Ma 450: Mathematics for Multimedia
Homework Assignment 1

Prof. Wickerhauser

Due Sunday, February 5th, 2023

1. Suppose that a, b, and c are positive integers, a divides $b+c$, and a divides $2b+c$.

   (i) Must a divide b?

   (ii) Must a divide c?

2. The greatest common divisor of $n \geq 2$ positive integers may be defined recursively by induction on n, using the greatest common divisor function $\gcd(a,b)$ for two positive integers a,b:

$$\gcd(a_1,\ldots,a_n) \overset{\text{def}}{=} \gcd(\gcd(a_1,\ldots,a_{n-1}),a_n).$$

   (Note: MATLAB/Octave already implements this generalized gcd.)

   The *least common multiple* $\operatorname{lcm}(a_1,\cdots,a_n)$ of $n \geq 2$ integers is the smallest positive integer divisible by every a_i. Namely, it satisfies

lcm-1: $(\forall i)a_i|\operatorname{lcm}(a_1,\cdots,a_n)$.

lcm-2: If N is divisible by every a_i, then $\operatorname{lcm}(a_1,\cdots,a_n)|N$.

   (i) Show that $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$.

   (ii) Find $\operatorname{lcm}(a_1,\ldots,a_n)$ using induction on n. (Note: MATLAB/Octave likewise implements this generalized lcm. You can use it to check you results.)

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

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

4. Let $a = 123\,456$ and $b = 78\,901$.

   (i) Find the greatest common divisor d of a,b.

   (ii) Find integers s and t such that $sa+tb=d$.

5. (i) Is there an integer x such that $85x-1$ is divisible by 2023? Find it, or prove that none exists.

   (ii) Is there an integer y such that $58y-1$ is divisible by 2023? Find it, or prove that none exists.

6. (i) Express the integer $1011\,1010\,1100$ (base 10) in hexadecimal.

   (ii) Find the rational number represented by the repeating hexadecimal expansion $0.\overline{CAFE}$ (base 16).

7. Prove that if p is a prime number, then $\sqrt{p}$ is not a rational number.

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

9. 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.)

10. 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.)