**18.781**
**PROBLEM SET 4.2**

JOHN WANG

## 1. Problem 1

**Problem 1.1.** *Find a primitive root modulo 23 and* $23^2$.

**Solution** Since 23 is a prime, we know there exists at least one primitive root. We can start computing the orders of $1 < i < 23$. We find:

$$ord_{23}(2) = 11 \tag{1.1}$$
$$ord_{23}(3) = 11 \tag{1.2}$$
$$ord_{23}(4) = 11 \tag{1.3}$$
$$ord_{23}(5) = 22 \tag{1.4}$$

Since $\phi(23) = 23 - 1 = 22$, we know that 5 is a primitive root since $ord_{23}(5) = \phi(23)$. For a primitive root modulo $23^2$, we perform the same search.

$$ord_{529}(2) = 253 \tag{1.5}$$
$$ord_{529}(3) = 253 \tag{1.6}$$
$$ord_{529}(4) = 253 \tag{1.7}$$
$$ord_{529}(5) = 506 \tag{1.8}$$

Since $\phi(529) = \phi(23^2) = 23 * (23 - 1) = 506$, we are done, and we have found that 5 is also a primitive root modulo $23^2$. □

**Problem 1.2.** *Show that* $3^8 \equiv -1 \pmod{17}$. *Explain why this implies* 3 *is a primitive root mod 17.*

**Solution** We know that $3^8 = 9^4 = 81^2$. Moreover, we know that $81^2 = 6561$, and we know that $6561 \equiv 16 \pmod{17} \equiv -1 \pmod{17}$. Now, suppose by contradiction that 3 is not a primitive root modulo 17. We know from Fermat's Little Theorem that $3^{16} \equiv 1 \pmod{17}$. However, since 3 is not a primitive root, we know that $3^k \equiv 1 \pmod{17}$ where $k < 16$. However, we know that $ord_{17}(3)|16$ from a lemma proven in class. Since $3^8 \equiv -1 \pmod{17}$, we know $ord_{17}(3) \neq 8$. Therefore, we must have $ord_{17}(3) = 2$, or 4. However, $3^2 = 9 \not\equiv 1 \pmod{17}$ and $3^4 = 81 \not\equiv 1 \pmod{17}$. This is a contradiction. Therefore, 3 must be a primitive root. □

## 2. Problem 2

**Problem 2.1.** *Let* $m$ *and* $n$ *be positive integers with* $m$ *odd. Show that* $(2^m - 1, 2^n + 1) = 1$.

**Solution** Suppose that $(2^m - 1, 2^n + 1) \neq 1$ by contradiction. Then, there must exist some prime $p$ such that $p|2^m - 1$ and $p|2^n + 1$. This means that $2^m \equiv 1 \pmod{p}$ and $2^n \equiv -1 \pmod{p}$. Moreover, this means that $2^n 2^n \equiv (-1)(-1) \equiv 1 \pmod{p}$, which means that $2^{2n} \equiv 2^m \pmod{p}$. This implies that $m \equiv 2n \pmod{p-1}$ by Euler's theorem. However, since $p - 1$ is even, we know that $m$ must also be even, which is a contradiction. □

## 3. Problem 3

**Problem 3.1.** *Show that if* $a^k + 1$ *is a prime and* $a > 1$ *then* $k$ *is a power of* 2.

**Solution** First, we will use a lemma.

**Lemma 3.1.** *If* $k$ *is a positive integer, then* $(a - b)|(a^k - b^k)$.

*Proof.* First, we can express $a^k - b^k$ as the following:

$$a^k - b^k = a^k - b^k + \sum_{i=1}^{k-1} a^i b^{k-i} - \sum_{i=1}^{k-1} a^i b^{k-i} \tag{3.2}$$

$$= \sum_{i=0}^{k-1} a^{i+1} b^{k-i-1} - \sum_{i=0}^{k-1} a^i b^{k-i} \tag{3.3}$$

$$= (a-b) \sum_{i=0}^{k-1} a^i b^{n-i-1} \tag{3.4}$$

Therefore, it is clear that $(a-b)|(a^k - b^k)$. □

Now, we will use the above lemma to prove that $k$ is a power of 2. First, suppose by contradiction that $k$ is not a power of 2. Then we can express $k$ as $k = rs$ where $r \in \{1, 2, 3, \ldots, k\}$ and $s \in \{1, 3, 5, \ldots, k\}$ where $s$ is odd. Now, we can write $a = 2^r$ and $b = -1$ so that $(a - b) = 2^r + 1$. Define $m = s$, so that $(a^m - b^m) = (2^{r^s} - (-1)^s) = 2^{rs} + 1$ since $s$ is odd. We see from the lemma that $(2^r + 1)|(2^{rs} + 1)$ so that $(2^r + 1)|(2^k + 1)$ which shows that $a^k + 1$ is not a prime. This is a contradiction, so $k$ must be a power of 2. □

**Problem 3.2.** *Show that if* $p|(a^{2^n} + 1)$ *then* $p = 2$ *or* $p \equiv 1 \pmod{2^{n+1}}$.

**Solution** First notice that if $a$ is odd, then $p = 2$ will always work since $a^{2^n} + 1 \equiv 0 \pmod 2$. Next, if $a$ is even, we see that $a^{2^n} \equiv -1 \pmod p$ so that $(a^{2^n})^2 \equiv 1 \pmod p$. This means that $a^{2^{n+1}} \equiv 1 \pmod p$. We want to show that $2^{n+1} = ord_p(a)$, since if this is the case, then $2^{n+1}|\phi(p)$ by a theorem shown in class, which implies $2^{n+1}|p - 1$ which can be rewritten as $p \equiv 1 \pmod{2^{n+1}}$.

So suppose by contradiction that $2^{n+1} \neq ord_p(a)$. Then there must exist some $k$ such that $a^k \equiv 1 \pmod p$ where $k < 2^{n+1}$ and $k|2^{n+1}$. If this is the case, then $k$ clearly must be a multiple of 2, since it divides $2^{n+1}$. This means that $k = 2^m$ for some $m < n + 1$. This means we must have $a^{2^m} \equiv 1 \pmod p$, where $m \leq n$. However we know that $(a^{2^m})^{(2^i)} \equiv 1 \pmod p$ for all $i \geq 0$. Rewritten, we see that:

$$a^{2^{m+i}} \equiv 1 \pmod p \quad \text{where } m \leq n \quad \forall i \geq 0 \tag{3.5}$$

However, this implies that $a^{2^n} \equiv 1 \pmod p$ since $n \geq m$ and $m + i = n$ for some $i \geq 0$. Clearly this is not true, so we have reached a contradiction. From here $p \equiv 1 \pmod{2^{n+1}}$ follows from the argument above. □

## 4. Problem 4

**Problem 4.1.** *Let* $a$ *and* $n > 1$ *be any integers such that* $a^{n-1} \equiv 1 \pmod n$*, but* $a^d \not\equiv 1 \pmod n$ *for every proper divisor* $d$ *of* $n - 1$*. Prove that* $n$ *is prime.*

**Solution** First, we must have $(a, n) = 1$, otherwise there would be a prime such that $p|a$ and $p|n$ which would imply $a^{n-1} \equiv 1 \pmod p$. Since this is the case, then we can calculate $h = ord_n(a)$. We know that by definition $a^h \equiv 1 \pmod n$, and by a lemma from class, we know that $h|(n-1)$. Since $h|(n-1)$ and we know that $h \leq n - 1$, we know that $a^h \neq 1 \pmod n$ by hypothesis. Therefore, we know that $h = n - 1$. However, since $n - 1 = h = ord_n(a)$ and $ord_n(a)|\phi(n)$ by definition, we find that $\phi(n) = n - 1$. This occurs only when $n$ is a prime. This completes the proof. □

## 5. Problem 5

**Problem 5.1.** *Show that the sequence* $1^2, 2^2, 3^3, \ldots$ *considered modulo* $p$ *is periodic with smallest period* $p(p-1)$.

**Solution** Let $j$ be the period. We want to show that $a_{i+j} \equiv a_i \pmod p$ for all $i$. Using the property of our sequence, namely that $a_i = i^i$, we see that $a_{i+j} = (i+j)^{i+j}$. Therefore, we have:

$$a_{i+j} = (i+j)^i (i+j)^j \tag{5.1}$$

$$= \left( \sum_{x=0}^{i} \binom{i}{x} i^x j^{i-x} \right) \left( \sum_{y=0}^{j} \binom{j}{y} i^y j^{j-y} \right) \tag{5.2}$$

$$= \sum_{x=0}^{i} \sum_{y=0}^{j} \binom{i}{x} \binom{j}{y} i^{x+y} j^{i+j-(x+y)} \tag{5.3}$$

Substituting $j = p(p-1)$ into the above expression, and noting that $p(p-1)^b \pmod p \equiv 0$ for all $b \in \mathrm{N}$, we find:

$$a_{i+p(p-1)} = \sum_{x=0}^{i}\sum_{y=0}^{j}\binom{i}{x}\binom{p(p+1)}{y} i^{x+y}(p(p-1))^{i+p(p-1)-(x+y)} \tag{5.4}$$

$$= i^{i+p(p-1)} \tag{5.5}$$

The last expression occurs because the only term without any $p(p-1)$ terms occurs when $x = i$ and $y = p(p-1)$. However, using Fermat's Little Theorem, we know that $i^{p-1} \equiv 1 \pmod p$, so that $i^{p(p-1)} = i^{(p-1)^p} \equiv 1^p \pmod p \equiv 1 \pmod p$. Thus, $i^{i+p(p+1)} \equiv i^i(1) \equiv i^i \pmod p$. Since $a_i = i^i$, we have shown that $a_{i+p(p-1)} \equiv a_i \pmod p$ which is sufficient to show that the sequence $1^1, 2^2, 3^3, \ldots$ is periodic with period $p(p-1)$. □

## 6. Problem 6

**Problem 6.1.** *Suppose* $(10a, q) = 1$*, and that* $k$ *is the order of* $10 \pmod q$*. Show that the decimal expansion of the rational number* $a/q$ *is periodic with smallest period* $k$*.*

**Solution** Note that computing $a/q$ yields the following recurrence, where $r_i$ is the $i$th remainder when divided by $q$:

$$10r_n = qk_{n+1} + r_{n+1} \tag{6.1}$$

$$r_0 = a \tag{6.2}$$

This can be rewritten in modulo form as $10r_n \equiv r_{n+1} \pmod q$. Since $r_0 = a$, we can actually write an explicit formula for this by first substituting $r_0 = a$, then computing $r_{n+1}$ using our recursive formula. This yields:

$$r_n \equiv 10^n a \pmod q \tag{6.3}$$

Now, since $k$ is the order of 10 modulo $q$, we know that it is the smallest integer such that $10^k \equiv 1 \pmod q$. Because of this, we know that the remainders are congruent to the following sequence modulo $q$:

$$a, 10a, 10^2a, \ldots, 10^{k-1}a, a, 10a, \ldots, 10^{k-1}a, \ldots \tag{6.4}$$

This follows since $r_n \equiv 10^n a \pmod q$ and as soon as $n = k$, we have $r_k \equiv a \pmod q$ and the sequence begins anew. Clearly, the sequence of remainders has a period of $k$, so the length of the period $\lambda$ of the decimal expansions is at most $k$. To show that the length is exactly $k$, we expand out the rational number $a/q = 0.\overline{q_1 q_2 \ldots q_\lambda}$:

$$\frac{a}{q} = \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \ldots + \frac{q_\lambda}{10^\lambda}\right) + \left(\frac{q_1}{10^{\lambda+1}} + \frac{q_2}{10^{\lambda+2}} + \ldots + \frac{q_\lambda}{10^{2\lambda}}\right) + \ldots \tag{6.5}$$

$$= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \ldots + \frac{q_\lambda}{10^\lambda}\right)\left(1 + \frac{1}{10} + \frac{1}{10^2} + \ldots\right) \tag{6.6}$$

$$= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \ldots + \frac{q_\lambda}{10^\lambda}\right)\left(\sum_{i=0}^{\infty}\frac{1}{10^{\lambda i}}\right) \tag{6.7}$$

$$= \left(\frac{q_1}{10} + \frac{q_2}{10^2} + \ldots + \frac{q_\lambda}{10^\lambda}\right)\left(\frac{10^\lambda}{10^\lambda - 1}\right) \tag{6.8}$$

$$= \left(\frac{q_1 10^{\lambda-1} + q_2 10^{\lambda-2} + \ldots + q_\lambda}{10^\lambda}\right)\left(\frac{10^\lambda}{10^\lambda - 1}\right) \tag{6.9}$$

$$= \frac{q_1 10^{\lambda-1} + q_2 10^{\lambda-2} + \ldots + q_\lambda}{10^\lambda - 1} \tag{6.10}$$

Therefore, we have shown that $q | 10^\lambda - 1$, which shows that $10^\lambda \equiv 1 \pmod q$. This means that $k | \lambda$, and since $\lambda \leq k$, we must have $k = \lambda$.

□