(Questions marked with a * are optional.)

(1) (a) Find all bases $b$ modulo 15 with $b \not\equiv \pm 1 \mod{15}$, for which 15 is a pseudoprime.
(b) Prove that there are 36 bases $b$ modulo 91 for which 91 is a pseudoprime.
(c) Show that if $p$ and $2p - 1$ are both prime numbers, and $n = p(2p - 1)$, then $n$ is a pseudoprime for precisely half of all possible bases modulo $n$.

(2) Let $n = pq$ be the product of two distinct odd primes.
(a) Set $d = (p - 1, q - 1)$. Prove that $n$ is a pseudoprime to the base $b$ if and only if $b^d \equiv 1 \mod{n}$. Show that there are $d^2$ bases to which $n$ is a pseudoprime.
(b) How many bases are there to which $n$ is a pseudoprime if $q = 2p + 1$? List all of them (in terms of $p$).
(c) For $n = 341$, what is the probability that a randomly chosen prime to $n$ is a base to which $n$ is a pseudoprime?

(3) (a) Find all Carmichael numbers of the form $5pq$ where $p$ and $q$ are prime.
[Hint: We showed in class that 561 is the only Carmichael number of the form $3pq$. Use the same method.]
(b) Prove that for any fixed prime $r$ there are only finitely many Carmichael numbers of the form $rqp$.
[Use the same method you used in part (a).]

(4) Suppose that $m$ is a positive integer such that $6m + 1$, $12m + 1$, and $18m + 1$ are all primes. Let $n = (6m + 1)(12m + 1)(18m + 1)$. Prove that $n$ is a Carmichael number.

(5) Let $b > 1$ be an integer. Let $p$ be a odd prime which does not divide $b$, $b - 1$ or $b + 1$. Put $n = (b^{2p} - 1)/(b^2 - 1)$. Prove that $n$ is composite, $2p|n - 1$, and $n$ is a pseudoprime to the base $b$. Thus, there are infinitely many composite integers which are pseudoprimes to the base $b$. 

1
(6) Let $n = p(2p - 1)$ as in question 1(c).
   (a) Prove that $n$ is an Euler pseudoprime to 25% of the bases.
   (b) If $p \equiv 3 \pmod{4}$, $n$ is a strong pseudoprime to 25% of the bases.

(7) Use Fermat factorization to factor: 8633; 809009; 4601.

(8) Prove that, if $n$ has a factor that is within $\sqrt{n}$ of $\sqrt{n}$, then Fermat factorization works on the first try (i.e., for $t = \sqrt{n} + 1$).

(9) (a) Let $n = 2701$. Use the $B$-numbers 52 and 53 for a suitable factor base $B$ to factor 2701.
   (b) Let $n = 4633$. Use the $B$-numbers 68, 152 and 153 for a suitable factor base $B$ to factor 4633.

(10) Find the rational approximation with the smallest denominator, which is strictly closer to $\pi$ than $\frac{355}{113}$.

(11) Determine the continued fraction expansions of $\sqrt{2}$, $\sqrt{3}$, $\sqrt{21}$, $\frac{241 - \sqrt{15}}{11}$. 