18.781, Fall 2007 Problem Set 9

Solutions to Selected Problems

Problem 1 When $x = y$, it is clear that

$$p^{-1}\sum_{t=0}^{p-1}\zeta_p^{t(x-y)} = p^{-1}\sum_{t=0}^{p-1}\zeta_p^0 = p^{-1}\sum_{t=0}^{p-1}1 = 1.$$

Now recall the fact that if α is not 0 in modulo p, then $\{0, \alpha, 2\alpha, \cdots, (p-1)\alpha\}$ is a complete residue system modulo p. Also $a \equiv b \pmod{p}$ implies that $\zeta_p^a = \zeta_p^b$.
Thus, when $x \not\equiv y \pmod{p}$, we have

$$\sum_{t=0}^{p-1}\zeta_p^{t(x-y)} = \sum_{t=0}^{p-1}\zeta_p^t = 0,$$

where the last equality can be verified easily. Therefore, we have

$$p^{-1}\sum_{t=0}^{p-1}\zeta_p^{t(x-y)} = 0$$

.
This gives the desired conclusion. $\square$

Problem 2 We can easily find that

$$\chi(a)g(a,\chi) = \sum_{t=0}^{p-1}\chi(at)\zeta_p^{at} = \sum_{x=0}^{p-1}\chi(x)\zeta_p^x = g(1,\chi)$$

because if a is not 0 in modulo p, then $\{0, a, 2a, \cdots, (p-1)a\}$ is a complete residue system modulo p.

Since $\chi(a)\chi(a^{-1}) = 1$, we have

$$g(a,\chi) = \chi(a^{-1})g(1,\chi).$$

$\square$

Problem 3 (a) The sum is going through $(a, b) = (0, p), (1, 0), (2, p-1), (3, p-2), \cdots, (p-1, 2)$. The number of these is p, hence by the convention of the definition of 1_p, we have $J(1_p, 1_p) = p$.

(b) This is equivalent to prove that $\sum_{t=0}^{p-1} \chi(t) = 0$ for nontrivial character χ. For the nontrivial character χ, there is α $(\in (\mathbb{Z}/p\mathbb{Z})^\times)$ such that $\chi(\alpha) \neq 1$. Then again by the fact that $\{0, \alpha, 2\alpha, \cdots, (p-1)\alpha\}$ is a complete residue system modulo p,

$$\sum_{t=0}^{p-1} \chi(t) = \sum_{t=0}^{p-1} \chi(\alpha t) = \sum_{t=0}^{p-1} \chi(\alpha)\chi(t) = \chi(\alpha) \sum_{t=0}^{p-1} \chi(t).$$

Since $\chi(\alpha) \neq 1$, we should have $\sum_{t=0}^{p-1} \chi(t) = 0$.

(c) (Note: for the nontrivial character $\chi, \chi(0)$ can be regarded as 0.) First, it is easily verified that

When $a, b \in \{2, 3, \cdots, p-1\}$, $a(1-a)^{-1} \equiv b(1-b)^{-1} (\text{mod } p)$ if and only if $a \equiv b$.

Also, $a(1-a)^{-1}$ is not $0, -1$. when $a \in \{2, 3, \cdots, p-1\}$. (For example, $a(1-a)^{-1} \equiv -1$ iff $a \equiv a - 1$, which is impossible.) Therefore, $\{a(1-a)^{-1}\}_{a=2,\cdots,p-1} = \{1, 2, \cdots, p-2\}$. This implies that

$$J(\chi, \chi^{-1}) = \sum_{a=2}^{p-1} \chi(a)\chi^{-1}(1-a) = \sum_{a=2}^{p-1} \chi(a(1-a)^{-1}) = \sum_{a=1}^{p-2} \chi(a) = -\chi(-1),$$

where the last equality holds because of (b).

(d) Write

$$J(\chi, \lambda)g(\chi\lambda) = \sum_{i=0}^{p-1} \chi(i)\lambda(1-i) \sum_{j=0}^{p-1} \chi(j)\lambda(j){\zeta_p}^j = \sum_{j=0}^{p-1}\sum_{i=0}^{p-1} \chi(ij)\lambda(j-ij){\zeta_p}^j = \sum_{j=1}^{p-1}\sum_{i=0}^{p-1} \chi(ij)\lambda(j-ij){\zeta_p}^j.$$

And also, by change of coordinate $(u := s + t, v := s)$, we have

$$g(\chi)g(\lambda) = \sum_{s=0}^{p-1}\sum_{t=0}^{p-1} \chi(s)\lambda(t){\zeta_p}^{s+t} = \sum_{u=0}^{p-1}\sum_{v=0}^{p-1} \chi(v)\lambda(u-v){\zeta_p}^u = \sum_{v=0}^{p-1} \chi(v)\lambda(-v) + \sum_{u=1}^{p-1}\sum_{v=0}^{p-1} \chi(v)\lambda(u-v){\zeta_p}^u$$

Since $\chi \cdot \lambda$ is not a trivial character, we have

$$\sum_{v=0}^{p-1} \chi(v)\lambda(-v) = \lambda(-1) \sum_{v=0}^{p-1} (\chi\lambda)(v) = 0.$$

Therefore, above two summations are same, so we have

$$J(\chi, \lambda)g(\chi\lambda) = g(\chi)g(\lambda)$$

which gives us desired result. $\square$

Problem 4 It is not hard to observe that $\mathbb{Z}/p\mathbb{Z}$ is isomorphic to $R/\pi R$ as a ring, with the isomorphism $f(a) := a$. (Here are some abuses of notation. If a is an element in $\mathbb{Z}$, it can be regarded as an element in $\mathbb{Z}/p\mathbb{Z}$, also since $\mathbb{Z} \in R$, a also can be regarded as an element in $R \to R/\pi R$.)

Therefore, $x^3 \equiv a \pmod{p}$ is solvable in the integers if and only if $x^3 \equiv a \pmod{\pi}$ in R. Now, by the problem 5 in Problem set 8, we can deduce the wanted conclusion. $\square$

Problem 5 It is easy to observe that $2 + 3\omega$ and 11 are primary primes. Therefore we have cubic reciprocity

$$\left(\frac{2+3\omega}{11}\right) = \left(\frac{11}{2+3\omega}\right).$$

This implies that $x^3 \equiv 2 + 3\omega(11)$ is solvable if and only if $x^3 \equiv 11(2 + 3\omega)$ is solvable. By the problem 4, this is equivalent to the existence of integer solution of $x^3 \equiv 11 \pmod{7}$.

By Fermat's theorem, if x is not a multiple of 7, $x^6 \equiv 1 \pmod{7}$, hence $(x^3 - 1)(x^3 + 1) \equiv 0 \pmod{7}$. This gives $x^3 \equiv -1, 0, 1 \pmod{7}$ for any integer x. Thus there is no integer solution of $x^3 \equiv 11 \pmod{7}$, and we can conclude that $x^3 \equiv 2 + 3\omega(11)$ is not solvable. $\square$

Problem 6 For fixed p, define I be the set of quadratic residues in modulo p, and J be the set of non residues. Then we have

$$g(1,p) = \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) {\zeta_p}^t = \sum_{t\in I} \left(\frac{t}{p}\right) {\zeta_p}^t + \sum_{t\in J} \left(\frac{t}{p}\right) {\zeta_p}^t = \sum_{t\in I} {\zeta_p}^t - \sum_{t\in J} {\zeta_p}^t.$$

Since

$$-1 = \sum_{t=1}^{p-1} {\zeta_p}^t = \sum_{t\in I} {\zeta_p}^t + \sum_{t\in J} {\zeta_p}^t,$$

we can have

$$g(1,p) = 1 + 2\sum_{t\in I} {\zeta_p}^t.$$

For any $t \in I$, there are exactly two values a in $\{1, \cdots, p-1\}$ satisfying $a^2 \equiv t \pmod{p}$. This implies that

$$1 + 2\sum_{t\in I} {\zeta_p}^t = 1 + \sum_{a=1}^{p-1} {\zeta_p}^{a^2} = \sum_{t=0}^{p-1} {\zeta_p}^{t^2},$$

so we get the desired conclusion. $\square$

Problem 7

$$\sum_{a=0}^{p-1} \hat{f}(a){\zeta_p}^{at} = p^{-1}\sum_{a=0}^{p-1}\sum_{i=0}^{p-1} f(i){\zeta_p}^{-ai}{\zeta_p}^{at} = p^{-1}\sum_{i=0}^{p-1}\sum_{a=0}^{p-1} f(i){\zeta_p}^{a(t-i)} = \sum_{i=0}^{p-1} f(i)\left(p^{-1}\sum_{a=0}^{p-1} {\zeta_p}^{a(t-i)}\right)$$

By the problem 1, the last summation is equal to

$$\sum_{i=0}^{p-1} f(i)\delta(i,t) = f(t),$$

as desired. $\square$

If you have any question, please contact me : Yoonsuk Hyun (yshyun@math.mit.edu)