HW 7

When I refer to specific theorem numbers, they’re from the book “Elementary Number Theory” by Jones and Jones, published by Springer. I sometimes use the shorthand CRT for the Chinese Remainder Theorem. I use the notation $\mathbb{Z}_n$ for the integers mod $n$, and $U_n = (\mathbb{Z}_n)^*$ for the group of units. Please let me know if there are any typos or mistakes by emailing arjun-at-cims-dot-nyu-dot-edu.

Problem 1. Let $n = p_1^{a_1} \ldots p_k^{a_k}$ and $m = q_1^{b_1} \ldots q_j^{b_j}$ be coprime numbers. Clearly,

$$f(nm) = \prod_{i=1}^{k} (-1)^{a_i} \prod_{r=1}^{j} (-1)^{b_j},$$

from which it follows that $f$ is multiplicative. By Lemma 8.1 in J & J,

$$h(n) = \sum_{d \mid n} f(d),$$

is also a multiplicative function.

The function $g(n)$ is also multiplicative: if $n$ and $m$ are coprime, $n \cdot m$ is a square iff both $n$ and $m$ are squares. This follows from inspecting the prime decomposition of $n$ and $m$.

To show that $h(n) = g(n) \forall n$, it is enough to show that it is true when $n$ is a prime power, since $h$ and $g$ are multiplicative functions (see Lemma 8.5 in J & J). For any prime $p$,

$$h(p^e) = \sum_{i=0}^{e} (-1)^i = \begin{cases} 0 & e \text{ odd} \\ 1 & e \text{ even} \end{cases},$$

since there are $e + 1$ alternating $+1$ and $-1$ entries in the sum. $p^e$ is a square iff $e$ is even, and this implies that $g$ agrees with $h$.

Problem 2. If $n = p_1^{a_1} \ldots p_k^{a_k}$, Theorem 8.5 of J&J says that

$$\mu(n) = \begin{cases} 0 & \text{if some } a_i > 1 \\ (-1)^k & \text{if all } a_i = 1 \end{cases}.$$ 

If $d$ is a divisor of $n$, it follows that $|\mu(d)| = 1$ iff $d$ is a product of distinct primes. There are $k$ primes in the prime factorization of $n$, and a product of any $r$ of these primes for $0 \leq r \leq k$ produces a divisor $d$ of $n$ for which $|\mu(d)| = 1$. For each $r$, there are $\binom{k}{r}$ distinct divisors that are a product of $r$ primes. So we must have,

$$\sum_{d \mid n} |\mu(d)| = \sum_{r=0}^{k} \binom{k}{r} = (1 + 1)^k,$$

where the last equality follows from the binomial theorem. The proof is similar to Theorem 8.8 in J&J.
Problem 3. Writing out the definitions, we see that

\[
D(n) = F_1 \mod 4(n) - F_3 \mod 4(n) = \sum_{d \mid n} f_1 \mod 4(d) - f_3 \mod 4(d).
\]

To show that \(D(n)\) is multiplicative, it’s clear from Lemma 8.1 that it’s enough to show that \(h(n) = f_1 \mod 4 - f_3 \mod 4(n)\) is multiplicative. This is just a matter of enumerating cases. Consider \(n \) and \(m\) coprime and notice that \(h(n)\) can take the values 1, \(-1\), or 0 depending on whether \(n\) is 1 mod 4, 3 mod 4 or 0 mod 2 respectively.

If either \(n\) or \(m\) is \(2\) or 0 mod 4, it’s clear that \(nm\) is \(2\) or 0 mod 4. Conversely, if \(nm\) is 2 or 0 mod 4, it means that at least one of \(n\) or \(m\) is 2 or 0 mod 4. Then, \(h(nm) = 0\) iff \(h(n)\) or \(h(m)\) = 0.

We may now assume that both \(n\) and \(m\) are \(1\) or \(3\) mod 4. Suppose \(h(n) = h(m) = \pm 1\); that is, they’re both of the form \(1\) mod 4 or \(3\) mod 4. Then, \(h(n)h(m) = 1\). Then, it follows from the basic rules for congruences that \(nm = 1\) mod 4 and hence \(h(nm) = 1\).

For the final case, assume \(n = 1\) mod 4 and \(m = 3\) mod 4. Then, \(nm = 3\) mod 4 and it follows that \(h(nm) = -1 = h(n)h(m)\). Since we’ve enumerated all cases and shown that \(h\) is multiplicative, we’re done.

Problem 4.

Part (a): For each solution \((x, y)\), let \(\alpha = x + iy\). This is a bijection from the solutions of \(x^2 + y^2 = n\) to the Gaussian integers such that \(|\alpha|^2 = n\): \(|\alpha|^2 = n\) iff \(x^2 + y^2 = n\).

Part (b): Let us say that \(\alpha\) is a solution to \(n\) if \(|\alpha|^2 = n\). There are four solutions associated to \(\alpha\) (through the four units): \(\{\alpha, i\alpha, -i\alpha\ \text{and} \ -\alpha\}\).

Let \(\alpha\) and \(\beta\) be the solutions in \(\mathbb{Z}[i]\) to \(m\) and \(n\) respectively. Then, \(\alpha\beta\) is a solution to \(mn\) since \(|\alpha\beta|^2 = mn\). Each of the four solutions \(\gamma \sim \alpha\) has a corresponding \(\delta \sim \beta\) such that \(\gamma\delta = \alpha\beta\). In other words, four distinct pairs of solutions for \(m\) and \(n\) map to one single solution to \(m \cdot n\). This means that

\[
\frac{1}{4} \square(m) \square(n) \leq \square(mn).
\]

We will show that the map is onto; i.e., that each solution \(\gamma\) to \(mn\) can be decomposed as \(\gamma = \alpha\beta\) to produce four pairs of solutions to \(m\) and \(n\).

Let \(m\) and \(n\) be coprime, and let them have the following prime decompositions in \(\mathbb{Z}\):

\[
m = p_1^{a_1} \cdots p_k^{a_k},
\]

\[
n = q_1^{b_1} \cdots q_j^{b_j}.
\]

As in HW 2 problem 5, we can either decompose each prime as \(p_i = c_i\bar{c}_i\), where \(c_i\) is irreducible, or the prime is irreducible in \(\mathbb{Z}[i]\). The same goes for the primes \(q_i\), and we will decompose them as \(q_i = d_i\bar{d}_i\) if possible. Therefore, rearranging the indices appropriately, we get

\[
mn = p_1^{a_1} \cdots p_k^{a_k} c \bar{c} q_1^{b_1} \cdots q_j^{b_j} d \bar{d},
\]

where \(c = \prod c_i\) and \(d = \prod d_i\). Suppose there is a solution \(\gamma\) to \(mn\), then all the real primes in the decomposition for \(mn\) must be raised to an even power, as we
showed in HW 2 Problem 5. Since the primes $p_i$ and $q_i$ are distinct due to the fact that $m$ and $n$ are coprime, it follows that

$$m = p^2 c \bar{c},$$
$$n = q^2 d \bar{d},$$

where $p = \prod p_i^{a_i}$ and $q = \prod q_i^{b_i}$. It follows that there is a pair of solutions $(\alpha, \beta) = (pc, qd)$. As before, this pair can be turned into 4 distinct pairs by multiplying with units. Hence we have that

\[
\frac{1}{4} \square(m) \square(n) \geq \square(mn),
\]

and we're done.

Part (c): As we discussed in problem 1, we only need to compare $D(n)$ and $\square(n)$ on prime powers. Let us see how $D(n)$ behaves first. Suppose $n = p^e$ for where $p$ is prime, and suppose first that $p = 1$ mod 4. Then,

\[
D(p^e) = F_1 \mod 4(p^e) - F_3 \mod 4(p^e) = (e + 1) - 0 = e + 1.
\]

If $p = 3$ mod 4,

\[
D(p^e) = \begin{cases} 
1 & e \text{ even}, \\
0 & e \text{ odd}.
\end{cases}
\]

Finally, if $n = 2^e$,

\[
D(2^e) = 1
\]

for all $e \geq 1$.

For the $\square$ function, we need to count solutions. If $p = 1$ mod 4, we know it decomposes as $p = c \bar{c}$ in $\mathbb{Z}[i]$ where $c$ and $\bar{c}$ are both irreducibles. There are four such representations, obtained by multiplying $c$ by the units $\{1, -1, i, -i\}$. We'd like to find solutions to $p^e$; i.e., a Gaussian integer $\alpha$ such that $p^e = \alpha \bar{\alpha}$. Uniqueness of the prime decomposition says that each factor of $\alpha$ must be associated to $c$ or $\bar{c}$ (through a unit). Then, $\alpha$ must be a product of $k$ factors associated to $c$ and $j$ factors associated to $\bar{c}$ such that $k + j = e$. That is,

\[
\alpha = uc^k \bar{c}^j,
\]

where $u$ is a unit. There are $e + 1$ combinations $k + j = e$, and 4 possible units $u$. Hence we have a total of $4(e + 1)$ solutions.

If $n = 2^e$, something special happens. 2 decomposes as $2 = (1 + i)(1 - i) = c \bar{c}$. However, $(1+i)^2 = 2i, (1-i)^2 = -2i$ which implies that the products we constructed above only produce certain kinds of elements. If $e$ is even, they produce elements of the form

\[
2^{e/2}u
\]

where $u$ is a unit in $\mathbb{Z}[i]$, and if $e$ is odd, the produce elements of the form

\[
2^{(e-1)/2}u(1 \pm i).
\]

There is further degeneracy since $(1+i) = i(1-i)$; i.e., they’re related through a unit. Hence, we get a total of only 4 solutions for all $e \geq 1$.

We skipped over this earlier, but we must verify that this degeneracy cannot happen for an odd prime power. If any of the solutions $\alpha$ we constructed for primes of the form $p = 1$ mod 4 are non-unique, we must have

\[
c^k \bar{c}^{-k} = uc^j \bar{c}^{-j}
\]
for distinct \( j \) and \( k \). A little manipulation results in the condition
\[
e^{k-j} = u e^{k-j}.
\]

If a complex number and its conjugate are associated to each other through a unit; i.e., \( x + iy = u(x - iy) \), we must have \( x = \pm y \). In particular, this means that
\[
e^{k-j} \bar{e}^{k-j} = 2x^2,
\]
where we assume without loss of generality that \( k > j \). Since
\[
p^e = e^e \bar{e}^e = 2x^2 e^{-(k-j)} \bar{e}^{-(k-j)},
\]
it follows that \( p \) must be divisible by 2. This is contrary to our assumption.

If \( p = 3 \mod 4 \), we know that it does not decompose in \( \mathbb{Z}[i] \). Then, it’s clear there are solutions to \( p^e \) iff \( e \) is even. There are a total of 4 solutions: \((\pm p^{e/2}, 0)\) and \((0, \pm p^{e/2})\).

**Problem 5.** Theorem 7.5 says
\[
\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) \left(\frac{-1}{p}\right).
\]
We know \(-1 \in U_p\) for all primes \( p \), and using Gauss’ lemma (cf. Corollary 7.7), we get that \(-1 \in Q_p\) iff \( p = 1 \mod 4 \). Hence,
\[
\left(\frac{-1}{p}\right) = \begin{cases} 
1 & p = 2 \\
1 & p = 1 \mod 4 \\
-1 & \text{otherwise}
\end{cases}
\]
Since \( 5 = 1 \mod 4 \), quadratic reciprocity gives
\[
\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).
\]
We know that
\[
U_5 = \{1, 2, 3, 4\} \text{ and } Q_5 = \{1, 4\}.
\]
Hence if \( p \neq 5 \),
\[
\left(\frac{p}{5}\right) = \begin{cases} 
1 & p = 1 \mod 5 \text{ or } 4 \mod 5 \\
-1 & \text{otherwise}
\end{cases}.
\]
Combining the two results and using the Chinese remainder theorem, we get that
\[
\left(\frac{-5}{p}\right) = \begin{cases} 
1 & p = 1 \mod 20 \text{ or } 9 \mod 20 \\
-1 & \text{otherwise}
\end{cases}.
\]

**Problem 6.**
Part (a): Using the basic rules of manipulating Legendre symbols,
\[
\left(\frac{331}{101}\right) = \left(\frac{28}{101}\right) = \left(\frac{2}{101}\right)^2 = \left(\frac{2}{101}\right) = \left(\frac{2}{7}\right) = \left(\frac{3}{7}\right) = -1
\]
using quadratic reciprocity.

4. HW 7
Part (b):

\[
\left( \frac{506}{301} \right) = \left( \frac{253}{301} \right) \left( \frac{2}{301} \right) = \left( \frac{401}{253} \right) \cdot 1 = \left( \frac{148}{253} \right) \text{ using Corollary 7.10}
\]

\[
= \left( \frac{37}{253} \right) \cdot 2^2 = \left( \frac{253}{37} \right)
\]

\[
= \left( \frac{31}{37} \right) = -1 \quad \text{we've skipped a few steps}
\]

Part (c): Write \( p^\pm = c \pm 1 \), and notice that \( p^+ = 1 \pmod{4} \). Then,

\[
\left( \frac{c - 1}{c + 1} \right) = \left( \frac{c + 1}{c - 1} \right) = \left( \frac{2}{c - 1} \right) = 1
\]

since \( c - 1 = -1 \pmod{8} \) (see Corollary 7.10).

**Problem 7.**

Part (a): Since \( n = 103 \) is prime, if we determine that \( 7 \in \mathbb{Q}_{103} \), then it must have exactly two square roots. This follows from the fact \( \mathbb{Z}_p \) has a primitive root if \( p \) is prime.

\[
\left( \frac{7}{103} \right) = - \left( \frac{103}{7} \right) = - \left( \frac{6}{7} \right) = 1.
\]

Part (b): Theorem 7.15 says that \( 7 \in \mathbb{Q}_{55} \iff 7 \in \mathbb{Q}_{11} \) and \( 7 \in \mathbb{Q}_5 \). Calculate

\[
\left( \frac{7}{11} \right) = - \left( \frac{11}{7} \right) = - \left( \frac{4}{7} \right) = -1,
\]

and so \( 7 \not\in \mathbb{Q}_{11} \). Hence it has no square roots mod 55.

Part (c): Again, 7 has no square roots mod 99 for the same reason as part (b).

**Problem 8.** Let \( u(n) = 1 \) for all \( n \), and note that \( \tau(n) = u * u \). We know that \( \mu \) and \( u \) are Dirichlet inverses (see example 8.4 in J & J). Using associativity of the Dirichlet product, we get

\[
(\mu * \mu) * \tau = (\mu * \mu) * (u * u) = I.
\]

**Problem 9.** There was a typo in the problem and I struggled a little to figure out what the problem was. Here is the correct definition of \( S(n) \):

\[
S(n) := \sum_{\gcd(i,n)=1} i^2.
\]

Let

\[
H(n) := \sum_{d \mid n} \frac{n^2}{d^2} S(d) = \sum_{d \mid n, \gcd(i,d)=1} \frac{n^2}{d^2} i^2.
\]

As indicated in the problem, there is one-one map from the summands in

\[
G(n) := \sum_{i=1}^{n} i^2
\]

to the summands in \( H(n) \). For each \( d \mid n \), there are \( \phi(d) \) different \( i \) that are coprime to \( d \), and this tells us that the total number of terms in the sum for \( H(n) \) is \( \sum_{d \mid n} \phi(d) = n \). So the total number of terms in \( H(n) \) is \( n \), each term sum is
smaller than or equal to \(n\), and each term if of the form \(k^2\) for some integer. Hence, to show that \(H(n) = G(n)\), we only need to show that all the terms in \(H(n)\) are distinct. But that is immediate, since for distinct divisors \(d_1\) and \(d_2\), we can never have \((n/d_1)i = (n/d_2)j\) for \(\gcd(i, d_1) = \gcd(j, d_2) = 1\). To prove this, suppose to the contrary that it happens for some \(d_1, d_2, i\) and \(j\). Then we would have

\[ d_1j = d_2i. \]

However, this implies both that \(i|j\) and \(j|i\), from which we deduce that \(i = j\). This produces the contradiction \(d_1 = d_2\).

So we’ve proved that

\[ G(n) = \frac{n(n + 1)(2n + 1)}{6} = N^2 * S, \]

where \(N^2(n) = n^2\). The Dirichlet inverse of \(N^2\) (by inspection) is just \(N^2\mu\) since

\[ N^2 * (N^2\mu) = \sum_{d|n} \frac{n^2}{d^2} d^2 \mu(d) = n^2 \sum_{d|n} \mu(d) = I(n). \]

Hence,

\[ S = G * N^2\mu = \sum_{d|n} \frac{n}{6d} \left( \frac{2n^2}{d^2} + \frac{3n}{d} + 1 \right) (d^2 \mu(d)). \]

**Problem 10.** The argument is similar to the proof of Theorem 5.8 in the textbook. Please review it. Let

\[ \Omega_d := \{i \leq n \mid \gcd(i, n) = d\}. \]

If \(i\) is such that \(\gcd(i, n) = d\), we must have \(\gcd(i/d, n/d) = 1\). Then, \(|\Omega_d|\) is just the number of \(k \leq n/d\) such that \(\gcd(k, n/d) = 1\). Hence,

\[ |\Omega_d| = \phi \left( \frac{n}{d} \right). \]

It’s clear that \(\cup_{d|n} \Omega_d = \mathbb{Z}_n\), and that it is a disjoint union of sets: every \(i \in \mathbb{Z}_n\) must be in one and only one of the \(\Omega_d\). Then we can write the expression for \(\triangle(n)\) as

\[ \triangle(n) = \sum_{d|n} d|\Omega_d| = \sum_{d|n} d\phi(n/d) = N * \phi(n), \]

where \(N(n) = n\). Since \(\phi * u = N\), \(\triangle * u = N * N = \sum_{d|n} d(n/d) = n\tau\). This is exactly what we set out to prove.