SKETCH OF SOLUTIONS (HOMEWORK IX)

20.1- (c) Let

$$s = 1^k + 2^k + \ldots + (p-1)^k \mod p$$

If $k = p-1$, then $s = p-1$ by fermat's little theorem.
If $k < p-1$ then $s = 0$: *proof:* notice that if a is a unit $\mod p$ then $a^k s \equiv s$ therefore $s(a^k - 1) \equiv 0$ so either s is zero or $x^k - 1$ has $p - 1 > k$ roots.

20.2 (a) i) 6, ii) 4, iii) 4, iv) 4
(b) Express $\phi(m) = ke_m(a) + r$ with $0 \le r < e_m(a)$ then

$$1 \equiv a^{\phi(m)} \equiv a^{ke_m(a)+r} \equiv a^r \mod m$$

therefore $r = 0$(by the definition of $e_m(a)$)

20.3 a) $e_{11} = 10$, $e_{13} = 12$, $e_{15} = 4$, $e_{17} = 8$, $e_{19} = 18$
(b) $e_{mn} = \text{lcm}(e_m, e_n)$
(c) $e_{11227} = 1836$
(d) chinese remainder theorem
(e) Let p^z be the highest power of p that divides $a^{e_p} - 1$, then $e_{p^k} = e_p p^{max\{0,k-z\}}$
(f) Compare [LeVeque] theorem 4-6.

20.4 (a) $2, 6, 7, 11$ (b) $d = 1 \to 1$, $d = 2 \to 12$, $d = 3 \to 3, 9$, $d = 4 \to 5, 8$, $d = 6 \to 4, 10$, $d = 12 \to 2, 6, 7, 11$

20.6 (a) g^5, g^7
(b) $\gcd(k, p-1) = 1$ *proof:* Suppose $\gcd(k, p-1) = 1$ then,there exist u, v such that $uk + v(p-1) = 1$. If t is such that $t < p-1$ and $(g^k)^t \equiv 1 \mod p$ then we get $tuk + tv(p-1) = t$ and

$$1 \equiv g^{(tuk)+tv(p-1)} \equiv g^t \mod p$$

i.e. g is not a primitive root!. Now suppose that g^k is a primitive root. If $\gcd(k, p-1) = G > 1$ then we get $(g^k)^{\frac{p-1}{G}} \equiv (g^{\frac{k}{G}})^{p-1} \equiv 1 \mod p$!
(c) The exponents of g which yield primitive roots are $5, 11, 13, 17, 19$

20.7 $5, 7, 17, 19$

20.8 Suppose a is a primitive root.Since p is odd, $p-1$ is even, say $p - 1 = 2k$. Therefore

$$1 \equiv b^{p-1} \equiv b^{2k} \equiv a^k \mod p$$

and thus a is not a primitive root.

21.1 (a) $x = 5$ (b) $x = 27$ (c) no solution (d)$x = 10, 14, 23, 27$

21.3 $I(a) \equiv -I(b) \mod p-1$

References

[LeVeque] LeVeque William J., *Topics in Number Theory Volumes I and II*, Dover **ISBN 0-486-42539-8** (2002)