the *order* of p modulo n_j (the smallest power of p that is $\equiv 1 \ mod \ n_j$).

15. All polynomials in which X^j occurs with nonzero coefficient only if $p|j$.
16. Reduce to the case when $j = d$ by showing that, if $\sigma^j(a) = a$ and $\sigma^f(a) = a$, we have $\sigma^d(a) = a$ (see the proof of Proposition I.4.2). Notice that the field $\mathbf{F}_{p^d}$, which is the splitting field of $X^{p^d} - X$, is contained in $\mathbf{F}_q$, because any root a of this polynomial also satisfies $X^q = X$ (to see this, raise both sides of $a^{p^d} = a$ to the p^d-th power f/d times).
17. Show that $b' = b^{(p^n-1)/(p^d-1)}$ is in $\mathbf{F}_{p^d}$ by showing that it is fixed under σ^d (i.e., raising to the p^d-th power); show that it is a generator by showing that all of the powers $(b')^j$, $j = 0, \ldots, p^d - 2$ are distinct (this follows from the fact that the first $p^n - 1$ powers of b are distinct).

§ II.2.

1. The sets of residues are: for $p = 3$, $\{1\}$; for $p = 5$, $\{1, 4\}$; for $p = 7$, $\{1, 2, 4\}$; for $p = 13$, $\{1, 3, 4, 9, 10, 12\}$; for $p = 17$, $\{1, 2, 4, 8, 9, 13, 15, 16\}$; for $p = 19$, $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$.
2. (b) From part (a) and Propositions II.2.2 and II.2.4 you know that $(\frac{2}{p}) = 1 \equiv 2^{(p-1)/2} \ mod \ p$. This means that the $((p-1)/2^\ell)$-th power of 2 is $\equiv -1 \ mod \ p$ for some $\ell \geq 2$. Since $2^{2^k} \equiv -1 \ mod \ p$, you can show that $g.c.d.((p-1)/2^\ell, 2^k) = 2^k$; and this immediately gives $p \equiv 1 \ mod \ 2^{k+\ell}$. (c) The only prime which is $\equiv 1 \ mod \ 64$ and $< \sqrt{65537}$ is 193, which does not divide 65537.
3. $g.c.d.(84, 1330) = 14$.
4. Write $(\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p})$, and consider the four possible cases of $p \ mod \ 8$.
5. $(\frac{91}{167}) = (\frac{7}{167})(\frac{13}{167}) = -(\frac{167}{7})(\frac{167}{13}) = -(\frac{-1}{7})(\frac{-2}{13}) = -(-1)(-1) = -1$
6. (a) 14; (b) 9; (c) 9α.
7. $a^3 - a$ (see the proof of Proposition II.2.4); 6, 60, 4080, 24, 210, 336.
8. Since $q \equiv 1 \ mod \ p$, there is a primitive p-th root of unity ξ in $\mathbf{F}_q$. Then $G = \sum_{j=1}^{p-1}(\frac{j}{p})\xi^j$ has square $(\frac{-1}{p})p$ (see the lemma in the proof of Proposition II.2.5).
9. (a) $(\frac{-1}{p})\sum_{j=1}^{p-1}(\frac{j}{p})a^j$; 6, 45, 3126, 906 (in the last case use: $1093 = (3^7 - 1)/2$). (b) Let $G = \sum_{j=1}^{p-1}(\frac{j}{p})2^j$. Then the least positive square root of $(\frac{-1}{p})p$ modulo $2^p - 1$ is g if $p \equiv 5 \ mod \ 8$; $-g$ if $p \equiv 3 \ mod \ 8$; $p + g$ if $p \equiv 7 \ mod \ 8$; $p - g$ if $p \equiv 1 \ mod \ 8$.
10. (a) $(\frac{1801}{8191}) = (\frac{8191}{1801}) = (\frac{987}{1801}) = (\frac{3}{1801})(\frac{7}{1801})(\frac{47}{1801}) = (\frac{1}{3})(\frac{2}{7})(\frac{15}{47}) = 1 \cdot 1 \cdot (\frac{3}{47})(\frac{5}{47}) = -(\frac{2}{3})(\frac{2}{5}) = -1$. (b) $(\frac{987}{1801}) = (\frac{1801}{987}) = (\frac{2 \cdot 407}{987}) = -(-1)(\frac{987}{407}) = (\frac{173}{407}) = (\frac{407}{173}) = (\frac{61}{173}) = (\frac{173}{61}) = (\frac{51}{61}) = (\frac{61}{51}) = (\frac{2 \cdot 5}{51}) = -(\frac{5}{51}) = -(\frac{51}{5}) = -1$.
11. (a) 1; (b) 1; (c) 1; (d) 1; (e) 1; (f) 1; (g) -1.
12. (a) $(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{(p-1)/2}(-1)^{(3-1)(p-1)/4}(\frac{p}{3}) = (\frac{p}{3})$, which $= 1$ if and only if $p \equiv 1 \ mod \ 3$. (b) $\left(\frac{3}{2^p-1}\right) = -\left(\frac{2^p-1}{3}\right) = -(\frac{1}{3}) = -1$.