Solutions to Homework 2

Q.1. Denote $[n] = \{1, \ldots, n\}$ for simplicity. We have

$$n^2 \cdot p_n = \#\{(a, b) \in [n] \times [n] : \mathrm{GCD}(a, b) = 1\}. \tag{1}$$

On the other hand,

$$\sum_{k=1}^{n} \phi(k) = \#\{(a, b) \in [n] \times [n] : \mathrm{GCD}(a, b) = 1 \text{ and } a \leq b\}. \tag{2}$$

Hence

$$n^2 \cdot p_n = 2\sum_{k=1}^{n} \phi(k) - 1,$$

since every unordered pair $\{a, b\}$ of elements of $[n]$ is counted twice in (1) and once in (2), except for $\{1, 1\}$, which is counted once in both. Theorem 1.7 in Suppl. Week 46 now implies that $n^2 \cdot p_n \to 6/\pi^2$, v.s.v.

Q.2. Let p be an odd prime. If a were a primitive root mod p, then $a(\text{mod } p)$ would be a generator of the group $\mathbb{Z}_p^{\times}$. But this is a cyclic group of even order $p-1$, hence any square will lie in the unique subgroup of order $(p-1)/2$ and cannot be a generator.

Q.3. $\phi(37) = 36$ and the divisors of 36 are $1, 2, 3, 4, 6, 9, 12, 18, 36$. Hence if $x \in [1, 36]$, then x is a primitive root modulo 37 if and only if $x^n \not\equiv 1 \pmod{37}$ for $n \in \{1, 2, 3, 4, 6, 9, 12, 18\}$. We can start testing with $x = 2$, and in fact this already works. For, modulo 37,

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 16,$$
$$2^6 \equiv 27, \quad 2^9 \equiv 31, \quad 2^{12} \equiv 26, \quad 2^{18} \equiv -1.$$

So 2 is one primitive root. The complete list of primitive roots modulo 37 is given by

$$\{2^t \pmod{37} : 1 \leq t \leq 36 \text{ and } \mathrm{GCD}(t, 36) = 1\}.$$

Now $\phi(36) = \phi(2^2 \cdot 3^2) = (2^2 - 2)(3^2 - 3) = 12$, so there are 12 possibilities for t, and one readily checks that these are

$$t \in \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}.$$

So it remains to compute $2^t \pmod{37}$ for each t in this list. Note that, since $37 \equiv 1(\text{mod } 4)$, if x is a primitive root then so is $37 - x$, so we really only need to compute half of them. Anyway, one finds that the complete list of primitive roots modulo 37 is

$$\{\pm 2, \pm 5, \pm 13, \pm 15, \pm 17, \pm 18\}.$$

Q.4(i) For each prime p, let S^p denote the set of those positive integers n such that the highest power of p dividing n is an even power. Then, as proven in the lectures,

$$S_2 = \bigcap_{p \equiv 3 \pmod 4} S^p. \tag{3}$$

Consider any such p. Let $pS^p := \{pn : n \in S^p\}$. Then $\mathbb{N}$ is the disjoint union of S^p and pS^p. Since $d(pS^p) = \frac{1}{p} d(S^p)$, it follows that $d(S^p) = 1 - \frac{1}{p+1}$. By (4) and the Chinese Remainder Theorem, it follows that

$$d(S_2) = \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p+1}\right).$$

So we just need to prove that the infinite product converges to zero. Taking logarithms in the usual manner, this is equivalent to showing that

$$\sum_{p \equiv 3 \pmod 4} \frac{1}{p+1} = +\infty.$$

But this fact follows from the analytic form of Dirichlet's theorem (Theorem 15.2 in the lecture notes).

(ii) From Theorem 10.1 in the lecture notes, we know that the complement S_3^c is given by

$$S_3^c = \{4^k(8l+7) : k,\, l \in \mathbb{N}_0\}.$$

Hence,

$$d(S_3^c) = \frac{1}{8}\left(\sum_{k=0}^{\infty} \frac{1}{4^k}\right) = \frac{1}{8} \times \frac{4}{3} = \frac{1}{6}$$

and so $d(S_3) = 1 - \frac{1}{6} = \frac{5}{6}$.

Q.5. This alternative proof of Theorem 9.3 is due to Donald Zagier. See

D. ZAGIER, A one-sentence proof that every prime $p \equiv 1 (\text{mod } 4)$ is a sum of two squares, *Amer. Math. Monthly* **97**, No. 2, (1990), p. 144.

Q.6. First, one computes $16144 = 2^4 \cdot 1009$, so

$$\left(\frac{16144}{377}\right) = \left(\frac{2}{377}\right)^4 \left(\frac{1009}{377}\right) = \left(\frac{1009}{377}\right).$$

Next, since $1009 = 2 \cdot 377 + 255$, we have

$$\left(\frac{1009}{377}\right) = \left(\frac{255}{377}\right).$$

Since $377 \equiv 1 \pmod 4$, Jacobi reciprocity implies that

$$\left(\frac{255}{377}\right) = \left(\frac{377}{255}\right).$$

Next, since $377 = 1 \cdot 255 + 122$ one has

$$\left(\frac{377}{255}\right) = \left(\frac{122}{255}\right) = \left(\frac{2}{255}\right)\left(\frac{61}{255}\right) = \left(\frac{61}{255}\right),$$

since $255 \equiv 7 \pmod 8$ and hence $\left(\frac{2}{255}\right) = +1$. Next, since $61 \equiv 1 \pmod 4$, Jacobi reciprocity implies that

$$\left(\frac{61}{255}\right) = \left(\frac{255}{61}\right).$$

Since $255 = 4 \cdot 61 + 11$, one deduces in turn that

$$\left(\frac{255}{61}\right) = \left(\frac{11}{61}\right).$$

Since $61 \equiv 1 \pmod 4$, Jacobi reciprocity and the fact that $61 = 5 \cdot 11 + 6$ now give that

$$\left(\frac{11}{61}\right) = \left(\frac{61}{11}\right) = \left(\frac{6}{11}\right).$$

Since $11 \equiv 3 \pmod 8$, we then have

$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = -\left(\frac{3}{11}\right).$$

Since both 3 and 11 are congruent to $3 \pmod 4$, Jacobi reciprocity implies that

$$-\left(\frac{3}{11}\right) = -\left[-\left(\frac{11}{3}\right)\right] = \left(\frac{11}{3}\right).$$

And now, finally, since $11 \equiv 2 \pmod 3$, we have

$$\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

So we conclude that

$$\left(\frac{16144}{377}\right) = -1.$$

Q.7(i) The proof is by contradiction. Suppose that the limit is not zero. Then there exists $\epsilon > 0$, an infinite sequence $N_1 < N_2 < \cdots$ of positive integers and subsets $A_i \subseteq [1, N_i]$ such that each $|A_i| \geq \epsilon N_i$ and each A_i is free of non-trivial solutions to $\mathcal{L}$. I claim that there is some constant $C > 0$, depending on $\mathcal{L}$ only, such that the following holds :

Let $(x_1, ..., x_n) \in \mathbb{N}^n$ be any non-trivial solution to $\mathcal{L}$. Let $t_1 < t_2 < \cdots < t_k$ be the full list of distinct integers such that every x_i equals one of the t_j. Then $t_{j+1}/t_j \leq C$ for each $j = 1, ..., k-1$.

Indeed, it is here that we use the fact that we are only interested in non-trivial solutions. Non-triviality implies that, for any fixed $j \in \{1, ..., k\}$,

$$\sum_{x_i = t_j} a_i \neq 0,$$

and it is this which implies the existence of the constant C, depending only on the coefficients $a_1, ..., a_n$.

Now choose a sequence $d_1, d_2, ...$ of positive integers which recursively satisfy

$$d_l > C \left(\sum_{i=1}^{l} N_i + \sum_{i=1}^{l-1} d_i \right).$$

We are going to construct a set $A \subseteq \mathbb{N}$ which is free of non-trivial solutions to $\mathcal{L}$ and satisfies $\overline{d}(A) \geq \epsilon$ - this will give the desired contradiction. For each $l > 0$, put

$$B_l = A_l + \xi_l = \{u + \xi_l : u \in A_l\},$$

where

$$\xi_l := \sum_{i=1}^{l} (N_i + d_i).$$

Then take

$$A = \bigsqcup_{l=1}^{\infty} B_l.$$

Indeed, by construction the B_l do not overlap and, crucially, the the choice of the numbers d_l ensures that any non-trivial solution to $\mathcal{L}$ in A must be entirely contained inside just one of the B_l. But each B_l is just a translate of the corresponding A_l, and hence is free of non-trivial solutions.

Finally, for each $l > 0$, let M_l be the rightmost element of B_l. It is clear from the construction that $|A \cap [1, M_l]| > \epsilon M_l$, and hence $\overline{d}(A) \geq \epsilon$, v.s.v.

(ii) Let $(x_1, ..., x_n)$ be any non-trivial solution to $\mathcal{L} : \sum_{i=1}^{n} a_i x_i = 0$, where $\mathcal{L}$ is invariant, i.e.: $\sum_{i=1}^{n} a_i = 0$. Let $k = \max\{|x_i| : i = 1, ..., n\}$. Now let A be subset of $\mathbb{N}$ of positive upper density. By Szemerédi's theorem, A

contains a non-trivial arithmetic progression of length $2k+1$, which we can write as

$$\{a-kd, a-(k-1)d, ..., a, a+d, ..., a+kd\}, \quad a, d, a-kd \in \mathbb{N}.$$

For $i = 1, ..., n$, set $y_i := a + x_i d$. Then

$$\sum a_i y_i = \left(\sum a_i\right) a + \left(\sum a_i x_i\right) d = 0 + 0 = 0,$$

so $(y_1, ..., y_n)$ is a solution to $\mathcal{L}$ inside A. Since the solution $(x_1, ..., x_n)$ was assumed to be non-tririval, so also is the solution $(y_1, ..., y_n)$. Hence A contains non-trivial solutions to $\mathcal{L}$, as desired.

Q.8(i) Regarding the function $d(n)$, we have

$$S := \sum_{n=1}^{N} d(n) = \sum_{n=1}^{N} \left(\sum_{d|n} 1\right) = \sum_{d=1}^{N} \lfloor \frac{N}{d} \rfloor.$$

Now $\lfloor N/d \rfloor = N/d + O(1)$, hence

$$S = N\left(\sum_{d=1}^{N} \frac{1}{d}\right) + \sum_{d=1}^{N} O(1) = N(\log N + O(1)) + O(N) = N \log N + O(N),$$

which implies that $S \sim N \log N$.

(ii) Regarding the function $\sigma(n)$, we have

$$\begin{aligned} S := \sum_{n=1}^{N} \sigma(n) &= \sum_{n=1}^{N} \left(\sum_{d|n} d\right) = \sum_{n=1}^{N} \left(\sum_{d|n} \frac{n}{d}\right) \\ &= \sum_{d=1}^{N} \left(\sum_{m=1}^{\lfloor N/d \rfloor} m\right) = \sum_{d=1}^{N} \left\{\frac{1}{2} \lfloor \frac{N}{d} \rfloor \left(\lfloor \frac{N}{d} \rfloor + 1\right)\right\} \end{aligned}$$

$$= \sum_{d=1}^{N} \left\{\frac{N^2}{2d^2} + O\left(\frac{N}{d}\right)\right\} = \frac{N^2}{2}\left(\sum_{d=1}^{N} \frac{1}{d^2}\right) + O\left(N \cdot \sum_{d=1}^{N} \frac{1}{d}\right).$$

Hence, as $N \to \infty$, one has

$$S \to \frac{N^2}{2}\zeta(2) + O(N \log N) = \frac{\pi^2}{12} N^2 + O(N \log N),$$

so that $S \sim \frac{\pi^2}{12} N^2$, v.s.v.

Q.9. Numbers of formulas below are in the Supplementary Lecture Notes for Week 46.

(i) Suppose Re$(s) > 2$. Then, by (1.5) and (1.6),

$$\frac{\zeta(s-1)}{\zeta(s)} = \zeta(s-1) \times \frac{1}{\zeta(s)} = \left(\sum_{n=1}^{\infty} \frac{1}{n^{s-1}}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right)$$
$$= \left(\sum_{n=1}^{\infty} \frac{n}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = \sum_{n=1}^{\infty} \frac{\sum_{d|n} \mu(d)\frac{n}{d}}{n^s} = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}.$$

To summarise, for Re$(s) > 2$ one has the series representation

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}.$$

(ii) Suppose Re$(s) > 1$. Then

$$(\zeta(s))^2 = \zeta(s) \cdot \zeta(s) = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) = \sum_{n=1}^{\infty} \frac{\sum_{d|n} 1}{n^s} = \sum_{n=1}^{\infty} \frac{d(n)}{n^s}.$$

(iii) Suppose Re$(s) > 2$. Then

$$\zeta(s)\zeta(s-1) = \left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{n}{n^s}\right) = \sum_{n=1}^{\infty} \frac{\sum_{d|n} d}{n^s} = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}.$$

Q.10. Here C_n denotes the cyclic group of order n. Let $p-1$ have prime factorisation

$$p - 1 = \prod_{i=1}^{k} q_i^{\alpha_i}.$$

Then

$$\mathbb{Z}_p^{\times} \cong C_{p-1} \cong \prod_{i=1}^{k} C_{q_i^{\alpha_i}}. \tag{4}$$

Let $x_1, ..., x_k$ be integers (mod p) which generate the cyclic factors in the product (4), and note that

$$x = \prod_{i=1}^{k} x_i^{u_i} \tag{5}$$

is a primitive root mod p if and only if $GCD(u_i, q_i) = 1$ for $i = 1, ..., k$.

CASE 1: $\mu(p-1) = 0$.

This means that $p-1$ is not squarefree, in other words that some $\alpha_i > 1$. Without loss of generality, suppose that $\alpha_1 > 1$. Now let $a := x_1^{q_1} \pmod{p}$.

Then x is a primitive root mod p if and only if ax is. Let $\mathcal{P}$ denote the set of all primitive roots mod p. Then, mod p,

$$S \equiv \sum_{x \in \mathcal{P}} x \equiv \sum_{x \in \mathcal{P}} ax \equiv aS.$$

But, since $\alpha_1 > 1$, we have $a \not\equiv 0 \pmod{p}$. Hence we must have $S \equiv 0 \pmod{p}$. This deals with Case 1.

CASE 2: $\mu(p-1) = (-1)^k$.

This means that each $\alpha_i = 1$. Then, by (5),

$$\sum_{x \in \mathcal{P}} x \equiv \sum_{u_1=1}^{q_1-1} \cdots \sum_{u_k=1}^{q_k-1} x_1^{u_1} \cdots x_k^{u_k} = \prod_{i=1}^{k} \left(\sum_{u_i=1}^{q_i-1} x_i^{u_i} \right). \tag{6}$$

Fix any i. Then $x_i^{q_i} \equiv 1 \pmod{p}$, hence, mod p,

$$0 \equiv x_i^{q_i} - 1 = (x_i - 1)(1 + x_i + \cdots + x_i^{q_i-1}).$$

Since $x_i \not\equiv 1$, it follows that

$$1 + x_i + \cdots + x_i^{q_i-1} \equiv 0 \pmod{p}.$$

In other words, every factor in the product (6) is congruent to $-1 \pmod{p}$. Hence the product is congruent to $(-1)^k = \mu(p-1)$, v.s.v.

Q.11. This is a well-known result called *Wolstenholme's Theorem*. For a presentation of the 'standard proof', see for example

http://projectpen.files.wordpress.com/2009/04/pen-a23-a24-version-edited2.pdf