Ma 450: Mathematics for Multimedia

Solution: to 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?

   Solution:

   (i) Yes, a must divide b, since it divides the difference $2b + c - (b + c) = b$.

   (ii) Yes, a must divide c, since if a divides $b+c$ then it divide $2(b+c)$, and thus it divides the difference $2(b + c) - (2b + c) = c$. $\square$

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:

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

   (Note: 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.)

   Solution:

   (i) *First proof, using two inequalities:*

   ($\geq$) Since ab is divisible by both a and b, it follows from lcm-2 that $\operatorname{lcm}(a, b)|ab$.

   Hence $d = \dfrac{ab}{\operatorname{lcm}(a, b)}$ is an integer. Observe that $d|a$, since $\dfrac{a}{d} = \dfrac{a \operatorname{lcm}(a, b)}{ab} = \dfrac{\operatorname{lcm}(a, b)}{b}$, which is an integer because $b|\operatorname{lcm}(a, b)$ by lcm-1. Similarly, $d|b$. Hence d is a common divisor of a and b, and by gcd-2 it follows that $d| \gcd(a, b)$, so $\gcd(a, b) \geq d$, so

$$\gcd(a, b) \geq \frac{ab}{\operatorname{lcm}(a, b)} \quad \Rightarrow \quad \operatorname{lcm}(a, b) \geq \frac{ab}{\gcd(a, b)}.$$

($\leq$) Write $a = x \gcd(a,b)$ and $b = y \gcd(a,b)$ using the two integer quotients $x = a/\gcd(a,b)$ and $y = b/\gcd(a,b)$. Then

$$N = \frac{ab}{\gcd(a,b)} = xy \gcd(a,b) = xb = ya$$

evidently satisfies $a|N$ and $b|N$. It follows from lcm-2 that $\mathrm{lcm}(a,b)|N$, so $\mathrm{lcm}(a,b) \leq N$, so

$$\mathrm{lcm}(a,b) \leq \frac{ab}{\gcd(a,b)}.$$

Combining the two inequalities yields the result.

Second proof, using prime factorization:

Let $P = \{p_1, \ldots, p_k\}$ be the set of distinct prime factors of a and b. Thus $p \in P$ if and only if $p|a$ or $p|b$, and $i \neq j$ implies $p_i \neq p_j$. Then the prime factorizations of a and b may be written as

$$\begin{array}{rcll} a &=& p_1^{n_1} \cdots p_k^{n_k}, & n_i \in \{0,1,2,\ldots\}, \\ b &=& p_1^{m_1} \cdots p_k^{m_k}, & m_i \in \{0,1,2,\ldots\}. \end{array}$$

Note that the exponent n_i is positive if and only if $p_i|a$, and so on. In this notation it is easy to see that

$$\begin{array}{rcl} ab &=& p_1^{n_1+m_1} \cdots p_k^{n_k+m_k}, \\ \gcd(a,b) &=& p_1^{\min(n_1,m_1)} \cdots p_k^{\min(n_k,m_k)}, \\ \mathrm{lcm}(a,b) &=& p_1^{\max(n_1,m_1)} \cdots p_k^{\max(n_k,m_k)}, \end{array}$$

and the result follows from the rules of exponents and the identity that $\min(n,m)+\max(n,m) = n+m$ for any numbers n, m.

(ii) As with gcd, the inductive step uses the definition of $\mathrm{lcm}(a,b)$:

$$\mathrm{lcm}(a_1, \ldots, a_n) \stackrel{\text{def}}{=} \mathrm{lcm}(\mathrm{lcm}(a_1, \ldots, a_{n-1}), a_n),$$

for $n > 2$. However, it requires proof that this formula produces a value satisfying lcm-1 and lcm-2. This may be done by induction on n.

The base case, $n = 2$, holds by part (i). Next, for $n > 2$, suppose that $\mathrm{lcm}(a_1, \ldots, a_{n-1})$ is the least common multiple and check the properties of $\mathrm{lcm}(a_1, \ldots, a_n)$ as defined:

First proof, checking lcm-1 and lcm-2 directly:

Let $M = \mathrm{lcm}(\mathrm{lcm}(a_1, \ldots, a_{n-1}), a_n)$. Then $a_n|M$ by definition. But also $a_i|\mathrm{lcm}(a_1, \ldots, a_{n-1})$ for all $i = 1, \ldots, n-1$ by the inductive hypothesis, so $(\forall i) a_i|M$. This proves that lcm-1 holds for M.

Now suppose that N is divisible by $a_1, \ldots, a_n$. Then N is divisible by $\mathrm{lcm}(a_1, \ldots, a_{n-1})$ by lcm-2 for the case $n-1$. But N is also divisible by a_n by hypothesis, so apply lcm-2 in the case $n = 2$ to conclude that N is divisible by M. This proves lcm-2 for the case n, so $M = \mathrm{lcm}(a_1, \ldots, a_n)$. This completes the proof by induction.

Second proof, using prime factorization:

It is convenient to use the complete (countably infinite, ordered) list of primes $P = \{2, 3, 5, 7, \dots\} = \{p_1, p_2, \dots\}$ and then write, for each i,

$$a_i = p_1^{m_{i1}} p_2^{m_{i2}} \cdots,$$

where $m_{ij} = 0$ for all but finitely many values of j (which depend on the prime factorization of a_i). But then

$$\operatorname{lcm}(a_1, \dots, a_n) = p_1^{\max(m_{11},\dots,m_{n1})} p_2^{\max(m_{12},\dots,m_{n2})} \cdots$$

and the formula $\operatorname{lcm}(a_1, \dots, a_{n-1}, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \dots, a_{n-1}), a_n)$ follows from the fact that

$$\max(m_1, \dots, m_{n-1}, m_n) = \max(\max(m_1, \dots, m_{n-1}), m_n).$$

□

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?

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

   (ii) 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. □

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 $sa + tb = d$.

   Solution: Use Octave. Its built-in `gcd()` performs the extended Euclid algorithm with the call `[d,s,t]=gcd(a,b)`, returning values satisfying $sa + tb = d$.

   (i) `gcd(123456,78901)` gives `ans = 1` by Euclid's algorithm.

   (ii) `[d,s,t]=gcd(123456,78901)` gives `d = 1, s = -1082, t = 1693` by the extended Euclidean algorithm. □

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.

   Solution: Use Octave. Its built-in `gcd()` performs the extended Euclid algorithm with the call `[d,x,y]=gcd(a,b)`, returning values satisfying $xa + yb = d$.

   (i) By Lemma 1.9, no such integer exists, since $85 = 5 \cdot 17$ and $2023 = 7 \cdot 17^2$ are not relatively prime: $\gcd(85, 2023) = 17 \neq 1$.

   (ii) Yes, such a y exists by Lemma 1.9 since $58 = 2 \cdot 29$ and $2023 = 7 \cdot 17^2$ are relatively prime: $\gcd(58, 2023) = 1$.

   Use the extended Euclid algorithm to find $y = 872$: $872 \cdot 58 - 1 = 50\,575 = 25 \cdot 2023$. □

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).

   Solution:

(i) $1011\,1010\,1100$ (base 10) equals $178AA1B46C$ (base 16). Find it using the Octave command `dec2hex(101110101100)` on a contemporary 64-bit computer.

This calculation can be also 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.

(ii) Let $x = 0.\overline{CAFE}$ (base 16) denote the number. Then

$$16^4 x - x = CAFE \text{ (base 16) } = 12 \times 16^3 + 10 \times 16^2 + 15 \times 16 + 14 = 51966$$

(This may also be found using Octave command `hex2dec("CAFE")`.) Solving gives $x = 51966/65535 \approx 0.7929503318837262$ □

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

   Solution: If $\sqrt{p}$ were a rational number, we could write $\sqrt{p} = a/b$ in lowest terms, namely using relatively prime $a, b \in \mathbf{Z}$. 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 $a_0 \in \mathbf{Z}$. But then $p = p^p a_0^2/b^2$, 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. □

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

   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:

   $$0.00000\,00000 \ldots 01 \text{ (base 2)} \times 2^{-1022} = 2^{-1074} \approx 4.9406 \times 10^{-324}.$$

   Note that only the first mantissa is written in base 2; all other expansions are decimal. □

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.)

   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.

   NOTE: a previous model solution set from 2014 contains this prime and is discoverable by a Google search, so you must find another. □

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.)

    Solution: First compute $\phi(M) = (17-1)(19-1) = 288$ and find the quasi-inverse with the extended Euclid algorithm:

```
p=17, q=19, en=23, M=p*q, phiM=(p-1)*(q-1)
[c,x,y]=gcd(en,phiM)  % then c=x*en+y*phiM, so x*en=c (mod phiM)
```

This gives the quasi-inverse $x = -25$ which must be shifted into the range $[1, \phi(M) - 1]$ by adding $\phi(M)$, giving $d = 263$. Use the MathWorks modular exponentiation function `crypt(a,e,M)` function to get cyphertext `crypt(314,23,323)==117` from cleartext 314. Likewise, `crypt(255,263,323)` gives the cleartext 221 from cyphertext 255. Check by applying the inverses: `crypt(117,263,323)==314`, `crypt(221,23,323)==255`. □