MA40238 NUMBER THEORY (2014/15 SEMESTER 1)
BRIEF SOLUTIONS TO 2012/13 EXAM
CHRISTMAS EDITION

Brief solutions to some problems in 2012/13 exams are provided. The numbers to definitions, propositions, theorems and exercises refer to the lecture notes posted on the unit webpage.

Problem 1.

(a) Omitted.

(b) See Definition 1.6.

(c) See Definition 1.20.

(d) See Proposition 1.21.

(e) See Theorem 1.26.

(f) We prove the first equation. For each element $\frac{h}{n}$ in the left-hand side, we can cancel the highest common factor in the numerator and denominator to get a fraction $\frac{a}{d}$. It is clear that $d \mid n$. Since a and d has no common factor larger than 1, we get $\mathrm{hcf}(a, d) = 1$. The condition $1 \leqslant h \leqslant n$ implies $0 < \frac{h}{n} \leqslant 1$, which can also be written as $0 < \frac{a}{d} \leqslant 1$, hence $1 \leqslant a \leqslant d$. Therefore $\frac{a}{d}$ is an element in the right-hand side.

Conversely, for each element $\frac{a}{d}$ in the right-hand side, since $d \mid n$, we can write $n = md$ for some positive integer m. We write $h = ma$, then $\frac{a}{d} = \frac{ma}{md} = \frac{h}{n}$. The condition $1 \leqslant a \leqslant d$ implies $0 < \frac{a}{d} \leqslant 1$, which can also be written as $0 < \frac{h}{n} \leqslant 1$, hence $1 \leqslant h \leqslant n$. Therefore $\frac{h}{n}$ is an element in the left-hand side.

To prove the second equation, we notice that the left-hand side is the sum of values of the function F at the numbers in the set $\left\{\frac{h}{n} \mid 1 \leqslant h \leqslant n\right\}$, while the right-hand side is the sum of values of the same function F at the numbers in the set $\bigcup_{d \mid n} \left\{\frac{a}{d} \mid 1 \leqslant a \leqslant d, \mathrm{hcf}(a, d) = 1\right\}$. Since the two sets are equal, the two sides are sums of values of F at the same points, therefore are also equal.

(g) To apply the formula

$$\sum_{1 \leqslant h \leqslant n} F\left(\frac{h}{n}\right) = \sum_{d \mid n} \sum_{\substack{1 \leqslant a \leqslant d \\ \mathrm{hcf}(a,d)=1}} F\left(\frac{a}{d}\right)$$

Date: December 7, 2014.

provided in part (f), we need to compute both sides. We start with the right-hand side. Since $F(x) = e^{2\pi imx}$, we know from the definition of $c_n(m)$ that

$$c_n(m) = \sum_{\substack{1 \leqslant h \leqslant n \\ \mathrm{hcf}(h,n)=1}} F\left(\frac{h}{n}\right).$$

We replace h and n by a and d respectively, then we get

$$c_d(m) = \sum_{\substack{1 \leqslant a \leqslant d \\ \mathrm{hcf}(a,d)=1}} F\left(\frac{a}{d}\right).$$

Therefore we have

$$\sum_{d \mid n} \sum_{\substack{1 \leqslant a \leqslant d \\ \mathrm{hcf}(a,d)=1}} F\left(\frac{a}{d}\right) = \sum_{d \mid n} c_d(m).$$

We then compute $\sum_{1 \leqslant h \leqslant n} F\left(\frac{h}{n}\right)$. For simplicity, we write this expression as $f(n)$. We consider two cases separately as follows.

If $n \mid m$, then for each h, $\frac{mh}{n}$ is an integer. Hence

$$f(n) = \sum_{1 \leqslant h \leqslant n} F\left(\frac{h}{n}\right) = \sum_{1 \leqslant h \leqslant n} e^{\frac{2\pi imh}{n}} = \sum_{1 \leqslant h \leqslant n} 1 = n.$$

If $n \nmid m$, using the formula for the sum of geometric series, we have

$$f(n) = \sum_{1 \leqslant h \leqslant n} F\left(\frac{h}{n}\right) = \sum_{1 \leqslant h \leqslant n} e^{\frac{2\pi imh}{n}} = e^{\frac{2\pi im}{n}} \cdot \frac{1 - e^{2\pi im}}{1 - e^{\frac{2\pi im}{n}}} = 0.$$

By the formula proved in part (f), we get

$$f(n) = \sum_{d \mid n} c_d(m).$$

By Möbius Inversion Theorem, we have

$$c_n(m) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) f(d).$$

Since $f(d) = d$ when $d \mid m$ and $f(d) = 0$ when $d \nmid m$, we get

$$c_n(m) = \sum_{\substack{d \mid n \\ d \mid m}} \mu\left(\frac{n}{d}\right) d,$$

as required.

Problem 2.

(a) See Definition 4.2.

(b) See Proposition 4.4 (1) and Proposition 4.5 (1).

(c) See Lemma 5.1.

(d) See Exercise 5.1 (2).

(e) See Definition 4.9. Please be noted that our definition of the Jacobi symbol requires slightly different assumptions on a and b. This issue is due to the inconsistency in literatures. Please stick to our definition (the one given in lecture notes.)

(f) See Proposition 4.14.

(g) Since $441 \equiv 1 \pmod 4$, by quadratic reciprocity, we have $(\frac{441}{1003}) = (\frac{1003}{441}) = (\frac{121}{441}) = (\frac{441}{121}) = (\frac{78}{121}) = (\frac{2}{121})(\frac{39}{121}) = (\frac{39}{121})$ where the last equality is due to $121 \equiv 1 \pmod 8$. Realising $121 \equiv 1 \pmod 4$, by quadratic reciprocity, we have $(\frac{39}{121}) = (\frac{121}{39}) = (\frac{4}{39}) = 1$. Therefore the original Legendre symbol $(\frac{441}{1003}) = 1$.

Problem 3.

(a) See Definition 9.10. Please be noted that we defined these notions only for subsets of $\mathbb{R}^2$, but the same definition applies to subsets of $\mathbb{R}^n$ for any n.

(b) See Theorem 9.11.

(c) See Exercise 10.2.

(d) See Definition 7.12, Definition 9.1, Definition 9.3, Proposition 7.14.

(e) For the first question, see Proposition 10.3.

For the quadratic field $K = \mathbb{Q}(\sqrt{-7})$, we have the discriminant $\Delta_K = -7$ and the Minkowski bound $M_K = \frac{2}{\pi}\sqrt{7} < 2$. Hence each ideal class contains an ideal of norm 1. Since the only ideal in $\mathcal{O}_K$ of norm 1 is $\mathcal{O}_K$ itself, we conclude that there is only one ideal class; i.e. $h_K = 1$. We proved in lectures that $h_K = 1$ iff $\mathcal{O}_K$ is a PID, hence $\mathcal{O}_K$ is a PID. We also proved in lectures that every PID is a UFD, hence $\mathcal{O}_K$ is also a UFD; i.e. the ring of integers in $\mathbb{Q}(\sqrt{-7})$ is a unique factorisation domain.

Problem 4.

Omitted.