Number theory: Final Exam

Due on June 13, 2023 at 3:10pm

Professor J Section A

V **U**

Problem 1

Prove that 2 is primative root of mod 11.

Solution

Note that the set of $\{2^x\}$ for $x \in \{1, 2, \cdots, 11\}$ is

2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
2	4	8	5	10	9	7	3	6	1	2

which is exactly $\{1, 2, \cdots, 10\}$ Thus by definition of primative root, the 2 is primative root of mod 11.

□

Problem 2

Suppose p and q are primes, $p = 4q + 1$. Prove that q is not a primitive root (mod p).

Solution:

By Law of Quadratic Reciprocity

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = (-1)^{q(q-1)} = 1 \tag{1}$$

And the fact that

$$p = 4q + 1 \equiv 1^2 \mod q \implies \left(\frac{p}{q}\right) = 1 \tag{2}$$

We have that

$$\left(\frac{q}{p}\right) = 1, \tag{3}$$

which means there exists x such that $q = x^2 \mod p$

Thus by fermat little theorem,

$$q^{\frac{p-1}{2}} = x^{p-1} \equiv 1 \mod p \tag{4}$$

Hence q's order is not $p - 1$, and therefore q is *not* primitive root of p

Problem 3

Suppose p and q are primes, $p = 2q + 1, p \equiv 2 \mod 5$. Prove that 5 is a primitive root (mod p).

Solution

By Law of Quadratic Reciprocity

$$\left(\frac{p}{5}\right)\left(\frac{5}{p}\right) = (-1)^{p-1} = 1 \tag{5}$$

Since $p \equiv 2 \neq x^2 \mod 5$ we have

$$\left(\frac{p}{5}\right) = -1 \tag{6}$$

Thus,

$$\left(\frac{5}{p}\right) = -1 \tag{7}$$

Meaning that $5 \not\equiv x^2 \mod p$. Therefore, we can't have

$$5^{(p-1)/2} = 5^q = 1 \mod p \tag{8}$$

Problem 3 continued on next page. . .

Also we can't have

$$5^2 = 1 \mod p \tag{9}$$

or

$$5 = 1 \mod p \tag{10}$$

Otherwise, we will have $p = 2, 3$ in which cases, $p = 2q + 1$ are not satisfied. Together, by the Fermat Little Theorem,

$$\mathrm{Ord}_p(5) = 2q = p - 1$$

Problem 4

Suppose

$$m1 > 2, m2 > 2, (m_1, m_2) = 1$$

Prove that there is no primitive root (mod $m_1 m_2$).

Solution

Let a be coprime to $m_1 m_2$. By Euler's theorem,

$$a^{\phi(m_1)} = 1 \mod m_1, a^{\phi(m_2)} = 1 \mod m_2$$

Let

$$L := \mathrm{lcm}(\phi(m_1), \phi(m_2))$$

, then $a^L = 1 \mod m_1$ and $a^L = 1 \mod m_2$. Hence

$$a^L = 1 \mod m_1 m_2$$

By definition of ϕ, if $m = p_1^{e_1} \cdots p_k^{e_k} > 2$,

$$\phi(m) = \prod_k p_k^{e_k - 1}(p_k - 1)$$

is apparently even.

Thus,

$$L \le \phi(m_1)\phi(m_2)/2 = \phi(m_1 m_2)/2 < \phi(m_1 m_2)$$

Apparently, a is not a primitive root. Since a is randomly chosen, we come to conclude that $\mod m_1 m_2$ has no primitive root.

Problem 5

Let $\Lambda(n)$ be given by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \geq 1 \\ 0 & \text{otherwise} \end{cases}$$

where p denotes a prime. It is known that

$$\sum_{n \leq x} \Lambda(n) \left[\frac{x}{n}\right] = \sum_{n \leq x} \log(n) \tag{11}$$

Let

$$\Psi(x) = \sum_{n \leq x} \Lambda(n) \tag{12}$$

(i) Prove that

$$\sum_{n \leq x} \log(n) = x \log(x) - x + O(\log(x))$$

(ii) Prove that

$$\sum_{n \leq x} \Psi\left(\frac{x}{n}\right) = \sum_{n \leq x} \Lambda(x) \left[\frac{x}{n}\right]$$

Solution

By Stirling's approximation, we have

$$\begin{aligned} \sum_{n \leq x} \log(n) &= \int_0^x \log(x) dx + O(\log(x)) \\ &= x \log(x) - x + O(\log(x)) \end{aligned}$$

For (ii), we have

$$\begin{aligned} \sum_{n \leq x} \Psi\left(\frac{x}{n}\right) &= \sum_{n \leq x} \sum_{m \leq x/n} \Lambda(m) \\ &= \sum_{m \leq x} \Lambda(m) \sum_{n \leq x/m} 1 \\ &= \sum_{m \leq x} \Lambda(m) \left[\frac{x}{m}\right] \\ &= \sum_{n \leq x} \Lambda(x) \left[\frac{x}{n}\right] \end{aligned}$$

$\square$

Problem 6

Prove that

$$\sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) = x\log(2) + O(\log(x)) \text{ if } x \geq 4 \tag{13}$$

Note that $\Psi(y) = 0$ if $0 < y \leq 1$. The left side of (5) is equal to

$$\sum_{n\leq x} \Psi\left(\frac{x}{n}\right) - 2\sum_{n\leq x/2} \Psi\left(\frac{x}{2n}\right)$$

Thus applying (4), we have

$$\begin{aligned}\sum_{n\leq x} \Psi\left(\frac{x}{n}\right) - 2\sum_{n\leq x/2} \Psi\left(\frac{x}{2n}\right) &= x\log(x) - x + O(\log(x)) - 2\left(\frac{x}{2}\log\left(\frac{x}{2}\right) - \frac{x}{2} + O(\log(x))\right) \\ &= x\log(2) + O(\log(x))\end{aligned}$$

Problem 7

Prove that

$$\sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) \leq \Psi(x) \tag{14}$$

and

$$\sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) \geq \Psi(x) - \Psi\left(\frac{x}{2}\right) \tag{15}$$

Solution

For (6), we have

$$\begin{aligned}\sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) &= \Psi(x) + \Psi\left(\frac{x}{2}\right) + \Psi\left(\frac{x}{3}\right) + \cdots - 2\left\{\Psi\left(\frac{x}{2}\right) + \Psi\left(\frac{x}{3}\right)\cdots\right\} \\ &= \left\{\Psi(x) - \Psi\left(\frac{x}{2}\right)\right\} + \left\{\Psi\left(\frac{x}{3}\right) - \Psi\left(\frac{x}{4}\right)\right\} + \cdots\end{aligned}$$

Note that $\Psi(y)$ is increasing for $y > 1$, we have

$$\Psi\left(\frac{x}{k}\right) - \Psi\left(\frac{x}{k+1}\right) \geq 0$$

Thus,

$$\sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) \geq \Psi(x) - \Psi\left(\frac{x}{2}\right)$$

For (7), we have

$$\begin{aligned}\sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) &= \Psi(x) + \Psi\left(\frac{x}{2}\right) + \Psi\left(\frac{x}{3}\right) + \cdots - 2\left\{\Psi\left(\frac{x}{2}\right) + \Psi\left(\frac{x}{4}\right)\cdots\right\} \\ &= \Psi(x) - \left\{\Psi\left(\frac{x}{2}\right) - \Psi\left(\frac{x}{3}\right)\right\} - \left\{\Psi\left(\frac{x}{4}\right) - \Psi\left(\frac{x}{5}\right)\right\} - \cdots \\ &\leq \Psi(x)\end{aligned}$$

Problem 8

Conclude that

$$\Psi(x) \geq x\log(2) + O(\log(x)) \tag{16}$$

and

$$\Psi(x) - \Psi\left(\frac{x}{2}\right) \leq x\log(2) + O(\log(x)) \tag{17}$$

SolutionBy (6) and (5)

$$\begin{aligned}\Psi(x) &\geq \sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) \\ &= x\log(2) + O(\log(x))\end{aligned}$$

By (7) and (5)

$$\begin{aligned}\Psi(x) - \Psi\left(\frac{x}{2}\right) &\leq \sum_{n=1}^{\infty} \Psi\left(\frac{x}{n}\right) - 2\sum_{n=1}^{\infty} \Psi\left(\frac{x}{2n}\right) \\ &= x\log(2) + O(\log(x))\end{aligned}$$