8. Let b be any integer greater than 1, let p be an odd prime not dividing b, $b-1$ or $b+1$. Set $n=(b^{2p}-1)/(b^2-1)$.
(a) Show that n is composite.
(b) Show that $2p|n-1$.
(c) Show that n is a pseudoprime to the base b; conclude that for any base b there are infinitely many pseudoprimes to the base b.
9. (a) Use the test (1) to show that $2047=2^{11}-1$ is composite.
(b) Explain why you should never test whether the Fermat number $2^{2^k}+1$ or the Mersenne number 2^p-1 is prime by checking (1) with $b=2$. What about using the test (2) with $b=2$? What about using (3) with $b=2$?
10. 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. **Note.** It is not known whether there are infinitely many Carmichael numbers of the form $n=(6m+1)(12m+1)(18m+1)$, but heuristic arguments suggest that there are.
11. Show that the following are Carmichael numbers: $1105=5\cdot 13\cdot 17$; $1729=7\cdot 13\cdot 19$; $2465=5\cdot 17\cdot 29$; $2821=7\cdot 13\cdot 31$; $6601=7\cdot 23\cdot 41$; $29341=13\cdot 37\cdot 61$; $172081=7\cdot 13\cdot 31\cdot 61$; $278545=5\cdot 17\cdot 29\cdot 113$.
12. (a) Find all Carmichael numbers of the form $3pq$ (with p and q prime).
(b) Find all Carmichael numbers of the form $5pq$ (with p and q prime).
(c) Prove that for any fixed prime number r, there are only finitely many Carmichael numbers of the form rpq (with p and q prime).
13. Prove that 561 is the smallest Carmichael number.
14. Give an example of a composite number n and a base b such that $b^{(n-1)/2}\equiv \pm 1 \bmod n$ but n is not an Euler pseudoprime to the base b.
15. (a) Prove that if n is an Euler pseudoprime to the base $b\in(\mathbf{Z}/n\mathbf{Z})^*$, then it is also an Euler pseudoprime to the base $-b$ and to the base b^{-1}.
(b) Prove that if n is an Euler pseudoprime to the base b_1 and to the base b_2, then it is also an Euler pseudoprime to the base $b=b_1b_2$.
16. Let n be of the form $p(2p-1)$, as in Exercise 1(d).
(a) Prove that n is an Euler pseudoprime for 25% of all possible bases $b\in(\mathbf{Z}/n\mathbf{Z})^*$.
(b) Find a class of numbers n of this type such that n is a strong pseudoprime for 25% of all possible bases.
17. Let n be of the form $(6m+1)(12m+1)(18m+1)$, as in Exercise 10. Prove that (a) if m is odd, then n is an Euler pseudoprime for 50% of all possible bases $b\in(\mathbf{Z}/n\mathbf{Z})^*$; and (b) if m is even, then n is an Euler pseudoprime for 25% of all possible bases.
18. (a) Using the big-O notation, estimate the number of bit operations required to perform the Miller–Rabin test on a number n enough times so that, if n passes all the tests, it has less than a $1/m$ chance of being composite (here n and m are very large).