**Class discussion: 24 October 2019**

**Proof by contradiction**

**Modular arithmetic**

* **Attention!** Read and reread daily, **Writing Proofs**, pg 133 – 135.

**REVIEW OF CHAPTER 5:**



**MODULAR ARITHMETIC:**



## Define a ≡ b mod m (for m > 0). Show that this is an equivalence relation on the set of integers, **Z**. In the following, assume that *a, b, c, d, m* are integers and that m > 0.

* + 1. Show that if a ≡ b mod *m*, then
			1. a + c ≡ b + c mod *m*
			2. a – c ≡ b – c mod *m*
			3. ac ≡ bc mod m
		2. Show that if ac ≡ bc mod m (and *c* is not 0) then it need not follow that a ≡ b.
		3. Show that if d = gcd(c, m) and ac ≡ bc mod m, then a ≡ b mod m/d.
		4. Show that as a special case of the above we have:

 If *c* and *m* are relatively prime and ac ≡ bc mod m, then a ≡ b mod *m*.

* + 1. Suppose that a ≡ b mod m and c ≡ d mod m. Prove that:
1. a + c ≡ b + d mod m
2. a – c ≡ b – d mod m
3. ac ≡ bd mod m
	* 1. Define addition and multiplication in Z4 and in Z5.
		2. Using modular arithmetic,
4. find the remainder when 2125 is divided by 7.
5. find the remainder when (419)(799) is divided by 5.

## Proof by Contradiction

aka ***reductio ad impossibile***

## Method

To prove a proposition $P$by contradiction:

1. Write, “We use proof by contradiction.”
2. Write, “Suppose $\~P"$
3. Deduce a logical contradiction C. (That is, find *C* for which $C∧\~C.$)
4. Write, “This is a contradiction. Therefore, *P* must be true.”

## Example

Remember that a number is *rational* if it is equal to a ratio of integers. For example, 3*.*5 = 7*/*2 and 0*.*1111…= 1*/*9 are rational numbers. On the other hand, we’ll prove by contradiction that$ \sqrt{2}$ is irrational.

**Proposition:** $\sqrt{2}$ *is* *irrational.*

*Proof.* We use proof by contradiction.

Suppose the claim is false; that is, $\sqrt{2}$ is rational.

Then we can write 2 as a fraction *a/b* in *lowest* *terms*.

Squaring both sides gives 2 = *a*2*/b*2 and so 2*b*2 = *a*2.

This implies that *a* is even; that is, *a* is a multiple of 2.

Therefore, *a*2 must be a multiple of 4. Because of the equality 2*b*2 = *a*2, we know 2*b*2 must also be a multiple of 4.

This implies that *b*2 is even and so *b* must be even. But since *a* and *b* are both even, the fraction *a/b* is not in lowest terms.

This is a contradiction. Therefore, $\sqrt{2}$ must be irrational.

## Potential Pitfall

Often students use an indirect proof when a direct proof would be simpler. Such proofs aren’t wrong; they just aren’t excellent. Let’s look at an example. A function *f* is *strictly* *increasing* if *f*(*x*) *> f*(*y*) for all real *x* and *y* such that *x > y*.

**Theorem.** *If* *f and* *g are* *strictly* *increasing* *functions,* *then* *f* + *g is* *a* *strictly* *increasing* *function.*

Let’s first look at a simple, direct proof.

*Proof.* Let *x* and *y* be arbitrary real numbers such that *x > y*. Then:

|  |  |
| --- | --- |
| *f*(*x*) *> f*(*y*)  | (since *f* is *strictly* increasing)  |
| *g*(*x*) *> g*(*y*)  | (since *g* is *strictly* increasing)  |

Adding these inequalities gives:

*f*(*x*) + *g*(*x*) *> f*(*y*) + *g*(*y*)

Thus, *f* + *g* is strictly increasing as well.

Now we *could* prove the same theorem by contradiction, but this makes the argument needlessly convoluted.

*Proof.* We use proof by contradiction. Suppose that *f* + *g* is not strictly increasing. Then there must exist real numbers *x* and *y* such that *x > y*, but

*f*(*x*) + *g*(*x*) ≤ *f*(*y*) + *g*(*y*)

This inequality can only hold if either *f*(*x*) ≤ *f*(*y*) or *g*(*x*) ≤ *g*(*y*). Either way, we have a contradiction because both *f* and *g* were defined to be strictly increasing. Therefore, *f* +*g* must actually be strictly increasing.

**Exercises** (As usual, assume unless otherwise stated, that our universe is Z.)

1. There is no smallest rational number greater than 0
2. If ais even then a2 is even. Prove by contradiction.
3. If a ≥ 2, then $a∤b or a∤(b+1)$
4. If n2 is odd, then n is odd.
5. Prove that $\sqrt[3]{2}$ is irrational.
6. Prove that a2 – 4b – 3 ≠ 0 for any integers a, b.
7. Prove that there exist no integers, a and b, such that 21a + 30b = 1.
8. If A and B are arbitrary sets, then $A⋂\left(B-A\right)=∅.$
9. Show that for any *n*, $4∤\left(n^{2}+2\right).$
10. Study the following proof (from our textbook). Is it logically correct? 

**Exercises:**

1. Prove by contradiction that there exists no largest even integer.
2. Prove by contradiction that $\sqrt[3]{1332}>11.$
3. There exist no integers a and b for which 21a+30b = 1.
4. Prove by contradiction that there exists no smallest positive real number.
5. Prove by contradiction that there exists no largest prime number. (Euclid’s proof)
6. Prove by contradiction that $\sqrt{3} is irrational.$
7. Prove by contradiction that if x is irrational, then so is x1/2.
8. Prove by contradiction that 21/3 is irrational.
9. Suppose n ∈ Z. If n is odd, then n2 is odd.
10. Suppose n ∈ Z. If n2 is odd, then n is odd.
11. Prove by contradiction that if 0 ≤ t ≤ /2, then cos t + sin t ≥ 1.
12. Let *n* be a positive integer. Prove that log2 n is rational if and only if n is a power of 2.
13. Prove the arithmetic-geometric mean inequality by contradiction.
14. Employing the method of proof by contradiction show that for any non-degenerate triangle (that is, every side has positive length), the length of the hypotenuse is *less than* the sum of the lengths of the two remaining sides.
15. Let a and b be integers. If a2 + b2 = c2, then a or b is even.
16. Prove that there are infinitely many prime numbers (Euclid).

[G. H. Hardy](https://en.wikipedia.org/wiki/G._H._Hardy) described proof by contradiction as "one of a mathematician's finest weapons," saying "It is a far finer gambit than any chess gambit: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game."

- G. H. Hardy, **A Mathematician’s Apology**