Amin Zolfagharian - 610300118

Problem 1.

3 is a primitive root modulo 7. Therefore either 3 or 3 + 7 is a primitive root modulo 49. Since $3^6 \overset{49}{\equiv} -6$ therefore 3 is a primitive root of 49. Now since if r is a primitive root modulo p^2 then it is a primitive root of p^α for $\alpha > 2$ then we know that 3 is a primitive root of 7^4. Therefore for any a such that $(a, 7^4) = 1$, there exists an i such that $3^i \overset{7^4}{\equiv}= a$. Since all primitive roots of 7^4, like r we know that $(r, 7^4) = 1$, then there exists i such that $3^i \overset{7^4}{\equiv} r$. Since all primitive roots are the ones with order exactly $\varphi(7^4)$, then we should have:

$$\varphi(7^4) = Ord(3^i) = \frac{Ord(3)}{(Ord(3), i)} = \frac{\varphi(7^4)}{(i, \varphi(7^4))}$$
$$\implies (i, \varphi(7^4)) = 1$$

Therefore all numbers 3^i, such that $(i, \varphi(7^4)) = 1$ are primitive roots. Therefore we have a total of $7^3 \cdot 6$ primitive roots modulo 7^4.

Problem 2.

We know that for any a, such that $(a, 2^\alpha) = 1$, there exists a β such that $5^\beta \overset{2^\alpha}{\equiv} a$ or $-5^\beta \overset{2^\alpha}{\equiv} a$. Since $Ord_{2^9}(5) = 2^7$, Then if a is of order 32:

$$a \overset{2^\alpha}{\equiv} 5^\beta \implies Ord(a) = 32 = \frac{Ord(5)}{(Ord(5), \beta)} = \frac{2^7}{(2^7, \beta)}$$
$$\implies (2^7, \beta) = 4 \implies \beta = 2^2 m \quad (\text{odd } m)$$

Similarly for -5. Therefore any element with order of 32 is of the form 5^β or -5^β such that $\beta = 2^2 m$, where m is odd and $1 \leq m < 2^7$.

Problem 3.

(i) First suppose $(k, p) = 1$. And p an odd prime. Let r be a primitive root modulo p. Then we can rewrite the sum:

$$\sum_{i=1}^{i=p-1} i^k = \sum_{j=1}^{j=p-1} (r^j)^k = r^k + r^{2k} + \cdots + r^{(p-1)k}$$

Since for any $1 \leq i \leq p-1$ there exists a j such that $i = r^j$. Also since $(k, p) = 1$, then $\{1k, 2k, \ldots, (p-1)k\} = \{1, 2, \ldots, p-1\}$. Therefore we have:

$$r^k + r^{2k} + \cdots + r^{(p-1)k} = r + r^2 + \cdots + r^{p-1}$$

And since r is primitive root, then $\{r, r^2, \dots, r^{p-1}\}$ is the set of all numbers less than p:

$$r + r^2 + \cdots + r^{p-1} = 1 + 2 + \cdots + p - 1 = \frac{p(p-1)}{2}$$

Since $p \neq 2$ then:

$$\sum_{i=1}^{i=p-1} i^k \overset{p}{\equiv} \frac{p(p-1)}{2} \overset{p}{\equiv} 0$$

If p is an odd prime and $p \mid k$, then we can write $k = p^n m$ such that $p \nmid m$. By Fermat's little theorem we have:

$$\sum_{i=1}^{i=p-1} i^k = \sum_{i=1}^{i=p-1} i^{(p^n-1)m} i^m \overset{p}{\equiv} \sum_{i=1}^{i=p-1} i^m$$

And we showed this in last part with the assumption $(k, p) = 1$. Therfore we have:

$$\sum_{i=1}^{i=p-1} i^k \overset{p}{\equiv} \sum_{i=1}^{i=p-1} i^m \overset{p}{\equiv} 0$$

The only case remained is $p = 2$ which is trivial:

$$\sum_{i=1}^{i=2-1} i^k \overset{2}{\equiv} 1^k \overset{2}{\equiv} 1$$

(ii) Suppose r is a primitive root modulo p. We know that either r or $r + p$ is a primitive root of p^2. If $p + r$ is the primitive root, then at first consider $r + p$ as a primitive root of p. Thus WLOG suppose r is a primitive root of p^2. And since r is a primitive root of p^2, then it is a primitive root of p^α. Now we can rewrite the sum:

$$1^n + 2^n + \cdots + (p^k - 1)^n = r^n + r^{2n} + \dots r^{\varphi(p^k)n}$$
$$= 1 + r^n + \cdots + r^{(\varphi(p^k)-1)n} = \frac{r^{\varphi(p^k)n} - 1}{r^n - 1}$$

Suppose $p \mid r^n - 1$. Then $r^n \overset{p}{\equiv} 1$. Since r is a primitive root of p, then $\phi(p) = p - 1 \mid n$. Contradition. Therefore $p \nmid r^n - 1$. And $(p^k, r^n - 1) = 1$. Suppose r' is the multiplicative inverse of $r^n - 1$:

$$\frac{r^{\varphi(p^k)n} - 1}{r^n - 1} \overset{p^k}{\equiv} (r^{\varphi(p^k)n} - 1)r' = (r^{\varphi(p^k)^n} - 1)r' \overset{p^k}{\equiv} 0$$

Problem 4.

Suppose r is a primitive root of $(\mathbb{Z}_m)^*$. Since $(\mathbb{Z}_n)^*$ has not primitive root, then there exists some $s < \varphi(n)$ such that $s = Ord_n(r)$.

$$r^s \overset{n}{\equiv} 1$$

We will show that $s\frac{\varphi(m)}{\varphi(n)}$ is the order of r modulo m. It is enough to show that if $m = p_{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, then for any p_i:

$$r^{s\varphi(m)/\varphi(n)} \overset{p_i^{\alpha_i}}{\equiv} 1$$

Then by CRT we would have $r^{s\varphi(m)/\varphi(n)} \overset{m}{\equiv} 1$. If $p_i \nmid n$, then $(\varphi(p_i^{\alpha_i}), \varphi(n)) = 1$:

$$r^{s\varphi(m)/\varphi(n)} \overset{p_i^{\alpha_i}}{\equiv} r^{s\varphi(p_i^{\alpha_i})\varphi(m/p_i^{\alpha_i})/\varphi(n)} \overset{p_i^{\alpha_i}}{\equiv} (r^{\varphi(p_i^{\alpha_i})})^{s\varphi(m/p_i^{\alpha_i})/\varphi(n)} \overset{p_i^{\alpha_i}}{\equiv} 1$$

Now if $p_i \mid n$ such that $n = p_i^\beta n_1$, with $(n_1, p_i) = 1$, then $(\varphi(m), \varphi(n)) = p_i^{\beta-1}(p_i - 1)$:

$$r^{s\varphi(m)/\varphi(n)} \overset{p_i^{\alpha_i}}{\equiv} r^{s\varphi(m/p_i^{\alpha_i})/\varphi(n_1)p_i^{\alpha_i-\beta}} \overset{p_i^{\alpha_i}}{\equiv} (r^{sp_i^{\alpha_i-\beta}})^{\varphi(m/p_i^{\alpha_i})/\varphi(n_1)}$$

For the last part we use the fact that if $a^b \overset{p^i}{\equiv} 1$ then $a^{pb} \overset{p^{i+1}}{\equiv} 1$:

$$a^{pb} - 1 = (a^b - 1)((a^b)^{p-1} + \dots + a^b + 1)$$

But we know that $p^i \mid a^b - 1$ and $((a^b)^{p-1} + \dots + a^b + 1) \overset{p}{\equiv} 1 + 1 + \dots + 1 = p \overset{p}{\equiv} 0$. Therefore $a^{bp} \overset{p^{i+1}}{\equiv} 1$. And with repeating this action: $a^{bp^j} \overset{p^{i+j}}{\equiv} 1$:

$$r^s \overset{p_i^\beta}{\equiv} 1 \implies r^{sp^{\alpha_i-\beta}} \overset{p_i^{\alpha_i}}{\equiv} 1$$
$$\implies (r^{sp_i^{\alpha_i-\beta}})^{\varphi(m/p_i^{\alpha_i})/\varphi(n_1)} \overset{p_i^{\alpha_i}}{\equiv} 1$$

Therefore $Ord_m(r) | s\frac{\varphi(m)}{\varphi(n)}$, which implies $Ord_m(r) \leq s\frac{\varphi(m)}{\varphi(n)}$. Since $s < \varphi(n)$ then:

$$\varphi(m) = Ord_m(r) \leq s\frac{\varphi(m)}{\varphi(n)} < \varphi(n)\frac{\varphi(m)}{\varphi(n)} = \varphi(m)$$

Which is a contradiction. Therefore there is no primitive root for $(\mathbb{Z}_m)^*$.

Problem 5.

Let g be a primitive root of p. Suppose $(-a^2)^r \overset{p}{\equiv} 1$, where r is the order of $-a^2$. We know that:

$$Ord(g^i) = \frac{Ord(g)}{(i, Ord(g))} = \frac{2q}{(i, 2q)}$$

This shows that r have a few options: $1, 2, q, 2q$. $r = 1$, if $r = 1$ then $-a^2 = 1$:

$$a^2 = -1$$

but since $p = 2q + 1 = 2(2k + 1) + 1 = 4k + 3$, then there is no such a. If $r = 2$ then $(-a^2)^2 \stackrel{p}{\equiv} a^4 \stackrel{p}{\equiv} 1$. This shows that $Ord(a) = 1, 2, 4$. We know that order can be 1 or 2. If $ord(a) = 1$ then $a = 1$ which is not. If $Ord(a) = 2$ then $a = \pm 1$. Which again is not since $1 < a < p - 1$. Now if $r = q$:

$$(-a^2)^q \stackrel{p}{\equiv} 1 \implies -a^{2q} \stackrel{p}{\equiv} 1 \implies -1 \stackrel{p}{\equiv} 1$$

Which is a contradiction. Then $r = 2q$. Thus $-a^2$ is a primitive root for p.

Problem 6.

In the privious problem set we saw that if $p \stackrel{4}{\equiv} 1$ then there exists some a such that $a^2 \stackrel{p}{\equiv} -1$. Since $p > 3$ we know that $n > 1$ thus $p \stackrel{4}{\equiv} 1$ and there indeed exists such a. Now we show that there is no b such that $b^2 \stackrel{p}{\equiv} 3$. Suppose the opposite:

$$b^2 \stackrel{p}{\equiv} 3 \implies (ab)^2 = x^2 \stackrel{p}{\equiv} -3$$

We can assume x is odd, otherwise consider $x + p$:

$$x^2 = (2k + 1)^2 \stackrel{p}{\equiv} -3 \implies 4k^2 + 4k + 4 \stackrel{p}{\equiv} 0$$
$$\stackrel{(4,p)=1}{\Longrightarrow} \stackrel{p}{\equiv} k^2 + k + 1 \stackrel{p}{\equiv} 0$$
$$\implies k^3 \stackrel{p}{\equiv} 1$$

Now we have $Ord(k) \mid 3$. Since $Ord(k) \mid \varphi(p) = 2^n$, then we must have $Ord(k) = 1$. Which means that $k = 1$. Thus $x = 3$, $x^2 \stackrel{p}{\equiv} 9 \stackrel{p}{\equiv} -3$. Which means that $p = 2$ or $p = 3$ which is a contradiction. Therefore there exists no such b that $b^2 \stackrel{p}{\equiv} 3$. Now let r be a primitive root of p. And $g^i \stackrel{p}{\equiv} i$. By last part we know that i is odd.

$$Ord(g^i) = \frac{Ord(g)}{(i, Ord(g))} = \frac{2^n}{(i, 2^n)} = \frac{2^n}{1} = 2^n = \varphi(p - 1)$$

This shows that 3 is a primitive root of p.

Problem 7.

Similar to the Problem 5, suppose $Ord_{2p+1}(a) = r$. r can have values 1, 2, p and $2p$. Since $2 \neq 1$ then $r \neq 1$. If $r = 2$ then $2^2 \stackrel{2p+1}{\equiv} 1$ This shows that $2p + 1 = 3$. Which is a contradiction. If $r = p$ then we would have:

$$2^p \stackrel{2p+1}{\equiv} 1 \implies (-2)^p \stackrel{2p+1}{\equiv} -1 \implies Ord(-2) \neq p$$
$$-2 \neq 1 \implies Ord(-2) \neq 1$$
$$(-2)^2 = 4 \stackrel{2p+1}{\equiv} 1 \implies p = 1 \implies Ord(-2) \neq 2$$

This shows that $Ord(-2) = 2p$ and thus -2 is a primitive root of $2p + 1$. Which we know is not true. Therefore $r = 2p$ and 2 is a primitive root of $2p + 1$.