Prime Numbers: Exercises

1. Use the Sieve of Eratosthenes to find all primes less than 200.

2. Suppose that $p, q, r, s$ are four distinct primes. Could $pq = rs$? Why or why not?

3. Use a calculator or computer to determine whether or not 30001 is prime.

4. The only primes less than $\sqrt{400} = 20$ are 2, 3, 5, 7, 11, 13, 17, and 19. Suppose that $n$ is a number less than 400 which is not divisible by any of these primes. What can you conclude about $n$? Justify your answer.

5. Prove rigorously that 397 is prime. (You may use a calculator to carry out the division algorithm, but construct a proof in which the number of divisions is minimum.)

6. Prove rigorously that 1999 is prime.

7. Prove that if $p$ is a prime then $\gcd(a, p) = 1$ if and only if $p \nmid a$ ($p$ does not divide $a$).

8. Find the prime factorization of the following numbers:
   (a) 4800
   (b) 2012
   (c) 371
   (d) $2^{20} - 1 = 1048575$.

9. If $n$ is an even positive integer, how many primes are there of the form $2^n - 1$?

10. How many primes can be written in the form $a^3 - 1$, where $a$ is an integer?

11. Let $n$ be an integer. If $d > 1$ is the smallest nontrivial positive divisor of $n$, prove that $d$ must be prime.

12. Which primes, if any, can be written in the form $a^4 - b^4$ for integers $a, b$? Prove your answer.

13. If $p$ is a prime, how many positive divisors does $p^n$ have? Prove your answer.

14. Show that if $a, b$ are positive integers and $a^3$ divides $b^2$ then $a \mid b$.

15. Suppose that $a = p_1^{u_1}p_2^{u_2} \cdots p_k^{u_k}$ and $b = p_1^{v_1}p_2^{v_2} \cdots p_k^{v_k}$, where $p_1, \ldots, p_k$ are distinct primes. Show that $\gcd(a, b) = p_1^{m_1}p_2^{m_2} \cdots p_k^{m_k}$, where $m_j = \min(u_j, v_j)$ for each $j = 1, \ldots, k$. 
16. Use the result of the previous problem to compute the following:

(a) \( \gcd(2^{35217}, 2^{53^{11}17}) \)
(b) \( \gcd(2^{10}, 3^{11}) \)

17. Show that if \( p, q \) are distinct primes then \( p^r \) and \( q^s \) are relatively prime for any positive integers \( r, s \).

18. Define \( G_n = 2^{2^n} - 1 \), for each positive integer \( n \).

(a) Evaluate \( G_1, G_2, \) and \( G_3 \).
(b) Prove that \( G_n \mid G_{n+1} \) for every positive integer \( n \).
(c) Prove that \( G_n \) has at least \( n \) distinct prime factors for each \( n \).
(d) Explain why part (c) proves that there are an infinite number of primes.

19. Define \( F_n = 2^{2^n} + 1 \), for each positive integer \( n \).

(a) Compute \( F_0, F_1, F_2, \) and \( F_3 \).
(b) Show that \( \gcd(F_n, F_{n+1}) = 1 \), for all positive integers \( n \).
(c) Explain why part (b) gives yet another proof that there are an infinite number of primes.

20. Show that \( p(x) = x^2 - x + 41 \) is prime for all \( x = 1, 2, 3, \ldots, 40 \). What does this imply about \( p(41) \)? Is \( p(41) \) prime?

21. In Fermat’s factorization method, which factors \( n \) by finding integers \( s, t \) such that \( n = s^2 - t^2 \), what are the integers \( s, t \) if \( n \) is prime?

22. Use Fermat factorization to factor the following:

(a) 2279
(b) 11413.

23. According to the famed prime number theorem, what is the approximate number of primes \( \leq 100,000 \)? How about the approximate number of primes not exceeding one million?