Section 05: Number Theory

1. GCD

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31).

(c) Find the multiplicative inverse of $6 \pmod 7$.

(d) Does 49 have an multiplicative inverse $\pmod 7$?

2. Extended Euclidean Algorithm

(a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

(b) Now, solve $7z \equiv 2 (\text{mod } 33)$ for all of its integer solutions z.

3. Euclid's Lemma[1]

(a) Show that if an integer p divides the product of two integers a and b, and $\gcd(p, a) = 1$, then p divides b.

(b) Show that if a prime p divides ab where a and b are integers, then $p \mid a$ or $p \mid b$. (Hint: Use part (a))

4. Prime Checking

You wrote the following code, `isPrime(int n)` which you are confident returns `true` if and only if n is prime (we assume its input is always positive).

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

[1]these proofs aren't much longer than proofs you've seen so far, but it can be a little easier to get stuck – use these as a chance to practice how to get unstuck if you do!

```
        potentialDiv++;
    }
    return true;
}
```

Your friend suggests replacing `potentialDiv < n` with `potentialDiv <= Math.sqrt(n)`. In this problem, you'll argue the change is ok. That is, your method still produces the correct result if n is a positive integer.

We will use "nontrivial divisor" to mean a factor that isn't 1 or the number itself. Formally, a positive integer k being a "nontrivial divisor" of n means that $k|n$, $k \neq 1$ and $k \neq n$. Claim: when a positive integer n has a nontrivial divisor, it has a nontrivial divisor at most $\sqrt{n}$.

(a) Let's try to break down the claim and understand it through examples. Show an example (a specific n and k) of a nontrivial divisor, of a divisor that is not nontrivial, and of a number with only trivial divisors.

(b) Prove the claim. Hint: you may want to divide into two cases!

(c) Informally explain why the fact about integers proved in (b) lets you change the code safely.

5. Modular Arithmetic

(a) Prove that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

(b) Prove that if $n \mid m$, where n and m are integers greater than 1, and if $a \equiv b \pmod{m}$, where a and b are integers, then $a \equiv b \pmod{n}$.