that only shows, say, 8 decimal places? Simply break up the numbers into sections. For example, when we compute 2^{35}, we reach the limit of our calculator display with $2^{26} = 67108864$. To multiply this by $2^9 = 512$, we write $2^{35} = 512 \cdot (67108 \cdot 1000 + 864) = 34359296 \cdot 1000 + 442368 = 34359738368$. Later, when we divide $2^{35}-1$ by $31 \cdot 127 = 3937$, we first divide 3937 into 34359738, taking the integer part of the quotient: $\left[\frac{34359738}{3937}\right] = 8727$. Next, we write $34359738 = 3937 \cdot 8727 + 1539$. Then

$$\begin{aligned}\frac{34359738367}{3937} &= \frac{(3937 \cdot 8727 + 1539) \cdot 1000 + 367}{3937} \\ &= 8727000 + \frac{1539367}{3937} \\ &= 8727391.\end{aligned}$$

Exercises

1. Give two different proofs that if n is odd, then $b^n + 1 = (b+1)(b^{n-1} - b^{n-2} + \cdots + b^2 - b + 1)$. In one proof use a polynomial identity. In the other proof use arithmetic to the base b.
2. Prove that if $2^n - 1$ is a prime, then n is a prime, and that if $2^n + 1$ is a prime, then n is a power of 2. The first type of prime is called a "Mersenne prime," as mentioned above, and the second type is called a "Fermat prime." The first few Mersenne primes are 3, 7, 31, 127; the first few Fermat primes are 3, 5, 17, 257.
3. Suppose that b is prime to m, where $m > 2$, and a and c are positive integers. Prove that, if $b^a \equiv -1 \ mod\ m$ and $b^c \equiv \pm 1 \ mod\ m$, and if $d = g.c.d.(a, c)$, then $b^d \equiv -1 \ mod\ m$, and a/d is odd.
4. Prove that, if $p \mid b^n + 1$, then either (i) $p \mid b^d + 1$ for some proper divisor d of n for which n/d is odd, or else (ii) $p \equiv 1 \ mod\ 2n$.
5. Let $m = 2^{24} + 1 = 16777217$.
   (a) Find a Fermat prime which divides m.
   (b) Prove that any other prime is $\equiv 1 \ mod\ 48$.
   (c) Find the complete prime factorization of m.
6. Factor $3^{15} - 1$ and $3^{24} - 1$.
7. Factor $5^{12} - 1$.
8. Factor $10^5 - 1$, $10^6 - 1$ and $10^8 - 1$.
9. Factor $2^{33} - 1$ and $2^{21} - 1$.
10. Factor $2^{15} - 1$, $2^{30} - 1$, and $2^{60} - 1$.
11. (a) Prove that if $d = g.c.d.(m, n)$ and $a > 1$ is an integer, then $g.c.d.(a^m - 1,\ a^n - 1) = a^d - 1$.
    (b) Suppose you want to multiply two k-bit integers a and b, where k is very large. Let ℓ be a fixed integer much smaller than k. Choose a set of m_i, $1 \le i \le r$, such that $\frac{\ell}{2} < m_i < \ell$ for all i and $g.c.d.(m_i, m_j) = 1$ for $i \ne j$. Choose $r = \left[4k/\ell\right] + 1$. Suppose that a large integer such as