MA246 Number Theory 2013

Test 3 Solutions

1. Let n be a positive integer; denote by $D(n)$ the set of *odd* divisors of n and by $\Phi_{odd}(n)$ the sum $\sum_{d \in D(n)} \varphi(d)$. Then $\Phi_{odd}(n)$ is equal to

(a) n. (b) $\Phi_{odd}(3n)$. (c) $\varphi(n)$. (d) $\Phi_{odd}(2n)$.

Solution: The set $D(n)$ coincides with the set $D(2n)$, since the odd divisors of $2n$ are also divisors of n. We deduce that the correct answer is **(d)**.

2. For how many integer values of $n \geq 1$ is there a primitive root modulo $n(n+1)$?

(a) 0. (b) 1. (c) 2. (d) infinitely many values.

Solution: If m is a positive integer and a primitive root modulo m exists, then either m is a prime power or it is twice a prime power. The two numbers n and $n+1$ are relatively prime and one of them is even; it follows that if there is a primitive root modulo $n(n+1)$, then one among $n, n+1$ must be two. This leaves as possibilities $n \in \{1, 2\}$ and hence $n(n+1) \in \{2, 6\}$, both of which admit primitive roots. The answer is **(c)**.

3. Let $n \geq 2$ be an integer such that there is a primitive root modulo n^2. Then

(a) n is prime. (b) n is even. (c) n is a square. (d) none of the above.

Solution: The assumption that n^2 admits a primitive root rules out the possibility that n is even (with the exception of $n = 2$), so that n must be either 2 or an odd prime power. Since the square of an odd prime power always admits a primitive root, it follows that n need not be prime, it may not be even and it may not be a square: for instance $n = 27$ shows that **(a)**, **(b)** and **(c)** are wrong. The correct answer is **(d)**.

4. Let n be a positive integer; for a primitive root a modulo n, denote by $\ell_a(x)$ the (finite) logarithm of x to the base a modulo n. Let a, b be elements of $\mathbb{U}_n$; if a and ab are primitive roots modulo n then $\ell_a(x)$ is equal to

(a) $\ell_{ab}(x)(1 + \ell_a(b))$. (b) $\ell_{ab}(x) - \ell_b(x)$. (c) $\frac{\ell_{ab}(x)}{\ell_b(x)}$. (d) $\frac{\ell_{ab}(x)}{b}$.

Solution: We have $x = (ab)^{\ell_{ab}(x)} = a^{\ell_{ab}(x)} b^{\ell_{ab}(x)} = a^{\ell_{ab}(x)} a^{\ell_a(b)\ell_{ab}(x)} = a^{\ell_{ab}(x) + \ell_a(b)\ell_{ab}(x)}$ and we deduce that the identity $\ell_a(x) = \ell_{ab}(x)(1 + \ell_a(b))$ holds: this is enough to deduce that the correct answer is **(a)**. It is also easy to check that the answers **(b)**, **(c)** and **(d)** are wrong.

5. Assume that 2 is a primitive root modulo 13 and denote by $\ell_2(x)$ the (finite) logarithm of x to the base 2 modulo 13. Then $\ell_2(7)$ is equal to

(a) 9. (b) 10. (c) 11. (d) 12.

Solution: Since $2 \cdot 7 \equiv 1 \pmod{13}$, we deduce that $7 \equiv 2^{-1} \pmod{13}$ and therefore $\ell_2(7) \equiv -1 \pmod{12}$, so that $\ell_2(7) = 11$: **(c)** is the correct answer.

6. The number of primitive roots g modulo 26 with $0 \leq g \leq 26$ is

(a) 0. (b) 4. (c) 5. (d) 6.

Solution: Since $26 = 2 \cdot 13$ is twice an odd prime, it does have primitive roots; the number of them is $\varphi(\varphi(26)) = \varphi(12) = \varphi(4)\varphi(3) = 4$: answer **(b)**.

7. The **sum** of the primitive roots g modulo 23 with $2 \le g \le 22$ is

(a) 139. (b) 140. (c) 141. (d) 142.

Solution: It is easy to check that 5 is a primitive root modulo 23, and hence the primitive roots modulo 23 are 5, $5^3 \equiv 10$, $5^5 \equiv 20$, $5^7 \equiv 17$, $5^9 \equiv 11$, $5^{13} \equiv 21$, $5^{15} \equiv 19$, $5^{17} \equiv 15$, $5^{19} \equiv 7$, $5^{21} \equiv 14$. Thus the required sum is $5+10+20+17+11+21+19+15+7+14 = 139$ and the answer is **(a)**.

8. If a is a primitive root modulo n, then
(a) $a+1$ is a primitive root modulo n.
(b) $a+1$ is not a primitive root modulo n.
(c) a^2 is a primitive root modulo n.
(d) the inverse of a modulo n is a primitive root modulo n.

Solution: It is easy to check that **(a)** is wrong $(n = 5, a = 3)$, **(b)** is wrong $(n = 5, a = 2)$, **(c)** is wrong $(n = 5, a = 3)$. On the other hand, it is clear that if a generates the group $\mathbb{U}_n$ of units modulo n, then also a generates it: answer **(d)**.

9. Let $n \ge 2$ be an integer and let $S_n = \left\{ m \in \mathbb{N} \;\middle|\; \frac{\varphi(m)}{m} = \frac{\varphi(n)}{n} \right\}$. Then the set S_n
(a) is infinite for all values of $n \ge 2$.
(b) is finite for all values of $n \ge 2$.
(c) is finite when n is not a prime power.
(d) is sometimes infinite and sometimes finite.

Solution: Recall the formula $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$; it follows that the quantity $\frac{\varphi(n)}{n}$ depends only on the prime factors of n and not on their exponents. In particular, S_n contains the infinite set $\{n, n^2, n^3, \ldots, n^a, \ldots\}$. The correct answer is **(a)**.

10. Let m, n be integers satisfying $1 \le m \le n$; then

(a) $\varphi(m) \le \varphi(n)$; (c) $\varphi(m) \ge \varphi(n)$;
(b) $\varphi(n) \le \varphi(mn)$; (d) $\varphi(m) \le \varphi(n + 10)$.

Solution: **(a)** is wrong $(6 = \varphi(9) \not\le \varphi(10) = 4)$; **(c)** is wrong $(1 = \varphi(2) \not\ge \varphi(3) = 2)$; **(d)** is wrong $(22 = \varphi(23) \not\le \varphi(33) = 20)$: **(b)** is the correct answer.

11. The number 5 is a primitive root modulo **both** of the following numbers:

(a) 4 and 13 (b) 3 and 11 (c) 3 and 729 (d) none of these.

Solution: $5^4 \equiv 1 \pmod{13}$ and $5^5 \equiv 1 \pmod{11}$, which rules out **(a)** and **(b)**. Next, 5 is a primitive root modulo 3. To be a primitive root modulo $729 = 3^6$ it suffices to show that $5^{3-1} \not\equiv 1 \pmod{3^2}$ or, equivalently, $25 \not\equiv 1 \pmod 9$ which is OK. So **(c)** is true.