$\begin{pmatrix} d & -c \\ y & -x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1+kn \\ 1+wn \end{pmatrix},$$

where k and w are some integers. If the coefficient matrix is not invertible, then by bringing it to echelon form we get the second row zero which means $x = yc/d$. Using this value of x we find

$$1 + wn = ay - b\frac{yc}{d} = a\frac{yd}{d} - b\frac{yc}{d} = \frac{y}{d}(ad - bc),$$

from which we get

$$d - y \equiv 0 \mod n.$$

Since $0 \le d, y < n-1$, we have $d = y$, and hence $x = c$. This shows that if (x, y) is a different solution, then the coefficient matrix is invertible. Let Δ be its determinant. Multiplying both sides by the inverse of the coefficient matrix we get

$$\begin{pmatrix} a \\ b \end{pmatrix} = \frac{1}{\Delta} \begin{pmatrix} -x & c \\ -y & d \end{pmatrix} \begin{pmatrix} 1+kn \\ 1+wn \end{pmatrix},$$

and hence

$$\begin{pmatrix} \Delta\, a \\ \Delta\, b \end{pmatrix} = \begin{pmatrix} c - x + un \\ d - y + vn \end{pmatrix},$$

for some integers u and v. From these we see that

$$x \equiv c + ta \mod n, \text{ and } y \equiv d + tb \mod n,$$

as claimed. Hence the above n solutions are all the solutions.

Next we show that for every $(a, b) \in R_n$, if $\gcd(a, b, n) = m > 1$, then there exists no pair $(c, d) \in R_n$ with $ad - bc \equiv 1 \mod 1$. Assume to the contrary that there is a pair $(c, d) \in R_n$ such that $ad - bc = 1 + kn$ for some integer k. Since m divides each of a, b, n, we have $ad - bc \equiv 0 \mod m$ and $1 + kn \equiv 1 \mod m$. This is a contradiction, proving our claim.

Putting these together we see that

$$\#SL(2, Z_n) = n \cdot \#R'_n = n^2 \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^2}\right),$$

where p_i are the distinct primes dividing n. Since

$$PSL(2, Z_n) \cong SL(2, Z_n)/\{\pm I\},$$

where I is the identity matrix, the cardinality of $PSL(2, Z_n)$ is half the above number when $n > 2$. When $n = 2$, there is no difference between I and $-I$, so $PSL(2, Z_n) \cong SL(2, Z_n)$, and we do not need to divide by 2 in the above formula. Without dividing by 2 the formula gives 6 as the cardinality when $n = 2$. Thus we have the result

$$\#PSL(2, Z_n) = |\Gamma : \Gamma(n)| = \begin{cases} 6 & \text{if } n = 2, \\ \dfrac{n^3}{2} \displaystyle\prod_{i=1}^{r} \left(1 - \frac{1}{p_i^2}\right), & \text{if } n > 2 \end{cases}$$

where p_i are the distinct primes dividing n.