Notes/Tricky Questions from Examlet 2:

(5 points) Let a and b be integers, b > 0. We used two formulas to define the quotient q and the remainder r of a divided by b. One of these is a = bq + r. What is the other? Solution: $0 \le r < b$

Don't forget constraints on r

2. (6 points) Use the Euclidean algorithm to compute gcd(1702, 1221). Show your work.

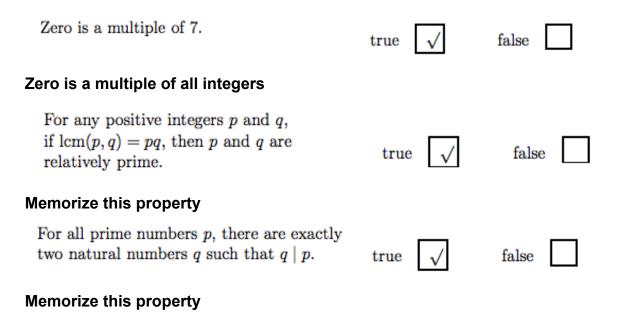
Solution: 1702 - 1221 = 481 $1221 - 481 \times 2 = 1221 - 962 = 259$ 481 - 259 = 222 259 - 222 = 37 $222 - 6 \times 37 = 0$ So gcd(1702, 1221) = 37 gcd(1702, 1221).

Memorize the Euclidean algorithm

1. (5 points) Is the following claim true? Informally explain why it is, or give a concrete counterexample showing that it is not.

Claim: For all positive integers a, b, and c, if gcd(a, bc) > 1, then gcd(a, b) > 1 and gcd(a, c) > 1. Solution: This is false. Consider a = b = 3 and c = 2. Then bc = 6. So gcd(a, bc) = 3 > 1 but gcd(a, c) = 1.

Know the properties of gcd



$k \equiv -k \pmod{7}$	true for all \boldsymbol{k}	true for some \boldsymbol{k}	\checkmark
	false for all \boldsymbol{k}		

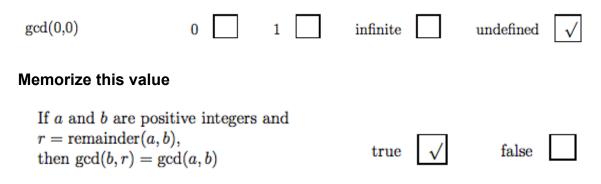
Not necessarily true for all values k

1. (5 points) Is the following claim true? Informally explain why it is, or give a concrete counterexample showing that it is not.

Claim: For all non-zero integers a and b, if $a \mid b$ and $b \mid a$, then a = b.

Solution: This is false. Consider a = 3 and b = -3. Then $a \mid b$ and $b \mid a$, but $a \neq b$.

Understand the properties of "divides"



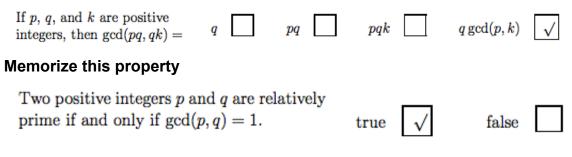
Memorize this property

 (5 points) Is the following claim true? Informally explain why it is, or give a concrete counterexample showing that it is not.

Claim: For any positive integers p and q, $p \equiv q \pmod{1}$.

Solution: This is true. $p \equiv q \pmod{1}$ is equivalent to $p - q = n \times 1 = n$ for some integer n. But we can always find an integer that will make this equation balance!

Remember what mod 1 implies



Review the definition of relatively prime

gcd(k,0) 0	k	undefined	
------------	---	-----------	--

Memorize this property

 (5 points) Is the following claim true? Informally explain why it is, or give a concrete counterexample showing that it is not.

For any positive integers s, t, p, q, if $s \equiv t \pmod{p}$ and $p \mid q$, then $s \equiv t \pmod{q}$.

Solution: Consider s = 1, t = 4, p = 3 and q = 6. Then $3 \mid 6$ and s and t are congruent mod 3, but but s and t aren't congruent mod 6.

Think of how divides and congruence mod k relate

Prove that if n is an integer, then $n^2 + 2$ is not divisible by 4.

Solution: Let n be an integer. From the Division Algorithm (aka definition of remainder), we know that there are integers q and r such that n = 4q + r.

There are five cases, depending on what the remainder r is:

Case 1: n = 4q. Then $n^2 + 2 = 16q^2 + 2 = 4(4q^2) + 2$. Case 2: n = 4q + 1. Then $n^2 + 2 = 16q^2 + 8q + 3 = 4(4q^2 + 2q) + 3$. Case 3: n = 4q + 2. Then $n^2 + 2 = 16q^2 + 16q + 6 = 4(4q^2 + 4q + 1) + 2$. Case 2: n = 4q + 3. Then $n^2 + 2 = 16q^2 + 24q + 11 = 4(4q^2 + 6q + 2) + 3$.

In all four cases, the remainder of n divided by 4 is not zero, so n isn't divisible by 4.

Be careful when using cases

For all real numbers k, m, n and r, if $r = \text{remainder}(m, n), k \mid m, \text{ and } k \mid n$, then $k \mid r$.

Solution: Let k, m, n and r be real numbers. Suppose that r = remainder(m, n), $k \mid m$, and $k \mid n$.

By the definition of remainder, m = nq + r, where q is some integer. (Also r has to be between 0 and n, but that's not required here.) So r = m - nq.

By the definition of divides, m = ks and n = kt, for some integers s and t. Substituting these into the previous equation, we get

$$r = m - nq = ks - ktq = k(s - tq)$$

s - tq is an integer because s, t, and q are integers. So r is the product of k and an integer, which means that $k \mid r$.

Don't forget what the remainder does

For all real numbers x and y, if $3x + y^2 + 2$ is odd, then x is even or y is even.

You must begin by explicitly stating the contrapositive of the claim:

Solution: Let's prove the contrapositive. That is, for all real numbers x and y, if x is odd and y is odd, then $3x + y^2 + 2$ is even.

Let x and y be real numbers. Suppose that x and y are both odd. Then there are integers p and q such that x = 2p + 1 and y = 2q + 1.

Then

$$3x + y^{2} + 2 = 3(2p + 1) + (2q + 1)^{2} + 2$$

= $(6p + 3) + (4q^{2} + 4q + 1) + 2$
= $6p + 4q^{2} + 4q + 6$
= $2(3p + 2q^{2} + 2q + 3)$

Let $t = 3p + 2q^2 + 2q + 3$. The above shows that $3x + y^2 + 2 = 2t$. Furthermore t must be an integer because p and q are integers. So $3x + y^2 + 2$ must be even.

The contrapositive allows you to avoid having to use cases in this problem

 (5 points) Is the following claim true? Informally explain why it is, or give a concrete counterexample showing that it is not.

For any positive integers s, t, p, q, if $s \equiv t \pmod{p}$ and $p \mid q$, then $s \equiv t \pmod{q}$.

Solution: Consider s = 1, t = 4, p = 3 and q = 6. Then $3 \mid 6$ and s and t are congruent mod 3, but but s and t aren't congruent mod 6.

 (5 points) Is the following claim true? Informally explain why it is, or give a concrete counterexample showing that it is not.

For any positive integers s, t, p, q, if $s \equiv t \pmod{p}$ and $q \mid p$, then $s \equiv t \pmod{q}$.

Solution: This is true.

Informally, since q is smaller, congruence mod q makes coarser distinctions than congruence mod q. So this is in the right direction and the relationship $q \mid p$ ensures that the details work out.

More formally, from $s \equiv t \pmod{p}$ and $q \mid p$, we get that s = t + pk and p = qj, where k and j are integers. So s = t + q(jk), which means that $s \equiv t \pmod{q}$.

Compare the previous two problems