Quiz Section 4: Number Theory

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 $(\bmod m)$: 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 $(\bmod m)$:

- 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 $a = -1$.

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 $a = -b$.

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 $a \equiv b \pmod{n}$.

Task 3 – Casing the Joint

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

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 $ux > vy$.)

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

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?

b) How many tiles will you need?

Task 6 – GCD

Compute the following GCDs.

a) $gcd(9, 6)$

b) $gcd(18, 14)$

c) $gcd(80, 44)$

d) $gcd(77, 43)$

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 $m = 8$

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

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

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 $m = 17$

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

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