**Class discussion: 3rd October 2017**

**Proof by contrapositive**

Prove each of the following by the *contrapositive method*.

1. If x and y are two integers for which x + y is even, then x and y have the same parity.
2. If x and y are two integers whose product is even, then at least one of the two must be even.
3. If x and y are two integers whose product is odd, then both must be odd.
4. If n is a positive integer of the form n = 3k + 2, then n is not a perfect square.
5. Let x$\in Z. If x^{2}-6x+5 is even, then x is odd.$
6. Let x$, y\in Z. If 7∤xy, then 7∤x and 7∤y.$

R. Hammack, Book of Proof, chapter 5, Contrapositive Proof





## **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.

**III** Using modular arithmetic,

1. find the remainder when 2125 is divided by 7.
2. find the remainder when (419)(799) is divided by 5.



[Johann Carl Fredrich Gauss](http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html) introduced modular arithmetic.

