# Section 05: Number Theory

## 1. Modular Arithmetic I

Let the domain of discourse be integers. Consider the following claim:

$$\forall a \forall b((a \mid b \wedge b \mid a) \rightarrow (a = b \vee a = -b))$$

.

For this question, you may use the following fact:
**Fact 1:** $\forall a \forall b(ab = 1 \rightarrow a = 1 \vee a = -1)$

(a) Translate the claim into English.

(b) Write a formal proof that the claim holds.

(c) Translate your proof to English.

## 2. Modular Arithmetic II

Let the domain of discourse be positive integers, and let $n$ and $m$ not be equal to 1. Consider the following claim:

$$\forall n\ \forall m\ \forall a\ \forall b\ ((n \mid m \wedge a \equiv_m b) \rightarrow a(\equiv_n b))$$

.

(a) Translate the claim into English.

(b) Write a formal proof that the claim holds.

(c) Translate your proof to English.

## 3. Euclid's Lemma[1]

Let the domain of discourse be integers. Consider the following claim:

$$\forall p \forall a \forall b\ ((Prime(p) \land p \mid ab) \rightarrow (p \mid a \lor p \mid b))$$

Recall the definition of prime given in lecture:

$$Prime(p) := \neg(p = 1) \land \forall x\ ((x \mid p) \rightarrow (x = 1 \lor x = p))$$

For this question, you can use the following facts:
**Fact 1:** If an integer $p$ divides $ab$ and $\gcd(p, a) = 1$, then $p$ divides $b$.
**Fact 2:** GCD(a,b) | a and GCD(a,b) | b.

(a) Translate the claim into English.

(b) Write a formal proof that the claim holds.

(c) Translate your proof to English.

## 4. Divisors and Primes

Write an English proof of the following claim about a positive integer $n$: if the sum of the divisors of $n$ is $n + 1$, then $n$ is prime.

*Hint*: note that $n \mid n$ is always true.

## 5. Have we derived yet?

Each of the following proofs has some mistake in its reasoning - identify that mistake.

(a) *Proof.* If it is sunny, then it is not raining. It is not sunny. Therefore it is raining. □

(b) Prove that if $x + y$ is odd, either $x$ or $y$ is odd but not both.

*Proof.* Suppose without loss of generality that $x$ is odd and $y$ is even.

Then, $\exists k\ x = 2k + 1$ and $\exists m\ y = 2m$. Adding these together, we can see that $x + y = 2k + 1 + 2m = 2k + 2m + 1 = 2(k + m) + 1$. Since $k$ and $m$ are integers, we know that $k + m$ is also an integer. So, we can say that $x + y$ is odd. Hence, we have shown what is required. □

(c) Prove that $2 = 1$. :)

*Proof.* Let $a, b$ be two equal, non-zero integers. Then,

| | |
|---|---|
| $a = b$ | |
| $a^2 = ab$ | [Multiply both sides by a] |
| $a^2 - b^2 = ab - b^2$ | [Subtract $b^2$ from both sides] |
| $(a - b)(a + b) = b(a - b)$ | [Factor both sides] |
| $a + b = b$ | [Divide both sides by $a - b$] |
| $b + b = b$ | [Since $a = b$] |
| $2b = b$ | [Simplify] |
| $2 = 1$ | [Divide both sides by b] |

[1] This proof isn't much longer than what you've seen before, but it can be a little easier to get stuck — use these as a chance to practice how to get unstuck if you do!

□

(d) Prove that $\sqrt{3} + \sqrt{7} < \sqrt{20}$

*Proof.*

$$\begin{aligned}
&\sqrt{3} + \sqrt{7} < \sqrt{20} \\
&(\sqrt{3} + \sqrt{7})^2 < 20 \\
&3 + 2\sqrt{21} + 7 < 20 \\
&19.165 < 20
\end{aligned}$$

It is true that $19.165 < 20$, hence, we have shown that $\sqrt{3} + \sqrt{7} < \sqrt{20}$ □

## 6. 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 $\pmod 7$?

## 7. Extended Euclidean Algorithm

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

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

(c) Prove that the solutions to the equation from (b) are the same as the equation $5z + 1 \equiv_{33} 3 - 2z$, with an English proof.

(d) Show that the equation $22x \equiv_{33} 15$ has no solutions, with an English proof.

## 8. Efficient Modular Exponentiation

(a) Compute $2^{71} \mod 35$ using the efficient modular exponentiation algorithm.

(b) How many multiplications does the algorithm use for this computation?