Number Theory Homework II

RDB

August 17, 2021

This homework is on Week 1 stuff.
In general, assume that variables like n, m, and k are integers.

Exercise 1

(a) Write the following integers in binary: 342, 2^{10}, and $(112)_3$.

(b) Write the following integers in base 5: ten, one-hundred and forty-one, two-hundred and thirteen, and one-thousand.

Solution 1

(a) 101010110_2, 10000000000_2, and 1110_2

(b) 20_5, 1031_5, 1323_5, and 13000_5.

Exercise 2 For each of the following pairs of integers a, b, find the greatest common divisor of a and b and also integers x, y such that $ax + by = \gcd(a, b)$.

(a) $527, 8$

(b) $842, 184$

(c) $1, 29$

(d) $1, n$

(e) $54, 10$

Solution 2

(a) $1;\ 527(-1) + 8(66) = 1$

(b) $2;\ 842(33) + 184(-151) = 2$

(c) $1;\ 1(1) + 29(0) = 1$

(d) $1;\ 1(1) + n(0) = 1$

(e) $2;\ 54(-2) + 10(11) = 2$

Exercise 3 For each of the following linear diophantine equations, give the general solution, if any solutions exist.

(a) $2x + 3y = 1$

(b) $60x + 17y = 7$

(c) $19x + 95y = -3$

(d) $x + ny = 1$ [The variable n is a parameter; assume that $n \neq 0$, but otherwise your solutions should have an n in them somewhere.]

Solution 3

(a) $x = -1 + 3t$, $y = 1 - 2t$

(b) $x = 7(2 + 17t)$, $y = 7(-7 - 60t)$

(c) The gcd is 19, which does not divide -3, so there are no solutions.

(d) $x = 1 + nt$, $y = -t$.

Exercise 4 Prove that

$$\gcd(n, 2) = 1 + \frac{1 + (-1)^n}{2}.$$

[Hint: This is not as fancy as it looks.]

Solution 4

If n is even, then $\gcd(n, 2) = 2$ and

$$1 + \frac{1 + (-1)^n}{2} = 2.$$

If n is odd, then $\gcd(n, 2) = 1$ and

$$1 + \frac{1 + (-1)^n}{2} = 1.$$

Exercise 5

(a) Prove that $\gcd(a, b) = \gcd(a-b, b)$. [Hint: Prove that the common divisors of (a, b) are the same as the common divisors of $(a - b, b)$.]

(b) Prove that $\gcd(n + 1, n) = 1$ for all $n \geq 1$. [Hint: Use the previous part. Or divide $n + 1$ by n.]

(c) Prove that $\gcd(F_{n+1}, F_n) = 1$ where F_n is the nth Fibonacci number. [Hint: Use the previous part and induction.]

Solution 5

(a) If d divides a and b, then it also divides $a - b$, since this is a linear combination of a and b. Therefore d is a common divisor of $a-b$ and b. On the other hand, if d divides $a - b$ and b, then d also divides a, since $a = (a - b) + b$ is a linear combination of $a - b$ and b. Therefore the set of common divisors of (a, b) and $(a - b, b)$ are the same, meaning that the *greatest* common divisor is unchanged.

(b) Using the previous part, we get $\gcd(n + 1, n) = \gcd(1, n) = 1$.

(c) With $n = 0$, we get $\gcd(F_1, F_0) = \gcd(1, 0) = 1$. Then, if we assume that $\gcd(F_{n+1}, F_n) = 1$, we get

$$\begin{aligned}\gcd(F_{n+2}, F_{n+1}) &= \gcd(F_{n+1} + F_n, F_{n+1}) \\ &= \gcd(F_n, F_{n+1}) \\ &= 1.\end{aligned}$$

Therefore, by induction, $\gcd(F_{n+1}, F_n) = 1$ for all $n \geq 0$.

Exercise 6 Prove a converse of Bézout's lemma: If $ax + by = g$ and g divides both a and b, then $g = \gcd(a, b)$. In particular, if $ax + by = 1$, then a and b are coprime. [**Edit:** You also must assume that $g > 0$!]

Solution 6
If $ax + by = g$, then every common divisor of a and b divides g, since $ax + by$ is a linear combination of a and b. In particular, $\gcd(a, b)$ divides g. On the other hand, since g is a common divisor of a and b, by definition g divides $\gcd(a, b)$. If two positive integers divide each other, then they are equal, so $g = \gcd(a, b)$.

[No points taken off for not mentioning $g > 0$.]

Exercise 7 An integer m is a *common multiple* of a and b provided that a and b both divide m. We call m the *least common multiple* provided that m is positive and divides all other common multiples. We call this $\operatorname{lcm}(a, b)$. This exercise will prove the famous formula

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

(a) Prove that

$$\operatorname{lcm}(a, b) = ab$$

if $\gcd(a, b) = 1$.

[Hint: Assume that m is a common multiple of a and b which divides ab. Show that ab/m is a common divisor of a and b.]

(b) Prove that

$$\operatorname{lcm}(ax, bx) = \operatorname{lcm}(a, b)x$$

for any integer x. Conclude that

$$\operatorname{lcm}(a/d, b/d) = \operatorname{lcm}(a, b)/d$$

for any common divisor d of a and b.

(c) Prove that

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

[Hint: Use the previous two parts.]

(d) Compute $\operatorname{lcm}(n, n + 1)$ for a positive integer n.

Solution 7

(**a**) Let m be a common multiple of a and b which divides ab, say $ab = mn$. If $m = ak$, then $ab = akn$, so

$$b = kn.$$

Similarly, if $m = bj$, then

$$a = jn.$$

This shows that $ab/m = n$ is a common divisor of a and b, so $n = 1$. Therefore $m = ab$.

Note that ab is a common multiple of a and b, so $m = \operatorname{lcm}(a, b)$ divides ab. The previous paragraph shows that $m = ab$.

(**b**) By definition, $\operatorname{lcm}(a, b)$ is a common multiple of a and b, say $\operatorname{lcm}(a, b) = ak = bj$. Then $\operatorname{lcm}(a, b)x = (ax)k = (bx)j$, so $\operatorname{lcm}(a, b)x$ is a common multiple of ax and bx. By definition, $\operatorname{lcm}(ax, bx)$ divides $\operatorname{lcm}(a, b)x$.

On the other hand, $\operatorname{lcm}(ax, bx)$ is a common multiple of ax and bX, say $\operatorname{lcm}(ax, bx) = axk' = bxj'$. Note that

$$\frac{\operatorname{lcm}(ax, bx)}{x} = ak' = bj',$$

so $\operatorname{lcm}(a, b)$ divides $\operatorname{lcm}(ax, bx)/x$, say

$$\frac{\operatorname{lcm}(ax, bx)}{x} = \operatorname{lcm}(a, b)N.$$

Multiplying by x shows that $\operatorname{lcm}(a, b)x$ divides $\operatorname{lcm}(ax, bx)$.

If two positive integers divide each other, then they are equal. Therefore $\operatorname{lcm}(ax, bx) = \operatorname{lcm}(a, b)x$.

If d is a common divisor of a and b, then

$$\operatorname{lcm}(a, b) = \operatorname{lcm}\left(\frac{a}{d}d, \frac{b}{d}d\right) = \operatorname{lcm}(a/d, b/d)d.$$

(**c**) Let $g = \gcd(a, b)$. By the previous part, we have

$$\operatorname{lcm}(a, b) = g \operatorname{lcm}(a/g, b/g).$$

Since $\gcd(a/g, b/g) = 1$, we get

$$\operatorname{lcm}(a, b) = g\frac{a}{g}\frac{b}{g} = \frac{ab}{g}.$$

(d) n and $n+1$ are coprime, so

$$\mathrm{lcm}(n, n+1) = n(n+1)$$

by part (a).

Exercise 8 You order \$143 worth of protein bars online in 16ct containers. The chocolate flavor costs \$15 per box and the vanilla costs \$17 per box. How many of each box did you buy? [Hint: If you bought x chocolate and y vanilla, then the total cost is $15x + 17y$.]

Solution 8
The amount of bars x and y that you bought must be integer solutions to the equation

$$15x + 17y = 143.$$

The gcd of 15 and 17 is 1, so this equation *does* have a solution. In fact, $x_0 = 143 \cdot 8$ and $y_0 = 143 \cdot -7$ will work, since

$$15(8) + 17(-7) = 1,$$

and multiplying by 143 gives

$$15(143 \cdot 8) + 17(143 \cdot -7) = 143.$$

The general solution to the equation is therefore

$$x = 143 \cdot 8 + 17t; \qquad y = 143 \cdot -7 - 15t.$$

The first equation is positive if and only if $t \geq -67$, while the second equation is positive if and only if $t \leq -67$. Therefore, they are *both* positive only when $t = -67$, which gives

$$x = 143 \cdot 8 + 17(-67) = 5$$

and

$$y = 143 \cdot -7 - 15(-67) = 4.$$

Exercise 9 You are opening a gym for mathematicians. They are very particular: It must be possible to work out with *every* weight in $\{0, 1, 2, 3, \ldots, 255\}$. (For instance, someone wants to bench exactly 114 pounds.) What is the fewest number of weights you can buy to achieve this goal? For example, you could use 255 1-pound weights. Can you do it with fewer?

Solution 9

You can use a binary system. Pick weights of size 1, 2, 4, 8, and so on, up to 128. Every weight up to 255 is expressible in exactly one way, namely its binary expansion. This takes eight weights.

Eight weights is a considerable improvement over 255 weights, but is it the *best* you could do? Yes!

Suppose that you have n weights. There are 2^n different ways to pick a collection of the weights, and therefore *at most* 2^n different weights you could represent. If we are to represent each of the 256 weights in $\{0, 1, 2, \ldots, 255\}$, we must have $2^n \geq 256$, or $n \geq \log_2 256 = 8$. So eight is the best that you could do.

Exercise 10 This exercise involves programming.

(a) Write a function `isprime` to check if a given integer n is prime by checking every possible divisor from 2 to $n-1$.

(b) Prove that, if n is not prime, then it must have at least one divisor $d \leq \sqrt{n}$. [Hint: Assume that n is not prime and that all divisors are $> \sqrt{n}$. Pick divisors a and b with $n = ab$. Find a contradiction.]

(c) Write a second function `isprimeSqrt` to check if n is prime by checking every possible divisor from 2 to $\sqrt{n}$.

(d) Go to https://bigprimes.org/, get a big prime, and test your two functions on it. Which is faster?

Solution 10

(a)

```
def isprime(n):
    for k in range(2, n):
        if n % k == 0:
            return False

    return True
```

(b) If $a, b > \sqrt{n}$, then $ab > n$. Therefore, if $n = ab$ for integers a and b, at least one factor is $\geq \sqrt{n}$ and one is $\leq \sqrt{n}$. So, if n is composite, it has at least one factor $\leq \sqrt{n}$.

(c)

```
from math import floor, sqrt

def isprimeSqrt(n):
    for k in range(2, floor(sqrt(n)) + 1):
        if n % k == 0:
            return False

    return True
```

(d) `isprimeSqrt` is considerably faster for large primes, because it only checks $\sqrt{n}$ numbers while `isprime` checks n numbers.