3. *(a – d 1/2 point each, e + f = 2 points.)*
(a) If k is even then $3k + 1 = 6m + 1$ ($k = 2m$). If k is odd then $3k + 1$ is even and greater than 2, hence not prime.
(b) $(3k + 1)(3m + 1) = 3(3km + k + m) + 1$, so a product of primes not equal to $3k + 2$ is of the form or $3k + 1$, or $3k$ if one of the primes is 3. Hence $3k + 2$ must have at least one prime divisor of the same form.
(c) $4k + 3$ has only odd prime factors, that is primes of the form $4k + 1$ or $4k + 3$. Now $(4k + 1)(4m + 1) = 4(4km) + 4(k + m) + 1$, so a product of odd primes not equal to $4k + 3$ is of the form $4k + 1$. Hence $4k + 3$ must have at least one prime factor of the same form.
(d) $6n + 5$ has only prime factors greater than 3. A prime greater than 3 obviously cannot be of the form $6k + \ell$, $\ell = 2, 3, 4$. A product of primes of the form $6k + 1$ is again of that form $((6k + 1)(6m + 1) = 6(6km) + 6(k + m) + 1)$. Hence $6k + 5$ must have at least one prime factor of the same form.
(e) And odd prime (greater than 3) is $\equiv \pm 1 \bmod 6$. Suppose $p_1, \dots, p_n$ are the only primes $\equiv -1 \bmod 6$, and let $N = 6p_1 \cdots p_n - 1$. Only odd primes (greater than 3) divide N, and if all of the prime factors of N are $\equiv 1 \bmod 6$, then so is N, a contradiction. So $p \equiv -1 \bmod 6$ for at least one prime factor p of N. By assumption, $p \in \{p_1, \dots, p_n\}$, so p divides $N - 6p_1 \cdots p_n = 1$, which is absurd. We conclude that there are infinitely many primes $\equiv -1 \bmod 6$.
(f) Put 4 in place of 6 in (e) (and delete "(greater than 3)").

14. *(2 points.)* Write $n = pm$ where p is prime and $m \geq 1$. Then

$$(a^n - 1) = (a^m - 1)(a^{m(p-1)} + a^{m(p-2)} + \cdots + a^m + 1).$$

If this is prime, then $a^m - 1 = 1$ (the other term is greater than 1). Hence $a = 2, m = 1$, that is $n = p$.

1. *(2 points.)* (a) $18 \equiv 1 \bmod 17$ and 18 is a multiple of 3. A complete system of residues modulo 17 consisting only of multiples of 3 is therefore given by $\{18a : a = 0, 1, \dots, 17\}$. (See problem 2.)
(b) $40 \equiv 1 \bmod 13$ and 40 is a multiple of 5. A complete system of residues modulo 13 consisting only of multiples of 5 is therefore given by $\{40a : a = 0, 1, \dots, 12\}$. (See problem 2.)

2. *(2 points.)* Obviously $E' \subseteq E$. If $(a, m) = 1$ then $ka \equiv 1 \bmod m$ for some $k \bmod m$ (for $ak + mk' = 1$ for some integers k, k'). If $y \in E$ then $ka(y - b) \equiv y - b \bmod m$, so $E' \ni ax + b \equiv y \bmod m$, where $x \equiv k(y - b) \bmod m$. Hence $E' = E$. Alternatively, if $E' \subsetneq E$, there exists $x, y \in E$ with $x \not\equiv y \bmod m$ such that $ax + b \equiv ay + b \bmod m$, that is $ax \equiv ay \bmod m$. Then $a(x - y) \equiv 0 \bmod m$. We are assuming $x \not\equiv y \bmod m$, so $a \equiv 0 \bmod m$, contradicting $(a, m) = 1$.

3. *(2 points.)* If m is any integer and $x = 5 + 12m$ then $x \equiv 1 \bmod 4$ and $x \equiv 2 \bmod 3$. Conversely if these two congruences hold then $x = 4m_1 + 1 = 3m_2 + 2$ for integers m_1, m_2, that is $4m_1 - 3m_2 = 1$. Then $(m_1, m_2) \in \{(1 + 3m, 1 + 4m) : m \in \mathbb{Z}\}$ (Euclidean algorithm). Hence $x = 4 + 12m + 1 = 3 + 12m + 2 = 5 + 12m$. We have proved that $x \equiv 1 \bmod 4$ and $x \equiv 2 \bmod 3$ if and only if $x \equiv 5 \bmod 12$.

4. *(1 points.)* We have $(a + b)(a - b) = a^2 - b^2 \equiv 0 \bmod p$, that is $p \mid (a + b)(a - b)$. Then $p \mid (a + b)$ or $(a - b)$ by uniqueness of factorization.

17. *(4 points.)* It is clear that $b \mid N$ if and only if $N - b \equiv 0 \bmod N$ if and only if $N \equiv b \bmod N$. Now
(a) $10^k \equiv 0 \bmod 2$ ($k \geq 1$), hence $N \equiv a_0 \bmod 2$;
(b) $10 \equiv 1 \bmod 3$ so $10^k \equiv 1 \bmod 3$, hence $N \equiv a_n + \cdots + a_0 \bmod 3$;
(c) $10 \equiv 2 \bmod 4$ so $10^k \equiv 2^k \equiv 0 \bmod 4$ ($k \geq 2$), hence $N \equiv 10a_1 + a_0 \bmod 4$;
(d) $10 \equiv 0 \bmod 5$, hence $N \equiv a_0 \bmod 5$;
(f) Note that $7 \cdot 11 \cdot 13 = 1001$, that is $10^3 \equiv -1 \bmod 7, 11$ and 13. Hence $N \equiv a_0 + 10a_1 + 10^2a_2 - (a_3 + 10a_4 + 10^2a_6) + \cdots \bmod 7, 11$ and 13.
(h) $10^k \equiv 1^k \equiv 1 \bmod 9$, hence $N \equiv a_n + \cdots + a_0 \bmod 9$;
(i) $N \equiv a_0 \bmod 10$;
(j) $10^{2k} \equiv (-1)^{2k} \equiv 1 \bmod 11$, $10^{2k+1} \equiv -1 \bmod 11$, hence $N \equiv a_0 - a_1 + \cdots + (-1)^n a_n \bmod 11$.

17 points, plus 3 points for a reasonable attempt at all questions = 20 points.