Interchanging the roles of p and q gives $b^d \equiv 1\ mod\ q$, and so $b^d \equiv 1\ mod\ n$. The converse is similar (actually, easier). There are d^2 bases in $(\mathbf{Z}/n\mathbf{Z})^*$. (b) four: ± 1, $\pm(4p+1)$. (c) $d^2/\varphi(341) = 100/300 = \frac{1}{3}$.

7. (a) See part (b). (b) Since $N - 1 = b(b^{n-1} - 1)/(b-1)$, where the numerator is divisible by n (because n is a pseudoprime to the base b) and the denominator is prime to n, it follows that $n|N-1$. Since $b^n \equiv 1\ mod\ N$ (namely, $(b-1)N = b^n - 1$), we have $b^{N-1} \equiv 1\ mod\ N$. One must also show that N is composite, but this is easy if we use the fact that n is composite by assumption (see the corollary to Proposition I.4.1). The fact that N is odd (whether b is odd or even) follows by writing N in the form $b^{n-1} + b^{n-2} + \cdots + b + 1$. (c) Start with 341, 91, or 217, respectively, and use part (b) to find a sequence of larger and larger pseudoprimes. Note that the condition $g.c.d.(b-1, n) = 1$ always holds when $b = 2, 3, 5$. (d) 15 is a pseudoprime to the base 4, but $N = (4^{15} - 1)/3$ is not. (To see the latter, note that 4 has order 15 in $(\mathbf{Z}/N\mathbf{Z})^*$, but $N - 1 = 4(4^{14} - 1)/3$ is not divisible by 3, let alone 15.)

8. (a) $n = \left(\frac{b^p-1}{b-1}\right)\left(\frac{b^p+1}{b+1}\right)$ (b) Note that n is odd (see the answer to 7(b) above), and so $2|n-1$. Next, since $(n-1)(b^2-1) = b^2(b^{2(p-1)} - 1) \equiv 0\ mod\ p$ and p does not divide $(b+1)(b-1) = b^2 - 1$, it follows that $p|n-1$. (c) Since n is an odd composite number, $b^{2p} \equiv 1\ mod\ n$, and $2p|n-1$, it follows that n is a pseudoprime to the base b. Since there are infinitely many primes greater than $b+1$, in this way we get infinitely many pseudoprimes to the base b.

9. (a) $3^{2046} \equiv 1013\ mod\ 2047$, so (1) fails for $b = 3$. (b) If composite, they will still be pseudoprimes to the base 2. To see this for $n = 2^{2^k} + 1$, we note that $2^{2^k} \equiv -1\ mod\ n$, and then $2^{n-1} \equiv 1\ mod\ n$ can be obtained from this by repeated squaring. For $n = 2^p - 1$, we have $n - 1 = 2(2^{p-1} - 1) \equiv 0\ mod\ p$, and so $2^p = n + 1 \equiv 1\ mod\ n$ implies $2^{n-1} \equiv 1\ mod\ n$. Using (2) with $b = 2$ also won't work, since both sides will be 1, even if the number is composite. Using (3) with $b = 2$ also won't work: for a Fermat number this follows because $2^{2^k} \equiv -1\ mod\ n$, and for a Mersenne number it follows by Proposition V.1.5.

10. Expand the parentheses to show that $n-1$ is divisible by $36m$, and hence by $6m$, $12m$, and $18m$.

12. We suppose $p < q$. The technique to answer (a)–(b) is given in part (c). (a) $561 = 3{\cdot}11{\cdot}17$; (b) $1105 = 5{\cdot}13{\cdot}17$; $2465 = 5{\cdot}17{\cdot}29$; $10585 = 5{\cdot}29{\cdot}73$. (c) Suppose $p < q$. Since $q - 1|rpq - 1 \equiv rp - 1\ mod\ q - 1$, we must have $rp - 1 = a(q-1)$ for some a, $1 < a < r$. Also $p - 1|rq - 1$, and so $p-1|a(rq-1) = r(aq) - a = r(a + rp - 1) - a \equiv (r-1)(a+r)\ mod\ p-1$. Thus, with r fixed and for each fixed a from 2 to $r-1$, there are only finitely many possibilities for p, namely, the primes such that $p-1$ is a divisor of $(r-1)(a+r)$. Then each prime p uniquely determines q, because $rp - 1 = a(q-1)$. Of course, not all a and p lead to a