Homework #10 Solutions

9.1.1. (a) Since $\phi(5) = 4$ and $2 \not\equiv 1 \pmod 5$, $\text{ord}_5(2) \in \{2, 4\}$. As $2^2 = 4 \not\equiv 1 \pmod 5$, it follows that $\text{ord}_5(2) = 4$.
(b) Since $\phi(10) = \phi(2 \cdot 5) = \phi(2)\phi(5) = 1 \cdot 4 = 4$ and $3 \not\equiv 1 \pmod{10}$, $\text{ord}_{10}(3) \in \{2, 4\}$. As $3^2 = 9 \not\equiv 1 \pmod{10}$, it follows that $\text{ord}_{10}(3) = 4$.
(c) We have $\phi(13) = 12$ and $10 \not\equiv 1 \pmod{13}$, so $\text{ord}_{13}(10) \in \{2, 3, 4, 6, 12\}$. When computing successive powers of 10, we can (and will) reduce the complexity of the computations in an ad hoc manner. Here we go:

$$\begin{aligned}
&10^2 \equiv (-3)^2 \equiv 9 \not\equiv 1 \pmod{13}\\
&10^3 = 10^2 \cdot 10 \equiv 9 \cdot (-3) \equiv -27 \equiv -1 \equiv 12 \not\equiv 1 \pmod{13}\\
&10^4 = 10^3 \cdot 10 \equiv (-1) \cdot (-3) \equiv 3 \not\equiv 1 \pmod{13}\\
&10^6 = 10^4 \cdot 10^2 \equiv 3 \cdot 9 = 27 \equiv 1 \pmod{13}.
\end{aligned}$$

Thus $\text{ord}_{13}(10) = 6$.

9.1.12. Let $s = \text{ord}_n(a)$, $t = \text{ord}_n(b)$, and $u = \text{ord}_n(ab)$. We have

$$(ab)^{st} = (a^s)^t (b^t)^s \equiv 1^t \cdot 1^s \equiv 1 \pmod n,$$

so u divides st by Theorem 9.1. On the other hand, by definition, $a^s, (ab)^u \equiv 1 \pmod n$, and it follows that

$$b^{su} \equiv (a^s)^u b^{su} \equiv a^{su} b^{su} \equiv (ab)^{su} \equiv ((ab)^u)^s \equiv 1^s \equiv 1 \pmod n.$$

Thus, again applying Theorem 9.1, we may conclude that t divides su. Since $(s, t) = 1$, we in fact have $t \mid u$. By symmetry, $s \mid u$ as well, which implies that $st \mid u$ because $(s, t) = 1$. Therefore $st = u$.

9.1.16. If $\text{ord}_m(a) = m - 1$, then we necessarily have $m \geq 2$, as the function $\text{ord}_m(-)$ only assumes positive values, and Corollary 9.1.1 implies that $m - 1$ divides $\phi(m)$. Thus $m - 1 \leq \phi(m)$. Since the definition of ϕ makes it clear that $\phi(m) \leq m - 1$ for $m \geq 2$, it must be that $\phi(m) = m - 1$. It now follows from Theorem 7.2 that m is prime.

9.1.17. As a primitive root modulo p is, by definition, relatively prime to p, we will assume throughout that r is an integer with $(r, p) = 1$. If r is a primitive root modulo p, then by definition we have $\text{ord}_p(r) = \phi(p) = p - 1$. For every prime q dividing $p - 1$, $0 < (p - 1)/q < p - 1$, so, because $\text{ord}_p(r)$ is the smallest positive integer d for which $r^d \equiv 1 \pmod p$, we must have $r^{(p-1)/q} \not\equiv 1 \pmod p$. Assume conversely that, for all prime divisors q of $p - 1$, $r^{(p-1)/q} \not\equiv 1 \pmod p$. Suppose for the sake of a contradiction that $t = \text{ord}_p(r) < p - 1$. By Corollary 9.1.1, t divides $p - 1$, so $(p - 1)/t$ is a positive integer greater than 1, and therefore has a prime divisor q. Writing $(p - 1)/t = qk$ for some integer k, and rearranging, we see that $p - 1 = qtk$, so q is also a prime divisor of $p - 1$. We then have

$$r^{(p-1)/q} = r^{tk} = (r^t)^k \equiv 1^k \equiv 1 \pmod p,$$

Date: May 3, 2018.

contrary to assumption. Thus we must have $\mathrm{ord}_p(r) = p-1$, i.e., r must be a primitive root modulo p.

9.1.19. For any integer $n \geq 0$ we have, tautologically, $2^{2^n} \equiv -1 \pmod{F_n}$. Squaring both sides of this congruence then gives $2^{2^{n+1}} \equiv (-1)^2 \equiv 1 \pmod{F_n}$. Therefore, by the definition of order, we have $\mathrm{ord}_{F_n}(2) \leq 2^{n+1}$.

9.1.21. We assume $a > 1$ so that $m = a^n - 1$ is positive for all positive integers n, and we observe that $(a, m) = 1$, as any common divisor of a and m would necessarily divide $a^n - m = a^n - (a^n - 1) = 1$. Since $a^n - 1 \equiv 0 \pmod{m}$, $a^n \equiv 1 \pmod{m}$, and therefore, by Theorem 9.1, $t = \mathrm{ord}_m(a)$ divides n. In particular, $t \leq n$. On the other hand, we have $a^t \equiv 1 \pmod{m}$ by definition, so that $m = a^n - 1$ divides $a^t - 1$. This implies that $a^n - 1 \leq a^t - 1$, hence that $a^n \leq a^t$, which forces $n \leq t$. Thus $n = t$, and Corollary 9.1.1 allows us to conclude that n divides $\phi(m)$.

9.2.9. Since $p \equiv 1 \pmod{4}$, i.e., since 4 divides $p-1$, Theorem 9.8 implies that there is an integer x relatively prime to p with $\mathrm{ord}_p(x) = 4$. Thus $x^4 \equiv 1 \pmod{p}$, which implies that x^2 is a root of $X^2 - 1$ modulo p. Because p is odd (being congruent to 1 modulo 4), it follows that $x^2 \equiv \pm 1 \pmod{p}$. However, we cannot have $x^2 \equiv 1 \pmod{p}$, as this would contradict the assumption that $\mathrm{ord}_p(x) = 4$. Therefore it must be that $x^2 \equiv -1 \pmod{p}$.

9.2.16. We first observe that $p - a^2 \equiv -a^2 \pmod{p}$, so $\mathrm{ord}_p(p - a^2) = \mathrm{ord}_p(-a^2)$, and it is enough to show that $-a^2$ is a primitive root modulo p (one can work directly with $p - a^2$, but working with $-a^2$ is a bit simpler). To this end, let $t = \mathrm{ord}_p(-a^2)$, so that, by Corollary 9.1.1, t divides $\phi(p) = 2q$. As 2 and q are prime, this means that $t \in \{1, 2, q, 2q\}$. If $t = 1$ or $t = 2$, then $a^4 = (-a^2)^2 \equiv 1 \pmod{p}$, so that $\mathrm{ord}_p(a)$ divides 4. But $\mathrm{ord}_p(a)$ also divides $\phi(p) = 2q$, which is not divisible by 4, so $\mathrm{ord}_p(a) = 1$ or $\mathrm{ord}_p(a) = 2$. The first equality is impossible because $1 < a < p-1$, so we cannot have $a \equiv 1 \pmod{p}$. If $\mathrm{ord}_p(a) = 2$, then $a^2 \equiv 1 \pmod{p}$, so p divides $a^2 - 1 = (a-1)(a+1)$, which implies that $a \equiv \pm 1 \pmod{p}$, another impossibility due to the assumption that $1 < a < p-1$. Thus $t \neq 1$ and $t \neq 2$. Now note that, because q is odd and $\phi(p) = 2q$, Euler's theorem gives

$$(-a^2)^q = (-1)^q (a^2)^q = -a^{2q} \equiv -1 \pmod{p}.$$

If $t = q$, then, using the above congruence, we would have $1 \equiv (-a^2)^q \equiv -1 \pmod{p}$, a contradiction since p is odd. The only remaining possibility is that $t = 2q = \phi(p)$, which means that $-a^2$ is indeed a primitive root modulo p.