1. Suppose \(a\) divides \(b\) and \(b\) divides \(c\) and \(c\) divides \(d\). Must \(a\) divide \(b + c + d\)?

**Solution:** Yes. Apply the transitive property of divisibility twice to see that \(a\) divides \(c\) and \(a\) divides \(d\). By the definition of divisibility there exist integers \(p, q, r\) with \(b = pa\), \(c = qa\), and \(d = ra\). Conclude by the distributive axiom that \(b + c + d = pa + qa + ra = (p + q + r)a\) is divisible by \(a\). □

2. Write a computer program that finds the greatest common divisor of three positive integers \(a, b, c\), assuming that the greatest common divisor function \(\gcd(x, y)\) for any two positive integers \(x, y\) has already been implemented.

**Solution:** Apply \(\gcd(x, y)\) twice. It is implemented in MATLAB, so the following anonymous function will work:

```
MATLAB Function: Greatest Common Divisor of Three Integers

\[ \gcd3 = @(a,b,c) \gcd(\gcd(a,b),c); \]
```

Test it with a couple of known cases: \(\gcd3(35,21,77)\) gives 7; \(\gcd3(35,21,15)\) gives 1.

3. Suppose that \(a + 3b\) and \(17a - b\) are relatively prime. Must \(a\) and \(b\) be relatively prime?

**Solution:** Yes. Any common divisor of \(a\) and \(b\) also divides both \(a + 3b\) and \(17a - b\). □

4. Suppose that \(a\) and \(b\) are relatively prime. Must \(a + 3b\) and \(17a - b\) be relatively prime?

**Solution:** No. For a counterexample, let \(a = 1\) and \(b = 1\). Then \(a\) and \(b\) are relatively prime, but \(a + 3b = 4\) and \(17a - b = 16\) share the common divisor 4. □

5. Find the greatest common divisor of the two numbers \(123456789\) and \(12345678901234567890\).

**Solution:** The larger of these numbers is evidently a multiple of the smaller, so the greatest common divisor is just the smaller number, \(123456789\), by the fourth useful fact on page 4.

6. Is there an integer \(x\) such that \(3702x - 1\) is divisible by 85? Find it, or prove that none exists.

**Solution:** Yes. Such an \(x\) exists if there is a solution to the equation \(3702x - 1 \equiv 0 \pmod{85}\), or \(3702x \equiv 1 \pmod{85}\). But \(\gcd(3702, 85) = 1\), so by Lemma 1.6 such a quasi-inverse exists.

We may use the extended Euclid algorithm to find the solution \(x = 38\): \((3702)(38) - 1 = 140675 = (85)(1655)\). The following is an implementation in MATLAB, translated from the pseudocode in our textbook:
MATLAB Function: Extended Euclid Algorithm

function [d, x, y] = gcdx(a,b)
a = abs(a); b = abs(b); x=0; y=1; xo=1; yo=0; c=a; d=b;
while d>0
    q = fix(c/d); r = rem(c,d);
    if r==0
        return
    end
    c=d; d=r; t=xo; xo=x; x=t-q*x; t=yo; yo=y; y=t-q*y;
end

However, MATLAB’s built-in \texttt{gcd()} performs the same function with the call \texttt{[d,x,y]=gcd(a,b)}, returning values satisfying \(xa + yb = d\).

7. Express the integer 1011 1010 1100 (base 10) in hexadecimal.

\textbf{Solution:} 1011 1010 1100 (base 10) equals 178AA1B46C (base 16). This calculation can be done on a 32-bit computer after the observation

\[101110101100 = 394961332 \times 256 + 108 = 394961332 \times 16^2 + 108.\]

But 394961332 (base 10) = 178AA1B4 (base 16) gives the leading hexadecimal digits, while 108 (base 10) = 6C (base 16) gives the two lowest-order hexadecimal digits. These last two calculations only need 32-bit integers.

8. Prove that if \(p\) is a prime number, then \(\sqrt{p}\) is not a rational number.

\textbf{Solution:} If \(\sqrt{p}\) were a rational number, we could write \(\sqrt{p} = a/b\) in lowest terms, namely using relatively prime \(a, b \in \mathbb{Z}\). But then \(pb^2 = a^2\), so \(p\) divides \(a^2\). By Lemma 1.3, \(p\) divides \(a\), so we can write \(a = pa_0\) with \(a_0 \in \mathbb{Z}\). But then \(p = p^2a_0^2/b^2\), so \(b^2 = pa_0^2\) and consequently \(p\) divides \(b^2\). Again by Lemma 1.3, \(p\) divides \(b\). Hence \(a, b\) share the common divisor \(p > 1\), contradicting the hypothesis that they are relatively prime.

9. Find the rational number represented by the repeating hexadecimal expansion 0.FACE (base 16).

\textbf{Solution:} Let \(x = 0.FACE\) (base 16) denote the number. Then

\[16^4x - x = FACE\ (base\ 16) = 15 \times 16^3 + 10 \times 16^2 + 12 \times 16 + 14 = 64206\]

Solving gives \(x = 64206/65535 \approx 0.979720759899290\)

10. What is the smallest positive subnormal number in IEEE double precision 64-bit binary floating-point format?

\textbf{Solution:} The exponent of a subnormal number is \(-1022\), although it is tagged with an unbiased exponent of \(-1023\). Use \(-1022\) with a mantissa full of 51 leading zeros and a single one in the least significant bit to get the smallest subnormal number:

\[0.000000000 \ldots 01\ (base\ 2) \times 2^{-1022} = 2^{-1074} \approx 4.9406 \times 10^{-324}.\]

Note that only the first mantissa is written in base 2; all other expansions are decimal.
11. Implement the Miller-Rabin primality test for odd $N$ satisfying $2 < N < 341,550,071,728,321$. Use it to find a 14-digit prime that is not known to Google. (Hint: you may seek and use an implementation available on the web.)

**Solution:** The stated limits on $N$ imply that no strong liars exist for the Miller-Rabin test. Function `NextPrime[49332378234519]` found online at Wolfram Alpha implements it and gives the result 49332378234571. Here the “random” input 49332378234519 is an arbitrary 14 digit number that happens to give a prime which does not appear in a Google search.

12. Using the primes $p = 17$ and $q = 19$, implement the RSA encryption algorithm with $e = 23$ and modulus $M = pq = 323$. Namely, find $d$ and $\phi(M)$. Then encode the cleartext value 314 and decode the cyphertext value 255. Check your results by decrypting the cyphertext and encrypting the cleartext. (Hint: search the web for RSA MATLAB.)

**Solution:** First compute $\phi(M) = (17 - 1)(19 - 1) = 288$ and find the quasi-inverse $d = 263$ with the extended Euclid algorithm. Use the MathWorks `crypt(314,323,23)` function to get cyphertext 117 from cleartext 314. Likewise, `crypt(255,323,263)` gives the cleartext 185 from cyphertext 255. Check by applying the inverses: `crypt(117,323,263)==314`, `crypt(185,323,23)==255`. 

\[\square\]