ASSIGNMENT 5: SOLUTIONS

Question 1.

Solution. Since $a = \omega + \omega^2 + \omega^4$ and $b = \omega^3 + \omega^5 + \omega^6$, it follows that

$$a + b = \sum_{i=1}^{6} \omega^i = -1$$

and

$$ab = \sum_{i=0}^{6} \omega^i + 2\omega^7 = 2.$$

Thus, a and b are roots of the polynomial $x^2 + x + 2$. By the quadratic formula, we find that

$$a, b = \frac{-1 \pm \sqrt{-7}}{2}.$$

□

Question 2. For simplicity, assume that $p \neq 2, 7$ below.

Solution. Let $f(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ be an irreducible factor of $1 + x + \ldots + x^6$, and let $n = \deg f$. Then $\mathbb{Z}/p\mathbb{Z}[x]/(f(x))$ is isomorphic to the finite field $\mathbb{F} = \mathbb{F}_{p^n}$. Letting ω denote the image of x under this isomorphism, we find that ω is a non-trivial 7^{th} root of unity since it satisfies $f(x)$ and $f(x) \mid x^7 - 1$ by construction.

Since the only relation used in the previous question to derive the properties and a and b was that $\sum_{i=0}^{6} \omega^i = 0$ (*i.e.* that ω is a 7^{th} root of unity), we find that the same relations hold for our new ω modulo p. In particular, for $a = \omega + \omega^2 + \omega^4$ and $b = \omega^3 + \omega^5 + \omega^6$ in $\mathbb{F}$, a and b are roots of $x^2 + x + 2 \pmod{p}$ and as suggested by the quadratic formula,

$$(2a+1)^2 \equiv (2b+1)^2 \equiv -7 \pmod{p}$$

or, letting s be a root of $x^2 + 7$ in $\bar{\mathbb{F}}_p$, we find that

$$a = \frac{-1+s}{2}, \qquad b = \frac{-1-s}{2}.$$

We show two different ways of proving this below.

For the first proof, we immediately observe that if $a, b \in \mathbb{F}_p$ then $\left(\frac{-7}{p}\right) = 1$, and furthermore, that $2a+1, 2b+1$ are the roots of $x^2 + 7 \pmod{p}$ in $\mathbb{F}$. Thus,

$$(2a+1)^{p-1} = (2a+1)^{2(p-1)/2} \equiv -7^{(p-1)/2} \equiv \left(\frac{-7}{p}\right).$$

Since the elements of $\mathbb{F}_p \subseteq \mathbb{F}$ are exactly the roots of $x^p - x$, we see that $a, b \in \mathbb{F}_p$ if and only if $\left(\frac{-7}{p}\right) = 1$, and $a, b \notin \mathbb{F}_p$ if and only if $\left(\frac{-7}{p}\right) = -1$.

One easily checks that $a^p = a$ if and only if $p \equiv 1, 2, 4 \pmod{7}$ (and $a^p = b$ otherwise), so $a \in \mathbb{F}_p$ (and respectively b, since $a + b = -1$) if and only if $p \equiv 1, 2, 4 \pmod{7}$. Thus,

$$\left(\frac{-7}{p}\right) = \begin{cases} 1 & p \equiv 1,2,4 \pmod{7} \\ -1 & p \equiv 3,5,6 \pmod{7} \\ 0 & p = 7. \end{cases}$$

Alternately, one observes that $s^p = s^{p-1}s = \left(\frac{-7}{p}\right)s$ and since p is odd,

$$a^p = \frac{-1+s^p}{2} = \frac{-1+\left(\frac{-7}{p}\right)s}{2} = \begin{cases} a = \frac{-1+s}{2} & p \equiv 1,2,4 \pmod{7} \\ b = \frac{-1-s}{2} & p \equiv 3,5,6 \pmod{7} \end{cases}$$

The result then follows. □

Question 3. This was an open ended question. As a "solution" I'm just going to go with what seemed like the obvious or reasonable observations to have made from the data, and give some indication of how to prove the observations hold more generally. I will of course stop short of seriously developing something like cubic reciprocity. You can look that up on your own.

Solution. For the case of $g(x) = x^3 - 2$, one observes that p an odd prime such that $p \equiv 2 \pmod 3$, then g always has a root modulo p. It isn't too hard to prove that if $p \equiv 2 \pmod 3$, then in fact, every element of $\mathbb{Z}/p\mathbb{Z}$ is a cube. It writing $p = 3k + 2$, and applying Fermat's little theorem can be used to prove that x^{2k+1} is a cube root of x mod p. This also proves that there is exactly one root mod p when $p \equiv 2 \pmod 3$.

Furthermore, one observes that for $p \equiv 1 \pmod 3$, there may or may not be a root to g modulo p, so some further condition is required. This less obvious condition can be stated as: for $p = 1 + 3k$, then g has a root modulo p if and only if $2^k \cong 1 \pmod p$. This statement is not hard to prove.

There are other ways to state the condition for when 2 is a cubic residue mod p. Most of these relate to the fact that $p \equiv 1 \pmod 3$ can be written as $p = a^2 + 3b^2$. In particular, this is related to the fact that $p \equiv 1 \pmod 3$ can be factored in the Eisenstein integers, while $p \equiv 2 \pmod 3$ cannot, as the Eisenstein integers are perhaps the "correct" ring in which to study cubic reciprocity (if we want something like the Legendre symbol).

On the other hand, when $g(x) = x^3 + x^2 - x - 1$, one immediately observes that for $p \neq 7$, g has a root modulo p if and only if $p \equiv \pm 1 \pmod 7$. Furthermore, since you're looking at a count of the roots, you'll notice that either all three of the roots are in $\mathbb{Z}/p\mathbb{Z}$, or none of them are. □

Question 4.

Solution. Using the Euler product expansion for the Riemann zeta function, we obtain that

$$\frac{\zeta(s)}{\zeta 2s} = \prod_p (1 + p^{-s}).$$

One can then show by induction that if we take the product over the first m primes, we have that

$$\prod_{i=1}^{m} (1 + p_i^{-s}) = \sum_{\substack{n \leq p_1 p_2 \ldots p_m \\ n \text{ is non-square}}} \frac{1}{n^s}.$$

Taking the limit of m to infinity gives the desired result. □

Question 5.

Solution. The first part of the question follows easily by using the prime factorization of n together with the multiplicative property of the Legendre symbol.

For the second part of the question, suppose that there are only finitely many primes $\mathcal{P} = \{p_i\}_{i=1}^n$ such that $\left(\frac{p_i}{q}\right) = -1$. If n is odd, set $m = p_1 p_2 \ldots p_n + q$; otherwise, set $m = p_1^2 p_2 \ldots p_n + q$. Then show that $\left(\frac{m}{q}\right) = -1$ and all the prime factors of m are not in $\mathcal{P}$. Therefore by the first part of this question, m has a prime factor p such that $\left(\frac{p}{q}\right) = -1$, but $p \notin \mathcal{P}$, a contradiction. □

Question 7.

Solution. There were a number of observations that could have been made and "explained", from the fact that both $\binom{40}{20}$ and $\binom{100}{50}$ have square factors, to observations regarding which primes appear in the factorizations over certain intervals. I'm not really sure what was supposed to be special about 20 and 50 in particular. Basically any decent effort to comment on these was considered enough. □