Hints for exercises in chapter 7

Exercise 7.1.2(b). Use the technique in the proof of Lemma 7.1.1.

Exercise 7.2.2. Let $k := \mathrm{ord}_m(a)$ and $A = \{1, a, a^2, \dots, a^{k-1} \pmod m\}$. Show that if b and b' are any two reduced residues mod m, then either bA and $b'A$ are disjoint or are equal. Therefore the sets of the form bA, where b is a reduced residue mod m, which are each of size k, partition the $\phi(m)$ reduced residues mod m. This implies that k divides $\phi(m)$ as desired.

Exercise 7.3.1. Let $k := \mathrm{ord}_q(2)$. We have $2^p \equiv 1 \pmod q$ and so k divides p by Lemma 7.1.2. Therefore $k = 1$ or p, but $k \neq 1$ as $2^1 \not\equiv 1 \pmod q$.

Exercise 7.4.1(a) If n is not of the form p or p^2, write $n = ab$ with $1 < a < b$. If $n = p^2$, then n divides $p \cdot 2p$.

Exercise 7.4.3(a). If $Q = \frac{p-1}{2}$, then

$$(p-1)!/Q! = (p-1)(p-2)\cdots(p-Q) \equiv (-1)(-2)\cdots(-Q) = (-1)^Q Q! \pmod p.$$

Exercise 7.5.2(b). As $(g^{\frac{p-1}{2}})^2 = g^{p-1} \equiv 1 \pmod p$, so $g^{\frac{p-1}{2}}$ is a square root of 1 (mod p); that is, $g^{\frac{p-1}{2}} \equiv 1$ or $-1 \pmod p$. But g has order $p-1$ and so $g^{\frac{p-1}{2}} \not\equiv 1 \pmod p$.

Exercise 7.10.2. Use Proposition 7.4.1.

Exercise 7.10.4. In every solution $n, n-1, n-2$ have prime factors $2, 3, p$ for some $p > 3$. At most one of these integers is divisible by p. Show that the other two lead to a solution to $2^n - 3^m = \pm 1$ and use exercise 7.10.3.

Exercise 7.10.5(b). Use Theorem 7.1.

(d) Make sure a is chosen so that $(q, a-1) = 1$.

Exercise 7.10.6(a). The trick is to write $z^p = ((z-y)+y)^p$ and then use the binomial theorem. One can also write $x_n = \frac{z^n - y^n}{z-y}$ and use exercise 2.5.20(a).

Exercise 7.10.12. Take the j and $p-j$ terms together.

Exercise 7.10.13. Let $M = a_0 + 1$ so that $a_n = 2^n M - 1$ for all $n \geq 0$. Let p be an odd prime dividing a_1. Then p divides a_p.

Exercise 7.10.16(b). Since n is not a Carmichael number, the subgroup in (a) is proper and so contains at most half the reduced residues. (c) Let $q = 2p-1$. Now $n - 1 \equiv p - 1 \pmod{2p-2}$, so that if $(a, n) = 1$, then $a^{n-1} \equiv a^{p-1} \equiv 1 \pmod p$ and $a^{n-1} \equiv a^{p-1} \equiv a^{\frac{q-1}{2}} \equiv \pm 1 \pmod q$.

Exercise 7.10.17(a). $M_p - 1 = 2^p - 2$ is divisible by p.

Exercise 7.12.1(b). Let $f(x_1, \dots, x_p) = (x_2, \dots, x_p, x_1)$ in part (a).

Exercise 7.17.4(c). Consider $\gcd(q^\ell - 1, (q^n - 1)/(q^\ell - 1))$. (d) Use Lemma 7.17.1.

Exercise 7.18.1. Let $g = \gcd(\lambda(p^e), \lambda(q^f))$ where p^e and q^f are powers of the two different primes dividing m (where $f \geq 2$ if $q = 2$), so that 2 divides g. Now

$$\lambda(m) = \mathrm{lcm}[\lambda(p^e) : p^e \| m] \leq \frac{1}{g} \prod_{p^e \| m} \lambda(p^e) \leq \frac{1}{g} \prod_{p^e \| m} \phi(p^e) = \frac{\phi(m)}{g} < \phi(m).$$

Exercise 7.18.5(a). Recall exercise 4.3.7.

Exercise 7.19.1. In one direction let $y = x^{n/g}$. In the other, write $g = an + b\lambda(m)$ so that if $x = y^a$, then $x^n \equiv (y^a)^n (y^{\lambda(m)})^b \equiv y^g \pmod{m}$.

Exercise 7.25.1(b). You might show that if $p \cdot 1 = q \cdot 1 = 0$ where p and q are distinct primes, then $1 = 0$.

Exercise 7.25.3(a). You might use the ideas in the proof of Theorem 7.6.

Exercise 7.28.6. Consider divisibility by F_r where 2^r is the highest power of 2 dividing $k - \ell$. Then we must have $p = F_r$ and so $2^{2^n} - 1 = 2^{2^r} + 1 + 2^{\ell + j2^r} + 2^\ell$. Consider this equation mod 2^4 and we severely limit the possibilities.

Exercise 7.30.1(b). Multiply through by $1 - x^{m_k}$ and then substitute in x to be a root of $\phi_{m_k}(x)$.

Exercise 7.33.1(b). Show that $|\phi_n(a)| > n$ if $\phi(n) > 2$, and for $\phi(n) = 2$ with $|a| > 2$. Analyze carefully the remaining few cases.

Exercise 7.33.2(b). Prove that $\Delta = (\alpha - \beta)^2$. (c) Use exercise 2.5.20, and be careful when p divides a.