MAT4003 Assignment 4

1

(a)

Check in $\mathbb{Z}_{11}^* = \{1, 2, 3, \ldots, 10\}$. There are $\phi(10) = 4$ primitive roots. Since

$$1^1 \equiv 3^5 \equiv 4^5 \equiv 5^5 \equiv 9^5 \equiv 10^1 \equiv 1 \pmod{11},$$

the remaining four $\boxed{2, 6, 7, 8}$ are all the primitive roots modulo 11.

(b)

Check in $\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. There are $\phi(\phi(26)) = 4$ primitive roots. Since

$$1^1 \equiv 3^3 \equiv 5^4 \equiv 9^3 \equiv 17^6 \equiv 21^4 \equiv 23^6 \equiv 25^1 \equiv 1 \pmod{26},$$

all primitive roots modulo 26 are $\boxed{7, 11, 15, 19.}$

2

(a)

Write $22 = 2^1 11^1$.

$$\begin{aligned} 5^{22/2} &= 5^{11} \equiv 22 \not\equiv 1 \pmod{23} \\ 5^{22/11} &\equiv 5^2 \equiv 2 \not\equiv 1 \pmod{23}. \end{aligned}$$

Therefore by p. 16 of Lecture Notes of Section 4, $\boxed{5}$ is a primitive root of 23.

(b)

Note that $529 = 23^2$. Since 5 is a primitive root of 23, by Theorem (4.12) either 5 or $5 + 23 = 28$ must be a primitive root of 529. But $28^{22} \equiv 1 \pmod{529}$. Therefore $\boxed{5}$ is a primitive root of 529.

3

Claim. $\boxed{3}$ is such a number.

Proof. 7^k : For $k = 1$ we use the algorithm on p. 16 of Lecture Notes of Section 4. Factor $6 = 2^1 3^1$. Then
$3^{6/2} \equiv 3^3 \equiv 6 \not\equiv 1 \pmod{7}; 3^{6/3} \equiv 3^2 \equiv 2 \not\equiv 1 \pmod{7}$. Therefore 3 is a primitive root modulo 7. Similarly for $k = 2$, factor $48 = 2^4 3^1$. Then
$3^{48/2} \equiv 3^{24} \equiv 22 \not\equiv 1 \pmod{49}; 3^{48/3} \equiv 3^{16} \equiv 3 \not\equiv 1 \pmod{49}$. Thus 3 is also a primitive root modulo 7^2. It follows from Theorem (4.13) that 3 is a primitive root modulo p^k for all $k \geq 1$.

$2(7^k)$: Given any k, we have proved that 3 is a primitive root modulo 7^k. Now we want to show that $n := \text{ord}_{2 \cdot 7^k} 3 = \phi(2 \cdot 7^k) = 6 \cdot 7^{k-1} = \phi(7^k)$.

Since 3 is a primitive root of 7^k, we have $3^{\phi(7^k)} \equiv 1 \pmod{7^k}$. Note that
$3^{\phi(7^k)} \equiv 1^{\phi(7^k)} \equiv 1 \pmod{2}$, and $(2, 7^k) = 1$. It follows from CRT that
$3^{\phi(7^k)} \equiv 1 \pmod{2 \cdot 7^k}$. Therefore $n | \phi(7^k)$. Also by definition of n,
$3^n \equiv 1 \pmod{2 \cdot 7^k}$. Again using CRT we have $3^n \equiv 1 \pmod{7^k}$. It follows that $\text{ord}_{7^k} 3 = \phi(7^k) | n$. Finally $n = \phi(7^k)$. $\square$

4

Consider $p = 4$, which is not a prime. And let $f(x) := 2x$. Then the congruence

$$f(x) = 2x \equiv 0 \pmod{4}$$

has *two* incongruent solutions, namely $x_{1,2} \equiv 0, 2 \pmod{4}$, instead of one.

5

Consider $x \in \{0, 1, \ldots p-1\}$. Clearly $x \equiv 1$ is not a solution to the congruence as $p - 1 \equiv -1 \not\equiv 0 \pmod{p}$. For $x \not\equiv 1$, congruence becomes

$$\frac{x^{p-1} - 1}{x - 1} \equiv 0 \pmod{p}.$$

Multiplying $x - 1$ on both sides yields

$$x^{p-1} \equiv 1 \pmod{p},$$

which by FLT is true for any x coprime to p. In this case
$x \equiv 2, 3, \cdots, p-1 \pmod{p}$. Therefore

$$\boxed{x \equiv 2, 3, \cdots, p-1 \pmod{p}.}$$

6

Lemma. Let p be prime with $p \geq 5$. If g is a primitive root modulo p, then g^{-1} is a primitive root modulo p with $g \not\equiv g^{-1} \pmod{p}$.

Proof. We prove the contrapositive. Assume g to be such that g^{-1} is not a primitive root modulo p. Then $(g^{-1})^x \equiv 1 \pmod{p}$ for some $x < \phi(p) = p - 1$. But then $g^x \equiv (g^{-1})^x g^x \equiv (gg^{-1})^x \equiv 1 \pmod{p}$. So g is not a primitive root either. Moreover, if g is a primitive root modulo p, then since $p \geq 5$,
$|g| \not\equiv 1 \pmod{p}$. It follows from Lemma (2.12) that $g^2 \not\equiv 1 \pmod{p}$, whence
$g \not\equiv g^{-1} \pmod{p}$. $\square$

Let p be prime with $p \geq 5$. There are precisely $\phi(\phi(p)) = \phi(p-1)$ primitive roots modulo p. It follows from Lemma above that those $\phi(p-1)$ roots can be partitioned into $\phi(p-1)/2$ pairs of mutual inverses modulo p.

7

Let g be the primitive root modulo p. Then $\{g, g^2, \dots g^{p-1}\}$ forms a reduced residue system modulo p, by Theorem (4.6). It follows that

$$S_k = \sum_{n=1}^{p-1} n^k \equiv \sum_{n=1}^{p-1} g^{kn} \equiv \frac{g^k - g^{kp}}{1 - g^k} \pmod{p}. \tag{1}$$

If $(p-1)|k, k = m(p-1)$,

$$S_k = \sum_{n=1}^{p-1} g^{(p-1)mn} \equiv \sum_{n=1}^{p-1} 1^{mn} \equiv p - 1 \equiv -1 \pmod{p}.$$

If $(p-1) \not| \ k$, multiply $g^k - 1$ on both sides of (1) :

$$(g^k - 1)S_k \equiv g^{kp} - g^k \equiv g^k - g^k \equiv 0 \pmod{p}.$$

By Theorem (4.1), $g^k \not\equiv 1 \pmod{p}$. Canceling $g^k - 1$ gives $S_k \equiv 0 \pmod{p}$. So

$$S_k \equiv \begin{cases} -1 & \text{if } (p-1)|k, \\ 0 & \text{otherwise.} \end{cases}$$

8

Suppose some odd prime p divides $2^m - 1$. Then $2^m \equiv 1 \pmod{p}$. By Theorem (4.1), $\text{ord}_p 2 | m$. Since m is odd, $\text{ord}_p 2$ is odd. Assume some odd prime q divides $2^n + 1$. Then $2^n \equiv -1 \pmod{q}$. So $\text{ord}_q 2 \not| \ n$. Also $2^{2n} \equiv 1 \pmod{q}$. It follows that $\text{ord}_q 2 | 2n$, whence $\text{ord}_q 2 | 2$. So $\text{ord}_p 2 \neq \text{ord}_q 2$, and $p \neq q$. Since $2^m - 1$ and $2^n + 1$ share no common prime factor, by FTA, $(2^m - 1, 2^n + 1) = 1$.

9

By Corollary (4.2), $\text{ord}_n a = (n-1) | \phi(n)$. So $n - 1 \leq \phi(n)$. But $\phi(n) \leq n - 1$. Therefore $\phi(n) = n - 1$. n is a prime. $\square$

10

Denote the sequence as (a_n).

Lemma 1. (a_n) is periodic with period $p(p-1)$.

Proof. If $p|n$, then $n \equiv 0 \pmod{p}$,

$$(n+t)^{n+t} \equiv (0+0)^{n+t} \equiv 0^n \equiv n^n \pmod{p}.$$

Assume $p \not| \ n$. Then by FLT,

$$(n+t)^{n+t} \equiv n^{n+p(p-1)} \equiv n^n 1^p \equiv n^n \pmod p. \quad \square$$

Lemma 2. If (a_n) is periodic with a period of h, then $p(p-1)|h$.

Proof. Write $h = pq + r, 0 \le r < p$. Since h is period, it holds for all $n \ge 1$

$$(n+h)^{n+h} \equiv (n+r)^{n+h} \equiv n^n \pmod p.$$

Specifically, with $n := p$, we have

$$r^{p+h} \equiv 0 \pmod p.$$

Since $r < p$, $(r, p) = 1$. So $(r^{p+h-1}, p) = 1$. Canceling r^{p+h-1} yields

$$r \equiv 0 \pmod p \implies r = 0 \implies p|h.$$

Also write $h = (p-1)q' + r', 0 \le r' < p-1$. Then for all positive integers n, k

$$(n+kh)^{n+kh} \equiv n^n \pmod p$$

Let $k := sp$, $s \ge 1$, we have

$$n^{n+kh} \equiv n^n \pmod p \implies n^{kh} \equiv 1 \pmod p.$$

By FLT,

$$n^{kh} \equiv [(n^{p-1})^{q'} n^{r'}]^k \equiv n^{kr'} \equiv n^{sr'} \equiv 1 \pmod p.$$

Let g be a primitive root of p, and set $n := g$. Pick $s := 1$ and 2, we have

$$g^{r'} \equiv g^{2r'} \equiv 1 \pmod p \implies 1 \equiv 2 \pmod{\mathrm{ord}_p g^{r'}}.$$

Thus $\mathrm{ord}_p g^{r'} = \frac{\mathrm{ord}_p g}{(\mathrm{ord}_p g, r')} = \frac{p-1}{(p-1, r')} = 1$. So $(p-1, r') = p-1$. But $0 \le r' < p-1$, whence $r' = 0$, $(p-1)|h$. Since $(p, p-1) = 1$, we have $p(p-1)|h$. $\square$

Let $t := p(p-1)$, and s be the smallest period of (a_n). We wish to show $t = s$. Since t and s are both periods of (a_n), it holds for all $n \ge 1$ that $a_n = a_{n+xt+ys}$, where $xt + ys > 0$. By Bézout's Lemma, $d := (s, t)$ gives another period of (a_n). This forces $d = s$, whence $s|t$. By Lemma 2, we also have $t|s$. Therefore $t = s$. $\square$

11

Lemma. Let p be a prime. Then $x^2 \equiv 1 \pmod{p^k} \iff x \equiv \pm 1 \pmod{p^k}$.

Proof. Consider $f(x) := x^2 - 1 \equiv 0 \pmod p$. By Lagrange's Theorem, there are exactly two solutions $x_{1,2} \equiv \pm 1 \pmod p$.
$f'(x_1) \equiv 2 - 1 \equiv 1 \not\equiv 0 \pmod p$. By Hensel's Lemma, $x_1 \equiv 1 \pmod p$ can be uniquely lifted to modulo p^k. Now $f'(x_2) \equiv -3 \pmod p$. If $p \ne 3$, then $f'(x_2) \not\equiv 0 \pmod p$. Again by Hensel's Lemma x_2 can be uniquely lifted to a root modulo p^k. Suppose $p = 3$. To lift x_2 to modulo 3^2, we try $-1 + 3 \equiv 2, -1 + 2 \cdot 3 \equiv 5, -1 + 3 \cdot 3 \equiv 8 \pmod 9$, with only $f(8) \equiv 0 \pmod 9$. In general, if $x \equiv 3^k - 1 \pmod{3^k}$ is the only solution to $f(x) \equiv 0 \pmod{3^k}$, then among the lifted $x, x + 3^k, x + 2 \cdot 3^k \pmod{3^{k+1}}$,

$$\begin{aligned} f(x) &\equiv 3^{2k} - 2 \cdot 3^k \equiv 3^k \pmod{3^{k+1}} \\ f(x+3^k) &\equiv f(2 \cdot 3^k - 1) \equiv -3^k \pmod{3^{k+1}} \\ f(x + 2 \cdot 3^k) &\equiv f(3^{k+1} - 1) \equiv 0 \pmod{3^{k+1}}. \end{aligned}$$

Only $f(3^{k+1} - 1) \equiv 0 \pmod{3^{k+1}}$. By induction, x_2 is uniquely lifted to modulo 3^k. Thus for any odd prime p, $f(x) \equiv 0 \pmod{p^k}$ has exactly two solutions. Since $x \equiv \pm 1 \pmod{p^k}$ are two solutions, the lemma follows. $\square$

Let g be a primitive root of n. Then

$$\prod_{i \in \mathbb{Z}_n^*} i \equiv \prod_{i=1}^{\phi(n)} g^i \equiv g^{1+2+\cdots+\phi(n)} \overset{n \geq 2}{\equiv} g^{\phi(n)/2} \pmod{n}.$$

If $n = 2$ or 4. Primitive roots are 1 and 3 respectively. We have

$$\prod_{i \in \mathbb{Z}_2^*} i \equiv 1^1 \equiv -1 \pmod{2}; \prod_{i \in \mathbb{Z}_4^*} i \equiv 3^{2/2} \equiv -1 \pmod{4}.$$

If $n = p^k$, where p is an odd prime. Then $\phi(n) = p^k - p^{k-1}$,

$$\prod_{i \in \mathbb{Z}_n^*} i \equiv g^{\frac{p-1}{2} p^{k-1}} \pmod{p^k}.$$

Since $(g^{(p-1)/2})^2 \overset{\text{FLT}}{\equiv} 1 \pmod{p^k}$, by Lemma, $g^{(p-1)/2} \equiv 1$ or $-1 \pmod{p^k}$. But $g^{(p-1)/2} \equiv 1$ is impossible as g is a primitive root modulo n. Therefore

$$\prod_{i \in \mathbb{Z}_n^*} i \equiv (-1)^{p^{k-1}} \equiv -1 \pmod{p^k}.$$

If $n = 2p^k$, where p is any odd prime. Then $\phi(n) = \phi(p^k) = p^k - p^{k-1}$. The argument coincides with the last case. Therefore in all cases,

$$\prod_{i \in \mathbb{Z}_n^*} i \equiv -1 \pmod{n}. \quad \square$$