CSE 311: Foundations of Computing I Spring 2023

Quiz Section 4: Number Theory – Solutions

Review

Divisibility: For $d \neq 0$ we write $(d \mid a)$ iff there is an integer k such that $a = kd$.
Division Theorem: For integers a and b with $b > 0$, there are unique integers q and r such that $a = qb + r$ and $0 \leqslant r < b$. The remainder r is also written as $a \bmod b$.
Mod Predicate $\pmod{m}$**:** For integer $m > 0$ and integers a and b, we write $a \equiv b \pmod{m}$ iff $m|(a - b)$. This is equivalent to $(a - b) = km$ for some integer k; it is also equivalent to $a = b + km$ for some integer k.
Properties of $\pmod{m}$**:**

- For $m > 0$, $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$

Prime: An integer $n > 1$ is prime iff its only positive divisors are 1 and n.
Unique Factorization Theorem: Every positive integer has a unique representation as a product of prime numbers (assuming that the primes in the product are listed with smaller ones first).
Greatest Common Divisor: $gcd(a, b)$ is the largest common divisor of a and b.
Properties of gcd: For positive integers a and b, $gcd(a, 0) = a$ and $gcd(a, b) = gcd(b, a \bmod b)$.
Multiplicative Inverse: For $m > 0$ and $0 \leqslant a < m$, the *multiplicative inverse of* a *modulo* m is a number b with $0 \leqslant b < m$ such that $ab \equiv 1 \pmod{m}$. It exists if and only if $gcd(a, m) = 1$.

Task 1 – Division of Labor

a) For the domain of integers give an English proof that if $ab = 1$ then $a = 1$ or $a = -1$.

Suppose that $ab = 1$. We can't have $a = 0$ since $0 \times b = 0$. Then we can divide by a and write $b = 1/a$. If $a > 1$ this is not an integer but b is supposed to be an integer so this can't be the case; the same holds for $a < -1$. We have ruled out all other options so $a = 1$ or $a = -1$ are the only options left. (Note that both are possible by setting $b = a$.)

b) Give an English proof of the following claim over the domain of integers: if $a \mid b$, $b \mid a$, and $a \neq 0$, then $a = b$ or $a = -b$.

Suppose that $a \mid b$, $b \mid a$, and $a \neq 0$. By the definition of divides, we have $b = ja$ and $a = kb$ for some integers j, k. Combining these equations, we see that $a = kb = k(ja) = (kj)a$. Since $a \neq 0$, we can divide both sides by a to see that $kj = 1$.
By the property of integer multiplication proved in part (a), $kj = 1$ is only possible if $j = k = 1$ or $j = k = -1$. If the first holds, then we have $a = kb = b$. If the second holds, then we have $a = kb = -b$. Hence, in either case, we have $a = b$ or $a = -b$.

Task 2 – This is really mod

Let n and m be integers greater than 1, and suppose that $n \mid m$. Give an English proof that for any integers a and b, if $a \equiv b \pmod{m}$, then $a \equiv b \pmod{n}$.

Let a and b be arbitrary integers and $n > 1$ and $m > 1$. Suppose that $a \equiv b \pmod{m}$. Then, by definition of $\pmod{m}$, $m \mid (a - b)$, so there exists an integer k such that $a - b = km$. Also, since $n \mid m$, there is an integer j such that $m = jn$. Thus, we have

$$\begin{aligned} a - b &= km \\ &= k(jn) \\ &= (kj)n. \end{aligned}$$

So, by definition, $n \mid (a - b)$, so $a \equiv b \pmod{n}$.

Task 3 – Casing the Joint

Prove that for every integer n, $n^2 \equiv 0 \pmod{3}$ or $n^2 \equiv 1 \pmod{3}$.

We give a proof by cases:

Case $n \equiv 0 \pmod{3}$:
In this case, by the multiplicative property of mod we have $n^2 \equiv 0^2 \equiv 0 \pmod{3}$.

Case $n \equiv 1 \pmod{3}$:
In this case, by the multiplicative property of mod we have $n^2 \equiv 1^2 \equiv 1 \pmod{3}$.

Case $n \equiv 2 \pmod{3}$:
In this case, by the multiplicative property of mod we have $n^2 \equiv 2^2 \equiv 4 \equiv 1 \pmod{3}$.

By the Division Theorem, these cases cover all possible integers n, so we have $n^2 \equiv 0 \pmod{3}$ or $n^2 \equiv 1 \pmod{3}$ for all integers n.

Task 4 – Primality Checking

The following code, `isPrime(int n)` uses the direct definition of primality to test if its input n is prime by trying all potential divisors of n between 2 and $n-1$. It therefore returns `true` if and only if n is prime.

```
public boolean isPrime(int n) {
    if (n <= 1)
        return false;
    int potentialDiv = 2;
    while (potentialDiv < n) {
        if (n % potenttialDiv == 0)
            return false;
        potentialDiv++;
    }
    return true;
}
```

In fact, we can make it run faster by replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)` since there will be many fewer values of `potentialDiv` to check.

But is the code still correct? This motivates the following;

a) Let n, a, and b be positive integers. Give an English proof that if $n = ab$, then one of a or b is at most $\sqrt{n}$.
(Hint: You may want to use a proof by contrapositive or by contradiction. You can use all properties of $\leqslant$ and $>$ symbols that you know, including the fact that for all positive numbers u, v, x, y, $u > v$ and $x > y$ implies that $ux > vy$.)

Suppose that $n = ab$. Suppose for a contradiction that $a, b > \sqrt{n}$. It follows that $ab > \sqrt{n}\sqrt{n} = n$. We cannot have both $ab = n$ and $ab > n$, so this is a contradiction. It follows that a or b is at most $\sqrt{n}$.

b) Why, informally, does part (a) imply that the modifed code will still be correct?

If n is not prime there will be a positive factor a of n that is not equal 1 or n, so $n = ab$ for some positive integer b which also can't be 1 or n. Then by part (a) either $a \leqslant \sqrt{n}$ or $b \leqslant \sqrt{n}$ so the smaller of the two numbers will be at most $\sqrt{n}$ and will be found by the algorithm.

Task 5 – Planning Your Tiling

Suppose that you had a rectangular room and wanted to tile the entire floor with square tiles of all the same size that are as big as possible (assuming no spacing between tiles and no partial tiles).

a) What is the largest square tile you could use if the room's dimensions are 308 cm by 224 cm?

Since the tiles are square, their side length must divide both of the dimensions evenly. Therefore the largest tiles will have length equal to the $\gcd(308, 224)$ cm.

We do the computation of the gcd using the tableau:

$$\begin{aligned} 308 &= 1 \times 224 + 84 \\ 224 &= 2 \times 84 + 56 \\ 84 &= 1 \times 56 + 28 \\ 56 &= 2 \times 28 + 0. \end{aligned}$$

Therefore the $\gcd(308, 224) = 28$, so tiles that are 28 cm on a side are the largest possible.

Note: This is the kind of problem in ancient Greece that may have motivated the creation of Euclid's algorithm: Instead of division with remainder, you repeatedly mark off squares with length equal to the shorter of two sides until they don't fit any more. This eventually leaves a rectangle that is too small to fit another square of this size. They then repeat this again with the smaller rectangle that is left over, using the shorter of its sides as the side of a new square tiling. This square tiling will run out also, leaving a smaller rectangle that you tile with smaller squares. Eventually the square tiles exactly fill the rectangle and that size can be used to tile all the larger squares. See minutes 6:00-8:00 in this video: https://www.youtube.com/watch?v=kiFfp-HAu64

b) How many tiles will you need?

$224 = 8 \times 28$ and $308 = 11 \times 28$ so there will be $8 \times 11 = 88$ tiles.

Task 6 – GCD

Compute the following GCDs.

a) $gcd(9, 6)$

$$\begin{aligned} gcd(9,6) &= gcd(6,3) & 9 &= 1 \times 6 + 3 \\ &= gcd(3,0) & 6 &= 2 \times 3 + 0 \\ &= 3 \end{aligned}$$

b) $gcd(18, 14)$

$$\begin{aligned} gcd(18,14) &= gcd(14,4) & 18 &= 1 \times 14 + 4 \\ &= gcd(4,2) & 14 &= 3 \times 4 + 2 \\ &= gcd(2,0) & 4 &= 2 \times 2 + 0 \\ &= 2 \end{aligned}$$

c) $gcd(80, 44)$

$$\begin{aligned} gcd(80,44) &= gcd(44,36) & 80 &= 1 \times 44 + 36 \\ &= gcd(36,8) & 44 &= 1 \times 36 + 8 \\ &= gcd(8,4) & 36 &= 4 \times 8 + 4 \\ &= gcd(4,0) & 8 &= 2 \times 4 + 0 \\ &= 4 \end{aligned}$$

d) $gcd(77, 43)$

$$\begin{aligned} gcd(77,43) &= gcd(43,34) & 77 &= 1 \times 43 + 34 \\ &= gcd(34,9) & 43 &= 1 \times 34 + 9 \\ &= gcd(9,7) & 34 &= 3 \times 9 + 7 \\ &= gcd(7,2) & 9 &= 1 \times 7 + 2 \\ &= gcd(2,1) & 7 &= 3 \times 2 + 1 \\ &= gcd(1,0) & 2 &= 2 \times 1 + 0 \\ &= 1 \end{aligned}$$

Task 7 – Multiplicative inverses

For each of the following choices of a and m, determine whether a has a multiplicative inverse modulo m. If yes, *guess* a multiplicative inverse of a modulo m *and check* your answer.

a) $a = 3$ and $m = 8$

We first compute $gcd(8, 3)$.

$$\begin{aligned} 8 &= 2 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Since the result is 1, we conclude that 3 *does* have a multiplicative inverse modulo 8. By trying a few values, we find that $3 \times 3 \equiv 1 \pmod{8}$, so 3 is the multiplicative inverse of 3 modulo 8.

b) $a = 6$ and $m = 28$

We first compute $gcd(28, 6)$.

$$\begin{aligned} 28 &= 4 \times 6 + 4 \\ 6 &= 1 \times 4 + 2 \\ 4 &= 2 \times 2 + 0 \end{aligned}$$

Since the result is 2, the gcd is not 1 and we conclude that 6 does *not* have a multiplicative inverse modulo 28.

c) $a = 5$ and $m = 29$

We first compute $gcd(29, 5)$.

$$\begin{aligned} 29 &= 5 \times 5 + 4 \\ 5 &= 1 \times 4 + 1 \\ 4 &= 4 \times 1 + 0 \end{aligned}$$

Since the result is 1, we conclude that 5 *does* have a multiplicative inverse modulo 29. By trying a few values, we find that $5 \times 6 \equiv 1 \pmod{29}$, so 6 is the multiplicative inverse of 5 modulo 29.

Task 8 – Extended Euclidean Algorithm Practice

For each of the following choices of a and m, use the Extended Euclidean Algorithm to compute the multiplicative inverse of a modulo m. (In all cases below, $gcd(m, a) = 1$.)

a) $a = 9$ and $m = 17$

Compute $gcd(17, 9)$: The forward pass of the Extended Euclidean Algorithm gives the tableau:

$$\begin{aligned} 17 &= 1 \times 9 + 8 \\ 9 &= 1 \times 8 + 1 \\ 8 &= 8 \times 1 + 0. \end{aligned}$$

Therefore $gcd(17, 9) = 1$ and the multiplicative inverse exists. Then, the rearranged tableau is

$$\begin{aligned} 8 &= 17 - 1 \times 9 \\ 1 &= 9 - 1 \times 8. \end{aligned}$$

Back-substituting, we get

$$\begin{aligned} 1 &= 1 \times 9 + (-1) \times 8 \\ &= 1 \times 9 + (-1) \times (17 - 1 \times 9) \\ &= 2 \times 9 - 1 \times 17. \end{aligned}$$

So 2 is the multiplicative inverse of 9 modulo 17.

b) $a = 9$ and $m = 14$

Compute $gcd(14, 9)$: The forward pass of the Extended Euclidean Algorithm gives the tableau:

$$\begin{aligned} 14 &= 1 \times 9 + 5 \\ 9 &= 1 \times 5 + 4 \\ 5 &= 1 \times 4 + 1 \\ 4 &= 4 \times 1 + 0. \end{aligned}$$

Therefore $gcd(14, 9) = 1$ and the multiplicative inverse exists. Then, the rearranged tableau is

$$\begin{aligned} 5 &= 14 - 1 \times 9 \\ 4 &= 9 - 1 \times 5 \\ 1 &= 5 - 1 \times 4. \end{aligned}$$

Back-substituting, we get

$$\begin{aligned} 1 &= 1 \times 5 - 1 \times 4 \\ &= 1 \times 5 + (-1) \times (9 - 1 \times 5) \\ &= (-1) \times 9 + 2 \times 5 \\ &= (-1) \times 9 + 2 \times (14 - 1 \times 9) \\ &= 2 \times 14 + (-3) \times 9. \end{aligned}$$

So $(-3) \times 9 \equiv 1 \pmod{14}$. The multiplicative inverse of 9 modulo 14 must also be between 0 and 13. Since $-3 \equiv 11 \pmod{14}$, we get that $11 \times 9 \equiv 1 \pmod{14}$ and 11 is the multiplicative inverse of 9 modulo 14.

c) $a = 34$ and $m = 43$

Compute $gcd(43, 34)$: The forward pass of the Extended Euclidean Algorithm gives the tableau:

$$\begin{aligned} 43 &= 1 \times 34 + 9 \\ 34 &= 3 \times 9 + 7 \\ 9 &= 1 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0. \end{aligned}$$

Therefore $gcd(43, 34) = 1$ and the multiplicative inverse exists. Then, the rearranged tableau is

$$\begin{aligned} 9 &= 43 - 1 \times 34 \\ 7 &= 34 - 3 \times 9 \\ 2 &= 9 - 1 \times 7 \\ 1 &= 7 - 3 \times 2. \end{aligned}$$

Back-substituting, we get

$$\begin{aligned} 1 &= 1 \times 7 + (-3) \times 2 \\ &= 1 \times 7 + (-3) \times (9 - 1 \times 7) \\ &= (-3) \times 9 + 4 \times 7 \\ &= (-3) \times 9 + 4 \times (34 - 3 \times 9) \\ &= 4 \times 34 + (-15) \times 9 \\ &- 4 \times 34 + (-15) \times (43 - 1 \times 34) \\ &= (-15) \times 43 + 19 \times 34. \end{aligned}$$

So, 19 is the multiplicative inverse of 34 modulo 43.