Carmichael number (for example, a might not divide $rp-1$).

13. Any Carmichael number not listed in Exercise 12(a)–(b) must be at least a product of three distinct primes all ≥ 7.
14. $n = 21$, $b = 8$.
16. (a) By Exercise 1(d), we need only look at the b for which $b^{p-1} \equiv (\frac{b}{2p-1}) = 1 \ mod\ 2p-1$. Since $n-1 \equiv p-1 \ mod\ 2p-2$, we have $b^{(n-1)/2} \equiv b^{(p-1)/2} \ mod\ p$ and $mod\ 2p-1$, i.e., $b^{(n-1)/2} \equiv b^{(p-1)/2} \ mod\ n$. Now $(\frac{b}{n}) = (\frac{b}{2p-1})(\frac{b}{p}) = (\frac{b}{p}) \equiv b^{(p-1)/2} \ mod\ p$, so condition (2) holds if and only if $b^{(p-1)/2} \equiv (\frac{b}{p}) \ mod\ 2p-1$. This holds for exactly half of all b for which $b^{p-1} \equiv 1 \ mod\ 2p-1$ (since in $(\mathbf{Z}/(2p-1)\mathbf{Z})^*$ such b must be a power g^j of a generator g such that $\frac{p-1}{2}j \equiv 0 \ mod\ 4$ if $(\frac{b}{p}) = 1$, $\frac{p-1}{2}j \equiv 2 \ mod\ 4$ if $(\frac{b}{p}) = -1$). (b) $n = p(2p-1)$ where $p \equiv 3 \ mod\ 4$ (by Proposition V.1.5).
17. Compute n modulo $72m$: $n \equiv 36m^2 + 36m + 1$. Thus, $\frac{n-1}{2} \equiv 18m(m+1) \ mod\ 36m$. If m is odd, this means that we always have $b^{(n-1)/2} \equiv 1 \ mod\ n$ (because $p-1 | 36m$ for each $p|n$), and so (2) holds if and only if $(\frac{b}{n}) = 1$, i.e., 50% of the time. If m is even, we still have $b^{(n-1)/2} \equiv 1 \ mod\ 6m+1$ and $mod\ 18m+1$, while $b^{(n-1)/2} \equiv b^{6m} \equiv (\frac{b}{12m+1}) \ mod\ 12m+1$. Thus, in that case (2) holds if and only if $(\frac{b}{12m+1}) = 1$ (so that $b^{(n-1)/2} \equiv 1 \ mod\ n$) and also $(\frac{b}{n}) = 1$, i.e., 25% of the time.
18. (a) $O(log^3 n \, log\, m)$; (b) $O(log^5 n)$.
19. (a) N is composite because n is composite (by the corollary to Proposition I.4.1); then proceed as in Exercise 9 to see that $2^{(N-1)/2} = 2^{2^{n-1}-1} \equiv 1 \ mod\ N$. But since $N \equiv -1 \ mod\ 8$, we also have $(\frac{2}{N}) = 1$. Thus, N is an Euler pseudoprime; by Proposition V.1.5, it is also a strong pseudoprime. (b) Use the same argument as in Exercise 7(c).
20. If the first possibility in (3) holds, then obviously $(b^k)^t \equiv 1 \ mod\ n$. Now suppose that $b^{2^r t} \equiv -1 \ mod\ n$. Write $k = 2^i j$ with j odd. If $i > r$, then $(b^k)^t \equiv 1 \ mod\ n$; if $i \leq r$, then $(b^k)^{2^{r-i}t} = (b^{2^r t})^j \equiv (-1)^j = -1 \ mod\ n$.
21. (a) Show that the necessary and sufficient conditions on b are: $(\frac{b}{17}) = 1$, $(\frac{b}{561}) = 1$. These conditions both hold 25% of the time, i.e., for 80 bases in $(\mathbf{Z}/561\mathbf{Z})^*$. (b) Since $b^{70} \equiv 1 \ mod\ 3$ and $mod\ 11$, it follows that 561 is a strong pseudoprime to the base b if and only if $b^{35} \equiv \pm 1 \ mod\ 561$, i.e., if and only if either (i) $b \equiv 1 \ mod\ 3$, $b \equiv 1 \ mod\ 17$, $(\frac{b}{11}) = 1$, or else (ii) $b \equiv -1 \ mod\ 3$, $b \equiv -1 \ mod\ 17$, $(\frac{b}{11}) = -1$. There are 10 such bases, 5 in case (i) and 5 in case (ii), by the Chinese Remainder Theorem. The 8 nontrivial bases $b \neq \pm 1$ are: 50, 101, 103, 256, 305, 458, 460, 511.
22. Use Exercise 7(a) of § I.3, which says that the only square roots of 1 are ± 1.
23. (a) $8^2 \equiv 18^2 \equiv -1 \ mod\ 65$; $14^2 \equiv 1 \ mod\ 65$, but $14^1 \not\equiv \pm 1 \ mod\ 65$. (b) The case when n is a prime power follows from the previous exercise, so